National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Interagency Report 7056

CARD TECHNOLOGY DEVELOPMENTS AND GAP ANALYSIS INTERAGENCY REPORT

MARCH 2004

William C. Barker
Deborah Howard
Tim Grance
Levent Eyuboglu

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national security-related information in Federal information systems. This special publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Acknowledgements

The authors, William C. Barker and Timothy Grance of NIST, and Deborah Howard and Levent Eyuboglu of Booz Allen Hamilton, wish to express their thanks to the staff at NIST and Booz Allen Hamilton who reviewed drafts of this document and provided valuable insights that contributed substantially to the technical content of this document. We also gratefully acknowledge and appreciate the contributions made by participants in the 8 and 9 July 2003 Storage and Processor Card-Based Technologies Workshop and by the government user community personnel who contributed their time and insights to the requirements interview process. Special thanks are due the speakers for their clear and comprehensive presentations and acute insights. The authors would like to acknowledge the assistance of the NIST Conference Program Staff, Laura Gooding, and Katie MacFarland without whose tireless efforts; the workshop would not have been a success. Finally, the authors would also like specifically acknowledge Teresa Schwarzhoff, Jim Dray, and Donna Dodson of NIST, and Edward Oppenheimer, Ketan Mehta, and Gene Troy of Booz Allen Hamilton for their extensive review and comment and keen and insightful assistance throughout the development of the document.

TABLE OF CONTENTS

Executive Summary

Federal government use of storage and processor cards for identification and other business purposes are growing at an impressive pace. The number of cards in use is growing into the tens of millions. Accompanying the growing use of storage and processor cards is a growing need for interoperability in the hardware and software associated with those cards necessary to support efficient procurement, maintenance, training, and operations.

The General Accounting Office (GAO) issued a report in January 2003 that evaluated the progress in promoting the use of smart cards across the Federal government. The "Progress in Promoting Adoption of Smart Card Technology" (GAO-03-144 report) sets forth recommendations regarding the role of the National Institute of Standards and Technology (NIST) in the United States Government Smart Card (GSC) program. As an initial response to the recommendations, NIST hosted the Storage and Processor Card-Based Technology Workshop. This workshop was organized to identify requirements for card-based storage and processor technologies, card industry capabilities and trends, interoperability requirements and issues, and requirements and capabilities for single-platform integration of multiple technologies. NIST not only developed and distributed card technology capabilities and requirements questionnaires and conducted interviews with Federal government agencies to further identify the state of current and planned technologies.

Workshop presentations and interviews disclosed several issues associated with 1] security and privacy, 2] multi-technology integration, 3] standardization of implementations across organizations, and 4] interoperability. These issues have been examined for evidence of gaps in existing standards and other factors that hamper government-wide application integration. It was found that varying requirements affecting the agencies' selection from among various card technologies appear to be based on the following factors:

- Policies and business processes unique to each agency
- Cost effectiveness of technologies
- Variation of security requirements from agency to agency
- Availability and maturity of technologies and related standards
- Need for interoperability among sectors and among organizations within sectors

These factors, along with the capabilities and limitations of new and existing technologies, were used to identify gap areas in the existing agency policies and regulations and relevant standards. With respect to policy, agency-unique rules and regulations for identification (ID) proofing need to be addressed for interoperability.

The following technology gaps have been identified:

- Biometrics interoperability
- Standards for co-existence of multiple technologies on a card
- Post-embedding printing standards
- Implementation of different options in formal standards can lead to non-interoperable solutions between cards and card readers

- Lack of standardized tests for optical effectiveness and clarity of holograms or diffraction gratings
- Need for common standards for identity methods and machine-readable travel documents (both inter-agency and international).

This report includes findings captured from the workshop, interviews, and questionnaires. Although requirements for co-location of different technologies on a common card were identified, no requirements for on-card interconnection of different technologies (e.g., optical stripe media, barcodes, magnetic stripes, and smart cards) were expressed. The overall conclusion derived from the findings is that although the building blocks (e.g., international standards and interagency specifications) are in place to support interoperable secure identification systems, business, management, and policy decisions limit the opportunities for interoperability. Specifically, policies regarding what personal information may be stored on card-based storage and processor systems need to be coordinated among agencies, and where necessary, codified in law. Just as importantly, responsibilities and infrastructures for entering and maintaining personal data onto the cards need to be established.

As each new card technology or application is developed, modification of the standards base will be needed to bridge the gap between existing and emerging card technologies and applications. However, to be useful, technical standards need to be consistent with policies that govern the relevant functional requirements for technology. In the case of card-based technologies, policy consensus needs to be established as a prerequisite to prioritization of technical standards activities. Gaps in card technology standards coverage necessarily result from technical innovation. However, the technologies supported by existing standards appear to be adequate to support most current user requirements. Policy and infrastructure developments can be expected to establish requirements not accounted for in existing standards. As these policy and infrastructure developments continue to occur, additional standards requirements are expected to emerge.

1. Introduction

Plastic cards that include information storage and processor components are used in the public and private sectors for identification, authentication, authorization, and mobile personal information storage. Many technologies (e.g., optical stripe media, barcodes, magnetic stripes, and contactless and smart card integrated circuit chips) have been implemented on card platforms. Card platforms now include anti-counterfeiting elements to increase the security of the physical platform. Some cards now support multiple technologies. Voluntary industry consensus suggests standards for many individual card technologies are already available. However, the full set of these technology elements has not been addressed in a single document with respect to issues associated with integration of multiple technologies on a common card platform. The General Accounting Office (GAO) issued a report, "Progress in Promoting Adoption of Smart Card Technology" (GAO-03-144 report, January 2003). This report evaluates the progress in promoting the use of smart cards by the Federal government and sets forth recommendations. Specifically, the report provides a set of recommendations to reinforce the role of the National Institute of Standards and Technology (NIST) in the United States Government Smart Card (GSC) program and recommends that—

> …NIST, continue to improve and update the government smart card interoperability specification by addressing government-wide standards for additional technologies—such as contactless cards, biometrics, and optical stripe media—as well as integration with PKI, to ensure broad interoperability among Federal agency systems.[1]

In support of the GAO recommendation, NIST initiated an effort to identify the state of operational and developmental storage and processor card-based technologies and the nature of user requirements for and constraints associated with integrating these technologies onto single platforms. To date, the NIST effort has included a NIST-hosted Storage and Processor Card-Based Technologies Workshop, distribution of requirements and capabilities questionnaires, and interviews with Federal government agencies to identify user requirements and the state of current and planned card programs. Each activity included fact-finding regarding individual technologies, integration of technologies, and interoperability of technology applications across organizational boundaries. This document reports the findings from these efforts and suggests priorities for follow-on activities.

1.1 Purpose

This *Card Technology Developments and Gap Analysis Interagency Report* (IR) provides information regarding current technical capabilities and limitations, current user requirements for individual and integrated technologies, and major impediments to technology exploitation. The report also identifies existing standards governing card technologies (see Appendix E). This document identifies gaps in standards coverage for card-based storage and processor technologies.

1.2 Scope

This report captures findings from the Storage and Processor Card-Based Technologies Workshop, government and industry questionnaires, and feedback from government managers. It makes recommendations regarding policies, infrastructures, standards, and specifications and identifies issues associated with integrating multi-technology composition, security, and interoperability.

---

[1] United States General Accounting Office, *Progress in Promoting Adoption of Smart Card Technology*, GAO-03-144 (January 2003)

1.3 Audience

This document has been created for Federal government, private industry, and public sector interests responsible for developing and implementing storage and processor card technologies programs.

2. Storage and Processor Card-Based Technologies Workshop

2.1 Overview

NIST hosted the Storage and Processor Card-Based Technologies Workshop on July 8 and 9, 2003. The purpose of the workshop was to develop and exchange information regarding the requirements, standards, capabilities, and gaps in standards coverage for individual and integrated storage and processor cards. Guest speakers from major Federal government programs, large local government programs, industry, major associations, and card suppliers from various countries participated in the 2 days of panel sessions.

2.2 Workshop Sessions

A 2-day workshop was organized into several panel sessions. Each set of presentations was followed by questions and comments. Two panel sessions were hosted on Day One of the workshop. In the first session, Federal government agency representatives discussed card technology requirements. In the second session, technology providers addressed current card technology capabilities. During Day Two, private industry representatives discussed security and privacy requirements and issues, integration and interoperability requirements and issues, and a forecast of future trends. Appendix D includes presentation viewgraphs and extracts from speaker observations and participant interactions. An overview of panel proceedings follows.

2.2.1 Federal Government Card Technology Requirements

Five speakers from the Federal government participated in a technology requirements discussion. Each speaker presented information concerning existing card technology implementations and projected future actions that might affect his or her organization's direction. Panelists included representatives from Department of Defense (DoD), Department of State, Department of Agriculture, and Transportation Security Administration (TSA).

The primary requirement for use of card-based storage and processor technology was as an authentication tool. Representatives emphasized effective infrastructure setup and ease of use as necessary to achieving total systems solutions.

2.2.1.1 Department of Defense Presentation

DoD, one of the major users of card-based technologies, uses cards as authentication mechanisms and as data storage media. Its requirements for cards as an authentication tool rather than a data storage device are based on the following:

- Synchronization of data on card and in database
- Reducing dependence on the storage limitations of cards
- Privacy and secrecy of information carried by and associated with combatant personnel.

DoD is in the process of resolving the difficulties associated with managing and maintaining a widely dispersed storage and processor card base. Managing the update process for information stored on cards is a particular challenge. Currently, the DoD has post-issuance portals to which cards can be returned for updating sensitive information (e.g., e-mail certificates). DoD wants to explore decentralization of the card update process. Ideally, all cardholders should be able to complete several card management tasks at their own workstations via a Web-enabled system. It is hoped that web enabling will reduce dependence on the issuance infrastructure. Several observations were made during the DoD session:

- DoD needs a more efficient implementation to permit organizations to recognize identification credentials at each other's facilities (for example, a faster public key infrastructure (PKI) implementation supporting physical access control). An observation was made that DoD needs PKI implementations that eliminate the necessity of multiple credentials for users who must access a number of different facilities that have unique credential requirements. DoD has determined that government agencies need to be able to accept each other's credentials based on an agreed set of rules. The challenge here is reaching agreement on a common set of rules and on appropriate federated cross-credentialing relationships.

- NIST IR 6887, Government Smart Card Interoperability Specification (GSC-IS), maximizes interoperability in DoD use of cards from different vendors. However, the need to reduce or eliminate middleware dependence suggests a need for additional interoperability specifications. Specifically, DoD perceives a need for a common implementation of Java card and/or Open Platform. The goal is to enable agencies to seamlessly integrate new cards from various vendors into their own systems. This need is acute in the contactless smart card arena.

- Different operating systems (e.g., Windows and Macintosh) should conform to common standards so that desktop computers will include capabilities to read any smart card.

- The requirements that drive physical access control within the DoD are increased security, reduced manpower, and convenience. An access control system should be as transparent to the user as possible within the constraints of security requirements. Less complex user interfaces may result in improved security through reducing human error. DoD has undertaken a pilot program that evaluated ease of use and security capabilities associated with implementing fingerprint biometric technology on a contactless chip. Another pilot program expanded the capabilities of the first pilot by increasing the card base and adding hand-geometry biometrics. The results of these pilot programs will support future physical access policy and standards development.

2.2.1.2 Department of State Presentation

The Department of State is contemplating using card-based technology as an authentication tool or a data storage device. However, different policy, technical, and business requirements underlie the authentication issues associated with various government travel documents[2] (e.g., U.S. passports, U.S. visa labels, and identification [ID] cards). Therefore, it is difficult to arrive at a standard solution that will accommodate all requirements. For data storage, the Department of State is considering Optical Card Reader B (OCR-B),[3] 2-D barcode, contact and contactless smart cards, magnetic stripe, and optical memory[4] technologies. Different technologies are favored for different document classes, but the State Department currently favors contactless smart card technology for its applications. The agency determined that International Organization for Standardization (ISO) 14443-based contactless smart card technology could best accommodate its various document formats. Legislation, such as the Patriot Act of 2002 (Public Law 107-56, October 26, 2001), mandates the collection of biometric identification on all people entering the United States. The legislative mandate drove the Department's decision to use facial imaging technology. The agency is now researching technologies that embed an ISO 14443 contactless chip into passports.

The following technology gaps were identified in the course of the Department of State session:

---

2 The International Civil Aviation Organization (ICAO), Document 9303.

3 Optical Card Reader B.

4 ICAO is no longer considering optical memory for Machine Readable Travel Documents (MRTD).

- Consensus is needed for durability tests and performance levels.
- A lack of biometrics interoperability exists.
- Tests are needed to support comparison of optical effectiveness and clarity of holograms or diffraction gratings.

