OFFICIAL FILE COPY
CLERK OF THE BOARD
OF COUNTY COMMISSIONERS
MIAMI-DADE COUNTY, FLORIDA

# Memorandum

MIAMI-DADE COUNTY

**Date:** March 3, 2015

**To:** Honorable Chairman Jean Monestime
and Members, Board of County Commissioners

**From:** Carlos A. Gimenez
Mayor

Agenda Item No. 8(F)(7)

Resolution No. R-208-15

**Subject:** Recommendation for Approval to Award: Automated Passport Control Kiosks

## Recommendation

It is recommended that the Board of County Commissioners (Board) approve award of *Request for Proposals No. 00118* to SITA Information Networking Computing USA, Inc. (SITA) to provide 144 Automated Passport Control kiosks in designated U.S. Customs and Border Protection service areas at Miami International Airport (MIA).

SITA is responsible for the delivery, installation, configuration of the kiosks, including all required hardware and software components. The vendor is also responsible for: (a) rendering ongoing on-site and on-call technical and maintenance support services; (b) training up to 15 Aviation Department employees on kiosk administration, diagnostics repair and maintenance; and (c) ensuring that the kiosks satisfy U.S. Customs and Border Protection business and technical requirements.

Each year, approximately 20 million international passengers enter the United States through MIA. It is anticipated that through the use of additional kiosks at MIA, the amount of time it takes for arriving passengers to clear customs will be reduced and the overall passenger experience will be improved.

## Scope

The impact of this item is countywide in nature.

## Fiscal Impact and Funding Source

The fiscal impact for the initial five-year term is $8,970,000. If the County exercises the one (1), five-year option-to-renew, the contract's cumulative value will be $16,483,000 for ten (10) years. All kiosk maintenance support services and extended warranty fees are fixed for the initial and option terms, inclusive of all required parts, components, and consumables to ensure optimum performance based on the projection of airline passenger usage over the contract term.

Negotiations with SITA yielded a cost savings of $1.6 million between the initial proposal and the final negotiated price. As part of these negotiations, one (1) additional site administrator will work at MIA for one (1) year during the implementation phase at no cost to the Aviation Department.

| Department | Allocation | Funding Source | Contract Manager |
|---|---|---|---|
| Aviation | $8,970,000 | Proprietary Funds | Maurice Jenkins |
| **Total** | **$8,970,000** | | |

## Track Record/Monitor

Melissa Adames of the Internal Services Department is the Procurement Contracting Manager.

**Delegated Authority**

If this item is approved, the County Mayor or County Mayor's designee will have the authority to exercise all provisions of the contract pursuant to Section 2-8.1 of the County Code and Implementing Order 3-38.

**Vendor Recommended for Award**

A Request for Proposals was issued under full and open competition on September 3, 2014. Three (3) proposals were received in response to the solicitation. The Evaluation/Selection Committee recommended SITA, the highest-ranked proposer, for award based on the criteria established in the solicitation.

| Awardee | Address | Principal |
|---|---|---|
| SITA Information Networking Computing USA, Inc. | 3100 Cumberland Boulevard<br>Suite 200<br>Atlanta, GA | James Peters |

**Vendors Not Recommended for Award**

| Proposers | Reason for Not Recommending |
|---|---|
| Dedo Interactive, Inc. | Evaluation Scores/Ranking |
| Vancouver Airport Authority | |

**Due Diligence**

Pursuant to Resolution R-187-12, due diligence was conducted in accordance with the Internal Services Department's Procurement Guidelines to determine Contractor responsibility, including verifying corporate status and that there are no performance or compliance issues. The lists that were referenced include: convicted vendors, debarred vendors, delinquent contractors, suspended vendors and federal excluded parties. There were no adverse findings relating to Contractor responsibility.

**Applicable Ordinances and Contract Measures**

- The two (2) percent User Access Program provision does not apply.
- The Local Preference Ordinance was applied, but did not impact the outcome.
- The Small Business Enterprise Selection Factor was applied, but did not impact the outcome.
- The Living Wage Ordinance does not apply.

Jack Osterholt
Deputy Mayor

# MEMORANDUM

**(Revised)**

**TO:** Honorable Chairman Jean Monestime
and Members, Board of County Commissioners

**DATE:** March 3, 2015

**FROM:** R. A. Cuevas, Jr.
County Attorney

**SUBJECT:** Agenda Item No. 8(F)(7)

**Please note any items checked.**

_____ **"3-Day Rule" for committees applicable if raised**

_____ **6 weeks required between first reading and public hearing**

_____ **4 weeks notification to municipal officials required prior to public hearing**

_____ **Decreases revenues or increases expenditures without balancing budget**

_____ **Budget required**

_____ **Statement of fiscal impact required**

_____ **Ordinance creating a new board requires detailed County Mayor's report for public hearing**

_____ **No committee review**

_____ **Applicable legislation requires more than a majority vote (i.e., 2/3's ____, 3/5's ____, unanimous _____ ) to approve**

_____ **Current information regarding funding source, index code and available balance, and available capacity (if debt is contemplated) required**

Approved _____ Mayor
Veto _____
Override _____

Agenda Item No. 8(F)(7)
3-3-15

RESOLUTION NO. R-208-15

RESOLUTION APPROVING AWARD OF CONTRACT RFP 00118 FOR AUTOMATED PASSPORT CONTROL KIOSKS IN THE TOTAL AMOUNT, INCLUDING RENEWAL PERIOD, NOT TO EXCEED $16,483,000.00 FOR THE MIAMI-DADE AVIATION DEPARTMENT; AND AUTHORIZING COUNTY MAYOR OR COUNTY MAYOR'S DESIGNEE TO EXECUTE SAME AND EXERCISE ANY CANCELLATION, RENEWAL AND OTHER PROVISIONS CONTAINED THEREIN

**WHEREAS,** this Board desires to accomplish the purpose outlined in the accompanying memorandum, a copy of which is incorporated herein by reference,

**NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF COUNTY COMMISSIONERS OF MIAMI-DADE COUNTY, FLORIDA,** that this Board approves award of Contract No. RFP 00118 for Automated Passport Control Kiosks as set forth in the incorporated memorandum in the total amount, including renewal period, not to exceed $16,483,000 for the purchase of goods and services, and authorizes the County Mayor or County Mayor's designee to execute same and exercise any cancellation, renewal, and other provisions contained therein.

The foregoing resolution was offered by Commissioner **Rebeca Sosa**, who moved its adoption. The motion was seconded by Commissioner **Sally A. Heyman** and upon being put to a vote, the vote was as follows:

| | | | |
|---|---|---|---|
| Jean Monestime, Chairman | | | **aye** |
| Esteban L. Bovo, Jr., Vice Chairman | | | **absent** |
| Bruno A. Barreiro | **absent** | Daniella Levine Cava | **aye** |
| Jose "Pepe" Diaz | **aye** | Audrey M. Edmonson | **aye** |
| Sally A. Heyman | **aye** | Barbara J. Jordan | **absent** |
| Dennis C. Moss | **aye** | Rebeca Sosa | **aye** |
| Sen. Javier D. Souto | **aye** | Xavier L. Suarez | **aye** |
| Juan C. Zapata | **absent** | | |

The Chairperson thereupon declared the resolution duly passed and adopted this 3rd day of March, 2015. This resolution shall become effective upon the earlier of (1) 10 days after the date of its adoption unless vetoed by the County Mayor, and if vetoed, shall become effective only upon an override by this Board, or (2) approval by the County Mayor of this Resolution and the filing of this approval with the Clerk of the Board.

MIAMI-DADE COUNTY, FLORIDA
BY ITS BOARD OF
COUNTY COMMISSIONERS

HARVEY RUVIN, CLERK

By: ***Christopher Agrippa***
Deputy Clerk

Approved by County Attorney as
to form and legal sufficiency.

Suzanne Villano-Charif

## AUTOMATED PASSPORT CONTROL KIOSKS

THIS SOFTWARE LICENSE, EQUIPMENT/DEVICES, IMPLEMENTATION, MAINTENANCE, AND SUPPORT AGREEMENT ("AGREEMENT") IS MADE AND ENTERED BY AND BETWEEN SITA INFORMATION NETWORKING COMPUTING USA INC., A CORPORATION ORGANIZED AND EXISTING UNDER THE LAWS OF THE STATE OF DELAWARE, HAVING ITS PRINCIPAL OFFICE AT 3100 CUMBERLAND BLVD., SUITE 200, ATLANTA, GA 30339 (HEREINAFTER REFERRED TO AS THE "CONTRACTOR"), AND MIAMI-DADE COUNTY, A POLITICAL SUBDIVISION OF THE STATE OF FLORIDA, HAVING ITS PRINCIPAL OFFICE AT 111 N.W. 1ST STREET, MIAMI, FLORIDA 33128 (HEREINAFTER REFERRED TO AS THE "COUNTY");

WITNESSETH:

WHEREAS, the Contractor has offered to provide Automated Passport Control Kiosks and associated services, on a non-exclusive basis, that shall conform to the Scope of Services (Appendix A); Miami-Dade County's Request for Proposals (RFP) No. RFP-00118 and all associated addenda and attachments, incorporated herein by reference; and the requirements of this Agreement; and,

WHEREAS, the Contractor has submitted a written proposal dated September 24, 2014, hereinafter referred to as the "Contractor's Proposal" which is incorporated herein by reference; and,

WHEREAS, the County desires to procure from the Contractor such Automated Passport Control Kiosks for the County, in accordance with the terms and conditions of this Agreement;

NOW, THEREFORE, in consideration of the mutual covenants and agreements herein contained, the parties hereto agree as follows:

### ARTICLE 1. DEFINITIONS

The following words and expressions used in this Agreement shall be construed as follows, except when it is clear from the context that another meaning is intended:

a) The words "Contract" or "Agreement" to mean collectively these terms and conditions, the Scope of Services (Appendix A), all other appendices and attachments hereto, all amendments issued hereto, No. RFP-00118 and all associated addenda, and the Contractor's Proposal.

b) The words "Contract Date" to mean the date on which this Agreement is effective.

c) The words "Contract/Agreement Manager" to mean Miami-Dade County's Director, Internal Services Department, or the duly authorized representative designated to manage the Contract.

d) The word "Contractor" to mean SITA Information Networking Computing USA, Inc. and its permitted successors and assigns.

e) The word "Days" to mean Calendar Days.

f) The word "Deliverables" to mean all documentation and any items of any nature submitted by the Contractor to the County's Project Manager for review and approval pursuant to the terms of this Agreement.

g) The words "directed", "required", "permitted", "ordered", "designated", "selected", "prescribed" or words of like import to mean respectively, the direction, requirement, permission, order, designation, selection or prescription of the County's Project Manager; and similarly the words "approved", acceptable", "satisfactory", "equal", "necessary", or words of like import to mean respectively, approved by, or acceptable or satisfactory to, equal or necessary in the opinion of the County's Project Manager.

h) The word "Documentation" to mean all manuals, user documentation, and other related materials pertaining to the Software which are furnished to the County in connection with the hardware or software provided.

i) The words "Equipment" or "Devices" to mean the hardware products identified on Appendix A, "Scope of Services" to be provided by the Contractor to the County under this Agreement.

j) The words "Extra Work" or "Additional Work" to mean additions or deletions or modifications to the amount, type or value of the Work and Services as required in this Contract, as directed and/or approved by the County.

k) The words "Final Acceptance Test" to mean a test that measures the total performance of the APC Kiosks after a 30-day reliability test is performed from the "Go Live" date. The vendor shall not receive the final milestone payment until the County provides written confirmation the kiosks have passed the Final Acceptance Test.

l) The words "APC Kiosks" or "Kiosk(s)" to mean Automated Passport Control Kiosks as identified within Appendix A, "Scope of Services".

m) The words "Notice to Proceed" to mean a written notice issued by the Project Manager authorizing Contractor to proceed with the work described in this Agreement.

n) The word "Maintenance" to mean the product updates and product upgrades required for the County to achieve optimal performance of the APC Kiosk hardware and software as outlined in Appendix A, "Scope of Services".

o) The words "Project Manager" to mean the County Mayor or the duly authorized representative designated to manage the Project.

p) The words "Scope of Services" to mean the document appended hereto as Appendix A, which details the work to be performed by the Contractor.

q) The words "Support" or "Technical Support" to mean the process to resolve reported incidents through error correction, patches, hot fixes, workarounds, replacements or any of the type of correction or modification required to fully utilize the Software capabilities, as outlined in Appendix A, "Scope of Services".

r) The word "subcontractor" or "sub-consultant" to mean any person, entity, firm or corporation, other than the employees of the Contractor, who furnishes labor and/or materials, in connection with the Work, whether directly or indirectly, on behalf and/or under the direction of the Contractor and whether or not in privity of Contract with the Contractor.

s) The words "Work", "Services" "Program", or "Project" to mean all matters and things required to be done by the Contractor in accordance with the provisions of this Contract.

t) The word "CBP" to mean the United States Customs and Border Protection.

u) The words "CBP Documents" to mean U.S. CBP *Automated Passport Control Service Technical Reference Manual (Version 2, Document Number 3209000-TFM v2) in Attachment 2 and the U.S. CBP Automated Passport Control: Business Requirements (Version 16, August 2014) in Appendix F.*

v) The words "CBP ICD" to mean U.S. CBP Automated Passport Control Service Release 2.0 Interface Control Document (Document Number 3209000-ICD) in Appendix H .

## ARTICLE 2. ORDER OF PRECEDENCE

If there is a conflict between or among the provisions of this Agreement, the order of precedence is as follows: 1) these terms and conditions, 2) the Scope of Services (Appendix A), 3) CBP *Automated Passport Control Service Technical Reference Manual (Appendix G)*, 4) the Price Schedule ( Appendix B), 5) Miami-Dade County's Requests For Proposal No. RFP-00118 and any associated addenda and attachments thereof and (6) the Contractor's Proposal.

## ARTICLE 3. RULES OF INTERPRETATION

a) References to a specified Article, section or schedule shall be construed as reference to that specified Article, or section of, or schedule to this Agreement unless otherwise indicated.

b) Reference to any agreement or other instrument shall be deemed to include such agreement or other instrument as such agreement or other instrument may, from time to time, be modified, amended, supplemented, or restated in accordance with its terms.

c) The terms "hereof", "herein", "hereinafter", "hereby", "herewith", "hereto", and "hereunder" shall be deemed to refer to this Agreement.

d) The titles, headings, captions and arrangements used in these Terms and Conditions are for convenience only and shall not be deemed to limit, amplify or modify the terms of this Contract, nor affect the meaning thereof.

## ARTICLE 4. NATURE OF THE AGREEMENT

a) This Agreement incorporates and includes all prior negotiations, correspondence, conversations, agreements, and understandings applicable to the matters contained in this Agreement. The parties agree that there are no commitments, agreements, or understandings concerning the subject matter of this Agreement that are not contained in this Agreement, and that this Agreement contains the entire agreement between the parties as to all matters contained herein. Accordingly, it is agreed that no deviation from the terms hereof shall be predicated upon any prior representations or agreements, whether oral or written. It is further agreed that any oral representations or modifications concerning this Agreement shall be of no force or effect, and that this Agreement may be modified, altered or amended only by a written amendment duly executed by both parties hereto or their authorized representatives.

b) The Contractor shall provide the services set forth in the Scope of Services "Appendix A", and render full and prompt cooperation with the County in all aspects of the Services performed hereunder.

c) The Contractor acknowledges that this Agreement requires the performance of all things necessary for or incidental to the effective and complete performance of all Work and Services under this Contract. All things not expressly mentioned in this Agreement but necessary to carrying out its intent are required by this Agreement, and the Contractor shall perform the same as though they were specifically mentioned, described and delineated.

d) The Contractor shall furnish all labor, materials, tools, supplies, and other items required to perform the Work and Services that are necessary for the completion of this Contract. All Work and Services shall be accomplished at the direction of and to the satisfaction of the County's Project Manager.

e) The Contractor acknowledges that the County shall be responsible for making all policy decisions regarding the Scope of Services. The Contractor agrees to provide input on policy issues in the form of recommendations. The Contractor agrees to implement any and all changes in providing Services hereunder as a result of a policy change implemented by the County, provided SITA shall not be responsible or liable for any delays or costs due to or associated with the implementation of such policy changes. The Contractor agrees to act in an expeditious and fiscally sound manner in providing the County with input regarding the time and cost to implement said changes and in executing the activities required to implement said changes.

## ARTICLE 5. CONTRACT TERM

The Contract shall become effective on the date that it is signed by the County or the Contractor, whichever is later and continue through the last day of the 60th month. The County, at its sole discretion, reserves the right to exercise the option to renew this Contract for one (1) additional five (5) year period. The County reserves the right to exercise its option to extend this Contract for up to one hundred-eighty (180) calendar days beyond the current Contract period and will notify the Contractor in writing of the extension and the parties shall execute a mutually agreeable amendment for the extension period.

This Contract may be extended beyond the initial one hundred-eighty (180) calendar day extension period by mutual agreement between the County and the Contractor, upon approval by the Board of County Commissioners.

## ARTICLE 6. NOTICE REQUIREMENTS

All notices required or permitted under this Agreement shall be in writing and shall be deemed sufficiently served if delivered by Registered or Certified Mail, with return receipt requested; or delivered personally; or delivered via e-mail (if provided below) and followed with delivery of hard copy; and in any case addressed as follows:

(1) **to the County Project Manager:**

Miami-Dade Aviation Department
Information Systems and Telecommunications Division
P. O. 025504
Miami, Florida 33102

Attention: Maurice Jenkins, Director Information Systems and Telecommunications
Phone: 305-876-0934
Email: mjenkins@miami-airport.com

and,

**to the Agreement Manager:**

Miami-Dade County
Internal Services Department
Procurement Management Services Division
111 N.W. 1st Street, Suite 1300
Miami, FL 33128-1974

Attention: Melissa Adames, Procurement Contracting Manager
Phone: (305) 375-4029
Email: madames@miamidade.gov

(2) **To the Contractor**

SITA Information Networking Computing USA Inc.
3100 Cumberland Blvd., Suite 200
Atlanta, GA 30339

Attention: David Menzel, Account Director
Phone: (770) 548-0682
Fax: (770) 612-2265
E-mail: david.menzel@sita.aero

Either party may at any time designate a different address and/or contact person by giving notice as provided above to the other party. Such notices shall be deemed given upon receipt by the addressee.

## ARTICLE 7. DELIVERY

7.1 Delivery of the APC Kiosks shall be according to Appendix A, "Scope of Services" and Appendix C, "Project Timeline". All services performed under this Agreement are contingent upon final acceptance by the County.

7.2 Documentation. The Contractor shall provide electronic copies of the associated Documentation to the County upon Final Acceptance.

7.3 Each proposal shall be inclusive of all delivery and shipping costs for the APC Kiosks, Hardware, Parts, and Equipment throughout the term of this Agreement, including any options or extensions exercised by the County.

## ARTICLE 8. MAINTENANCE AND SUPPORT SERVICES

Contractor shall provide the County with hardware and software technical support and maintenance services in the manner outlined in Appendix A, "Scope of Services" for the APC Kiosks and associated services throughout the term of this Agreement, including any options or extensions exercised by the County. All APC Kiosk consumables, spares, and replacement parts shall be included within the cost of ongoing maintenance and support services and purchase of extended hardware warranty.

## ARTICLE 9. GRANT OF LICENSE

9.1 License. Contractor agrees to provide the County with licensed Software and Documentation in accordance with the provisions contained within this agreement.

9.2. Contractor grants the County a perpetual, non-transferrable, non-exclusive, irrevocable license to use the licensed APC Kiosk Software, Systems, Hardware/Devices and Documentation in accordance with the terms of this Agreement.

a) Contractor shall require that all of its subcontractors and suppliers grant the County, its agents, suppliers and vendors perpetual, non-transferrable, non-exclusive, irrevocable licenses to use any third party software, in both subject and object form for any purpose not expressly forbidden by the terms hereof. Such licenses shall include but not be limited to the unrestricted right by the County to provide licensed software, the Documentation and Programs therefore, to any other person(s) or entity(ies) for their use in connection with providing goods and/or services to MDAD or the County. The Contractor shall copy the third-party software in machine readable format for purposes of backup.

b) As used above, "irrevocable" means, the right of the County to continue using the licensed software or third party software irrespective of any breach or default pursuant to the terms of this Agreement

c) Contractor shall provide the County with documentation, satisfactory to MDAD, confirming that the Contractor has acquired on the County's behalf all software licenses required hereunder.

## ARTICLE 10. SYSTEM ENHANCEMENTS OR MODIFICATIONS

10.1 System Enhancements or Modifications. The County may, from time to time, under the performance of the Agreement request that the Contractor incorporate certain features, enhancements or modifications into the System to adhere to the changing United States (US) Automated Passport Control Business Requirements or the business requirements of the County. When requested by the County, the Contractor shall provide the requested system enhancements or modifications subject to necessary review and final approval of US CBP and agreement subsequent Statement of Work or Work Order. Upon the County's request for System enhancements/modifications, the County shall prepare a Statement of Work ("SOW") for the specific Project that shall define in detail the Services to be performed and

requirements the enhancement/modification the System must meet. The Contractor shall submit a proposal outlining how the work will be completed including all costs pertaining to furnishing the County with the requested system enhancements/modifications.

a) After the SOW has been accepted a detailed requirements and detailed design document shall be submitted illustrating the complete financial terms that govern the SOW, proposed Project staffing, anticipated Project schedule, and other information relevant to the Project. Each SOW executed hereunder shall automatically incorporate the terms and conditions of this Agreement.

b) Following the County's acceptance of all enhancements/modification, the Contractor shall provide the County, if so requested with written confirmation of the date the enhancements/modification was applied to the System, and any and all Documentation relating to the Software and or enhancements/modification thereto.

c) The Contractor shall provide the County, at no cost, all updates and upgrades required to specifically maintain the integrity, security, and operation of the kiosk software to the US CBP APC Business Requirements and comply with US CBP APC Business Requirements.

i. All updates, and upgrades provided by the Contractor exclude future CBP phase introduction, APC client workflow re-architecture, Phase 4 Visitors, Facial Recognition/Matching, or integration with mobile passport control.

ii. Any requests made by the County for future enhancements listed above, outside of the defined Scope of Services (Appendix A) shall be billed on a time and materials basis in accordance with the outlined price schedule defined within Appendix B.

## ARTICLE 11. SOFTWARE ESCROW

The County requires that the Contractor maintain a software escrow account throughout the life of the Agreement to protect against failure of the Contractor to provide the agreed upon services. A copy of the Contractor's licensed software source code, and Contractor enhancements or modifications or customization or Developed Works of source code is to be kept by a trusted third party to ensure that the County will have access to the source code in the event that the Contractor is unable to support the software. The Contractor is required to maintain the most current version of the application with the escrow agent including, but not limited to all incremental releases and upgrades as well as any System enhancements, modifications, or Developed Works created for the County. The terms and conditions associated with such software escrow services are outlined in Appendix F, "Escrow Agreement."
Solely in the event of a release event as defined under the Escrow Agreement, the Contractor grants to County, a non-exclusive, perpetual, paid in full license, to install, use, copy, publicly perform and digitally perform, modify and create derivative works, for the sole purpose of continuing the benefits afforded to the County under this Agreement, including the development of patches and upgrades solely for County's internal use. County shall have a right to modify and customize the Software, or to have the Software modified and customized by third-parties.

## ARTICLE 12. IMPLEMENTATION SERVICES

a) The County shall accept or reject the APC Kiosks within fifteen business (15) days of receipt which commences after the completion of installation, implementation, configuration and testing by Contractor unless otherwise provided elsewhere in this Agreement.

b) If the Contractor fails to provide deliverables within the time specified or if the APC Kiosks delivered fails to conform to the requirements or are found to be defective in material or workmanship, then the County may reject the delivered APC Kiosks or may accept some items and reject the balance of the delivered APC Kiosks. The County shall notify Contractor of such rejection in writing and specify in such notice, the reasons for such rejection. Contractor agrees to deliver a fix or workaround replacement of the APC Kiosks for such rejected

items within fifteen (15) business days of Contractor's receipt of the County's rejection notice.

c) The Contractor shall bear the risk of loss or damage to delivered APC Kiosks until the time the Project Manager certifies that the kiosks have successfully completed the Final Acceptance test whether such loss or damage arises from acts or omissions (whether negligent or not) of the Contractor or the County or from any other cause whatsoever, except loss or damage arising solely from the negligence or willful acts of the County.

d) Contractor agrees to install, implement and test APC Kiosks in specified locations at MIA facilities. Contractor agrees and acknowledges that Contractor will not have exclusive access to said locations during installation, implementation and testing as the location will be usable to traveling passengers, CBP agents and MDAD staff. Contractor further agrees and acknowledges that no barriers (walls, screens, etc.) will be erected in said location during installation, implementation and testing. Contractor agrees to commence installation of the APC Kiosks according to the Implementation Timeline herein attached as Appendix C unless a different time for implementation is otherwise mutually agreed upon by the parties hereto. All implementation services will be performed during normal business hours. Whenever possible, however some services to be provided may be required outside of normal business hours to accommodate County operations. Work to be performed outside normal business hours will be mutually agreed by both parties. Contractor shall diligently pursue and complete such implementation services in accordance with the Implementation Schedule, so that such the APC Kiosks are in good working order and ready for use by the dates set forth in the Schedule.

e) Contractor agrees to do all things necessary for proper implementation of the APC Kiosks and to perform its implementation obligations hereunder in an orderly, skillful and expeditious manner, with sufficient labor and materials to ensure efficient and timely completion of such obligations. If applicable, Contractor shall coordinate with the Project Manager all work with all other Contractors and/or County personnel performing work to complete APC Kiosk installation. The County shall be responsible for resolving all disputes relating to Site access between Contractor and/or County personnel. Contractor shall provide all materials necessary to properly implement the APC Kiosks. The County shall attempt to provide reasonable working and secure storage space for the performance by Contractor of the implementation services described herein.

f) Unless otherwise agreed to by the County, Contractor agrees as part of the implementation to perform all required services to successfully achieve all objectives set forth in the scope of work , including, but not limited to, (a) system configuration; (b) interface development ; (c) software testing; (d) acceptance and user acceptance testing; (e) training; (f) cooperating with all other vendors supplying peripheral or ancillary equipment that will interface with the APC Kiosks; and (g) any additional services necessary to ensure Contractor's compliance with this Article 12.

g) Testing shall consist of the tests described in the Scope of Services which are to be conducted collectively by the Contractor and the County. The purpose of these tests is to demonstrate the complete operability of the APC Kiosks in conformance with the requirements of the Contract. This will include an actual demonstration of all required functionality. All tests shall be in accordance with test plans and procedures prepared by Contractor and previously approved by the County. In the event of any outstanding deficiencies at the conclusion of installation testing, as determined by the County, Contractor shall be responsible for instituting necessary corrective measures, and for subsequently satisfactorily demonstrating and/or re-demonstrating system performance.

**ARTICLE 13. TESTS**

The Contractor shall configure and program the APC Kiosks to conform to the Scope of Services herein attached as "Appendix A". The APC Kiosks will be subject to several tests, including a Final Acceptance test as further defined in the Scope of Services, Implementation Plan, and Acceptance Criteria to be developed by both parties and pending final approval from MDAD to assure System performance, the County's Project Manager will coordinate all testing of the APC Kiosks and provide Final Acceptance upon completion of all milestones and deliverables as outlined in the Scope of

Services.

Final acceptance cannot occur until all designated tests from the preliminary acceptance list have been resolved. The selected Proposer shall provide a checklist (report) for all kiosk hardware, software, and training in a form acceptable to the County and CBP. Final acceptance is described as "equipment delivered, installed and tested to meet CBP specifications for the hardware, equipment, software, and CBP interface" to the satisfaction of the County and CBP. Failure of the APC Kiosks to satisfy the acceptance criteria and conform to the requirements set forth in the Scope of Services by the timeframes set forth in the Implementation Timeline herein attached as "Appendix C" may result in the County withholding payment until satisfactory acceptance is granted to the Contractor.

After Final Acceptance is granted, any modifications, fixes, enhancements, and/or new releases of the APC Kiosks and associated software require separate testing periods and sign-off from the County Project Manager prior to migrating it into the production software. The testing protocol shall be as follows:

a) Contractor's Project Manager will provide written notice to the County Project Manager of modifications, fixes, enhancements, and/or new releases of the software available for testing.
b) The Contractor's Project Manager will coordinate all user acceptance testing dates, acceptance criteria, and training for the new functionality for the test group.
c) The County will be granted five (5) business days or other timeframe agreed to by both parties in writing to perform testing based on the outlined functionality being delivered to the County on the Acceptance Criteria sign off sheet;
d) The County's Project Manager will provide the Contractor with written notice of acceptance (sign-off) or rejection (with documented material nonconformities in the functionality) within 15 business days, unless more time is needed, in which case the County will notify the Contractor in writing accordingly;
e) Deficiencies found will be noted on the Acceptance Criteria sign off sheet and the Contractor will be provided an opportunity to correct the issues. The Contractor will be required to provide the County with an updated timeline and work around (fix) within three (3) business days unless additional time is requested in writing and agreed by both parties;
f) Once the release is accepted, the functionality will be moved into the production module. And updated documentation will be provided to the County.

## ARTICLE 14. REVIEWING DELIVERABLES

The Contractor agrees to submit all Deliverables required to be submitted for review and approval by the County in accordance with the specific requirements in the Scope of Services, and as specified in Appendix D "Acceptance Criteria". The Contractor understands that the County shall have final approval on all Deliverables.

In reviewing the Deliverables, the Contractor understands that the County will provide the Contractor with:

i. a written notification of the County's approval,

ii. a written notification that each Deliverable is approved subject to the Contractor providing prompt correction of a minor deficiency, or,

iii. in the case of a Deliverable that does not meet the requirements of the Agreement, a written notification of the County's disapproval. The County's disapproval notification will state with reasonable detail to sufficiently advise the Contractor of the basis on which the Deliverable was determined to be unacceptable.

The Contractor understands that failure by the County to provide a notice of approval does not constitute approval.

Furthermore:

a) For each Deliverable made hereunder, the County shall have ten (10) business days, commencing on the first business day after receipt by the County of the Deliverable, to determine whether the Deliverable is approved as submitted, is approved subject to the correction by the Contractor of minor discrepancies, or whether it is unacceptable and therefore disapproved.

b) Unless an extension of time has been granted by the County, within five business days after receipt of the County's notification of "disapproval", the Contractor shall deliver to the County the necessary revisions and/or modifications for a second review by the County.

c) If after the second review period the Deliverable remains unacceptable for the County's approval, the County may direct the Contractor to:

   a. Proceed with the Work subject to the correction of all outstanding deficiencies which led to the County's determination that a Deliverable was not acceptable for approval on or before a specific date established by the County for correcting such deficiency or deficiencies; or,

   b. Suspend all Work being performed in regard to the execution of the Agreement, except those services necessary for the correction of outstanding deficiencies, until such time that all such outstanding deficiencies have been corrected by the Contractor and resubmitted to the County for approval. Any suspension of the Work under this provision shall not alter the County's right to assess liquidated damages in the event that the Work are not completed in accordance with other provisions of this Agreement.

d) The County shall have the right to approve or accept part of any Deliverable. Any such approval shall be regarded as partial and conditional upon the County's approval or acceptance of all aspects of the Deliverable. The Contractor must correct any deficiencies within the time the County specifies for such correction in the County's notice concerning a partial approval (including approvals subject to correction of minor deficiencies) or, if no time is given, promptly. If the County does not subsequently approve or accept all aspects of the Deliverable, the earlier conditional acceptance or approval may, in the sole absolute discretion of the County, be regarded as void and of no effect.

**ARTICLE 15. SYSTEM WARRANTY**

The Contractor warrants at no cost to the County, for a period of one (1) year from the County's Final Acceptance, that the System(s) and all related components provided by the Contractor under the performance of this Agreement shall:

(i) Be free from defects in material and workmanship under normal use and remain in good working order, wear and tear excepted;

(ii) Function properly and in conformity with the warranties in this Agreement;

(iii) Meet the performance standards set forth in the Scope of Work and the Original Equipment Manufacture's published specifications.

During the Warranty Period, Contractor agrees to use all reasonable efforts and resources to provide to the County all corrections and/or modifications necessary to correct problems with the Equipment/Devices provided by the Contractor that are reported to Contractor, at no additional cost to the price identified in the Price Schedule or to provide a full refund of any amounts paid under this contract and accept the return of the System in the sole discretion of the County.

During the Warranty Period, Contractor shall enforce the manufacturer's warranty and maintenance obligations relating to

the Equipment/Devices and related Software it provides.

In the event the Software System(s) does not satisfy the conditions of performance set forth in the Scope of Services, Solicitation, and Contractor's proposal, the Contractor's obligation is to provide a Fix or a Work Around at the Contractor's cost and expense, or to provide different equipment, software and services required to attain the performance requirements set forth in the Scope of Services, Solicitation, and Contractor's proposal or to provide a full refund of any amounts paid under this contract and accept the return of the System in the sole discretion of the County. Failure by the Contractor to comply with warranty provisions hereof may be deemed by the County as a breach of the Contractor's obligations hereof.

The Contractor shall provide an extended warranty that shall meet the same system warranty coverage as described above and provided during the first year factory warranty period.

## ARTICLE 16. THIRD PARTY WARRANTIES

In addition to the foregoing warranties, the Contractor hereby assigns to the County, and the County shall have the benefit of, any and all subcontractors' and suppliers' warranties and representations with respect to the Solution provided hereunder. In the Contractor's agreements with subcontractors and suppliers, the Contractor shall require that such parties (i) consent to the assignment of such warranties and representations to the County; (ii) agree that such warranties and representations are enforceable by the County in its own name; and (iii) furnish to the County, the warranties and obligations as set forth in Articles 15 "System Warranty".

## ARTICLE 17. FEES AND PAYMENT

17.1 Fees. The County shall pay the Fees or other considerations for the Software, Equipment, and Documentation as set forth on Appendix B "Price Schedule" attached hereto. All amounts payable hereunder by the County shall be payable to the Contractor upon invoice as defined in Appendix B. The County shall have no obligation to pay the Contractor or any additional sum in excess of this amount, except for a change and/or modification to the Agreement, which is approved and executed in writing by the County and the Contractor. All Services undertaken by the Contractor prior to the County's approval of this Agreement shall be done at the Contractor's risk and expense.

17.2 Travel. With respect to travel costs and travel related expenses, the Contractor agrees to adhere to CH. 112.061 of the Florida Statutes as they pertain to out-of-pocket expenses including employee lodging, transportation, per diem, and all miscellaneous cost-and fees. The County shall not be liable for any such expenses that have not been approved in advance, in writing, by the County.

17.3 Fixed Pricing. Prices shall remain firm and fixed for the term of the Agreement, including any option or extension periods; however, the Contractor may offer incentive discounts to the County at any time during the Agreement term, including any renewal or extension thereof.

## ARTICLE 18. METHOD AND TIMES OF PAYMENT

The Contractor agrees that under the provisions of this Agreement, as reimbursement for those actual, reasonable and necessary costs incurred by the Contractor, which are directly attributable or properly allocable to the Services, the Contractor may invoice the County periodically, pursuant to Appendix B – Price Schedule. All invoices shall be taken from the books of account kept by the Contractor, shall be supported by copies of payroll distribution, receipt bills or other documents reasonably required by the County, shall show the County's contract number, and shall have a unique invoice number assigned by the Contractor. It is the policy of Miami-Dade County that payment for all purchases by County agencies and the Public Health Trust shall be made in a timely manner and that interest payments be made on late payments. In accordance with Florida Statutes, Section 218.74 and Section 2-8.1.4 of the Miami-Dade County Code, the time at which payment shall be due from the County or the Public Health Trust shall be forty-five (45) days from receipt of a proper invoice. The time at which payment shall be due to small businesses shall be thirty (30) days from receipt of a

proper invoice. All payments due from the County or the Public Health Trust, and not made within the time specified by this section shall bear interest from thirty (30) days after the due date at the rate of one percent (1%) per month on the unpaid balance. Further, proceedings to resolve disputes for payment of obligations shall be concluded by final written decision of the County Mayor, or his or her designee(s), not later than sixty (60) days after the date on which the proper invoice was received by the County or the Public Health Trust.

In accordance with Miami-Dade County Implementing Order 3-9, Accounts Receivable Adjustments, if money is owed by the Contractor to the County, whether under this Contract or for any other purpose, the County reserves the right to retain such amount from payment due by County to the Contractor under this Contract. Such retained amount shall be applied to the amount owed by the Contractor to the County. The Contractor shall have no further claim to such retained amounts which shall be deemed full accord and satisfaction of the amount due by the County to the Contractor for the applicable payment due herein.

Invoices and associated back-up documentation shall be submitted in duplicate by the Contractor to the County as follows:

Miami-Dade Aviation Department
Information Systems and Telecommunications Division
P. O. 025504
Miami, Florida 33102

Attention: Maurice Jenkins, Director Information Systems and Telecommunications
Phone: 305-876-0934
E-mail: mjenkins@miami-airport.com

The County may at any time designate a different address and/or contact person by giving written notice to the other party.

## ARTICLE 19. INDEMNIFICATION AND INSURANCE

The Contractor shall defend, indemnify, and save harmless the County, and its officers, employees, agents and instrumentalities (collectively "Indemnitees"), from any and all claims, demands, liability, losses or damages, including attorneys' fees and costs of defense, which the County or its officers, employees, agents or instrumentalities may incur as a result of claims, demands, suits, causes of action or proceedings of any kind or nature arising to or resulting from the performance of this Agreement by the Contractor or its employees, agents, servants, partners, principals or subcontractors except as expressly limited herein. The Contractor shall pay all claims and losses of any nature whatsoever in connection therewith and shall investigate and defend all claims, suits or actions of any kind or nature in the name of the county, when applicable, including appellate proceedings, and shall pay all costs, judgments and attorney's fees which may issue thereon; provided however, that the Contractor's obligation to indemnify or hold harmless the Indemnitees for damages to persons or property caused in whole or in part by any act, omission, or default of any Indemnitee arising from the contract or its performance shall be limited to the greater of $1 million ($1,000,000.00) or the Contract amount. This indemnification provision is in addition to and cumulative with any other right of indemnification or contribution which any Indemnitee may have in law, equity, or otherwise. The Contractor expressly understands and agrees that any insurance protection required by this Agreement or otherwise provided by the Contractor shall in no way limit the responsibility to indemnify, keep and save harmless and defend the County or its officers, employees, agents and instrumentalities as herein provided.

Upon County's notification, the Contractor shall furnish to the Internal Services Department, Procurement Management Division, Certificates of Insurance that indicate that insurance coverage has been obtained, which meets the requirements as outlined below:

A. Worker's Compensation Insurance for all employees of the Contractor as required by Florida Statute 440.

B. Commercial General Liability Insurance in an amount not less than $1,000,000 combined single limit per occurrence for bodily injury and property damage. Miami-Dade County must be shown as an additional insured with respect to this coverage. The mailing address of Miami-Dade County 111 N.W. 1st Street, Suite 1300, Miami, Florida 33128-1974, as the certificate holder, must appear on the certificate of insurance.

C. Automobile Liability Insurance covering all owned, non-owned and hired vehicles used in connection with the work, in an amount not less than *$1,000,000 combined single limit per occurrence for bodily injury and property damage.

D. Professional Liability Insurance in an amount not less than $1,000,000 per claim.

*Under no circumstances are Contractors permitted on the Aviation Department, Aircraft Operating Airside (A.O.A) at Miami International Airport without increasing automobile coverage to $5 million. Only vehicles owned or leased by a company will be authorized. Vehicles owned by individuals will not be authorized. $1 million limit applies at all other airports.

The insurance coverage required shall include those classifications, as listed in standard liability insurance manuals, which most nearly reflect the operation of the Contractor. All insurance policies required above shall be issued by companies authorized to do business under the laws of the State of Florida with the following qualifications:

The company must be rated no less than "A-" as to management, and no less than "Class VII" as to financial strength by Best's Insurance Guide, published A.M. Best Company, Oldwick, New Jersey, or its equivalent, subject to the approval of the County Risk Management Division.

OR

The company must hold a valid Florida Certificate of Authority as shown in the latest "List of All Insurance Companies Authorized or Approved to Do Business in Florida", issued by the State of Florida Department of Financial Services and are members of the Florida Guaranty Fund.

Certificates of Insurance must indicate that for any cancellation of coverage before the expiration date, the issuing insurance carrier will endeavor to mail thirty (30) day written advance notice to the certificate holder. In addition, the Contractor hereby agrees not to modify the insurance coverage without thirty (30) days written advance notice to the County.

Compliance with the foregoing requirements shall not relieve the Contractor of this liability and obligation under this section or under any other section in this Agreement.

Award of this Contract is contingent upon the receipt of the insurance documents, as required, within ten (10) business days. If the insurance certificate is received within the specified timeframe but not in the manner prescribed in this Agreement, the Contractor shall have an additional five (5) business days to submit a corrected certificate to the County. If the Contractor fails to submit the required insurance documents in the manner prescribed in this Agreement within fifteen (15) business days, the Contractor shall be in default of the contractual terms and conditions and award of the Contract may be rescinded, unless such timeframe for submission has been extended by the County.

The Contractor shall be responsible for ensuring that the insurance certificates required in conjunction with this Section remain in force for the duration of the contractual period of the Contract, including any and all option years or extension periods that may be granted by the County. If insurance certificates are scheduled to expire during the contractual

period, the Contractor shall be responsible for submitting new or renewed insurance certificates to the County at a minimum of thirty (30) calendar days in advance of such expiration. In the event that expired certificates are not replaced with new or renewed certificates which cover the contractual period, the County shall suspend the Contract until such time as the new or renewed certificates are received by the County in the manner prescribed herein; provided, however, that this suspended period does not exceed thirty (30) calendar days. Thereafter, the County may, at its sole discretion, terminate this contract.

## ARTICLE 20. MANNER OF PERFORMANCE

a) The Contractor shall provide the Services described herein in a competent and professional manner satisfactory to the County in accordance with the terms and conditions of this Agreement. The County shall be entitled to a satisfactory performance of all Services described herein and to full and prompt cooperation by the Contractor in all aspects of the Services. At the request of the County, the Contractor shall promptly remove from the project any Contractor's employee, subcontractor, or any other person performing Services hereunder. The Contractor agrees that such removal of any of its employees does not require the termination or demotion of any employee by the Contractor.

b) The Contractor agrees to defend, hold harmless and indemnify the County and shall be liable and responsible for any and all claims, suits, actions, damages and costs (including attorney's fees and court costs) made against the County, occurring on account of, arising from or in connection with the removal and replacement of any Contractor's personnel performing services hereunder at the behest of the County. Removal and replacement of any Contractor's personnel as used in this Article shall not require the termination and or demotion of such Contractor's personnel.

c) The Contractor agrees that at all times it will employ, maintain and assign to the performance of the Services a sufficient number of competent and qualified professionals and other personnel to meet the requirements to which reference is hereinafter made. The Contractor agrees to adjust its personnel staffing levels or to replace any its personnel if so directed upon reasonable request from the County, should the County make a determination, in its sole discretion, that said personnel staffing is inappropriate or that any individual is not performing in a manner consistent with the requirements for such a position.

d) The Contractor warrants and represents that its personnel have the proper skill, training, background, knowledge, experience, rights, authorizations, integrity, character and licenses as necessary to perform the Services described herein, in a competent and professional manner.

e) The Contractor shall at all times cooperate with the County and coordinate its respective work efforts to most effectively and efficiently maintain the progress in performing the Services.

f) The Contractor shall comply with all provisions of all federal, state and local laws, statutes, ordinances, and regulations that are applicable to the performance of this Agreement.

## ARTICLE 21. EMPLOYEES OF THE CONTRACTOR

All employees of the Contractor shall be considered to be, at all times, employees of the Contractor under its sole direction and not employees or agents of the County. The Contractor shall supply competent employees. Miami-Dade County may require the Contractor to remove an employee it deems careless, incompetent, insubordinate or otherwise objectionable and whose continued employment on County property is not in the best interest of the County. Each employee shall have and wear proper identification.

## ARTICLE 22. INDEPENDENT CONTRACTOR RELATIONSHIP

The Contractor is, and shall be, in the performance of all work services and activities under this Agreement, an independent contractor, and not an employee, agent or servant of the County. All persons engaged in any of the work or services performed pursuant to this Agreement shall at all times, and in all places, be subject to the Contractor's sole

direction, supervision and control. The Contractor shall exercise control over the means and manner in which it and its employees perform the work, and in all respects the Contractor's relationship and the relationship of its employees to the County shall be that of an independent contractor and not as employees and agents of the County.

The Contractor does not have the power or authority to bind the County in any promise, agreement or representation other than specifically provided for in this Agreement.

## ARTICLE 23. AUTHORITY OF THE COUNTY'S PROJECT MANAGER

a) The Contractor hereby acknowledges that the County's Project Manager will determine in the first instance all questions of any nature whatsoever arising out of, under, or in connection with, or in any way related to or on account of, this Agreement including without limitations: questions as to the value, acceptability and fitness of the Services; questions as to either party's fulfillment of its obligations under the Contract; negligence, fraud or misrepresentation before or subsequent to acceptance of the Contractor's Proposal; questions as to the interpretation of the Scope of Services; and claims for damages, compensation and losses. The Project Manager is not authorized to waive or modify this agreement without authority from the Board of County Commissioners.

b) The Contractor shall be bound by all determinations or orders and shall promptly comply with every order of the Project Manager, including the withdrawal or modification of any previous order and regardless of whether the Contractor agrees with the Project Manager's determination or order. Where orders are given orally, they will be issued in writing by the Project Manager as soon thereafter as is practicable.

c) The Contractor must, in the final instance, seek to resolve every difference concerning the Agreement with the Project Manager. In the event that the Contractor and the Project Manager are unable to resolve their difference, the Contractor may initiate a dispute in accordance with the procedures set forth in this Article. Exhaustion of these procedures shall be a condition precedent to any lawsuit permitted hereunder.

d) In the event of such dispute, the parties to this Agreement authorize the County Mayor or designee, who may not be the Project Manager or anyone associated with this Project, acting personally, to decide all questions arising out of, under, or in connection with, or in any way related to or on account of the Agreement (including but not limited to claims in the nature of breach of contract, fraud or misrepresentation arising either before or subsequent to execution hereof) and the decision of each with respect to matters within the County Mayor's purview as set forth above shall be conclusive, final and binding on parties. Any such dispute shall be brought, if at all, before the County Mayor within 10 days of the occurrence, event or act out of which the dispute arises.

e) The County Mayor may base this decision on such assistance as may be desirable, including advice of experts, but in any event shall base the decision on an independent and objective determination of whether Contractor's performance or any Deliverable meets the requirements of this Agreement and any specifications with respect thereto set forth herein. The effect of any decision shall not be impaired or waived by any negotiations or settlements or offers made in connection with the dispute, whether or not the County Mayor participated therein, or by any prior decision of others, which prior decision shall be deemed subject to review, or by any termination or cancellation of the Agreement. All such disputes shall be submitted in writing by the Contractor to the County Mayor for a decision, together with all evidence and other pertinent information in regard to such questions, in order that a fair and impartial decision may be made. Whenever the County Mayor is entitled to exercise discretion or judgment or to make a determination or form an opinion pursuant to the provisions of this Article, such action shall be fair and impartial when exercised or taken. The County Mayor, as appropriate, shall render a decision in writing and deliver a copy of the same to the Contractor. Except as such remedies may be limited or waived elsewhere in the Agreement, Contractor reserves the right to pursue any remedies available under law after exhausting the provisions of this Article.

## ARTICLE 24. MUTUAL OBLIGATIONS

a) This Agreement, including attachments and appendices to the Agreement, shall constitute the entire Agreement between the parties with respect hereto and supersedes all previous communications and representations or agreements, whether written or oral, with respect to the subject matter hereto unless acknowledged in writing by the duly authorized representatives of both parties.

b) Nothing in this Agreement shall be construed for the benefit, intended or otherwise, of any third party that is not a parent or subsidiary of a party or otherwise related (by virtue of ownership control or statutory control) to a party.

c) In those situations where this Agreement imposes an indemnity obligation on the Contractor, the County may, at its expense, elect to participate in the defense if the County should so choose. Furthermore, the County may at its own expense defend or settle any such claims if the Contractor fails to diligently defend such claims, and thereafter seek indemnity for costs from the Contractor.

**ARTICLE 25. QUALITY ASSURANCE/QUALITY ASSURANCE RECORD KEEPING**

The Contractor shall maintain, and shall require that its subcontractors and suppliers maintain, complete and accurate records to substantiate compliance with the requirements set forth in the Scope of Services. The Contractor and its subcontractors and suppliers, shall retain such records, and all other documents relevant to the Services furnished under this Agreement for a period of three (3) years from the expiration date of this Agreement and any extension thereof.

**ARTICLE 26. AUDITS**

The County, or its duly authorized representatives or governmental agencies, shall until the expiration of three (3) years after the expiration of this Agreement and any extension thereof, have access to and the right to examine and reproduce any of the Contractor's books, documents, papers and records and of its subcontractors and suppliers which apply to all matters of the County. Such records shall subsequently conform to Generally Accepted Accounting Principles requirements, as applicable, and shall only address those transactions related to this Agreement.

Pursuant to Section 2-481 of the Miami-Dade County Code, the Contractor will grant access to the Commission Auditor to all financial and performance related records, property, and equipment purchased in whole or in part with government funds. The Contractor agrees to maintain an accounting system that provides accounting records that are supported with adequate documentation, and adequate procedures for determining the allowability and allocability of costs.

**ARTICLE 27. SUBSTITUTION OF PERSONNEL**

In the event the Contractor wishes to substitute personnel for the key personnel identified by the Contractor's Proposal, the Contractor must notify the County in writing and request written approval for the substitution at least ten (10) business days prior to effecting such substitution.

**ARTICLE 28. CONSENT OF THE COUNTY REQUIRED FOR ASSIGNMENT**

The Contractor shall not assign, transfer, convey or otherwise dispose of this Agreement, including its rights, title or interest in or to the same or any part thereof without the prior written consent of the County.

**ARTICLE 29. SUBCONTRACTUAL RELATIONS**

a) If the Contractor will cause any part of this Agreement to be performed by a Subcontractor, the provisions of this Contract will apply to such Subcontractor and its officers, agents and employees in all respects as if it and they were employees of the Contractor; and the Contractor will not be in any manner thereby discharged from its obligations and liabilities hereunder, but will be liable hereunder for all acts and negligence of the Subcontractor, its officers, agents, and employees, as if they were employees of the Contractor. The services performed by the Subcontractor will be subject to the provisions hereof as if performed directly by the Contractor.

b) The Contractor, before making any subcontract for any portion of the services, will state in writing to the County the

name of the proposed Subcontractor, the portion of the Services which the Subcontractor is to do, the place of business of such Subcontractor, and such other information as the County may require. The County will have the right to require the Contractor not to award any subcontract to a person, firm or corporation disapproved by the County.

c) Before entering into any subcontract hereunder, the Contractor will inform the Subcontractor fully and completely of all provisions and requirements of this Agreement relating either directly or indirectly to the Services to be performed. Such Services performed by such Subcontractor will strictly comply with the requirements of this Contract.

d) In order to qualify as a Subcontractor satisfactory to the County, in addition to the other requirements herein provided, the Subcontractor must be prepared to prove to the satisfaction of the County that it has the necessary facilities, skill and experience, and ample financial resources to perform the Services in a satisfactory manner. To be considered skilled and experienced, the Subcontractor must show to the satisfaction of the County that it has satisfactorily performed services of the same general type which is required to be performed under this Agreement.

e) The County shall have the right to withdraw its consent to a subcontract if it appears to the County that the subcontract will delay, prevent, or otherwise impair the performance of the Contractor's obligations under this Agreement. All Subcontractors are required to protect the confidentiality of the County's and County's proprietary and confidential information. Contractor shall furnish to the County copies of all subcontracts between Contractor and Subcontractors and suppliers hereunder. Within each such subcontract, there shall be a clause for the benefit of the County in the event the County finds the Contractor in breach of this Contract, permitting the County to request completion by the Subcontractor of its performance obligations under the subcontract. The clause shall include an option for the County to pay the Subcontractor directly for the performance by such Subcontractor. Notwithstanding, the foregoing shall neither convey nor imply any obligation or liability on the part of the County to any subcontractor hereunder as more fully described herein.

