Federal Deposit Insurance Corporation deploys smart cards and PKI to internal staff and field agents

The path to implementation of PKI/smart cards by the Federal Deposit Insurance Corporation (FDIC) shows the use of technology, timelines, and reflect the costs that the FDIC incurred. Furthermore, lessons learned are provided at the end of this section to assist agencies as they build their business cases. This case study was selected because FDIC has moved beyond the planning phase and is actually implementing PKI/ smart card technology.

THE FEDERAL DEPOSIT INSURANCE CORPORATION

The Federal Deposit Insurance Corporation's mission is to maintain the stability of and public confidence in the nation's financial system. FDIC has about 7,800 employees.

FDIC generated its first certificate policy and certification practices statement in 1998. The FDIC's Electronic Travel Voucher (ETV) system was its pilot program. ETV currently makes use of encryption and digital signature technology. FDIC has issued 3,500 certificates in FY 2000 and plans to issue about 5,000 more in FY 2001 to complete the PKI enabling within the corporation.

In addition, FDIC is using Entrust profiles on Datakey 330 smart cards. FDIC is currently using smart cards, combined with photo ID proximity badges, to perform PKI administration. FDIC also implemented secure extranet applications using digital certificates for FDIC external clients. This is a low assurance PKI used for authentication purposes only. FDIC maintains the PKI in-house because it will be used for the core functions of the agency. FDIC spent $5.0 million in FY 2000 and plans to spend $2.5 million in FY 2001.

FDIC is currently working on developing a high level Application Programming Interface (API) to make it PKI consistent irrespective of which PKI product is used. This will facilitate the development and wide-deployment of PKI-enabled applications.

Table 1 provides the FDIC mission and vision statements. The FDIC has insured deposits and promoted safe and sound banking practices since 1933.

FDIC's Mission and Vision Statements

FDIC Mission
"The FDIC, an independent agency created by Congress, contributes to stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, and managing receiverships."

FDIC Vision
"To assure that the FDIC is an organization dedicated to identifying and addressing existing and emerging risks in order to promote stability and public confidence in the nation's financial system."

The implementation of PKI/smart cards promotes both the FDIC mission and vision by:

- Addressing potential risks due to security breaches
- Ensuring only authorized personnel gain access to sensitive data
- Improving the ability to track and detect suspicious activity across FDIC systems
- Ensuring the confidentiality, integrity, and availability of its information are maintained.

Background

FDIC has successfully combined picture identification badges with smart card chips mounted on the badge. The badges, controlled by the security office, are issued after an employee has participated in the FDIC personnel security program. Unlike a generic token, these are registered to a specific user.

To implement these badges, a product search was undertaken that was limited to those devices capable of operating within the FDIC's PKI. Datakey 330 smart card chips were selected and have been tested. The new Datakey 330 cards have undergone Federal Industry Processing Standards (FIPS) 140-1 level 2 verification. FDIC is currently using smart cards, combined with photo ID proximity badges, to perform PKI administration.

Following pilot testing, it is expected that FDIC will begin using smart cards for all high-risk electronic transactions that require a digital signature. When this technology is combined with a picture badge, the FDIC will be able to satisfy user cryptographic requirements associated with General Accounting Office (GAO) authorization.

Low Assurance PKI

FDIC uses a low assurance PKI for a number of SSL Web-based applications on its extranet with its member institutions and other parties that are external to the agency, such as other state or Federal agencies. Browser certificates are used to control access to the extranet Web server. The extranet PKI uses a 128-bit RSA encryption via SSL, and employs Entrust WebCA software. The extranet PKI currently has about 2,000 certificates issued and is from the medium assurance PKI. The extranet uses software-based protection mechanisms (Web browser certificates). It provides authentication only.

Electronic Travel Voucher System Pilot

FDIC has approximately 3,500 field representatives with laptops. All field representatives will have to use ETV to get reimbursed. The electronic system is interfaced with the National Finance Center (NFC). Previously, it took up to two months for field employees to be repaid, but after the implementation of smart cards it now takes two days for a direct deposit to reach the employee's account. The paper reimbursement process used to cost about $50 a transaction to process, whereas the new process costs less than $10. FDIC processes about 80,000 to 100,000 vouchers every year. This results in savings of about $3.2 to $4.0 million.