2.2.1.3 Department of Agriculture Presentation

The Department of Agriculture has successfully implemented a magnetic stripe-based benefits program. A magnetic stripe card is used primarily as an authentication tool that enables the user to access the database on line. The Department chose to align its implementation with existing electronic funds transfer practices. It also required state programs to be interoperable so that a user from one state could shop for merchandise in any other state. Because the requirements were based on standard electronic funds transfer industry practices, the Department of Agriculture managed to achieve its objectives with minimum difficulty.

2.2.1.4 Transportation Security Administration Presentation

The TSA is contemplating using card technology as an authentication tool and storage device. The TSA hopes to improve security, enhance commerce, and protect personal privacy by establishing a system-wide common credential among all transportation modes. Given a focus on business issues, the varying requirements of different transportation agencies have resulted in multiple physical access credential types. TSA needs to be able to establish interfaces with other Federal agency databases. If all the credentials from different agencies could be consolidated, significant cost savings would be achieved.

2.2.2 Current Card Technology Capabilities

In the second panel discussion, several technology providers presented information about the capabilities of existing and emerging card technologies. The vendors represented various card technology areas (e.g., contact and contactless smart cards, barcodes, and optical cards). Vendors of special security features (e.g., digital watermark and holograms) were also represented. Speakers offered opinions about existing standards, technology conflicts, products, and future standardization needs.

2.2.2.1 Smart Cards

One presentation included an assessment of card operating systems, protocols, memory capacities, and functionality as they relate to smart cards. It was also noted that integrating Universal Serial Bus (USB) interfaces with smart cards provides faster transaction speeds than had previously been experienced. With respect to memory requirements, vendors stated that smart cards with 32 Kilobyte (KB) Electronically Erasable Programmable Read-Only Memory (EEPROM) were common, as are 64 KB cards. Smart card capabilities include encryption, digital signatures, on-card key generation, and on-card biometrics matching.

Several outstanding technical challenges were observed:

- Implementing PKI with contactless cards
- Providing discrete memory access through a contactless interface
- Executing complex algorithms on dual interface cards (i.e., cards that combine contact and contactless interface).

Other observations included a (1) necessity for developing new standards that are required to address the changing user requirements, such as added security, (2) requirement to update existing standards as required to accommodate technological advances, and (3) need to test all new technologies to validate their compliance with standards.

Issues related to managing card issuance and maintenance were also raised. Significant card management issues associated with multi-application smart cards result from the interactions between those who manage card issuance and update and those who are responsible for the processes being supported or enabled by the cards. Decisions regarding who owns the card and who has authority to update, modify, and maintain the card and applications are critical to program success. Two management alternatives were discussed: (1) in an issuer-centric model, the issuer is the only owner of the card and manages all administrative tasks, such as card update and maintenance, whereas (2) in the alternative application provider empowered model, there is no centralized card management by a single issuer. Rather, each product application is owned and managed separately by user organizations. Standardization on a common management model would facilitate interoperability.

2.2.2.2 Contactless Smart Cards

Contactless smart cards were discussed in the Current Card Technologies session. Much of the discussion focused on transit industry implementations. The new applications, including transit applications, are demanding higher transaction speeds. Contactless smart card technology accommodates these higher transaction speeds. A major driver in the trend toward multi-technology cards is the deployment of an increased number of smart card based regional transit applications. The benefits of the contactless cards include enhanced security, transaction speed, and multi-application capability. There are three options for migrating to contactless smart cards: 1] using multi-technology cards, 2] adding smart card stickers [5] to existing 125 kilohertz (kHz) proximity cards, and 3] deploying multi-technology readers that are capable of reading both technologies. The first option was described as more susceptible to failure; the second, less expensive but offering potential policy-related problems (e.g., consequences of inferior sticker reliability); and the third, the most expensive.

2.2.2.3 Barcodes

Barcodes were discussed as an alternative data storage technology. An ultra-high density barcode scheme was described during the second panel session. Ultra-high density barcodes easily print in various resolutions through a wide variety of printing technologies and can achieve up to 32,000 bytes of memory capacity. Barcodes also can be read very easily using standard scanners. This provides an additional backup capability to smart cards in case chips fail. It was observed that ultra-high density barcode is a recent technology with an unproven track record.

2.2.2.4 Optical Memory Cards

Optical memory cards offer high-capacity data storage capabilities for authentication and other functions. The important characteristics of the optical cards are high data capacity (4 MB); counterfeit resistance, reliability, speed of transaction, and standards compliance. It is a write-once, read-multiple-times type of technology. Once the data is written to the card, the piece of memory is irreversibly and permanently marked with visible information that identifies the cardholder that can never be changed. Combining the optical memory with a contactless chip on the same card can increase storage capacity, resulting in added security. Only a limited number of entities use the technology. Except for the Immigration and

[5] Stickers, also known as tags, are contactless devices with an adhesive back. This allows a transition from other card technologies to contactless smart card technology.

Naturalization Service's (INS) extensive use of the cards, the infrastructure today is very limited for the optical cards. One optical memory provider recommended new standards for interoperability within the Federal government in the following areas:

- Identify the best practice for the combination of optical memory and contactless technology
- Establish new standards in the transportability of original biometric images.

2.2.2.5 Digital Watermarking and Kinegrams®

Digital watermarking technology is used to covertly encode and decode digital information that is presented in analog format (e.g., photographs and broadcast music). This technology will help detect occurrences of tampering with the original information. Security afforded by digital watermarking technology is difficult to defeat. Digital watermarking can be combined with other technologies (e.g., smart cards) to provide authenticity of information printed on the card.

The Kinegram® is a specific visual authentication security product that is designed to prevent the copying and counterfeiting of documents (e.g., banknotes and cards). The kinechip can be used with a smart card to enhance the visual security of the card media. Using this technology, a machine-readable digital certificate is optically encoded on the surface of the card and can be compared with the one that is electronically stored on the chip to ensure protection against counterfeiting. It may be technically possible to integrate the Kinegram® technology into existing smart card readers.

2.2.2.6 Technology Issues and Findings

Several issues emerged in the Current Card Technologies session.

Interoperability discussions during the session identified problems associated with requirements for cards and readers purchased from different and competing suppliers to work interchangeably. The ISO 14443 standard was observed to have interoperability deficiencies associated with security mechanisms and the absence of a standard command set that governs access to the application areas of the chip. All the fixed logic memory cards available in the market depend on proprietary encryption algorithms rather than Federally approved algorithms. This complicates the task of government evaluation of the cryptographic strengths and weaknesses of these cards. It was suggested that, in the future, secure and interoperable contactless smart card systems should be available.

A general need exists for open security standards. Future cards should use standard encryption algorithms that are embedded in the card and the reader operating systems. Effective key management procedures and secure tamperproof readers will also be necessary for true interoperability.

Employing multiple technologies on one card was also discussed during the Current Card Technology session. Speakers pointed out that card printing during the card manufacturing stage offers the highest level of quality and interoperability compared to printing during issuance. Print problems are directly linked to the type and amount of data printed on the card. Therefore, limiting the amount of data printed during issuance is likely to minimize the print issues. There is no ISO standard on post-embedding printing or on dimensions, shape, and the color of the contact plates on contact-based smart cards. A graphic that may fit well on one contact smart card may cause a printing problem on another smart card because of variations in contact plate size. Furthermore, every new item printed during post-issuance is a potential point of failure. To help prevent these issues, issuers need to involve card manufacturers in the printing process.

It was observed that higher failure rates could be expected for cards using multiple technologies because each technology has inherent reliability problems. These problems can be aggravated when the technologies co-exist on a common card. Therefore, performance monitoring is particularly important to successful multi-technology card implementation. It was stated that microprocessor cards are much more reliable than non-microprocessor cards. Most problems experienced in the field have been user or implementation related. This experience underlines the importance of user education and training. Lack of compliance with the relevant standards is another area of failure with the contactless smart cards. An important lesson learned that was shared in this session was that all personal identification number (PIN) based smart card applications need to have a means of on-card PIN unblocking without returning the card to its issuer.

The salient finding regarding card technology integration and interoperability was that the building blocks are in place to support interoperable secure ID systems. However, business and policy considerations, such as middleware acquisition responsibilities and agreement on who is responsible for loading and maintaining the cards, currently limit interoperability. Administrative and management issues, such as issuing cards and maintaining user data, remain as difficult issues associated with multi-application cards.

2.2.3 Security and Privacy Issues

DoD participants emphasized that privacy concerns are a major factor dictating the types and amount of information placed on the Department's Common Access Card (CAC). When agencies accept credentials from each other, they may have to do so in an environment that requires them to avoid sharing too much privacy-sensitive cardholder data. It was noted that widely available technologies are more attractive to attackers.

A Department of State participant voiced concern about the subjective nature of privacy and security and the consequent effects on interoperability. As a result of privacy concerns associated with fingerprint biometrics, the Department of State decided to use facial imaging on its travel documents. Variations in security requirements among agencies as they apply to government documents threaten the integrity of the mechanisms used by one agency that rely on the integrity of mechanisms governed by other agencies. For example, the integrity of a passport is questionable when the birth certificate that was used as the basis for issuing the passport is not subject to the same rigorous security standards that were applied in the passport issuing process.

During the Security and Privacy session, it was observed that contactless card standards, such as ISO 14443, do not include security provisions. This is a significant barrier to interoperability of contactless cards with other technologies.

2.2.4 Multi-technology Integration Requirements and Issues

Several issues were surfaced during the Multi-technology Integration session.

According to the panelists, different technologies that co-exist on the same card may adversely affect each other in a manner that increases the number of card failures. For example, the reader used to swipe a magnetic stripe may brush the contact on the chip. Card vendors observed that numerous potential card management issues might arise in the implementation of multi-technology cards when each on-card technology is implemented by a different agency. The ownership of the card and each of its applications, as well as the access rules and security procedures associated with use of the card, need to be determined to facilitate cardholders training and alerting agency/user personnel to potential problems.

During the Multi-technology Integration session, vendors mentioned printing problems associated with multi-technology cards. A lack of common standards for post-embedding printing results in issuers having to choose their own card designs and to dictate the amount of data to be printed on the card. Because the standards permit variations in the color of plastic, thickness of the card, and exact location of the contacts or antenna, considerable variation may exist in the cards manufactured by different vendors. This variation may result in problems when an agency has a pre-set process to print or embed material on certain locations on a card.

2.2.5 Interoperability Requirements and Issues

During the Interoperability session, Federal government participants pointed out that unique requirements of individual agencies could result in multiple physical access credentials per employee. This could potentially result in unnecessary cost to the Federal government. The use of multiple credentials also creates inefficiencies resulting from an excessive number of policy and technical processes being established by different agencies.

It was also noted that lack of biometrics interoperability resulted in implementations that use multiple biometrics templates from different vendors. For example, one card may potentially carry two fingerprint templates: one for airport access, and one for government physical access.

A Department of State participant emphasized that no standardized tests existed for a comparison of optical effectiveness and clarity of holograms or diffraction gratings. This issue could potentially result in holograms from different vendors with varying reliability and quality levels.

Panelists reported difficulty in implementing PKI in the contactless environment and expressed a need for guidelines for implementing PKI in that environment.

The group also suggested that test procedures for emergent technologies be established to validate their compliance with standards.

2.2.6 Technology Gaps Identified

The following technology gaps were identified:

- No consensus on durability tests and performance levels
- Lack of biometrics interoperability
- No standardized tests for comparison of optical effectiveness and clarity of holograms or diffraction gratings.
- No comprehensive specifications or guidance regarding storage and processor card security requirements
- No web-based portal for card maintenance
- No consensus for physical characteristics of card-enhanced or chip-enhanced travel documents

It is particularly noteworthy that current standards address only a subset of the security issues associated with storage and processor cards. There is currently no authoritative taxonomy of storage and processor card security issues, much less a comprehensive set of specifications and guidance regarding security requirements.

Widely dispersed implementation of very large numbers of cards introduces serious management challenges. DoD participants observed the need for remote management of large numbers of cards in the field. They noted that centralized maintenance (changing/updating) of card data results in inconvenience to users and administrators. A need for a Web-based portal for users to be able to perform a certain level of card maintenance through their desktops was described.

A Department of State participant observed a problem associated with embedding a contactless chip on a travel document. Standardization of the location of the chip on the document is difficult in the absence of standardized document configurations.