## ARTICLE 30. ASSUMPTION, PARAMETERS, PROJECTIONS, ESTIMATES AND EXPLANATIONS

The Contractor understands and agrees that any assumptions, parameters, projections, estimates and explanations presented by the County were provided to the Contractor for evaluation purposes only. However, since these assumptions, parameters, projections, estimates and explanations represent predictions of future events the County makes no representations or guarantees; and the County shall not be responsible for the accuracy of the assumptions presented; and the County shall not be responsible for conclusions to be drawn therefrom; and any assumptions, parameters, projections, estimates and explanations shall not form the basis of any claim by the Contractor. The Contractor accepts all risk associated with using this information.

## ARTICLE 31. SEVERABILITY

If this Agreement contains any provision found to be unlawful, the same shall be deemed to be of no effect and shall be deemed stricken from this Agreement without affecting the binding force of this Agreement as it shall remain after omitting such provision.

## ARTICLE 32. TERMINATION AND SUSPENSION OF WORK

a) The County may terminate this Agreement if an individual or corporation or other entity attempts to meet its contractual obligation with the County through fraud, misrepresentation or intentional material misstatement.

b) The County may, as a further sanction, terminate or cancel any other contract(s) that such individual or corporation or other entity has with the County and that such individual, corporation or other entity shall be responsible for all direct and indirect costs associated with such termination or cancellation, including attorney's fees.

c) The foregoing notwithstanding, any individual, corporation or other entity which attempts to meet its contractual obligations with the County through fraud, misrepresentation or material misstatement may be debarred from County contracting for up to five (5) years in accordance with the County debarment procedures. The Contractor

may be subject to debarment for failure to perform and all other reasons set forth in Section 10-38 of the County Code.

d) In addition to cancellation or termination as otherwise provided in this Agreement, the County may at any time, in its sole discretion, with or without cause, terminate this Agreement or any portion of this Agreement, upon thirty (30) days written notice, and at its sole option at any time, without cause, when in its sole discretion it deems such termination is in the best interest of the Department. In such circumstance, the County will solely be responsible for paying the contractor the costs actually incurred by the Contractor in performing the contracts services through the date of termination, less payments for same received, but the County shall not be responsible for any other costs or damages, including but not limited to lost profits, loss of opportunity, borrowing costs, carrying costs, damage to reputation, loss of goodwill, or loss of income.

e) In the event that the County exercises its right to terminate this Agreement, the Contractor shall, upon receipt of such notice, unless otherwise directed by the County:

i. Stop work on the date specified in the notice ("the Effective Termination Date");

ii. Take such action as may be necessary for the protection and preservation of the County's materials and property;

iii. Cancel orders;

iv. Assign to the County and deliver to any location designated by the County any non-cancelable orders for Deliverables that are not capable of use except in the performance of this Agreement and has been specifically developed for the sole purpose of this Agreement and not incorporated in the Services;

v. Take no action which will increase the amounts payable by the County under this Agreement; and

f) In the event that the County exercises its right to terminate this Agreement pursuant to Article 32 (d), the Contractor will be compensated as stated in the payment Articles herein for the:

i. Portion of the Services completed in accordance with the Agreement up to the Effective Termination Date;

ii. Non-cancelable Deliverables that are not capable of use except in the performance of this Agreement and has been specifically developed for the sole purpose of this Agreement, but not incorporated in the Services.

g) All compensation pursuant to this Article are subject to audit.

**ARTICLE 33. EVENT OF DEFAULT**

a) An Event of Default shall mean a breach of this Agreement by the Contractor. Without limiting the generality of the foregoing, and in addition to those instances referred to herein as a breach, an Event of Default shall include the following:

i. the Contractor has not delivered Deliverables on a timely basis;

ii. the Contractor has refused or failed to supply enough properly skilled staff personnel;

iii. the Contractor has failed to make prompt payment to subcontractors or suppliers for any Services;

iv. the Contractor has become insolvent (other than as interdicted by the bankruptcy laws), or has assigned the proceeds received for the benefit of the Contractor's creditors, or the Contractor has taken advantage of any insolvency statute or debtor/creditor law or if the Contractor's affairs have been put in the hands of a receiver;

v. the Contractor has failed to obtain the approval of the County where required by this Agreement;

vi. the Contractor has failed to provide "adequate assurances" as required under subsection b below;

vii. the Contractor has failed in the representation of any warranties stated herein.

b) When, in the opinion of the County, reasonable grounds for uncertainty exist with respect to the Contractor's ability to perform the Services or any portion thereof, the County may request that the Contractor, within the timeframe set forth in the County's request, provide adequate assurances to the County, in writing, of the Contractor's ability to perform in accordance with the terms of this Agreement. Until the County receives such assurances, the County may request an adjustment to the compensation received by the Contractor for portions of the Services which the Contractor has not performed. In the event that the Contractor fails to provide to the County the requested assurances within the prescribed timeframe, the County may:

i. treat such failure as a repudiation of this Agreement; and

ii. resort to any remedy for breach provided herein or at law, including but not limited to, taking over the performance of the Services or any part thereof either by itself or through others.

c) In the event the County shall terminate this Agreement for default, the County or its designated representatives may immediately take possession of all applicable equipment, materials, products, documentation, reports and data.

## ARTICLE 34. NOTICE OF DEFAULT - OPPORTUNITY TO CURE

If an Event of Default occurs in the determination of the County, the County may so notify the Contractor ("Default Notice"), specifying the basis for such default, and advising the Contractor that such default must be cured immediately or this Agreement with the County may be terminated. Notwithstanding, the County may, in its sole discretion, allow the Contractor to rectify the default to the County's reasonable satisfaction within a thirty (30) day period. The County may grant an additional period of such duration as the County shall deem appropriate without waiver of any of the County's rights hereunder. The default notice shall specify the date the Contractor shall discontinue the Services upon the Termination Date.

## ARTICLE 35. REMEDIES IN THE EVENT OF DEFAULT

If an Event of Default occurs, the Contractor shall be liable for all damages resulting from the default, including but not limited to:

a) lost revenues;

b) the difference between the cost associated with procuring Services hereunder and the amount actually expended by the County for re-procurement of Services, including procurement and administrative costs;

c) proration of the remaining balance of monies paid in advance for annual Maintenance and Support services; and

d) such other direct damages.

The Contractor shall also remain liable for any liabilities and claims related to the Contractor's default. The County may also bring any suit or proceeding for specific performance or for an injunction.

## ARTICLE 36. PATENT AND COPYRIGHT INDEMNIFICATION

a) The Contractor shall not infringe on any copyrights, trademarks, service marks, trade secrets, patent rights, other intellectual property rights or any other third party proprietary rights in the performance of the Work.

b) The Contractor warrants that all Deliverables furnished hereunder, including but not limited to: equipment, programs, documentation, software, analyses, applications, methods, ways, processes, and the like, do not infringe upon or violate any copyrights, trademarks, service marks, trade secrets, patent rights, other intellectual property rights or any other third party proprietary rights.

c) The Contractor shall be liable and responsible for any and all claims made against the County for infringement of patents, copyrights, service marks, trade secrets or any other third party proprietary rights, by the use or supplying of any programs, documentation, software, analyses, applications, methods, ways, processes, and the like, in the course of performance or completion of, or in any way connected with, the Work, or the County's continued use of the Deliverables furnished hereunder. Accordingly, the Contractor at its own expense, including the payment of attorney's fees, shall indemnify, and hold harmless the County and defend any action brought against the County with respect to any claim, demand, cause of action, debt, or liability.

d) In the event any Deliverable or anything provided to the County hereunder, or portion thereof is held to constitute an infringement and its use is or may be enjoined, the Contractor shall have the obligation to, at the County's option to (i) modify, or require that the applicable subcontractor or supplier modify, the alleged infringing item(s) at its own expense, without impairing in any respect the functionality or performance of the item(s), or (ii) procure for the County, at the Contractor's expense, the rights provided under this Agreement to use the item(s).

e) The Contractor shall be solely responsible for determining and informing the County whether a prospective supplier or subcontractor is a party to any litigation involving patent or copyright infringement, service mark, trademark, violation, or proprietary rights claims or is subject to any injunction which may prohibit it from providing any Deliverable hereunder. The Contractor shall enter into agreements with all suppliers and subcontractors at the Contractor's own risk. The County may reject any Deliverable that it believes to be the subject of any such litigation or injunction, or if, in the County's judgment, use thereof would delay the Work or be unlawful.

## ARTICLE 37. CONFIDENTIALITY

a) All Developed Works and other materials, data, transactions of all forms, financial information, documentation, inventions, designs and methods obtained from the County in connection with the Services performed under this Agreement, made or developed by the Contractor or its subcontractors in the course of the performance of such Services, or the results of such Services, or which the County holds the proprietary rights, constitute Confidential Information and may not, without the prior written consent of the County, be used by the Contractor or its employees, agents, subcontractors or suppliers for any purpose other than for the benefit of the County, unless required by law. In addition to the foregoing, all County employee information and County financial information shall be considered Confidential Information and shall be subject to all the requirements stated herein. Neither the Contractor nor its employees, agents, subcontractors or suppliers may sell, transfer, publish, disclose, display, license or otherwise make available to others any part of such Confidential Information without the prior written consent of the County. Additionally, the Contractor expressly agrees to be bound by and to defend, indemnify and hold harmless the County, and their officers and employees from the breach of any federal, state or local law in regard to the privacy of individuals.

b) The Contractor shall advise each of its employees, agents, subcontractors and suppliers who may be exposed to such Confidential Information of their obligation to keep such information confidential and shall promptly advise the County in writing if it learns of any unauthorized use or disclosure of the Confidential Information by any of its employees or agents, or subcontractor's or supplier's employees, present or former. In addition, the Contractor agrees to cooperate fully and provide any assistance necessary to ensure the confidentiality of the Confidential Information.

c) It is understood and agreed that in the event of a breach of this Article damages may not be an adequate remedy and the County shall be entitled to injunctive relief to restrain any such breach or threatened breach. Unless otherwise requested by the County, upon the completion of the Services performed hereunder, the Contractor shall immediately turn over to the County all such Confidential Information existing in tangible form,

and no copies thereof shall be retained by the Contractor or its employees, agents, subcontractors or suppliers without the prior written consent of the County. A certificate evidencing compliance with this provision and signed by an officer of the Contractor shall accompany such materials.

## ARTICLE 38. PROPRIETARY INFORMATION

As a political subdivision of the State of Florida, Miami-Dade County is subject to the stipulations of Florida's Public Records Law.

The Contractor acknowledges that all computer software in the County's possession may constitute or contain information or materials which the County has agreed to protect as proprietary information from disclosure or unauthorized use and may also constitute or contain information or materials which the County has developed at its own expense, the disclosure of which could harm the County's proprietary interest therein.

During the term of the contract, the Contractor will not use directly or indirectly for itself or for others, or publish or disclose to any third party, or remove from the County's property, any computer programs, data compilations, or other software which the County has developed, has used or is using, is holding for use, or which are otherwise in the possession of the County (hereinafter "Computer Software"). All third-party license agreements must also be honored by the contractors and their employees, except as authorized by the County and, if the Computer Software has been leased or purchased by the County, all hired party license agreements must also be honored by the contractors' employees with the approval of the lessor or Contractors thereof. This includes mainframe, minis, telecommunications, personal computers and any and all information technology software.

The Contractor will report to the County any information discovered or which is disclosed to the Contractor which may relate to the improper use, publication, disclosure or removal from the County's property of any information technology software and hardware and will take such steps as are within the Contractor's authority to prevent improper use, disclosure or removal.

## ARTICLE 39. PROPRIETARY RIGHTS

a) Contractor shall retain all rights, title and interests in and to all materials, data, documentation and copies thereof furnished to the County by the Contractor, as a result of the Services the Contractor performs in connection with this Agreement. The Contractor shall not, without the prior written consent of the County, use such documentation furnished by the County on any other project in which the Contractor or its employees, agents, subcontractors or suppliers are or may become engaged. Submission or distribution by the Contractor to meet official regulatory requirements or for other purposes in connection with the performance of Services under this Agreement shall not be construed as publication in derogation of the County's copyrights or other proprietary rights.

b) All rights, title and interest in and to certain inventions, ideas, designs and methods, specifications and other documentation related thereto developed by the Contractor and its subcontractors specifically for the County, hereinafter referred to as "Developed Works" shall remain the property of the Contractor.

c) Except as otherwise provided in subsections a and b above, or elsewhere herein, the Contractor and its subcontractors and suppliers hereunder shall retain all intellectual proprietary rights in and to all Licensed Software provided hereunder, that have not been customized to satisfy the performance criteria set forth in the Scope of Services. Notwithstanding the foregoing, the Contractor hereby grants, and shall require that its subcontractors and suppliers grant, if the County so desires, a perpetual, irrevocable and unrestricted right and license to use, duplicate, disclose and/or permit any other person(s) or entity(ies) to use all such technical data and other Documentation for the operations of the County or entities controlling, controlled by, under common control with, or affiliated with the County, or organizations which may hereafter be formed by or become affiliated with the County. Such license specifically includes, but is not limited to, the right of the County to use

and/or disclose, in whole or in part, the technical documentation, to any person or entity outside the County for such person's or entity's use in furnishing any and/or all of the Deliverables provided hereunder exclusively for the County or entities controlling, controlled by, under common control with, or affiliated with the County, or organizations which may hereafter be formed by or become affiliated with the County. No such License Software, specifications, data, documentation or related information shall be deemed to have been given in confidence and any statement to the contrary shall be void and of no effect.

**ARTICLE 40. LOCAL, STATE, AND FEDERAL COMPLIANCE REQUIREMENTS**

Contractor agrees to comply, subject to applicable professional standards, with the provisions of any and all applicable Federal, State and the County orders, statutes, ordinances, rules and regulations which may pertain to the Services required under this Agreement, including, but not limited to:

a) Equal Employment Opportunity (EEO), in compliance with Executive Order 11246 as amended and applicable to this Contract.

b) Miami-Dade County Florida, Department of Small Business Development Participation Provisions, as applicable to this Contract.

c) Environmental Protection Agency (EPA), as applicable to this Contract.

d) Miami-Dade County Code, Chapter 11A, Article 3. All contractors and subcontractors performing work in connection with this Contract shall provide equal opportunity for employment without regard to race, color, religion, ancestry, national origin, sex, pregnancy, age, disability, marital status, familial status, sexual orientation, or veteran status. The aforesaid provision shall include, but not be limited to, the following: employment, upgrading, demotion or transfer, recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The Contractor agrees to post in a conspicuous place available for employees and applicants for employment, such notices as may be required by the Dade County Fair Housing and Employment Commission, or other authority having jurisdiction over the work setting forth the provisions of the nondiscrimination law.

e) "Conflicts of Interest" Section 2-11 of the County Code, and Ordinance 01-199.

f) Miami-Dade County Code Section 10-38 "Debarment".

g) Miami-Dade County Ordinance 99-5, codified at 11A-60 et. seq. of Miami-Dade Code pertaining to complying with the County's Domestic Leave Ordinance.

h) Miami-Dade County Ordinance 99-152, prohibiting the presentation, maintenance, or prosecution of false or fraudulent claims against Miami-Dade County.

The Contractor shall hold all licenses and/or certifications, obtain and pay for all permits and/or inspections, and comply with all laws, ordinances, regulations and building code requirements applicable to the work required herein. Damages, penalties, and/or fines imposed on the County or Contractor for failure to obtain and maintain required licenses, certifications, permits and/or inspections shall be borne by the Contractor. The Project Manager shall verify the certification(s), license(s), permit(s), etc. for the Contractor prior to authorizing work and as needed.

Notwithstanding any other provision of this Agreement, Contractor shall not be required pursuant to this Agreement to take any action or abstain from taking any action if such action or abstention would, in the good faith determination of the Contractor, constitute a violation of any law or regulation to which Contractor is subject, including but not limited to laws and regulations requiring that Contractor conduct its operations in a safe and sound manner.

**ARTICLE 41. NONDISCRIMINATION**

During the performance of this Contract, Contractor agrees to not discriminate against any employee or applicant for employment because of race, color, religion, ancestry, national origin, sex, pregnancy, age, disability, marital status, familial status, sexual orientation, or veteran status, and will take affirmative action to ensure that employees and applicants are afforded equal employment opportunities without discrimination. Such action shall be taken with reference

to, but not limited to: recruitment, employment, termination, rates of pay or other forms of compensation, and selection for training or retraining, including apprenticeship and on the job training.

By entering into this Contract, the Contractor attests that it is not in violation of the Americans with Disabilities Act of 1990 (and related Acts) or Miami-Dade County Resolution No. R-385-95. If the Contractor or any owner, subsidiary or other firm affiliated with or related to the Contractor is found by the responsible enforcement agency or the County to be in violation of the Act or the Resolution, such violation shall render this Contract void. This Contract shall be void if the Contractor submits a false affidavit pursuant to this Resolution or the Contractor violates the Act or the Resolution during the term of this Contract, even if the Contractor was not in violation at the time it submitted its affidavit.

## ARTICLE 42. CONFLICT OF INTEREST

The Contractor represents that:

a) No officer, director, employee, agent, or other consultant of the County or a member of the immediate family or household of the aforesaid has directly or indirectly received or been promised any form of benefit, payment or compensation, whether tangible or intangible, in connection with the award of this Agreement.

b) There are no undisclosed persons or entities interested with the Contractor in this Agreement. This Agreement is entered into by the Contractor without any connection with any other entity or person making a proposal for the same purpose, and without collusion, fraud or conflict of interest. No elected or appointed officer or official, director, employee, agent or other consultant of the County, or of the State of Florida (including elected and appointed members of the legislative and executive branches of government), or a member of the immediate family or household of any of the aforesaid:

   i) is interested on behalf of or through the Contractor directly or indirectly in any manner whatsoever in the execution or the performance of this Agreement, or in the services, supplies or work, to which this Agreement relates or in any portion of the revenues; or

   ii) is an employee, agent, advisor, or consultant to the Contractor or to the best of the Contractor's knowledge any subcontractor or supplier to the Contractor.

c) Neither the Contractor nor any officer, director, employee, agency, parent, subsidiary, or affiliate of the Contractor shall have an interest which is in conflict with the Contractor's faithful performance of its obligation under this Agreement; provided that the County, in its sole discretion, may consent in writing to such a relationship, provided the Contractor provides the County with a written notice, in advance, which identifies all the individuals and entities involved and sets forth in detail the nature of the relationship and why it is in the County's best interest to consent to such relationship.

d) The provisions of this Article are supplemental to, not in lieu of, all applicable laws with respect to conflict of interest. In the event there is a difference between the standards applicable under this Agreement and those provided by statute, the stricter standard shall apply.

e) In the event Contractor has no prior knowledge of a conflict of interest as set forth above and acquires information which may indicate that there may be an actual or apparent violation of any of the above, Contractor shall promptly bring such information to the attention of the County's Project Manager. Contractor shall thereafter cooperate with the County's review and investigation of such information, and comply with the instructions Contractor receives from the Project Manager in regard to remedying the situation.

## ARTICLE 43. PRESS RELEASE OR OTHER PUBLIC COMMUNICATION

Under no circumstances shall the Contractor without the express written consent of the County:

a) Issue or permit to be issued any press release, advertisement or literature of any kind which refers to the

County, or the Work being performed hereunder, unless the Contractor first obtains the written approval of the County. Such approval may be withheld if for any reason the County believes that the publication of such information would be harmful to the public interest or is in any way undesirable; and

b) Communicate in any way with any contractor, department, board, agency, commission or other organization or any person whether governmental or private in connection with the Services to be performed hereunder except upon prior written approval and instruction of the County; and

c) Except as may be required by law, the Contractor and its employees, agents, subcontractors and suppliers will not represent, directly or indirectly, that any product or service provided by the Contractor or such parties has been approved or endorsed by the County.

## ARTICLE 44. BANKRUPTCY

The County reserves the right to terminate this contract, if, during the term of any contract the Contractor has with the County, the Contractor becomes involved as a debtor in a bankruptcy proceeding, or becomes involved in a reorganization, dissolution, or liquidation proceeding, or if a trustee or receiver is appointed over all or a substantial portion of the property of the Contractor under federal bankruptcy law or any state insolvency law.

## ARTICLE 45. GOVERNING LAW

This Contract, including appendices, and all matters relating to this Contract (whether in contract, statute, tort (such as negligence), or otherwise) shall be governed by, and construed in accordance with, the laws of the State of Florida. Venue shall be Miami-Dade County.

## ARTICLE 46. FIRST SOURCE HIRING REFERRAL PROGRAM

Pursuant to Section 2-2113 of the Code of Miami-Dade County, for all contracts for goods and services, the Contractor, prior to hiring to fill each vacancy arising under a County contract shall (1) first notify the South Florida Workforce Investment Board ("SFWIB"), the designated Referral Agency, of the vacancy and list the vacancy with SFWIB according to the Code, and (2) make good faith efforts as determined by the County to fill a minimum of fifty percent (50%) of its employment needs under the County contract through the SFWIB. If no suitable candidates can be employed after a Referral Period of three to five days, the Contractor is free to fill its vacancies from other sources. Contractor will be required to provide quarterly reports to the SFWIB indicating the name and number of employees hired in the previous quarter, or why referred candidates were rejected. Sanctions for non-compliance shall include, but not be limited to: (i) suspension of contract until Contractor performs obligations, if appropriate; (ii) default and/or termination; and (iii) payment of $1,500/employee, or the value of the wages that would have been earned given the noncompliance, whichever is less. Registration procedures and additional information regarding the FSHRP are available at https://iapps.southfloridaworkforce.com/firstsource/.

## ARTICLE 47. PUBLIC RECORDS AND CONTRACTS FOR SERVICES PERFORMED ON BEHALF OF A PUBLIC AGENCY

The Contractor shall comply with the state of FL Public Records Law, s. 119.0701, F.S., specifically to: (1) keep and maintain public records that ordinarily and necessarily would be required by the public agency in order to perform the service; (2) provide the public with access to public records on the same terms and conditions that the public agency would provide the records and at a cost that does not exceed the cost provided in Chapter 119, F.S., or as otherwise provided by law; (3) ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law; and (4) meet all requirements for retaining public records and transfer, at no cost, to the public agency all public records in possession of the Contractor upon termination of the contract and destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. All records stored electronically must be provided to the public agency in a format that is compatible with the information technology systems of the public agency. If the Contractor does not comply with a public records request, the public agency shall enforce contract provisions in accordance with the contract.

## ARTICLE 48. VENDOR REGISTRATION/CONFLICT OF INTEREST

a) Vendor Registration: The Contractor shall be a registered vendor with the County – Internal Services Department, Procurement Management Services Division, for the duration of this Agreement. In becoming a Registered Vendor with Miami-Dade County, the Contractor confirms its knowledge of and commitment to comply with the following:

1. ***Miami-Dade County Ownership Disclosure Affidavit***
(Section 2-8.1 of the County Code)

2. ***Miami-Dade County Employment Disclosure Affidavit***
*(Section 2.8-1(d)(2) of the County Code)*

3. ***Miami-Dade Employment Drug-free Workplace Certification***
*(Section 2-8.1.2(b) of the County Code)*

4. ***Miami-Dade Disability and Nondiscrimination Affidavit***
*(Section 2-8.1.5 of the County Code)*

5. ***Miami-Dade County Debarment Disclosure Affidavit***
*(Section 10.38 of the County Code)*

6. ***Miami-Dade County Vendor Obligation to County Affidavit***
*(Section 2-8.1 of the County Code)*

7. ***Miami-Dade County Code of Business Ethics Affidavit***
*(Section 2-8.1(i) and 2-11(b)(1) of the County Code through (6) and (9) of the County Code and Section 2-11.1(c) of the County Code)*

8. ***Miami-Dade County Family Leave Affidavit***
*(Article V of Chapter 11 of the County Code)*

9. ***Miami-Dade County Living Wage Affidavit***
*(Section 2-8.9 of the County Code)*

10. ***Miami-Dade County Domestic Leave and Reporting Affidavit***
*(Article 8, Section 11A-60 11A-67 of the County Code)*

11. ***Subcontracting Practices***
*(Ordinance 97-35)*

12. ***Subcontractor /Supplier Listing***
*(Section 2-8.8 of the County Code)*

13. ***Environmentally Acceptable Packaging***
*(Resolution R-738-92)*

14. ***W-9 and 8109 Forms***
(as required by the Internal Revenue Service)

15. ***FEIN Number or Social Security Number***
In order to establish a file, the Contractor's Federal Employer Identification Number (FEIN) must be provided. If no FEIN exists, the Social Security Number of the owner or individual must be provided. This number becomes Contractor's "County Vendor Number". To comply with Section 119.071(5) of the Florida Statutes relating to the collection of an individual's Social Security Number, be aware that the County requests the Social Security Number for the following purposes:
Identification of individual account records
- To make payments to individual/Contractor for goods and services provided to Miami-Dade County
- Tax reporting purposes
- To provide a unique identifier in the vendor database that may be used for searching and sorting departmental records

16. ***Office of the Inspector General***
(Section 2-1076 of the County Code)

17. ***Small Business Enterprises***
The County endeavors to obtain the participation of all small business enterprises pursuant to Sections 2-8.2, 2-8.2.3 and 2-8.2.4 of the County Code and Title 49 of the Code of Federal Regulations.

18. ***Antitrust Laws***
By acceptance of any contract, the Contractor agrees to comply with all antitrust laws of the United States and the State of Florida.

b) Conflict of Interest: Section 2-11.1(d) of Miami-Dade County Code requires that any County employee or any member of the employee's immediate family who has a controlling financial interest, direct or indirect, with Miami-Dade County or any person or agency acting for Miami-Dade County, competing or applying for a contract, must first request a conflict of interest opinion from the County's Ethics Commission prior to their or their immediate family member's entering into any contract or transacting any business through a firm, corporation, partnership or business entity in which the employee or any member of the employee's immediate family has a controlling financial interest, direct or indirect, with Miami-Dade County or any person or agency acting for Miami-Dade County. Any such contract or business engagement entered in violation of this subsection, as amended, shall be rendered voidable. For additional information, please contact the Ethics Commission hotline at (305) 579-2593.

## ARTICLE 49. SURVIVAL

The parties acknowledge that any of the obligations in this Agreement will survive the term, termination and cancellation hereof. Accordingly, the respective obligations of the Contractor and the County under this Agreement, which by nature would continue beyond the termination, cancellation or expiration thereof, shall survive termination, cancellation or expiration hereof.

## ARTICLE 50. ANNUAL APPROPRIATION

The County's performance and obligation to pay under this Agreement is contingent upon an annual appropriation by the Board of County Commissioners. Cancellation will not cause any penalty or expense to the County, except as to the portions of payments agreed upon and for which funds have been appropriated and budgeted. Service/Maintenance can be cancelled at any time that the Contractor is notified in writing, at least thirty (30) days prior to cancellation. There will be no early termination charges from the Contractor for canceling service/maintenance during the year.

## ARTICLE 51. FORCE MAJEURE

Except as otherwise expressly provided herein, neither party hereto shall be considered in default in the performance of its obligations hereunder to the extent that such performance is prevented or delayed by any cause, existing or future, which in not within the reasonable control of such party including, but not limited to, acts of God or the public enemy, fires, explosions, riots, strikes (not including strikes of the Contractor's staff personnel), terrorism or war. Notwithstanding the foregoing, the failures of any of the Contractor's suppliers, subcontractors, or the like shall not excuse the Contractor's performance except to the extent that such failures are due to any cause without the fault and reasonable control of such suppliers, subcontractors, or the like including, but not limited to, acts of God or the public enemy, fires, explosions, riots, strikes (not including strikes of the Contractor's staff personnel), terrorism or war.

## ARTICLE 52. TECHNICAL SUPPORT PERFORMANCE MEASURES

The County has established performance metrics in regards to the technical support and maintenance services to be provided under this Agreement. Should the Contractor not meet the required response or resolution timeframes for the reported issues as outlined with the Scope of Services (Appendix A), the County reserves the option of assessing penalties for failure of the Contractor to meet the response and resolution times required.

*Performance measure penalties will be applied at the following rates:*

| | |
|---|---|
| Response Time | $250 per day |
| Resolution Time | $250 per day |
| Failure of Contractor to meet monthly service levels as stated within Scope of Services | $500 per incident |
| Failure of Contractor to resolve or implement a County approved work-around within four (4) hours from notification and approval from MDAD of critical or major problems. | $2,500 per day |
| Three or more documented complaints in any given month from County Management or Users regarding Contractor's responsiveness. | $250 per incident |

The County will advise the Contractor in writing of its intent to assess performance measure penalties within 5 days of becoming aware of occurrence of any delay. The time frame for measurement of response time and the resolution time shall begin at the exact time the problem was reported to the Contractor. The time frame for the repair shall begin as soon as the Contractor arrives at the site or begins work on the problem. Partial hours may be treated as whole hours at the discretion of County, and performance penalty amounts may be withheld from payments.

IN WITNESS WHEREOF, the parties have executed this Agreement effective as of the contract date herein set forth below.

**CONTRACTOR**

By: _____

Name: MARCIA M. GIPSON
VICE PRESIDENT
SITA

Title: _____

Date: 19 December 2014

Attest: _____
Corporate Secretary/Notary Public

JANEAN BROWN
NOTARY PUBLIC
COBB COUNTY, GEORGIA
MY COMMISSION EXPIRES MAY 19, 2015

Corporate Seal/Notary Seal

**MIAMI-DADE COUNTY**

By: _____

Name: Carlos A. Gimenez

Title: Mayor

Date: _____

Attest: _____
Clerk of the Board

Approved as to form
and legal sufficiency

_____
Assistant County Attorney

# APPENDICES

- APPENDIX A – SCOPE OF SERVICES
- APPENDIX B – PAYMENT SCHEDULE
- APPENDIX C – IMPLEMENTATION TIMELINE *(Updated timeline- provided by SITA)*
- APPENDIX D – DELIVERABLE ACCEPTANCE FORMS
- APPENDIX E- CHANGE ORDER FORM
- *APPENDIX* F – U.S. CUSTOMS AND BORDER PROTECTION "*AUTOMATED PASSPORT CONTROL: BUSINESS REQUIREMENTS*" VERSION 16, August 2014
- APPENDIX G – U.S. CUSTOMS & BORDER PATROL "*AUTOMATED PASSPORT CONTROL SERVICE TECHNICAL REFERENCE MANUAL* (VERSION 2), DOCUMENT NUMBER 3209000-TRM V2
- APPENDIX H – U.S. CUSTOMS & BORDER PATROL "AUTOMATED PASSPORT CONTROL SERVICE (RELEASE 2.0 V4) INTERFACE CONTROL DOCUMENT(DOCUMENT NUMBER 3209000-ICD)
- APPENDIX I - SOFTWARE ESCROW AGREEMENT *(Actual Escrow Agreement Form to be executed upon Final System Acceptance as defined in Appendix A)*

## APPENDIX A – SCOPE OF SERVICES
## Automated Passport Control Kiosks

**Summary**

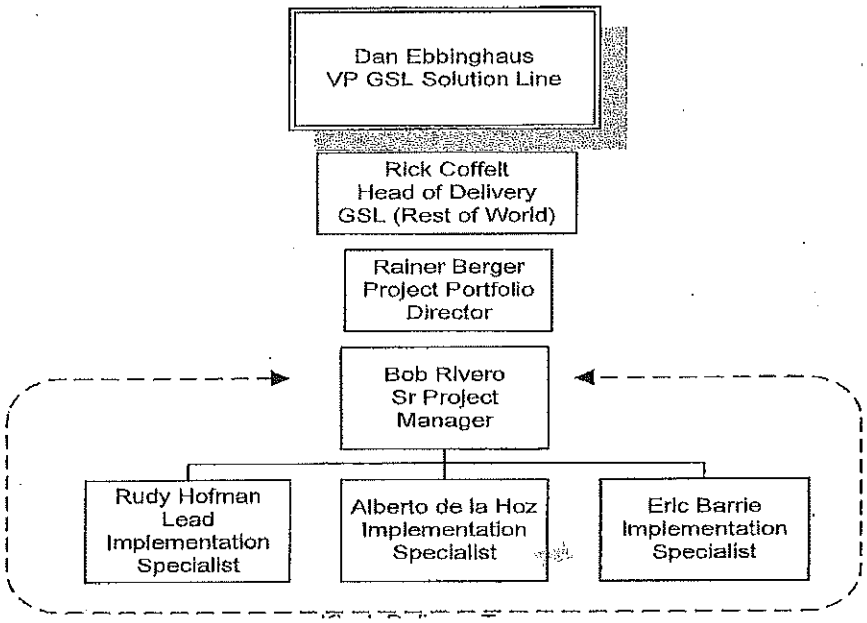
This Scope of Work ("SOW") incorporates the Contractor, "SITA"'s Proposal dated September 24, 2014 (RFP-0018) for the Miami Dade Aviation Department (MDAD) Automated Passport Control Project. Therefore this SOW together with the Proposal forms the complete Scope of Work to be performed by the Contractor under the terms of the Agreement, including all clarifications and changes to the Proposal identified below. For the avoidance of doubt, upon any conflict in the Proposal and in the terms of this SOW, the terms of this SOW shall control.

**Start of Implementation**

1.1. Implementation of the Service(s) will start within 10 working days from the Effective Date of the Service Agreement.

**Project Organization and Staffing**

2.1. This section provides additional details to Section 7.2 of SITA's Proposal. Additional details are provided in the organizational structure. SITA will provide an experienced implementation team with a Project Manager and Implementation Engineers. The size of the team is dependent on the number of kiosks to be deployed in a single phase, but generally one project manager and two Implementation Engineers will be assigned.




(a) The Project Delivery team listed above will be deployed against the indicative project implementation schedule below. During the course of the project, the Project Manager will be on site in Miami approximately 50% of the project and the Implementation Engineers will be on site in Miami for approximately 75% of the project time.

**Implementation Strategy**

3.1. Sections 9.3 to 9.7 of the Proposal highlight SITA's implementation strategy. SITA understands that delivery will include the installation of up to 144 Phase III (all ADA/ section 508 compliant, including accessible to the sight impaired) APC Kiosks in the US Customs and Border Protection (CBP) Federal Inspection Station (FIS) at Miami International Airport (MIA), Miami, FL, USA to an operational and CBP certified level. The following phasing schedule is the perceived deployment schedule however SITA will remain flexible to work with MDAD to adjust phasing and volumes based on the needs of the Customer.

Phase I: 36 APC Kiosks- Initial Purchase

Phase II: 36 APC Kiosks (12-18 months after initial purchase)

Phase III: 36 APC Kiosks (24-30 months after Phase II)

Phase IV: 36 APC Kiosks (12 months after Phase III)

3.2. Software configuration shall collect all Phase III information needed by CBP and shall be fully compliant with CBP's most current "Automated Passport Control Service: Technical Reference Manual (CBPTRM)". The initial phase of kiosks will be LPR compliant and follow the guidelines of the CBP Business Requirements Version 16. Compliance with future versions of CBP Business Requirements will be addressed through the Change Control process.

**County Responsibilities during Implementation**

4.1. County responsibilities in Section 10.2.2 and Section 16 in the Proposal are revised below. The County requirement for escorting support listed in Section 16 of the Proposal is removed.

(a) Access to the kiosks to SITA or SITA 3rd party engineers in order to analyze and troubleshoot incidents on the products during the operation of the service;

(b) Construction works required for the mounting of the access gates or kiosks to the floor at the required locations; and

(c) Secured stable power and Local Area Network (LAN) connection to each installed access gate or kiosk.

(d) Installation of power connections in accordance with local safety standards, one connection per access kiosk including a power cord long enough to reach the access kiosk connector;

(e) Floor strengthening, if necessary

(f) Preparation of fixing points for securing the access kiosk in accordance with the standard SITA mounting.

(g) Network access to the kiosks and e-Pass Monitoring Server(s) in order that remote SITA support staff can access and troubleshoot issues remotely

(h) Staff to direct and assist passengers during the operational phase of the project

(i) Agreement to Project Plan

4.2. A project plan will be prepared by the Contractor and agreed with the County at the beginning of the implementation for each phase.

**Change Control**

5.1. Section 9.5 of the Proposal outlines Scope and Change Management. The below section provides additional detail on Scope and Change Management. During the implementation of the Service(s), any work that is required to be performed over and above the work stated in this Schedule, shall be performed following an agreement between the parties on the scope and any related consequences (for the Charges, the Project Plan, etc) arising out of or in relation to such additional work.

5.2. Each party may request additional work over and above the work stated in this Schedule, using the change request form (Attachment 1) which will be provided at the time of contract agreement, signed by appropriately authorized representatives of the parties.

5.3. The following process shall apply to any changes in scope identified between signature of this Service Agreement by the Customer and the cutover of the Service(s):

(a) Change Request Made by Customer

5.3.a.1. Changes requested by the Customer shall be submitted to SITA using the Change Request Form for SITA to assess the impact and cost. SITA will allocate a change request number. If the analysis of the impact of the change and/or the development of the solution requires the allocation of resources and involves significant cost, SITA will submit a price for this work to the Customer. The Customer formal agreement to pay for the work must be obtained before the work is carried out.

5.3.a.2. If SITA is unable to implement the change requested, the Change Request Form will be returned to the Customer indicating the reason(s) in detail.

5.3.a.3. When the costs and impact of the change have been assessed SITA will return the Change Request Form to the Customer for acceptance. If Customer does not accept the change it will return the form completed with the reasons for non-acceptance.

(b) Change Request Submitted by SITA

5.3.b.1. If a change is requested by SITA a completed Change Request form will be submitted to the Customer for acceptance. If the Customer does not accept the change the form will be completed as Not Accepted and returned to SITA.

(c) Authorizations and Approvals

5.3.c.1. If the change is accepted the Change Request Form will be signed by an authorized representative of the Customer and SITA. The authorized Change Request Form shall then become part of this Service Agreement, as an amendment to it.

**Acceptance Testing**

6.1. As part of the project planning, SITA will specify and agree with the Customer the Acceptance Testing criteria and the execution of the Acceptance Testing.

6.2. The check list provided in Section 16 to this Addendum is an enhanced acceptance check list and replaces the check list provided in Appendix D to the Proposal

6.3. Any Acceptance Testing document(s) issued by SITA shall include acceptance certificate(s) to be signed by the Customer to document successful completion of Acceptance Testing.

(a) SITA will provide two Customer acceptance forms for formal acceptance. The initial acceptance form documents completion of pre-go live acceptance testing and is provided prior to formal production launch and the start of the 30 day warranty period. The second acceptance form will

document successful completion of the 30 day warranty period and full customer acceptance of the solution.

**Project Approach**

6.4. The project management and project implementation approach discussed in SITA's Proposal (Section 9) is revised to include:

(a) SITA will review the existing infrastructure prior to each phase to ensure it is adequate to support the planned implementation. If the infrastructure is not sufficient SITA will recommend upgrades. SITA and MDAD will implement agreed upgrades under their individual purviews.

(b) With early notification of a forthcoming implementation, SITA can further expedite items such as: Architectural Design reviews, SSL Certificate extensions, Standard Maintenance and name identifiers.

**Maintenance and Support Level Definitions**

Pursuant to Section 17.1, Maintenance and Support Level Definitions, of SITA's response, the following is a replacement for the support of the APC kiosks:Priority 1:

Priority 1 is reserved for all Incidents, which disable the proper operation of the complete system. SITA's response is targeted to restoring the service to operational capability, and includes but is not limited to:

a) Troubleshooting and isolation of malfunctioning equipment including flaws caused by software malfunction or operator/user error, to full restoration;
b) Replacement and/or on-line repair of failed equipment.

This consists of hardware break-fix and the provision of any physical and/or logical intervention of any SITA provided system or infrastructure at a customer location. Various services are provided to support customer sites:

- Providing the appropriate on-site skills to perform unit repair or unit exchange in accordance with the SITA contract and/or manufacturer's instructions. SITA will ensure that the appropriate level of training and skills are available to return equipment to full usability.
- Providing problem analysis, including identification of the source of the Problem.
- Obtain a replacement unit or component parts from the stock of available maintenance spares, or directly from the manufacturer when necessary.
- Restoring hardware to a working state with its functioning Operating System by exchange, physical repair, and adjustments of equipment and components.

**1.A.1 Priority 2:**

Priority 2 is reserved for Incident, which leave the system operational, but reduce the operational capability of the SITA solution. SITA's response would include:

a) Off-line repair or return of failed equipment to the repair center of the manufacturer;
b) Provision of scheduled updates and/or system recall of hardware as dictated by Manufacturer or SITA;
c) Hardware and firmware upgrades to all specified equipment, as required by SITA.

d) Troubleshooting and isolation of malfunctioning equipment including flaws caused by software malfunction or operator/user error, to full restoration;
e) Replacement and/or on-line repair of failed equipment.

### 1.A.2 Priority 3:

Priority 3 is reserved for an Incident, which impacts one kiosk:
a) Off-line repair or return of failed equipment to the repair center of the manufacturer;
b) Provision of scheduled updates and/or system recall of hardware as dictated by Manufacturer or SITA;
c) Hardware and firmware upgrades to all specified equipment, as required by SITA.
d) Replacement and/or on-line repair of failed equipment.

**Level 1 and 2 Support Team**

Pursuant to Section 17.2.3, Level 2 Support Team, is amended to be titled Level 1 and 2 Support team, and is replaced with the following:

Level 1 Support Team will be responsible for the following:

- Hardware support
- Incidents Management together with SITA's SPOC
- Technical support and assistance in the use of SITA products
- Preventive Hardware maintenance and support of all installed equipment and make sure that it is working as expected
- Hardware replacement, when required
- Knowledge transfer to customer staff

Level 2 Support Team will be responsible for the following:

- Technical support including identification and escalation of Problems, and Incident analysis.
- Corrective maintenance for all SITA provided Hardware and Software
- Warranty and spares management
- Contact of other support groups to ensure resolution of Incidents or Problems
- Interface with others systems, networks and operating environments, as required to resolve Incident and Problems or implement Changes
- Knowledge transfer to customer staff

**Service Level Management**

9.1. Pursuant to Section 17.4, Service Level Management, of SITA's response, the following charts replace the Priority Level definition and the Service Level Agreement requirements, which SITA will use for the support of the APC kiosks:

**Priority Level Definition**

| Priority Level | Impact | Description |
|---|---|---|
| 1 | Business efficiency impact | System failure that completely interrupts the critical business processes, affecting all users. |
| 2 | Business high impact | • System failure that partially interrupts or degrades business critical processes and there is no alternative available.<br>• An incident affects multiple users. |
| 3 | Business critical impact | • System failure that interrupts non-critical business processes.<br>• Failure of a system or component but alternative available at customer location.<br>• Incidents affects single user, and a workaround is available. |

**Service Level Agreement:**

| Priority | Response Time | Resolution Time | Status Updates |
|---|---|---|---|
| 1 | 10 minutes | 2 Hour | 15 minutes |
| 2 | 15 Minutes | 4 Hour | 1 hour |
| 3 | 1 Hour | 6 Hour | 2 Hour |

9.2. In addition the following should be added to this Section 17.4, any Incident that last more than the defined Resolution Time in the Service Level Agreement will be escalated into Level 2, and if Level 2 is unable to resolve the Incident within 2 hours, then they will engage Level 3. The frequency of the status updates are defined by the Service Level Agreement and will remain effective until the Incident is resolved.

**Resolver Group Escalation:**

| Support Level | Definition |
|---|---|
| Level 1 | Service provided by the onsite team who will investigate the reported error and make best efforts to correct the problem |
| Level 2 | Level 1 will engage Level 2 Technical Support to troubleshoot for resolution |
| Level 3 | Level 2 will engage Level 3 Technical Support to troubleshoot for resolution |

**Management Escalation:**

| Escalation | Contact |
|---|---|
| Level 1 | Level 2 Site Administration<br>Contact: To be confirmed upon hiring |
| Level 2 | Leila Gaines<br>Sr. Manager, Service Operations<br>Miami<br>+1 786546 5872 |
| Level 3 | Marcia M. Gipson<br>Vice President, Service Operations<br>The Americas<br>+1 404 229 6906 |

**Staffing Details**

All hardware and software maintenance is the responsibility of SITA. SITA will hire two (2) Level 1 Technicians with Phase I, or the first 36 kiosks. Further one (1) additional Level 1 Technician will be added with each of Phase II and Phase IV. This will provide a total of four (4) additional Level 1 Technicians across the four Phases of 144 kiosks.

9.3. SITA will hire one (1) Level 2 Administrator during the first year of the agreement at SITA's expense to be dedicated to Miami. The work schedule for the Level 2 Administrator would be during normal business hours, Monday through Friday, and would be available and on call during alternate hours.

The shift schedule for Technicians is as follows:

| | Time | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sunday | Tech1 | | | | | | | | X | X | X | X | X | X | X | X | | | | | | | | | |
| | Tech2 | | | | | | | | | | | | | | * | * | * | * | * | * | * | * | | | |
| | Tech3 | | | | | | @ | @ | @ | @ | @ | @ | @ | @ | @ | @ | | | | | | | | | |
| | Tech4 | | | | | | | | | | | & | & | & | & | & | & | & | & | & | & | & | & | & | |
| Monday | Tech1 | | | | | | | | X | X | X | X | X | X | X | X | | | | | | | | | |
| | Tech2 | | | | | | | | | | | | | | * | * | * | * | * | * | * | * | | | |
| | Tech3 | | | | | | @ | @ | @ | @ | @ | @ | @ | @ | @ | @ | | | | | | | | | |
| | Tech4 | | | | | | | | | | | & | & | & | & | & | & | & | & | & | & | & | & | & | |
| Tuesday | Tech1 | | | | | | | | X | X | X | X | X | X | X | X | | | | | | | | | |
| | Tech2 | | | | | | | | | | | | | | * | * | * | * | * | * | * | * | | | |
| | Tech3 | | | | | | | | | | | | | | | | | | | | | | | | |
| | Tech4 | | | | | | | | | | | & | & | & | & | & | & | & | & | & | & | & | & | & | |
| Wednesday | Tech1 | | | | | | | | | | | | X | X | X | X | X | X | X | X | | | | | |
| | Tech2 | | | | | | | | | | | | * | * | * | * | * | * | * | * | | | | | |
| | Tech3 | | | | | | | | | | | | | | | | | | | | | | | | |
| | Tech4 | | | | | | | | | | | | | | | | | | | | | | | | |
| Thursday | Tech1 | | | | | | | | | | | | | | | | | | | | | | | | |
| | Tech2 | | | | | | | | | | | | * | * | * | * | * | * | * | * | | | | | |
| | Tech3 | | | | | | | | | | | | | | | | | | | | | | | | |
| | Tech4 | | | | | | | | | | | | | | | | | | | | | | | | |
| Friday | Tech1 | | | | | | | | X | X | X | X | X | X | X | X | | | | | | | | | |
| | Tech2 | | | | | | | | | | | | | | * | * | * | * | * | * | * | * | | | |
| | Tech3 | | | | | | @ | @ | @ | @ | @ | @ | @ | @ | @ | @ | | | | | | | | | |
| | Tech4 | | | | | | | | | | | | | | | | | | | | | | | | |
| Saturday | Tech1 | | | | | | | | | | | | | | | | | | | | | | | | |
| | Tech2 | | | | | | | | | | | | * | * | * | * | * | * | * | * | | | | | |
| | Tech3 | | | | | | @ | @ | @ | @ | @ | @ | @ | @ | @ | @ | | | | | | | | | |
| | Tech4 | | | | | | | | | | | & | & | & | & | & | & | & | & | & | & | & | & | & | |

This schedule is subject to change based on passenger flow, and is subject to staff being allowed into the FIS areas during the US CBP down times. Any adjustments will be made in collaboration with Miami-Dade Aviation Department to ensure we have optimized coverage.

## Training

This section updates the proposed training approach and applies to each phase of the APC Kiosk program. Pursuant to Section 18, SITA's Approach to Training, the following statement is updated:

To facilitate training, MDAD will need to provide a training class room with projector. The training will consist of the class room training, followed by hands on APC Kiosk and Ambassador Application training.

In addition the table below provides the details of the class room training courses to be provided.

9.4. APC Kiosk End User

| | |
|---|---|
| **Title:** | **APC Kiosk End User (GSL 001)** |
| **Description:** | This course is designed to train airport ambassador and CBP staff to become familiar with the APC solution. The training session will be broken into a class room session and hands on Kiosk session, in the FIS area. This course is run as part of the initial handover by SITA education and professional services (2x trainers). |
| **Content:** | • The SITA APC Kiosk<br>• The APC process<br>• Information videos, processes and benefits<br>• Referral & Exception handling<br>• Queue reporting<br>• Outage reporting<br>• Contingences<br>• Using the system and completing full transactions<br>• Training on receipt paper replacement<br>• Training to identify, what to look for when a Kiosk may require cleaning |
| **Audience:** | Airport operations ambassadors & CBP staff |
| **Class Size:** | 20 |
| **Pre-Requisites:** | • Familiarity with Graphical User Interfaces (GUI) and touch screen self-service systems<br>• Knowledge of the airport and CBP (resources, processes, etc.)<br>• FIS area access |
| **Documentation:** | PowerPoint slide deck and APC process manual for each student |
| **Location:** | A Customer or Airport User-provided training room |
| **Duration:** | ½ Business day |

## 9.5. APC Kiosk Train the Trainer

| | |
|---|---|
| **Title:** | **APC Kiosk Train The Trainer (GSL 002)** |
| **Description:** | This course is designed to train the trainer. The courses consists of the "**APC Kiosk End User**" with technical / operational and administration. Upon completion the trainer will be able to run their own internal APC training courses. This course is run as part of the initial handover by SITA education and a senior deployment specialist from professional services (2x trainers). |
| **Content:** | As per "**APC Kiosk End User**" course with the following:<br>• The SITA APC Kiosk – Admin Level<br>• The APC Process – Eligibility and Triage Questioning<br>• Operations training - Referrals and Exceptions<br>• Technical training – Operation and Support<br>• Administration training - Kiosk Management System |
| **Audience:** | Terminal Operations Managers and Senior Agents |
| **Class Size:** | 20 (max) |
| **Pre-Requisites:** | Knowledge of Computers, Graphical User Interfaces (GUI) and Touch screen Self Service Systems<br>Understanding of CBP and FIS area processes / procedures. |
| **Documentation:** | PowerPoint slide deck<br>APC process manual<br>APC Kiosk Technical manuals (Including maintenance documents)<br>FIS area access |
| **Location:** | A Customer or Airport User-provided training room |
| **Duration:** | 1 day |

CHANGE REQUEST FORM TEMPLATE

| Change Request Form Number: |
|---|
| **SECTION A Contract Details** |
| Contract Name: |
| Parties: |
| Reference no: |
| Effective date (if known): |
| **SECTION B Details of proposed Change** |
| **Title of the proposed Change:** |
| **Service(s) to which the proposed Change relates:** |
| **Description of the proposed Change:** [*Describe the proposed Change in detail with an explanation of its importance*] [*Attach supporting information if appropriate*] |
| **Clause(s) and/or schedule(s) of the Contract which will be modified (if any):** [*if necessary, provide wording of any new / amended provisions*] |
| **SECTION C Impact of proposed Change Request (for information, impact assessment and resource planning only)** |
| ☐ Cost<br>☐ Delivery date / timetable / other date<br>☐ Functionality<br>☐ Performance<br>☐ Resources<br>☐ Other system<br><br>☐ Documentation<br>☐ Training needs<br>☐ Third Party<br>☐ Other (please specify) _____ |
| **Description of Impact(s):** [*provide a detailed description of the selected impact(s)*] |
| **SECTION D - Cost** |
| **Cost implications of the proposed Change:** [*Include details of whether the current cost (if any) is reduced or increased*] |
| **SECTION E - Approval of proposed Change**<br>SITA and Customer confirm that they have each read the information contained in this Change Request Form, approve the proposed Change Request as set out above, and agree that the Contract shall be treated as having been amended accordingly.<br>**For and on behalf of SITA**<br>**Signed:**<br>(Authorized Signatory)<br>**Name:**<br>**Title:**<br>**Date:**<br>**For and on behalf of Customer:**<br>**Signed:**<br>(Authorized Signatory)<br>**Name:**<br>**Title:**<br>**Date:** |

## Executive Summary

SITA is pleased to provide the Miami-Dade Aviation Department (MDAD) with a commercial proposal for the provision of Automated Passport Control Kiosks (APC) with Phase III functionality, Support and Maintenance of APC, and Delivery and Installation of APC in the US Customs and Border Protection (CBP) Federal Inspection Station (FIS) of Miami International Airport (MIA), Miami, FL, USA.

