

## **Scope of Work**

# **For a FIPS 201 Compliant Credentialing Solution Proof-of-Concept**

**Date: December 21<sup>st</sup>, 2007**

**TABLE OF CONTENTS**

**SECTION C SPECIFICATIONS AND WORK STATEMENT..... 3**

C.1 SCOPE..... 3

    C.1.1 *Applicable Documents*..... 3

    C.1.2 *Definitions* ..... 3

C.2 BACKGROUND ..... 4

C.3 REQUIREMENTS ..... 5

    C.3.1 *General Requirements*..... 5

    C.3.2 *CLIN Descriptions and Requirements*..... 5

        C.3.2.1 CLIN 0001 – City-Wide Needs Assessment..... 5

        C.3.2.2 CLIN 0002 – Proof of Concept Solution Design ..... 6

        C.3.2.3 CLIN 0003 – Implementation of limited FIPS 201 compliant platform..... 6

        C.3.2.4 CLIN 0004 – Implementation of Digital signature email ..... 7

        C.3.2.5 CLIN 0005 – Implementation of “Leave slip” Application..... 7

        C.3.2.6 CLIN 0006 Acceptance Testing ..... 8

        C.3.2.7 CLIN 0007 Pilot Operations ..... 8

        C.3.2.8 CLIN 0008 – Development of a city-wide Implementation Plan ..... 8

        C.3.2.9 CLIN 0009 – Optional Smart Card Reader Keyboards..... 9

        C.3.2.10 CLIN 0010 – Optional Card supporting smart chip and HID antenna..... 9

    C.3.3 *Statement of Work* ..... 9

    C.3.4 *Vendor Responsibilities*..... 9

    C.3.5 *Functional/Technical Specifications* ..... 10

        C.3.5.1 Smart Cards ..... 10

## **Section C            SPECIFICATIONS AND WORK STATEMENT**

### **C.1 SCOPE**

The objective of this project is to provide city executives with information to enable them to make a business decision regarding a city-wide credentialing system.

The scope of the project includes a city-wide assessment of ID management needs across multiple agencies, and the implementation of a proof-of-concept (solution limited in features and number of users) evaluating the benefits of such a solution. The project will also produce the design of a complete solution and the development of a corresponding implementation plan.

The proof of concept consists in providing 10 users a solution enabling logical access control of selected applications and digital signature, in addition to existing physical access capabilities.

The solution will be fully compliant with a Presidential Directive mandating the use of specific industry standards, and therefore will also enhance the interoperability capabilities of the city's public safety agencies.

The pilot solution implemented will be operated for 3 months. From the lessons learned during this pilot, and from the citywide assessment of agencies' needs, an implementation plan will be developed. This plan will be presented to city executives such that they can make relevant decisions.

#### **C.1.1 Applicable Documents**

Federal Government: FIPS-201-1

NIST:                            HSPD Directive 12

#### **C.1.2 Definitions**

**HSPD Directive 12**, issued by President Bush in August 2004, presents certain guidelines and a definitive timeline for improving secure identification processes for federal employees and contractors. Some of the main control objectives of the Presidential Directive are that agencies should create credentialing processes such that official identification is:

- (a) Issued based on sound criteria for verifying an individual employee's identity;
- (b) Strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- (c) Can be rapidly authenticated electronically; and
- (d) Issued only by providers whose reliability has been established by an official accreditation process.

**FIPS 201-1** stands for the Federal Information Processing Standard. It essentially defines policies, methods and guidelines for processing, protecting and managing information.

**PKI**, or public key infrastructure, is based on certificates verified by certificate authorities such as Verisign. Certificates are a method of encrypting sensitive information with a private “key” that can only be de-encrypted by an entity that has been given a public “key”. This security technique has become the accepted standard for strong security.