3. Interviews and Questionnaires

As part of its response to GAO recommendations, representatives of several Federal government organizations that are implementing card technology systems (see Appendix A) were interviewed. The purpose of the interviews was to employ an additional method to capture information regarding current and future requirements, capabilities, issues, standards, and gaps in standards coverage for various storage and processor card technologies. In addition, two questionnaires were developed to capture data from various industry resources on current card technology requirements and capabilities (see Appendix B).

3.1 Government Agency Interviews

Various Federal government representatives were interviewed regarding the scope of their current and future requirements, standards requirements, and perceptions of integration and interoperability issues associated with storage and processor card-based technologies. Many of the interviewees indicated that their agencies were currently conducting pilots to evaluate the feasibility and cost effectiveness of implementing multiple technologies on a single card platform.

The interview results that were obtained suggest that the requirements driving card technology choices vary considerably from agency to agency. Most interviewees stated that their agency's technology selections were based on agency determination regarding the best currently available solutions. Only one of the people interviewed reported a card procurement decision based on a formal agency requirement/specification. Security and privacy requirements, automation of data, and the migration of legacy systems are factors driving the selection and use of card technologies. Although one reason that agencies are piloting different technology solutions is the absence of common interagency policy and guidance, most interviewees noted that interagency policy and guidance issues must be addressed and should be considered in order to achieve government-wide interoperability.

Figure 1 depicts interview results. The applications, technologies, requirements, and issues listed in Figure 1 summarize the responses by government representatives to interview questions (see Appendix A). Figure 2 lists future card technology requirements and trends identified through interviews.

Figure 1. Current Technology Environment

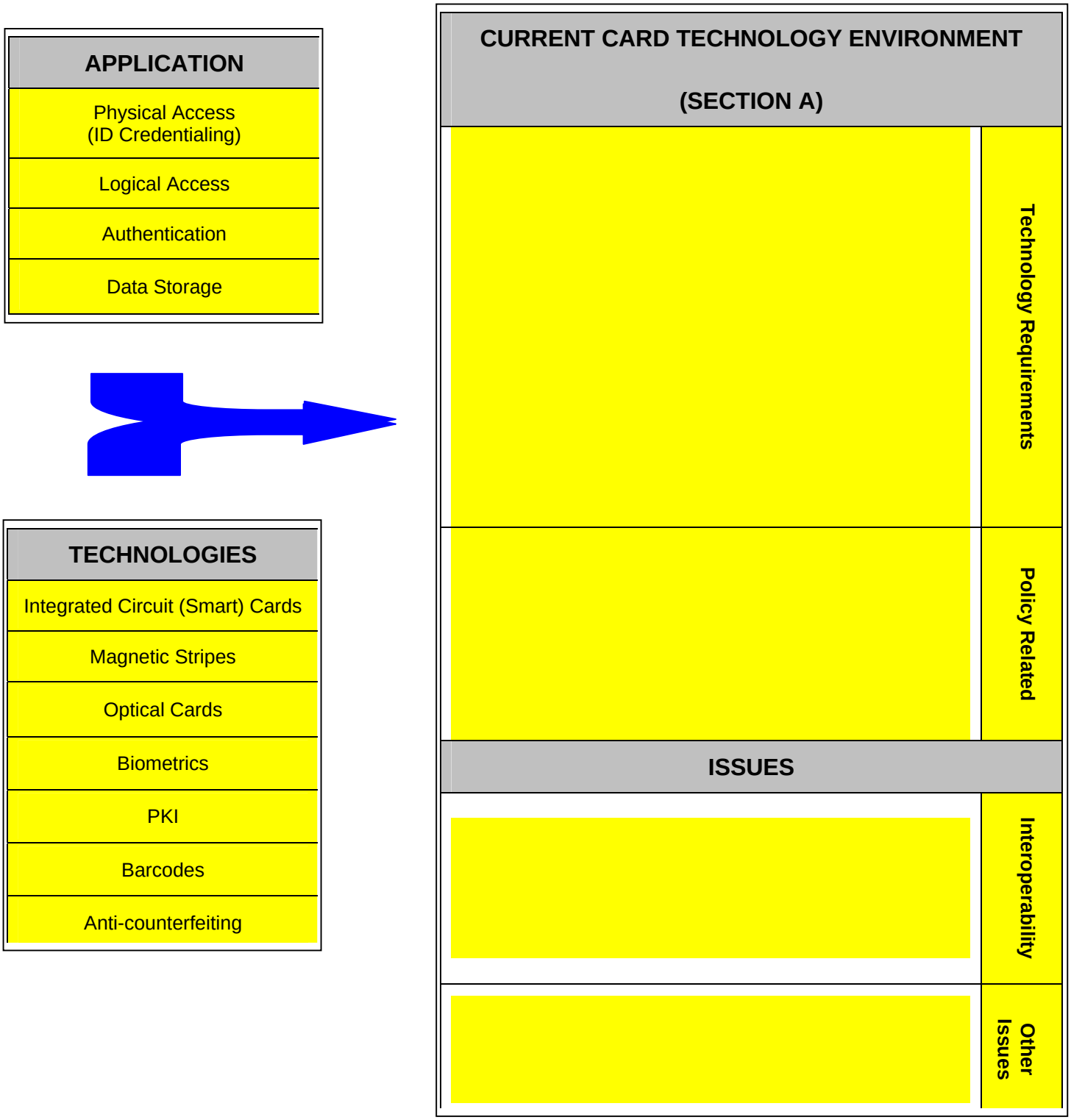
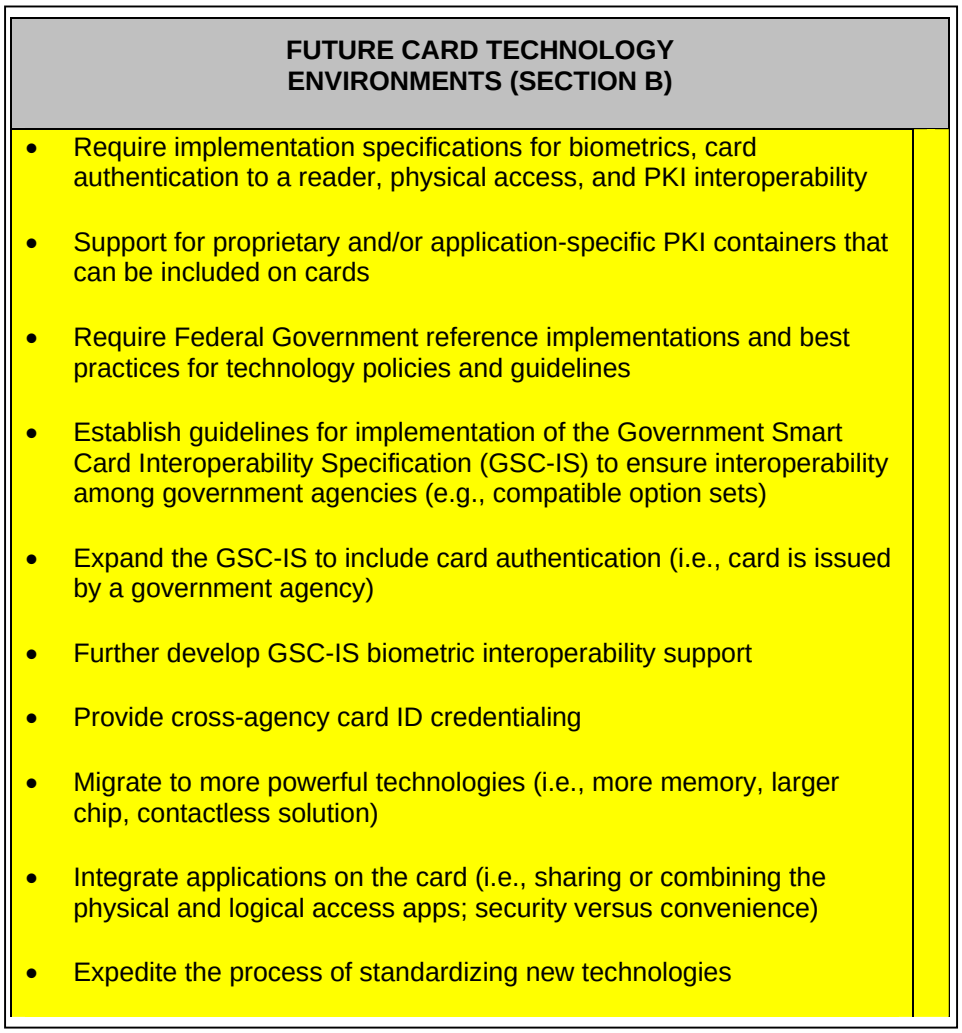


Figure 2. Future Trend Environments



3.2 Questionnaire Responses

NIST developed a capabilities and requirement questionnaire to support determination of what storage and processor card-based technologies are available by the industry or required by government agencies. The questionnaires were distributed during the 2-day workshop and posted to the NIST Web site for a 3-month period.

To display a clear comparison of the capabilities and requirements responses, Figure 3 represents the total population of respondents from the capabilities and requirement questionnaires (see Appendix B). Questions were combined and key words separated by a "/" to represent the consensus of Yes/No responses. The column heading "CAP" represents the collective Yes/No responses from the capabilities questionnaire, whereas the Yes/No responses from the requirement questionnaire are under the "REQ" column. A black cell represents questions not included on one of the questionnaires.

Respondent keys are as follows,

- ● **All** of the responses were yes to the question
- ◕ **Most** of the responses were yes
- ◑ At least **half** of the responses were yes
- ◔ **Few** of the responses were yes/most of the responses were no
- ○ **None** of the responses were yes/all responses were no to the question

Figure 3. Questionnaire Findings

CARD TECHNOLOGY CAPABILITIES AND REQUIREMENT FINDINGS

[redacted]	[redacted]	[redacted]
Do you offer/require identification cards?	●	●
Do you offer/require transaction cards?	◑	◑
Have you performed a Business Case Analysis for your card requirements?	[redacted]	●
Do you have any cost limitation requirements?	[redacted]	●
Do you offer/require any specific form factors for the card readers?	◕	●
Do you have/offer a capability/requirement to display text on your cards?	◕	●
If yes to the above question:		
Do you have any font requirements?	[redacted]	●
Do you have any font restrictions, such as character size limits?	◑	●
Do you have a maximum limit on the number of characters displayed?	◑	●
Do you have a capability/requirement for a photograph of the cardholder to appear on the card?	●	●
If yes to the above question:		
Do you have any size requirements for the photograph?	[redacted]	●
Do you have any size restrictions?	◑	●
Do you have any color requirements?	[redacted]	●
Do you have any color restrictions?	◑	●

[redacted]	[redacted]	[redacted]
Do you have any resolution requirements?	[redacted]	●
Do you have any resolution restrictions?	◕	●
Do you have a capability/requirement for other biometric imagery to appear on the card?	◕	◑
If yes to the above question:		
Do you have any size requirements?	[redacted]	◑
Do you have any size restrictions?	◔	◑
Do you have any resolution requirements?	[redacted]	◑
Do you have any resolution restrictions?	◑	◑
Do you have/offer a capability/requirement for digital biometric data on the card?	●	●
If yes to the above question:		
Do you have minimum data capacity requirements?	[redacted]	●
Do you have maximum data capacity requirements?	[redacted]	●
Do you have any data storage format requirements?	[redacted]	●
Do you have/offer a capability/requirement to include bar codes on identity/transaction cards?	●	●
If yes to the above question:		
Do you have any quantitative requirements?	[redacted]	●
Do you have any quantitative restrictions?	◕	●
Do you have any format requirements?	[redacted]	●
Do you have any format restrictions?	◕	●
Do you have a capability/requirement to display holographic images on your cards?	◑	◑
If yes to the above question:		
Do you have any size requirements?	[redacted]	◑

[redacted]	[redacted]	[redacted]
Do you have any size restrictions?	◑	◑
Do you have any format requirements?	[redacted]	◑
Do you have any format restrictions?	◑	◑
Do you have a requirement for general storage of digital data on the cards?	●	●
If yes to the above question:		
Do you have minimum data capacity requirements?	[redacted]	●
Do you have maximum data capacity requirements?	[redacted]	●
Do you have any retrieval access time requirements?	[redacted]	●
Do you require multiple storage formats?	[redacted]	●
Do you have/offer an installed base or other basis for preference for magnetic storage (e.g., magnetic stripe)?	◕	●
If yes to the above question:		
Do you have minimum data capacity requirements?	[redacted]	●
Do you have maximum data capacity requirements?	[redacted]	●
Do you have any retrieval access time requirements?	[redacted]	●
Do you require multiple storage formats?	[redacted]	●
Do you have any form factor requirements for the readers?	[redacted]	●
Do you have an installed base or other basis for preference for optical storage (e.g., laser recording)?	◑	○
If yes to the above question:		
Do you have minimum data capacity requirements?	[redacted]	○
Do you have maximum data capacity requirements?	[redacted]	○
Do you have any retrieval access time requirements?	[redacted]	○
Do you require multiple storage formats?	[redacted]	○