The proposed solution is the SITA APC self-service kiosk to automate the capture of travel documents, biometric and customs declaration data as required by the US Customs and Border Protection Agency (CBP) for Immigration processing of US and Canadian citizens entering the United States as well as visitors (non US and non Canadian) from those countries which participate in the Visa Waiver Program (VWP) and have filed a travel authorization via the US CBP Electronic Travel Authorization System (ESTA).

The current 36 APC units installed and operational in MIA are the same SITA APC Kiosks we will offer in this response to the proposal.

SITA is proud to confirm that the proposed solution conforms to the requirements outlined in the RFP. The APC Kiosk features all the components, software and quality assurance criteria to ensure state-of-the-art of biometric data capture to meet specifications for Automated Passport Control.

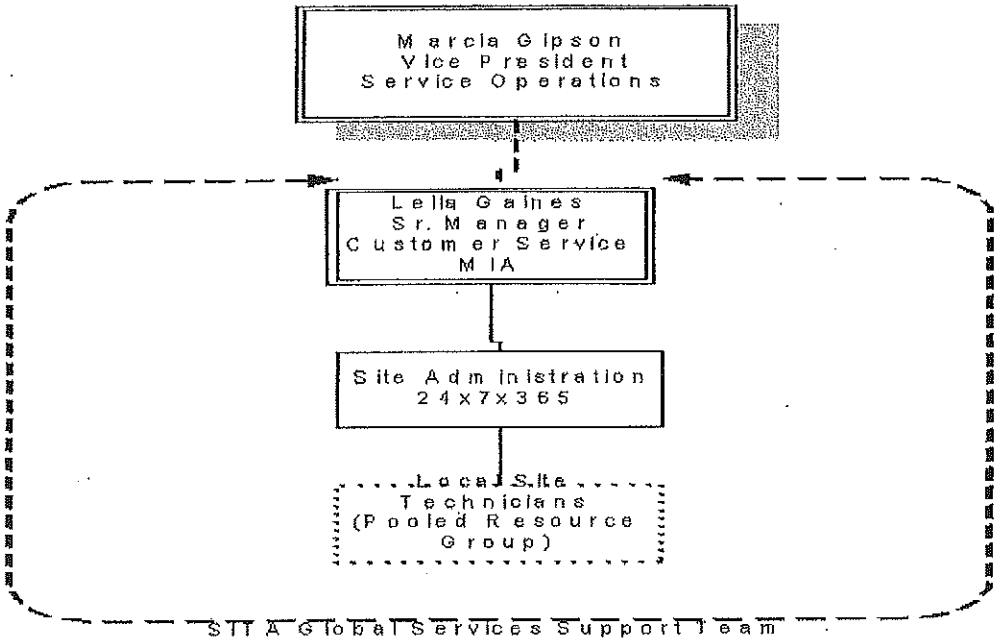
The primary functions of the kiosks are as follows:

- Capture and validation of travel document (passport) data
- Capture face and fingerprint biometric data, for Visa Waiver visitors
- Capture customs declaration data, replicating current CBP declaration form
- Transfer the data to the CBP Automated Passport Control system
- Print a receipt for presentation at the CBP officer

Unlike other market approaches for APC kiosks, the SITA solution utilizes a proven market solution deployed worldwide in the automated border control systems industry. SITA is committed to providing the most advanced solution possible for its clients. We look forward to continuing to provide unmatched service and an unparalleled product solution to Miami-Dade County.

## 2. Organization Chart

### 5.1 Technical Support Services Organization Chart




### 5.2 Management Structure and Assignment of Work

SITA's structure provides a single end to end program owner who reaches across the SITA organization to ensure our customers receive the highest level of support. Beyond the program owner, there are specific personnel assigned with unique qualifications and fields of specialization. These fields of specialization include Customer Relationship Management, Customer Service Management and Delivery. The key service areas are specifically Customer Service Management and Delivery.

Overall APC Program Owner – Ray Batt
Overall Customer Relationship Owner – David Menzel
Delivery Portfolio Owner – Rainer Berger
Head of Delivery – Rick Coffelt
APC Program Senior Customer Service Manager – Lelia Gaines

## EXPERIENCE AND QUALIFICATIONS OF KEY PERSONNEL

### Key Technical Support Management Personnel

The Local SITA Global Services team consists of the following individuals who will be on-site to support and manage the operation once the project is delivered and accepted. Key personnel are lead by Mrs. Leila Gaines Senior Manager of Customer Service and Local Site Administration, who will successfully manage the Level 1 and Level 2 operations for the project. Also included in our support solution will be Local Site Technicians from a pooled group of local on-site resources.

In order to support the operation requirements outlined in the RFP, as well as comply with the SLAs, we will add resources to the staff with each incremental procumbent phase of the kiosks. Our pricing reflects the incremental resources associated with this effort.

Below is a RACI Chart which delineates the responsibilities for the support staff.

| Area of responsibility | Leila Gaines Sr. Manager Customer Service | Site Administration Support | Local/ On-Site Pooled Resources |
|---|---|---|---|
| Overall Operational Management | X | | |
| Incident Management | | X | X |
| Problem Management | | X | |
| Change Management | | X | Support |
| Preventative Maintenance | | | X |
| Consumables Replacement for the Kiosks | | | X |
| Remote Monitoring of the Kiosks | | X | |
| Monthly Reporting | | Support | X |

**Leila Gaines- Geography Sr. Manager Service Operations –**
Key Responsibilities include:
Organize, lead, motivate and develop a professional team of Service & Infrastructure Operations staff, manage Service Operations support to internal and external customers in accordance with the terms of the customer contract and Service Level Agreements (SLAs), manage the correct functioning and maintenance of all internal and external systems and products serviced by Service & Infrastructure Operations

APC Responsibilities

Act as the customer Single Point of Contact (SPOC), when required, co-ordinate the scheduling of intervention with customers and internal resolver groups ensuring the highest level of customer service and communications are maintained to resolve the fault and incident within the prescribed SLA, ensure shortest restoral times possible, initiating the timely escalations to specialized resolver groups inside and outside SITA, according to the customer contracts, SLAs and monitoring requirements, ensure the Service Operations team adheres to the highest working standards for all incidents and problems by providing guidance, support and direct management, manage the first line responsibility and budgets for the different teams under Service Operations, including quality of service provided and escalations, manage local suppliers in the provision of services for the SITA Service Operations center and report on services provided to management, identify knowledge and documentation gaps, and ensure there is a process to get up-to-date information through a knowledge repository.

**SITE ADMINISTRATORS KEY RESPONSIBILITIES**

APC Responsibilities include:

To ensure the correct functioning and maintenance of all internal and external customer IT equipment and services, when required, act as the customer SPOC and co-ordinate the scheduling of the onsite intervention with Customer's, internal resolver groups, and local Field Operations resources ensuring the highest level of customer services and communications are maintained to resolve the fault and incident within the prescribed SLA, manage the replacement of faulty equipment through the use of spares, and ensuring the timely replenishment the spare according to prescribed availability and sparing policy, carry out site surveys for new customer premises for preparation for new product and services installation under the guidance of senior team members, adhere to industry best practices in order to deliver quality Field Operations, reporting and escalating all observed problems to proper SITA operational escalation points, carry out preventive maintenance of equipment in accordance with agreed schedules and to manufacturer specifications, report on the monthly performance of the workshop and provide feedback to the Global Operations regional management teams, to ensure the field services team adheres to the highest working standards for all interventions and repair targets by providing guidance, support and direct management, manage the first line responsibility and budgets for the local maintenance facility, field operations service provided and escalations, perform tests on hardware and software components and be responsible for the co-ordination of local acceptance testing with the customer and 3rd parties, supervise staff and ensure adequate training and development is provided to them and carry out annual reviews and input into performance appraisal process, ensure day-to-day supervision of activities of a group of individuals by providing appropriate personal support to enable co-workers to function to their operational potential, confirm and prioritize day-to-day tasks, as and when needed, coach fellow co-workers on operational issues relying on strong working knowledge of the activities in the group, in consultation with the line manager, support and report on the adherence to local standard policies and procedures (absence tracking, sick leave, overtime, confidentiality), ensure that all staff provide the required Field Service incident and change data and that it is recorded in the correct fields in the Service Management Tool records for all assigned Incidents & Change Orders.

**SITE TECHNICIAN KEY RESPONSIBILITIES**

APC Responsibilities include:

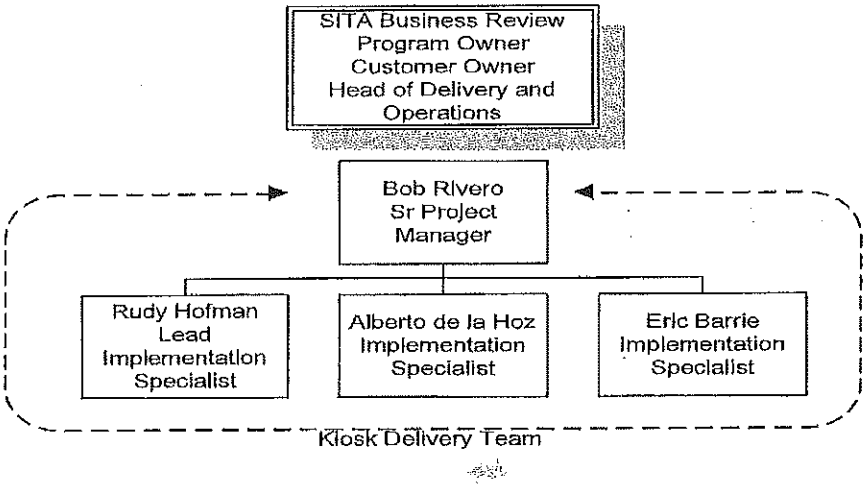
Carry out local repairs of faulty equipment and services to the highest standards and co-ordinate the resolution with the appropriate resolver group, ensure shortest possible repair cycle by initiating the timely return of faulty SITA and Customer equipment according to the customer maintenance contract and SLAs and monitoring closely the

replacement of faulty items and spares, manage the replacement of faulty equipment through the use of spares, monitoring and manage consumables for the Kiosks, reporting and escalating all observed problems to proper SITA operational escalation points, carry out preventive maintenance of equipment in accordance with agreed schedules and to manufacturer specifications, report on the monthly performance and provide feedback to the Operations regional management teams, perform tests on hardware and software components and be responsible for the co-ordination of local acceptance testing with the Customer, assist with Change order was needed and directed by the customer and SITA Senior Management staff.

## KEY PROJECT PERSONNEL AND PROJECT ORGANIZATIONAL STRUCTURE

The project organization for the Miami Dade County APC implementation program includes senior level Project Managers and uniquely qualified Implementation Engineers that have a direct line into SITA senior level management to ensure complete success of our projects. A typical project structure would have a Senior Project Manager and appropriate Implementation Engineers to support the quantity of kiosks required by the customer.

The Miami Dade County RFP specifically defines a potential four phase implementation of 36 kiosks for each phase. This phased approach will require a single Senior Project Manager and two Implementation Engineers in each of the phases. All of our primary delivery team members have previous experience with implementation of APC kiosks in Miami. Our team maintains the appropriate badges for MIA and FIS, which will help ensure an expedited, low risk implementation. SITA also has the ability to augment the primary team as necessary to ensure critical milestones are achieved.



**Bob Rivero, Senior Project Manager**

Senior Project Manager with experience delivering projects where high performance and a commitment to customer satisfaction are paramount. Over ten years of Information Technology experience in project management, business analysis, consulting, software development, programming, training, and marketing support. Capabilities include:

Project Manager a disciplined approach to plan, organize and manage projects. Managed application and infrastructure projects and provided clients efficient cost-effective solutions across multiple industries including airline; financial services; retail; software; government; mining and manufacturing including legacy mainframe systems.

Technical Manager Contact between software engineers and customers, managed the customer service/trouble ticket system for defect tracking and enhancement requests for infrastructure projects; as release manager co-developed and co-manage the release criteria with IBM, our development partner, for every major product release.

Sr. Business Analyst analyzed business processes and continually proposed innovative solutions.

Software Developer developed software solutions in the healthcare; airline; retail; aerospace, food service; software; industries including legacy mainframe systems.

Marketing Support experienced in direct / partner sales of software and solutions to technology and C-level managers.

Excellent written and verbal communication skills

SITA APC EXPERIENCE

Managing the delivery of over 100 Automated Passport Control (APC) Kiosks projects to multiple international airports in the US and overseas. Work in partnership with MIA, kiosk vendors and US Customs and Border Protection (CBP) to deliver the projects on time and under budget.

**Rudy Hoffman, Lead Implementation Specialist**

Seasoned IT professional with a comprehensive business and technical skill set that includes expertise in; project management, business process improvement, database design and development, leadership, team management, process modeling, customer service analysis, network design and the airline industry.

Technical Engineer: Senior field engineer for a worldwide data communications upgrades involving airport and airline customers, specializing in processes, procedures and technical knowledge. Managed large site installations from pre-stage to final go live. Versatile experience working with local vendors and new sites on cabling, network designs, construction and implantation plans issues.

Database Administrator/Developer: Designed, developed and maintained an online Microsoft SQL Server database with ASP front end for use by a worldwide team supporting a major data circuit migration. Designed SQL queries and

SSIS packages to provide subsets of data for display to users. Developed a MS SQL database with ASP.NET front end to streamline the data entry and data tracking process with business rules built-in to ensure data integrity. Developed customer reports for use by management for business management. Developed cost analysis reports and automated alerts based on business rules which eased customer maintenance and property management issues.

SITA APC EXPERIENCE

Successfully deployed more than 100 APC Kiosks for US airports while working closely with customers and vendors to ensure prompt delivery of equipment. Has worked with vendors' technicians to promptly assemble, update and deploy kiosks. Coordinated with Customs and Border Protection to successfully test and place into operations the kiosks. Continually works to ensure the prompt and accurate delivery of specified hardware and software to guarantee all project requirements are met.

**Alberto de la Hoz, Implementation Specialist**

Experienced Miami based IT professional with a full technical and operational lifecycle of Government Security Solution projects including system design, software and hardware installations, network configurations, airline and government certifications and other technical support requirements.

Lead Implementation Specialist: Translated and aligned technical, business and operational requirements of GSL Border Management systems by providing technical implementation support to Government Security Solution Biometrics projects. Implemented and supported installation of the biometrics hardware, core hardware components, implementation of software as per installation and configuration. Coordinated with cross functional teams and third party providers to ensure project technical implementations are done in accordance with approved designs and keep within the customer agreed requirements.

Lead Support Analyst: Resolved system and network configuration issues and act as a liaison between the company and clients, identifying network issues and requirements customers may encounter. Implemented and supported of desktop devices, applications, peripherals, network devices, airline specific equipment (Kiosk, Flight Information and Checking Systems, Bag tags and Boarding Card Printers, Ramp Information Display Systems and Printers) using a variety of airline, proprietary checking and baggage tracking software.

SITA APC EXPERIENCE

Successfully deployed more than 30 APC Kiosks for US airports while working closely with customers and vendors to ensure prompt delivery of equipment. Has worked with vendors' technicians to promptly assemble, update and deploy kiosks. Coordinated with Customs and Border Protection to successfully test and place into operations the kiosks. Continually works to ensure the prompt and accurate delivery of specified hardware and software to guarantee all project requirements are met.

**Eric Barrie, Implementation Specialist**

Over 12 years of experience in planning, developing, and implementing state of the art information solutions facilitating corporate growth. Full project lifecycle installations and upgrades of server including project management, technical expert, and solutions adviser

Implementation Specialist: Interpret and support technical, business and operational requirements of Government Security Solutions Line (GSL) iBorders solutions by providing technical implementation support. Successful at developing long-range plans and managing application integration / data networking projects across multiple platforms.
Project Manager: Managed hardware assessment and IT environment readiness projects in support of hospital customers' clinical IT application upgrades. Project management and planning including contract oversight, activation and reporting, forecasting, time approval, scheduling, prioritization and dashboard tracking.
Sr. Systems Administrator Project manager for multiyear data archive restoration project. Implemented virtualization environment utilizing technologies such as VWmare ESX hosts, Network Attached Storage (NAS), iSCSI storage and Fiber Channel (FC) storage used. Provided 3rd level support for multiple software vendors.

SITA APC EXPERIENCE

Successfully deployed more than 30 APC Kiosks for US airports while working closely with customers and vendors to ensure prompt delivery of equipment. Has worked with vendors' technicians to promptly assemble, update and deploy kiosks. Coordinated with Customs and Border Protection to successfully test and place into operations the kiosks. Continually works to ensure the prompt and accurate delivery of specified hardware and software to guarantee all project requirements are met.

The project management and delivery lead for this project will be Mr. Rivero and Mr. Rudy Hoffman. Mr. de la Hoz will work directly with Mr. Hoffman. Mr. Barrie will be specifically designated to augment if necessary.

## ASSIGNMENT OF WORK OF PROJECT TEAM

SITA will provide a focused team to deliver each of the phases required by MDAD. While Miami-Dade County has suggested that the APC Kiosk program will be done in phases, SITA also has the ability to be flexible to support a more rapid or larger quantity implementation as needed. Some of the specific roles of the SITA project delivery team are identified in the RACI below.

| Area of responsibility | Rick Coffelt Head of Delivery | Berger Portfolio Rainer Project Director | Rivero Project Bob Sr. Manager | Lead Implementation Specialist | Alberto de la Hoz Implementation Specialist | Barrie Implementation Specialist |
|---|---|---|---|---|---|---|
| SITA Project Sponsor | X | | | | | |
| Immediate Project Escalation | | X | | | | |
| Quality Assurance | | X | X | | | |
| Overall Project Management | | | X | | | |
| Liaison to CBP | | | X | | | |
| Project Scheduling/ Installation Scheduling | | | X | | | |
| Arranging for transport/storage of Kiosks | | | X | | | |
| Technical Interface to customer/CBP | | | | X | X | |
| Assembly of Kiosks | | | | X | X | Support |
| Software implementation and SSL certificate installation | | | | X | X | Support |
| Implementation/Installation of Kiosks in FIS Area | | | | X | X | Support |
| Integration and On-site testing and acceptance testing | | | | X | X | Support |
| Implementation of Reporting Server | | | | X | | |
| Validation of Reports for MDAD | | | X | X | | |
| User/Ambassador Training | | | | X | X | Support |
| Transition to Operations | | | X | | | Support |

## APPROACH TO PROVIDING SERVICES

### Project Management Methodology and Strategy

In the following section we explain the Methodology we will utilize in the deployment and management of the APC kiosks. Also included in this section is information related to SITA's project methodology and/or project approach, training approach as well as the change management approach; all of which confirm our ability to manage the deployment and the maintenance of the APC kiosks at MDAD.

### Project Management Methodology

SITA's Project Management methodology is based on the Project Management Institute® (PMI) Project Management Body of Knowledge® (PMBOK) Fourth Edition, which provides a comprehensive structure for the overall scope of project management activities. As an augmentation to our structured Project Management Methodology, SITA has developed a Standard Delivery Process. Together, the methodology and delivery process puts forward a "best in class" service to our customers.

Our service model utilizes proven processes and methodologies built on ITIL (IT Infrastructure Library) best practices. Key operational objectives of SITA's service model include:

- Focusing on first time fixes
- Making use of remote diagnostics and fixes whenever possible to reduce cost and minimize downtime
- Optimizing the use of IT Assets
- Software management and control
- Standardization and simplification

## APC KIOSKS - SCOPE OF WORK TO BE DELIVERED

SITA will provide an experienced Senior Project Manager to work collaboratively with MIA ensuring provisions of this proposal are quickly and efficiently fulfilled. SITA will provide four phased deliveries of APC kiosks under this request and will utilize its experience with MIA and the US CBP to ensure the kiosks are rapidly installed and ready for operation. Please find detailed cut sheets with clearly marked dimensions of the APC Kiosk in Appendix B.

#### Project Kick-Off Phase

It is important at the start of any project to establish the main project players, stakeholders and project governance. SITA does this during a structured project start up phase. SITA, SITA-partners and key customer stakeholders will play important roles in setting up this project to be successful. Areas of focus during the Kick-off Phase are:

- Project Kick-off
- Main Stakeholder identification
- Agreed Project Plan
- Governance
- Communications Plan
- Risk Management
- Project Change Management
- Roles and Responsibilities
- Base lined Project Schedule

**Project Work Tasks**

SITA will be responsible for performing tasks throughout various stages of this project. The following is a list of these tasks which will result in the successful completion of this project:

- Project management
- Delivery and installation of certified APC Kiosks (all ADA / section 508 Compliant, including accessible to the sight impaired) at MIA
- Software configuration shall collect all Phase III information needed by CBP and shall be fully compliant with CBP's most current "Automated Passport Control Service: Technical Reference Manual (CBPTRM)".
- Install and configure the Kiosk solution locally at the airport to integrate with CBP
- Provisioning and Installation of Reporting and Management software as per specification
- Provisioning and installation of rack-mountable reporting and monitoring (RMS) server
- Final Integration and on-site testing with the CBP APC in accordance with the CBP OIT On boarding and Integration Testing process and agreed site OAT test plan
- Acceptance testing in accordance with the CBP OIT Integration Testing Plan
- Local Go Live
- Transition to on-site operational support with on-site training
- Support during the initial operational phase and operations
- Maintenance-Manuals – electronic files and required hard copies

## IMPLEMENTATION STRATEGY

### Delivery Schedule

SITA's proposed delivery schedule in Section 4.10 provides a detailed phased view of major deliverables envisioned for the project and is representative of the more detailed project schedule that will be finalized during the first two weeks after project award. This phased approach is repeatable for as many phases as Miami-Dade County deems necessary to meet its business goals.

### Key contributors and focus areas to successful Delivery

SITA utilizes its past experience with large scale airport projects, as well as current APC project deployments to define key metrics. Due to the decentralized architecture of our Kiosk System, SITA is able to start acceptance testing when the very first kiosks are delivered and installed. All that is required is access to the existing infrastructure via the Airports LAN/Internet and the SSL certificates installed. Once we have done the first series of test we will be able to work on a reduced test set to speed up overall implementation. There is no need to have central system in place first.

SITA believes that a successful project is directly attributed to how effectively a joint customer, supplier, and third party team functions together.

## APPROACH TO TRAINING MDAD STAFF

Training is critical for a successful implementation. SITA, in support of MDAD operations, will continue to train MDAD Ambassadors to better support the use of the kiosks and enhance the traveler experience with the upcoming implementation of Legal Permanent Residents (LPR's) or Green Card holders in Q4 2014. Additional information on the training provided by SITA can be found in Section 10 of this proposal.
SITA confirms that we will provide refresher information and implement additional training as needed to local airport staff, US CBP agents and any additional personnel deemed necessary by MDAD that covers the following areas:

- High level awareness / workshops for interested parties of the implementation
- Ambassador Kiosk training
- Ambassador application
- CBP staff training
- Train the trainer within the MDAD airport organization

## SCOPE AND CHANGE MANAGEMENT

SITA believes that strong project governance is a key element of project success, but SITA is also very cognizant that flexibility in operational airport environments must be maintained. SITA's project personnel are empowered to make on-site project based decisions that do not impact project scope and timely delivery. There are however times in any project when significant changes must be addressed. SITA's project methodology provides for project change management as a built-in component of its project governance.

A project change request to document a significant change should be submitted in writing with the following details:

- name and contact details of person requesting the change;
- description of change;
- origin of and reason for change;
- reference documentation;
- assumptions;
- details of change;
- impact of change (including but not limited to impact on milestones and timescales);
- impact on terms and conditions; and
- Supporting details relevant to the specific change action using the format above.

A change request is a "request" that does not in itself provide an obligation. It does identify a requested change and allows key project stakeholders the opportunity to review potential impacts before making an obligation.

At such time MDAD personnel submits a change order request, SITA will submit a Scope of Work (SOW) and provide a price quote (unless the changes have a zero pricing affect). Both MDAD and CBP must approve both the SOW and quote (if applicable) for all change orders before work will begin. However, the final decision on software changes will be provided by the CBP Office of Information and Technology. Until such time as a requested change order receives the appropriate approvals, SITA will continue to perform the project as originally agreed.

Any agreement to a requested or recommended change shall become valid once it has received appropriate approvals.

## PROJECT SCHEDULE AND MILESTONES

The Project Schedule/Milestones are provided in Appendix C and demonstrate SITA's ability to deploy and deliver the APC Kiosk solution in a timely manner for MIA. Our proposed schedule is based on the experience SITA has in deploying these kiosks and working directly with MIA and CBP for procurement, shipping and

installation of the kiosks. SITA will have the kiosks delivered, assembled and ready for final installation on time with the current version of the kiosk software.

## PLACE OF PERFORMANCE

It is assumed that the deployment of 144 kiosks will be done in phases and installed in the US CBP Federal Inspection Station (FIS) – US Pre-Clearance - at Miami International Airport per the following schedule:

Phase I: 36 APC Kiosks- Initial Purchase

Phase II: 36 APC Kiosks (12-18 months after initial purchase)

Phase III: 36 APC Kiosks (24-30 months after Phase II)

Phase IV: 36 APC Kiosks (12 months after Phase III)

## APPROACH TO PROJECT ORGANIZATION AND MANAGEMENT

SITA's strong partnership with MDAD and MIA and its existing install base of the 36 APC kiosks and connectivity at MDAD provide a significant opportunity to expedite the delivery of future APC kiosk requirements with little impact to ongoing operations. SITA's approach is to continue to work with US Customs and Border Protection both locally in Miami Dade and through the central office in Washington DC to ensure future implementations follow the same process as extensions of an already provided service. Additionally, SITA maintains a ready inventory of APC kiosks that allow us to respond rapidly to urgent requests.

SITA's approach for extensions of existing APC kiosks services is centered on a collaborative working environment that allows the airport department to fulfill its responsibilities (electrical power, local area network connections) in parallel to SITA delivering and installing the APC Kiosk devices. This parallel work provides a rapid and efficient joint work-effort to quickly address growing needs at the airport.

### Project Organization

As described in section 4.2, SITA will provide an experienced Project Manager and installation team to work cohesively with the airport authority, ensuring provisions of this proposal are quickly and efficiently fulfilled. SITA will manage the phased delivery of thirty-six (36) APC kiosks under this request and will utilize its experience with the US CBP to ensure the kiosks are rapidly placed through the US CBP certification process. To expedite this effort, SITA will immediately procure the first kiosk and ship it to the airport for installation, testing and certification.

SITA will utilize the fastest shipping method possible to ensure rapid delivery of the kiosk. This usually includes air transport from the manufacturing facility. The SITA Project Manager will provide details of the kiosk delivery including shipping and tracking information to the airport authority. While awaiting delivery of the

kiosk, the SITA Project Manager and the Implementation Engineers will work with the airport authority staff to ensure any facility prerequisites are addressed prior to delivery of the kiosks.

SITA will have the kiosks and core components delivered, assembled and ready for final installation on time with the current CBP Phase III compliant version of the kiosk software.

Installation is dependent on local civil works (electrical power and MDAD Local Area network) and coordination with local MDAD IT requirements being provided by MDAD.

The Activation, US CBP Soft Launch and Go-Live date for the kiosks that is typically required for new vendor installations will be bypassed if installations are accomplished as extensions of the service already provided by SITA. Therefore, the typical CBP on boarding process which is currently outlined as 6-8 weeks based on the CPB on-boarding procedures can also be bypassed. SITA's test plan is in two phases - one is an APC checklist that we use for setting up the kiosks and the second is the CBP on boarding; both of which can be found in Appendix D.

With early notification of a forthcoming implementation, SITA can further expedite items such as: SSL Certificate extensions, Standard Maintenance and name identifiers.

## CONTRACTOR'S ROLE

SITA will deliver a solution that will allow MDAD to capture the travel document, biometric and customs declaration data required by the US Customs and Border Protection Agency (CBP) for immigration processing of visitors to the United States (citizens, non-resident and non-citizens). The delivery phase is scheduled to begin immediately following project kick-off.

### Management Team Responsibilities

SITA will deliver the following components.

- 36 APC kiosks (ADA/Section 508 compliant units to be determined by customer), including all hardware and software required to operate the kiosks in compliance with CBP requirements for Automated Passport Control for Phase I.
- Customization of the APC Kiosk software as required to collect the information needed by CBP (Phase III process)
- Customization of the APC kiosk software to include integration with the CBP Automated Passport Control (APC) Services
- Delivery of the kiosks to site by air freight
- Kiosk installation

- Installation and configuration of the APC kiosk software
- Final integration on-site testing support with the CBP Automated Passport Control Services on-site, achieving certification by CBP in accordance with the agreed CBP OIT Integration Testing Plan
- On-site support during cutover and during the initial operational phase of the project
- Training of Airport staff (Train the Trainer)

**County Roles**

The County will be required to provide the following staffing needs:

Providing airport liaison with US CBP Staff to direct and assist passengers during the operational phase of the project
Customer Representative Staff in the FIS that have the ability to monitor the live status and usage of APC Kiosks,
Ambassadors who will assist the travelers on the APC process
Support Staff who are responsible for keeping the kiosk in operation,
On-site I.T. support staff

## PROJECT SCHEDULE

The table below provides the proposed delivery schedule:

| Task / Milestone | Week Due | Deliverable / Criteria | Responsible |
|---|---|---|---|
| Contract Award | Week 1 | Signed contract | SITA and MDAD |
| SITA and Customer assign project manager | Week 1 | Project Managers assigned to the project by both SITA and the customer. Names and contact details shared with both project manager | SITA and MDAD |
| Project Governance agreed | Week 1 | Main project stakeholders agree project R&R, Communications, Risk Management, Project Change Management and baseline schedule | SITA and MDAD |
| Project Schedule | Week 1 | Project Schedule provided based on current project understanding, including the delivery plan | SITA |
| Network Design | Week 2 | Network design and IP's confirmed | SITA and MDAD |

| Task / Milestone | Week Due | Deliverable / Criteria | Responsible |
|---|---|---|---|
| Kiosks Ship | Week 2 | Kiosks air shipped to site | SITA |
| Build out Kiosk area (civil works) | Week 3 | Provide power and network connectivity/cabling to kiosk deployment | MDAD |
| Kiosks on site | Week 3 | Kiosks cleared through customs and delivered to site | SITA |
| Kiosks assembly, installation and prelim network test | Week 3 | Final assembly, install and test kiosks in deployment area | SITA and MDAD |
| Device Naming | Week 3 | Establish OIT compliant workstation names | CBP and SITA |
| Testing Plan Reviewed | | SITA Test Plan | SITA, MDAD and CBP |
| Integration testing | Week 3 | Integration testing with existing SITA APC infrastructure | SITA, MDAD and CBP |
| Production Verification | Week 3 | Verification Testing | CBP, SITA, MDAD |
| SITA Support Training | Week 4 | Training to SITA local on-site personnel | SITA |
| Airport Authority and CBP training | Week 4 | Training to Airport Authority and CBP officer | SITA, MDAD and CBP (CBP if required) |
| Operational Support | Week 4 | SITA project team transitions to operations team | SITA and MDAD |
| Customer Acceptance | Week 4 | Customer Acceptance of the APC Kiosks | SITA and MDAD |
| Project Completed/ Close out | Following Customer Acceptance | Official close-out of the project | SITA and MDAD |

## APC KIOSK OVERVIEW

The SITA APC Kiosk is a multimodal biometric system that performs the process of citizen's enrollment or traveler's biometric verification, in a seamless and prompt manner. The Kiosk assists the traveler during biometric capture, performing numerous automatic adjustments and quality control checks.

The result is the acquisition of biometric data in accordance to International norms and standards, such as ICAO facial image recommendations, NIST fingerprint standards, EU specifications and other internationally accepted rules.

The Kiosk is ergonomically designed to adapt to travelers ranging from 4 feet 7 inches to 6 feet 10 inches in height in height, even allowing its use from a wheel chair, with optimal results for data capturing.

The APC Kiosk is optimized to fulfill ICAO recommendations by taking the traveler photo in frontal position at eye level, assuring the best results for facial recognition within ICAO parameters.

The APC Kiosk was designed with the end user in mind, thus optimizing the process flow. User feedback from previous projects, as well as the structural and architectural conditions found during previous deployments, is the basis for continuous development and improvements.

The APC Kiosk includes several features that provide:

- Quick biometric verification process- including liveness detection
- Quality assured biometric data collection;
- Ergonomic usability to the traveler.

One of the features that provides speed and quality of biometric capture is the automatic height adjustment of the illumination & camera module. The system detects the ideal height for the camera to perform the face capture, and gives any user the same ideal conditions to capture full frontal pictures.

In the context of CBP's requirements for Automated Passport Control, the biometric capture devices and software included in the Kiosk are used to optimize the biometric verification. The facial and fingerprint recognition engines run on the kiosk computing platform and are used to ensure that the traveler using the Kiosk is correctly authenticated. In addition, the combination of 3D sensors and software can confirm liveness of the person by detecting when a static photo or a video are presented in front of the camera. If the face is considered to be a fake, then the image is not captured and the passenger can be directed to a manual investigation/inspection.

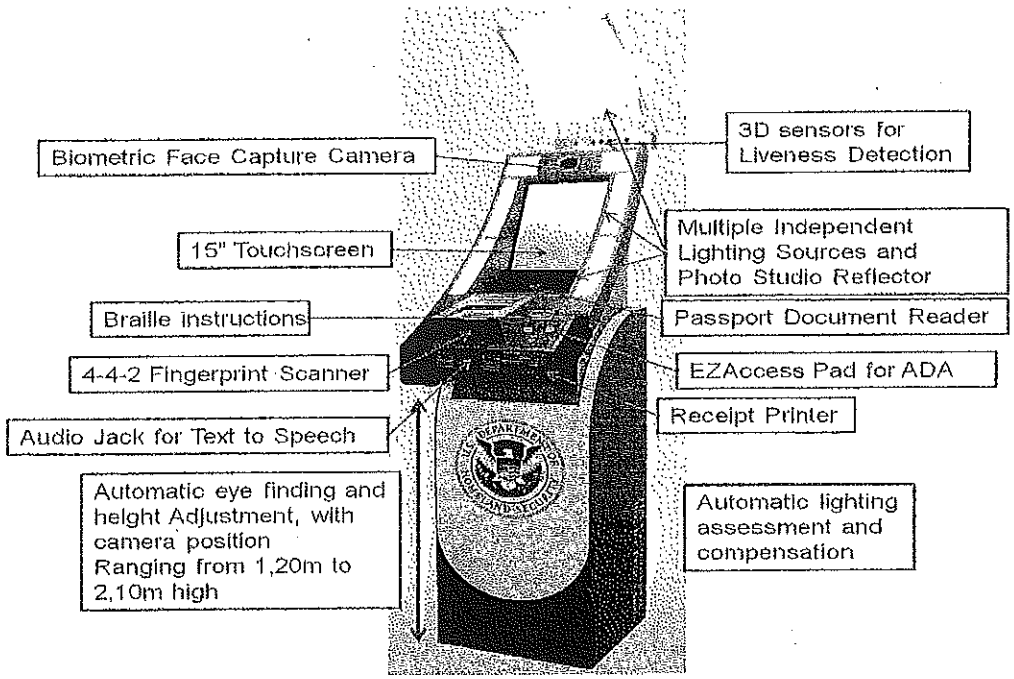
The APC Kiosk features all the components, software and quality assurance criteria to ensure state-of-the-art of biometric data capture to meet and exceed the specifications for Automated Passport Control.

The Kiosk is low maintenance and has easy access for users in an ample height range, including children or people in wheelchairs. It also has a small footprint and it's easy to deploy and to operate. It supports the user

through all the stages of the traveler verification workflow, providing usage instructions and feedback in the form of configurable text, pictures and animations, displayed on an embedded LCD screen.

## APC Kiosk Components and Design

The following image shows the SITA APC Kiosk with all the standard components.




### Component Description

- Anti-vandalism Chassis - Ergonomically conceived chassis with elegant design and an anti-vandalism finish. The chassis is highly modular, so will host all other components.
- Touch TFT - 15" TFT monitor. The interface between the traveler and the kiosk.
- APC system - Provides guidance during the process and allows the traveler to answer any questions on the screen.
- Receipt Printer - Thermal Printer to issue a receipt containing the traveler's image, passport information, country of citizenship, flight info, and CBP results and is identified as Automated Passport Control receipt. (sample picture included with attachments)

- Passport Document Reader - Embedded passport reader which can read the Machine Readable Zone (MRZ).
- Face Capture Camera - Facial camera selected for fast and accurate image capture for biometric verification. Takes live frontal eyes-level pictures of the traveler, according to ICAO recommendations.
- Fingerprint Reader - High precision 4-finger ('slap') fingerprint device.
- Integrated CPU - Central Processing Unit that supports all devices and applications of the identification module, providing Web Services available to systems operating the Kiosk.
- Lighting - Set of LED lights properly adapted to support live photos taken in any existing airport environment light conditions.
- Signage – Lighting technology for queue management to display availability of kiosk to the passenger ( sample pictures are included with attachments)

**Physical Characteristics**

- Materials - Ionized Steel
- Finishing - Epoxy painting
- Maintenance – generally maintenance free. Easy access.
- Security - Anti-vandalism

**Connectors**

- 1 x US Power Plug
- 2 x RJ45 Ethernet (other connection interfaces available)

**Dimensions**

- Length 11.8 inches
- Width 11.8 inches
- Height Up to 74.8 inches
- Weight up to 331 lbs

**Environmental Description**

- Operating Temperature +0°C / +40°C
- Storage Temperature -20°C / +65°C
- Power < 300 W (including all components)
- Certifications CE, RoHs, UL/TUV

## APC KIOSK FUNCTIONS

The APC Kiosk system is a multi-functional and adaptable unit, which can be configured for different business requirements. In the context of the current CBP Automated Passport Control requirements, the Kiosk will perform the following functions:

- Kiosk to display availability – green light for available, white light for in use and red light for not in service.
- Initiate the session with the traveler(s) and CBP's Automated Passport Control (APC) Service;
- Request and receive the APC Service system status message;
- Meet the business, technical, and operational requirements;
- Request and receive the latest flight list information from APC Service;
- Display information and instructions to the travelers;
- Collect the necessary travel information from each traveler;
- Prepare and send the Validate Travel Request;
- Process vetting results from the Validate Traveler Response;
- Prepare and print receipts for each traveler as specified;
- Request and receive the Terminate Session messages;
- Record and document session information.

In addition to these required functions, it is important to highlight that the introduction of non-United States Citizen travelers to be processed by the APC system requires the capture of fingerprint biometric data. Both fingerprint and facial photographically captured biometrics will be performed by the APC Kiosk, in compliance with international standards, such as ICAO, NIST and other references.

## APC KIOSK HARDWARE SPECIFICATIONS

The proposed APC Kiosk comprises the following components:

- **Traveler Display** – A 15" touch-screen LCD to be used by the traveler as the main interface with the APC system. It will provide the traveler with messages from CBP, guidance instructions about the APC process and live images of the captured biometrics.
- **Facial Biometric Camera** – A camera system that performs automatic height and camera settings adjustment, to capture ICAO compliant facial photographic images.
- **Dynamic LED Illumination system** – A framework of fixed LED arrays vertically aligned at the tower, on each side of the camera and traveler information display. The LED frame is sectioned in various groups of LEDs, which lighten up at different heights and intensities according to the height of the passenger. It creates symmetric lighting around the face, in combination with the automatic height adjustment and compensates external environmental circumstances. The illumination is automatically adaptable to the ambient conditions and camera settings, and compensates for backlight. This technology assures a symmetrical illumination of the face, following ICAO recommendations.
- **Passport Reader** – An embedded passport reader which will scan the MRZ data and use OCR to capture the traveler personal information.
- **Slap Fingerprint Scanner** – An FBI EBTS certified 4-finger slap scanner is integrated in the Kiosk structure, to perform non-US Citizens biometric capture.
- **Thermal slip printer** – A thermal printer will issue each traveler with a Passage Granted Receipt or a Referral Code - according to the verification output. The receipt contains the traveler's image (see the picture to the right).
- **Embedded PC** – A computer placed inside the Kiosk with pre-installed biometric capture and processing software – APC software suite.

## LIFE CYCLE OF HARDWARE

For optimal life, it is recommended to upgrade / enable new features as soon new CBP phases are implemented, in addition to regular maintenance.

The kiosk is specified to support both the current US CBP business requirement phases and has built-in enhanced features that will be required in future US adoption of biometric entry processes. The processes will mandate facial recognition, enhanced document verification and authentication.

The operational life cycle of these units are designed to support the current mandated requirements of commissioning date and advance phases of APC. We anticipate these requirements will become mandated in the next 12-24 months.

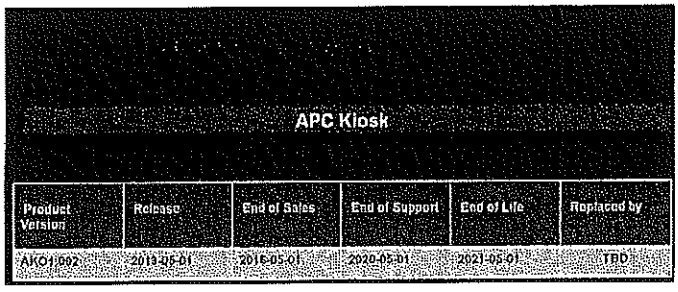
The operational life cycle of the APC kiosks is designed to enable support of advance capabilities. This will ensure that no retrospective installation will be required for optics, document and fingerprint readers. These components are all using the latest technology that meets and exceeds the US requirements mandated for APC.

Today they conform to higher ICAO standards for facial capture. The software and the hardware are continually reviewed to make sure that integrity is maintained to the latest ISO/IEC, NIST and NIFQ standards. SITA does not foresee any change in design of form factor or in component changes to support known US entry processes for the lifetime of the contract.

SITA recommends adherence to the manufacturers specifications for preventative maintenance for MIA to maintain the optimum operation of the kiosk through the lifetime of the contract term.

The number of times an upgrade will be required is dictated by CBP's future phase requirements, implementations and mandates. When a new requirement or phase upgrade is required, a software upgrade maybe required to update workflow processes and to enable a license feature for activating pre-loaded features.

System updates and maintenance will be carried out at as agreed with scheduled windows. A list of approved and certified operating system patches for kiosks and servers will be supplied, as required for deployment.



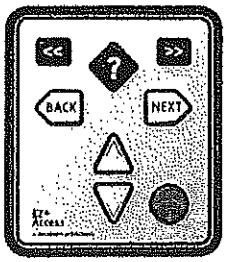

The delivery and/or support team will need to re-validate any operating system patches and follow change management procedures. Prior to rolling out to all kiosks at the onsite location, it is recommended to create an extra group in windows update services or in the SCCM (systems center configuration management), and add a test Kiosk to apply the approved patches.

Kiosk application and firmware updates will be delivered via digital download (ftp, website) or USB memory stick with detailed instructions. Should manual patches be required onsite, then SITA will provide the level 1 team (if applicable) with the instructions and software to perform the patching as needed.

## ADA / SECTION 508 COMPLIANCE

All ADA kiosks offered are ADA/Section 508 compliant and will be provided as follows:

- The ADA/Section 508 compliant kiosks are compliant with height and reach restrictions to make the unit workable for someone in a wheel chair. Note that the area in front of the kiosk must allow for positioning of a wheelchair, turning etc. (This is the responsibility of MIA).
- The touch screen will be operable by a gloved hand or prosthetic.
- The user interface will employ colors/contrast and fonts suitable for the visually impaired and color blind.
- The kiosk will be operable by blind persons using an integrated EZ-Access device.
  - The EZ-Access device, shown to the right, is a multi button keyboard (select, back, up, down etc.)




USB

Operation of the kiosk using this device will be as follows:

- Plugging in a headset will trigger a call to the ADA page, which will allow the customer to adjust the volume and request privacy (in which case a privacy screen will layered over the user interface to someone shoulder surfing the blind person without them knowing it).

stop

- The blind user selects options from voice menus using the EZ-Access device to navigate the menus. Keystrokes entered using the EZ-Access device are recognized and used to drive the voice interaction.
- There is also a Braille pad attached to the kiosk with basic instructions on where to find the headset jack socket.
- At the completion of the session, the EZ-Pass kiosk will revert back to normal operating mode for the next customer.

SITA has a great deal of experience delivering ADA/Section 508 compliant kiosk solutions. The QuikTrak ticketing kiosks used by Amtrak across the United States (more than 300 deployed) were designed and built by SITA, including both hardware and software. These devices are fully ADA/Section 508 compliant utilizing the EZ-Access device as described above.

## KIOSK MANAGEMENT SOFTWARE

The APC Software suite is responsible for:

- integrating all the hardware components of the Kiosk;
- providing an ergonomic user experience;
- assuring the quality level of the captured biometrics; and
- Communicating with CBP's APC Service, via the embedded kiosk server software.

The Software will be responsible for the communications between the Kiosk and the APC system, according to the specifications defined in CBP's APC Technical Reference Manual. The XML messages will be verified by the APC Software, before being sent to the APC System, to assure that they are well formed and valid. These messages include the traveler information, responses to declaration questions and other requests. The APC Software will also be responsible for receiving the Response messages from the APC system, such as vetting responses and Flight List update.

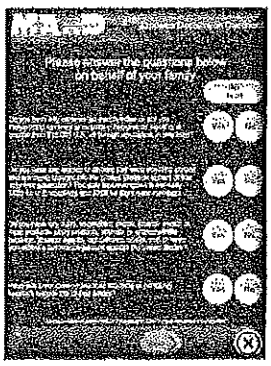
Additionally, the Software will also make sure that each traveler or family unit member answers the mandatory Declaration Questions. The APC Software will only allow the traveler to move forward on the verification process once all answers are provided.

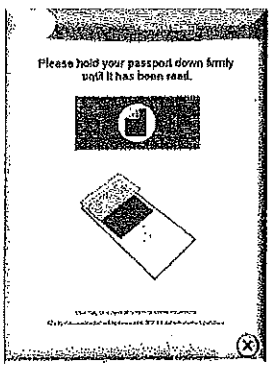
The APC software allows for a complete customization of the screens, including, but not limited to, wallpapers, fonts, font size and color, logos and other images, animations, videos and audio messages.

The traveler can select their language at the first step of the workflow. SITA confirms it will configure the Kiosks with those languages outlined in the RFP.

The traveler experience is optimized by the intuitive usage of the Kiosk hardware and software (clear animations are displayed for each action to be performed by the traveler), the accuracy of the captured biometrics (which reduces the need to repeat the capture process) and overall high speed of the process.

The following screenshots are examples of possible customizations of the instructions provided to the traveler during the APC process.





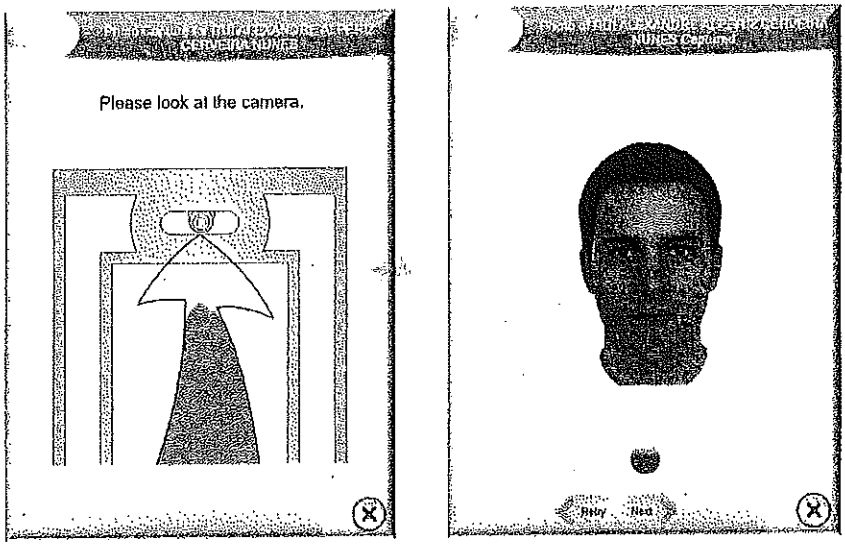
Good-quality biometric images are of the utmost importance for the success of the program. In order to assure both accuracy and quickness of the process, both the fingerprint and facial biometrics are assured to be compliant with the ICAO and NIST standards. To achieve the desired high quality output, the APC software suite provides clear instructions and is teamed with the integrated hardware devices to achieve excellence in the biometric quality.

## Face Capture

The automatic height adjusting mechanism is designed to optimize face capture. It is combined with dynamic illumination to compensate for environmental lighting variations. The face capture component of the Kiosk aims at generating the highest quality ICAO compliant face images of the travelers. A quality analysis tool ensures the quality of the face capture resulting in better recognition performance (in terms of false acceptance and rejection rates) and time needed.

The process of collecting the face image begins with the presentation of the live image on the screen. The acquisition process is initiated through the user interface, and processed by the APC software, which manages the camera settings, illumination and height adjusting mechanism. There is no need for direct intervention in the settings of the camera, since it is automatically configured for each capture.

The APC software guides the traveler during the face capture, providing clear instructions and providing a live image of the capture. When the Kiosk is adjusting the camera height, lighting intensity and other camera settings, the traveler is instructed to look at the camera. When all the settings are correctly adjusted to the traveler and surrounding conditions, the APC Kiosk performs the facial image capture.



When the image is captured, the system displays it and starts the internal process of normalizing the raw image to ICAO standards. Once the image is processed, the passenger is informed if the process was successful or not, and the resulting normalized image is shown.

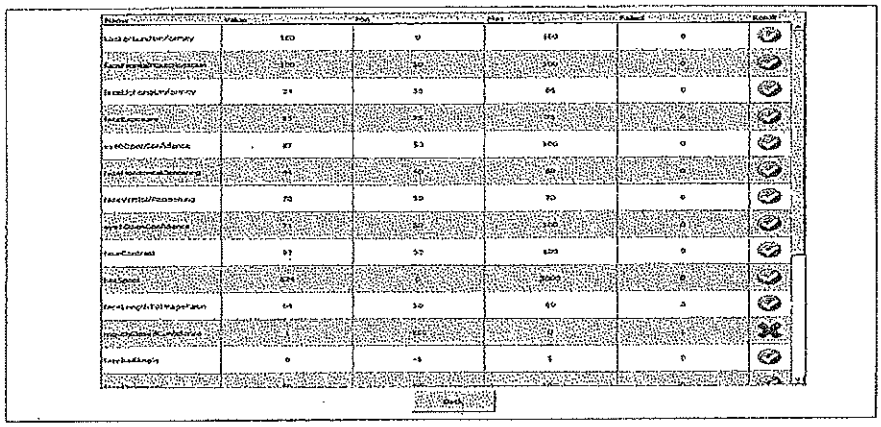
The APC software image pre- and post-processing assures that the final image meets international standards and best practices, such as ICAO Doc. 9303 Part 1 Volume 2 and the validation parameters that are defined in detail in ISO / IEC FCD 19794-5. Among the verified and assured parameters, are the following listed by CBP:

- Pose: Full Frontal or Frontal Token
- Angle: +/- 5 degrees in all three dimensions
- Expression: Neutral
- Eyes: Open with >90 pixels from pupil to pupil
- Background: plain with no texture
- Lighting: No shadows or point lighting
- Size: Minimum 640 x 480 pixel
- Face Size: >1/2 width of frame and>3/4 height of frame
- Camera: 24 bit color

Furthermore, the APC software face component also checks the following parameters:

- Degree of confidence in the eye detection
- Check for open mouth
- Check for glasses
- Head tilt (tilt)
- Head rotation (pan)
- Brightness of the face
- Sharpness of the face
- Contrast of the face
- Color Balance of the face
- Centering of the face
- Eye Shadow
- Shadows in the face
- Brightness of the background
- Shadows of the background
- Consistency of the background

The APC software has a Quality Assessment screen that shows the score of the picture in each verified metric. This screen can be shown to an operator for diagnosis of issues. In normal operation, it is hidden and only used to generate instructions to the traveler when the picture is not valid. This QA screen is shown in the following picture.