**MPD:** Metropolitan Police Department  
**HSEMA:** Homeland Security Emergency Management Agency  
**F/EMS:** Fire and Emergency Medical Services

## **C.2 Background**

It is critical for effective and efficient emergency response for First Responders to be fully vetted, identified and authenticated rapidly on the scene of emergency. Compliance with FIPS 201 is one of the ways in which the District can ensure that their emergency personnel are who they say they are.

The District of Columbia has recently upgraded its ID System. A new Employee Credentialing and Identification Management system has been implemented. This system is the first step in building a true Identification Management System Architecture (IDMS). Currently, the IDMS credential system serves as a Three-in-One device:

1. Electronic Employee benefits delivery (i.e. SmarTrip)
2. Real-time electronic access to District facilities
3. Improved Flash Pass identification with holographic technologies to discourage duplication.

The next steps to make it fully FIPS 201 compliant include implementing smart-chip enabled cards, a logical access control system, and credentials backwards-compatible with the current IDMS and HID antenna system. The program initially targets the First Responder environment, which will include HSEMA, MPD, PSD, and F/EMS. It will provide benefits that include:

- Consolidation of all Credentialing and Access Control Systems allowing Fire/EMS, MPD and other District Agencies to carry uniquely identifiable IDs that are interoperable (e.g., MPD will have after-hours access to District facilities.)
- On-demand access control to allow District First Responders to access federal facilities such as the FBI, Department of Justice, White House
- Strong security features through PIN(s) and biometric technologies discouraging duplication and fraud.
- Real-time electronic authentication to ensure only valid and active personnel are allowed at the scene of an emergency incident
- Real-time reporting and tracking of personnel access to District and Federal facilities for improved security

However it appears that besides the public safety agencies, other agencies such as the DC Public Schools (DCPS) could leverage the benefits of such credentialing technologies to

enhance their business process. Such technologies would also facilitate interoperability across District agencies. In addition, the implementation of a unique architecture serving a District wide users' community would greatly maximize the city's return on investment to the greater benefit of its citizens.

The objectives of this project include a city-wide assessment of ID management needs across multiple agencies, and the implementation of a proof-of-concept (solution limited in features and number of users) demonstrating the benefits of such a solution to the city's executives.

### **C.3 Requirements**

#### **C.3.1 General Requirements**

Mandatory system attributes shall include, but are not limited to:

- a) All equipment shall include a minimum three year warranty except as otherwise noted;
- b) In the answer to this solicitation the vendor shall demonstrate that its solution is scalable. In doing so, the vendor shall describe the minimum capacity supported by its solution and propose a path to scale from this minimum to a potential city-wide deployment. The vendor shall include the proposed equipment, software and services increments necessary to scale the proposed solution from pilot configuration to operational configuration, and price each of those increments.
- c) The vendor is required to ensure the proposed solution in this pilot project can be integrated into the existing system.
- d) The proposed solution shall support existing cards (HID antennas). New cards issued within this proof of concept project and beyond are required to support both the HID antennas and the smart chips.
- e) The proposed solution must be a GSA HSPD-12 certified compliant end-to-end solution.
- f) The vendor shall demonstrate in its response to this solicitation how the proposed solution for the proof of concept can evolve in order to support future needs and applications.

#### **C.3.2 CLIN Descriptions and Requirements**

##### **C.3.2.1 CLIN 0001 – City-Wide Needs Assessment**

The vendor shall meet and collect information from District agencies to document the agencies; ID Management needs and credentialing processes. The agencies the vendor will meet with shall include at least DCHR, DCPS, OCTO, OCFO, and OCP.

OCTO's needs assessment will be done first in order to finalize the scope of the proof of concept phase in a very short time frame.

## *FIPS 201 Compliant Credentialing Solution Proof-of-Concept*

The vendor shall work with PSD, MPD, FIRE/EMS, EMA and OCTO to confirm the previously documented business requirements and processes that would best meet the needs of the District.

The findings need to be documented into a report that will include:

- The details of the business requirements for each agency, and
- The details of the operational business processes and procedures.