[redacted]	[redacted]	[redacted]
Do you have any form factor requirements for the readers?	[redacted]	○
Do you have/offer a read/write storage capability/requirement?	◕	●
If yes to the above question:		
Do you have a requirement for the minimum number of writes that a card must be able to accommodate in its lifetime?	[redacted]	●
Do you have a requirement for the maximum number of writes that a card must be able to accommodate in its lifetime?	[redacted]	●
Do you require processing capabilities to be embedded in your cards? (REQ) Does your product include an embedded processor? (CAP)	◕	●
If yes to the above question:		
Do you require physical input/output interfaces?	[redacted]	●
Do you require electronic input/output interfaces?	[redacted]	●
Do you require logical input/output interfaces?	[redacted]	●
Do you require more than one specific processor type?	[redacted]	●
Do you require any minimum processor capabilities?	[redacted]	●
Do you have cryptographic security requirements?	[redacted]	●
If yes to the above question:		
Embedded processors?	[redacted]	●
Digital Signatures?	[redacted]	●
Other?	[redacted]	●

4. Findings

- Based on the evidence of the interview responses, many card technology user organizations either have not conducted business case analyses or have not communicated business case analysis information to personnel managing implementation. Some responses to questions regarding the technology selection process indicated that the organizations are in the technology evaluation phase of their implementation. The stakeholders are engaged in piloting more than one technology and evaluating the effectiveness of the solution for their environment. That said, there seems to be general agreement that agency-specific user requirements drive card technologies requirements. The total cost of infrastructure and per unit cost of a card make up a significant part of the user requirements, which tend to be a mixture of the following five factors:

- **COST EFFECTIVENESS OF A TECHNOLOGY.** Cost is a primary factor in the choice of a suitable card technology. Most users were looking for unit card costs of no more than two to five dollars. Very significant cost differences exist among card technology implementations.

- **POLICIES AND BUSINESS PROCESSES UNIQUE TO EACH AGENCY.** Each agency has followed different technology implementations to satisfy similar business functions mainly because of the uniqueness of its internal policies and processes. For example, ID proofing seems to be one common business function that is undertaken by many government organizations. However, the differences in policy setup, based on contrasting security and cardholder privacy requirements, cause divergence from the common goal of ID proofing. This drives each agency to different technology solutions.

- **VARYING SECURITY REQUIREMENTS.** Security requirements (e.g., support for biometric requirements, digital signature, and personal data) play an important role in selection and use of card technologies. Some card technologies offer stronger security mechanisms.

- **AVAILABLE TECHNOLOGIES AND THE RELATED STANDARDS.** Some ID card implementations are driven mainly by available card technology capabilities and standards applicable to user requirements. Agencies are often forced to combine multiple technologies on one card to achieve performance and security objectives.

- **NEED FOR INTEROPERABILITY.** Given the growing number of interagency applications and of technologies in use, agencies require interoperability to achieve efficient operations. This requires equipment from multiple vendors to work together within a specific card technology and for different technologies to co-exist in an integrated manner.

The combination of these factors has forced agencies to either keep their legacy card technologies (e.g., bar code and magnetics), or enhance their existing card technology with added security features (e.g., holograms or digital watermarks). In addition, advances in card technologies (e.g., smart and optical cards) led various agencies to adopt different technologies for similar applications (e.g., physical access). This broad spectrum of available card technology led to even more complex integration issues and hampered interoperability across the agencies.

4.1 Status of Standards, Specifications, and Implementation Guidelines

ISO/IEC standards alone do not guarantee full interoperability for all the components involved in a card technology. Rather, they are designed to provide common guidelines to address general compatibility requirements. Interoperability involves coordinated policies, procedures, and management and use practices as well as hardware, software, and protocol compatibility. For example, ISO 7816 for contact-based smart cards provides a mature set of formal standards. However, the financial industry introduced

the more robust Europay Mastercard Visa (EMV) specification to address, not only additional functionality, but also other interoperability attributes.

Application level interoperability is different from card-to-reader interoperability. ISO/IEC 14443 does not currently address interoperable application level issues (e.g., application selection, message structure, transaction flow, and selection of available security mechanisms). Therefore, a card and a card reader from different manufacturers may not necessarily interoperate unless applications guidelines are developed for interoperation of ISO 14443-compatible devices.

So far, most biometrics technology centers on proprietary technologies, often creating incompatibility issues among different systems. Present biometric standards are relatively new, and not without issues. BioAPI, an open system standard for a biometric API, was approved as an official American National Standards Institute (ANSI) standard in February 2002. However, because of the relatively small number of deployed compliant systems, the standard lacks broad international status and industry acceptance. Notable shortfalls/problem areas in the biometric standards area include the following:

- Existing systems interoperate at the image level only.
- Templates have not been adequately tested as vehicles for interoperability. (Test of fingerprint minutia templates may be done by NIST starting this year.)
- No common face template is contemplated by vendors at this time.
- All existing iris templates are proprietary.

The introduction of the JavaCard and MULTOS Virtual Machines into the smart card world represents a significant step toward a multi-application environment. Currently, Global Platform, which is built on Java Card operating system, and MULTOS are the only such environments in wide existence. As the need to expand the usage of a card to different applications becomes an industry requirement, such as in transit and retail payment, a need for a true multi-application environment will become a necessity. The lack of standards for many of the new added security features (e.g., digital watermarks, Kinechip, and high-density barcodes) could pose potential integration problems when they are combined in multi-technology cards.

Technology standards can address only technical issues and requirements for specific functions. However, differences in issuer (agency) specific policy and processes contribute to the outstanding issues discussed in the workshop. It was noted that the variations in policies for ID proofing, credentialing requirements, and perceived level of security required resulted in unique physical access implementations based on similar technologies. Emphasis was placed on the need to achieve standardization of policies and implementation and use procedures to achieve interoperable implementations on an interagency basis.

Appendix E is a current bibliography of storage and processor card standards.

4.2 Integration Issues

A significant proportion of integration issues are caused by non-technical issues, including incompatible business processes, lack of clearly defined partnership relationships among stakeholders, and policy and procedural issues (see Section 4.1).

In large-scale physical access implementations in which cardholders are widely dispersed, the card management process becomes very labor intensive, expensive, and time consuming. Card management

functions (e.g., issuance, updating, replacing, and monitoring) need to be decentralized. Ideally, some functions (e.g., changes to credentials) should be handled at an individual user level (e.g., at the desktop). Maintaining and updating data on the card once it is issued requires complex software implementation. Maintaining the central database and robust IT infrastructure to control and monitor the remote processes will probably remain a lingering challenge.

4.3 Multi-technology Composition Issues

Agency-specific requirements such as the need for added security and the use of a single card for multiple functionalities drove the convergence of multiple technologies onto a single card. One main issue introduced with these cards is the potential increase in the card failure rate in the field. The total number of failures increases by the sum of all the individual failure rates for each technology present on the card. The existing standards specifications are inadequate for the issues arising from integrating, or even just composing, different technologies on one card. Agencies dictate the graphics layout of their cards, making proprietary decisions on the physical location of security features (i.e., watermarks, Kinegrams®), barcodes, optical stripe, and demographic data on the card. For example, the location of the barcode varies from the Common Access Cards (CACs) to the government travel documents. No standard dictates the placement of added security features, such as digital watermarking and Kinegram® on the card. Conversely, the physical, mechanical, and operational characteristics of each card technology may damage one another when they co-exist on the same card. For example, the acceptable card elasticity for magnetic stripe cards can cause cracking of the chip in smart cards.

Currently, multi-application cards are used with separate readers for each technology. A card with a contactless chip, a barcode, and a magnetic stripe requires a contactless reader, barcode reader, and magnetic stripe reader for each respective technology. Building readers to read all three technologies would be cost effective in the long term, easier to manage and maintain, and more convenient.

Multi-technology cards may cause card management issues when they are shared with other government agencies. For example, if a government physical access card were also to be used in a transit application, it would be necessary to identify organizations responsible for administering, maintaining, updating, and monitoring the card.

4.4 Security Issues

Current standards address only a subset of the security issues associated with storage and processor cards. There is currently no authoritative taxonomy of storage and processor card security issues, much less a comprehensive set of specifications and guidance regarding security requirements. There is a need to 1] develop a standard taxonomy of storage and processor card security issues and objectives, 2] establish the availability and maturity of technical, procedural, and organizational alternatives for dealing with security issues and achieving security objectives, and 3] develop standards and guidelines necessary to enable organizations to achieve applicable security objectives in an interoperable manner.

4.4.1 Range of Security Concerns

The security issues associated with storage and processor cards vary in character from technology to technology and from application to application. In some cases, the data owners and users are concerned primarily with the integrity of the information stored on and/or processed by the card. Normally, the integrity of any processing executed on the card is a significant concern. In other cases, confidentiality protection for some of the information is also required.

Some security issues are technical in nature (e.g., cryptographic techniques, physical security techniques). Other issues are associated with the management infrastructure in which the cards are used.

4.4.1.1 Card Management and Control Issues

Smart card management approaches often give control of some card functions to one party and control of other functions to another party. Examples of entities that may control some aspect of a card's functionality include the 1) card's manufacturer, 2) the card's software programmer, 3) a card issuer, 4) the owner of the data processed and stored on a card, 5) a reader or other terminal device, and 6) the card holder. When one of these entities attacks functions controlled by another party, a "trust split" is said to occur.

For example, an automatic teller machine or point-of-sale terminal may illicitly capture private information (e.g., a PIN, an account number, an other identifying information) or record altered transaction amounts. Transaction monitoring and parameter checking are among potential countermeasures for this type of attack. This can involve independent monitoring/audit back-end processors.

Trust splits are inherent in the systems supported by multi-application cards. Mutual suspicion among components is strongly advisable. The various controlling entities and system components need to be authenticated to each other. (E.g., the reader/terminal should be able to authenticate the card's validity and the cardholder's identity, and the card or cardholder should be able to authenticate the reader/terminal.) Trust splits are reduced where the data owner and the cardholder are the same. Some countermeasures, such as adding some kind of display to the card, are not yet economically feasible.

4.4.1.2 Technical Controls

a. Photographic and Printed Content

In the case of photographic information and printed information, there is no attempt to conceal the information, but it is necessary to discourage undetected alteration of the information or forging of false credentials. Techniques such as inclusion of cryptographically protected and verifiable versions/summaries/hashes of the information on the card[6], digital watermarking, or Kinegrams© can be employed as countermeasures. (See, for example, Section 2.2.2.5.)

b. Magnetic and Optical Storage Media

In the case of magnetic and optical storage media, cryptographic protection may be required to provide confidentiality protection, integrity protection, or both. The same may also be the case for encoded printed components (e.g., barcodes – see Section 2.2.2.2).

In general, confidential information should not be stored on storage cards in unencrypted form.

c. Smart Cards and Contactless Smart Cards

Concerns related to both the confidentiality/integrity of information and the integrity of processes are associated with smart cards. Consequently both logical protection (e.g., cryptography) and physical protection against technical surveillance and tampering are often necessary.

[6] E.g., in printed, optically etched, photographic/holographic, or magnetic form.

In many cases, confidential information necessarily exists on smart cards in unencrypted form (e.g., during cryptographic processing where a cryptographic process is executed by smart card circuitry). Also, communication between a smart card and some terminal device is often used to manage information stored on a card or capabilities enabled by a card. As a result, security concerns exist with respect to extraction of information from smart cards and/or tampering with card functionality.

(1) Non-invasive attacks

Electrical currents generate electromagnetic fields (electromagnetic radiation). Non-invasive attacks involve reception and analysis of electromagnetic radiation produced by normal operation of a card. Examples include, but are not limited to, analog radiation produced by current associated with communications interfaces and power supplies. Non-invasive attacks (e.g., side channel or eavesdropping attacks) are difficult to prevent.

In the case of contactless smart cards, the strength of the electromagnetic radiation associated with input and output is necessarily sufficient to permit remote interception of information communicated between the card and its associated reader/terminal. Cryptographic integrity and confidentiality protection is frequently necessary to protect the integrity of the processes supported by the cards. (E.g., protection against both capture of sensitive and/or private information and spoofing of security processes[7]).