The location of the face in the captured image is automatically performed in real-time without any human intervention, by detecting characteristic points of the face, such as the eyes. The APC software also automatically performs live-ness detection, to assure that no spoofing is permitted (such as holding a printed photo to be captured).

The image normalization process includes automatic repositioning of the face, changing the scale relative to the size of the image and eliminating rotation of the head slopes up to 15º. The correction of color balance, brightness and contrast is also performed in real time.

The facial photographically captured biometric can be output in a number transmittable formats, such as JPEG, JPEG 2000, and PNG.

The following images show the reference measures in compliance with ICAO Doc.9303 Part 1, Vol 2 (on the left) compared with an image generated by the APC software (on the right).

Geometric Characteristics of the Captured Image

- Image Width W
- Image Height W/0.75
- Y coordinate of Eyes 0.6 * W
- X coordinate of First (right) Eye 0.375 * W
- X coordinate of Second (left) Eye = 0.625 * W (0.625 * W) - 1
- Width from eye to eye (inclusive) 0.25 *W

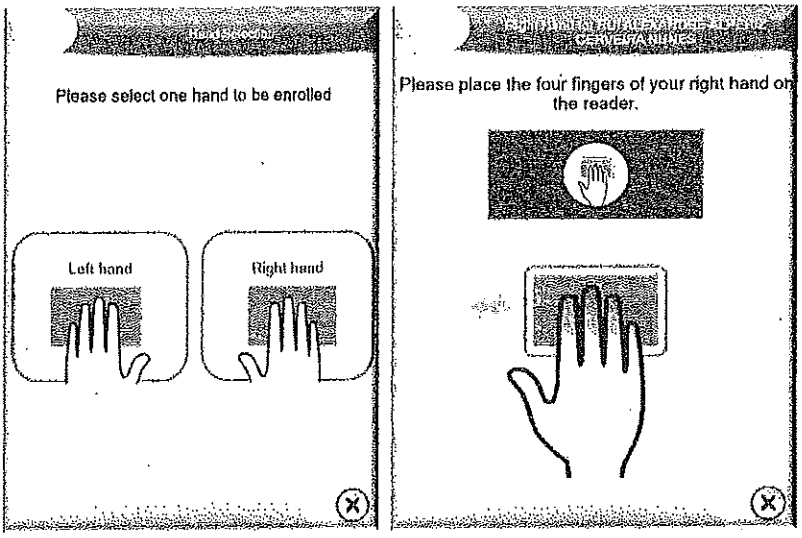
For accurate image cropping with automatic background removal, the APC can be offered with the option of an illuminated backdrop that can be ordered through a change order. Together with the background removal software, the Illuminated Backdrop allows a 100% white background, 100% accurate face image crop, which is not possible to achieve with traditional backdrops, as compared in the images below:

**Fingerprint Capture**

When the traveler is required to perform a fingerprint capture, the APC fingerprint module automatically activates the fingerprint reader.

The fingerprint module shows the image of two hands and highlights the fingers which must be captured. It also shows a live image of the capture, a side-bar which informs about the capture progress, and the NFIQ score given to each captured finger. The software may also warn the traveler for any error that occurred during the capture.

Shown below is an example screen simplified as appropriate for self-service use.

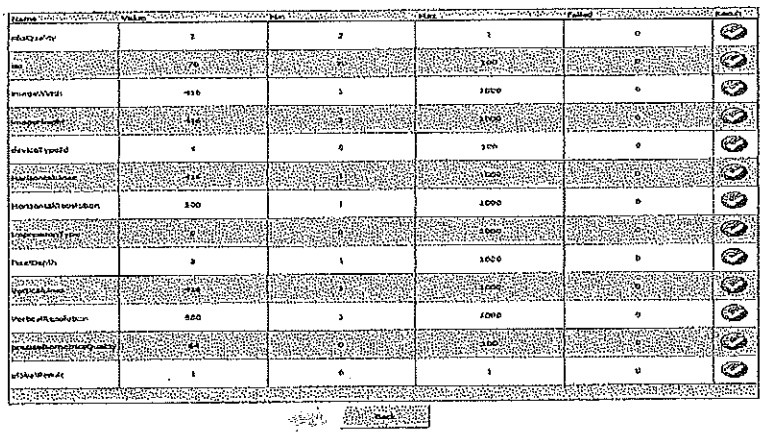



Once the fingerprints are captured, the APC software automatically performs quality checks. This feature ensures that all recorded fingerprints meet the same standards of quality. The real time verification software is based on the

standard NIST Fingerprint Image Software 2 algorithm (NFIS2), and automatically scores each fingerprint according to the NFIQ five levels of quality thresholds. The following parameters are evaluated for each fingerprint:

- Selection of finger(s)
- Image capture and display
- Quality Checks:
  - Isolate fingerprint, guidance and validation to ensure presence of the core;
  - Appropriate contrast peaks and valleys;
  - Sufficient Coverage;
  - Sufficient detail;
  - Sufficient signal to noise ratio;
- Image size
- Position and orientation of the image
- Distortion

Similarly to the Face Capture module, the APC fingerprint module also generates a detailed Quality Assessment screen, which can be viewed by an operator or used to generate user instructions when the capture does not meet the required quality requirements.



If the image achieves all parameter thresholds for quality assessment, it is automatically accepted. Otherwise, the system makes a configurable number of recaptures until the required quality is met. The APC software includes all the tools required to ensure the quality of captured image, optimized for all types of algorithms for fingerprint recognition. The algorithm used by the APC software meets FBI standards for Wavelet Scalar Quantization (WSQ) Gray-scale Fingerprint Image Compression Algorithm exchanges.

The APC software will only accept the fingerprints that achieve the required NFIQ scoring stated in the table provided by CBP:

| Number of Finger | Name of Finger | NFIQ Required Scoring |
|---|---|---|
| 1 | Right Thumb | 1-2 |
| 2 | Right Index | 1-2 |
| 3 | Right Middle | 1-2 |
| 4 | Right Ring | 1-2-3 |
| 5 | Right Pinky | 1-2-3 |
| 6 | Left Thumb | 1-2 |
| 7 | Left Index | 1-2 |
| 8 | Left Middle | 1-2 |
| 9 | Left Ring | 1-2-3 |
| 10 | Left Pinky | 1-2-3 |

APC CBP Service Workflow

The APC Service workflows have been designed by CBP and depend on the citizenship of the traveler:

- APC Service Phase I – US Citizens only.
- APC Service Phase II – US and Canadian citizens.
- ***APC Service Phase III – US, Canadian citizens and Visa Waiver Countries (biometric capture required)***
- APC Service Phase IV – US, Canadian citizens, Visa Waiver and all others (biometric capture required)

As requested in the RFQ, the Kiosk offered is for Phase III functionality.

The SITA APC kiosk is the first Phase III complaint kiosk deployed in North America.

### 5.2.1 US Citizen and Canadian Workflow

The US Citizen and Canadian Inspection process starts with the traveler approaching a Kiosk, which is displaying a welcome message where he/she is asked about their nationality (US, Canadian or an ESTA member – Visa Waiver) and the number of persons travelling together as a family unit.

The Kiosk shows the "Customs Declaration Questions" screen, in which the traveler is required to answer every question. The Kiosk will not allow the traveler to move forward in the inspection process if any answer is missing.

The traveler, or one family unit member at a time, places his/her Passport on the Kiosk document reader, which will scan the MRZ data. If the traveler is not a US citizen, the process is concluded. If he is a US citizen, he will be asked to perform the facial image capture.

The Kiosk assists the traveler during the face capture process. It provides instructions in the user display, while automatically adjusting the height of the camera and other camera settings. When the valid picture of the traveler (or every family unit member) is taken, the Kiosk proceeds to issue the relevant data to CBP's APC system for several verifications.

If the CBP APC system verifies that the traveler actually is not a US citizen, the process is immediately concluded. If the traveler is referred, the Kiosk prints a receipt with Referral Code and the session is terminated.

In the case of Granted Passage, the Kiosk displays the Flight Information and asks the traveler to verify it. If it is wrong, the traveler can manually enter the correct flight information. When it is correct, the Kiosk prints a receipt with Passage Granted and terminates the session. The process is then concluded.

## VISA WAIVER PROGRAM - VWP

For citizens of those countries participating in the VWP, the process starts with the Kiosk first asking the traveler's nationality and number of travelers in the family unit and then requiring the completion of the 'Customs Declaration Questions' screen.

Each traveler must then place his/her passport in the document reader, indicate their reason for travel, perform the 4-print fingerprint capture and then perform a face photo capture.

The Kiosk sends the traveler's data to the CBP's APC system, which performs a number of verifications/checks.

At this point the process can take one of the following two directions:

- **For non-VWP Country travelers**, the APC system will check for referrals. If the traveler is "Referred", the Kiosk prints a "receipt with referral code" and terminates the session. If the traveler is not referred, meaning that he gets a "Granted Passage", the Kiosk displays the traveler's flight information and asks him to verify it. If needed, the traveler can manually enter the information. Then, the Kiosk prints a "Receipt with Passage Granted" and terminates the session.
- **For VWP Countries**, the CBP APC system will check for the ESTA status. If it is not active, the system will immediately check for referrals and follow the process described in the previous bullet-point. If the traveler has an active ESTA, the system will check for pre-verified biographic data.

When the traveler has enrolment data on file, the system may submit the captured 4-print and photo for biometric verification. If the traveler has no enrolment data on file, the additional data may be captured, sent to the APC system, and submitted for biometric verification. If the biometrics are verified, the CBP APC System will then check for referrals and follow the process described in the previous bullet point.

## LEGAL PERMANENT RESIDENTS – LPR

SITA's APC kiosks, with software version 4.3.8, will now support **Legal Permanent Residents (LPR)** or Green Card holders.

For US LPR's, the process starts with the kiosk first asking the traveler's nationality and number of travelers in the family unit and then requiring the completion of the 'Customs Declaration Questions' screen.

Each LPR traveler must then place his/her LPR ID1 card and passport in the document reader, indicate their reason for travel (LPR), perform the 4-print fingerprint capture and then perform a face photo capture.

### Facial Matching

The SITA hardware and software can support future APC phase IV facial capturing and 1:1 matching. At the present time, the technology exists and CBP will publish the Phase IV business and technical requirements when appropriate. SITA is also working with CBP to perform the first facial matching pilot, which will most likely form part of the Phase I requirements in the future.

The capture of a good-quality facial image is of high importance particularly when capturing a live facial image of the traveler and comparing it with an image stored on the chip of the traveler's electronic travel document or on a database. The SITA APC Kiosk is equipped with an optimized facial capture system to accommodate this requirement.

The face capture and matching module of the proposed APC Kiosk benefits from the significant expertise acquired after deploying hundreds of Biometric Enrollment and Automated Border Control solutions which perform similar face matching processes. The proposed solution provides travelers with an extremely positive user experience, while letting the Kiosk automatically adjust to the characteristics of each traveler and the environmental lighting conditions. This feature performs the face recognition process with highest possible speed, accuracy and security, according to ICAO Doc. 9303 recommendations and ISO/IEC 19794-5 specifications.

During the Automated Passport Control clearance phase, the facial comparison system is able to perform biometric matching between the live facial image captured at the APC Kiosk and a photo stored on a travel document or against a database.

The facial detection and matching process aims at computing the best possible score within the smallest time-frame and using the minimum number of attempts. This approach differentiates itself from common face detection and matching procedures being distinguished as a "de facto" technique in the current biometrics state of the art system.

Common recognition methods act as "brute-force" detectors and matchers that try to compute a recognition score for each acquired sample image, resulting in poor performance and identification times. The proposed method tackles these poor performance issues and improves identification times with a high accuracy level by following a sensor fusion approach.

Each sample frame is scrutinized (Quality Assessment module) in order to extract multiple image quality metrics and features which will help the system to quickly auto-adjust (Quality Adjustment module) to respond to several established quality requirements. This process results in a boosted full-frontal face image, according to ISO/IEC 19794-5 specifications, thus increasing the probability of achieving the best possible recognition score.

The APC application utilizes a specifically designed quality analysis tool to ensure the quality of the face capture for biometric verification. Any facial image approved by the APCs quality analysis tool ensures high recognition performances, in terms of false acceptance and rejection rates, and time needed to obtain an acceptable matching score.

The Quality Assessment module also acts as an image quality "inspector", giving clearance only to high quality full-frontal ICAO compliant samples. This feature will prevent the system from wasting time trying to match impractical low quality face images which would result in poor recognition scores. If the document's chip image does not present a reliable level of quality, the APC Kiosk can automatically adapt by raising the matching threshold for preventing false matches.

By allowing the Quality Assessment module to feedback information, this module automatically tunes several hardware specific parameters such as biometric camera exposure time, diaphragm aperture, lens focus, color temperature and saturation, electronic gain, brightness, contrast and sharpness. In addition to that, this module also controls the multi-independent light source illumination system (MILSIS®) which guarantees the best possible light exposure, resulting in a seamless homogeneous facial surface.

In order to optimize the efficiency of the facial image matching processes, only the images that have been accepted by the Quality Analysis module, based on ICAO recommendations, will be applied for the matching process. The system checks the quality of the facial image according to the following set of metrics:

- Degree of confidence in the eye & live detection
- Check for closed eyes
- Check for open mouth
- Distance between the eyes & grey scaling
- Head tilt (tilt)
- Head rotation (pan)
- Brightness / Contrast & Sharpness of the face
- Color Balance of the face
- Size of the face
- Centering of the face
- Eye Shadow (free)
- Shadows in the face (free)
- Brightness, Shadows of the background

The proposed method leverages the symbiotic relationship between Quality Assessment and Quality Adjustment modules as well as the plug-in-based software architecture, which is an outcome of long term research and development. This feature provides a distinct experience in Automated Border Control Systems, ensuring a service level of maximum four (4) seconds for face detection and matching. The matching process can be

executed in parallel with other APC Kiosk internal processes for an improved overall passport control processing speed.

The face matching module is an integrating part of the proposed SITA APC Kiosk software suite, which does not require any further integration with additional systems. By simply activating the face matching module on the SITA APC Kiosk application, the kiosk will be able to not only capture an ICAO compliant face image but also to perform the biometric matching between two photos as well.

## KIOSK ARCHITECTURE – TRANSACTION MANAGER

SITA has chosen an architecture where the Transaction Manager is considered to be local to each kiosk. The 'local' Transaction Manager application installed in each Kiosk communicates directly with the CBP APC Services. This is the default and standard configuration for SITA's APC deployments.

**Utilizing a local Transaction Manager within each kiosk ensures the highest level of availability for the overall system. Any problem within a single kiosk does not stop the other kiosks operating correctly. Also, there is no dependency on a 'local' airport server, thus removing another single point of failure. Each kiosk communicates directly with CBP.**

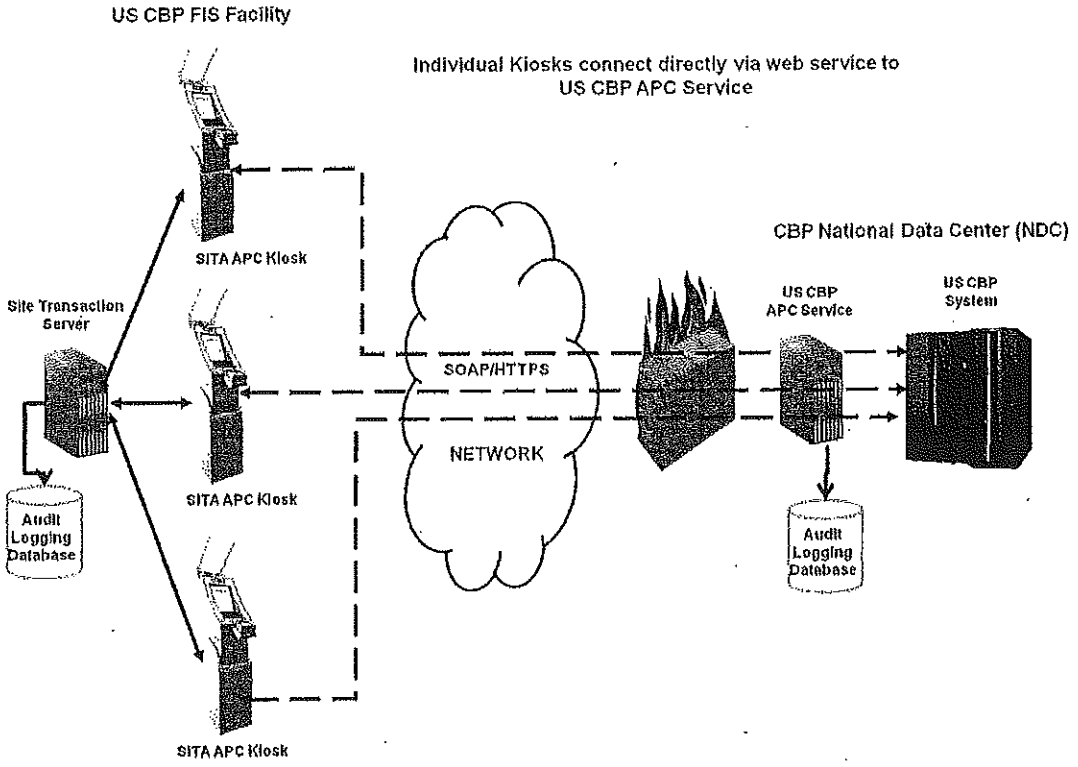
### Failover Strategy and Recovery from Unexpected Power Outage

Each kiosk communicates directly with the CBP Server, the kiosk acts as its own individual, local server, rather than having to be routed through one intermediate remote server. This means that the kiosks operate independently in a resilient manner with less points of failure.

The Transaction Manager is an integration layer comprising web-services to make the APC Kiosk functionalities available to front-end client applications with customized user interfaces, as well as to backend systems. In the APC Technical Architecture diagram (provided by CBP) the Transaction Manager has the role of central "Site's Server". The Transaction Manager may be deployed at different points of the technical architecture.

In the event of a power outage, Kiosks will restart automatically upon power restoration. The server room infrastructure location will continue using a UPS (uninterruptable power supply).

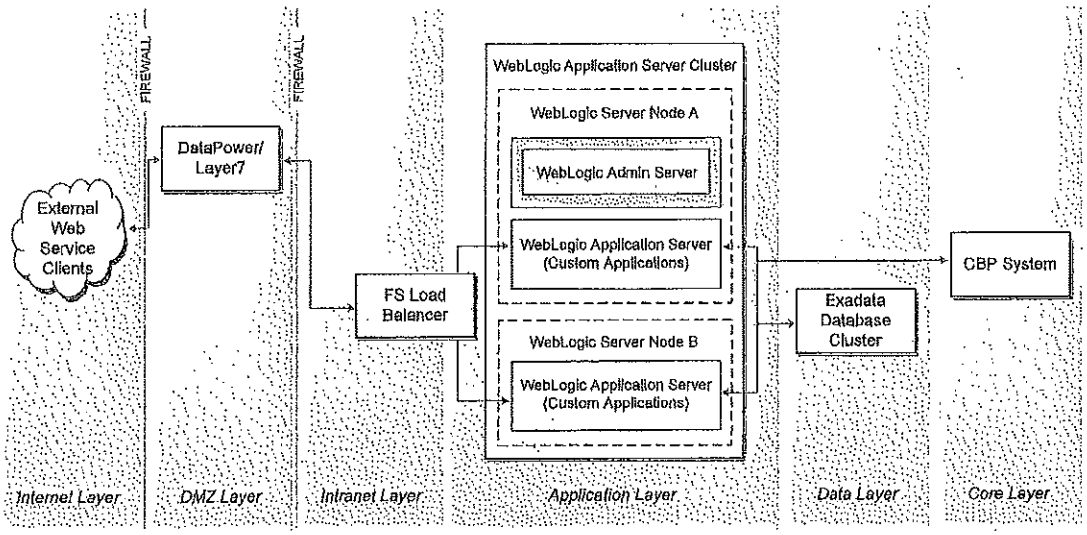
## SITA APC Kiosk High Level Technical Architecture (Network Redundancy)




**INTERFACE TO CBP:**

The Transaction Manager coordinates the workflow configuration for each Kiosk, including the composition of tasks that must be performed in a process and how to handle the exceptions. It plays a key role in the setting and monitoring of the business rules. The Transaction Manager also presents the single interface between the Kiosk and the CBP APC Service Server.

The CBP side of the interface supports high availability. The architecture consists of F5 network load balancers, with web logic middleware that has logical clusters using web logic and the CBP web services .EAR / .WAR files deployed to the web logic cluster. The following CBP diagram depicts the logical architecture:




## SECURITY AND DATA PROTECTION

### Encryption of Information

SSL is a secure protocol developed for sending information securely over the Internet and used with https web service connections.

SSL encrypts the data being transmitted so that a third party cannot "eavesdrop" on the transmission and view the data being transmitted. Only the user's computer and the secure server are able to recognize the data. This protocol is used for secure connectivity to CBP. Two way SSL public certificates are used from either Entrust or VeriSign.

### Application Security Framework

Kiosks are physically connected using RJ45 connectors over Cat5/5e/6 networking cabling. They are logically configured to use a V-LAN segment, connected to a Cisco 3750 switch and Cisco ASA 5505 firewall / router for secure separation to other networks. V-LAN's are created. Trunking used for separation between Kiosk, Local LAN and Internet networks. Network protocols supported are TCP/IP4 and TCP/IP6, DHCP, DNS for name resolution and NTP to support synchronization.

CBP require Kiosk hostnames to have 10 characters in the format of airport code/APC/kiosk number (example: JFKAPCK001) for each kiosk unit. It will take two weeks for CBP OIT to create internal compliant workstation names and corresponding CBP objects.

Microsoft windows security hardening is used to secure operating system, applications on kiosks and server. This involves implementation of windows policies, permissions, groups, profiles and firewall restrictions.

Firewall security is implemented at the Kiosk, network and CBP interface levels. Kiosks use software firewalls from the operating system, Cisco network firewall devices. Firewalls are implemented for interfaces, between airport location and CBP APC web service. Ports used:

| Port Number | Related Product |
|---|---|
| 6130 | Kiosk SW |
| 2967 (TCP / UDP) | Symantec |
| 80 & 8530 | Windows Update Services |
| 53 | DNS |
| 123 (UDP) | NTP |

CBP connectivity requires Kiosks to interface with secure CBP APC web services via the Internet using the following:

- 2-way SSL Public Certificates are required
- Entrust or VeriSign Certificates submitted to CBP OIT
- Certificates must be sent (encrypted) and loaded, to include testing and production environments
- Only one certificate is needed for each environment (example, one certificate for test and one for production)
- Web Services (SOAP / HTTPS & XML)

The CBP side of the interface, a DMZ Layer hosts an XML Appliance that provides the Kiosk System with a basic service access point to the APC Service. The XML appliance is configured to prevent and control unauthorized access to the server and other services not available to systems outside the CBP network. The solution is fully compliant with CBP ICD published document "3209000-ICD-Schema 2.0 v4.doc".

**Data Exchange Process**

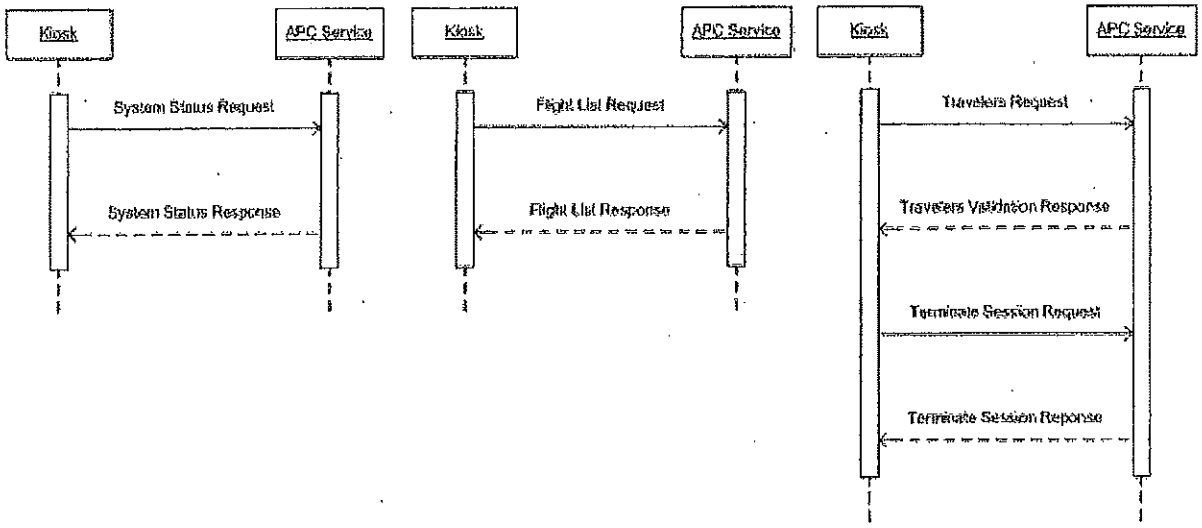
In accordance with US CBP Automated Passport Control Service Release 2.0 Interface Control Document v3 (Section 3.1).The APC Service supports four operations: System Status, Flight List, Traveler Validate and Traveler End Session. The System Status request allows the client to obtain the current state of the APC Service. Upon receiving the request, the APC Service sends a response indicating whether or not it is available for processing. The Flight List request signals the APC Service to obtain flight information from CBP's internal systems. Afterwards, the APC Service will format and send the appropriate flight manifest in the response message. The Traveler Validate request initiates vetting processing of a traveler for a border crossing. A response is sent to the client indicating the results of the traveler processing. Following a Traveler Validate request, a client sends a Traveler End call to request an end to the traveler processing. Upon receiving the request, the APC Service will process the traveler confirmation and send a response back indicating that the session for the traveler has completed.

The APC Service provides four web service operations that allow the Kiosk System to request information from the APC Service. In each of the four dialogues, the Kiosk System initiates the message request and the APC Service provides a message response. The web services operations are:

1. Flight List
2. Traveler Validate
3. Traveler End

4. System Status

System Status and Flight List are standalone requests; they are informational services that inform on system availability and provide flight information, respectively. On the other hand, Traveler Validate and Traveler End are used in sequence as part of an interactive workflow that processes a traveler.




**Data Collection**

SITA has designed the solution to comply with the CBP requirements on data exchange – which are outlined in the CBP Automated Passport Control Service - Interface Control Document. Below is an overview of the process.

The traveler places his/her Passport on the Kiosk document reader, which will scan the MRZ data. If the traveler is not a US citizen, the process is concluded. If he/she is a US citizen, he/she will be asked to perform facial image capture.

- The biographic and/or biometric data is transmitted to CBP via a web services server which interfaces with CBP's APC Service for traveler processing.
- The Kiosk interfaces with the APC Service to request traveler processing data, but is isolated from CBP's internal networks and systems.

These additional functions are performed by the Kiosk

- Request and receive the APC Service system status message
- Request and receive the latest flight list information from APC Service
- Initiate the session with the traveler(s) and the APC Service
- Prepare and send the Traveler Request(s)
- Process vetting results from the Travelers Validation Response message
- Prepare and print receipts for each traveler as specified
- Request and receive the Terminate Session messages
- Record and document session information

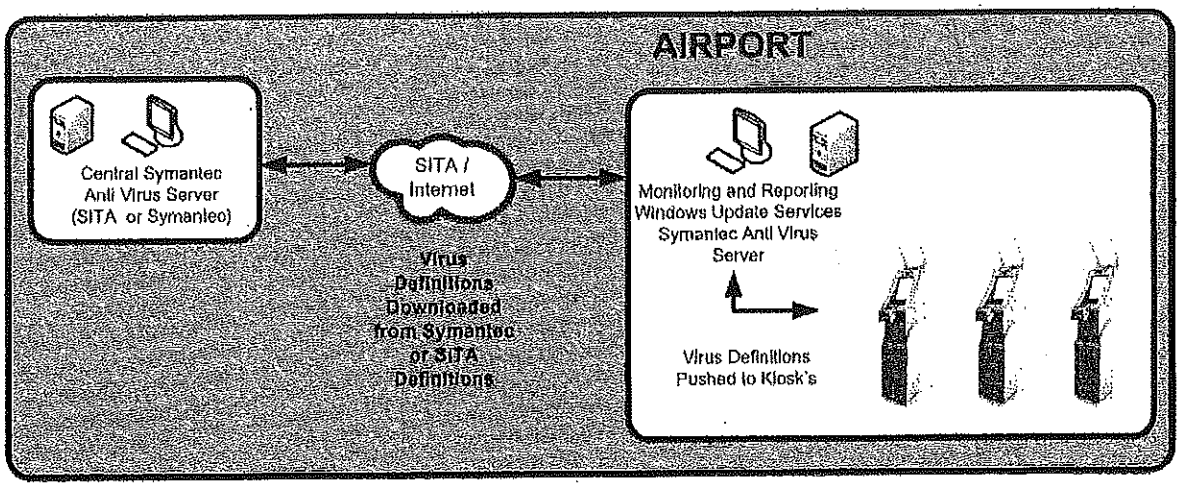
The Kiosk System shall not store any privacy sensitive data such as MRZ data, personal traveler data or referral codes. This information and the detailed security rules are applied as per the US CBP's Interface Control Document for Phase III and its associated Privacy Impact assessment document.

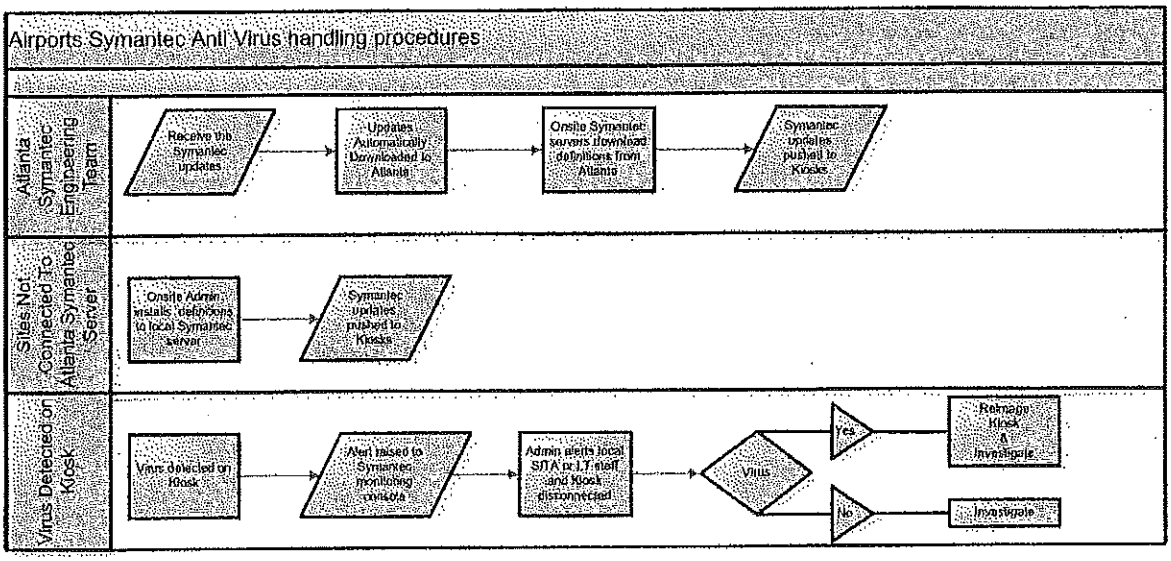
The communication between the Kiosk System and the APC Server occurs via a two-way SSL connection. Prior to establishing communication between the systems, the APC Service will need the Kiosk System's (a) publicly routable IP address and (b) public certificate (2048 bits). In addition, the Kiosk System will need the APC Service's CA certificate chain.

## ANTI-VIRUS SOFTWARE

Symantec anti-virus client software is deployed onto each Kiosk. An onsite Symantec management server downloads definitions and updates from either SITA or Symantec cloud. Local administrators approve definitions and these are distributed to each Kiosk. Definitions updates are scheduled weekly or daily.

The following workflows depict definition updates for a centrally managed solution, sites not connected and virus detection steps to be taken:






## DATA REPORTING METHODS AND METRICS

The proposed solution includes a Reporting tool, based on the collected of operational data. The value of management information gathered from the thousands of APC processes performed at a certain airport is huge. Using the i-Shield platform, accredited users can generate, view and run reports, and check the status of the reports generation. Reports provide accurate and comprehensive decision-support information, under dimensions such as citizenship, age, gender, and group size, including consolidated data for the entire system, or a breakdown per Kiosk and according to different time slices, such as weekly and daily.

- *Integration to data warehouse* – The proposed solution can be integrated with the airport data warehouse, both for data storage and for generation of reports.

- *Data dictionary/ list of what data will be available* – The APC solution can provide the Audit and Logging tool with any non-personal data considered relevant for CBP and/or the Airport Operator, such as:
  - Time stamps
  - Processing times
  - Authentication results
  - Biometric matching results
  - System incidents
  - Any other data that complies with CBP business rules.

- *In order to be in compliant with CBP rules* - the proposed solution allows no passenger personal data to be stored and/or processed by the Reporting tool. This means that the following data is excluded from the provided reports:
  - Passenger biographic data, such as name, date of birth and citizenship.
  - Travel document data, such as Document number, issuance and expiry date.

- Reason for travelling.
- Biometric data.
- Any other personal data processed by the APC system.

- *Real time reporting* – The operational reports can provide information regarding any selected period, which is configurable according to the preferences of the user. If desired, a daily report can give an overview of the APC processes performed in the previous hours. In order to have access to real time operational data, the CBP officers may use the Ambassador Monitoring Application. This web-based application that runs on any mobile device, such as a tablet, can be configured to provide information regarding the real time activity of the APC Kiosk solution, regarding processing times, throughput capacity, and other operational KPIs.

- *Included Reporting options* – The reports generated by the proposed APC solution can be configured according to the preferences of the contracting authority. In any case, only data in compliance with CBP permissions can be stored and processed. According to CBP rules, the provided reports are not allowed to display traveler's personal data. Nevertheless, the provided reports include very useful operational information, which allow the authority to have a global overview to the operations during a certain period of time (e.g. Weekly reports). Examples of these reports are in Appendix E of this proposal.

## APPROACH TO SOFTWARE MAINTENANCE

SITA provides quarterly and bi-annual releases of APC software. Releases will be made on demand to support new CBP APC business rules or process updates are mandated.

Software will be delivered via ftp download, CD / DVD or USB media and provided with full installation or upgrade installations to enable quick deployment.

### Software Maintenance

SITA will engage with providers of third-party software included in the SITA system in order to resolve faults or keep applications up-to-date.

SITA will patch or update third-party software applications when they have been tested and shown to be functional by SITA staff.

## PROVISIONS BY MDAD

As SITA has a strong partnership with MDAD, it is expected that the MDAD Airport Authority will maintain its current standards and continue to provide the following during this project:

- Placement direction, installation of data and power infrastructure,
- Storage of kiosks, and other equipment as needed for the initial delivery
- Disposal of packing debris (wooden transport crates, packing material, etc.)
- Any escorting, badges and permits required by SITA staff and contractors who will be required to enter the airport and Federal Inspection Service (FIS) in order to perform installation and support of the kiosks
- Providing airport liaison with US CBP Staff to direct and assist passengers during the operational phase of the project
- Disposal of the kiosks, if required, at any time during the contract term
- Civil works if required

## SUPPORT AND OPERATIONS

From our extensive experience partnering with MIA and MDAD, SITA will continue to provide unmatched Maintenance & Support as we understand the requirements from MIA. Based on the specifications outlined in the RFP, aggressive SLAs require additional staffing to meet the needs of MIA. SITA will provide two additional team members to meet the standards and requirements of the airport authority. Additional team members may be required as the life of the contract extends to continue to provide outstanding support through the lifecycle of MIA and SITA's partnership.

Pricing will reflect the additional on-site team members and extended remote Level 3 staff that will be available to MIA 24x7x365. These additional staff members will be provide unmatched service to MIA that will allow the requirements of the SLAs to be met without issue. Should MIA decide to revise the SLA requirement, SITA can adjust the price according to meet the SLA and needs of MIA. The support is offered and priced based on the specific SLA requirements outlined in the RFP.

SITA's approach to a Kiosk implementation is to ensure there is a robust transition from the project team to steady-state operations. Support and maintenance services following live deployment will be provided by SITA for an operations period to be agreed on by contract.

### Maintenance & Support Level Definitions

The following sections describe the support levels which SITA uses internally for the support of the APC kiosks.

#### Maintenance Level 1: (Highest priority support)

Level 1 is reserved for all faults which disable the proper operation of the complete system. SITA's response is targeted to restoring the service to operational capability, and includes but is not limited to:

a) Troubleshooting and isolation of malfunctioning equipment, including flaws caused by software malfunction or operator/user error, to full restoration;
b) Replacement and/or on-line repair of failed equipment.

The restored service must be:

- Available: equipment must be able to be used, and function, as designed.
- Reliable: equipment must work consistently; intermittent working/not working is unacceptable.

#### Level 1 Hardware Maintenance

Consisting of hardware break-fix and the provision of any physical and/or logical intervention at a customer location, hardware maintenance is concerned with restoring hardware to operational service. This entails ensuring that the IT equipment and operating system are fit for purpose in accordance with contractual requirements. Various services are provided to support customer sites:

- Providing the appropriate on-site skills to perform unit repair or unit exchange in accordance with the SITA contract and/or manufacturer's instructions. SITA will ensure that the appropriate level of training and skills are available to return equipment to full usability.
- Providing problem analysis, including identification of the source of the problem.
- Obtain a replacement unit or component parts from the stock of available maintenance spares, or directly from the manufacturer when necessary.
- Restoring hardware to a working state with its functioning Operating System by exchange, physical repair, and adjustments of equipment and components.

**Maintenance Level 2: Break/fix maintenance and lower priority support**

Level 2 is reserved for faults which leave the system operational, but reduce the operational capability of the SITA solution. (An example here would be a single failed kiosk). SITA's response would include:

a) Off-line repair or return of failed equipment to the repair center of the manufacturer;
b) Provision of scheduled updates and/or system recall of hardware as dictated by Manufacturer or SITA;
c) Hardware and firmware upgrades to all specified equipment, as required by SITA.

**Maintenance Level 3: Software Support**

Level 3 technical specialists will assist as required to troubleshoot problems. When a serious software problem is identified which is impacting the system, SITA will allocated Level 3 staff to investigate and fix the problem. Software updates will be released and installed if necessary to the problem devices (in agreement with the customer's staff, so that they are involved and aware of any changes.)

**Overview of Support**

SITA-Support gives you the power and flexibility to contract for the services that best fit your business needs. The service families that make up SITA-Support are described below:

- **National & Global Support Services** –on-site service provisioning, maintenance and support services, maintenance services, preventative maintenance and project management.
- **IT Asset Management** – these services assist in the lifecycle management and optimization of IT assets across the enterprise.
- **Infrastructure Management** – providing local/central management services and support of the server infrastructure within the scope

Our service model uses proven processes and methodologies built on ITIL (IT Infrastructure Library) best practices. Key operational objectives of SITA's service model include:

- Focusing on first time fixes

- Making use of remote diagnostics and fixes whenever possible to reduce cost and minimize downtime
- Optimizing use of IT Assets
- Software management and control
- Standardization and simplification

**Incident Management**

The customer will contact SITA's on-site local staff.

The SPOC will own and manage all incidents through to resolution. The local staff will route all incidents and allocate them to the appropriate resolver group. All Incidents will be assessed and assigned a priority based on the impact to the business and against any contracted Service Level Agreement (SLA). As part of the incident life cycle, incident management provides escalation up to the point of resolution and closure of an incident. They also identify known errors and provide workarounds where applicable. SITA's customized Support Model for MIA includes: On-site Incident Management

Due to the nature of the proposed solution (i.e. infrastructure hosted at the customer site) SITA may not have access to the systems. Diagnostic and management tools can be used to investigate and resolve actionable events and incidents in co-ordination with the customer's staff. Whenever appropriate in the solution, SITA will implement and use diagnostic and management tools. When it is not possible to resolve problems using the data provided by these tools, or if the problem is better diagnosed and resolved onsite, the Onsite Resolver Group will manage and oversee the process until completion.

**Escalation Process**

Our escalation procedures are based on industry standards and are designed to ensure that operations suffer the minimum disruption as a result of any incident. The objective of the escalation procedure is to ensure that should an incident not be able to be resolved within a pre-determined time frame, successively more senior SITA staff will be notified. Senior staff will become involved in the incident resolution to either resolve it or to determine what other action can be taken, as soon as possible.

SITA will provide an escalation contact matrix in the support agreement.

**Level 2 Support Team**

L2 support staff will be responsible for the following:

- Hardware support for any of the SITA products
- Incidents Management together with SITA's SPOC
- Technical support and assistance in the use of SITA products

- Corrective Maintenance for all SITA provided Hardware and Software
- Preventive Hardware maintenance and support of all installed equipment and make sure that it is working as expected.
- Warranty & Spares management
- Work with vendors (as appropriate) to resolve problems
- Contact other support groups as required
- Interface with other systems, networks and operating system environments
- Hardware replacement when required
- Knowledge transfer to customer staff

**Level 3 Support**

Problems which cannot be resolved by the on-site technician or L2 will be referred to the Level 3 (L3) support teams.

The L3 team provides Advanced Application Support (CoE – Center of Expertise for each product) and also manages Hardware support from local suppliers. If a problem cannot be resolved after a thorough investigation has been completed and all diagnostic procedures have been carried out, the local investigator will contact the third level (L3) support team. L3 are formed by Application Software Support and Hardware manufacturers for each product.

In addition, CoE team will work with end users and the local team to identify and resolve problems where application services are unavailable or are producing unexpected results.

The purpose of level 3 support is to provide comprehensive back-to-back support up to the level where resolution of a problem depends on the correction of source code of the application, or manufacturer hardware repair.

This level of support addresses problems at the source code level and provides an advanced level of application support to second level support staff. In addition, periodic software updates will be provided as part of the Level 3 Support service in the form of minor software version updates. These minor versions will include corrections for known defects as well as new functions or software enhancements

The level 3 problem tickets will be managed by SITA Level 2 support. They will be responsible for opening the ticket to Level 3, schedule time to maintenance/update releases, test releases, update and close problem tickets.

The Level 3 support consists of two groups that provide assistance to the local team:

- SITA Center of Expertise (CoE) performing Advanced Application Support for each Product
- Hardware Supplier support

The Standard Support Model promotes to monitor and manage the Service and required infrastructure centrally. The central teams will be granted administrative privileges to perform their duties centrally, while on-site field services will still be required to perform any hardware break-and-fix activity.

Although, it had been considered mandating centrally managed kiosks, we decided to take the optional approach and strongly recommend the central management of kiosks by outlining its value proposition, e.g.

- Centrally managed kiosks are restored faster than locally managed kiosks. Typically takes 20 minutes to restore kiosk service from the time that the alarm is noticed. Takes same amount of time to restore service locally, however, sites do not have a 24x7 team monitoring kiosks remotely and hence, it will take around 20 minutes from when a tech arrives on location (which could take more than 2 hours if the tech is not on-site).
- Central monitoring of kiosks requires less local staffing and is less expensive in most cases considering the absence of a reliable monitoring tool for local support models and the fact that local site staff does not monitor the kiosk health status on a continuous basis. In order to provide 24x7 at any airport, one would need to have 4 or 5 individuals at any point in time. Within SCC there are several teams that are currently doing central monitoring, already staffed.

**The Level 3 support is responsible for the following:**

- Problem Diagnosis: Identify the cause when application services are unavailable or are producing unexpected results. Access the system remotely and/or work with end users to perform detailed diagnostics. Determine what changes have taken place since they system was functioning as expected.
- Problem Resolution: Take action to resolve problems directly where possible, or with input and assistance from other resolver groups. Provide assistance to other resolver groups, where required, to enable problem resolution. Implement workarounds or install software patches that have been provided.
- Problem Packaging: When more specialized advanced support is required, package problems and forward to other resolver groups
- Correct Application Corruption due to Application Errors: In the event that data is corrupted due to an application or interface data translation error, support will be provided to correct or restore the data.
- Perform Advanced Diagnostics at:
  - Application code level
  - Interface protocol level
  - Database structure level
  - System configuration level
- Advanced support liaison: Liaise with advanced support groups and end users to perform advanced diagnostics and provide additional information
- Provide Codes Fixes and Workarounds: Application code fixes or software patches will be provided to correct application software defects. In some situations, a workaround solution may be provided on an interim basis, until a permanent code fix is available. Code fixes will be addressed by means of minor software revisions that will be provided with release notes.
- Evaluate Code Modification Requests: Requests to modify code or provide minor enhancements will be evaluated, and any consensual modifications will be addressed by means of minor software revisions that

will be provided with release notes. Requests for enhancements will be logged in a database and considered for inclusion in future releases.

- Assist 2nd level support personnel by performing advanced level diagnostics to determine the cause of application errors, unexpected results, and performance problems related to the application and system as a whole.
- Advanced Application Support: Assist 2nd level support personnel, if required, with guidance on the use of advanced or complex functions, such as modification of parameters or adjustments of rules.
- Advanced Configuration and Configuration Management Support: Assist 2nd level support personnel, if required, with guidance on maintaining and managing the application configuration, e.g. support with installing updates and maintaining the latest application software levels.

**Operations Reporting**

A standard report format will be agreed between MIA and SITA for each report. Reports will follow the agreed format and be distributed to a specific customer distribution list by email. The report(s) usually include:

- Operational Activities
- Technical issues
- Problems
- Action Item status
- Problem resolutions

**Service Level Management-**

SITA will work with MIA to meet and exceed the SLA requirements set forth in the RFP. Pricing has been provided based on MIA's outlined requirements, which are in line with the Priority Level definitions for the SITA products and meet the customer needs. These levels are measured according to the business impact of each problem, as follows:

| Priority Level | Impact | Description |
|---|---|---|
| Priority 1 | Business efficiency impact | System failure that interrupts non-critical business processes.<br>Failure of a system or component but alternative available at customer location.<br>Incident affects single user.<br>Work around is available. |
| Priority 2 | Business high impact | System failure that partially interrupts or degrades business critical processes and there is no alternative available.<br>An incident affects multiple users. |

| | | |
|---|---|---|
| Priority 3 | Business critical impact | System failure that completely interrupts the critical business processes, affecting all users |

In the following table, SITA proposes the response and restore times to MIA.

The "Restore Time" starts counting from the moment the ticket / call is communicated to SITA, either through direct (on-site) contact, and/or by e-mail and/or by SMS, and/or through the Service-Desk system dedicated to this solution.

"Pre-Diagnostic" means the initial study of the situation and root cause of the reported incident, as well as the possible consequences and predicted restore time.

SITA accepts the SLA requirements and understands that restore and diagnostic requirements are as follows:

| Priority | Response Time | Restore Time | Status Updates | SLA |
|---|---|---|---|---|
| 1 | 10 minutes | 2 Hours | 15 minutes | Maximum of 4 incidents can occur in a single month<br>Maximum of 20 incidents can occur in the last 12 months<br>100% of incidents must be addressed within the restore time |
| 2 | 15 Minutes | 6 hours | 2 hours | Maximum of 1 incident can occur in a single month<br>Maximum of 4 incidents can occur in the last 12 months<br>100% of incidents must be addressed within the restore time |
| 3 | 1 Hour | 48 Hours | Four Hours | Maximum of 1 incident can occur in a single month<br>Maximum of 2 incidents can occur in the last 12 months<br>100% of incidents must be addressed within the restore time |

**Monitoring Services**

SITA offer a developed MIB configuration file that is configured for alerts / alarms and can be amended to support specific requests, which is deployed onto each Kiosk. The MIB configuration can either be integrated with SITA's local or remote monitoring software. Or provided to Miami for integration into any in house monitoring tools, such as Microsoft SCOM / SCCM products and integrated as a SNMP pack.

SITA Global Services offer a local monitoring solution called KMOSS that is integrated with an offsite central network monitoring solution called NGOSS. All computing and networking resource monitoring will be performed by Next Generation Operations Support System (NGOSS). All events, defined as relevant, produced by NGOSS will be displayed in a list topology map as well as having alarms raised with a problem signature. The NGOSS console is managed and pro-actively monitored by the SITA Global Services (SGS) teams, such as the GSL

Service Desk or the SITA Command Center (SCC) team. NGOSS monitors logical, physical and network objects in the system that includes:

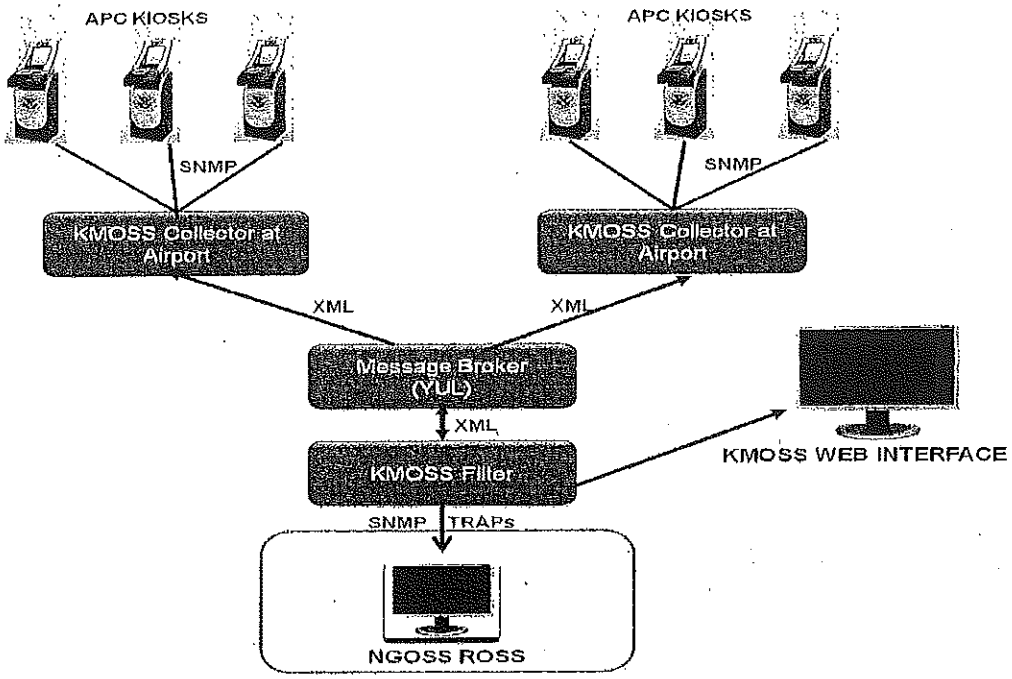
System resources:

- Monitoring hardware, Operating system and database systems.
- Monitored objects include processor, CPU, file systems, disks, processes, threads, and operations.

Network resources:

- Monitoring of switches, Firewalls, Routers, Gateways, Peripherals, IPSec, IPDSLAM,
- Access points and controllers, VPN Concentrators and connectivity boxes.

The monitored objects include Ethernet media, spanning tree, bandwidth, QOS queue, COS, E1channels, IPSec Tunnel, services, counters, packets, queues, and blocks.