### C.3.2.2 CLIN 0002 – Proof of Concept Solution Design

The objective of the Proof-of-Concept is to provide both a secure physical access to the OCTO War Room located at One Judiciary Square, and secure logical access to the LAN using the computers dedicated to this room.

From the computers located in the War Room, the users will be able to access the LAN and their personal files once they slide their card in the smartcard reader keyboards attached to those computers.

Additionally the users will have logical access to selected applications described below. Those applications are expected to be digital signature for email, and for a “leave slip” form.

The vendor will design the solution that provides these services. The vendor will take into account the existing hardware and software deployed to install in the OCTO War Room 10 keyboards, a card reader (if necessary), and necessary hardware and software components to provide the solution. The vendor shall produce a detailed design document including architecture diagram, blueprints and bill of materials.

The vendor will also develop a project implementation plan.

The following phase will not start before OCTO’s approval of the design document and the project implementation plan.

### C.3.2.3 CLIN 0003 – Implementation of limited FIPS 201 compliant platform

Additional upgrades are needed particularly for agencies involved in public safety to improve the District’s general security and alignment with the Federal FIPS 201 standard. The FIPS 201 compliant platform required in this CLIN and technology will enable the following key functions:

- Electronic authentication with encrypted PKI certificate technology;
- Acceptance of the digital certificates in the cards of District employees for controlled access to selected applications.
- Acceptance of District cardholders for controlled access to District locations
- Logging and real-time reporting of cards authenticated at a site; and
- Real-time access to and display of authenticated resources available in the region (as well as nationally).

## *FIPS 201 Compliant Credentialing Solution Proof-of-Concept*

The biggest opportunity for cost-savings, and for the card to be widely adopted for daily routine use, is if the new system can be integrated with the existing system's IDMS (ID management system) and also perform all the access functions of the existing Citywide card.

Therefore the cards provided by the vendor will support the HID antennas and the smart chip.

Also, it is preferred that the vendor, rather than implementing a new partial IDMS, interface its solution to the existing IDMS.

In its proposal, the vendor shall include any development related to this integration.

This CLIN includes:

- The delivery of all required software and hardware to support the authentication and the credentialing functions, including the Cards Management System (CMS),
- The installation of such software and hardware,
- The development of required customized interfaces as necessary,
- The integration of software and hardware in the District network,
- The delivery and installation of 10 smartcard reader keyboards,
- The delivery and installation including wiring of 1 card reader (and necessary miscellaneous hardware enabling proper installation) to physically access the War Room,
- The delivery of 10 smartcards, the enrollment of 10 users and the distribution of the cards to those users. The cards will meet the requirements described in section C.3.5
- The activation of the 10 smart cards.

### C.3.2.4 CLIN 0004 – Implementation of Digital signature email

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

The vendor shall provide a solution enabling the users authenticated with the cards to digitally sign their emails. The vendor shall work with OCTO City-wide Messaging to interface this application with the electronic mail system and ensure the non-disturbing and proper operation of the solution.

The vendor shall perform all development and integration necessary to implement this solution. The vendor shall ensure basic functionality of the package through system testing and ensure that the software meets all the users' requirements.

### C.3.2.5 CLIN 0005 – Implementation of "Leave slip" Application

District employees need to fill in using a form called a "leave slip" to take leave. The objective of this CLIN is to automate this process by authenticating the user through the deployed Logical Access Control System, fill in user's specific fields in the form, and finally authenticate through digital signature.

## *FIPS 201 Compliant Credentialing Solution Proof-of-Concept*

The vendor shall customize the application based on the unique District business requirements identified previously.

The vendor shall ensure basic functionality of the package through system testing and ensure that the software meets all the users' requirements.

### C.3.2.6 CLIN 0006 Acceptance Testing

The vendor shall ensure basic functionality of the features and functionalities implemented through system testing and ensure they meet the business requirements identified in previous phases. The vendor will work with OCTO information system managers to conduct integration testing with the designated production servers and Web applications. The vendor will also work with OCTO regarding user acceptance testing. User acceptance testing is conducted by the end users who are responsible for accepting the package when it meets their expectations. Finally, the vendor shall perform a stress test that demonstrates the system's operational ability during periods of extremely high demand.