In some cases, security algorithms, cryptographic keys, and security protocols can be compromised by power analysis attacks that exploit power consumption characteristics of smart cards (e.g., simple power analysis attacks, differential power analysis attacks, and "high order" power analysis attacks. Few practical countermeasures to power analysis attacks have been developed in industry.

Analysis of the times of execution of smart card operations generally requires the attacker to have access to the card and the ability to measure the times required for partial operations. These "timing analysis" attacks have been used to disclose active security keys. (Note that non-linear key updates may be employed as a countermeasure to this consequence of successful timing analysis.)

Software protocol attacks, fault generation attacks, and so called "glitch attacks" exploit chip abnormalities. Such attacks often require "trial and error" procedures and/or detailed analysis of chip responses to power fluctuations, different clock rates, etc. (e.g., changing the output of internal components such as flip-flop circuits). Randomized multithreading of operations can prevent prediction of instruction execution timing. (Use of a randomized clock input can serve this purpose as well.) Some chips employ other countermeasures such as sensors that disable the chip upon detection of voltages, clock speeds, or temperatures that vary too far from norms. Most such countermeasures are insufficiently robust to provide high-assurance protection.

Researchers at the University of Cambridge in England have developed a way to attack and cause faults in cards by flooding the chip (or areas on a chip) with energy pulses (e.g., using a photographer's flash gun and a microscope).[8] Simply shielding the processor e.g., by adding a top metal layer to the chip is not necessarily an adequate countermeasure because silicon becomes transparent to the light in an infrared flash and the chip can therefore be attacked from the rear. Electromagnetic pulses and X-rays could also be used in a similar manner.

[7] For example, recording an identification exchange may permit subsequent playback of access control information by an intruder who thereby gains access to restricted facilities.

[8] *Sergei P. Skorobogatov, Ross J. Anderson: Optical Fault Induction Attacks, Cryptographic Hardware and Embedded Systems Workshop (CHES-2002), San Francisco, CA, USA, 13-15 August 2002* [www.cl.cam.ac.uk/Research/Security/tamper/].

Input/output interruption attacks, such as blocking or clamping off (e.g., with a diode) contacts via which vendor-originated program update signals reach chips have been employed for a number of years. Vendors have developed a range of countermeasures that are reasonably effective in preventing users from receiving unpaid for services by blocking signals that restrict capabilities (e.g. limit cable or satellite channels that a user can access or decrementing/invalidating telephone access cards).

(2) Invasive Attacks

Invasive techniques for probing and analyzing a smart card usually start with removing the processor from a card. A common technique for accessing the circuitry of the exposed chip involves subsequent scraping away any remaining plastic covering remaining behind the chip, then dissolving with acid the chip's protective resin layer and washing the chip with acetone to reveal the silicone surface.

On-chip signals can then be read using micro probing needles or electron beam testers. The contents of an exposed chip's memory can sometimes be read by identifying the chip's test pads using a confocal microscope, then initiating test routines. Because some manufacturers often blow test pad fuses following running of acceptance test cycles, it may be necessary to bridge blown fuses using microprobe needles in order to re-enable test routines that dump the chip's memory.

It is also possible to alter the functionality of a chip with lasers, ultrasonics, or focused ion beams. For example, the contents of an exposed chip can be read or altered using focused ion beam editing techniques. It is possible to overwrite read-only memory at the bit level using a laser cutter microscope. (One consequence of such an attack is extraction of DES keys stored in ROM or EEPROM.)

Anti-tamper measures such as capacitive sensors and optical sensors buried in opaque coatings can be used to detect tampering and subsequently disable chips. These techniques have a mixed track record with respect to reliability. Other countermeasures include visual scrambling (circuit designs that randomize chip lay-out) and de-correlation of the location of data on the chip with its logical address location (useful with dynamically updated memory such as RAM).

4.4.2 Current Security Challenges

In addition to the need for storage and processor card security standards and guidelines, several specific security challenges were identified in the course of the 8-9 July 2003 Storage and Processor Card-Based Technologies Workshop:

- Faster PKI authentication is needed in physical access and transit applications. This raises a number of issues such as identification of and agreement on certification authorities, certification management processes, and distribution of processing requirements among cards and readers/terminals.

- Availability of reliable and affordable biometric identification capabilities is needed. Some users perceive biometrics to be an increasingly important requirement for authentication of the cardholder with the card (e.g., border control and identity theft considerations).

- A common framework for data integrity, authentication, and general security mechanisms is needed. Unlike ISO 7816, the ISO/IEC 14443 does not currently address a means to achieve a common framework for data integrity, authentication, and general security mechanisms (e.g., 3DES, AES, and RSA). Most existing ISO 14443-based card technology implementations center on proprietary security schemes. These are not approved for protection of Federal government information.

4.5 Interoperability Issues

Although ISO 7816 parts 1 through 4 provide a relatively sound framework for interoperability, the ability to choose among different available options does not guarantee interoperability. Further application-level guidelines need to be developed for interagency use of cards.

Biometrics authentication is being implemented by many government agencies because of its capability to uniquely identify individuals. However, existing biometrics implementations are mostly stand-alone systems that are not integrated with other identification mechanisms or processes. This is partly attributed to variations in proprietary biometric templates implemented by different vendors, but it inhibits interoperability.

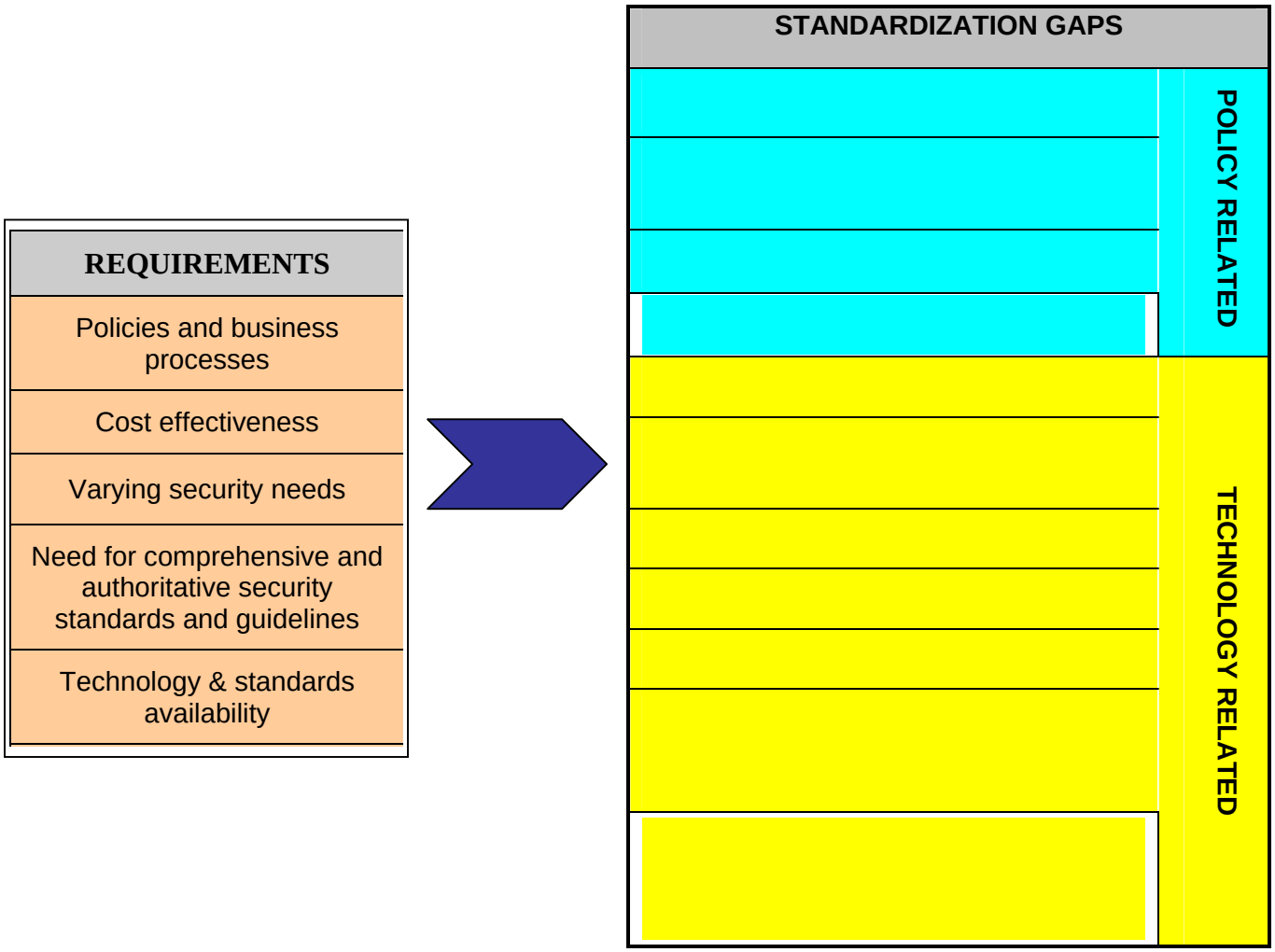
Current implementations of ISO 14443 card technology create interoperability problems when cards from different vendors are introduced into an existing infrastructure. This results in requirements for middleware updates and changes that are analogous to updating the Windows® operating system every time a new application is installed.

Ultra high-density barcodes offer a viable solution to many on-card data storage needs. However, this proprietary technology lacks interoperability standards.

4.6 Summary

Figure 4 presents a high-level summary of the user requirements identified in this section and the policy and technical related issues and standardizations gaps that are detailed in Section 5 of this document.

Figure 4. Card Technology Requirements and Standards Gaps



5. Conclusions

Several issues were identified in Section 4 based on the analysis of existing storage and processor card technologies. There appears to be no consensus on requirements from the user community that participated in the conference for additional technical standards. However, most contributors to this report agree on a need to establish additional policy-related standards and regulations as a prerequisite to accomplishing true interoperability and efficient integration. The following summarizes the analysis of policy and technical issues and standardization gaps.

Policy Issues and Standardization Gaps

The following three issues were identified and need to be addressed:

- There is a consensus on a need for a common policy standard for identity credentialing. Agencies have different interpretations on the definitions of the principal participants, steps involved, and commonly accepted degree of identity proof required for the identification process.
- Administration and management of a multi-technology card shared by different agencies have not been clearly defined. Examples are the ownership scheme; card base management, including application loading and updating; system management and maintenance; and monitoring.
- Some agencies with existing legacy systems want to transition into newer card technologies. Business cases need to be developed for these prospective transition programs. Currently, no common strategies are defined to guide agencies in migrating to the newer technologies. Agencies need to conduct user requirements analyses to establish a consensus on the number of card technologies that can and should co-exist on a card. A related area of concern is the ability to use existing infrastructures when migrating from one technology to another.

Technology Issues and Standardization Gaps

Existing ISO/IEC standards have been designed primarily for the communication between the smart cards and reader/writer devices. However, these standards do not define the local information types and protocols for transfer of transaction records among smart cards, card interface devices, applications interfaces, and central processing hosts or server computers. Standards or guidelines that define and identify the communication protocols, data formats, and rules for transaction reporting are needed, although such standards or guidelines may often be agency specific. In the case of agency-specific requirements, the guidelines should be locally generated. However, future government-wide standards may need to be derived from common user requirements. At present, the requirements consensus among users that is prerequisite to government-wide standards remains incomplete.

Current standards address only a subset of the security issues associated with storage and processor cards. There is currently no authoritative taxonomy of storage and processor card security issues, much less a comprehensive set of specifications and guidance regarding security requirements. There is a need to:

- Develop a standard taxonomy of storage and processor card security issues and objectives,
- Establish the availability and maturity of technical, procedural, and organizational alternatives for dealing with security issues and achieving security objectives, and
- Develop standards and guidelines necessary to enable organizations to achieve applicable security objectives in an interoperable manner.

Formal standardization of GSC-IS on behalf of the GSC community is needed. GSC-IS represents the first true smart card interoperability specification for logical and physical access control in Federal government applications. However, the basic GSC-IS smart card service provider model is flexible enough to support a much broader range of applications. It does not preclude use of current storage technologies, including optical technologies. GSC-IS is based on the ISO 7816 standards, and NIST is pursuing formal standardization of GSC-IS on behalf of the GSC community.