## Maintenance Schedules

### Proactive Preventative Maintenance

Proactive daily & weekly maintenance tasks should be performed on the kiosks and these tasks can be carried out by trained personal onsite.

### Preventative Maintenance Support

SITA will monitor and perform preventative maintenance to prolong the operational life of the equipment. This includes:

a) Provision of standard preventive maintenance of equipment, based on SITA's recommendations and manufacturer's recommendations;

b) Adjustments and replacement of repairable items as deemed necessary by periodic inspection of equipment.

SITA will perform the following preventative and regular maintenance activities as part of their responsibilities. These activities are prescribed by the hardware vendor and subject to SLA restrictions. Details will be provided in manuals, but as a summary, please see the list below.

- Daily wiping/cleaning of all reader surfaces: passports, fingerprints, etc.
- Daily cleaning of camera lens;
- Daily cleaning of the fingerprint readers.
- Daily blowing out/vacuuming of air intake vents at bottom of units;
- Weekly dismantling of air intake filter to clean it;
- Weekly inspection of Fingerprint readers.

Customer Defined Level 2 - hardware related (reboot, printer, replacement, etc) will be handled by SITA Level 1 staff.

Customer Defined Level 3 - software issues, upgrades, CBP mandated changes will be handled by SITA with full support via the "SPOC" = SITA Level 2 and SITA Level 3.

## On-Site Inventory

### Consumables and Spares Management

SITA will provide a full Bill of Materials List once the Implementation reaches the Hand-Over stage. It will be submitted electronically and reviewed by both parties for integrity. SITA will work with MIA and/or its maintenance provider to replace defective hardware during the warranty period.

SITA will provide management of spares including provisioning, logistics, managing OEM warranties and performing/coordinating repair activities, during the whole contract period. The spare parts will be stored on site (e.g. at the Airport), and the spares management will be coordinated by the Local staff. SITA will provide the paper and consumables to support the maintenance of the kiosks.

## APPROACH TO TRAINING

**Training Course Delivery**

SITA recommends that at least five (5) days or 16 hours should be allocated for operational and transition support training. A classroom training session will be offered during the business hours of 8AM – 5:30PM local time. It is expected the training session will be up to half a business day to complete.

To facilitate training, MDAD will need to provide a training class room with projector and refreshments. The training will consist of the class room training, followed by hands on APC Kiosk and Ambassador Application training. The class room training module will be delivered using Microsoft Power point and covering the following:

- Training material hand outs (APC Overview, CBP processes, Kiosks & Ambassador App)
- APC Process
- Information Videos of processes and benefits
- System Administration
- Exception Handling
- Queue Management
- Ambassador Application overview
- Outage Reporting
- Maintenance Training
- Contingences

The APC Kiosk training module will be onsite at the APC Kiosk covering the following:

- APC Kiosk location
- APC process manual issued to each trainee that covers items from the earlier class room module
- Using the system and completing full transactions
- Reviewing referral codes and their meanings
- Training on receipt paper replacement
- Training to identify, what to look for when a Kiosk may need to be cleaned
- Ambassador application hands on session using a tablet

MDAD "**Train the Trainer**" will be one to one training for one (1) business day, consisting of the standard course and technical / operations and administration training.

## ON-SITE TRAINING AT HANDOVER

The *Standard Support Model* includes: On-site training at handover.

SITA will provide training to designated customer staff on the systems included as part of our proposal to ensure that users are able to work with the system in their specific functions. Training includes instruction on how to operate SITA products, as well as problem-reporting procedures. The instructions most commonly target trainer and end-user audiences.

Training will include both theoretical and practical hands-on experience.

Training will take place at the airport at the time of handover. Training is usually given in English. If the customer wants an alternative language then this can be arranged with SITA at extra cost. Alternatively the customer can provide a local technical translator.

### SITA Trainers

SITA trainers are all experts on the SITA systems and applications and have very strong domain knowledge in their area of expertise. In addition they will have valuable experience of supporting SITA systems and will be able to answer the customer's questions about the products being delivered.

### Train-the-Trainer Approach

SITA advocates a 'train-the-trainer' approach. There are several benefits to this approach including mentorship that builds a successful and long term operational relationship; the flexibility to customize classes based on need; and the customer's development of competency and expertise in parallel with the implementation.

Our experience shows that active involvement of key staff is crucial to gaining the full ongoing benefits from the project.

### Warranty Information

Standard warranty is provided for a one year term. However, SITA has extended this warranty to conform to the requirements outlined in the RFP. SITA warrants the supplied hardware for the term of the contract- five years.

## KEY VALUE-ADDED FEATURES

SITA's APC Kiosks provide the following features that highlight SITA's exceptional product offering:

- Automatic Face Finder with Automatic Height Adjustment of the camera and lighting in a vertical course of 70 cm (1.4 to 2.1m), to immediately ensure full-frontal poses for full compliance with ICAO

recommendations for face image capture. This technology allows the field-of-view coverage of travelers on wheelchairs, without the use of tilt/ wide-angle lens to avoid image distortion.

- Automatic lighting adjustment to cater for varying environmental lighting conditions, supported by multi-independent LED illumination system. The usage of LED illumination technology instead of flashes prevents blinding the user or causing changes in the facial expression during the capture.
- Real-time automatic adjustments of camera focus and settings (white-balance, contrast, exposure, brightness).
- Instant and real-time biometric quality analysis of face image, fingerprint, to ensure that all the generated biometric data meets ICAO standards.

## Ambassador Application

The Ambassador application is used for interactive monitoring of the solution and designed to be used by local ambassadors, management and on site I.T support staff. The second application is a centrally based monitoring capability for I.T administrators, that enables local or offsite monitoring of the solution using SNMP and MIB configuration files deployed to each Kiosk, integrated with SITA monitoring products KMOSS and NGOSS. Or a customer's in house solution that supports SNMP, The third application is APC reporting that is server based and also integrated with the ambassador application.

### Ambassador Staff Interactive Monitoring

The Ambassador application is an interactive application that runs upon a desktop or tablet and supports Windows, IOS and Android operating systems. It is installed on the local SITA APC server, which collects data feeds from all Kiosks and presents useful data via the Ambassador Client applications.

As a best practice, it is recommended that Ambassador Staff in the FIS have the ability to monitor the live status and usage of APC Kiosks, to gain optimal performance and throughput of the solution. By providing real time availability information, the application leads to a more efficient guidance of the travelers inside the FIS area, by helping reducing excessive dwell time for travelers to find an available Kiosk. To address this, SITA provide an interactive dashboard monitoring application, called the "**Ambassador App**".

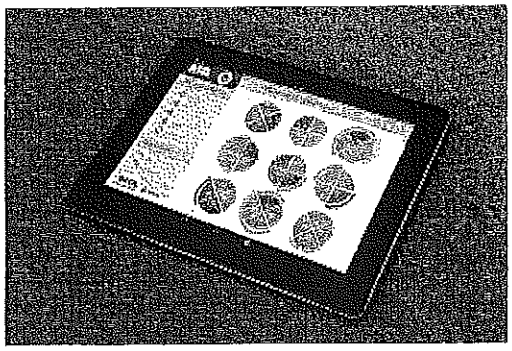
The application visually presents the active status of each Kiosk (Use Me First, Free, Busy, Out of Service, and ADA Kiosk) and paper status (low and out of paper). It delivers advanced Queue Management using a mobile tablet, via Wi-Fi, or monitoring station for Ambassadors and Support Staff to use, by providing a graphical overall representation of the operating APC Kiosks in the different terminal areas. The Ambassador Monitoring Station is a very useful tool for both Ambassadors who assist the travelers on the APC process, and for the Support Staff who are responsible for keeping the kiosk in operation.

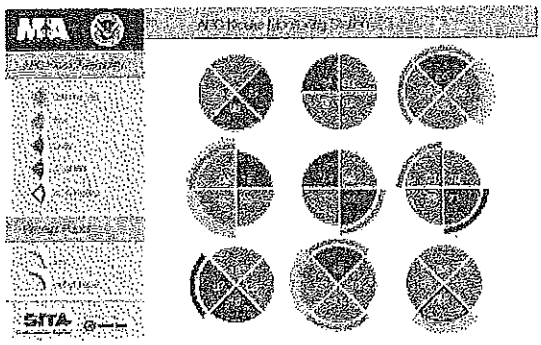
Each Kiosk is identified in the graphical interface by its unique ID, which supports the application user to clearly understand to which physical Kiosk in the FIS corresponds to each icon Kiosks icon displayed.

### Interactive Monitoring / Ambassador Application

SITA provide an interactive dashboard tablet application called the "**Ambassador App**", designed to provide real time status of kiosks directly to ambassador staff in the FIS area. The software visually presents the active status of each Kiosk (Use me First, Free, Busy and Disabled/Out of Service, and ADA location) and its paper status (low and out of paper).

**SITA offers the Kiosk Ambassador Monitoring tool, which can be used for queue management as well as other functions.**





The Ambassador Monitoring Station delivers advanced Queue Management in a mobile tablet, via Wi-Fi, for Ambassadors and Support Staff or can be accessed by management, using a Windows desktop. The software visually presents the active status of each Kiosk (Use me First, Free, Busy and Disabled/Out of Service, and ADA location) and its paper status (low and out of paper).

The local server combined with the Ambassador Monitor server application can provide logging & reporting capabilities, for management information reporting and auditing capabilities for remote performance monitoring and distribute output in real-time to the Ambassador Client

The main advantages of this Queue Management Solution are the following:

- Provides proactive real-time status of Kiosks directly to Ambassadors.
- Allows for optimal usage of Kiosks by eliminating hot spots, bottlenecks and congestion through excessive dwell time to find available Kiosks. It enables even distribution of kiosk usage in FIS.
- Proactive monitoring of Kiosks for paper replenishment to avoid excessive down time.

Optimize support to traveler using Proactive Management of operations.

## APPROACH TO SOFTWARE ESCROW

SITA will place the source code of each delivered release; including maintenance with a third party United States based company, "**Iron Mountain**" on CD / DVD or USB media. The media will be stored at an "**Iron Mountain**" storage facility located in the United States. SITA's APC Kiosk Wi-Fi Compatibility

Wi-Fi connectivity is supported for accessing the Ambassador application, via Wireless access points. Wi-Fi access between Kiosks and wireless access points will be available in a future Kiosk model.

## ADA SECTION 508 COMPLIANCE

### ADA section 508 Compliance

Below are pictures which illustrate the ADA features as described in Section 7.4?

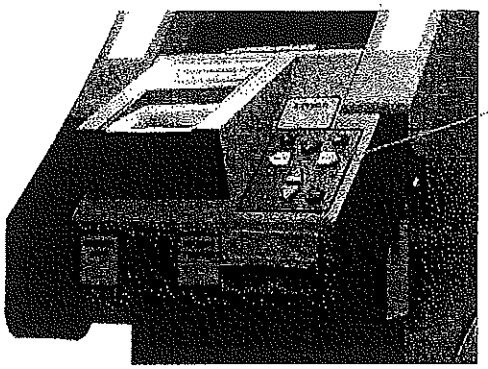
Font Type and Size: The user interface employs colors/contrast and fonts rigorously selected according to ADA defined standards, so that the readability is as high as possible for the visually impaired and color blind. Furthermore, the touch screen user display complies with the ADA requirements regarding the color and contrast settings, refresh rate, as well as usability (such as operability with one hand, a gloved hand or prosthetic, and required force below 5 lbs).

Audio Interface: The APC Kiosk includes an audio headset plug, which allows the traveler to listen to a text-to-speech version of the displayed messages. The audio messages can be interrupted, paused and restarted at any time. Plugging in a headset will trigger a call to the ADA page, which will allow the user to adjust the volume and request privacy (in which case a privacy screen will layered over the user interface to stop someone shoulder surfing the blind person without them knowing it). The sound level is automatically reset after every use, and a volume gain of at least 20 dB above the ambient level is selectable.

Stickers: The ADA version of the APC Kiosk includes stickers which present not only the standard text, but also the Braille version of the messages. These stickers are placed on every part of the Kiosk which would require an action from the traveler, such as the document reader and the receipt printer

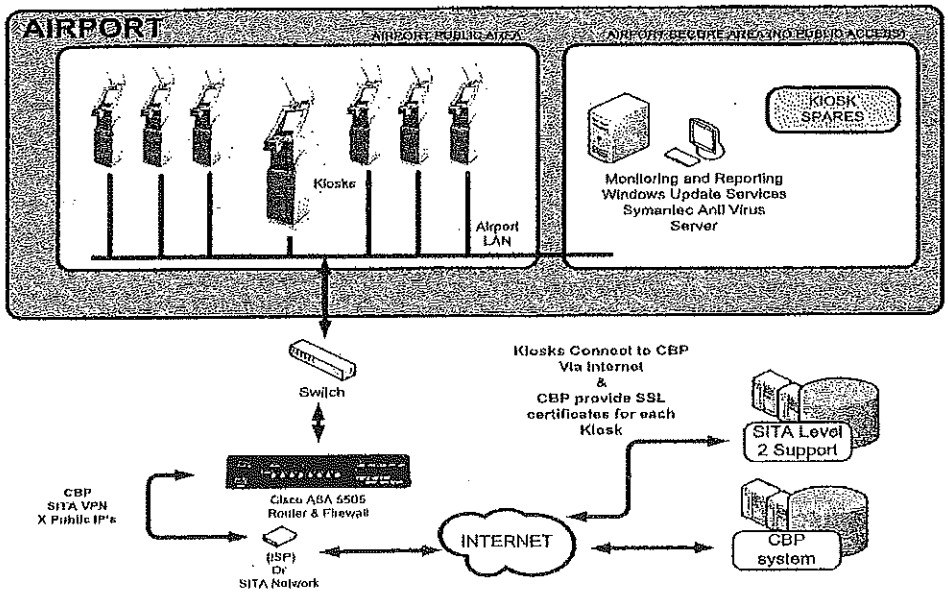
The motion protection bar prevents wheelchair users from accidentally hitting the Kiosk.

**Automatic Height Adjustment:** used to adapt the height of the man-machine interaction components, improving the usability for both able bodied as well as those with disability or accessibility issues.

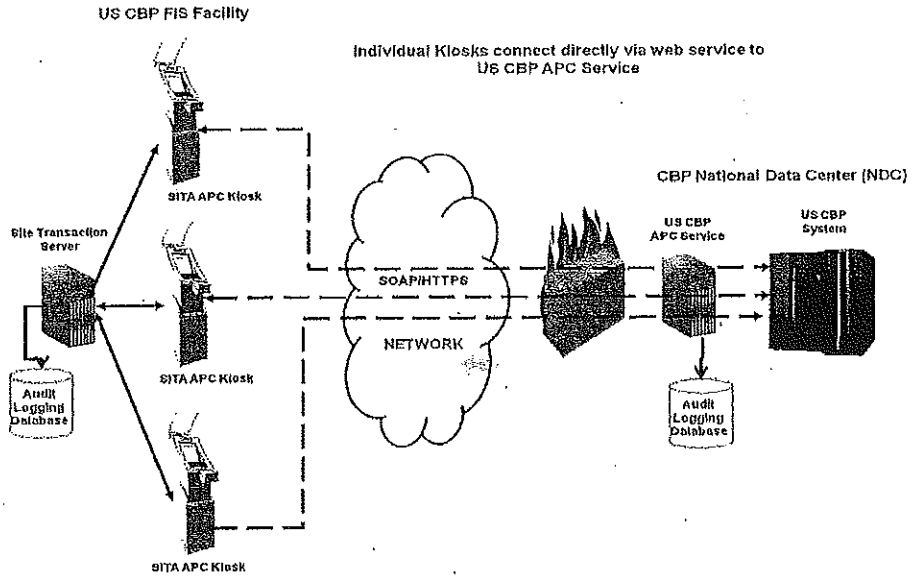


**EZ Access:** The APC Kiosk integrates an EZ Access Keypad, which allows the user to manage the entire APC workflow, with the 8 buttons of different colors and formats, while driving the audio interaction, without requiring the use of the touch screen.

## ATTACHMENT 1: INFRASTRUCTURE AND NETWORK DIAGRAMS




SITA APC Kiosk High Level Technical Architecture
(Network Redundancy)



## ATTACHMENT 2: LIST OF SPARE PARTS

- iBiometrics Camera
- 4/4/2 Fingerprint Module
- Frame with embedded touch screen
- Proaction Module + MILSIS system
- eReader Document Reader
- Receipt Printer
- Frontal cover module for Receipt Printer
- Processing unit
- USB Industrial hub
- Power supply 110AC-24DC
- Power supply 110/240AC-12DC
- PC Power supply

Due to the modularity of the APC Kiosk, the components listed above can be upgraded.

# APPENDIX B: PAYMENT SCHEDULE

## A. APC KIOSK PAYMENT SCHEDULE FOR INITIAL FIVE YEAR TERM:

| Deliverable | Description | Price per Kiosk | Total Amount Due |
|---|---|---|---|
| 1 | Phase I : 36 Kiosks | $34,111.06 | $1,227,997.99 * |
| 2 | Phase II : 36 Kiosks | $34,111.06 | $1,227,997.99 * |
| 3 | Phase III : 36 Kiosks | $34,111.06 | $1,227,997.99 * |
| 4 | Phase IV : 36 Kiosks | $34,111.06 | $1,227,997.99 * |
| | | Subtotal for APC Kiosk Devices: | $4,911,991.96 |

**Total Amount Due for each phase shall be paid upon Final Acceptance of the APC Kiosks by the County Project Manager.*

| Price Breakdown / Ancillary Costs | |
|---|---|
| **Description** | **Total Price** |
| Software License Fee – Unlimited Kiosks / Users | $ 1.00 |
| Equipment / Devices ($32,000 per Kiosk Device) | $ 4,608,000 |
| Testing, Configuration, and Implementation Services Phase 1 - $63,800 / Phase II - $63,800 / Phase III - $63,800 / Phase IV - $63,800 | $ 255,200 |
| Training Services ($1,000 Per Phase for Required 1.5 days of Training) | $ 4,000 |
| Miscellaneous Costs Phase 1 - $12,199 / Phase II - $12,198 / Phase III - $12,198 / Phase IV - $12,198 | $ 48,792 |
| Software Escrow Year 1 – $8,050 / Year 2 – $800 / Year 3 – $800 / Year 4 – $800 / Year 5 - $800 | $ 11,250 |
| **Subtotal for Initial Five Year Term** | **$ 4,927,243** |
| **Extended Warranty / Hardware / Equipment and Consumables (Contract Year 1)** | $ 64,804 |
| Phase I | $ 64,804 |
| Phase II | $ 0 |
| Phase III | $ 0 |
| Phase IV | $ 0 |
| **Extended Warranty / Hardware / Equipment and Consumables (Contract Year 2)** | $ 241,088 |
| Phase I | $ 173,044 |
| Phase II | $ 68,044 |
| Phase III | $ 0 |
| Phase IV | $ 0 |
| **Extended Warranty / Hardware / Equipment and Consumables (Contract Year 3)** | $ 352,894 |
| Phase I | $ 176,447 |
| Phase II | $ 176,447 |

| | | |
|---|---|---|
| Phase III | $ 0 | |
| Phase IV | $ 0 | |
| **Extended Warranty / Hardware / Equipment and Consumables (Contract Year 4)** | | $ 435,057 |
| Phase I | $ 180,019 | |
| Phase II | $ 180,019 | |
| Phase III | $ 75,019 | |
| Phase IV | $ 0 | |
| **Extended Warranty / Hardware / Equipment and Consumables (Contract Year 5)** | | $ 630,080 |
| Phase I | $ 183,770 | |
| Phase II | $ 183,770 | |
| Phase III | $ 183,770 | |
| Phase IV | $ 78,770 | |
| **Subtotal for Extended Warranty / Hardware / Equipment and Consumables – (Initial Five Year Term)** | | **$ 1,723,923** |
| **Maintenance and Technical Support Services –Contract Year 1** | | $ 220,342 |
| Phase I | $ 220,342 | |
| Phase II | $ 0 | |
| Phase III | $ 0 | |
| Phase IV | $ 0 | |
| **Maintenance and Technical Support Services –Contract Year 2** | | $ 429,971 |
| Phase I | $ 224,749 | |
| Phase II | $ 205,222 | |
| Phase III | $ 0 | |
| Phase IV | $ 0 | |
| **Maintenance and Technical Support Services – Contract Year 3** | | $ 438,570 |
| Phase I | $ 229,244 | |
| Phase II | $ 209,326 | |
| Phase III | $ 0 | |
| Phase IV | $ 0 | |
| **Maintenance and Technical Support Services – Contract Year 4** | | $ 555,364 |
| Phase I | $ 233,829 | |
| Phase II | $ 213,513 | |
| Phase III | $ 108,022 | |
| Phase IV | $ 0 | |

| | | |
|---|---|---|
| Maintenance and Technical Support Services – Contract Year 5 | | $ 674,492 |
| Phase I | $ 238,505 | |
| Phase II | $ 217,783 | |
| Phase III | $ 110,182 | |
| Phase IV | $ 108,022 | |
| Subtotal for Maintenance & Support Total (Initial Five Year Term) | | $ 2,318,739 |
| Subtotal for Initial Five Year Term – Equipment and Services: | | $ 4,927,243 |
| Subtotal for Extended Warranty and Consumables (Initial Five Year Term): | | $ 1,723,923 |
| Subtotal for Maintenance & Technical Support Services (Initial Five Year Term) | | $ 2,318,739 |
| FINAL COST FOR INITIAL FIVE YEAR TERM | | $ 8,969,905 |

## B. OPTIONAL YEARS TO RENEW

1. Extended Warranty for Hardware / Equipment / Devices and Consumables

| Description | | Total Amount Due |
|---|---|---|
| Extended Warranty / Hardware / Equipment and Consumables (Contract Year 6) | | $ 750,836 |
| Phase I | $ 187,709 | |
| Phase II | $ 187,709 | |
| Phase III | $ 187,709 | |
| Phase IV | $ 187,709 | |
| Extended Warranty / Hardware / Equipment and Consumables (Contract Year 7) | | $ 767,376 |
| Phase I | $ 191,844 | |
| Phase II | $ 191,844 | |
| Phase III | $ 191,844 | |
| Phase IV | $ 191,844 | |
| Extended Warranty / Hardware / Equipment and Consumables (Contract Year 8) | | $ 784,744 |
| Phase I | $ 196,186 | |
| Phase II | $ 196,186 | |
| Phase III | $ 196,186 | |

| | | |
|---|---|---|
| Phase IV | $ 196,186 | |
| Extended Warranty / Hardware / Equipment and Consumables (Contract Year 9) | | $ 802,980 |
| Phase I | $ 200,745 | |
| Phase II | $ 200,745 | |
| Phase III | $ 200,745 | |
| Phase IV | $ 200,745 | |
| Extended Warranty / Hardware / Equipment and Consumables (Contract Year 10) | | $ 822,128 |
| Phase I | $ 205,532 | |
| Phase II | $ 205,532 | |
| Phase III | $ 205,532 | |
| Phase IV | $ 205,532 | |
| Extended Warranty / Hardware / Equipment and Consumables Total for OTR Years 6-10 | | $ 3,928,064 |

2. Maintenance and Technical Support Service Fees

| Description | | Total Amount Due |
|---|---|---|
| Maintenance and Technical Support Services Fees – Contract Year 6 | | $ 687,980 |
| Phase I | $ 171,995 | |
| Phase II | $ 171,995 | |
| Phase III | $ 171,995 | |
| Phase IV | $ 171,995 | |
| Maintenance and Technical Support Services Fees – Contract Year 7 | | $ 701,740 |
| Phase I | $ 175,435 | |
| Phase II | $ 175,435 | |
| Phase III | $ 175,435 | |
| Phase IV | $ 175,435 | |
| Maintenance and Technical Support Services Fees – Contract Year 8 | | $ 715,776 |
| Phase I | $ 178,944 | |
| Phase II | $ 178,944 | |
| Phase III | $ 178,944 | |

| | | |
|---|---|---|
| Phase IV | $ 178,944 | |
| **Maintenance and Technical Support Services Fees – Contract Year 9** | | $ 730,092 |
| Phase I | $ 182,523 | |
| Phase II | $ 182,523 | |
| Phase III | $ 182,523 | |
| Phase IV | $ 182,523 | |
| **Maintenance and Technical Support Services Fees – Contract Year 10** | | $ 744,692 |
| Phase I | $ 186,173 | |
| Phase II | $ 186,173 | |
| Phase III | $ 186,173 | |
| Phase IV | $ 186,173 | |
| **Maintenance & Technical Support Services Total (OTR Years 6-10):** | | **$ 3,580,280** |

3. Software Escrow Fees

| Software Escrow Fees | Annual Fees |
|---|---|
| Software Escrow Agreement Fees (Year 6) | $ 800 |
| Software Escrow Agreement Fees (Year 7) | $ 800 |
| Software Escrow Agreement Fees (Year 8) | $ 800 |
| Software Escrow Agreement Fees (Year 9) | $ 800 |
| Software Escrow Agreement Fees (Year 10) | $ 800 |
| **Software Escrow Fees OTR Years 6-10:** | **$ 4,000** |

4. *OPTIONAL ITEMS: Professional Service Fee Schedule:*

During the term of the resultant contract, should the County wish to employ the Contractor for projects or services outside the scope of the services, all work performed will be billed on a time and materials basis as defined in the below rate schedule:

| Service | Proposed Hourly Rate |
|---|---|
| Project Manager | $ 250 |
| Programmer | $ 200 |
| Trainer | $ 150 |
| On-Site Training (Per Day) | $ 1,000 |

## APPENDIX C - PROJECT TIMELINE

SITA understands the requirement to have each phase of 36 kiosks delivered and operational with 30 days of notice to proceed. As part of the start up for each phase SITA will provide a detail project schedule that will be aligned with the general implementation plan provided below.

| Task / Milestone | Week Due | Deliverable / Criteria | Responsible |
|---|---|---|---|
| Contract Award | Week 1 | Signed contract | SITA and MDAD |
| SITA and Customer assign project manager | Week 1 | Project Managers assigned to the project by both SITA and the customer. Names and contact details shared with both project manager | SITA PM<br>MDAD |
| Project Governance agreed | Week 1 | Main project stakeholders agree project R&R, Communications, Risk Management, Project Change Management and baseline schedule | SITA PM<br>MDAD |
| Project Schedule | Week 1 | Project Schedule provided based on current project understanding, including the delivery plan | SITA PM |
| Network Design | Week 2 | Network design and IP's confirmed | SITA Implementation Engineer<br>MDAD |
| Kiosks Ship | Week 2 | Kiosks air shipped to site | SITA PM |
| Build out Kiosk area (civil works) | Week 3 | Provide power and network connectivity/cabling to kiosk deployment | MDAD |
| Kiosks on site | Week 3 | Kiosks cleared through customs and delivered to site | SITA PM |
| Kiosks assembly, installation and prelim network test | Week 3 | Final assembly, install and test kiosks in deployment area | SITA Implementation Engineer<br>MDAD |
| Device Naming | Week 3 | Establish OIT compliant workstation names | CBP<br>SITA PM |
| Testing Plan Reviewed | | SITA Test Plan | SITA PM<br>MDAD and CBP |
| Integration testing | Week 3 | Integration testing with existing SITA APC infrastructure | SITA Implementation Engineer<br>MDAD and CBP |

| Task / Milestone | Week Due | Deliverable / Criteria | Responsible |
|---|---|---|---|
| Production Verification | Week 3 | Verification Testing | SITA Implementation Engineer<br>CBP and MDAD |
| SITA Support Training | Week 4 | Training to SITA local on-site personnel | SITA PM |
| Airport Authority and CBP training | Week 4 | Training to Airport Authority and CBP officer | SITA PM, SITA Implementation Engineer<br>MDAD and CBP (CBP if required) |
| Operational Support | Week 4 | SITA project team transitions to operations team | SITA PM<br>MDAD |
| Customer Initial Acceptance | Week 4 | Customer Acceptance of the APC Kiosks | SITA PM<br>MDAD |
| Post Installation Support | Week 4 | 48 hour Post Implementation Support | SITA Implementation Engineer |
| 30 Day Support Period | Week 4 to Week 8 | 30 Day Support Period | SITA Operations Team |
| Project Completed/ Close out | Following Customer Acceptance | Final Customer Acceptance<br>Official close-out of the project | SITA PM<br>MDAD |

## APPENDIX D – ACCEPTANCE CRITERIA

### Deliverable Acceptance Procedures

The parties intend for the APC Kiosks to be brought into Production Mode, in phases, as each phase of the APC Kiosks are deployed as set forth in Appendix A "Scope of Services" and Appendix C "Project Timeline". Each phase of the APC Kiosks implementation will be subjected to its own testing and Final Acceptance will be deemed to have occurred upon the APC Kiosks (i) satisfying the Final Acceptance Criteria and (ii) module being used in Production Mode.

Contractor will notify County in writing (via email) when the APC Kiosks are ready for acceptance testing. County will commence testing on such APC Kiosks within three (3) County Work Days of being notified by Contractor, provided County has been given access to such APC Kiosks. County will have up to five (5) days, in its own discretion, to conduct its first round of acceptance tests and will use reasonable measures to determine whether the APC Kiosks are in conformance with the Final Acceptance Criteria, and will notify Contractor in writing as to any deficiency, in list form (to be incorporated by mutual agreement into a punch list during the System acceptance periods described in Appendix C "Project Timeline"). Contractor will promptly commence work on resolving such punch list issues and will, as necessary, redeliver such APC Kiosks for further testing, which County will commence within two (2) days of receiving Contractor's notice that the APC Kiosks are ready for such further testing. The parties shall agree, upon such redelivery, as to the time County requires to complete the additional acceptance testing. The process will be repeated until either the APC Kiosks have substantially conformed to the Final Acceptance Criteria and the APC Kiosks are put into Production Mode.

The above process will be repeated for each phase of APC Kiosks delivered under this Agreement.

Final Acceptance of the APC Kiosks will be deemed to have occurred on the APC Kiosks systems meeting the Final Acceptance Criteria APC Kiosk checklist defined below Such Final Acceptance shall be evidenced by (i) a written acknowledgement by the County Project Manager (which acknowledgement shall not be arbitrarily or unreasonably withheld) that the APC Kiosk Systems meets all such functional and technical requirements or (ii) County's use of the System in a Production Mode. "Production Mode" means any use by the County of the System or any of its modules to process any day-to-day business activity on behalf of the County.

The APC Kiosks to be deployed under this Agreement shall conform to the following check-list for System acceptance:

## APC Kiosk Check List

*This check list assumes that kiosks are being installed on an existing certified APC Kiosk base and that there is an existing gateway to CBP (open firewall, active and routable IP) from the hosting site. If this is not the case additional certification steps with CBP may be required*

**Pre-Deployment** – prior to deploying new APC Kiosks, review infrastructure and CBP connectivity to ensure it is adequate to support the new installation

### Device Readiness

1. Verify power in all modules of APC Kiosk
2. Update the kiosk Operating System with the following
    a. Computer name
    b. Enable RDP
    c. Verify **documnetcheck.xml** has "UV Brightness" set (See path above)
    d. Verify time zone and time
    e. IP address
3. Run the update file to update the system
4. Edit d:\program files\Vision Box\Server\workflow\sita\KioskSitsConfiguration.XML to change Kiosk name and skin to JBU.
5. Copy all .KEY files to a shared Thumb Drive for handover to operations (Thumb drive, Keys dir)
6. Import Auto Reboot and Auto Start-up routines into Task Scheduler (Thumb Drive, Start up Batch dir)
    a. Update User list
    b. Copy associated batch files to server directory
    c. Enable the airline schedules
7. Turn off mouse pointer (ELO settings)
8. Recalibrate ELO
9. Calibrate Passport Reader

### Device Checks

10. Insert passport in passport reader and verify it reads correctly
11. Verify elevator, illumination and camera function by taking picture
12. Take fingerprints to validate fingerprint reader
13. Verify printer by printing receipt

### CPB On-boarding

1. Verify device connectivity via airport infrastructure to CBP System
1. Update Device names
    a. Names should 10 characters in the format of airport code/APC/kiosk number (example: MIAAPCK001)
    b. Establish internal CBP compliant workstation names and corresponding CBP objects
2. Download flight list from CBP
3. Production Verification (testing)

### Go Live Check List

1. Verify check list is complete
2. Verify flight list is down loaded and device has been verified for production

3. Receive customer acceptance
4. Transition devices to operational support
5. Transition devices to production

## DELIVERABLE ACCEPTANCE FORM
## USER ACCEPTANCE TEST

PROJECT: AUTOMATED PASSPORT CONTROL (APC) KIOSKS

In compliance with the requirements detailed in the above contract (including any modifications or amendments), the following project deliverable has been delivered, reviewed and formally accepted by the County and the Contractor. This document constitutes full acknowledgment by the County of acceptance and delivery of the deliverable detailed below.

It is understood that any future changes to this deliverable after this acceptance is given will require a formal Change Request Form be submitted.

DELIVERABLE NAME: USER ACCEPTANCE TEST (UAT)

**Deliverable Description:** During the User Acceptance Test period, the Contractor and the County collectively will check, verify, and adjust the APC Kiosk Systems as needed to meet the technical specifications listed in RFP No. RFP-00118, the Scope of Services, and the current CBP technical requirements. During the User Acceptance Test period, the Contractor is required to:

- Verify compliance with tasks outlined within APC Kiosk Checklist
- Verify and update the test scenarios
- Ensure configurations are working properly
- Train County personnel on the operation of the Kiosks and associated components
- Conduct final functionality control tests, additions/modifications, and software integration
- Verify the normal operation of the Kiosks and ensure compatibility of peripheral and software applications
- Resolve user problems and/or deficiencies identified by the County
- Correct and manage errors
- Update the Kiosk documentation

**Deliverable Date:** _____

**Accepted Unconditionally:** Yes / No

**Accepted Conditionally:** Yes / No

**Acceptance Conditions:** _____

**Not Accepted:** _____

**Reason:** _____

**General Comments:** _____

_____

**Delivered By:** _____

Signature Name Date

**Accepted By:** _____

Signature Name Date

## FINAL SYSTEM ACCEPTANCE FORM

**PROJECT: AUTOMATED PASSPORT CONTROL (APC) KIOSKS**

In compliance with the requirements detailed in the above contract (including any modifications or amendments), the following project deliverable has been delivered, reviewed and formally accepted by the County and the Contractor. This document constitutes full acknowledgment by the County of acceptance and delivery of the APC Kiosk System. The System must successfully pass a 30 Day Reliability Period that starts on the system "Go Live" date prior to MDAD granting Final System Acceptance and the commencement of the one year warranty.

It is understood that any future changes to this deliverable after this acceptance is given will require a formal Change Request Form be submitted.

The Warranty Period on this deliverable starts on: _____and is valid for a twelve month period.

**DELIVERABLE NAME: FINAL SYSTEM ACCEPTANCE**

**Deliverable Description:** The delivered APC Kiosk System meets the business requirements of the County. The Contractor has successfully completed the required APC Kiosk System setup and Integration and has satisfied the criteria as specified in Appendix A "Scope of Services" within the Agreement and RFP No. RFP-00118.

**Deliverable Date:** _____

**Accepted Unconditionally:** Yes / No

**Accepted Conditionally:** Yes / No

**Passed 30 Day Reliability Period:** Yes / No

**Acceptance Conditions:** _____

_____

**Not Accepted:** _____

**Reason:** _____

**General Comments:** _____

_____

_____

**Delivered By:** _____

**Signature** **Name** **Date**

**Accepted By:** _____

**Signature** **Name** **Date**

## Appendix E – Change Order Process

At such time MDAD personnel submits a change order request, SITA will submit a Scope of Work (SOW) and provide a price quote (unless the changes have a zero pricing affect). Both MDAD and CBP must approve both the SOW and quote (if applicable) for all change orders before work will begin. However, the final decision on software changes will be provided by the CBP Office of Information and Technology. Until such time as a requested change order receives the appropriate approvals, SITA will continue to perform the project as originally agreed.

Any agreement to a requested or recommended change shall become valid once it has received appropriate approvals and mutually agreed upon.

| Change Request Form<br>Number: _____ |
|---|
| **SECTION A**<br>**Contract Details** |
| Contract Name: |
| Parties: |
| Reference no: |
| Effective date (if known): |
| **SECTION B**<br>**Details of proposed Change** |
| **Title of the proposed Change:** |
| **Service(s) to which the proposed Change relates:** |
| **Description of the proposed Change:** [*Describe the proposed Change in detail with an explanation of its importance*] [*Attach supporting information if appropriate*] |
| **Clause(s) and/or schedule(s) of the Contract which will be modified (if any):** [*if necessary, provide wording of any new / amended provisions*] |
| **SECTION C**<br>**Impact of proposed Change Request**<br>**(for information, impact assessment and resource planning only)** |
| ☐ Cost<br>☐ Delivery date / timetable / other date<br>☐ Functionality<br>☐ Performance<br>☐ Resources<br>☐ Other system<br><br>☐ Documentation<br>☐ Training needs<br>☐ Third Party<br>☐ Other (please specify)<br>_____ |
| **Description of Impact(s):** [*provide a detailed description of the selected Impact(s)*] |
| **SECTION D - Cost** |
| **Cost implications of the proposed Change:** [*Include details of whether the current cost (if any) is reduced or increased*] |
| **SECTION E - Approval of proposed Change** |
| SITA and Customer confirm that they have each read the information contained in this Change Request Form, approve the proposed Change Request as set out above, and agree that the Contract shall be treated as having been amended accordingly.<br><br>**For and on behalf of SITA**<br><br>**Signed:**<br>(Authorised Signatory)<br>**Name:**<br>**Title:**<br>**Date:**<br><br>**For and on behalf of Customer:**<br><br>**Signed:**<br>(Authorised Signatory)<br>**Name:**<br>**Title:**<br>**Date:** |

## APPENDIX F
## Software Escrow Agreement

# APPENDIX F

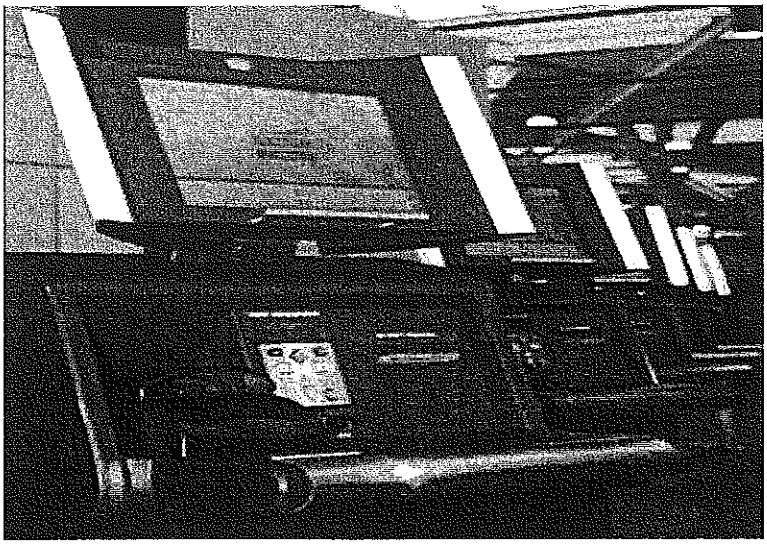
## U.S. CUSTOMS AND BORDER PROTECTION "*AUTOMATED PASSPORT CONTROL: BUSINESS REQUIREMENTS*" VERSION 16, August 2014

U. S. Customs and Border Protection

# Automated Passport Control: Business Requirements

Version 16

August 4, 2014



# Change Control Log

| Revised by | Date | Description of Revisions |
|---|---|---|
| J. Best | 09/13/2012 | Addition of photo on receipt |
| J. Best | 09/25/2012 | Addition of biometric requirements |
| J. Best | 12/21/2012 | Addition of biometric specifications/information |
| J. Best | 12/27/2012 | Modification of Declaration Questions |
| M. Nuriddin | 03/8/2013 | Rewording of requirement for clarification (23) |
| J. Best | 03/25/2013 | Addition of technical limitations on admission for non-immigrants based on passport validity. |
| J. Best | 06/28/2013 | Updated Requirements |
| J. Best | 07/24/2013 | Removal of ADA requirements |
| J. Best | 11/20/2013 | Update all Requirements |
| D. Sanchez | 04/04/2014 | Inclusion of VWP under the age of 14 and over the age of 79 to use the kiosks. |
| D. Sanchez | 04/04/2014 | Addition of standard language package requirement. |
| S. Ha | 8/04/2014 | Addition of new referral and failed conformation handling |

## Table of Contents

1. Introduction ..... 4
1.1 Background ..... 4
1.2 Purpose ..... 4
2. Definitions ..... 5
3. Business Requirements ..... 5
4. Appendix A ..... 13
5. Appendix B ..... 14
6. Appendix C ..... 15

# 1. Introduction

## *1.1 Background*

U. S. Customs and Border Protection (CBP) is one of the Department of Homeland Security's largest components. CBP is responsible for protecting the United States' front line, while facilitating legitimate trade and travel. CBP is continuously working to improve the entry process for travelers and realize the goal of increased security while expediting the flow of legitimate travel. CBP is undergoing modernization efforts to streamline the inspection process, increase officer efficiency and reduce operating costs in order to provide better services and a more welcoming environment for all travelers entering the United States. Modernization efforts include the search for technology or other methods that can assist, facilitate and/or expedite the entry process.

Over 30 countries across the world have incorporated automation into the border clearance process. CBP has developed a data entry interface service, known as Automated Passport Control (APC), to facilitate the inspection process. The data entry service allows for interested airport authorities or terminal operators to provide APC data entry points (DEPs) in a Federal Inspection Services (FIS) area. The DEPs allow eligible travelers to transmit their travel information to CBP prior to speaking with a CBP Officer. The CBP Officer is then able to focus on identity verification, admissibility and questioning to determine purpose and intent of travel. This process will ultimately reduce the traveler's time spent with the CBP Officer, increase throughput, reduce processing times and enhance the overall traveler experience.

The intent of APC is to collect traveler information and transfer that information to CBP for law enforcement purposes. APC has been included in the Airport Technical Design Standard (ATDS), allowing airport authorities or terminal operators the option of utilizing kiosks or other technology to facilitate date entry. An airport authority or terminal operator can opt to implement APC in their respective FIS. The data entry equipment is provided by, maintained and owned by the airport authority or terminal operator. In order to initiate the APC implementation process, interested parties must coordinate with local CBP representatives. Local CBP representatives will submit a field facility request through proper channels and a Program Manager will be assigned to the project. All APC hardware, software and related communication must comply with CBP APC business and technology requirements. A technical requirements document is available upon request from CBP.

## *1.2 Purpose*

The purpose of this document is to identify, at a high level, the business requirements for APC DEPs. Airport Authorities or terminal operators can opt to include kiosks or other technology as DEPs in an FIS as long as the components of the program (hardware, software, signage and/or other related material) meet the CBP business requirements and are agreed upon by the CBP Office of Field Operations.

## 2. Definitions

**APC:** Automated Passport Control

**APC Services:** Interface requirements between CBP and Airport Authorities to include a process flow description, process flow diagram, service processing concept, inputs and outputs, data elements, and reporting elements.

**Data Entry Point (DEP):** physical equipment used to facilitate Automated Passport Control Services including, but not limited to kiosks.

**Family Unit:** Members of a family residing in one household. This includes all persons, regardless of age who: 1. Are related by blood, marriage or adoption, 2. Lived together in one household at their last permanent residence, and 3. Intend to live together in one household after their arrival in the United States.

**Kiosk User or User Group:** the population eligible to use self service kiosks.

**Family Unit:** members of a family residing in one household and traveling together on the same flight.

**FIS:** Federal Inspection Services

## 3. Business Requirements

This section describes the business requirements for APC. Each business requirement has been prioritized as Critical, Important, or Optional. The disposition for each business requirement indicates the current status which is shown as "In process", "Deferred" or "In Production". The term 'system' in Section 3 refers to any physical equipment and/or any interface associated to the APC process.

| Req# | Requirement | Priority | Disposition | Comments |
|---|---|---|---|---|
| 1 | Business entities seeking to implement APC must coordinate with CBP at the local level and Headquarters. | Critical | | Local CBP must submit a project plan (FRR) to Mission Support, Facilities Division. |
| 2 | The system shall comply with CBP's Interface Control Document (ICD). | Critical | | Technical Agreement unique to each airport or location using APC |
| 3 | The system shall have the capability to communicate secure messages to CBP and receive messages from CBP. | Critical | | Messages and security outlined in ICD. |

| Req# | Requirement | Priority | Disposition | Comments |
|---|---|---|---|---|
| 4 | The system shall allow APC Services to review and/or audit any code, encryptions, network connections and any other related technical specifications. | Critical | | |
| 5 | The system shall be compliant with applicable privacy laws, regulations, agreements and policies. | Critical | | |
| 6 | The system shall be accessible to an individual or family unit in the following languages:<br>• English<br>• French<br>• Spanish<br>• Italian<br>• Japanese<br>• Portuguese<br>• Korean<br>• German<br>• Chinese | | | Standardized language package for all kiosks. Airports can add additional languages to accommodate traveler populations specific to them. |
| 7 | The system shall display a welcome banner. | Important | | Branding subject to CBP approval |
| 8 | The system shall display a notice informing the user that all information collected will be forwarded to CBP for law enforcement purposes and the user may be subject to random or further inspections. | Critical | | Language located in Appendix C. |
| 9 | The system shall display a Paperwork Reduction Act (PRA) notice. | Critical | | Language located in Appendix C. |
| 10 | The system shall be accessible to an individual traveler or family unit. | Critical | | See Family Unit definition in Section 2 of the BRD. |
| 11 | The system shall include a touch screen monitor. | Critical | | |

| Req# | Requirement | Priority | Disposition | Comments |
|---|---|---|---|---|
| 12 | The system shall require each individual traveler or member of a family unit to swipe, scan or insert a passport to collect passport information. | Critical | | |
| 13 | The system shall collect all of the following information for each traveler:<br>• First Name<br>• Last Name<br>• Date of Birth<br>• Citizenship<br>• Passport Number<br>• Passport Country of Issuance<br>• Passport Expiration Date | Critical | | |
| 14 | The system shall allow additional travelers in the family unit to be added once head of household or responsible party completes initial transactions. | Critical | | System should prompt the responsible party to add additional travelers in a family unit |
| 15 | The system shall provide a means to cancel additional family members if this option was selected in error. | | | |
| 16 | The system shall require each user or responsible party to confirm the biographic and passport information collected for each traveler. | Critical | | |

| Req# | Requirement | Priority | Disposition | Comments |
|---|---|---|---|---|
| 17 | The system shall require a non-USC user to select a class of admission. The system should ask the traveler: "What is the primary purpose of travel?"<br>Responses:<br>• B1-Temporary Visitor for Business (Canadian Citizens only)<br>• B2- Temporary Visitor for Pleasure (Canadian Citizens only)<br>• WB-Temporary Visitor for Business (Visa Waiver Travelers)<br>• WT-Temporary Visitor for Pleasure or Transit (Visa Waiver Travelers)<br>• Other-Lawful Permanent Residents or other visa classifications | Critical | | An answer must be provided for each non-USC passport.<br><br>The 'other' option should cease processing and refer the subject to traditional primary processing. |
| 18 | The system shall require each traveler who meets CBP biometric guidelines to submit fingerprint images. | Critical | Phase III | Fingerprint images collected shall be NFIQ equivalent (Referenced in ICD and Appendix A of this document). |
| 19 | The system shall incorporate a fingerprint image capture device that is FBI EBTS Appendix F certified. | Critical | Phase III | See Appendix A |
| 20 | The system shall secure a photograph immediately after fingerprint capture for each traveler meeting CBP biometric guidelines (non-USC travelers). Photographs are required for all travelers. | Critical | Phase III | See photograph recommendations in Appendix B |
| 21 | The system shall waive fingerprints for each non-USC traveler meeting CBP biometric guidelines 13 years of age and younger; and 80 years of age and older.<br>Photographs are required for all travelers. | Critical | Phase I, II and III. | |
| 22 | The system shall reject expired passports and refer user to a primary officer. | Critical | | |

| Req# | Requirement | Priority | Disposition | Comments |
|---|---|---|---|---|
| 23 | The system shall obtain a flight list from CBP once daily. | Critical | | |
| 24 | The system shall provide the user with flight information to confirm. | Critical | | |
| 25 | The system shall allow a user to manually select the correct flight information from a list provided on a touch screen monitor if the flight returned is not confirmed. | Critical | | The flight must be on the flight list provided by CBP specific to the particular airport. |
| 26 | The system shall provide the traveler with code share flight numbers in addition to the flight list provided by CBP. | Important | | Including codeshares reduces confusion and makes a more seamless process for the traveler. |

| Req# | Requirement | Priority | Disposition | Comments |
|---|---|---|---|---|
| 27 | The system shall allow an individual traveler or responsible party to answer CBP declaration questions by checking a "yes" or "no" box. Declaration Questions:<br>• Do you have any commercial merchandise or are you transporting currency or monetary instruments equal to or greater than $10,000 U.S., or foreign equivalent, in any form?<br>• Do you have any articles to declare that were acquired abroad and are being brought into the United States in excess of the duty free exemption? The duty free exemption is normally $800 for U.S. residents and $200 for flight crew members.<br>• Do you have any fruits, vegetables, plants, insects, meats or meat products, dairy products, animals or animal/wildlife products, disease agents, cell cultures, snails, soil; or have you visited a farm/ranch/pasture outside the United States?<br>• Have you been close to (such as touching or handling) livestock outside the United States? | Critical | | The declaration questions are only answered one time for the entire family unit by the responsible party.<br><br>Instructions that the declaration questions apply to entire family unit must be included. |
| 28 | The system shall not allow user to proceed without answering declaration questions. | Critical | | |
| 29 | The system shall provide user with 'Yes' and 'No' certification response boxes to permit travelers to verify all information is true and correct. | Critical | | "Are you sure all the answers you provided are true and correct?" |
| 30 | The system shall not proceed until certification is answered. | Critical | | |

| Req# | Requirement | Priority | Disposition | Comments |
|---|---|---|---|---|
| 31 | The system will transmit the user or family unit's collected data to CBP Automated Passport Control Services. | Critical | | Transmittal information in ICD. |
| 32 | The system shall receive messages from CBP Automated Passport Control Service. | Critical | | |
| 33 | The system shall provide a printed receipt with CBP codes and number of travelers in the group to each user. | Critical | | Example: Receipt 1 of 3, 2 of 3 and 3 of 3 or 1 of 1. |
| 34 | The receipt shall include:<br>• Automated Passport Control or other program identifier<br>• CBP branding<br>• The number of travelers in family unit.<br>• Biographic information of each individual user.<br>• Photo image of traveler<br>• Carrier Code and Flight number.<br>• Date of transaction<br>• CBP generated security code.<br>• CBP provided referral codes.<br>• Class of Admission Chosen (for non-USC's only)<br>• An "X" across the front if the traveler is being referred for further inspection based on referral codes. | Critical | | All receipt designs must be approved by CBP. |
| 35 | CBP must approve all receipt designs. | | | |
| 36 | CBP must approve any changes to receipt design after initial approval. | | | |
| 37 | The system shall inform the passenger where to go upon completion of the transaction. | Critical | | |
| 38 | The system shall provide a thank you message to the user or family unit upon completion. | Important | | |

| Req# | Requirement | Priority | Disposition | Comments |
|---|---|---|---|---|
| 39 | The system shall time out after allotted time on each screen page. | Important | | Allotted time to be decided |
| 40 | The Graphical User Interface (GUI) must be approved by CBP. | | | APC screens |
| 41 | Any GUI changes after initial approval must be presented to and approved by CBP. | | | |
| 42 | The system will allow for internal audits and reporting capabilities. | Important | | Reporting for system usage, usage time, system failures, response times, etc.<br><br>This capability is designed for the kiosk owner to monitor usage. CBP does not have a data retention requirement. |
| 43 | The system will not maintain CBP records or user information or otherwise permit use or distribution of CBP or user information unless specifically authorized in writing by CBP. | Important | | CBP will maintain records in currently available systems. |
| 44 | The system shall include a camera. | Critical | | |
| 45 | The system shall include e-passport verification. | Optional | Deferred | |
| 46 | The system shall include biometric technology. | Critical | | Fingerprint Technology-Must meet OBIM specifications. |
| 47 | DEPs shall be located in an area approved by CBP. | Critical | | |
| 48 | All design layouts and kiosk placement must be approved by CBP. | Critical | | |

| Req# | Requirement | Priority | Disposition | Comments |
|---|---|---|---|---|
| 49 | DEPs shall be properly secured and not pose a safety risk to the public. | | | Example: Any free standing equipment must be secured to ground and/or wall as not to fall over. Any monitors must be secured to equipment. |
| 50 | The system hardware, other than components used by the public, shall be located in a locked area. | Critical | | |
| 51 | Access to equipment, hardware and software shall be limited to designated persons vetted by CBP or individuals already maintaining access to the preclearance or FIS area. | Critical | | Designated persons are individuals who have a need to service, repair, audit, or maintain data entry points. |
| 52 | DEP owners must provide CBP Officers with work stations that meet ATDS. | Important | | Airport Technical Design Standards can be provided upon request. |
| 53 | CBP will approve all proposed work stations. | | | |
| 54 | DEP owners must provide anti-fatigue mats for each CBP APC work station. | | | |
| 55 | Automated Passport Control shall not be branded. The APC process, hardware, software, GUI and/or any related advertising can only display an airport authority logo and a CBP logo. | | | |
| 56 | All media communications regarding APC should be coordinated with CBP Office of Public Affairs | Important | | This includes press releases and ribbon cutting events. |
| 57 | The system shall not print a CBP referral receipt until all messages within the communication dialog are received. | Critical | | All messages need to be successfully processed before a receipt containing a CBP issued referral is printed. |

| Req# | Requirement | Priority | Disposition | Comments |
|---|---|---|---|---|
| 58 | The system shall print a System Failure (SF code) receipt in events where faults are received from the APC Service. | Critical | | System Failure (SF) referral receipts are to provide the traveler with evidence they experienced a technical difficulty with the APC system. |
| 59 | The system shall print a System Failure (SF code) receipt in events where the vendor provided APC system fails to transmit the final dialog message to CBP. | Critical | | In the event the TravelerEndRequest or TerminateSessionRequest (see ICD) fails to be successfully transmitted by the vendor system, a SF code receipt should be provided to the traveler(s). |
| 60 | The system shall print a Cancel Session (CA code) receipt in events where travelers cancel their session after being vetted by CBP. | Critical | | In events where a traveler cancels their session after their information has been transmitted to CBP, the vendor system should provide the traveler(s) with a Cancelled Session (CA) receipt. |

NO PRIVATE RIGHT CREATED. This document does not confer or create any right, privilege, or benefit for any private person.

