SETECS
Secure Transactions and Electronic Commerce Systems

Tel: (301) 587–3000 **Fax:** (301) 587-7877 **http://**www.setecs.com **E-mail:** info@setecs.com

Digital World

IT Applications and Environments based on PIV Cards

This document is the White Paper suggesting an integrated security system, in a given public/business environment, based on smart cards, PKI, secure Web services and other security technologies. It may be used as the source of ideas towards implementation and deployment of various IT applications and working environments, based on PIV cards. The ”Digital World” concept envisions an unified and integrated security system for various IT applications, physical access control system, and distributed, wireless applications, using hand–held devices.

Such an initiative can be organized in the form of several parallel projects. For consistency, planning and scheduling the individual projects may be organized in the following five groups:

1. Security Infrastructure Projects

The goal of these projects is to establish security infrastructure across the specified environment, which will provide common security services to all other components of the security system.

1.1 Integrated IDMS

The purpose of this system is to integrate various existing proprietary and legacy Human Resources (HR) systems into an unified IDMS, compliant with the FIPS 201 data model. The system would be the source of personal data for issuance of PIV cards.

1.2 FIPS 201 (HSPD–12) Card Management System

The purpose of this system is to accept data from the IDMS, enroll applicants, issue them PIV compliant smart cards, and perform post–issuance maintenance of these cards.

1.3 Public–Key Infrastructure (PKI)

This system provides generation and distribution of public–key (X.509) certificates. Certificate Authority (CA) servers must be installed in individual security domains, to reflect their security policies, and also integrated across the environment in the large–scale PKI. The system must be integrated with the IDMS and CMS to receive data about certificate owners.

1.4 Role–based Authorization and Access Control System (RBAC)

This system must maintain unified set of roles and policies across the selected environment and enforce authentication and authorization to various IT applications based on those policies.

2. Secure IT Applications

Secure IT applications are standard or customized applications extended with security services, based on usage of X.509 certificates, PIV smart cards, and other security technologies.

2.1 Security for Microsoft Environments

This is the set of security applications for MS environment based on PIV cards: login into the workstation, login into the network, secure browsing, and secure processing of local files.

2.2 Secure E–mail

This application provides protection of E–mail letters (encryption and digital signature) using PIV cards. It can be used with Microsoft Outlook or Mozilla Thunderbird mailers.

2.3 Secure Web Services

This is security technology that can be used with any Web–based application. It provides authentication (single sign–on), authorization and access control services in a Web environment.

2.4 Secure PDF Documents

This is security technology that can be used with any PDF document. It provides encryption and digital signatures for PDF documents, plus authentication, authorization and control of access for users.

3. PAC Systems

Physical Access Control Systems (PACS) can be nicely used with PIV cards for control of access to buildings and offices, visitors' management and access to facilities.

3.1 Enrollment and Access Rights Management

This is the system that combines data from PIV CMS Servers with PACS Servers, so that data about PIV cards are immediately available for management of access rights.

3.2 FIPS 201 (PIV) Compliant Readers

The goal of this project is to upgrade existing smart card readers at the doors of offices and facilities to become PIV–compliant, accept and use PIV cards for control of physical access.

3.3 Integrated PAC Systems

This system provides control of access to buildings and offices. It must be integrated with the IDMS and CMS to receive data about card holders and their cards, and also integrated across multiple locations in the DC, to provide control of access to multiple, distributed locations and facilities.

3.4 Lobby PACS Station

This is the PC that can accept PIV cards and verify visitors in lobbies of the buildings in the selected environment. The stations are integrated with PACS Servers and other PIV Card servers for updates of data and keep the log of visitors.

4. PIV Cards with Hand–Held and Mobile Devices

This set of products enable usage of PIV cards with mobile notebooks and hand–held devices. They can be used for various LACS and PACS applications.

4.1 FRAC Applications

Those are applications on hand–held devices that use First Responders Access Cards (FRAC) for identification, authentication and authorization of first responders.

4.2 Police Department Applications

Those are applications to be used by police officers in their patrol cards in combination with notebook computers.

4.3 Parking Ticketing Applications

Those are applications for controlling parking meters, issuance and administration of parking tickets.

5. Other Applications based on PIV Cards

This is a diverse set of applications where some form of a smart card can be used.

5.1 Public Transportation Cards

Proprietary public transportation cards can be replaced by PIV cards, extending them with payments and other types of smart card applications.

5.2 Smart Cards for Public Services

Those are smart cards that can be used for distribution of food stamps, in schools, public libraries, etc.