The following additional technology issues were identified:

- Existing standards do not address a true multi-application platform with multiple security domains that enable software applications from different vendors to share the same media. Although significant cost savings and ease of card and system management benefits might result from development of such a platform, the workshop and subsequent interviews revealed neither the validated requirements nor the technical capabilities necessary to the development. No consensus among the user community regarding additional requirements for interconnecting multiple technologies, either on a card or in a reader/processor device was identified in either workshop proceedings or user interviews.

- With respect to the design of multi-technology cards, the issue of the physical location of each technology on the same card is a concern. No standard exists that defines the technologies that may co-exist on a single card. The detailed location and layout of different combinations of components have not been specified, nor have physical and mechanical specifications for some technologies or groups of technologies been specified. Such specification of the mutual effects of co-existing technologies and varying operational requirements of each technology may prove useful in the future. For example, when chip failure occurs on a contactless smart card, the magnetic stripe also present on the card may also be affected. The life expectancy of the magnetic stripe is then reduced as a result of a chip-related problem. However, consensus is needed regarding requirements for multi-technology card components, and investigation of the compatibility attributes and conditions for technology combinations must occur before useful standardization efforts can be initiated.

- A need for standardization of post-embedding printing processes has been stimulated by high production failure rates. Varying printing requirements on the exact location of the text and graphics cause problems during post-issuance printing.

- New biometrics standards have developed rapidly in recent years. However, consensus needs to be developed regarding a common means of interpreting biometric data for different types of biometrics images, including fingerprinting, iris scan, and face scan. Such consensus is prerequisite to effective standards development. A first step might be identification and testing of several fully supported biometric technologies that are available from multiple vendors. This might establish a basis for consensus development regarding interpretation of biometric data.

- A study is needed that addresses security provisions and application-level interfaces to enable development of guidelines for achieving interoperability among ISO 14443-complient components.

- There are no standardized tests for comparison of optical effectiveness and clarity of holograms or diffraction gratings.

- Differences exist among standards offered by ICAO and other ISO organizations regarding identity methods and machine-readable travel documents.

Summary

This report includes findings captured from the workshop, interviews, and questionnaires. Note that although requirements for co-location of different technologies exist on a common card, no requirements for on-card interconnection of different technologies were stated. In the absence of user requirements, efforts to build, design, or research an interacting set of technologies on a common card are premature at present.

The overall conclusion derived from the findings is that although the building blocks are in place to support interoperable secure identification systems, business, management, and policy decisions limit the opportunities for interoperability. Specifically, policies regarding what personal information may be stored on card-based storage and processor systems need to be coordinated among agencies, and where necessary, codified in law. Just as importantly, responsibilities and infrastructures for entering and maintaining personal data onto the cards need to be established.

As each new card technology or application is developed, modification of the standards base will be needed to bridge the gap between existing and emerging card technologies and applications. However, to be useful, technical standards need to be consistent with policies that govern the relevant functional requirements for technology. In the case of card-based technologies, policy consensus needs to be established as a prerequisite to prioritization of technical standards activities. Gaps in card technology standards coverage necessarily result from technical innovation. However, technologies supported by existing standards appear to be adequate to support current user requirements. Policy and infrastructure developments can be expected to establish requirements not provided for in existing standards. As these policy and infrastructure developments occur, additional standards requirements are expected to emerge. The primary need, as perceived by the user community, is a requirement for consistent and compatible policies and training to support interagency interoperability.

Appendix A—Interview Guide

Multiple Storage and Processor Card-Based Technology Interview Guide

NIST hosted a workshop on 8 and 9 July to identify current and planned Federal government activities and related needs, general issues, existing voluntary industry consensus standards, gap areas in standards coverage, and industry capabilities in the field of storage and processor card technologies. The workshop supports the development of a standard roadmap, and a guideline on storage and processor card technologies to include multi-technology composition issues.

Purpose of Interview

The goal of the workshop was to develop and exchange information on the standards for and capabilities of multi-technology storage and processor cards. The purpose of this interview is to validate data captured at the workshop. Analysis and aggregate findings of the data gathered as a result of these interviews will be published and available from the NIST website at a later date.

Name: _____ **Title:** _____
Organization: _____ **Date:** _____

A. Discuss the Current Situation with Card Technologies

1. What card technologies are currently being used? Why were these particular technologies chosen?

2. Were there other technologies considered? Why weren't they chosen?
    a. Have you considered card technologies and rejected them for reasons other than they would not meet your requirements. If so, please state what the technologies are, and why they were rejected.
    b. Did you encounter integration and/or interoperability issues?

3. Have you performed a Business Case Analysis?
    a. If yes, is it open to the public and available on your web site? Please list resource.
    b. What are the main cost drivers for your card application?

4. What are the current Card Technology Requirements?
    a. Please describe the text that's required to be displayed on your cards. Include such details as how many characters are required, font requirements, maximum lengths, character size requirements, etc.
    b. If you use different color backgrounds or borders for different employee/contractor designations, please list these requirements.
    c. If a photograph is required to be displayed on your card, please discuss your minimum/maximum size, color, and resolution requirements?
    d. Are there requirements to print on the front and/or back of your cards? If so, please state the requirements.
    e. If there is a requirement for other biometric imagery to appear on the card, please describe the minimum/maximum size and resolution requirements.

f. For any requirements of storing digital biometric data on the card, please discuss your minimum data capacity and storage format requirements.

g. If a barcode is included on your card for identity/transaction cards, what are your quantitative and format requirements?

h. If holographic images are displayed on your cards, what are the size and format requirements?

i. For requirements dealing with general storage of digital data on the cards, what are your minimum data capacity, minimum storage and retrieval access time, and data storage format requirements?

j. What are your data format and form factor requirements for an installed base of or other basis for preference for magnetic storage (e.g., magnetic stripe)?

k. For read/write storage requirements, what is the minimum number of write events that a card must be able to accommodate in its lifetime?

l. How long does the card remain active in your system?

m. For requirements dealing with processing capabilities to be embedded in your cards, identify any required specific processor type. What minimum processing capabilities are required (e.g., MIPS)? What input/output interfaces are required? Physical? Electronic? Logical? Data Format?

5. What are the security requirements for your card?
    a. Please list your cryptographic security requirements (e.g., embedded processors, digital signatures)?
    b. What other anti-counterfeiting measures do you require (e.g. embossing, 3D images, etc.)?

6. Do you have other specific requirements for your card (performance, scalability, etc.)?

7. Do you have requirements that card manufacturers can produce but card reader manufacturers cannot resolve without extraordinary costs?

8. Are there applicable standards governing your card technology, and if so, are you planning to conform to those standards. If not, why not?
    a. Are the current standards adequate for your requirements?
    b. Is there a lack of standards covering your card technologies? If so what is required?
    c. What are the specialized needs of your applications where existing standards do not apply or force you to deviate from existing standards?

9. Is your card application unique to a Federal government office, or are there similar applications used elsewhere in government. If so, please identify as completely as possible those Federal government agencies with similar card applications.

B. Discuss the Future Environment with Card Technologies

1. What future trends do you envision for the card technology industry? For your organization?
    a. Are there special technologies (RFID, contactless, use of track 1 or 3, special use for track 2, micro printing, etc.) other than ones stated so far that you will need or think you may need in the future?

b. Have you considered tokens instead of cards? If so, what were the results of your analysis?

2. Do you anticipate your requirements changing?

3. What new standards would you like to see?

Appendix B—Requirements and Capabilities Questionnaires

Workshop on Storage and Processor Card-based Technology
Card Technology Requirements Questionnaire

Workshop Overview

NIST will be hosting a workshop to identify current and planned Federal government activities and related needs, general issues, existing voluntary industry consensus standards, gap areas in standards coverage, and industry capabilities in the field of storage and processor card technologies. The workshop will support development of a standard roadmap, and a guideline on storage and processor card technologies to include multi-technology composition issues.

Purpose of the Questionnaire

The purpose of the questionnaire is to capture data prior to the workshop from various Federal government agencies. Analysis and aggregate findings of the data gathered as a result of this questionnaire will be presented during the workshop on July 8 and 9, 2003.

The goal of this questionnaire is to capture data from various resources on current card technology requirements. This information will help in identifying capabilities of multi-technology storage and processor cards.

Please submit the completed questionnaire to nist_workshop@bah.com with the subject line "Card Technology Requirements Questionnaire"

Name: _____ **Title:** _____
Organization: _____ **Date:** _____

Questionnaire on Card Technology Requirements

Please place an X in the appropriate column for each question.

Do you require identification cards?		
Do you require transaction cards?		
Have you performed a Business Case Analysis for your card requirements?		
Do you have any cost limitation requirements?		
Do you require any specific form factors for the card readers?		
Do you have a requirement to display text on your cards?		
If yes to the above question:		
Do you have any font requirements?		
Do you have any font restrictions, such as character size limits?		
Do you have a maximum limit on the number of characters displayed?		
Do you have a requirement for a photograph of the cardholder to appear on the card?		
If yes to the above question:		
Do you have any size requirements for the photograph?		

Do you have any size restrictions?		
Do you have any color requirements?		
Do you have any color restrictions?		
Do you have any resolution requirements?		
Do you have any resolution restrictions?		
Do you have a requirement for other biometric imagery to appear on the card?		
If yes to the above question:		
Do you have any size requirements?		
Do you have and size restrictions?		
Do you have any resolution requirements?		
Do you have any resolution restrictions?		
Do you have a requirement for digital biometric data on the card?		
If yes to the above question:		
Do you have minimum data capacity requirements?		
Do you have maximum data capacity requirements?		
Do you have any data storage format requirements?		
Do you have a requirement to include bar codes on identity/transaction cards?		
If yes to the above question:		
Do you have any quantitative requirements?		
Do you have any quantitative restrictions?		
Do you have any format requirements?		
Do you have any format restrictions?		
Do you have a requirement to display holographic images on your cards?		
If yes to the above question:		
Do you have any size requirements?		
Do you have any size restrictions?		
Do you have any format requirements?		
Do you have any format restrictions?		
Do you have a requirement for general storage of digital data on the cards?		
If yes to the above question:		
Do you have minimum data capacity requirements?		
Do you have maximum data capacity requirements?		
Do you have any retrieval access time requirements?		
Do you require multiple storage formats?		
Do you have an installed base or other basis for preference for magnetic storage (e.g., magnetic stripe)?		
If yes to the above question:		
Do you have minimum data capacity requirements?		
Do you have maximum data capacity requirements?		
Do you have any retrieval access time requirements?		
Do you require multiple storage formats?		

[redacted]	[redacted]	[redacted]
Do you have any form factor requirements for the readers?		
Do you have an installed base or other basis for preference for optical storage (e.g., laser recording)?		
If yes to the above question:		
Do you have minimum data capacity requirements?		
Do you have maximum data capacity requirements?		
Do you have any retrieval access time requirements?		
Do you require multiple storage formats?		
Do you have any form factor requirements for the readers?		
Do you have a read/write storage requirement?		
If yes to the above question:		
Do you have a requirement for the minimum number of writes that a card must be able to accommodate in its lifetime?		
Do you have a requirement for the maximum number of writes that a card must be able to accommodate in its lifetime?		
Do you require processing capabilities to be embedded in your cards?		
If yes to the above question:		
Do you require physical input/output interfaces?		
Do you require electronic input/output interfaces?		
Do you require logical input/output interfaces?		
Do you require more than one specific processor type?		
Do you require any minimum processor capabilities?		
Do you have cryptographic security requirements?		
If yes to the above question:		
Embedded processors?		
Digital Signatures?		
Other?		

Thank you for taking the time to fill out the questionnaire.