## Appendix A

The Federal Bureau of Investigation approved list for forensic grade products (Appendix F) can be found at: http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_cert. Use the link to 'FBI Certified Product List'. This list shows commercial products that have passed the FBI's technical specifications and are acceptable for capture and transmission of biometrics.

The National Institute of Standards of Technology (NIST) Fingerprint Image Quality (NFIQ) number is a prediction of a matcher's performance. The number reflects the predictive positive or negative contribution of an individual sample to the overall performance of a fingerprint matching system.

The scoring table below shows the National Institute of Standards and Technology Fingerprint Image Quality (NFIQ) thresholds for prints captured for each finger.

| Number of Finger | Name of Finger | NFIQ Required Scoring |
|---|---|---|
| 1 | Right Thumb | 1-2 |
| 2 | Right Index | 1-2 |
| 3 | Right Middle | 1-2 |
| 4 | Right Ring | 1-2-3 |
| 5 | Right Pinky | 1-2-3 |
| 6 | Left Thumb | 1-2 |
| 7 | Left Index | 1-2 |
| 8 | Left Middle | 1-2 |
| 9 | Left Ring | 1-2-3 |
| 10 | Left Pinky | 1-2-3 |

## Appendix B

Photographic images should be ICAO conformant, meaning the face image would be captured as a digital photograph using JPEG, JPEG 2000, PNG, etc. The utility of a face image for either machine or human recognition is highly dependent on the quality of the photograph; therefore APC refers to the ICAO standards as "best practices" assuring a high quality capture. It is recommended that any Data Entry Point (DEP) mechanism ensures a face photograph maximizes

as many ICAO quality parameters as possible, in order to translate into better identification services. The key parameters relate to size of the face relative to the full image frame, the angle, pitch, and yaw of the subject's head, and the evenness and intensity of the lighting. To the extent that subjects are cooperative and habituated to the DEP, simple mechanisms for adjusting lighting, focus, and size (e.g. zoom) and then snapping the picture when the subject's head is at the right angle all increase quality.

A recommended approach is to employ a "quality in the loop" image capture step that employs software capable of analyzing the image and then controlling the shutter. There are several commercial and non-commercial software packages that can be used to add this quality loop. The preferred parameters are:

- Pose: Full Frontal or Frontal Token
- Angle: +/- 5 degrees in all three dimensions
- Expression: Neutral
- Eyes: Open with >90 pixels from pupil to pupil
- Background: plain with no texture
- Lighting: No shadows or point lighting
- Size: Minimum 640 x 480 pixel
- Face Size: >1/2 width of frame and >3/4 height of frame
- Camera: 24 bit color

## Appendix C

**Disclaimer:**

You are about to use a kiosk that is owned by [____] and that is used to facilitate processing by U.S. Customs and Border Protection (CBP) of travelers intending to enter the United States. The

information you provide at this kiosk will be transmitted to CBP for official use and retention consistent with applicable U.S. laws and policies. The use of this kiosk is voluntary; if you do not wish to use this kiosk, please proceed directly to CBP primary examination. Regardless of whether you choose to use this kiosk, as a traveler seeking to enter the United States, you are subject to examination and inspection by CBP.

All information provided by you at this kiosk (whether on your behalf or on behalf of any travelers in your family unit) must be true and correct. Information you provide to CBP through this kiosk is considered a written statement, and you may be subject to sanctions, including criminal penalties, if you knowingly and willfully make a materially false, fictitious or fraudulent statement or representation.

For information about the CBP Privacy Policy and the Privacy Act of 1974, visit www.cbp.gov.

**Paperwork Reduction Act Notice:**

The U.S. Paperwork Reduction Act says we must tell you why we are collecting this information, how we will use it, and whether you have to give it to us. The information collected at this kiosk is needed to carry out the customs, agriculture, currency, and other applicable laws of the United States. CBP requires submission of this information to insure that travelers are complying with these laws and to allow us to figure and collect the right amount of duty and tax. Your response at this kiosk is mandatory; in some instances, you may also be required to complete a CBP Form 6059B. A U.S. agency may not conduct or sponsor an information collection and a person is not required to respond to this information unless it displays a current valid Office of Management and Budget (OMB) control number. The control number for this collection is 1651-0111. The estimated average time to complete this submission is 5 minutes per respondent. If you have any comments regarding the burden estimate you can write to U.S. Customs and Border Protection, 90 K Street, NE, 10th Floor, Washington, D.C. 20229. Exp. Mar. 14, 2014.

**Certification:**

By submitting the information provided at this kiosk to CBP, I am certifying that all information submitted is truthful.

# APPENDIX G

## Automated Passport Control Service Technical Reference Manual (Version 2)

U.S. Customs & Border Protection
Passenger Systems Program Office

# Automated Passport Control Service Technical Reference Manual (Version 2)

## January 24, 2014

**Document Number:**
**3209000-TRM v2**

# Change Control Log

| Revised by | Date | Description of Revisions |
|---|---|---|
| J. Muhlenberg | 8/24/2012 | Initial Document. |
| E. Connolly | 8/31/2012 | Updates |
| P. Williams | 10/18/2012 | Changed the document title |
| C. Swallow | 10/24/2012 | Updated diagrams, APC references, and added in Receipt Referral Codes |
| C. Swallow | 11/13/2012 | XML and editorial updates. |
| C. Swallow | 10/16/2012 | Added biometric section |
| C. Swallow | 12/17/2012 | Updated Diagrams and Tables |
| Judy Titterton | 12/17/2012 | Edited and formatted to PSPO standards |
| C. Swallow | 12/17/2012 | Include Process Flows |
| Y. White | 12/19/2012 | Updated the domain model. |
| C. Swallow | 12/27/2012 | Updated domain model and incorporating feedback. |
| C. Swallow | 2/19/2013 | Updates to sections 5.1 and 5.2 |
| C. Swallow | 3/12/2013 | Updated process flow diagrams |
| C. Swallow | 7/26/2013 | Document overhaul to replicate more up to date information represented in the Phase 2 ICD (7/25/13), including diagrams, sample messages, sample message tables, section descriptions. |
| M. Nuriddin | 7/30/2013 | Revised – version 2 |
| C. Swallow | 1/24/2014 | Document overhaul to replicate more up to date information represented in the Phase 3 ICD, including diagrams, sample messages, tables, and descriptions. Also included most recent work flow diagrams from 3209-015 User CR. |

# Table of Contents


1. INTRODUCTION ..... 1
   1.1 PURPOSE ..... 1
   1.2 SYSTEM OVERVIEW ..... 1
   1.3 BACKGROUND ..... 1
   1.4 DOCUMENT REFERENCES ..... 1
   1.5 REFERENCES AND STANDARDS ..... 2
2. SYSTEM DESCRIPTION ..... 3
   2.1 SYSTEM IDENTIFICATION ..... 3
      2.1.1 Kiosk System ..... 3
      2.1.2 APC Service ..... 4
3. INTERFACE OVERVIEW ..... 5
   3.1 FUNCTIONAL ALLOCATION AND DATA TRANSFER ..... 5
      3.1.1 APC Service ..... 5
   3.2 TRANSACTIONS ..... 9
      3.2.1 Data Exchange Transactions ..... 9
   3.3 SECURITY AND INTEGRITY ..... 9
   3.4 CONNECTION METHODS AND COMMUNICATION ..... 9
      3.4.1 IP Addresses ..... 9
      3.4.2 2-Way SSL Certificates ..... 9
4. DETAILED INTERFACE SPECIFICATIONS ..... 11
5. REQUIREMENTS ..... 12
   5.1 SECURITY AND ARCHITECTURAL REQUIREMENTS ..... 12
   5.2 INTEGRATION TESTING ..... 12
   5.3 DELIVERY AND ACCEPTANCE ..... 12
   5.4 KIOSK REGISTRATION ..... 12
6. BIOMETRICS ..... 13
   6.1 FINGERPRINT CAPTURED BIOMETRICS ..... 13
      6.1.1 Fingerprint Images ..... 13
      6.1.2 NFIQ Scores ..... 13
   6.2 FACIAL PHOTOGRAPHICALLY CAPTURED BIOMETRICS ..... 14
7. PROCESS FLOWS ..... 15
8. OPEN DISCUSSION ITEMS ..... 19

# List of Figures

Figure 1. APC Service High Level Technical Architecture....3
Figure 2. APC Service Message Dialogue....5
Figure 3. APC Service Message Domain Model, Part 1....7
Figure 4. APC Service Message Domain Model, Part 2....8
Figure 5. Two-Way SSL Authentication....10
Figure 6. United State Citizens (USC)....16
Figure 7. Canadian Citizens (CAN)....17
Figure 8. Foreign National – US Visa Waiver....17

# List of Tables

Table 1. Document References....2
Table 2. References and Standards....2
Table 3. NFIQ Scores....13
Table 4. Open Discussion Items....19

# APC Service Technical Reference Manual

## 1. Introduction

### 1.1 Purpose

The purpose of this document is to provide the technical requirements that will need to be supported to interface a third party system with the Automated Passport Control (APC) Service. This third party system (referred in this document as the Kiosk System) will be used to facilitate and expedite border crossings at Customs and Border Protection (CBP) approved airports.

### 1.2 System Overview

CBP/Office of Information and Technology (OIT) is developing a non-airport specific Web service that will help facilitate and expedite border crossings for U.S., Canadian, and authorized Visa Waiver citizens at designated North American airports. This service will be offered so that an airport authority can develop third party data collection methods and systems that will assist the CBP Officer in completing the administrative portion of a border crossing inspection prior to speaking with an officer. The third party collection methods, hardware, software, and processes are referenced in this document as the Kiosk System for simplicity. The third party solution does not have to include a self-service kiosk system. The third party is free to offer alternative solutions to CBP and the airport authorities for their approval. Future service expansions will consist of U.S. eligible Visa Waiver travelers and select foreign nationals.

### 1.3 Background

CBP is one of the Department of Homeland Security's largest components. CBP is responsible for protecting the United States' front line, while facilitating legitimate trade and travel. CBP is continuously working to improve the entry process for travelers and realize the goal of increased security while expediting the flow of legitimate travel. The goal of the self-service kiosk in a CBP environment is to allow a traveler or family unit a portion of an inspection prior to speaking with a CBP Officer.

The intent of the kiosk system is to collect traveler information and transfer that information to CBP for law enforcement and border inspection purposes. A self-service kiosk option has been added to the Airport Technical Design Standard (ATDS), allowing Airport Authorities the option to use kiosks to facilitate data collection. CBP/OIT worked to develop a technology requirements package to provide to interested airport authorities. Under the ATDS, Airport Authorities can opt to incorporate kiosks as equipment in their respective Federal Inspection Services (FIS) areas. The kiosk equipment is provided by, maintained, and owned by the Airport Authority. Any kiosk procured and installed by an Airport Authority must comply with Automated Passport Control Services technology requirements and meet CBP Business requirements.

For information about this project, contact CBP Office of Field Operations (OFO) Andrew Douglas (ANDREW.H.DOUGLAS@CBP.DHS.GOV) or Jeni Best (jeni.m.best@cbp.dhs.gov).

### 1.4 Document References

Table 1 lists the documents used as references for the APC Service Technical Reference Manual.

**Table 1. Document References**

| User Reference Document Name | Document Identification Number | Location |
|---|---|---|
| U.S. Customs and Border Protection Fiscal Year 2009–2014 Strategic Plan | | http://cbpnet.cbp.dhs.gov/xp/cbpnet/oc/resources/cbp_mission_lp.xml |
| CBP's Missions, Goals, and Priorities, FY2011-2013 | 2011-2013 | http://cbpnet/linkhandler/cbpnet/oc/resources/goals2.ctt/goals2.pdf |
| CBP Information Systems Security Policy and Procedures Handbook, Version 3.0, Feb 8, 2012 | HB 1400-05D Information Systems Security Policies and Procedures Handbook | http://pods.cbp.dhs.gov/docs/office%20of%20information%20&%20technology%20(oit)/handbooks/hb%201400-05d.pdf |
| Department of Homeland Security National Security Systems Policy Directive 4300B, Version 4.3, September 30, 2007 | DHS National Security Systems Policy Directive 4300A | http://oitpal.cbp.dhs.gov/pal/code/AssetView.cfm?AssetID=10290 |
| National Institute of Standards and Technology Special Publication 800-64, Revision 2, Security Considerations in the Information System Development Life Cycle, October 2008 | NIST 800-64 Rev. 1 | http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf?bcsi_scan_E653FC67EE2638AB=hCChem36fG899nlGsA7uvCEAAABaQzqF&bcsi_scan_filename=SP800-64-Revision2.pdf |

## 1.5 References and Standards

Table 2 lists references and information processing standards are used or referenced within this document.

**Table 2. References and Standards**

| Reference/Standard | Document Identification Number | Document Location |
|---|---|---|
| National Information Exchange Model (NIEM) | | www.niem.gov |
| Flight information and information processing standards | | IATA, ICAO, and ISO 3166-1 etc. |
| U.S. Department of State Passport Technical Standards | | ICAO 9303 |

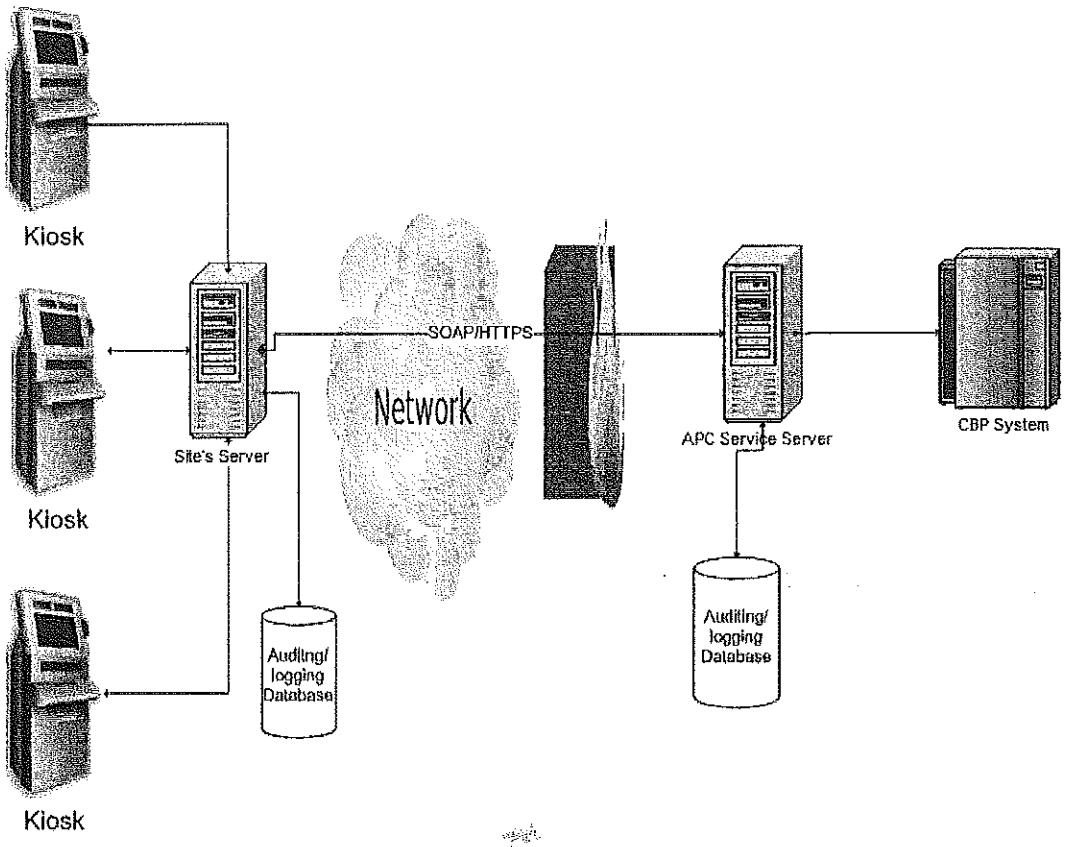
# 2. System Description

This section identifies the systems participating in the APC Service interface, the interfacing entities, and the interfaces to which this document applies.

## 2.1 System Identification

Figure 1 illustrates the high-level system components and interfaces that are used in the APC Service. The principle components of the system are the Kiosk System and the APC Service. The Kiosk System requests information from the APC Service while the APC Service interacts with various CBP systems to obtain a response relevant to the Kiosk System's request.

**Figure 1. APC Service High Level Technical Architecture**




### 2.1.1 Kiosk System

The Kiosk System is a self-service entry point used by Airport Authorities to collect traveler information and transfer that information to CBP for law enforcement purposes. The Kiosk System is: (1) a piece of equipment in the form of a kiosk or other CBP approved device that allows a traveler to input data and (2) a site server that allows the kiosk to interface with CBP's APC Service for traveler processing. The Kiosk System is neither managed nor implemented by CBP; third-party vendors are responsible for its system implementation. While it interfaces with

the APC Service to request traveler processing data, the Kiosk System is isolated from CBP's internal networks and systems.

The following functions will be performed by the Kiosk System:

- Meet the business, technical, and operational requirements
- Display information and instructions to the traveler(s)
- Collect the necessary travel information from each traveler
- Collect biometrics from traveler(s), if relevant
- Prepare and send the Traveler Validate Request(s)
- Process vetting results from the Traveler Validate Response message
- Request and receive the Traveler End message
- Prepare and print receipts for traveler as specified
- Record and document session information
- Request and receive the APC Service system status message
- Request and receive the latest flight list information from APC Service

### 2.1.2 APC Service

The APC Service is a web service that implements the high level requirements described in this section. The APC Service is the primary interface to CBP for the Kiosk System and will facilitate traveler vetting, flight manifest lookups, and flight confirmations. The APC Service and the Kiosk System support the overall goal of the Automated Passport Control program.

The following functions will be performed by the APC Service

- Read and validate the Flight List Request
- Prepare and send the Flight List Response
- Read and validate the Traveler Validate Request(s)
- Calculate the referral code according to the business rules for each traveler
- Prepare and send the Traveler Validate Response message
- Read and validate the Traveler End Request from the Kiosk System
- Prepare and send Traveler End Response(s)
- Prepare and send the Border Crossing record notifications to the appropriate CBP systems
- Read and validate the System Status Request
- Prepare and send System Status Response

The APC Service is hosted in the CBP National Data Center (NDC) and supported by the CBP Office of Information Technology (OIT) network and operations center. This center monitors and supports the network and servers to provide connectivity and system monitoring between the airport and NDC.

# 3. Interface Overview

## 3.1 Functional Allocation and Data Transfer

The APC Service supports four operations: System Status, Flight List, Traveler Validate and Traveler End Session. The System Status request allows the client to obtain the current state of the APC Service. Upon receiving the request, the APC Service sends a response indicating whether or not it is available for processing. The Flight List request signals the APC Service to obtain flight information from CBP's internal systems. Afterwards, the APC Service will format and send the appropriate flight manifest in the response message. The Traveler Validate request initiates vetting processing of a traveler for a border crossing. A response is sent to the client indicating the results of the traveler processing. Following a Traveler Validate request, a client sends a Traveler End call to request an end to the traveler processing. Upon receiving the request, the APC Service will process the traveler confirmation and send a response back indicating that the session for the traveler has completed.

The subsequent sections review the aforementioned data exchanges. Refer to them for details regarding the message components used to communicate with the APC Service.

### 3.1.1 APC Service

The APC Service provides four web service operations that allow the Kiosk System to request information from the APC Service. In each of the four dialogues, the Kiosk System initiates the message request and the APC Service provides a message response. The web services operations are:

- Flight List
- Traveler Validate
- Traveler End
- System Status

System Status and Flight List are standalone requests; they are informational services that inform on system availability and provide flight information, respectively. On the other hand, Traveler Validate and Traveler End are used in sequence as part of an interactive workflow that processes a traveler. Figure 2 shows the message dialogue that may occur between the Kiosk System and the APC Service.

**Figure 2. APC Service Message Dialogue**

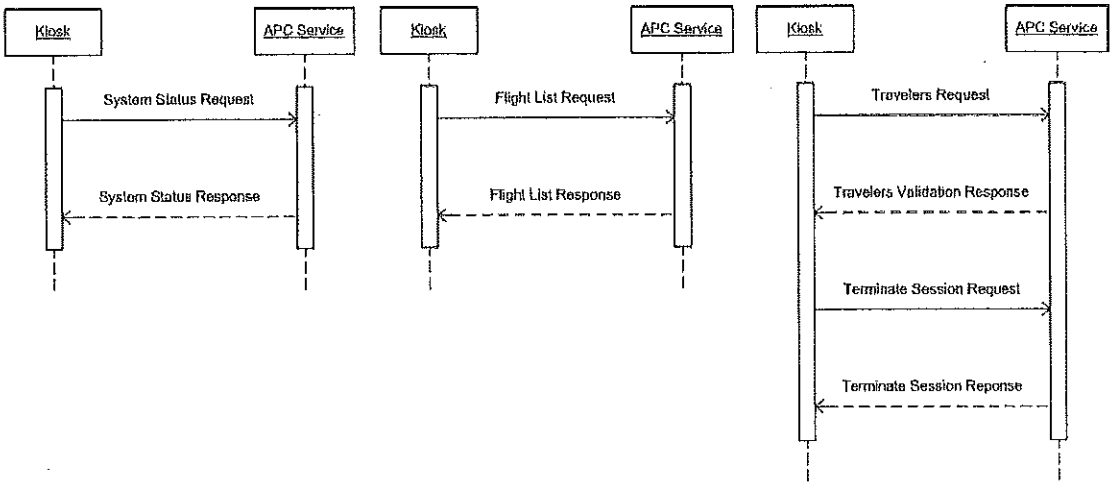



Figure 3 and 4 below document the basic XML Domain Model diagram. It describes the relationship of the dialogue of request and response message structures and from the APC Service and the Kiosk System.

**Figure 3. APC Service Message Domain Model, Part 1**

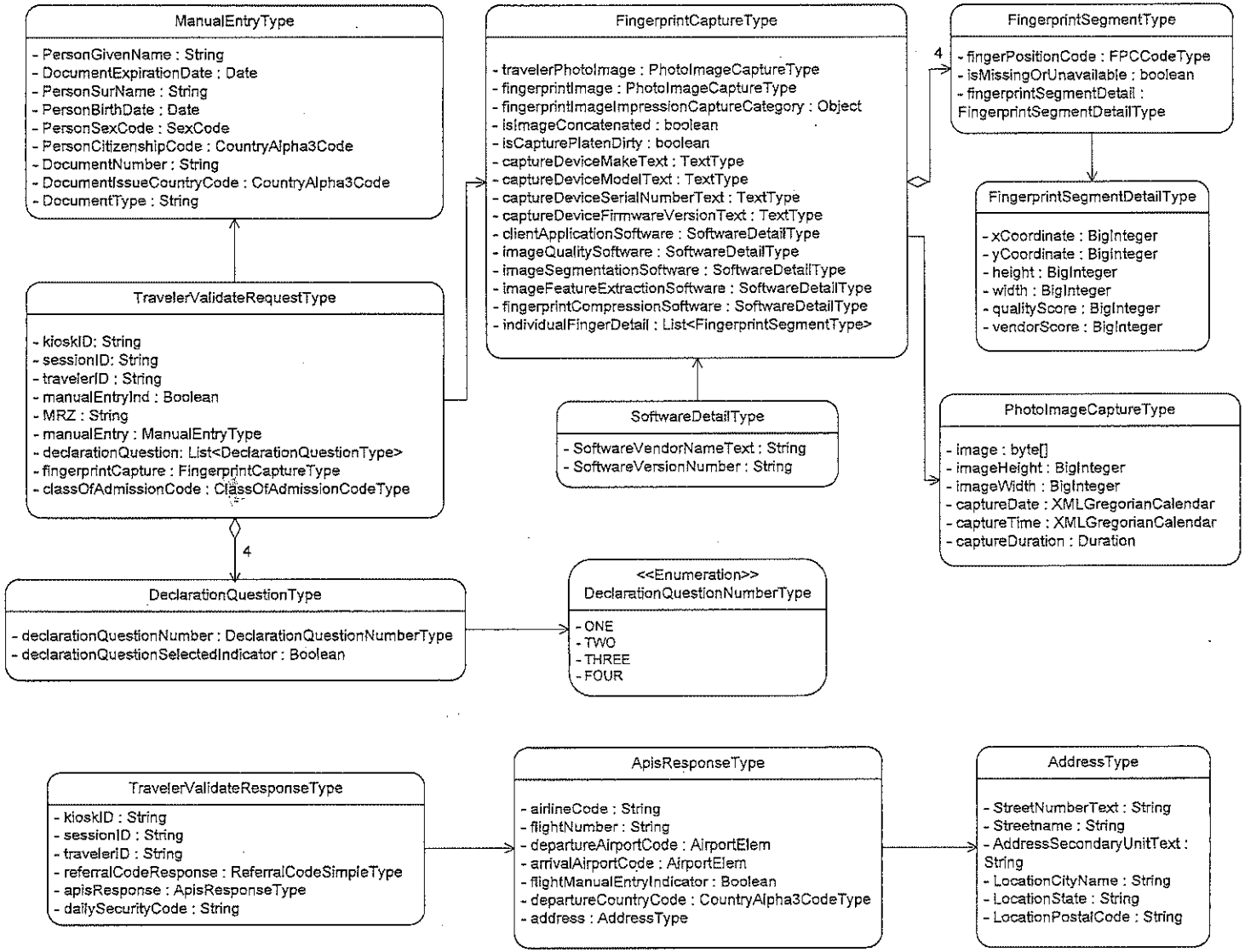
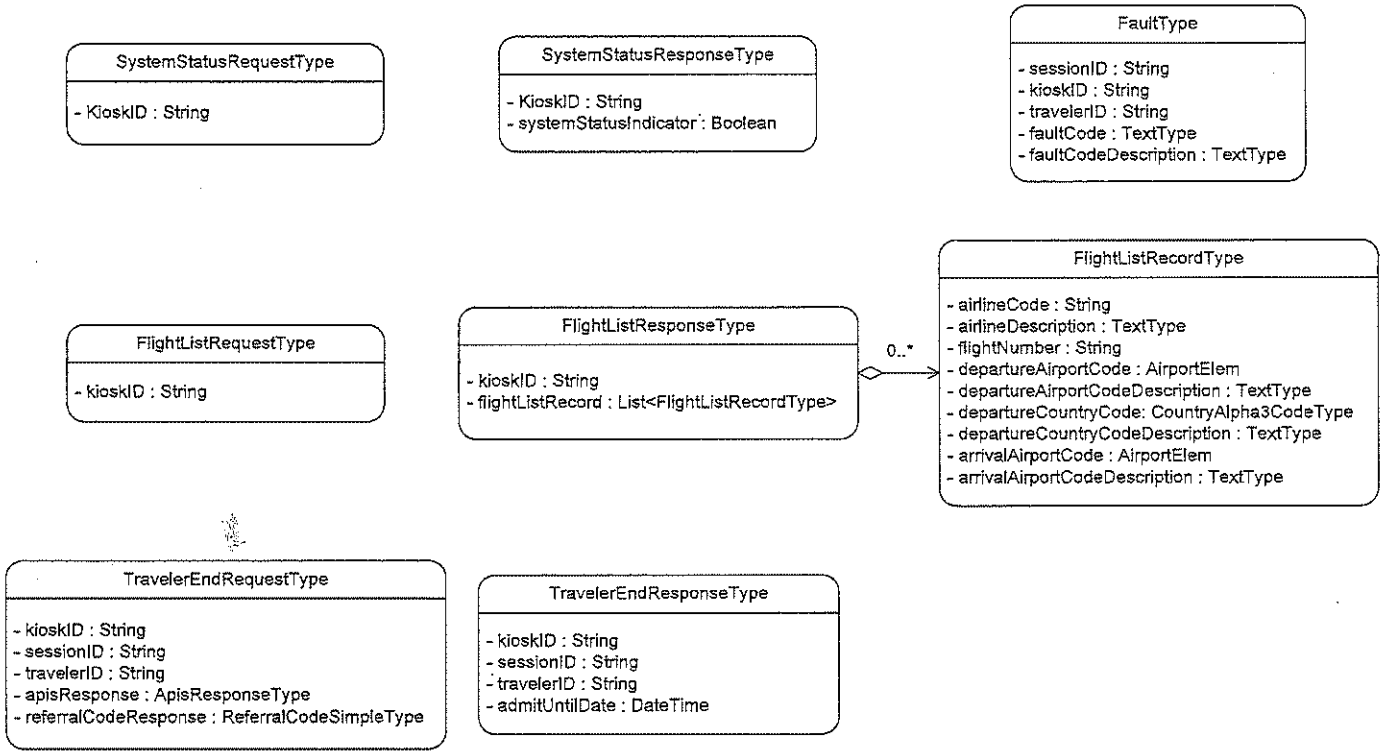



**Figure 4. APC Service Message Domain Model, Part 2**



150


SystemStatusRequestType
- KioskID : String
SystemStatusResponseType
- KioskID : String
- systemStatusIndicator : Boolean
FaultType
- sessionID : String
- kioskID : String
- travelerID : String
- faultCode : TextType
- faultCodeDescription : TextType
FlightListRequestType
- kioskID : String
FlightListResponseType
- kioskID : String
- flightListRecord : List<FlightListRecordType>
0..*
FlightListRecordType
- airlineCode : String
- airlineDescription : TextType
- flightNumber : String
- departureAirportCode : AirportElem
- departureAirportCodeDescription : TextType
- departureCountryCode: CountryAlpha3CodeType
- departureCountryCodeDescription : TextType
- arrivalAirportCode : AirportElem
- arrivalAirportCodeDescription : TextType
TravelerEndRequestType
- kioskID : String
- sessionID : String
- travelerID : String
- apisResponse : ApisResponseType
- referralCodeResponse : ReferralCodeSimpleType
TravelerEndResponseType
- kioskID : String
- sessionID : String
- travelerID : String
- admitUntilDate : DateTime

151

## 3.2 Transactions

The transactions between the APC Service and the Kiosk System will consist of requests and responses. The information and data structures for the transaction exchanges are described in the Interface and Control Document (ICD).

### 3.2.1 Data Exchange Transactions

The National Information Exchange Model (NIEM) will be used to implement the XML data structures for the APC Service. The use of NIEM is DHS mandated and it provides the basic data types for XML validation.

Information on NIEM can be found at http://www.niem.gov/.

Information on the APC Service Information Exchange Package (IEPD) may be requested from CBP when needed.

## 3.3 Security and Integrity

The Kiosk System is hosted on an airport's network. The interface protocol between the airport network and the APC Service will be HTTPS/SOAP XML messages sent to and from an XML appliance and the Kiosk System. The XML appliance provides an isolation layer that protects the security and integrity of the CBP network. The SSL certificates and IP addresses, port number information, protocols, virus software and other technical controls are configured to ensure the security and information integrity of the CBP network. AES-256 encryption is required for messages sent from the kiosk to CBP.

Message information integrity is maintained through the use of XML and XSD validation schemas to ensure that each transaction is unique and accurate.

The Kiosk System shall not store any privacy sensitive data such as MRZ data, personal traveler data or referral codes. This information and the detailed security rules will be explained in the Privacy Impact assessment document.

## 3.4 Connection Methods and Communication

### 3.4.1 IP Addresses

Each site must provide CBP a publically routable IP address to be used in the Production environment and a separate IP address to be used in the Non- Production environment. If failover is included in the network design, IP addresses for each server should be provided. CBP recommends that a site provide no more than four (4) IP addresses to CBP.

### 3.4.2 2-Way SSL Certificates

The communication between the Kiosk System and the APC Server occurs via a two-way SSL connection utilizing mutual authentication. Certificates need to be from a publically recognized certificate authority, certified in the Federal Information Processing Standards (FIPS), a standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology (NIST).

It is CBP's recommendation to use VeriSign or Entrust, both of which are acceptable registered certificate providers. Each Airport will utilize a single SSL Certificate to communicate with the CBP production site. A separate SSL certificate will be required for communication between the Airport non-production environment and CBP's non-production (test) environment. The one non-production certificate will be used for communication with both the CBP System Acceptance Test (SAT) and the CBP Quality Assurance (QAX) environments.

Prior to establishing communication between the systems, the APC Service will need to register the Kiosk System's

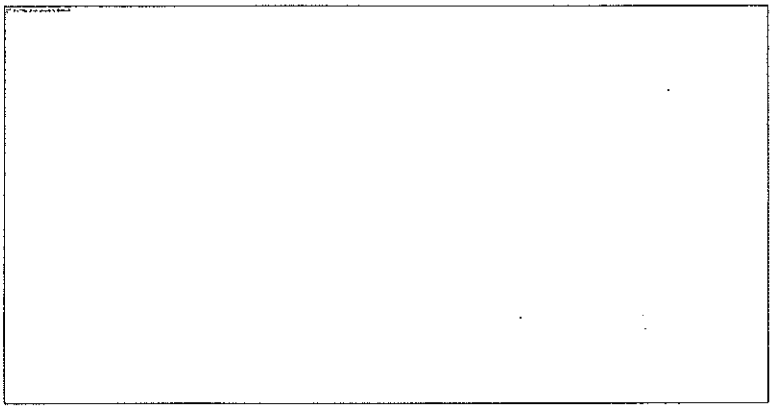
(a) publicly routable IP address, and
(b) public certificate (2048 bits) from a CBP approved Certificate.

In addition, the Kiosk System will need the APC Service's Certificate Authority certificate chain to authenticate the APC Service.

To successfully connect to the APC Service both parties must exchange and install the certificates prior to initiating the SSL conversation.

Figure 5 illustrates the certificate configuration for two-way SSL authentication between two applications.

**Figure 5. Two-Way SSL Authentication**



The SSL client (the APC Kiosk Server) initiates a connection to the SSL server (the APC Service) by opening a connection to the SSL server. Next, the SSL server presents its certificate to the SSL client for verification and then requests that the SSL client present its certificate to the SSL server for verification. Once this protocol is completed and the certificates match then the communications dialogue between the Kiosk System and the APC Service may commence.

# 4. Detailed Interface Specifications

Specific details on the interface will be provided to each vendor as they become an approved participant. Once an agreement is in place, an Interface Control Document (ICD) will be created between CBP and the vendor, which will detail the interface specifications. This ICD will include message structure, processing times, IP addresses, port information, and estimated message sizes.

# 5. Requirements

## 5.1 Security and Architectural Requirements

To ensure that the kiosk system is meeting the CBP security and technical architecture requirements, the Kiosk System will have to go through an integration test and acceptance process with CBP to ensure compliance and conformance with CBP's technical and architectural requirements.

The Kiosk System can be audited at any time to ensure that the system meets the security and technical requirements. If a Kiosk System is found to not meet those technical requirements then the appropriate actions will be taken by CBP to address the situation.

## 5.2 Integration Testing

The integration testing will be an iterative process where the kiosk system will undergo a series of integration and acceptance tests to ensure that the Kiosk System meets the environmental, business, architectural, technical, and security requirements and controls needed to ensure compliance with CBP system requirements.

Any technical or functional items and noted issues and problems to be addressed will be noted and resolved by the kiosk before any installation at any airport. Modifications and updates to the kiosk system will be reviewed and this integration test process repeated.

## 5.3 Delivery and Acceptance

To ensure that the Kiosk system meets CBP requirements, there will be a final sign off acceptance agreement between the Kiosk System, the APC Service Program Manager, and CBP business owner and the airport organization before processing travelers can begin.

## 5.4 Kiosk Registration

Any kiosk that will be included in this program will need to be registered with CBP to include the airport location and a unique kiosk identifier. If a kiosk is to be taken offline or moved, CBP must be notified prior to that move.

# 6. Biometrics

The introduction of foreign national travelers being processed by the APC Service and Kiosk System will require the use of biometric capturing. The two forms of biometric capturing and submission will be the traveler's fingerprints and facial photo.

## 6.1 Fingerprint Captured Biometrics

Fingerprint Captured Biometrics sent to the APC Service for processing will need to follow the recommended standards described in this section for fingerprint image criteria and image quality thresholds.

### 6.1.1 Fingerprint Images

It is strongly recommended that the resolution for fingerprint images be 39.37 ppmm (1000 ppi). It should be noted that as the class resolution is increased, more detailed ridge and structure information becomes available in the fingerprint image. However, in all cases the class resolution shall be at least 19.69 ppmm (500 ppi). The variable-resolution fingerprint image data contained in the record may be in a compressed form. A list of FBI-approved forensic grade products can be found at the following link: http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_cert

Click FBI Certified Products List; this listing shows commercial products that have passed the FBI's technical specifications and are acceptable for capture and transmission of biometrics to the APC Service for processing.

### 6.1.2 NFIQ Scores

National Institute of Standards and Technology (NIST) Fingerprint Image Quality (NFIQ) number is a prediction of a matcher's performance; it reflects the predictive positive or negative contribution of an individual sample to the overall performance of a fingerprint matching system.

NFIQ has five levels of quality thresholds that are intended to be predictive of the relative performance of a minutia based fingerprint matching system, where an NFIQ score of 1 is the highest quality, and an NFIQ score of 5 is the lowest. Refer to Table 3 for required NFIQ scores for each associated finger.

**Table 3. NFIQ Scores**

| Number of Finger | Name of Finger | NFIQ Required Scoring |
|---|---|---|
| 1 | Right Thumb | 1-2 |
| 2 | Right Index | 1-2 |
| 3 | Right Middle | 1-2 |
| 4 | Right Ring | 1-2-3 |
| 5 | Right Pinky | 1-2-3 |
| 6 | Left Thumb | 1-2 |
| 7 | Left Index | 1-2 |

| Number of Finger | Name of Finger | NFIQ Required Scoring |
|---|---|---|
| 8 | Left Middle | 1-2 |
| 9 | Left Ring | 1-2-3 |
| 10 | Left Pinky | 1-2-3 |

A list of certified software vendors that meet FBI standards for Wavelet Scalar Quantization (WSQ) Gray-scale Fingerprint Image Compression Algorithm exchanges can be found at the following link: https://www.fbibiospecs.org/wsq/Implementations/Default.aspx

## 6.2 Facial Photographically Captured Biometrics

Facial Photographically Captured Biometrics is captured photographs of the face that produce a digital image. The digital image will need to conform with ICAO, meaning that the photograph of the face will need to follow ICAO photograph standards and be captured using transmittable formats of JPEG, JPEG200, PNG, etc.

The utility of a photographed facial image for either machine or human recognition is highly dependent on the quality of the photograph itself. Therefore, APC refers to the ICAO photograph standards as "best practices" to assure a high quality capture. Kiosk vendors are recommended to build in mechanisms that can ensure the facial photograph captured maximizes as many of the ICAO quality parameters as possible, translating into better identification services. The ICAO quality parameters relate to the size of the face relative to the full image frame, the angle, pitch, and yaw of the subject's head, and the evenness and intensity of the lighting. To the extent that subjects are cooperative and habituated to the kiosk, simple mechanisms for adjusting lighting, focus, and size (e.g. zoom) and then snapping the picture when the subject's head is at the right angle all increase quality.

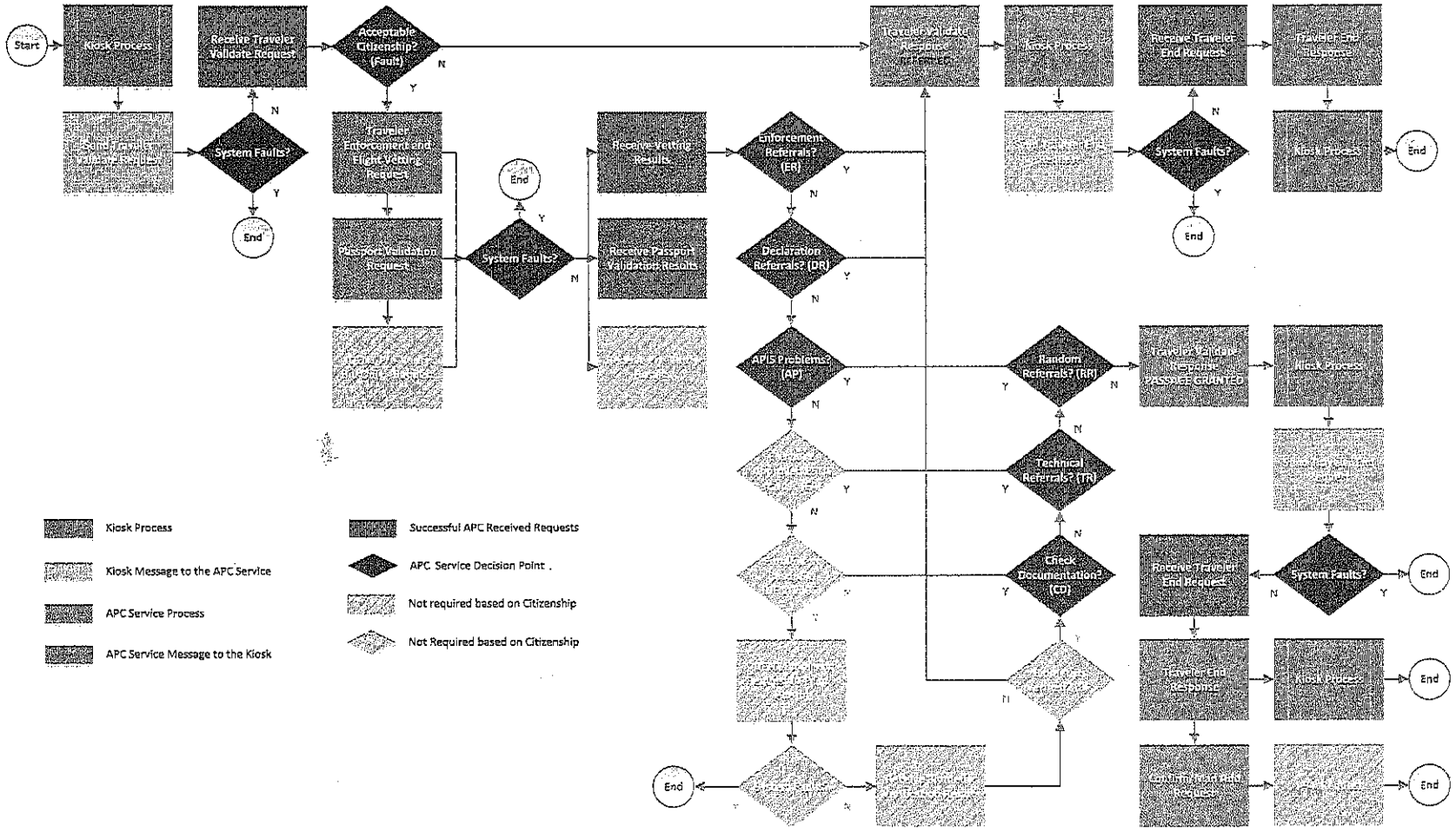
A recommended approach is to employ a "quality in the loop" image capture step that employs software capable of analyzing the image and then controlling the shutter. There are several commercial and non-commercial software packages that can be used to add this quality loop. The Pre-Face product from Aware Inc., has been tested and shown to be effective in performing this function. The preferred parameters are:

- Pose: Full Frontal or Frontal Token
- Angle: +/- 5 degrees in all three dimensions
- Expression: Neutral
- Eyes: Open with >90 pixels from pupil to pupil
- Background: plain with no texture
- Lighting: No shadows or point lighting
- Size: Minimum 640 x 480 pixel
- Face Size: >1/2 width of frame and >3/4 height of frame
- Camera: 24 bit color

# 7. Process Flows

The following visualizations represent the processing workflow for the three types of travelers currently able to utilize APC kiosks, United States Citizens, Canadian Citizens, and Foreign Nationals of US Visa Waiver Countries.

**Figure 6. United State Citizens (USC)**




159

**Figure 7. Canadian Citizens (CAN)**

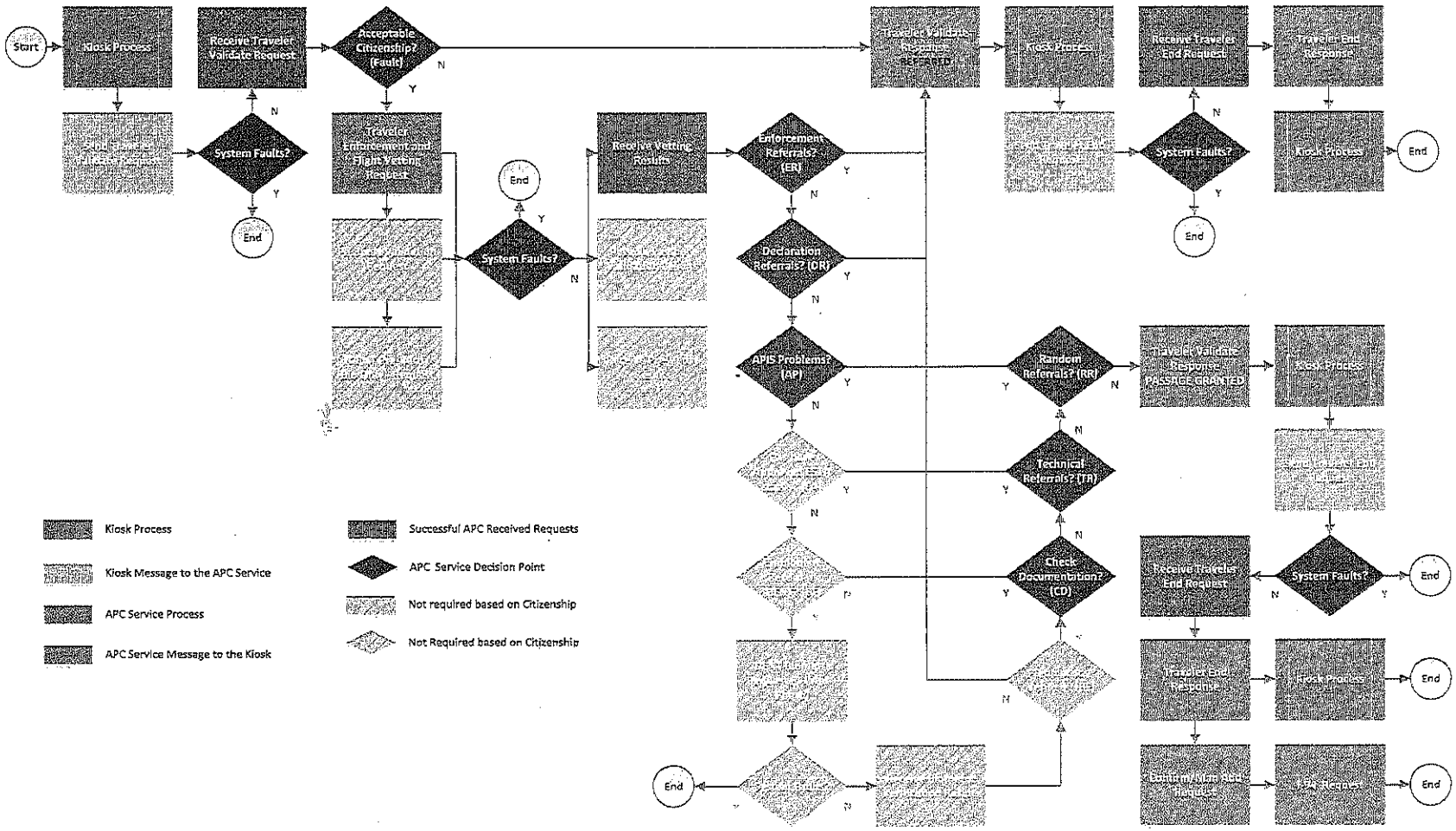
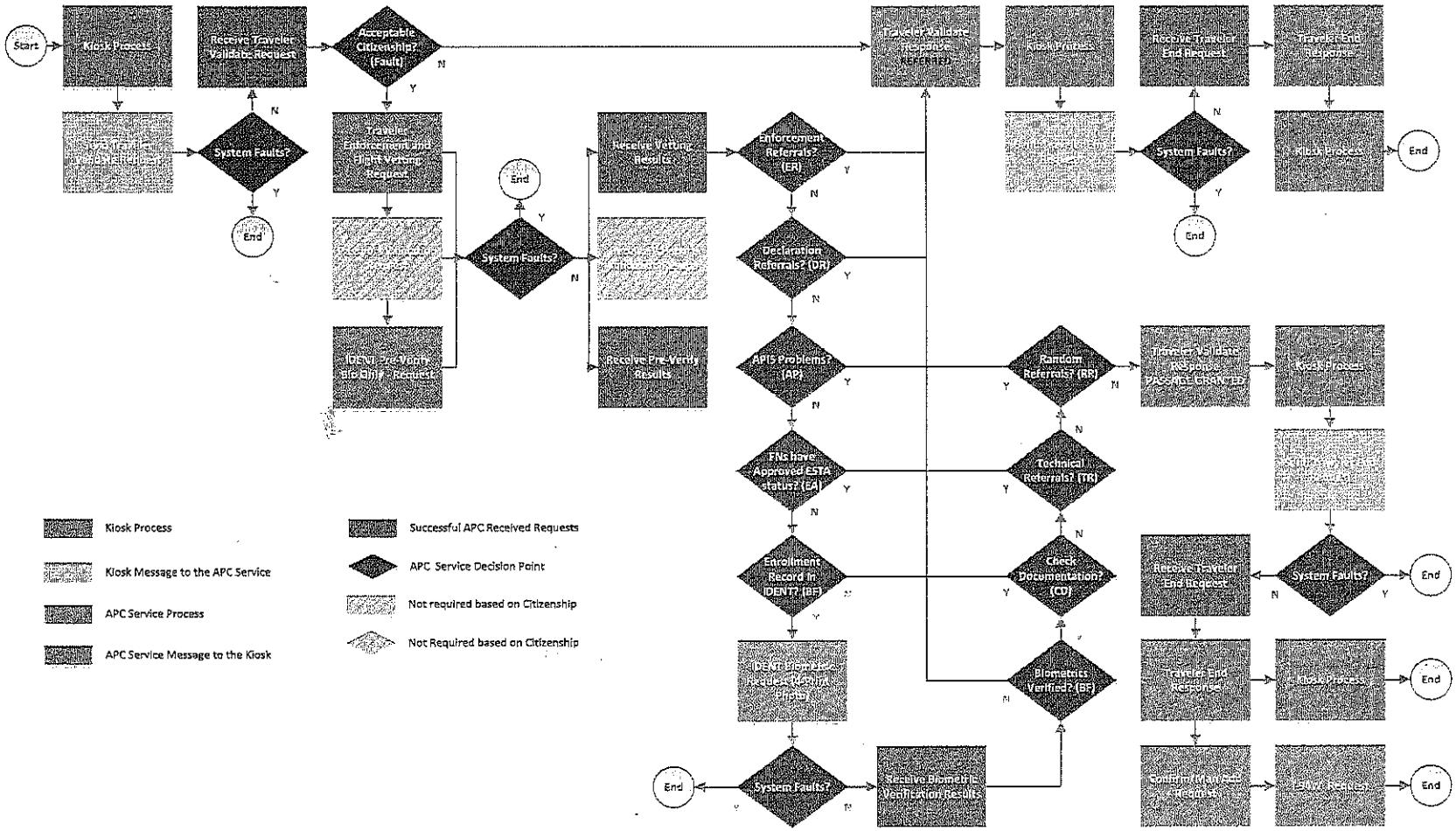


**Figure 8. Foreign National – US Visa Waiver**



# 8. Open Discussion Items

This section contains items and information that needs to be clarified throughout this document and other items that need to be discussed between the two parties involved with this exchange. Table 4 lists open discussion items.