In addition to quantitative advantages such as cost savings, qualitative advantages to using the ETV include:

- Quality of data check
- Expedience of service
- Reimbursement is a direct deposit to the checking account.

ETV uses digital signatures and some encryption. Although the transition to PKI was a significant change for the employees, the expedience with which they are reimbursed has led to this technology being welcomed by the field representatives. As a result of the success of the ETV pilot program, FDIC has expanded the program to a fully operational, on-going cryptographic smart card endeavor.

PKI Enabling Within FDIC

FDIC generated its first certificate policy (CP) and certification practices statement (CPS) in 1998. Development of the version 1 policy took approximately 1 month and underwent OIG review. FDIC is planning plans that future development and revisions should last no more than 3 months. A single CP[1] is being generated to address four assurance levels. This will use the DoD CP as a template. FDIC is reviewing the Federal Bridge Certificate Policy for cross certification purposes. Each CA will have a Certification Practices Statement (CPS).[2] Each of the assurance levels will have a separate certificate profile. Specifically, the approach is to use Federal Information Processing Standards (FIPS) 140-1 validated hardware cryptographic modules for the CA. High assurance digital signatures will also become part of the smart card capabilities.

Through a competitive bid process, FDIC selected the firm Entrust as its PKI provider. Within FDIC, the PKI is run internally (not outsourced) and managed by the people who manage the issuance of passwords. The current architecture consists of an Entrust Manager (version 3.0c1) and an ICL X.500 version 7B Directory Service. The client software that is deployed to the user is the Entrust Client v3 for desktop users and Entrust Entelligence v4.2a (with Entrust ICE/ True Delete/ Secure Delete) for the laptop users. The infrastructure is currently being upgraded to Entrust Manager v4, with the hopes of increasing it to Entrust Authority (version 5) very soon. Additionally, the hosting CA platform will support a FIPS 140-1 level 4 cryptographic module to contain the CA signature keys, once upgraded.

Entrust provides free toolkits that enable the Secure Communication Manager (SCM) to interface with high level cryptographic Application Programming Interface. SCM is an FDIC developed middleware application that is intended to reduce the complexity of the underlying mechanisms while facilitating service requests through simple service calls. The SCM was modified to recognize hardware tokens.

The FDIC is working with other government agencies in defining a high-level API that would work with developed government off-the-shelf (GOTS) applications. This interface will be PKI consistent regardless of which PKI product is used. This will facilitate the development and wide deployment of PKI applications and will make support across multiple PKI products less difficult. FDIC has established links with the Department of Energy, Department of Treasury's Financial Management Services Division, NIST and GAO. FDIC has also had some contact with the Environmental Protection Agency and feels that the Department of Army may show interest.

Certain client software upgrades need to be made before migrating to Entrust 5.0 Manager. FDIC is testing the build for a corporate desktop upgrade that will bring everything up to version 4.X. FDIC is also procuring the software necessary for establishing a full PKI for the Extranet. FDIC will shadow the internal directory to the extranet Border Directory and cross certify with customers. FDIC expects to cross certify with the Federal Bridge CA at the low assurance level using this interface.

Phase 1 of the PKI enabling will involve 2,500 examiners who are in the field most of the time. These examiners need assurance that there is only one key set, but this cannot be accomplished with

a floppy disk that can be copied, whereas it can be accomplished by a smart card. The issuance of smart cards will be coordinated with the badge issuance office. The badge issuance vehicle will also be the issuer of smart cards.

Phase 2 will include the rollout of PKI on all desktops. Currently, this phase is expected to commence in early 2001.

The smart card will also be used for physical access except in places where office space is leased and it may not be possible. In other staffed access controlled areas where the badge is presented to the reader, it actually scans the image of the bearer of the card and provides physical verification to the guard. The computer room where the CA is located has a guard posted, and access is limited, by card key badge, to authorized personnel. There are still areas within the FDIC where five-button security (cypher locks) will continue to exist.