Please submit the completed questionnaire to nist_workshop@bah.com with the subject line "Card Technology Requirements Questionnaire"

Appendix C—APPENDIX C: FREQUENTLY ASKED QUESTIONS

Question	Answer
What are the primary factors affecting government selections from available card technologies?	• Agency-unique policies and business processes; • Cost effectiveness of technologies; • Agency-specific security requirements; • Availability and maturity of technologies and related standards; • Need for interoperability among sectors and among organizations within sectors.
What are the most common government uses for storage and processor cards?	Identification, authentication, and access authorization are the most common government uses for storage and processor cards. Facilities access records, account activity records, and personnel/medical records are not yet widely employed uses for the cards.
Are there current operational government requirements for incorporation of multiple storage, processor, and photographic elements onto a single card?	Yes. A number of user responses indicated requirements incorporation of multiple storage, processor, and photographic elements onto a single card.
What are the technologies most commonly required for incorporation onto storage and processor cards?	User responses indicated that magnetic stripe storage, smart card processor chips, photographs of the bearer, and proximity communications components were the most commonly required components. Several very large users require bar-code components, and one very large user requires an optical storage capability.
Are there current operational government requirements for interconnection of storage and processor components on a single card?	The need for the interconnection of contact and contactless interface to a single microprocessor chip has been identified. However, the user responses did not indicate a requirement for interconnection of storage and processor components on a single card.
What are the major impediments to inter-organizational storage and processor card interoperability?	The most commonly cited impediment to inter-organizational storage and processor card interoperability is the absence of common policies. Specific policy issues identified included those regarding establishment of proof of identity and those establishing responsibilities for card maintenance (information input and update). User responses cited a need for policies regarding what personal information may be stored on government-issued cards to be coordinated among agencies and, where necessary, codified in law.
What technology gaps have been identified by	• Interoperable biometric hardware and

users?	software; • Common middleware; • Post-embedding printing standards; • Availability of standard tests for comparison of optical effectiveness and clarity of holograms or diffraction gratings.
What standardization gaps have been identified by users?	• Common standards for identity methods (including policies for establishment of proof of identity); • Common standards for machine-readable travel documents; • Placement of components on card real-estate; • Policies for establishing responsibilities for card maintenance (information input and update); • Common guidelines for achieving ISO 14443 compliance.
Have most government card users conducted business case analyses?	No. Also, there is an absence of guidance for migrating to new technologies.
Have administration and management of a multi-technology card shared by different agencies been clearly defined?	No. Gaps include ownership scheme, card base management, application loading and updating, system management and maintenance, and monitoring requirements.
Do existing ISO/IEC standards define local information types and protocols for transferring transaction records among cards, card interface devices, and central processors?	With the exception of magnetic stripe based financial transactions, most applications use proprietary methods to store and retrieve data from the card. Existing ISO/IEC standards have been designed primarily to specify communication between cards and reader/writer devices.
Is there sufficient consensus among users regarding communications protocols, data formats, and rules for transaction reporting to support standardization of information types and protocols for transferring transaction records among cards, card interface devices, and central processors?	No. Existing standards and guidelines are agency-specific.

Appendix D—Workshop Session Highlights

STORAGE AND PROCESSOR CARD-BASED TECHNOLOGIES WORKSHOP TRANSCRIPT HIGHLIGHTS

July 8 and 9, 2003

This Appendix includes the PowerPoint presentations included in the July 8 and 9, 2003 Storage and Processor Card Workshop and some excerpts from the workshop transcripts. Because the presentation graphic files are very large, they are included in this document as links to separate files[9]. For each presentation, the workshop session, presentation title, and the size of the graphics file associated with the presentation is provided. Excerpts from the presentation transcript follow. The text of the transcript excerpts is as captured from workshop tapes, and has not been modified for purposes of either readability or content interpretation. In order to assist the reader to maintain some context, the transcript excerpts are flagged with respect to content type or issue addressed. The flags can be used as an aid to searching the text for specific issues or information types. The following flags are provided:

- Best Practices
- Business Process
- Capability
- Comparison
- Definition
- Industry Needs
- Information (General Information)
- Integration
- Interoperability
- Issue
- Lessons Learned
- Limitation
- Migration Strategy
- Multiple Applications
- Multi-technology Issues
- Recommendation
- Requirement

[9] The exception to this rule is the *Opening Remarks* presentation.

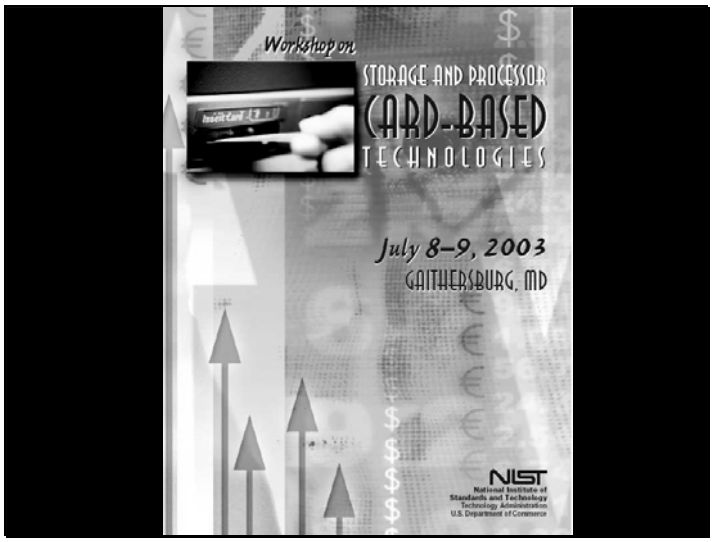
- Security
- Standardization
- Technology
- Trends

OPENING REMARKS AND WORKSHOP OVERVIEW

Tim Grance, Computer Scientist

National Institute of Standards and Technology Conference Objective

The goal of the conference is to surface the various requirements for card technologies from the full spectrum of card technologies, identify the capabilities of these technologies, and outline the issues in using them. The analysis of requirements, capabilities, and issues will provide guidance for further standardization needs in card technology industry. The ultimate purpose for the conference is to produce a roadmap of the gap areas and the relevant standards and produce a publication of general value to the Federal government and to industry to use this as a solid reference point.



Welcome to the Workshop on
Storage and Processor Card-based Technologies
NIST · Gaithersburg, MD
July 8-9, 2003

Workshop purpose is to identify:

- **Current and planned Federal government activities and related needs,**
- **General issues,**
- **Existing voluntary industry consensus standards,**
- **Gap areas in standards coverage, and industry capabilities in the field of storage and processor card technologies.**

Tim Grance
Computer Security Division
Systems and Network Security Group

Workshop on Storage and Processor Card-based Technologies

Objectives:

- **Determine government requirements for card interoperability specifications,**
- **Enhance interoperability among federal agency systems,**
- **Develop and exchange information on the standards for and capabilities of multitechnology storage and processor cards,**
- **Support the development of a standards roadmap, and a guideline on storage and processor card technologies to include multitechnology composition issues.**

Workshop on Storage and Processor Card-based Technologies

Workshop topics:

- **Federal Government Card Technology Requirements**
- **Card Technology Business Case Analysis**
- **Current Card Technology Capabilities**
- **Multitechnology Integration Requirements/Issues**
- **Interoperability Requirements/Issues**
- **Privacy and Security Issues**
- **Technology Roadmap and Gap Analysis**

Computer Security Division
Systems and Network Security Group

Agenda

July 8, 2003

Time	Session
7:30 AM - 8:30 AM	**REGISTRATION**
8:30 AM - 8:45 AM	**OPENING REMARKS & WORKSHOP OVERVIEW** *Timothy Grance, Computer Scientist* **NIST**
8:45 AM - 9:10 AM	**CARD TECHNOLOGY OVERVIEW** *Edward Oppenheimer, Sr. Associate* **Booz Allen Hamilton**
9:10 AM - 9:35 AM	**BUSINESS CASE ANALYSIS** ***Willy Dommen, Principal*** **Booz Allen Hamilton**
9:35 AM - 9:45 AM	**QUESTIONS AND COMMENTARY**
9:45 AM - 10:05 AM	**BREAK**
10:10 AM - 12:40 PM	**PANEL DISCUSSION:** **FEDERAL GOVERNMENT CARD TECHNOLOGY REQUIREMENTS**
12:40 PM - 1:00 PM	**QUESTIONS AND COMMENTARY**
1:00 PM - 2:00 PM	**LUNCH**
2:10 PM - 5:00 PM	**PANEL DISCUSSION:** **CURRENT CARD TECHNOLOGY** CAPABILITIES [3:40 Break]
5:00 PM - 5:20 PM	**QUESTIONS AND COMMENTARY**
5:20 PM - 5:30 PM	**SESSION WRAP-UP**

Agenda

July 9, 2003

Time	Session
8:45 AM - 9:00 AM	**RECAP DAY 1 AND WORKSHOP OVERVIEW**
9:00 AM - 11:00 AM	**PANEL DISCUSSION:** **SECURITY AND PRIVACY ISSUES**
11:00 AM - 11:20 AM	**QUESTIONS AND COMMENTARY**
11:20 AM - 11:40 AM	**BREAK**
11:45 AM - 12:45 PM	**PANEL DISCUSSION:** **MULTITECHNOLOGY INTEGRATION REQUIREMENTS/ISSUES**
12:45 PM - 1:00 PM	**QUESTIONS AND COMMENTARY**
1:00 PM - 2:00 PM	**LUNCH**
2:05 PM - 3:35 PM	**PANEL DISCUSSION:** **INTEROPERABILITY REQUIREMENTS/ISSUES**
3:35 PM - 3:55 PM	**QUESTIONS AND COMMENTARY**
3:55 PM - 4:10 PM	**BREAK**
4:15 PM - 4:45 PM	**PANEL DISCUSSION:** **TECHNOLOGY ROAD MAP & GAP ANALYSIS**
4:45 PM - 5:00 PM	**QUESTIONS AND COMMENTARY**
5:00 PM - 5:15 PM	**WORKSHOP WRAP-UP**

SESSION: FEDERAL GOVERNMENT CARD TECHNOLOGY REQUIREMENTS

Presentation: Evolution of the DoD CAC Program

Presented By: Mary Dixon, Office of the Secretary of Defense

File Size: 1,854 KB PDF File

Transcript Excerpts:

Information: We've been doing Smart Card pilot program since, I think the early 1990's, always coming up with great business cases but always the kind of dollars that you couldn't extract out of the budget. So it doesn't really count unless you can get to the money. There are lots of great advantages to Smart Cards, but no dollars.

Requirement: You are going to have to have the attribute of non-repudiation which they had determined was only going to be possible if you could do something to protect the private keys or the signing keys so that no one knew what those were, including the card holder. And you had the public key infrastructure program that was getting started, and they knew that their long-term goal was that they needed some type of hardware token again so that they could have more security for the PKI credentials.

Requirement / Lessons Learned:
I would say that you want to keep the number of media on your card down because every single one of those represents a single point of failure. And trying to make sure that all of those media all end up with the same approximate life expectancy, as you would like is difficult to say the least. DoD did the bar codes and the magnetic stripe primarily to support some legacy applications. They are there as migration technologies.

Information: DoD is issuing CAC at a rate of 6.66 to 9.30 cards per day per workstation.

Information: DoD chose to start with the cards issuance and at the same time is rolling out the readers and the middleware. But it does take a little time for everything to catch up. DoD is also in the process of doing some testing on 64K cards, contactless technology, using the 14443 parts one through four with FIPS approved algorithm on it.

Lessons Learned: So we said we will start small. We will start with the things we know we can do first. We will focus on that. We will design it so that we can evolve over time to do more and more things as time progresses.

Requirement: Well, we decided that when we move forward with the Common Access Card that the strategy would be that we would use this card as an authentication token and we would not use it as a data storage device. We would try to use the card to access the databases and use the data directly from the databases as opposed to storing it on a card to accomplish a number of objectives. Number one, we wanted to get rid of the problem of which data was more current, what was on the card or what was in the database. Secondly, we wanted to make sure that we weren't constantly rushing out to get the next higher capacity card even though it looks like we are. Finally, we also needed to mitigate our war fighters' concerns if they are captured. And if you put a lot of information on here, particularly information that would be considered privacy data or information that could be helpful to the captor, then this is not a good thing. And so we wanted to mitigate that risk by putting the smallest amount of data as we could on here

that helps to mitigate that risk. As well as mitigating the cardholder's concerns over privacy… As a result, the only thing that's on the card is also printed on the card for the military card.

Requirement: Now that's all a nice goal but we have to balance that with communications availability. So if there's an application that would need to use this card and it needs data and they're in a poor communication environment, then we might have to balance and agree to put certain amounts of data on that card. But that's always a balancing act and it's a risk mitigation and a risk management decision that gets made. But the going in position is we don't want this to be a data storage device.

Requirement: Security policy dictates the PIN be locked after three bad PIN tries. We resorted to Biometrics on the database to unlock the PIN so the user can get into their card. This function is not currently available in the field but this is the strategy DoD is working on.

Requirement: The other thing we're working on is our post-issuance portal. Need a capability to download applets to the card in the field. This is basically a web-centric approach to allow people to change their e-mail certificates using their identity certificate on their card should their e-mail address change. Ultimately, we want to get those capabilities as close to the person's desktop as possible so that they don't have to go back to the issuance workstations.

Requirement: We also have a contractor verification system which is to try to help us improve our identity management system for contractors. The system is not connected to the master database of users and therefore intensive paper process is in place to issue CAC cards to the contractors. We are web-enabling that process so the contractor personnel will be in the master database for CAC issuance.