**Table 4. Open Discussion Items**

| Item # | Title | Description |
|---|---|---|
| | | |

# APPENDIX H

## U.S. CUSTOMS & BORDER PATROL "AUTOMATED PASSPORT CONTROL SERVICE (RELEASE 2.0 V4) INTERFACE CONTROL DOCUMENT (DOCUMENT NUMBER 3209000-ICD)

U.S. Customs and Border Protection

Passenger Systems Program Directorate

# Automated Passport Control Service Release 2.0 Interface Control Document

**August 12, 2014**

**Document Number: 3209000-ICD**

**v4**

*For Official Use Only (FOUO)*

# Change Control Log

| Revised by | Date | Description of Revisions |
|---|---|---|
| CBP OIT | 10/28/2013 | Previous Document |
| CBP OIT | 11/25/2013 | - Updated diagrams, tables, and SOAP samples with schema and messaging enhancements.<br>- Overall document refinements. |
| CBP OIT | 4/25/2014 | Incorporation of Legal Permanent Residents |
| CBP OIT | 8/11/2014 | Incorporate Kiosk assignment of SF and CA Referral Codes |

# Table of Contents

**1. INTRODUCTION** ..... 1
1.1 PURPOSE ..... 1
1.2 SYSTEM OVERVIEW ..... 1
1.3 BACKGROUND ..... 1
1.4 CONTACT INFORMATION ..... 2
1.5 DOCUMENT REFERENCES ..... 2
**2. SYSTEM DESCRIPTION** ..... 3
2.1 SYSTEM ARCHITECTURE ..... 3
2.2 KIOSK SYSTEM ..... 3
2.3 APC SERVICE ..... 4
2.4 APC WEB SERVICE DIALOGUES ..... 5
2.5 KEY PROCESSING FIELDS ..... 6
2.6 APC SERVICE MESSAGE DOMAIN MODELS ..... 7
**3. MESSAGE EXCHANGE SPECIFICATIONS** ..... 10
3.1 WSDL AND XML SCHEMAS ..... 10
3.2 NATIONAL INFORMATION EXCHANGE MODEL (NEIM) ..... 10
3.3 MESSAGE EXCHANGE ..... 10
3.4 REQUEST MESSAGES ..... 12
3.4.1 Flight List Request ..... 12
3.4.2 Traveler Validate Request ..... 12
3.4.3 Traveler End Request ..... 20
3.4.4 System Status Request ..... 21
3.5 RESPONSE MESSAGES ..... 22
3.5.1 Flight List Response ..... 22
3.5.2 Traveler Validate Response ..... 24
3.5.3 Traveler End Response ..... 27
3.5.4 System Status Response ..... 28
3.5.5 Fault Element ..... 28
**4. COMMUNICATIONS** ..... 29
4.1 IP ADDRESSES ..... 29
4.2 2-WAY SSL CERTIFICATES ..... 30
**5. SECURITY AND INTEGRITY** ..... 31
**6. ENVIRONMENT INFORMATION** ..... 31
**7. PROCESSING TIME SPECIFICATIONS** ..... 32
**8. SPECIAL PROCESSING** ..... 32
**9. RECEIPT REFERRAL CODES** ..... 32
**10. SAMPLE FAULT MESSAGES** ..... 33
**11. OPEN ITEM DISCUSSIONS** ..... 35

# Table of Figures and Tables

Figure 1. APC Service High-Level Technical Architecture ..... 3
Figure 2. APC Service Message Dialogue ..... 5
Figure 3. APC Service Message Domain Model, Part I ..... 8
Figure 4. APC Service Message Domain Model, Part II ..... 8
Figure 5. FlightListRequest SOAP Message Example ..... 12
Figure 6. TravelerValidateRequest SOAP Message Example ..... 18
Figure 7. TravelerEndRequest SOAP Message Example ..... 21
Figure 8. SystemStatusRequest SOAP Message Example ..... 22
Figure 9. FlightListResponse SOAP Message Example ..... 23
Figure 10. TravelerValidateResponse SOAP Message Example ..... 26
Figure 11. TravelerEndResponse SOAP Message Example ..... 27
Figure 12. SystemStatusResponse SOAP Message Example ..... 28
Figure 13. SOAP Fault Message Example ..... 29
Figure 14. Two-Way SSL Authentication ..... 30

Table 1. Document References ..... 2
Table 2. Common Data Type Definitions ..... 11
Table 3. FlightListRequest ..... 12
Table 4. TravelerValidateRequest Element ..... 12
Table 5. Manual Entry Element ..... 13
Table 6. DeclarationQuestion Element ..... 15
Table 7. FingerprintCapture Element ..... 15
Table 8. PhotoImageCapture Element ..... 16
Table 9. SoftwareDetail Element ..... 16
Table 10. FingerprintSegment Element ..... 17
Table 11. FingerprintSegmentDetail Element ..... 17
Table 12. DeclarationQuestionNumber Enumeration Element ..... 17
Table 13. ClassOfAdmissionCode Values Accepted (Not an Enumeration Element) ..... 18
Table 14. TravelerEndRequest Element ..... 21
Table 15. SystemStatusRequest Element ..... 22
Table 16. FlightListResponse Element ..... 22
Table 17. FlightListRecord Element ..... 23
Table 18. TravelerValidateResponse Element ..... 25
Table 19. ApisResponse Element ..... 25
Table 20. Address Element ..... 26
Table 21. TravelerEndResponse Element ..... 27
Table 22. SystemStatusResponse Element ..... 28
Table 23. Fault Element ..... 29
Table 24. APC Service Message Time Specification ..... 32
Table 25. APC Service Receipt Referral Codes ..... 33
Table 26. Sample APC Service Fault Messages ..... 33
Table 27. APC Service Open Discussion Items ..... 35

# Automated Passport Control Service / Kiosk System

# Interface Control Document

## 1. Introduction

### 1.1 Purpose

The purpose of this document is to provide the interface specifications between the Kiosk System and the U.S. Customs and Border Protection (CBP) Automated Passport Control (APC) Service. This document provides a high-level overview of the technical architecture, describes the message request and response dialogues, outlines message components, and provides data validation rules. For purposes of this document the term "Kiosk" includes authorized entry devices which may be devices physically installed at ports or mobile devices using an approved application. The term "Kiosk System" is used to refer to the third party system interfacing with the APC Service.

### 1.2 System Overview

APC is a service for ports wanting to utilize third party self-service kiosks and other entry devices to support CBP primary processing of international travelers. The APC Service will perform initial traveler vetting and manifest lookups for the third party kiosk system. The APC Service is designed to support the following types of travelers entering the US at international Airports and Seaports:

- United States Citizens presenting a US Passport
- Canadian Citizens presenting a Canadian passport and entering under B1 or B2 Class of Admission
- Citizens of Visa Waiver Countries presenting a Passport from their Country of citizenship, entering under WB and WT Class of Admission, who are enrolled in the Electronic System for Travel Authorization (ESTA).
- United States Lawful Permanent Residents (US LPR) presenting a C1 or C2 document.

The APC Service is an internet facing web service that the Kiosk System will utilize to allow a traveler or traveler group to complete an expedited inspection.

Visa Wavier Travelers and Non-Canadian LPRs within the ages of 14 and 79 who use the APC service will be subject to biometric verification.

### 1.3 Background

CBP is one of the Department of Homeland Security's largest components. CBP is responsible for protecting the United States' front line, while facilitating legitimate trade and travel. CBP is continuously working to improve the entry process for the traveler and realize the goal of increased security while expediting the flow of legitimate travel. The goal of the self-service

kiosk in a CBP environment is to allow a traveler or family unit to complete a portion of an inspection prior to speaking with a CBP Officer.

The intent of the kiosk system is to collect traveler information and transfer that information to CBP for law enforcement and border inspection purposes. A self-service kiosk option has been added to the Airport Technical Design Standard (ATDS), allowing Port Authorities the option to use kiosks to facilitate data collection. CBP/OIT worked to develop a technology requirements package to provide to interested port authorities. Under the ATDS, Port Authorities can opt to incorporate kiosks as equipment in their respective Federal Inspection Services (FIS) areas. Stationary kiosk equipment and supporting servers are provided by, maintained, and owned by the Port Authority. Any kiosk procured and installed by a Port Authority must comply with Automated Passport Control Services technology requirements and meet CBP Business requirements. Similarly, any kiosk application operating on a mobile device must comply with Automated Passport Control Services technology requirements and meet CBP Business requirements.

## 1.4 Contact Information

Questions and comments related to this ICD should be sent to the APC OIT Group (APCOITGroup@cbp.dhs.gov).

## 1.5 Document References

The following documents were used as references for this APC Service / Kiosk System ICD:

**Table 1. Document References**

| User Reference Document Name | Document Identification Number | Location |
|---|---|---|
| 2012-2016 Border Patrol Strategic Plan | 2012-2016 Border Patrol Strategic Plan | http://www.cbp.gov/sites/default/files/documents/bp_strategic_plan.pdf |
| DHS Sensitive Systems Policy Directive 4300A Version 8, March 14, 2011 | DHS National Security Systems Policy Directive 4300A | http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf |
| National Institute of Standards and Technology Special Publication 800-64, Revision 2, Security Considerations in the Information System Development Life Cycle, October 2008 | NIST 800-64 Rev. 1 | http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf |

The following APC documentation is relevant to this ICD:

- Automated Passport Control Service / Kiosk System Onboarding Guide
- Business Requirements (BRD)
- Technical Reference Manual (TRM)
- Interface Control Document (ICD), including the Environmental Supplement and APC Service's WSDL and XML schemas
- Automated Passport Control Integration Test Plan

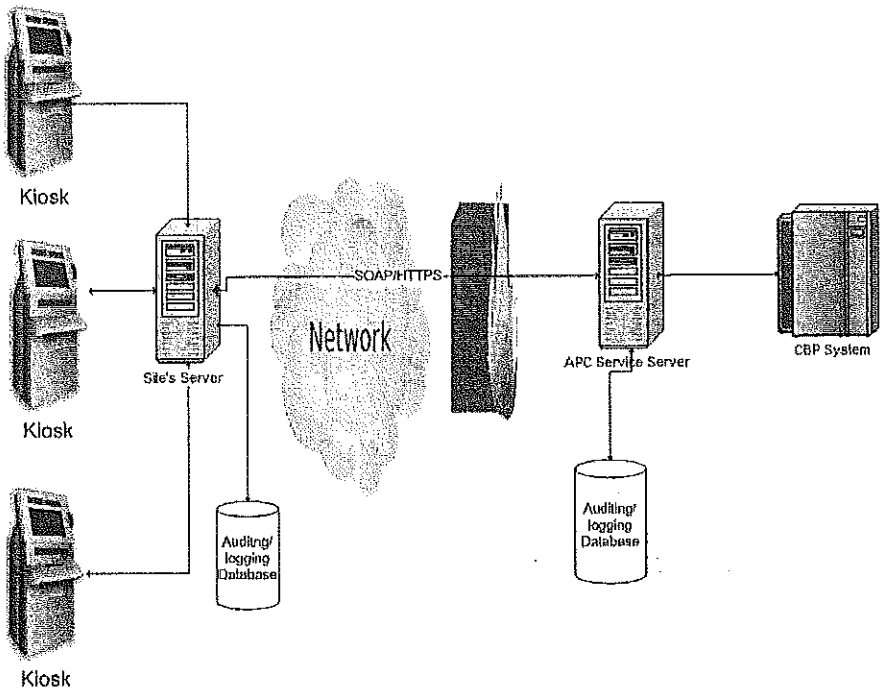
- APC Frequently Asked Questions (FAQ)

# 2. System Description

## 2.1 System Architecture

Figure 1 illustrates the recommended high-level system components and interfaces used in the APC Service. The principle components are the Kiosk System and the APC Service. The Kiosk System requests information from the APC Service while the APC Service interacts with various CBP systems to obtain a response relevant to the Kiosk System's request

**Figure 1. APC Service High-Level Technical Architecture**




Each port will utilize a single SSL Certificate to communicate with the CBP production site. A separate SSL certificate will be required for communication between the port non-production environment and CBP's non-production (test) environment. The one non-production certificate will be used for communication with both the CBP System Acceptance Test (SAT) and the CBP Quality Assurance (QAX) environments.

## 2.2 Kiosk System

The Kiosk System is a self-service entry point used by Port Authorities to collect traveler information and transfer that information to CBP for law enforcement purposes. The Kiosk System is: (1) a piece of equipment in the form of a kiosk or other CBP approved device that allows a traveler to input data and (2) a server(s) that allows the kiosk to interface with CBP's APC Service for traveler processing. The Kiosk System is neither managed nor implemented by

CBP; third-party vendors are responsible for its system implementation. While it interfaces with the APC Service to request traveler processing data, the Kiosk System is isolated from CBP's internal networks and systems.

The following functions will be performed by the Kiosk System:

- Request and receive flight list information from the APC Service
- Meet the business, technical, and operational requirements
- Display information and instructions to the traveler(s)
- Collect the necessary travel information from each traveler
- Collect biometrics from traveler(s), if relevant
- Prepare and send the Traveler Validate Request(s)
- Process vetting results from the Traveler Validate Response message
- Request and receive the Traveler End message
- Prepare and print receipts for traveler as specified
- Record and document session information
- Request and receive the APC Service system status message
- Process APC generated Fault messages

## 2.3 APC Service

The APC Service is a web service that implements the high level requirements described in this section. The APC Service is the primary interface to CBP for the Kiosk System. The APC Service and the Kiosk System support the overall goal of the Automated Passport Control program.

The following functions are performed by the APC Service

- Read and validate the Flight List Request
- Prepare and send the Flight List Response
- Read and validate the Traveler Validate Request(s)
- Calculate the referral code according to the business rules for each traveler
- Prepare and send the Traveler Validate Response message
- Read and validate the Traveler End Request from the Kiosk System
- Prepare and send Traveler End Response(s)
- Prepare and send the Border Crossing record notifications to the appropriate CBP subsystems
- Read and validate the System Status Request
- Prepare and send System Status Response
- Prepare and send Fault response when required.

The APC Service is hosted in the CBP National Data Center (NDC) and supported by the CBP Office of Information Technology (OIT) network and operations center. This center monitors

and supports the network and servers to provide connectivity and system monitoring between the port and NDC.

## 2.4 APC Web Service Dialogues

The APC Service provides four web service dialogues that allow the Kiosk System to request information from the APC Service. In each of the four dialogues, the Kiosk System initiates the message request and the APC Service provides a message response. The web services operations are:

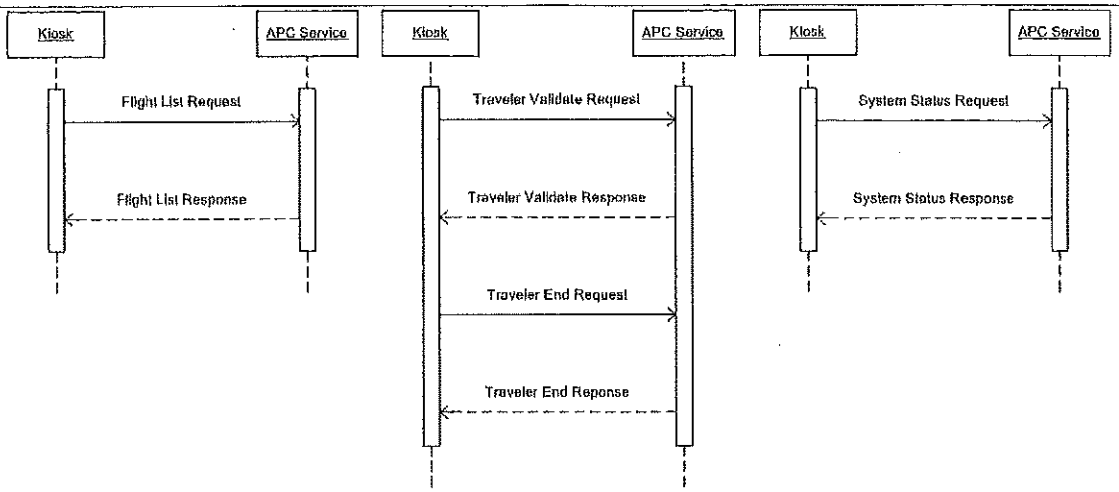
- Flight List
- Traveler Validate
- Traveler End
- System Status

The System Status request allows the client to obtain the current state of the APC Service. Upon receiving the request, the APC Service sends a response indicating whether or not it is available for processing. The Flight List request signals the APC Service to obtain flight information from CBP's internal subsystems. Afterwards, the APC Service will format and send the appropriate flight manifest in the response message.

Traveler Validate and Traveler End dialogues are used in sequence as part of an interactive workflow that processes a traveler. The Traveler Validate is sent from the kiosk to initiate vetting processing of a traveler for a border crossing; the APC service returns a response with the initial vetting results. The kiosk, in-turn, sends a **TravelerEndRequest** to the APC Service notifying the service to complete traveler processing. Upon completion of processing the APC service returns a **TravelerEndResponse** to the kiosk which serves as authorization for the kiosk to print the traveler receipt. For integrity of operations, with the exception of a System Failure (SF) referral code, the APC Service interface requires that the kiosk receive a valid **TravelerEndResponse** message from APC Services prior to printing/displaying the traveler receipt. The Kiosk may print a System Failure (SF code) receipt in events where faults are received from the APC Service or in events where the vendor provided APC system fails to transmit the final dialog message to the APC Service.

Figure 2 illustrates the message dialogue between the Kiosk System and the APC Service.

**Figure 2. APC Service Message Dialogue**




## 2.5 Key Processing Fields

Processing fields critical to the APC Service include the following:

**Kiosk Identifiers**—The KioskID must be unique system wide. The kioskID must identify the traveler's physical position to the port and terminal within the port (when there is more than one international terminal). CBP will assign KioskIDs upon receipt of a request from the Port Authority.

The current kiosk format is pppmcctnnn where

- ppp is the Port Code,
- m is the mode of transportation (A=Air, S=Sea)
- cc is a constant (currently "PC" for Kiosks, MC for Mobile),
- t is the terminal identifier;
- nnn is the unique kiosk number within the port and terminal. (e.g.AIR: AUSAPC1001, YYZAPC3010; SEA: FLLSPC1001).

The KioskID shall adhere to the ISO/IEC 8859-1 character set [A-Z][0-9].

**Session Identifier** -- The Session Identifier, generated by the kiosk/kiosk application must be distinct and unique system wide. The SessionID must adhere to the ISO/IEC 8859-1 character set [A-Z][0-9]. CBP suggests the following approach:

- kkkkkkkkkkyyyyMMDDHHmmssSSS

Where kkkkkkkkkk is the kioskID and yyyyMMDDHHmmssSSS is the date/time group to milliseconds.

Non-stationary kiosks which serve multiple concurrent sessions may need to incorporate a suffix to ensure uniqueness of the session identifier.

**Traveler Identifier** -- The TravelerID, assigned by the Kiosk/kiosk application, must be distinct and unique within a session. The TravelerID must adhere to the ISO/IEC 8859-1

character set [A-Z][0-9]. The combination of SessionID + KioskID + TravelerID must be unique.

**Airport and Seaport Codes** are based on the three character IATA definitions.

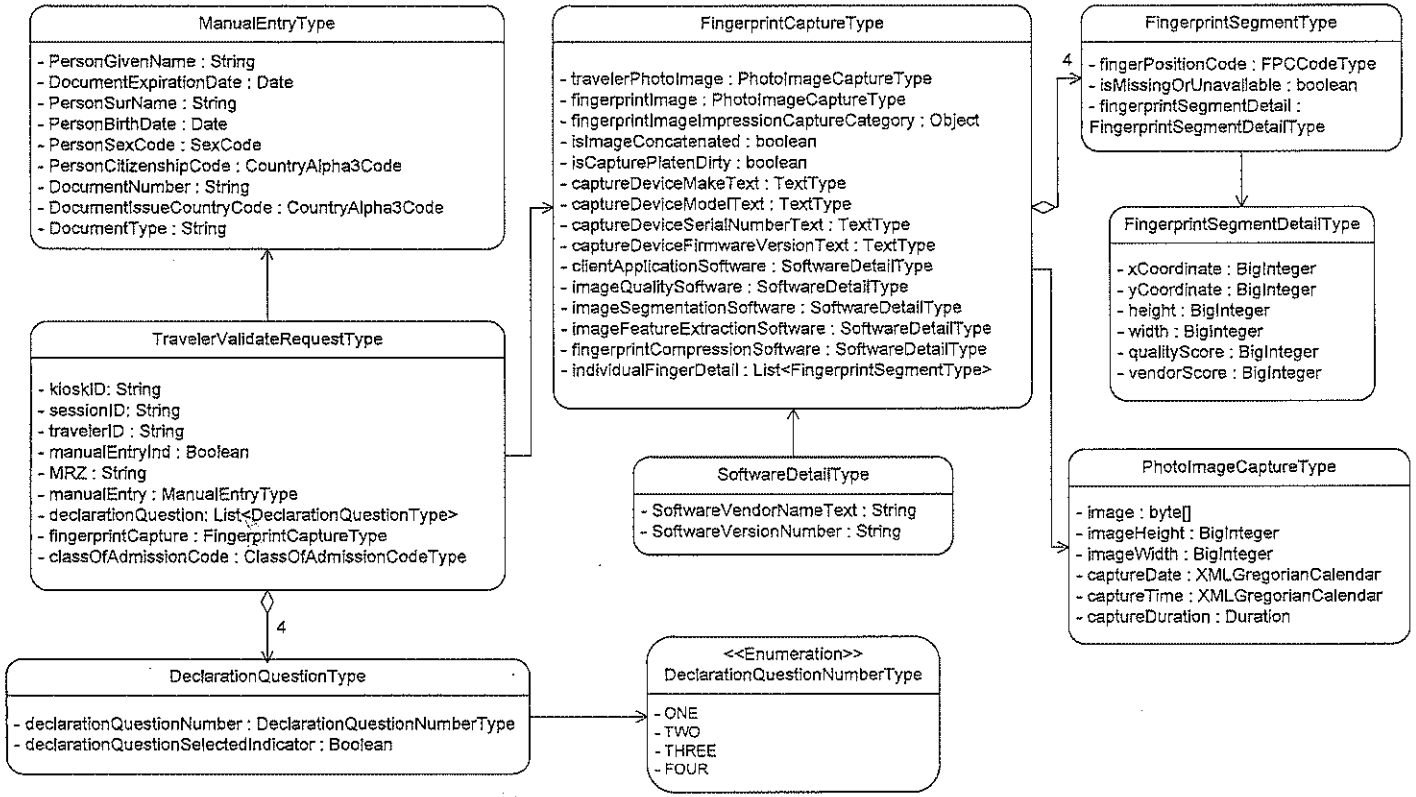
**Carrier codes and flight numbers** are based on International Civil Aviation Organization (ICAO) definitions and will be based on what the carriers transmit in the manifests. This information is sent to the CBP's Advance Passenger Information System (APIS). The Vessel Code is based on the International Maritime Organization (IMO) Ship Identification Number (IMO Number).

**Country Codes and Country Names** are based on the ISO 3166-1 3-character standard.

## 2.6 APC Service Message Domain Models

The APC Domain Model, Part 1 is presented in Figure 3; Part 2 is presented in Figure 4.

**Figure 3. APC Service Message Domain Model, Part I**



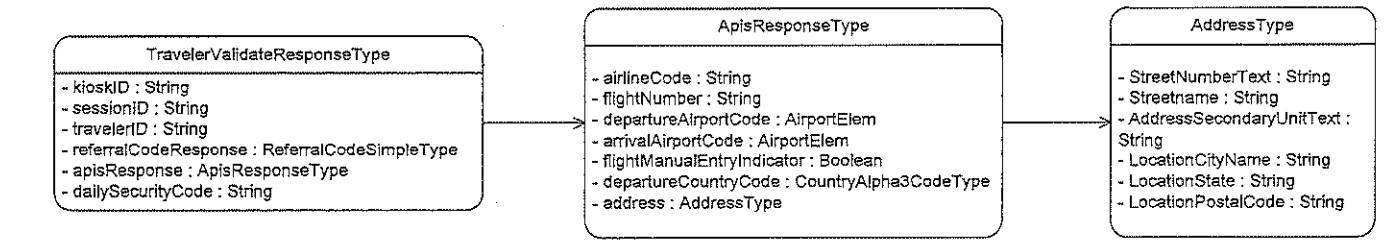
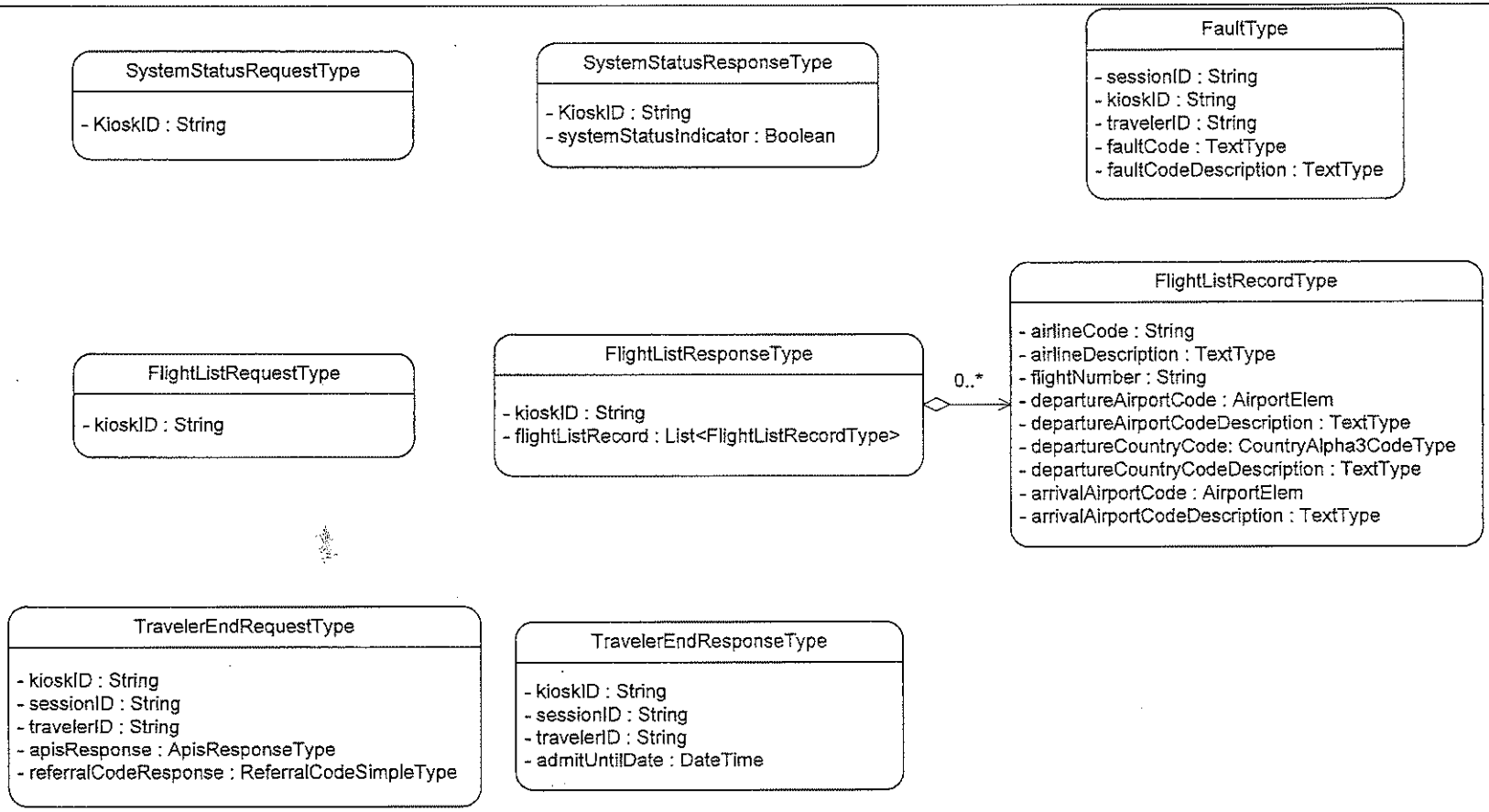




**Figure 4. APC Service Message Domain Model, Part II**

175


SystemStatusRequestType
- KioskID : String
SystemStatusResponseType
- KioskID : String
- systemStatusIndicator : Boolean
FaultType
- sessionID : String
- kioskID : String
- travelerID : String
- faultCode : TextType
- faultCodeDescription : TextType
FlightListRequestType
- kioskID : String
FlightListResponseType
- kioskID : String
- flightListRecord : List<FlightListRecordType>
0..*
FlightListRecordType
- airlineCode : String
- airlineDescription : TextType
- flightNumber : String
- departureAirportCode : AirportElem
- departureAirportCodeDescription : TextType
- departureCountryCode: CountryAlpha3CodeType
- departureCountryCodeDescription : TextType
- arrivalAirportCode : AirportElem
- arrivalAirportCodeDescription : TextType
TravelerEndRequestType
- kioskID : String
- sessionID : String
- travelerID : String
- apisResponse : ApisResponseType
- referralCodeResponse : ReferralCodeSimpleType
TravelerEndResponseType
- kioskID : String
- sessionID : String
- travelerID : String
- admitUntilDate : DateTime

176

# 3. Message Exchange Specifications

## 3.1 WSDL and XML Schemas

**The APC WSDL provides definitive guidelines for message exchange between the kiosk application and the APC Service. The APC Service's WSDL is available for use in application development. In the event of a discrepancy between the WSDL and this ICD, the WSDL takes precedence.**

All character data submitted must adhere to the ISO/IEC 8859-1 (Part 1, Latin-1 Western European) character set; restrictions are specified where applicable. Separate specifications are given within the body of this document for image data.

The APC Service transactions are a simple request/response data exchange via SOAP web services. There is a 1:1 ratio between a request and a response and errors are managed via SOAP web services fault handling. NIEM is used to implement the XML data structures for the APC Service.

Subsequent sections of this ICD define the elements of message calls between the Kiosk System and the APC Service and specify APC processing criteria and constraints. Kiosk developers should leverage Web Service tools from JAX-WS, WCF or the platform of their choice to generate source that will create and validate messages for the APC Services. Other interactive tools that can validate messages against the schema like SoapUI can be useful for testing the interface during development.

It is expected that the Kiosk System will perform XML validation on an XML message before sending the data to the APC Service to confirm that the XML message is well-formed and valid.

The URLs for accessing the APC WSDL and XML schemas are documented in the Environmental Supplement to this ICD. This supplement is available to approved vendors upon request to the APC OIT Group (APCOITGroup@cbp.dhs.gov).

## 3.2 National Information Exchange Model (NEIM)

The National Information Exchange Model (NIEM) is used to implement the XML data structures for the APC Service. The use of NIEM is DHS mandated and it provides the basic data types for XML validation.

Information on NIEM can be found at http://www.niem.gov/.

## 3.3 Message Exchange

Message Exchange between the Kiosk System and the APC Service will consist of requests and responses to invoke the APC Service functions.

Specifications for Request messages are presented in Section 3.4 of this document; specifications for Response messages are presented in Section 3.5. The Sample messages that are provided in these subsections are presented as **examples only**.

Each message element is defined in terms of the following characteristics:

**Element** – The name of the element.
**Data Type** – The type of data that defines the element.

**Size** – The maximum size of the data type. An asterisk "*" denotes there is no limit on the size (i.e., unbounded). A format of "x | y" indicates the minimum and maximum size of an element that has a collection of values. A "--" indicates that the size is not applicable; see the element's data type instead. In general, when a size is specified for a String type it is considered the maximum useful length. String fields that are longer than the specified data format may be truncated.

**Rqd** – Whether or not the element is required; "Y" for yes and "N" for no. Note, a required element does not mean that the element value is not nullable. Refer to the APC Service xml schemas for specific detail.

**Description** – The purpose of the element.

Data types that are commonly referenced in the schema elements are described in Table 2.

**Table 2. Common Data Type Definitions**

| Data Type | Format or Allowed Values | Description |
|---|---|---|
| Boolean | Allowed Values:<br>`true`<br>`false` | A binary indicator denoting either true or false. Values conform to the NIEM `niem-xsd:boolean` format. |
| CountryAlpha3Code | Allowed Values:<br>*See ISO 3166 alpha-3 country codes.* | The three letter identification of a country as defined by ISO 3166 alpha-3. |
| Date | Format:<br>`YYYY-MM-DD` | A date value that conforms to the NIEM `niem-xsd:date` format. |
| DateTime | Format:<br>`YYYY-MM-DDThh:mm:ssTZD` | A date and time value that conforms to the NIEM `niem-xsd:dateTime` format. |
| SexCode | Allowed Values:<br>`F`<br>`M`<br>`U` | A code value that identifies the gender of a person. "F" indicates female, "M" indicates male and "U" indicates unknown/unidentified. |
| String | n/a | A value consisting of a series of alphanumeric characters that is encoded in UTF-8 format. Strings can be of unlimited length unless where noted. The type conforms to the NIEM `niem-xsd:string` format with the following modifications:<br>• Lowercase alphabetical data will be converted to uppercase letters in the response message.<br>• Spaces will remain as spaces.<br>• Non-alphabetical and non-numeric characters will be converted to spaces when used for searching. |

## 3.4 Request Messages

Each of the following request messages may be sent by the Kiosk:

- Flight List Request
- Traveler Validate Request
- Traveler End Request
- System Status Request

Reference for the corresponding response element specification can be found in section 3.5

### 3.4.1 Flight List Request

The request for the flight list is initiated by the Kiosk System using the **FlightListRequest** message element. The suggested frequency for submission of this request is twice daily. The **FlightListRequest** is applicable only to airport kiosks and does not apply to sea and mobile processing.

The elements that comprise the message request are displayed in Table 3 Figure 5 shows an example **FlightListRequest** SOAP message.

**Table 3. FlightListRequest**

| FlightListRequest | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| KioskID | String | 10 | Y | A system wide unique identifier for the kiosk. |

**Figure 5. FlightListRequest SOAP Message Example**

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope                    xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:ns="http://cbp.dhs.gov/globalentry/kioskservice/extension/2.0"
xmlns:ns1="http://niem.gov/niem/structures/2.0">
   <soap:Header/>
   <soap:Body>
      <ns:FlightListRequest>
         <ns:Airport_Elem>JFK</ns:Airport_Elem>
         <ns:KioskID>JFKAPC101</ns:KioskID>
         <ns:RequestDate>2014-01-28T12:30:17-07:00</ns:RequestDate>
      </ns:FlightListRequest>
   </soap:Body>
</soap:Envelope>
```

### 3.4.2 Traveler Validate Request

The request for validation of the traveler data is initiated by the Kiosk System using the **TravelerValidateRequest** message element. The elements that comprise the message request are displayed in Table 4 through **Table 13**. Figure 6 shows an example of the **TravelerValidateRequest** SOAP message.

**Table 4. TravelerValidateRequest Element**

| TravelerValidateRequest | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| KioskID | String | 10 | Y | A system wide unique identifier for the kiosk. Must adhere to the ISO/IEC 8859-1 character set [A-Z][0-9]; special characters are not allowed. Assigned by the APC OIT Group |
| SessionID | String | 65 | Y | A value that uniquely identifies the session. Must adhere to the ISO/IEC 8859-1 character set [A-Z][0-9]; special characters are not allowed. |
| TravelerID | String | 10 | Y | The unique identification value associated with the traveler for the session. Must adhere to the ISO/IEC 8859-1 character set [A-Z][0-9]; special characters are not allowed. |
| ManualEntryInd | Boolean | | Y | If set to false then the traveler document data was scanned and the MRZ is required.<br>If set to true then the traveler document data was entered manually and the following elements are used to identify the traveler: PersonGivenName, DocumentExpirationDate, PersonSurName, PersonBirthDate, PersonSexCode, PersonCitizenshipCode, DocumentNumber, DocumentIssueCountryCode, and DocumentType.<br>Data must be entered exactly as it appears in the MRZ. |
| MRZ | String | 100 | C | Data read from the MRZ. Required when ManualEntryInd=False |
| ManualEntry | ManualEntryType | | C | Manual Entry of PassengerData. Required when ManualEntryInd=TRUE |
| DeclarationQuestion | DeclarationQuestion Type | -- | Y | The declaration questions that are asked of the traveler. Occurs four times, one for each declaration question. |
| FingerprintCapture | FingerprintCaptureType | -- | C | The biometric capture of the traveler.<br>Required for Visa Wavier travelers and non-Canadian LPRs who are between 14 and 79 (< 80). Biometric data should not be collected or transmitted for U.S and Canadian Citizens including Canadian US LPRs, or for any traveler under 14 or over 79 years of age. |
| ClassOfAdmissionCode | ClassOfAdmissionCodeType | - | C | The code that indicates that type of travel being conducted by the traveler in the country. Required for all foreign nationals including Canadians. Not Applicable to US citizens and US LPRs. |

**Table 5. Manual Entry Element**

Data Submitted in the Manual Entry Element must adhere to the ISO/IEC 8859-1 character set [A-Z][0-9] $!;#% and space. Fields must be entered as they appear in the MRZ.

| ManualEntry | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| PersonGivenName | String | 50 | Y | The first name and middle names of the traveler as they appear in the MRZ of the travel document |
| DocumentExpiration Date | Date | -- | Y | The expiration date of the document provided by the traveler. |
| PersonSurName | String | 50 | Y | The last name (surname) of the traveler as it appears in the MRZ of the travel document. |
| PersonBirthDate | Date | -- | Y | The birth date of the traveler. |
| PersonSexCode | SexCode | -- | Y | The gender of the traveler. |
| PersonCitizenshipCode | CountryAlpha3Code | 3 | Y | The code of the country where the traveler has citizenship. |
| DocumentNumber | String | 16 | Y | The number assigned to the document from the document's issuing office. |
| DocumentIssueCountryCode | CountryAlpha3Code | -- | Y | The code of the country that issued the document of the traveler. |
| DocumentType | String | 2 | Y | The type of document. Must be valued P, C1 or C2. |

**Table 6. DeclarationQuestion Element**

This element must be provided for each Declaration Question; a total of four occurrences.

| DeclarationQuestion | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| DeclarationQuestionNumber | DeclarationQuestionNumberType | -- | Y | A code that identifies the declaration question. |
| DeclarationQuestionSelectedIndicator | Boolean | -- | Y | The true or false value that was provided by the traveler in response to the associated question. |

**Table 7. FingerprintCapture Element**

**This element is required for all Visa Waiver Travelers between the ages of 14 and 79 (<80) and for US LPRs between the ages of 14 and 79 (<80) who are not Canadian Citizens. This element should not be submitted for US and Canadian Citizens (including Canadian Citizens traveling as US LPRs) or any Visa Waiver or US LPR traveler under the age of 14 or over 79.**

**Travelers requiring biometric verification must be preregistered in the IDENT system. The APC Schema provides for a four finger slap, thumb excluded.**

| FingerprintCapture | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| TravelerPhotoImage | PhotoImageCaptureType | * | Y | A face photo image of the traveler. .The image must not exceed 192KB; jpeg format is recommended. |
| FingerprintImage | PhotoImageCaptureType | * | Y | The fingerprint capture of the traveler.<br>Four finger fingerprints shall have a class resolution at least 19.69 ppmm (500 ppi) and shall be processed in.wsq (Wavelet Scalar Quantization) format. The image must not exceed 500 KB. |
| IsImageConcatenated | Boolean | -- | Y | A true value indicates that the fingerprint image is concatenated and false indicates that it is not. |
| IsCapturePlatenDirty | Boolean | -- | Y | A true value indicates that the fingerprint platen is dirty and false indicates that it is not. |
| CaptureDeviceMakeText | String | 25 | Y | The manufacturer of the fingerprint scanner. e.g. - "Cross Match" |
| CaptureDeviceModelText | String | 25 | Y | The model of the fingerprint scanner.<br>e.g. - "GuardianV900251RevA" |
| CaptureDeviceSerialNumberText | String | 50 | Y | The serial number of the fingerprint scanner.<br>e.g. – "000550782.B2007" |
| CaptureDeviceFirmwareVersionText | String | 50 | Y | The firmware version of the fingerprint scanner.<br>e.g. – "V95.35 LSCAN 500C (c) CMT" |

| FingerprintCapture | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| ClientApplicationSoftware | SoftwareDetailType | -- | Y | The name and version of the client application software.<br>e.g. –<br>"APC" (software vendor name)<br>"2.0" (software vendor version) |
| ImageQualitySoftware | SoftwareDetailType | -- | Y | The name and version of the fingerprint quality scoring software used during the capture.<br>e.g. –<br>"Cogent" (software vendor name)<br>"10.7.2" (software vendor version) |
| ImageFeatureExtractionSoftware | SoftwareDetailType | -- | N | The name and version of the fingerprint image feature extraction software used during the capture. It is recommended this attribute be populated with no value. This element will be removed in a future release of the schema. |
| Fingerprint CompressionSoftware | Software DetailType | -- | Y | The name and version of the fingerprint image compression software used during the capture.<br>e.g. –<br>"Aware NFIQ" (software vendor name)<br>"10.9.8" (software vendor version) |
| IndividualFingerDetail | FingerprintSegmentType | -- | Y | The coordinates of the fingerprint segments in the slap image. |

**Table 8. PhotoImageCapture Element**

| PhotoImageCapture | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| Image | Base64 | -- | Y | The image that was captured; a base 64 encoded photo. |
| ImageHeight | Integer | -- | Y | The height of the image in pixels. |
| ImageWidth | Integer | -- | Y | The width of the image in pixels. |
| CaptureDate | DateTime | -- | Y | The capture date of the image. |
| CaptureTime | DateTime | -- | Y | The capture time of the image. |
| CaptureDuration | Duration | -- | Y | The capture duration of the image. The duration should be the period of time that the fingerprint screen is being displayed. |

**Table 9. SoftwareDetail Element**

| SoftwareDetail | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| SoftwareVendorNameText | String | 50 | Y | The name of the software vendor. |
| SoftwareVersionNumber | String | 50 | Y | The version number of the software. |

**Table 10. FingerprintSegment Element**

| FingerprintSegment | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| FingerPositionCode | Integer | -- | Y | A code that identifies the finger position.<br>The acceptable codes are:<br>2 – Right index finger<br>3 – Right middle finger<br>4 – Right ring finger<br>5 – Right little finger<br>7 – Left index finger<br>8 – Left index finger<br>9 – Left ring finger<br>10 – Left little finger |
| IsMissingOrUnavailable | Boolean | -- | Y | A value of true if the finger was unable to be captured or missing and false if the finger is available in the capture. |
| FingerprintSegmentDetail | FingerprintSegmentDetailType | -- | N | Provides detailed segment data of the finger identified in FingerPositionCode.<br>If IsMissingOrUnavailable is false then this element is required.<br>If the IsMissingOrUnavailable element value is true then this value is ignored. |

**Table 11. FingerprintSegmentDetail Element**

| FingerprintSegmentDetail | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| XCoordinate | Integer | -- | Y | The top left x-coordinate position of finger in the slap image. |
| YCoordinate | Integer | -- | Y | The top left y-coordinate position of finger in the slap image. |
| Height | Integer | -- | Y | The height, in pixels, of the finger in the slap image. |
| Width | Integer | -- | Y | The width, in pixels, of the finger in the slap image. |
| QualityScore | Integer | -- | Y | The NFIQ quality score for the finger. |
| VendorScore | Integer | -- | Y | The vendor quality score for the finger. |

**Table 12. DeclarationQuestionNumber Enumeration Element**

| DeclarationQuestionNumber | |
|---|---|
| **Value** | **Description** |
| ONE | The declaration question posed to the traveler that is identified as question "1". |
| TWO | The declaration question posed to the traveler that is identified as question "2". |

| DeclarationQuestionNumber | |
|---|---|
| **Value** | **Description** |
| THREE | The declaration question posed to the traveler that is identified as question "3". |
| FOUR | The declaration question posed to the traveler that is identified as question "4". |

**Table 13. ClassOfAdmissionCode Values Accepted (Not an Enumeration Element)**

| ClassOfAdmissionCode | |
|---|---|
| **Value** | **Description** |
| B1 | Canadian Citizen temporary visitor for business (including Peace Corps). |
| B2 | Canadian Citizen temporary visitor for pleasure. |
| WB | For business purposes under the Visa Waiver Program |
| WT | For pleasure purposes under the Visa Waiver Program |

**Figure 6. TravelerValidateRequest SOAP Message Example**

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <TravelerValidateRequest xmlns="http://cbp.dhs.gov/globalentry/kioskservice/extension/2.0">
      <KioskID>MCO4APC002</KioskID>
      <SessionID>20140117132857394l</SessionID>
      <TravelerID>1</TravelerID>
      <ManualEntryInd>false</ManualEntryInd>
    <MRZ>
<![CDATA[P<USACANGA<<MANGA<<<<<<<<<<<<<<<<<<<<<<<<1256082253USA6611075M1212318989890000000009 2
]]></MRZ>
      <DeclarationQuestion>
        <DeclarationQuestionNumber>ONE</DeclarationQuestionNumber>
        <DeclarationQuestionSelectedIndicator>false</DeclarationQuestionSelectedIndicator>
      </DeclarationQuestion>
      <DeclarationQuestion>
        <DeclarationQuestionNumber>TWO</DeclarationQuestionNumber>
        <DeclarationQuestionSelectedIndicator>false</DeclarationQuestionSelectedIndicator>
      </DeclarationQuestion>
      <DeclarationQuestion>
        <DeclarationQuestionNumber>THREE</DeclarationQuestionNumber>
        <DeclarationQuestionSelectedIndicator>false</DeclarationQuestionSelectedIndicator>
      </DeclarationQuestion>
      <DeclarationQuestion>
        <DeclarationQuestionNumber>FOUR</DeclarationQuestionNumber>
        <DeclarationQuestionSelectedIndicator>false</DeclarationQuestionSelectedIndicator>
      </DeclarationQuestion>
      <FingerprintCapture>
        <TravelerPhotoImage>
          <Image>  </Image>
          <ImageHeight>651</ImageHeight>
          <ImageWidth>488</ImageWidth>
          <CaptureDate>2014-01-17T13:29:33.9749783+00:00</CaptureDate>
          <CaptureTime>2014-01-17T13:29:33.9749783+00:00</CaptureTime>
          <CaptureDuration>PT20S</CaptureDuration>
        </TravelerPhotoImage>
        <FingerprintImage>
          <Image>  </Image>
          <ImageHeight>1500</ImageHeight>
```

```
          <ImageWidth>1600</ImageWidth>
          <CaptureDate>2014-01-17T13:29:22.8783436+00:00</CaptureDate>
          <CaptureTime>2014-01-17T13:29:22.8783436+00:00</CaptureTime>
          <CaptureDuration>PT20S</CaptureDuration>
        </FingerprintImage>
        <IsImageConcatenated>false</IsImageConcatenated>
        <IsCapturePlatenDirty>false</IsCapturePlatenDirty>
        <CaptureDeviceMakeText xmlns="http://niem.gov/niem/ansi-
nist/2.0">CROSSMATCH</CaptureDeviceMakeText>
        <CaptureDeviceModelText xmlns="http://niem.gov/niem/ansi-nist/2.0">Patrol
ID</CaptureDeviceModelText>
        <CaptureDeviceSerialNumberText xmlns="http://niem.gov/niem/ansi-
nist/2.0">002017661.B2012</CaptureDeviceSerialNumberText>
        <CaptureDeviceFirmwareVersionText
xmlns="http://niem.gov/niem/domains/screening/2.1">V117.41 L SCAN 500C
LT</CaptureDeviceFirmwareVersionText>
        <ClientApplicationSoftware xmlns="http://niem.gov/niem/domains/screening/2.1">
          <SoftwareVendorNameText>VISION-BOX, SA</SoftwareVendorNameText>
          <SoftwareVersionNumber>5.0</SoftwareVersionNumber>
        </ClientApplicationSoftware>
        <ImageQualitySoftware xmlns="http://niem.gov/niem/domains/screening/2.1">
          <SoftwareVendorNameText>VISION-BOX, SA</SoftwareVendorNameText>
          <SoftwareVersionNumber>8.0</SoftwareVersionNumber>
        </ImageQualitySoftware>
        <ImageFeatureExtractionSoftware xmlns="http://niem.gov/niem/domains/screening/2.1">
          <SoftwareVendorNameText>Cogent</SoftwareVendorNameText>
          <SoftwareVersionNumber>10.7.2</SoftwareVersionNumber>
        </ImageFeatureExtractionSoftware>
        <FingerprintCompressionSoftware xmlns="http://niem.gov/niem/domains/screening/2.1">
          <SoftwareVendorNameText>Cogent</SoftwareVendorNameText>
          <SoftwareVersionNumber>10.7.2</SoftwareVersionNumber>
        </FingerprintCompressionSoftware>
        <IndividualFingerDetail>
          <FingerPositionCode xmlns="http://niem.gov/niem/ansi-nist/2.0">2</FingerPositionCode>
          <IsMissingOrUnavailable>false</IsMissingOrUnavailable>
          <FingerprintSegmentDetail>
            <XCoordinate>117</XCoordinate>
            <YCoordinate>540</YCoordinate>
            <Height>420</Height>
            <Width>276</Width>
            <QualityScore>1</QualityScore>
            <VendorScore>1</VendorScore>
          </FingerprintSegmentDetail>
        </IndividualFingerDetail>
        <IndividualFingerDetail>
          <FingerPositionCode xmlns="http://niem.gov/niem/ansi-nist/2.0">3</FingerPositionCode>
          <IsMissingOrUnavailable>false</IsMissingOrUnavailable>
          <FingerprintSegmentDetail>
            <XCoordinate>510</XCoordinate>
            <YCoordinate>549</YCoordinate>
            <Height>401</Height>
            <Width>252</Width>
            <QualityScore>1</QualityScore>
            <VendorScore>1</VendorScore>
          </FingerprintSegmentDetail>
        </IndividualFingerDetail>
        <IndividualFingerDetail>
          <FingerPositionCode xmlns="http://niem.gov/niem/ansi-nist/2.0">4</FingerPositionCode>
          <IsMissingOrUnavailable>false</IsMissingOrUnavailable>
          <FingerprintSegmentDetail>
            <XCoordinate>879</XCoordinate>
            <YCoordinate>545</YCoordinate>
            <Height>409</Height>
            <Width>240</Width>
            <QualityScore>1</QualityScore>
            <VendorScore>1</VendorScore>
          </FingerprintSegmentDetail>
        </IndividualFingerDetail>
        <IndividualFingerDetail>
          <FingerPositionCode xmlns="http://niem.gov/niem/ansi-nist/2.0">5</FingerPositionCode>
          <IsMissingOrUnavailable>false</IsMissingOrUnavailable>
```

```
          <FingerprintSegmentDetail>
            <XCoordinate>1236</XCoordinate>
            <YCoordinate>553</YCoordinate>
            <Height>394</Height>
            <Width>244</Width>
            <QualityScore>1</QualityScore>
            <VendorScore>1</VendorScore>
          </FingerprintSegmentDetail>
        </IndividualFingerDetail>
      </FingerprintCapture>
      <ClassOfAdmissionCode>WB</ClassOfAdmissionCode>
    </TravelerValidateRequest>
  </s:Body>
</s:Envelope>
```

### 3.4.3 Traveler End Request

The request to complete Traveler processing is initiated by the Kiosk System using the **TravelerEndRequest** message element. Submission of the **TravelerEndRequest** message is critical to the integrity of the APC Service. This message provides APC with confirmation of the final traveler information. Upon receipt, the APC Service initiates completion of traveler processing including manifest confirmation, when appropriate, and recording information the CBP Officer requires for traveler action. With the exception of a System Failure (SF) referral, no referral should be printed at the Kiosk until the corresponding **TravelerEndResponse** message is received at the kiosk. The Kiosk may print a System Failure (SF) referral receipt in events where faults are received from the APC Service and in events where the vendor provided APC system fails to transmit the final **TravelerEndRequest** message to the APC Service.