Program Management and Support

Program management and support are on-going throughout the lifecyle of the project. These program management activities include the following:

- Training
- Help desk
- On-going maintenance
- Audit

Training within the FDIC is an on-going process based on a "train the trainer" model. FDIC has numerous help desk facilities. The on-going maintenance contract FIDC has with Entrust is its Silver program, which costs 18 percent of the contract value per year. Administrators and government oversight personnel perform auditing to ensure contract compliance.

Certificate Life Cycle Management

The on-going certificate lifecycle management process is clearly defined within the FDIC and is explained in detail below.

Certificate Issuance. The core users have been issued certificates. The FDIC opted to develop an automated registration tool to support the ETV rollout. In contrast, the use of smart cards will eventually require a human in the loop to issue a key because FDIC will use High assurance cards that require a human validate the cardholder.

Certificate Renewal. Certificate renewal is automated within Entrust. The certificate policy specifies the validity period. When the certificate nears expiration, it is automatically renewed unless explicitly denied.

Certificate Distribution. Certificates are distributed within the Entrust product to the client. Encryption certificates populate the X.500 directory and the signature certificates are concatenated with the signature of the CA.

Certificate Backup and Recovery. The Entrust Manager is backed up daily. Recovery requires RA intervention. The RA must establish that the user is whom they claim to be. There is also an information security officer reporting system that is used to make recovery requests.

Testing and Maintenance. New software versions must be tested in lab and test environments. Older versions of the software are not supported by the vendor and therefore need upgrading.

FDIC Timeline

FDIC was able to successfully complete PKI enabling of its pilot project at the scheduled time. It plans to roll out PKI/smart cards to all its employees and some contractors by March or April 2001.

FDIC had planned to complete the rollout by January 2001, but a delay in deploying Windows 2000 software had delayed the full implementation by a few months. As explained earlier, FDIC has decided to keep the PKI endeavor in-house and has not contracted out any portion of it. FDIC has established the tentative timeline shown in Table 2 for implementing PKI/smart cards.

Major FDIC PKI/Smart Card Implementation Timeline

Needs Study	January '97
Low Assurance PKI	January '98
Certificate Practices	August-Sept '98
ETV Decision	Early '98
ETV Cut Over	December '99
Issuance - 3500 Cards	November '00
Full rollout	March-April '01

Decision to Not Outsource

The crux of FDIC's decision to not outsource relates to the future vision for PKI/smart cards. FDIC will use smart cards for its high dollar value obligations in the future. Such a critical and core function should not be outsourced to an outside vendor because the potential for significant losses is high. By keeping this function in-house, FDIC retains control of the function and can take appropriate steps to protect against losses.

The other deciding factor was that a GAO sanction will not allow for this core function to be outsourced, and FDIC is obtaining this GAO sanction. Because many financial obligations will be made with digital signatures, it can be expected that the GAO will become involved. The concern is that data integrity could be compromised. GAO will sanction only a high level of assurance that will require a person in the loop for face-to-face identity proofing.

Costs

Thus far, the cost of PKI enabling within FDIC has been $1 million for the program management of the infrastructure alone. The $1 million does not include CA contract support, FDIC contract support or government personnel time.

The costs of planning and project review were not assigned to the PKI/smart cards endeavor. Rather they were subsumed in the overall operations cost of the agency.

As an agency, FDIC had the advantage of being able to roll up the costs of hardware with its enterprise-wide laptop upgrade. Only the costs for the tokens and the readers were assigned to the PKI/smart cards project. This meant that the only costs were those for standing up the PKI, which was $1 million in program management costs. FDIC did not incur middleware costs as the SCM was developed in house, so that in house applications can call a high level API.

The ETV pilot, which has been described in detail previously in this report, cost approximately $2.75 million to stand up. All of these costs were incurred in FY 2000. The cost of issuing cards and readers was $357,000 for approximately 3,000 tokens and is expected to be $678,300 in FY 2001 for approximately 5,700 tokens. A one-time testing cost of $100,000 was incurred in FY 2000.