Deliverables include a test plan document (to be approved by OCTO before the testing is actually started), and a report documenting the results of the tests.

The vendor will provide correction to all necessary components of the solution until it meets all the requirements.

### C.3.2.7 CLIN 0007 Pilot Operations

For a duration of 3 months the vendor shall support the operations of the proof of concept. This includes trouble shooting operational issues, maintaining relevant data bases, fixing bugs in the application, and collecting on a regular basis feedback from the users on the benefits to their operations that are provided or omitted by the implemented solution. The lessons learned from the pilot operations will be documented in an operational report.

### C.3.2.8 CLIN 0008 – Development of a city-wide Implementation Plan

Based on the findings of the City-Wide Needs Assessment and the results of the proof-of-concept operations, the vendor shall identify applications and features that will support adequately the needs expressed by the city, and design a solution that will meet those requirements. The vendor shall present this design to the stakeholders and modify the design of the solution as necessary to obtain District approval. If necessary the vendor shall propose several design options.

Upon approval of the design by the District, the vendor shall develop an implementation plan for the solution. The plan will be phased and include:

- Overview of the project,
- Proposed organization to execute the project
- A Work Breakdown Structure,
- Schedule,
- Resources requirements
- Cost estimate, including hardware, software and services including project management services, installation, configuration, optimization, development, training, testing and technical support.

## *FIPS 201 Compliant Credentialing Solution Proof-of-Concept*

- Risk assessment and mitigation plan for those risks

The plan will be documented and presented in such a manner that the city's executives are able to make a business decision regarding the next phases of the project.

### C.3.2.9 CLIN 0009 – Optional Smart Card Reader Keyboards

The smart card reader Keyboards will be able to read the cards described in section C.3.5. The vendor shall price the keyboards in quantities of 10, 20, 50 and 100.

### C.3.2.10 CLIN 0010 – Optional Card supporting smart chip and HID antenna

The cards will meet the requirements described in section C.3.5. and support both the HID antenna and smart chips. The vendor shall price the cards in quantities of 10, 20, 50, 100, 1,000, 2,000, 5,000, 10,000 and 20,000.

### **C.3.3 Statement of Work**

This statement of work (SOW) describes the services, equipment, and subsystems to be provided by the vendor for engineering, installing, testing, documenting, operating and maintaining equipment and services for the system being acquired under this solicitation.

### **C.3.4 Vendor Responsibilities**

The vendor's responsibilities include, but are not limited to, the following requirements. The vendor shall refer to appropriate paragraphs of this section for more detail.

- a) The vendor shall provide project management and scheduling to ensure proper coordination and timely completion of the system;
- b) The vendor shall provide a description of its technology including, but not limited to, architecture, features, implementation options, security features and performance;
- c) The vendor shall develop and deliver a system design pursuant to the requirements as defined in Section C of this solicitation;
- d) The vendor shall provide and install the system as defined in an approved detailed design document that has been approved by the District of Columbia;
- e) The vendor shall supply and warehouse all equipment until installation;
- f) The vendor shall prepare test plans and procedures and conduct those tests as per the plan. Those tests shall include, but not be limited to, installation test, integration tests, field tests, security tests and performance tests;
- g) The vendor shall conduct operations and system administration training for the system to District of Columbia representatives;
- h) The vendor shall provide "as-built" documentation, including wiring and cable diagrams, system manuals, equipment manuals, security manuals and maintenance manuals;
- i) The vendor shall as an option provide twelve (12) months of maintenance services of the system;

*Office of the Chief Technology Officer of the District of Columbia*

### **C.3.5 Functional/Technical Specifications**

#### **C.3.5.1 Smart Cards**

The vendor shall provide cards that meet the following requirements:

The embedded physical access control “HID antenna” that transmits a unique serial number to District door keys for access rights, and

The gold Federal-standard FIPS 201 chip embedded at the lower-center of cards (see the image below), which stores

- A PKI certificate for encryption and decryption;
- The cardholder’s PIN number and standard identification text data; and
- Biometrics data (facial image and fingerprint).