The **TravelerEndRequest** message includes provisions for the kiosk to cancel a session for a traveler who previously received a PG referral; this is the only instance where kiosk cancellation is permitted. If the kiosk attempts to cancel a passenger who had not received a PG referral, the APC Service will return a fault in the **TravelerEndRequest.** Additionally, except to cancel a PG traveler, the APC Service will return a fault in the **TravelerEndRequest** if the kiosk returns a **ReferralResponseCode** that does not match the **ReferralCodeResponse** in the **TravelerValidateResponse.** The Kiosk notifies the APC Service to cancel a traveler who had received a preliminary PG referral by sending a TR Referral in the TravelerEndRequest. When the traveler is canceled, the original referral is invalidated and the Kiosk should print a CA (Cancel) Referral receipt for the Traveler.

APC waits up to 15 minutes from the time the **TravelerValidateRequest** message is sent to receive the **TravelerEndRequest** message from the kiosk. If the **TravelerEndRequest** message is not received within the 15 minute time window, the APC Service terminates the traveler session with no action; the traveler is locked-out. On subsequent retry, a traveler with any referral code other than PG will receive the same referral code on another attempt; a traveler who received a preliminary PG referral will receive a TR referral. If the APC Service receives a **TravelerEndRequest** following the termination due to timeout, the APC Service will return a fault transaction specifying session not found. A timeout will invalidate the original referral.

A TravelerEndRequest message should not be sent when the APC response to a TravelerValidiateRquest message is a fault. The fault message services as notification to terminate any further processing of the traveler. If APC receives a **TravelerEndRequest** message following transmission of a fault message, APC will respond with another fault stating the "No traveler request found in cache."

The elements that comprise the **TravelerEndRequest** message are displayed in **Table 14.**

**Table 14. TravelerEndRequest Element**

| TravelerEndRequest | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| KioskID | String | 10 | Y | A system wide unique identifier for the kiosk. |
| SessionID | String | 65 | Y | A value that uniquely identifies the session. |
| TravelerID | String | 10-- | Y | The unique identification value associated with the traveler for the session |
| ApisResponse | ApisResponseType | -- | M | Pre-arrival and departure manifest data as provided by APIS.<br>All fields except departure country code are mandatory in the ApisResponseElement for any traveler that specifies FlightManualEntryIndicator ='TRUE'. . Sea and mobile passengers are not provided an option for manual flight (vessel) add. |
| ReferralCodeResponse | String | 2 | N | The referral code assigned by the APC Service or a cancellation request for a traveler who previously received a PG.<br>Cancellation is only applicable to travelers who were assigned a PG. TR designates cancellation of the session for a traveler who had received a PG referral code. Except for cancel, return of a referral code different from that assigned by APC will generate a fault.<br>A cancellation will invalidate the original referral. |

**Figure 7. TravelerEndRequest SOAP Message Example**

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
  <s:Body xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <TravelerEndRequest xmlns="http://cbp.dhs.gov/globalentry/kioskservice/extension/2.0">
      <KioskID>MCO4APC002</KioskID>
      <SessionID>20140117132857394I</SessionID>
      <TravelerID>1</TravelerID>
      <ApisResponse>
        <FlightManualEntryIndicator>false</FlightManualEntryIndicator>
      </ApisResponse>
      <ReferralCodeResponse>PG</ReferralCodeResponse>
    </TravelerEndRequest>
  </s:Body>
</s:Envelope>
```

### 3.4.4 System Status Request

The request for the system status is initiated by the Kiosk System using the **SystemStatusRequest** message element. The purpose of the System Status Request is to determine the status of the system following a failure. As such, the System Status Request should only be transmitted when there is a concern that the system is not operating. The

elements that comprise the message request are displayed in **Table 15**. Figure 8 shows an example **SystemStatusRequest** SOAP message.

**Table 15. SystemStatusRequest Element**

| SystemStatusRequest | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| KioskID | String | 10 | Y | KioskID for the kiosk submitting the request. If other than a kiosk is submitting the request, a KioskID for the site should be provided |

**Figure 8. SystemStatusRequest SOAP Message Example**

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Body>
    <g:SystemStatusRequest xmlns:g="http://cbp.dhs.gov/globalentry/kioskservice/extension/2.0">
      <g:KioskID>kioskidxx</g:KioskID>
    </g:SystemStatusRequest>
  </env:Body>
</env:Envelope>
```

## 3.5 Response Messages

The APC Service will generate a response message to answer a request sent from the Kiosk System. Responses messages are:

- Flight List Response
- Traveler Validate Response
- Traveler End Response
- System Status Response
- Fault Element

In the following subsections, specifications are defined for each response message. Refer to Figure 2 for a depiction of the message dialogue between the Kiosk System and the APC Service. In addition, refer to Section 3.4 to review the corresponding request message specification.

### 3.5.1 Flight List Response

The response for a flight list request is provided by the APC Service using the **FlightListResponse** message element. The elements and child elements that comprise the message response are displayed in Table 16 and Table 17. Figure 9 shows an example SOAP message response for a flight list response. This response message is applicable only to Airport kiosk processing and is not applicable to sea and mobile processing.

**Table 16. FlightListResponse Element**

| FlightListResponse | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| KioskID | String | 10 | Y | A system wide unique identifier for the kiosk. |
| FlightListRecord | FlightListRecordType | 0 \| * | N | The requested 3 character airport code following the IATA definition. |

**Table 17. FlightListRecord Element**

| FlightListRecord | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| AirlineCode | String | 5 | Y | The code of the flight's airline. |
| AirlineDescription | String | 40 | Y | The name or description of the flight's airline. |
| FlightNumber | String | 20 | Y | The flight number. |
| DepartureAirportCode | String | 3 | Y | The IATA code of the airport from which the flight departs. |
| DepartureAirportCodeDescription | String | 40 | Y | The name of the airport from which the flight departs. |
| DepartureCountryCode | String | 3 | Y | The code of the country from which the flight departs. |
| DepartureCountryCodeDescription | String | 40 | Y | The name of the country from which the flight departs. |
| ArrivalAirportCode | String | 3 | Y | The IATA code of the airport in which the flight arrives. |
| ArrivalAirportCodeDescription | String | 40 | Y | The name of the airport in which the flight arrives. |

**Figure 9. FlightListResponse SOAP Message Example**

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Body>
    <ns0:FlightListResponse xmlns:ns2="http://niem.gov/niem/ansi-nist/2.0"
xmlns:ns1="http://niem.gov/niem/structures/2.0" xmlns:ns3="http://niem.gov/niem/niem-
core/2.0"

xmlns:ns0="http://cbp.dhs.gov/globalentry/kioskservice/extension/2.0"
xmlns:ns7="http://niem.gov/niem/domains/screening/2.1">
      <ns0:KioskID
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">JFKAPC101</ns0:
KioskID>
      <ns0:FlightListRecord>
        <ns0:AirlineCode
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:type="ns3:TextType">DL</ns0:AirlineCode>
        <ns0:AirlineDescription
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">DELTA AIR LINES
INC.</ns0:AirlineDescription>
```

```
        <ns0:FlightNumber
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">822</ns0:Flight
Number>
        <ns0:DepartureAirportCode>YVR</ns0:DepartureAirportCode>
        <ns0:DepartureAirportCodeDescription
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">VANCOUVER
INTL</ns0:DepartureAirportCodeDescription>
        <ns0:DepartureCountryCode>CAN</ns0:DepartureCountryCode>
        <ns0:DepartureCountryCodeDescription
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">CANADA</ns0:Dep
artureCountryCodeDescription>
        <ns0:ArrivalAirportCode>JFK</ns0:ArrivalAirportCode>
        <ns0:ArrivalAirportCodeDescription
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">JOHN F KENNEDY
INTL</ns0:ArrivalAirportCodeDescription>
      </ns0:FlightListRecord>
      <ns0:FlightListRecord>
        <ns0:AirlineCode
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:type="ns3:TextType">DL</ns0:AirlineCode>
        <ns0:AirlineDescription
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">DELTA AIR LINES
INC.</ns0:AirlineDescription>
        <ns0:FlightNumber
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">745</ns0:Flight
Number>
        <ns0:DepartureAirportCode>YVR</ns0:DepartureAirportCode>
        <ns0:DepartureAirportCodeDescription
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">VANCOUVER
INTL</ns0:DepartureAirportCodeDescription>
        <ns0:DepartureCountryCode>CAN</ns0:DepartureCountryCode>
        <ns0:DepartureCountryCodeDescription
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">CANADA</ns0:Dep
artureCountryCodeDescription>
        <ns0:ArrivalAirportCode>JFK</ns0:ArrivalAirportCode>
        <ns0:ArrivalAirportCodeDescription
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">JOHN F KENNEDY
INTL</ns0:ArrivalAirportCodeDescription>
      </ns0:FlightListRecord>
    </ns0:FlightListResponse>
  </soap:Body>
</soap:Envelope>
```

### 3.5.2 Traveler Validate Response

The response to a **TravelerValidateRequest** is provided by the APC Service using the **TravelerValidateResponse** message element. The **TravelerValidateResponse** message acknowledges receipt of the **TravelerValidateRequest** message and provides to the kiosk a traveler referral code based on initial traveler vetting, subject to final processing. For all referral codes other than a PG, the kiosk should not offer the traveler the option of selecting additional flight information. Receipt of the **TravelerValidateResponse** is not the basis for printing a receipt. The kiosk must receive the **TravelerEndResponse** prior to printing a receipt.

The elements and child elements that comprise the message response are displayed in the tables that follow.

**Table 18. TravelerValidateResponse Element**

| TravelerValidateResponse | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| KioskID | String | 10 | Y | The value submitted in the request message that uniquely identifies the servicing kiosk. |
| SessionID | String | 65 | Y | The value submitted in the request message that uniquely identifies the session. |
| TravelerID | String | 10 | Y | The value submitted in the request message that uniquely identifies the traveler for the session |
| ReferralCodeResponse | String | 2 | N | A code that indicates if the traveler is granted passage or if the traveler is referred for additional enforcement processing. |
| ApisResponse | ApisResponseType | -- | Y | Pre-arrival and departure manifest data provided by APIS. |
| DailySecurityCode | String | 15 | Y | A code generated daily to confirm authenticity. |

**Table 19. ApisResponse Element**

| ApisResponse | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| AirlineCode | String | 8 | C | The code that identifies the airline of the flight or "AV" for Sea. Mandatory when FlightManualEntryIndicator='TRUE'. |
| FlightNumber | String | 20 | C | The flight number or Vessel IMO number. Mandatory when FlightManualEntryIndicator='TRUE'. |
| DepartureAirportCode | String | 3 | C | The IATA code of the port from which the flight/vessel departs. Mandatory when FlightManualEntryIndicator='TRUE'. |
| ArrivalAirportCode | String | 3 | C | The IATA code of the port in which the flight/vessel arrives. Mandatory when FlightManualEntryIndicator='TRUE'. |
| FlightManualEntryIndicator | Boolean | -- | Y | Specifies whether or not the flight information was entered manually. When the Kiosk sends FlightManualEntryIndicator='TRUE', the flight data should be different from the APIS response and the required flight elements must be populated with valid data.. When flight data does not change, the kiosk should send FlightManualEntryIndicator='FALSE'.<br>The APC system always sets this indicator false in the TravelerValidateResponse message. |
| DepartureCountryCode | CountryAlpha3Code | 3 | N | The code of the country from which the flight/vessel departs. |

| ApisResponse | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| Address | AddressType | | N | The address on the manifest |

**Table 20. Address Element**

| Address | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| StreetNumberText | String | 8 | N | Street Number |
| StreetName | String | 60 | N | Street Name |
| AddressSecondaryUnitText | String | 35 | N | Apartment or Unit Number |
| LocationCityName | String | 70 | N | City Name |
| LocationState | String | 10 | N | U.S. State Name |
| Location PostalCode | String | 10 | N | U.S. Postal Code |

**Figure 10. TravelerValidateResponse SOAP Message Example**

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns0:TravelerValidateResponse xmlns:ns2="http://niem.gov/niem/domains/screening/2.1"
xmlns:ns1="http://niem.gov/niem/structures/2.0" xmlns:ns3="http://niem.gov/niem/niem-core/2.0"
xmlns:ns0="http://cbp.dhs.gov/globalentry/kioskservice/extension/2.0"
xmlns:ns5="http://niem.gov/niem/ansi-nist/2.0">
      <ns0:KioskID
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">MCO4APC002</ns0:KioskID>
      <ns0:SessionID
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">20140117132857 3941</ns0:Se
ssionID>
      <ns0:TravelerID
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">1</ns0:TravelerID>
      <ns0:ReferralCodeResponse>PG</ns0:ReferralCodeResponse>
      <ns0:ApisResponse>
        <ns0:AirlineCode
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">BA</ns0:AirlineCode>
        <ns0:FlightNumber
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">888</ns0:FlightNumber>
        <ns0:DepartureAirportCode>YUL</ns0:DepartureAirportCode>
        <ns0:ArrivalAirportCode>MCO</ns0:ArrivalAirportCode>
        <ns0:FlightManualEntryIndicator
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">false</ns0:FlightManualEnt
ryIndicator>
        <ns0:Address>
          <ns3:StreetNumberText
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1"/>
          <ns3:StreetName
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">SIXTH
STREET</ns3:StreetName>
          <ns3:AddressSecondaryUnitText
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1"/>
          <ns3:LocationCityName
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">SPRINGFIELD</ns3:LocationC
ityName>
          <ns3:LocationState
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ns3:ProperNameTextType">VA</ns3:LocationState>
            <ns3:LocationPostalCode
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">22152</ns3:LocationPostalC
ode>
         </ns0:Address>
      </ns0:ApisResponse>
      <ns0:DailySecurityCode
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">wepGTzNqMDV37ul</ns0:Daily
SecurityCode>
   </ns0:TravelerValidateResponse>
  </soap:Body>
</soap:Envelope>
```

### 3.5.3 Traveler End Response

The **TravelerEndResponse** message is sent to the kiosk in response to the **TravelerEndRequest** as confirmation that all required processing for the traveler has been successfully completed. It is critical that the kiosk receive this response prior to printing any referral receipt. In cases of session cancel, the Kiosk should print a CA (Cancel) Referral Receipt when the **TravelerEndResponse** message is received.

The APC Service returns a fault in response when any error occurs during the traveler confirmation process. When a fault is returned, the APC service will not return a **TravelerEndResponse** message. In these instances, the Kiosk should print a SF (System Failure) Referral Receipt.

The elements that comprise the **TravelerEndResponse** message are displayed in Table 21. Figure 11 shows an example SOAP message for the **TravelerEndResponse**.

**Table 21. TravelerEndResponse Element**

| TravelerEndResponse | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| KioskID | String | 10 | Y | A system wide unique identifier for the kiosk. |
| SessionID | String | 65 | Y | A value that uniquely identifies the session. |
| TravelerID | String | 10 | Y | The unique identification value associated with the traveler for the session |
| AdmitUntilDate | Date | 8 | N | Admit Until Date; format conforms to NIEM standard |

**Figure 11. TravelerEndResponse SOAP Message Example**

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns0:TravelerEndResponse xmlns:ns2="http://niem.gov/niem/domains/screening/2.1"
xmlns:ns1="http://niem.gov/niem/structures/2.0" xmlns:ns3="http://niem.gov/niem/niem-

core/2.0" xmlns:ns0="http://cbp.dhs.gov/globalentry/kioskservice/extension/2.0"
xmlns:ns5="http://niem.gov/niem/ansi-nist/2.0">
      <ns0:KioskID
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">MCO4APC002</ns0:KioskID>
      <ns0:SessionID
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">20140117132857394l</ns0:Se
ssionID>
```

```
      <ns0:TravelerID
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">1</ns0:TravelerID>
      <ns0:AdmitUntilDate xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">
        <ns3:Date>2014-04-17</ns3:Date>
      </ns0:AdmitUntilDate>
    </ns0:TravelerEndResponse>
  </soap:Body>
</soap:Envelope>
```

### 3.5.4 System Status Response

The response for system status is provided by the APC Service using the **SystemStatusResponse** message element. The elements and child elements that comprise the message response are displayed in Table 22. Figure 12 shows an example **SystemStatusResponse** SOAP message.

**Table 22. SystemStatusResponse Element**

| SystemStatusResponse | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| KioskId | String | 10 | Y | KioskID for the requesting site. |
| SystemStatusIndicator | Boolean | -- | Y | The APC Service status indicator. A true value indicates that the system is up; a value of false indicates that the system is down. |

**Figure 12. SystemStatusResponse SOAP Message Example**

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns2:SystemStatusResponse xmlns:ns1="http://niem.gov/niem/structures/2.0"
xmlns:ns2="http://cbp.dhs.gov/globalentry/kioskservice/extension/2.0"
xmlns:ns3="http://niem.gov/niem/niem-core/2.0" xmlns:ns4="http://niem.gov/niem/ansi-nist/2.0"
xmlns:ns5="http://niem.gov/niem/domains/screening/2.1"
xmlns:ns6="http://niem.gov/niem/appinfo/2.0" xmlns:ns7="http://niem.gov/niem/appinfo/2.1"
xmlns:ns8="http://niem.gov/niem/domains/infrastructureProtection/2.1">
      <ns2:KioskID>kioskidxx</ns2:KioskID>
      <ns2:SystemStatusIndicator>true</ns2:SystemStatusIndicator>
    </ns2:SystemStatusResponse>
  </soap:Body>
</soap:Envelope>
```

### 3.5.5 Fault Element

A fault may be returned for numerous reasons, examples of which are identified in **Table 26**. The specific reason for each fault is embedded in the fault message. The elements that comprise the Fault message are defined in Table 23. Figure 13 shows an example SOAP message for a fault response. Return of a fault signals termination of traveler processing; a referral receipt should not be printed.

When APC sends the Fault message in response to a TravelerEndRequest message, any assigned referral code is invalidated.

When APC sends the Fault message in response to a TravelerValidiateRequest message, the kiosk should not send the TravelerEndRequest message. If APC receives a TravelerEndRequest message following transmission of a fault message, APC will respond with another Fault message stating "No traveler request found in cache."

OFO has specified that the Kiosk print a System Failure (SF) Referral Receipt in response to a fault receipt from the APC Service.

**Table 23. Fault Element**

| Fault | | | | |
|---|---|---|---|---|
| **Attribute** | **Data Type** | **Size** | **Rqd** | **Description** |
| KioskID | String | 10 | N | A system wide unique identifier for the kiosk. |
| SessionID | String | 65 | N | The unique session identifier. |
| TravelerID | String | 10 | N | The unique identification value associated with the traveler for the session |
| FaultCode | String | 10 | Y | The fault code associated with the error condition identified by the system. |
| FaultCodeDescription | String | 40 | Y | A description of the fault. |

**Figure 13. SOAP Fault Message Example**

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Server</faultcode>
      <faultstring>KIOSKID: YULAPCK09 not found in database</faultstring>
      <detail>
        <ns0:FaultElem xmlns:ns7="http://niem.gov/niem/domains/screening/2.1"
xmlns:ns3="http://niem.gov/niem/niem-core/2.0" xmlns:ns2="http://niem.gov/niem/ansi-

nist/2.0" xmlns:ns1="http://niem.gov/niem/structures/2.0"
xmlns:ns0="http://cbp.dhs.gov/globalentry/kioskservice/extension/2.0">
          <ns0:KioskID
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">YULAPCK09</ns0:KioskID>
          <ns0:SessionID
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">143D917BBF8</ns0:SessionID
>
          <ns0:TravelerID
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">1</ns0:TravelerID>
          <ns0:FaultCode
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">Soap:Sender</ns0:FaultCode
>
          <ns0:FaultCodeDescription
xmlns:ns10="http://niem.gov/niem/domains/infrastructureProtection/2.1">Bad
KioskID</ns0:FaultCodeDescription>
        </ns0:FaultElem>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>Server Functions
```

# 4. Communications

## 4.1 IP Addresses

Each site must provide CBP a publically routable IP address to be used in the Production environment and a separate IP address to be used in the Non- Production environment. If failover is included in the network design, IP addresses for each server should be provided. CBP recommends that a site provide no more than four (4) IP addresses to CBP.

The IP addresses must be sent to APC OIT GROUP (APCOITGroup@cbp.dhs.gov) in an encrypted file; the encryption password ***must*** be sent in separate correspondence. Failure to follow these procedures will render the submitted IP addresses obsolete; new IP addresses will be required.

Note: Word documents may be password protected; emails transmitting the document should be encrypted. Alternatively, the IP addresses can be pasted in an email that is encrypted for transmission.

## 4.2 2-way SSL Certificates

The communication between the Kiosk System and the APC Server occurs via a two-way SSL connection utilizing mutual authentication. Certificates need to be from a publically recognized certificate authority, certified in the Federal Information Processing Standards (FIPS), a standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology (NIST).

It is CBP's recommendation to use VeriSign or Entrust, both of which are acceptable registered certificate providers. Each port will utilize a single SSL Certificate to communicate with the CBP production site. A separate SSL certificate will be required for communication between the port non-production environment and CBP's non-production (test) environment. The one non-production certificate will be used for communication with both the CBP System Acceptance Test (SAT) and the CBP Quality Assurance (QAX) environments.

Prior to establishing communication between the systems, the APC Service will need to register the Kiosk System's

(a) publicly routable IP address, and
(b) public certificate (2048 bits) from a CBP approved Certificate.

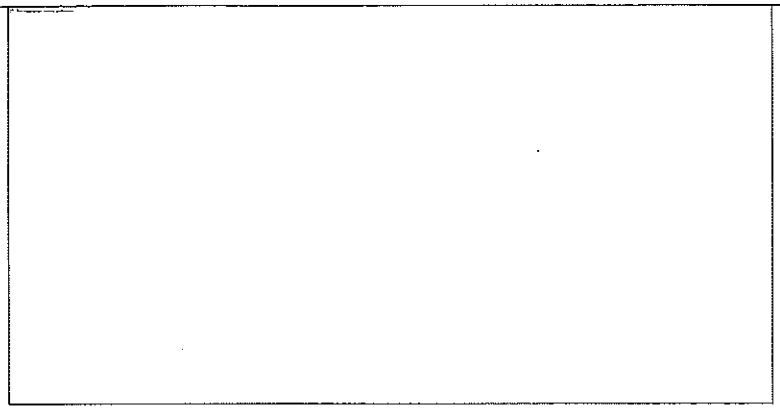
In addition, the Kiosk System will need the APC Service's Certificate Authority certificate chain to authenticate the APC Service.

To successfully connect to the APC Service both parties must exchange and install the certificates prior to initiating the SSL conversation. Figure 14 illustrates the certificate configuration for two-way SSL authentication between two applications.

The certificates must be sent to the APC OIT GROUP (APCOITGroup@cbp.dhs.gov).as encrypted files; the encryption password(s) must be sent in separate correspondence. Failure to follow these procedures will render the submitted certificates obsolete; new certificates will be required.

Note: Word documents may be password protected; emails transmitting the document should be encrypted.

**Figure 14. Two-Way SSL Authentication**



The SSL client (the APC Kiosk Server) initiates a connection to the SSL server (the APC Service) by opening a connection to the SSL server. Next, the SSL server presents its certificate to the SSL client for verification and then requests that the SSL client present its certificate to the SSL server for verification. Once this protocol is completed and the certificates match then the communications dialogue between the Kiosk System and the APC Service may commence.

# 5. Security and Integrity

The Kiosk System is hosted on a port's network. The interface protocol between the port network and the APC Service will be HTTPS/SOAP XML messages sent to and from an XML appliance and the Kiosk System. The XML appliance provides an isolation layer that protects the security and integrity of the CBP network. The SSL certificates and IP addresses, port number information, protocols, virus software and other technical controls are configured to ensure the security and information integrity of the CBP network. AES-256 encryption is required for messages sent from the kiosk to CBP.

Message information integrity is maintained through the use of XML and XSD validation schemas to ensure that each transaction is unique and accurate.

The Kiosk System shall not store any privacy sensitive data such as MRZ data, personal traveler data or referral codes. This information and the detailed security rules will be explained in the Privacy Impact assessment document.

# 6. Environment Information

The APC Service maintains both Test and Production environments. Connection to CBP APC Service should be configured with the Fully Qualified Domain Names and not the External IP Addresses. IP Addresses are subject to change in the event of server conversions.

A request for information on the CBP environment and associated domain values should be sent to the APC OIT GROUP (APCOITGroup@cbp.dhs.gov. Upon receipt of a request from an approved vendor, the APC OIT Group will send specific information including the following:

- Environment
- Fully Qualified Domain Name (FQDN)
- External IP Addresses
- External Port
- Specification of requirement for Certificate Setup (required for all environments)

- URL of the end point for the service to call the methods
- URL of the end point for the service to request the WSDL

# 7. Processing Time Specifications

Table 24 describes the following information:

- Average Transaction Load per day per kiosk (TPD) – This value indicates, on average, the number of request/response transaction pairs that are being processed per day per kiosk.
- Expected Average Response Time per Transaction – The expected average time, in seconds, APC Service will take to process the entire request and response transaction.
- Timeout per Transaction – The time, in seconds, after which APC Service will timeout if the transaction has not completed processing.

All values are calculated based on current production information evaluated during November 2013. As more travelers are processed via APC as a result of additional kiosk stations in existing and new locations then the TPD values may increase. Fluctuations in the transaction volume may affect transaction processing times. Thus, an increase in the transaction load may cause an increase in the response time.

**Table 24. APC Service Message Time Specification**

| Message Name | Average Transaction Load per day per kiosk (TPD) | Expected Average Response Time per Transaction (seconds) | Timeout per Transaction (seconds) |
|---|---|---|---|
| Flight Request / Response | 30 | 20 | 30 |
| Traveler Validate Request / Response | 15000 | 10 | 90 |
| Traveler End Request / Response | 15000 | 10 | 90 |

# 8. Special Processing

There are no special processing requirements.

# 9. Receipt Referral Codes

**Table 25** below details a list of the receipt referral codes that are currently generated by the APC Service. With the exception of the System Failure (SF) and Cancel (CA) referral codes, the Kiosk must print on the Referral Receipt the exact referral received from the APC Service. When the Kiosk cancels a traveler, the Kiosk invalidates the preliminary referral and must print the receipt with a CA (Cancel) Referral. When the Kiosk receives a fault response from APC, the fault invalidates the preliminary referral and the Kiosk should print a SF (System Failure) Receipt.

The APC schema does not include an enumeration element for Referral Codes. This element has been defined as a simple type; the Kiosk should accept whatever code is sent by APC. This provides flexibility to expand and/or change specific codes in the future.

**Table 25. APC Service Receipt Referral Codes**

| Referral Condition | Referral Code | Referral Description |
|---|---|---|
| Enforcement Referral | ER | Traveler has enforcement type issues |
| Random Referral | RR | Traveler is selected for random compliance |
| Declaration Referral | DR | Traveler answers Yes to any general declaration question |
| APIS Problem | AP | Traveler is not found on a manifest |
| Entry Authorization | EA | Visa Waiver traveler does not have an approved ESTA status |
| Biometric Failure | BF | Traveler has no Enrollment Record on file or biometrics cannot be verified (applicable to Visa Waiver travelers). |
| Check Documentation | CD | Referral based on<br>• Foreign national traveler's passport expiration date is less than 6 months<br>• USC or US LPR traveler's document query results in a mismatch or not "Issued" status |
| Technical Referral | TR | Referral based on<br>• Traveler has attempted use the kiosk during the configurable enforcement lockout<br>• Biometric pre-verify check returned a fault response<br>• The return code from a vetting query was other than normal completion<br>• A cancellation command from the kiosk that the traveler processing has been terminated. |
| Passage Granted | PG | Traveler receives Passage Granted |

# 10. Sample Fault Messages

Table 26 below provides a sample of fault messages that may be generated by the APC Service. This is not an inclusive list of fault message. A fault message terminates Traveler processing regardless of where in the processing sequence the fault occurred. A referral receipt should not be printed for any traveler whose processing terminates with a fault.

**Table 26. Sample APC Service Fault Messages**

| # | Soap: Reason |
|---|---|
| 1 | ApisResponse unknown object class |
| 2 | Bad Apis information |
| 3 | Bad Confirm or Manadd completion code |

| # | Soap: Reason |
|---|---|
| 4 | Bad document type |
| 5 | Bad KioskID |
| 6 | Bad ManualEntry |
| 7 | Bad MRZ |
| 8 | Bad SessionID |
| 9 | Bad Traveler Data |
| 10 | Bad TravelerID |
| 11 | Can not parse date of birth in mrz: + mrz |
| 12 | Class Of Admission %s cannot be used by %s., coa, doc_cntry) |
| 13 | Class Of Admission %s is not accepted by APC., coaValue) |
| 14 | Class Of Admission must be specified |
| 15 | Did not receive external responses in time |
| 16 | Document Country of Issue must match Nationality of Traveler |
| 17 | Document must be from USA, CAN, or country in Visa Waiver Program. |
| 18 | Duplicate question numbers for custom questions or out of order custom questions |
| 19 | Encountered: + ex.getMessage() + while processing mrz: + mrz errorParsingString + - + mrz |
| 20 | Incorrect length while processing LPR mrz: + mrz |
| 21 | Incorrect length while processing Passport mrz: + mrz |
| 22 | Invalid Admit Until Date |
| 23 | Invalid Class Of Admission %s., coa) |
| 24 | Invalid document type. |

| # | Soap: Reason |
|---|---|
| 25 | Invalid document type: + mrz.charAt(0) |
| 26 | Invalid Mrz: |
| 27 | KIOSKID: + kioskID + not found in database |
| 28 | ManualEntryInd is missing |
| 29 | Missing Document Expiration Date |
| 30 | Missing photo image. Non US citizens, LPR travelers (with non-Canadian nationality) or non Canadian Citizens must provide photo image. |
| 31 | Must be all four custom questions in the request |
| 32 | No traveler request found in cache. |
| 33 | Non US citizens, LPR travelers (with non-Canadian nationality) or non Canadian Citizens must provide fingerprint image. |
| 34 | Non US citizens, LPR travelers (with non-Canadian nationality) or non Canadian Citizens must send finger prints. |
| 35 | Petition number not found for LPR: |
| 36 | Referral in terminate session must match one in validate traveler responseTraveler already being processed |
| 37 | TravelerEndRequest is missing apisResponse. |
| 38 | TravelerID: + travelerID + is missing referral code response. |
| 39 | Values cannot be null |

# 11. Open Item Discussions

This section will contain items and information that needs to be clarified through this document and other items that needs to be discussed between the two parties involved with this exchange. Please see Table 27 for a list of Open Discussion items.

**Table 27. APC Service Open Discussion Items**

| Item # | Title | Description |
|---|---|---|
| | | |

# Appendix A. Abbreviations

| Abbreviation | Definition |
|---|---|
| APC | Automated Passport Control |
| APIS | Advance Passenger Information System |
| ATDS | Airport Technical Design Standard |
| CBP | U.S. Customs and Border Protection |
| CBSA | Canadian Border Services Agency |
| FIS | Federal Inspection Services |
| IATA | International Air Transport Association |
| ICAO | International Civil Aviation Organization |
| IEPD | Information Exchange Package |
| NDC | National Data Center |
| NIEM | National Information Exchange Model |
| SSL | Secure Sockets Layer |
| WSDL | Web Services Definition Language |

# Memorandum

MIAMI-DADE COUNTY

Date: October 14, 2014

To: Lester Sola
Director
Internal Services Department

Thru: Miriam Singer, CPPO
Assistant Director
Internal Services Department

From: Josh Brown
Procurement Contracting Officer 2
Chairperson, Evaluation/Selection Committee

Subject: Report of Evaluation/Selection Committee for RFP No. RFP-00118: Automated Passport Control (APC) Kiosks

---

The County, on behalf of the Miami-Dade Aviation Department (MDAD), issued a solicitation to obtain proposals from qualified firms to provide Automated Passport Control (APC) Kiosks capable of processing both international and domestic passengers to be located in designated United States Customs and Border Protection (CBP) areas throughout the Miami International Airport (MIA).

Each year approximately 20 million international passengers enter the United States through MIA. The CBP currently processes passengers in person with a CBP agent or by an existing Automated Passport Control Kiosk. MDAD requires additional APC Kiosks to automate processing and clearance times for arriving United States citizens and international passengers due to the continued and anticipated growth in international travel. MDAD and the CBP face multiple challenges to address extended processing and clearance times. It is anticipated that through the use of additional APC Kiosks, the amount of time it takes for arriving passengers to clear customs will be reduced and the overall passengers experience will be improved.

The Evaluation/Selection Committee has completed the evaluation of proposals submitted in response to the solicitation following the guidelines published in the solicitation.

**Evaluation/Selection Committee meeting dates:**

- September 25, 2013 – Kick off Meeting
- September 29, 2014 – Evaluation Meeting #1

**Responsiveness Review:**
The Solicitation closed on September 24, 2014 with three proposals received from Sita Inc., Dedo Interactive Inc., and Innovative Travel Solutions by YVR. All proposals were reviewed by the RFP Chairperson and deemed to be responsive.

**Verification of compliance with contract measures:**
The solicitation included a selection factor entitling a SBE/Micro Business Enterprise to receive an additional 10 percent (10%) of the total technical evaluation points on the technical portion of the Proposer's proposal. The selection factor did not affect the outcome of the scoring as no Proposer was a certified SBE/Micro Business Enterprise.

**Verification of compliance with minimum qualification requirements:**
The solicitation had minimum qualification requirements which were reviewed by the Chairperson for each submission. All of the proposers met the minimum qualification requirements set forth within the solicitation.

**Local Certified Service-Disabled Veteran's Business Enterprise Preference:**
Veteran's Preference was considered in accordance with the applicable ordinance. None of the proposers qualified.

**Evaluation/Selection Committee Background Check:**
On October 8, 2014, the Miami-Dade County Office of the Commission Auditor (OCA) issued the results of the Evaluation/Selection Committee background checks on all appointed voting members and technical advisors assigned to RFP No. RFP-00118 (see attached memo). Research conducted by OCA found that Mr. Maurice Jenkins, a member of the Evaluation/Selection committee, serves as a member of the Sita Customer Advisory Board, the Sita Airport Steering Committee, and has participated in the 2013 & 2014 Sita Air Transport IT Summit.

Based on these findings, OCA requested the opinion of Joe Centorino, Executive Director and General Counsel, of the Miami-Dade Commission on Ethics & Public Trust. Mr. Centorino rendered an opinion that there is no actual conflict of interest (see attached email). However, in an excess of caution due to the appearance of a conflict, the County has chosen to remove Mr. Jenkins from the Evaluation/Selection committee and omit his scores from the final results.

**Evaluation Results / Summary of Scores:**
The Evaluation/Selection Committee was tasked with evaluating, scoring, and ranking the responsive proposals submitted in reference to the RFP. An evaluation meeting was held to discuss the technical merits of each proposal and the ability of the proposed solution to meet the operational needs of the County as outlined in the Solicitation. After completion of the technical review of the proposal received, the Evaluation/Selection Committee conducted scoring in accordance with the criteria outlined within the RFP. The Evaluation/Selection Committee's scoring was conclusive and the Committee unanimously voted to forego oral presentations as the proposals received were written in sufficient detail to make a final recommendation.

The scoring is as follows:

| Proposer | Technical Score (Max. 320 pts) | Price (Max. 80 pts) | Total Combined Score (Max. 400 pts) | Price Submitted |
|---|---|---|---|---|
| Sita Inc. | 271 | 39 | 310 | $ 10,504,747.00 |
| Dedo Interactive Inc. | 190 | 54 | 244 | $ 5,994,446.83 |
| Innovative Travel Solutions by YVR | 223 | 52 | 275 | $ 8,225,000.00 |

**Local Preference:**
Local Preference was considered in accordance with applicable ordinance, but did not affect the outcome.

**Negotiations:**
The Evaluation/Selection Committee recommends that the County enter into negotiations with the highest ranked proposer, Sita, Inc. The following individuals will participate in the negotiations:

Josh Brown, Procurement Contracting Officer 2, Internal Services Department

Todd Lewis, Systems Project Manager, Ross and Barruzini

Chris Bradley, Staff Vice President, AvairPros

Tania Dip, Administrative Officer 3, Miami-Dade Aviation Department

**Justification for Recommendation:**
The Evaluation/Selection Committee recommends that the County proceed to negotiations with Sita, Inc. for the purchase of the required Automated Passport Control (APC) Kiosks to be implemented within the Miami International Airport. The APC Kiosks offered by Sita, Inc. are capable of meeting all of the technical and business requirements of both Miami-Dade County and the United States Customs and Border Protection Department as outlined within the solicitation. Additionally, Sita's proposal best addressed MDAD's needs for on-site staff to provide maintenance and support services including technical support. The extensive preventative maintenance schedule includes weekly and daily activities that service the kiosks and associated hardware.

Sita, Inc. will be responsible for delivering all APC Kiosks inclusive of the required equipment, hardware, software, and licenses. Additionally, they will be responsible for the implementation, installation, training, testing, repairs, and maintenance support services for the Kiosks throughout the contract term including any renewals or extensions issued by the County.

**Consensus Statement:**
Copies of the consensus statement, composite scores, and individual score sheets for each Evaluation/Selection Committee member are attached.

Approved

Lester Sola
Director

10/14/14
Date

Miriam, I would like to see our effort to negotiate the #2 firm price down.

RFP No. RFP-00118
Title: Automated Passport Control Kiosks
EVALUATION OF PROPOSALS - FINAL

COMPOSITE

| SELECTION CRITERIA / PROPOSERS | Maximum Points Per Member | Maximum Total Points (4 members) | PROPOSER NAME DEDO INC | PROPOSER NAME YVR | PROPOSER NAME SITA INC |
|---|---|---|---|---|---|
| Proposer's relevant experience, qualifications, and past performance | 30 | 120 | 71.00 | 106.00 | 100.00 |
| Relevant experience & qualifications of key personnel, including key personnel of subcontractors, that will be assigned to this project, and experience and qualifications of subcontractors | 30 | 120 | 73.00 | 82.00 | 100.00 |
| Proposer's approach to providing the services requested in this Solicitation and capability to meet operational and business needs expressed. | 20 | 80 | 46.00 | 35.00 | 71.00 |
| Proposer's proposed price will be evaluated based on the value of the proposed APC Kiosks and associated services and the overall best value to the County. | 20 | 80 | 54.00 | 52.00 | 39.00 |
| TOTAL POINTS | 100 | 400 | 244 | 275 | 310 |
| Ranking | | | 3 | 2 | 1 |

Signature: Josh Brown
Print Name: JOSH BROWN
Date: 9-29-14

Chairperson:
Print Name: DAKOTA THOMPSON
9-30-14

Reviewed By

Local Preference: No Proposers claimed local preference.

Selection Factor 10% SBE/Micro: No Proposers were certified SBE/Micro's, therefore, the Selection Factor did not affect the final ranking.

RFP NO. RFP-00118
TITLE: Automated Passport Control Kiosks
EVALUATION OF PROPOSALS

## COMMITTEE MEMBER NAME
Pedro Garcia

| SELECTION CRITERIA / PROPOSERS | Maximum Points | PROPOSER NAME SITA INC. | PROPOSER NAME DEDO INTERACTIVE | VANCOUVER APT A. PROPOSER NAME ITS BY YVR |
|---|---|---|---|---|
| Proposer's relevant experience, qualifications, and past performance | 30 | 25 | 21 | 29 |
| Relevant experience & qualifications of key personnel, including key personnel of subcontractors, that will be assigned to this project, and experience and qualifications of subcontractors | 30 | 25 | 23 | 27 |
| Proposer's approach to providing the services requested in this Solicitation and capability to meet operational and business needs expressed. | 20 | 18 | 16 | 10 |
| Proposer's proposed price will be evaluated based on the value of the proposed APC Kiosks and associated services and the overall best value to the County. | 20 | 10 | 19 | 13 |
| TOTAL POINTS | 100 | 78 | 79 | 79 |

9/24/2014 Pedro J. Garcia
SIGNATURE

9-29-2014
DATE

RFP NO. RFP-00118
TITLE: Automated Passport Control Kiosks
EVALUATION OF PROPOSALS

## COMMITTEE MEMBER NAME
Todd Lewis

| SELECTION CRITERIA / PROPOSERS | Maximum Points | PROPOSER NAME DEDO | PROPOSER NAME YVR | PROPOSER NAME SITA |
|---|---|---|---|---|
| Proposer's relevant experience, qualifications, and past performance | 30 | 20 | 22 | 25 |
| Relevant experience & qualifications of key personnel, including key personnel of subcontractors, that will be assigned to this project, and experience and qualifications of subcontractors | 30 | 15 | 20 | 25 |
| Proposer's approach to providing the services requested in this Solicitation and capability to meet operational and business needs expressed. | 20 | 10 | 10 | 20 |
| Proposer's proposed price will be evaluated based on the value of the proposed APC Kiosks and associated services and the overall best value to the County. | 20 | 10 | 10 | 8 |
| TOTAL POINTS | 100 | 55 | 62 | 78 |

9/24/2014 _____
SIGNATURE

29 SEPT 2014
DATE

RFP NO. RFP-00118
TITLE: Automated Passport Control Kiosks
EVALUATION OF PROPOSALS

COMMITTEE MEMBER NAME
Chris Bradley

| SELECTION CRITERIA / PROPOSERS | Maximum Points | DEDO PROPOSER NAME | SITA PROPOSER NAME | YVR PROPOSER NAME |
|---|---|---|---|---|
| Proposer's relevant experience, qualifications, and past performance | 30 | 10 | 25 | 30 |
| Relevant experience & qualifications of key personnel, including key personnel of subcontractors, that will be assigned to this project, and experience and qualifications of subcontractors | 30 | 20 | 30 | 25 |
| Proposer's approach to providing the services requested in this Solicitation and capability to meet operational and business needs expressed. | 20 | 10 | 18 | 10 |
| Proposer's proposed price will be evaluated based on the value of the proposed APC Kiosks and associated services and the overall best value to the County. | 20 | 15 | 11 | 14 |
| TOTAL POINTS | 100 | 55 | 84 | 79 |

9/24/2014
SIGNATURE

9/29/14
DATE

RFP NO. RFP-00118
TITLE: Automated Passport Control Kiosks
EVALUATION OF PROPOSALS

COMMITTEE MEMBER NAME
Dialas Burke-Wheeler

| SELECTION CRITERIA / PROPOSERS | Maximum Points | PROPOSER NAME DECO | PROPOSER NAME VVB | PROPOSER NAME SITA |
|---|---|---|---|---|
| Proposer's relevant experience, qualifications, and past performance | 30 | 20 | 25 | 25 |
| Relevant experience & qualifications of key personnel, including key personnel of subcontractors, that will be assigned to this project, and experience and qualifications of subcontractors | 30 | 15 | 10 | 20 |
| Proposer's approach to providing the services requested in this Solicitation and capability to meet operational and business needs expressed. | 20 | 10 | 5 | 15 |
| Proposer's proposed price will be evaluated based on the value of the proposed APC Kiosks and associated services and the overall best value to the County. | 20 | 10 | 15 | 10 |
| TOTAL POINTS | 100 | 55 | 55 | 70 |

9/24/2014
SIGNATURE

9/29/14
DATE

# Memorandum

MIAMI-DADE COUNTY

**Date:** October 17, 2014

**To:** Charles Anderson
Commission Auditor
Office of the Commission Auditor

**From:** Lester Sola
Director
Internal Services Department

**Subject:** Evaluation/Selection Committee Background Check for RFP No. RFP-00118: Automated Passport Control (APC) Kiosks

---

In a memorandum dated October 8, 2014, the Office of the Commission Auditor (OCA) advised that a background check of one of the voting members of the Evaluation/Selection Committee for RFP-00118, revealed that Maurice Jenkins, Miami Dade Aviation Department's (MDAD) Director of Information Technology and Communications, serves as a member of the SITA, Inc. (SITA) Customer Advisory Board, the SITA Airport Steering Committee, and has participated in the 2013 & 2014 SITA Air Transport IT Summits. SITA is a current MDAD contractor, and a proposer to the referenced solicitation.

Mr. Joe Centorino, Executive Director and General Counsel of the Miami-Dade Commission on Ethics & Public Trust, opined that based on the information provided and reviewed by his office, there is no actual conflict of interest. However, in an excess of caution, the County has chosen to remove Mr. Jenkins from the Evaluation/Selection committee and omit his scores from the final results.

In accordance with the County Mayor's Guidance Memo dated September 10, 2014, going forward, please submit the results of background checks of the selection/evaluation committee members to the Committee Chairperson, prior to the initial committee meeting.

c: Joseph Centorino, Executive Director, Commission of Ethics and Public Trust
Miriam Singer, Assistant Director, ISD
Clerk of Board

# Memorandum

MIAMI-DADE COUNTY

**Date:** August 25, 2014

**To:** Those Listed Below

**From:** Carlos A. Gimenez
Mayor

**Subject:** Appointment of Selection Committee for Miami-Dade Aviation Department Request for Proposals (RFP) for Automated Passport Control Kiosks – RFP No. 00118

---

In accordance with Implementing Order 3-34, I am hereby appointing those listed below as the Selection Committee for Miami-Dade Aviation Department Request for Proposals (RFP) for Automated Passport Control Kiosks – RFP No. 00118.

Selection Committee
Josh Brown, ISD (Non-Voting Chairperson)
Maurice Jenkins, MDAD
Pedro Garcia, MDAD
Todd Lewis, Ross and Barruzini
Chris Bradley, AvairPros
Diane Coyle, British Airways
Dialas Burke-Wheeler, MDAD (Alternate)

Technical Advisors
Tania Dip, MDAD
Debbie Shore, MDAD

You are directed to assist me in the selection process considering the factors delineated in the solicitation. If you are unable to participate in the selection process, contact this office through Small Business Development (SBD) by memorandum from your department director documenting the reason why you cannot participate. Only in cases of **dire** urgency may you be excused from participation.

Each Selection Committee member shall be responsible for evaluating, rating and ranking the proposals based on the criteria and procedure contained in the solicitation. The Selection Committee will meet to review the written proposals. If required, the Selection Committee will select firms to make oral presentations to the Selection Committee at a properly noticed public hearing. If proposers are invited to make oral presentations, the Selection Committee may re-rate and re-rank the proposals based upon the written documents combined with the oral presentation. You may utilize staff of the issuing department and the using agency to conduct a preliminary review of the proposals for responsiveness. All requests for responsiveness determinations shall be made in writing by the issuing department to the County Attorney's Office.

The alternate committee member will serve only in the event of an approved substitution. No substitution of committee members shall be allowed after the first official meeting of the committee. The Internal Services Department (ISD) may substitute the chairperson to ensure the appropriate level of staffing expertise as deemed necessary to accommodate the needs of this solicitation.

Upon completion of the evaluation process, the Selection Committee Chairperson shall prepare and submit a memorandum to include a narrative of the evaluation and justification of the recommended firm(s) and attach supporting documentation which MUST include the following information:

Name of firm(s)
Quality Rating Score
Price
Adjusted Score (if applicable)
Committee's Overall Ranking

This report should be submitted to me through ISD for review and consideration.

As a matter of administrative policy and to maintain a fair and impartial process, all individuals appointed to the Selection Committee (including the Chairperson) and staff are instructed to refrain from discussing the solicitation with prospective lobbyists and/or consultants. Selection Committee members are reminded that in accordance with the Cone of Silence Ordinance 98-106, there are restrictions on communications regarding the solicitation with potential proposers, service providers, lobbyists, consultants, or any member of the County's professional staff. Violation of this policy could lead to termination of County service.

All questions must be directed to the staff contact person designated by the issuing department.

c: Lester Sola, Director, ISD
Emilio T. Gonzalez, Director, MDAD
Gary T. Hartfield, SBD Division Director, ISD

Selection Committee
Josh Brown, ISD (Non-Voting Chairperson)
Maurice Jenkins, MDAD
Pedro Garcia, MDAD
Todd Lewis, Ross and Barruzini
Chris Bradley, AvairPros
Diane Coyle, British Airways
Dialas Burke-Wheeler, MDAD (Alternate)

Technical Advisors
Tania Dip, MDAD
Debbie Shore, MDAD

# SELECTION COMMITTEE
# MIAMI-DADE AVIATION DEPARTMENT
# AUTOMATED PASSPORT CONTROL KIOSKS
# RFP NO. 00118

| Committee Member/ Title | Department | Start Year With County | Ethnicity/ Gender | Education | Professional License(s)/ Certification(s) | Telephone # |
|---|---|---|---|---|---|---|
| Josh Brown (Non-Voting Chairperson) | ISD | --- | --- | --- | --- | 305-375-4725 |
| Maurice Jenkins Director ISD/Telecommunications | MDAD | 1988 | Black Male | Bachelor of Business Administration – Computer Information Systems | --- | 305-876-0934 |
| Pedro Garcia Chief of Telecommunications | MDAD | 1988 | Hispanic Male | Master's in Engineering; Bachelor of Science in Electrical Engineering | Professional Engineer; General Contractor; Real Estate License | 305-876-7523 |
| Todd Lewis Systems Project Manager | Ross and Barruzini | --- | White Male | Bachelor of Science in Electrical Engineering | Engineer in Training | --- |
| Chris Bradley Staff Vice President | AvairPros | --- | White Male | Master of Business Administration | Certified Project Management Professional (PMP) | --- |
| Diane Coyle Station Manager | British Airways | --- | White Female | | | --- |
| Dialis Burke-Wheeler Chief, Terminal Properties (Alternate) | MDAD | 1989 | Black Female | Bachelor's in Administration | Real Estate License | 305-876-8047 |
| **TECHNICAL ADVISORS** | | | | | | |
| Tania Dip Administrative Officer 3 | MDAD | 2004 | Hispanic Female | Bachelor of Science in Business Management | --- | 305-876-0968 |
| Debra Shore Senior Aviation Cost Manager | MDAD | 2008 | White Female | Bachelor of Arts in Political Science/Environmental Studies | International Airport Professional | 305-869-4585 |