Ongoing help desk support that is staffed by contractors from Computer Associates is expected to be approximately $300,000 for the first two years when the PKI/smart cards are being put in place. When proficiency has increased, helpdesk

costs are expected to decline. System administration, including auditing and training, is expected to require three FTEs and have a recurring cost of approximately $300,000 per year. Ongoing maintenance is provided under the Entrust Silver program, which is 18 percent of program management costs or approximately $200,000 each year throughout the life cycle of the project.

	Year 1 (FY 2000) Total Costs	Year 2 (FY 2001) Total Costs
Number of New Certificates	**3000**	**5700**
PROJECT REVIEW		
PLANNING		
Policy Development		
Implementation Plan		
Test & Acceptance Plan		
Bid Evaluation Strategy		
Bidder Communications		
Bid Review		
Award Negotiations		
APPLICATIONS ENABLING		
Program Management	1,000,000	1,000,000
Toolkits		
Application Upgrades		
Installation/Modify Applications		
Smart Cards	66,000	125,400
Card Readers	291,000	552,900
Issuance Stations		
Test and Evaluation	100,000	
Support		
Upgrade/Product Improvement		
TOTAL APPLICATIONS ENABLING	**$1,457,000**	**$1,678,300**
OPERATIONAL CAPABILITY		
Program Management		
Concept Exploration (Pilot)	2,750,000	
Training - System Administrator		
Training - End User		
Documentation		
Auditing		
Helpdesk Support	300,000	300,000
System Administration	300,000	300,000
Vendor Relations Management	200,000	200,000
TOTAL OPERATIONAL CAPABILITY	3,550,000	800,000
CERTIFICATE LIFE CYCLE MANAGEMENT		
TOTAL COSTS BY YEAR	**$5,007,000**	**$2,478,300**

Notes:
1. Planning and project review costs were not directly assigned to the PKI Smart Cards project.
2. Certificate life cycle management is part of vendor relations management costs.
3. Year 1 costs include the cost of the ETV pilot, which is $2.75 million.

LESSONS LEARNED

These two case study candidates demonstrate that it is possible to implement PKI/smart cards irrespective of the size of the agency. Although there is currently no uniform methodology of implementing PKI/smart cards, there are three different methods that an agency can use. An agency can either outsource the activities or decide to conduct all the operations in-house like FDIC decided. The advantages and drawbacks of both have been discussed. A third method involves a government-owned/contractor operated type ownership, where a user owns the PKI, but a contractor provides customized PKI services.

Benefits Versus Risks

The FDIC was aware of the general risks posed by use of PKI and smart cards and the obstacles to successful implementation. However, FDIC believes that the benefits outweigh the risks and have, therefore, proceeded with the implementation of cryptographic smart cards. In fact, discussions with agency personnel from FDIC reveal that they believe there is no better option for security available and that implementing PKI/smart cards is an inevitable decision.

Costs Versus Benefits

FDIC incurred substantial costs in implementing PKI/smart cards. The incremental costs of each added layer of security should be analyzed against the extra benefit that the added security feature provides. FDIC used PKI to enhance their security and realize higher levels of authentication, data integrity, nonrepudiation, and confidentiality. They also purchased smart cards due to the added benefits of portability, scalability, and interoperability. Although biometrics technologies offer a higher level of security, they felt that the currently high costs of biometrics readers makes this option not feasible for now

Preparing for Implementation

The implementation of PKI/smart cards infrastructure requires significant planning and consideration throughout your agency. Below is a checklist of some of the important factors that your agency should consider before implementing cryptographic smart cards. This checklist is distilled from literature review and is based on lessons learned from the case study and interviews with both PKI and smart card subject matter experts.

1. Prepare a Certificate Policy and a Certificate Policy Statement

A certificate policy is a bare minimum requirement that has to be prepared before operating a PKI infrastructure in a disciplined environment. A certificate policy will provide the map for your agency's business model for electronic transactions. Additionally, a certificate policy statement should be prepared if your agency is going to operate its own certificate authority (CA) or have a contractor operate the CA on behalf of the agency. This certificate policy statement defines the operating procures for your CA, namely, key management.