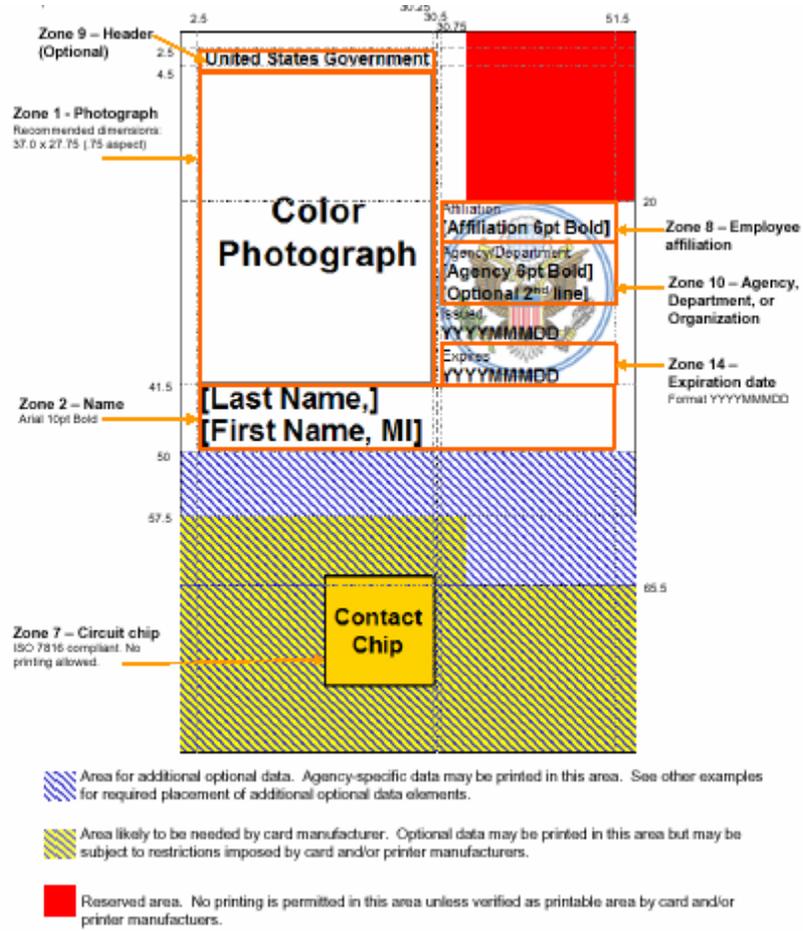
#### **Identification Card Standards**

##### **Standard 1. – Card Characteristics**

1. Must comply with standard ISO/ IEC 7810 Physical Characteristics for Contact Cards
2. Must possess a Smart Chip - ISO/ IEC 7816 Contact Chip
3. Must comply with standard - ISO/ IEC 14443 (Parts 1- 4 Draft) Proximity Card for contact-less cards
4. Must be fully interoperable with other Agencies, Federal and Local - ISO/ IEC 24727 (Future) Interoperability Specification [NIST IR 6887]
5. Printed Material must be of such that it will not rub off during the life of the PIV Card, nor shall the printing process deposit debris on the printer rollers during printing and laminating. Printed material shall not interfere with the contact and contact-less ICC(s) and related components, nor shall it obstruct access to machine-readable information.
6. Card shall pass the following ANSI (American National Standards Institute) tests [ANSI322]; card flexure, static stress, plastic exposure, impact resistance, structural integrity, surface abrasion, temperature and humidity-induced dye migration, ultraviolet light exposure, and a laundry.

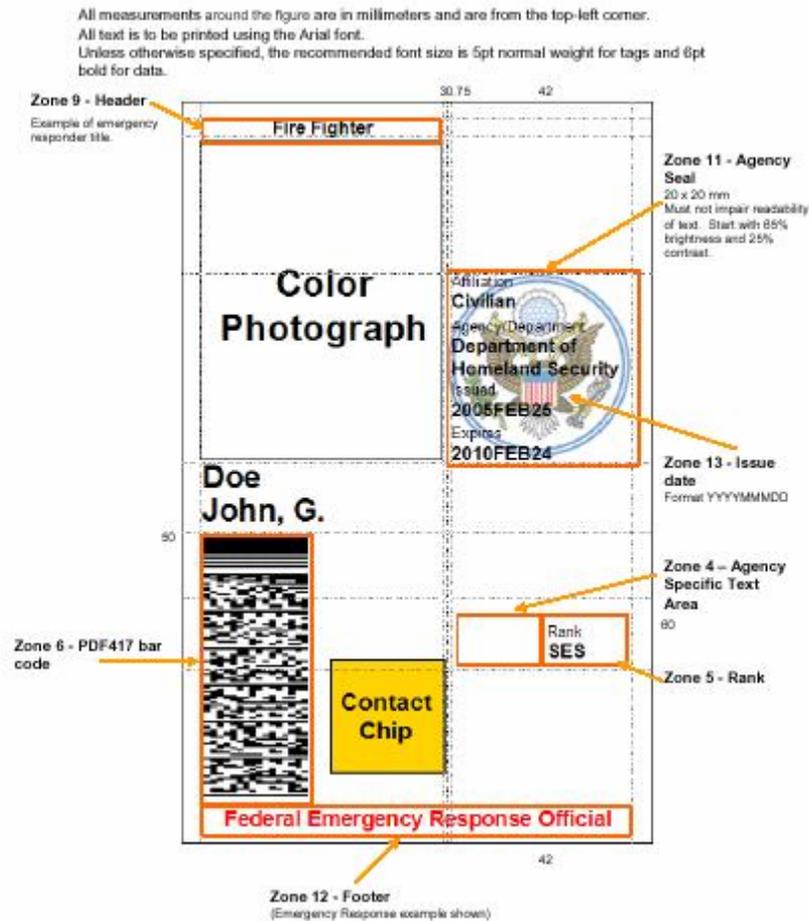
#### **Front of Card**

*FIPS 201 Compliant Credentialing Solution Proof-of-Concept*



**Back of Card**

## FIPS 201 Compliant Credentialing Solution Proof-of-Concept



Additional identifying features shall be added to card layout to ensure it is distinguishable as a District First Responder Authentication Credential from specific agencies including MPD, F/EMS, EMA, PSD and others.

### Standard 2 – Feature Specification

1. Must support Cryptographic (2048 Bit RSA, 256 Bit AES, SHA 256) Standard
2. Must display Image of the Card Holder Fingerprint
3. Must display Photographic Image of Card Holder
4. Must Display Full Name, which must be under Photo
5. Must display Employee affiliation (i.e. Employee, Contractor)
6. Must display Agency Affiliation (i.e. OCTO, EMA)
7. Must display Expiration Date



Example of DC Gov issued Card

**Standard 3 - Card Content**

1. Must contain Electronic Content Digitally Signed By PIV Issuer
2. Must contain Digital Photograph (1 or 2) of applicant
3. Must contain Digital Fingerprint Images (Left and right index)
4. Must contain PKI Certificates (One per access level)
5. Must contain User Identity (PIN - Personal Identification Number)
6. Must have information of PIV Issuer Identity
7. Must contain a CHUID (Card Holder Identification Number)
  - a. The CHUID includes the following, the Federal Agency Smart Credential Number (FASC-N), which uniquely identifies each card, the expiration date of the card and an asymmetric digital signature.

**Standard 4 - Optional Logic Elements**

1. Cryptographic Digital Signature (Private Key)
2. Cryptographic Challenge/ Response
3. Encryption/ Decryption
4. Key Variable Processing (PIN- based notarization)
5. Biometric Data Processing