2. Determine Your Agency's Need for Interoperability

If your agency has a high need to transact business with other agencies, the Federal Bridge Certification Agency (FBCA) is a very efficient mechanism to provide the interoperability required for this interface. The advantage of linking with the Federal Bridge is that you enter into one certificate management arrangement with the bridge and have access to all other Federal Bridge users rather than having to draft bilateral agreements with every agency with which you conduct business. If your agency chooses to operate with the FBCA, it should con-

sider the certificate policy of the bridge in framing your own certificate policy. Additionally, the GSA Smart Access Common ID Program contract is a means of obtaining interoperable smart cards that can used between agencies.

3. Consider Phasing In Implementation

Discussions with agencies about their PKI enabling efforts indicate that it is more practical to adopt a phased in approach to PKI. This incremental implementation allows your agency to learn from and deal with any mistakes you may make in the pilot process and allows for the scaling up of such activities as program management and helpdesk capabilities. It also allows the cost of implementation to be spread over more than one fiscal year, which could prove beneficial in securing necessary funding.

4. Departmentwide Implementation and Policies

The substantial infrastructure investment and ongoing certificate issuing costs of PKI suggest that a department-wide approach be taken to achieve centralization of infrastructure and economies of scale. The substantial marketing efforts that will be required to establish incentives and to encourage adoption of PKI digital signatures by users and constituents suggest that a centralized marketing campaign would be more effective and economical. A number of commonalities could exist among agency functions and users that will have to be established. Although each agency has a different mission, the commonalities would suggest that a unified approach could be taken to meeting information security requirements. Several PKI solutions are being tested in pilot projects within specific departments that use certificates from several vendors. It is possible that any PKI applications going forward can be met by an enterprise approach to PKI within each department. The same is true of smart cards, as all agencies within a department could issue the same smart card with the same amount of memory.

5. Define the Registration Process

Your agency may decide to incorporate your certificate registration process into the existing personnel or facility office business practice of issuing identification cards. For most agencies, the smart card will replace identification cards; so this step is really streamlining PKI into an existing business process, resulting in a nominal cost impact to your agency. For example, when a new employee is hired, the subscriber agreement that is required to obtain a digital certificate and a smart card can be part of the rest of the hiring package. The smart card can be issued as part of the normal in-processing.

6. Establish a Certification Revocation Policy and Validation Procedures

Several options are available to establish certification revocation policy that disables certificates if the smart card is stolen or inoperable, or when an employee terminates. The revocation of certificates ensures that security remains intact. Two common certificate revocation approaches are Certificate Revocation Lists (which is the most common today) and the Online Certificate Status Protocol (OCSP) approach of "Validation Authority." One key decision that should be made in establishing the revocation policy is how stringent the policy will be. A very stringent policy leads to a number of revocations, while a less stringent policy results in fewer revocations. It is extremely important for your agency to put in place validation procedures, expired certificates procedures, and Certificate Revocation Lists. Also, your agency should decide who has the responsibility of providing long-term signature validation services.

7. Forecast Liability Issues

Your agency should determine up front what liability, if any, it will assume for failures in the certificates it issues and under what conditions it will assume such liability. It may be better for your

agency to posit the use of PKI as a method of preserving trust rather than creating trust.

8. Determine Use of Smart Card

A smart card has several potential uses, including physical access, logical access, electronic purse, transit cards, and medical information storage. Every agency will not require every one of these functions. Therefore, an agency needs to consider how the smart card is to be used in support of its mission and vision. An agency could first implement a card with a few applications and add additional applications after the initial set of applications are deemed stable; however, it is important at the outset to develop a vision for how the card will be used both in the near-term and long-term. This allows agencies that plan multiple applications to buy smart cards with the appropriate amount of memory at the beginning so that new cards will not have to be issued later. Rather, the new application can simply be added to the existing card thereby reducing reissuance costs.

This case study was derived from a comprehensive business case produced for the General Services Administration by Booz·Allen & Hamilton.
For a complete copy of the report please visit
HYPERLINK "http://www.smart.gov/pkibusinesscase.doc"
http://www.smart.gov/pkibusinesscase.doc
or contact the Alliance at www.smartcardalliance.org; info@smartcardalliance.org.