Interoperability: So just because I have a card does not mean that I should automatically be granted access to any base or any building in the entire Department of Defense, because maybe I shouldn't be. But it does mean that you should be able to accept this as proof of my identity and that I am affiliated with the Department if there was some way to check to make sure that that card was still valid. Now until we get to the point where we are really capable of doing PKI in a much more rapid process than we can today in a physical access arena, CAC will allow us to be able to authenticate the DOD ID holders that are going to a different base other than their home base. CAC will allow to eliminate multiple credentials that a visitor must have if they have to access several different government buildings. So it's a visitor process that doesn't require you to have a second or a third or a fourth or a fifth credential depending upon which building you're going to.

Interoperability: The other part, the cross credentialing, is to try to work with other Federal agencies as well as our contractor partners. That we can accept each other's credentials based on the fact that we have a common set of rules about what we've done to identity-proof the individuals and that we understand how they have issued those cards as security of their process so that then if that's acceptable to us, we can do a process of checking the credential without having to get a lot of privacy information about that individual.

Limitations: All of a sudden somebody said, "Oh, wait – this isn't going to work if I take my card with me when I travel, that means I can't leave the card and my pin here with my secretary so she can read the e-mail." Some of our systems folks who worry about the secretary said, "Now, when you send an encrypted e-mail, is there some way to decrypt that e-mail, check it for viruses and then re-encrypt it without anybody knowing?" Well, no, that wouldn't be possible either. So, there are a number of issues that come up as you start to introduce CAC that people have to come to grips with and they have to figure out what does this mean in terms of their existing business processes. Some of them you cannot guess ahead of time because you just don't know about them. So these are the kinds of things that we work with.

Interoperability: So, we have a government smart card interoperability specification (GSC-IS) that allowed us to have two different vendors cards in our initial implementation of our system and we have not had any major problems. But this is not the end of what's inoperability. This takes care of interoperability at a high level. There's a whole lot of other interoperability issues or things that become important such as: we would like to reduce our dependence upon middleware piece because every time we change a card today or frequently, we have to then make some changes to our middleware products so that they can read the new card. This is not a good thing when you have three million computers and you have to touch every one of those machines every time you change a card. This does not give you the kind of flexibility you need.

Interoperability: So what are the other places where we need to move towards interoperability? Well, it would really be helpful if some of our operating system vendors such as – I understand the latest Macintosh computer now can read the CAC with no middleware. It shouldn't be just for the common access card, it ought to be something that they can do so that it'll read any smart card. And so that's something that would be of particular help to and a big savings to the Department of Defense in particular, and, I'm sure, to anybody that wants to deploy smart cards.

Interoperability: The reader industry and the contact in the contactless (ph.) world, the more we can get standards out there, the contact side is pretty well taken care of. It's hard for me to find anybody reporting a reader – a contact reader – that hasn't worked with any of our cards; but on the contactless side, making sure that we have the right standards so that they can be read. Some of the other things so that all of these things become standard and it becomes more like buying a – I'm not saying it should be exactly like – but more like buying a floppy disc.

Requirement: A lot of people get all enraptured with all the technology, but I have to tell you, that the key piece for DoD is identity management. Then, if you don't have a good way to identity proof that person that's other than the paper credentials that they show you, then all that technology does very little for you. For example, the airline industry probably doesn't care if I'm Mary Dixon, they care about two things. They care about, one, am I going to pay my bill, and, two, that I am not one of those bad people that's going to get on that plane and blow up the airplane. The technology strengthens that binding of the confirmed identity with a credential that you can carry around with you. That's my pitch because sometimes I think people forget about that.

Interoperability: *(continued from above requirement)* The standards of the interoperability make all of this affordable. So final statement here: "We need to have a common policy on identity proofing, so that we're all following the same rules within the Federal government, interoperability requirements and technology standards for physical and logical access." Because we need to know can I read this credential outside of my own building campus, or do I care if I can or not. And if I do, then this becomes more important. Do I want to have multiple identity credentials or do I want to have one identity credential that can be used in multiple places? So that the physical accesses or the logical accesses still granted by other people – not by this card, but that I can use this card to confirm that I am the person that was given the access whether to the computer system or to the building and to improve security. So all those things are important and can only be done if we have some common policy within the Federal government at least on these items.

Q/A for Mary Dixon

Q: Have you any hard evidence as to what failure rates you think you have because you have the contact, the contact list and other technologies on the card?

A: I can tell you that the biggest failure rate I have is with the barcode technologies because we have printers that are very sensitive to all kinds of the environmental debris and oil on your hands.

SESSION: FEDERAL GOVERNMENT CARD TECHNOLOGY REQUIREMENTS

Presentation: Federal Government "Card" Technology Requirements

Presented By: John Mercer, US State Department

File Size: 2,858 KB PDF File

Transcript Excerpts:

Information: There is a disclaimer in this that I am not giving State Department policy.

Interoperability: There is an organization called the International Civil Aviation Organization or ICAO and they write travel documents specifications. Well, I thought ISO wrote them all – well there's an agreement. There's a memorandum of agreement that establishes a liaison between ICAO and ISO – SC17, WG3 – which is cards and identity methods and machine readable travel documents that describe how all this takes place. This arose because ICAO wrote the first passport machine-readable specification in 1980 and by 1985, ISO had covered it with 7501 and they began not to say the same things. So when you have standards that don't say the same thing, you're going to have some problems.

Requirement: There are six methods of data storage that are contemplated for travel documents: 1) OCR-B which is the familiar one, just letters, 2) 2-D barcode, 3) contactless smart card, 4) Contact, 5) Magnetic stripe and 6) Optical memory. There are three sizes, or three forms, or three types of documents. We have 1) passport books which is in ISO language – ID3, 2) visa labels which are big (US size) and smaller (European size), and 3) ID cards – there are two kinds of ID cards: ID1, which is our familiar card that everyone else is going to be talking about and ID2 which is a slightly larger European ID format. The questions is, "What data storage methods will work for the various format types?" Well, OCR-B, 2-D barcode, and contactless will work across the board. There's a little problem with where are you going to put the contactless chip under a visa label or how are you going to embody the contactless chip into a visa label and the accountability of it. Potential solution was mentioned in the ID news article last week. Contact, magnetic stripe, and optical memory don't fit for three of my four or four of my five document formats.

Interoperability (Document Storage Requirement):
Now if I'm going to build a universal standard that I'm going to write to and expect other people to read and write to, contact, magnetic stripe, and optical memory are out of the question. I so realized a long time ago that ICAO was going to have to go with the contactless chip as their platform.

Requirement: Difficult to meet – Department of State has four types of services: citizenship status and where they are. So we've got citizens in the U.S., the State Department generally provides them passport services. Citizens who are abroad, we provide overseas citizens services. Non-citizens who are in the U.S. are dealt with by DHS. DHS provides services and enforcement. And non-citizens abroad, we take care of them and we may provide them with visas. It is difficult to issue visas to every visitor and even more complex to standardize different types of travel document and their form factors.

Requirement: Legislative – And the clear intent is to get a biometric ID on everybody… every alien coming into the United States in one way or the other. Section 303 of Patriot (or Border Security) Act says that the biometric on the U.S. visa is going to be selected by NIST in consultation with DHS and State and such. And biometric on the visa waiver countries be in accordance with ICAO requirements.

By reciprocity, we need to comply with ICAO requirements so our passports can be read by other countries machines.

Requirement: In May of this year, ICAO chose facial imaging – facial images – as the biometric of choice for global interoperability. Why not fingerprints? Well, there are a whole lot of cultures that don't like to give fingerprints. And actually, the question of the, you know, when are we going to start fingerprinting American citizens to give passports and the answer to that is well after I retire and I plan on being around for a while. That's kind of a non-starter - not a culturally acceptable thing. People from Australia say, "We're not coming. We won't go to your country if you make us to have fingerprints." We adopt… ICAO recommended facial image, which we figure is 10/12K anyway by way of size, a contactless chip is how it's to be stored for travel documents.

Requirement: Working towards adopting the newly revised government smart card interoperability standard v2.1 to which contactless has been added.

Requirement: We said we've got to get the digital imaging – that is printing picture on the passport instead of laminating a photograph.

Technology Selection Considerations: Where are you going to put your visa labels, how are you going to update it, what kind of common operating system are you going to have? And just because it's built to standard, doesn't mean it's going to interoperate. Now you have also the choice of biometrics – how fast are you going to acquire it, how fast are you going to report it, what's your level of certainty? What's the policy of the administration or laws that are applicable, the standards that support this type of business: what's our risk of failure? What's our security?

Interoperability: When ICAO… one of the weakest points of the ICAO section in the selection this May, was they said, "Okay, we're going to secure it all by some sort of PKI or maybe PKI light." Now PKI light is not a term ever defined which means that we don't know exactly how that's all going to play out and we're going to need to have something that will play out and be acceptable to passport readers of all nations.

Requirement: State is seeking information on how to allow a contactless chipless sufficient size to be embodied into a passport book platform so that it can function and read on standard ISO 1443 readers.

Requirement: Remote Card Production – now if you can get everybody to go onto an e-visa then you can begin to more easily accept an e-passport, but that's way not yet going to happen.

Integration: There are number of issues in integrating multiple technologies into one card. The real questions to be answered are: integration is really for whose good? Why are we doing this? Do we have an investment in this and how much do we care about the investment as we progress through the old system. What are the different stakeholders in our process? Will they be able to utilize the technologies? You're going to have reading among different users – how many iterations, how many times do I have to prove I'm me before the system accepts that I'm me. And then how much cost can the system afford? Take an example of airline industry, I don't know how the airlines are keeping to fly, how much more costs can they absorb in terms of identifying people? I don't know. And what's the back-up? What's your fail-safe? What's your fail plan? What if "A" doesn't work, what's "B"? And how much more efficient are we going to get this new system that leads more to the maps to the future.

Interoperability: Well, we have what I'm going to call the plug compatible problem – just because I built it to the standard, doesn't necessarily mean that it's going to interoperate. Both privacy and security are subjective. There are levels of trust – who is writing and who is reading what's written? How do you

prevent the ones you don't want to read it from? So there are levels of integrity and security and what's your authentication. It's my perception that ICAO's work has just begun with regards to trying to get all of these proposed contactless cards to actually interoperate with each other because now they have to get down to the specifics.

Information: No one trusts the chip. You have to learn to become accustomed to technology and accept it for what it is. Of course, that's why we chose 14443 which is zero to ten centimeters readability, so it's no way you can read it from space. Sometimes with this card, you have a hard time reading it from contact, but it has to work. Can card-based technologies enable privacy? Yeah, I think so, privacy from whom though? Can they enable security - yeah, but again, from whom or from what? Can biometrics be the saving grace – quite likely. If I have privacy and I have to put my fingerprint down to access a record and that record can't be accessed unless my fingerprint or face image or whatever is shown, then that's okay – that's a plus for the privacy guys. They have to know that.

Requirement: All of the document components have to contribute to the security of the entire document. You can't have a weak link in there. You know, on passports, even the glues in the paper and the threads all have to contribute to the security of the document. Birth certificate is a good example, where there are no standards. How do you trust one? What are the security indicators that says that's a valid record or not? They're lacking.

Standardization: Standardize birth certificates.

Standardization: Durability testing is big gap. The materials testing, the B-10 guys – they need a consensus on what the tests are to say that such and such durability exists on a document. They have to be done for performance level, a company guarantees a card: yeah, it's a ten-year card – how do you know? As in ten years happen since this is invented. What's your testing?

Standardization: Inability of biometrics to interoperate is a big gap at this point. They only interoperate at the image level. Minutia points and templates are proprietary solutions.

Standardization: I need tests for the comparison of the optical effectiveness and clarity of holograms or diffraction gratings. The folks in Kinegram® say, "We've got the best hologram." I'm going to agree with them. They look very, very good. What objective standards do I have?

SESSION: FEDERAL GOVERNMENT CARD TECHNOLOGY REQUIREMENTS

Presentation: Electronic Benefit Transfer: The Modern Benefit Delivery System

Presented By: Lizbeth Silberman, US Department of Agriculture

File Size: 1,066 KB PDF File

Transcript Excerpts:

Requirement: In terms of the technology requirements, it's generally compatible with the debit card system. Our regulations layout minimum requirements that the state card needs to have: ISO standards apply, they all need to have a four-digit pin, and a signature panel is required because we do require manual transactions with the signature when the system is not operating. But beyond that, the enhancements vary from state to state. There are some states that have digital photos; there are two states that are operating chip cards - Ohio and Wyoming. There are other antique counterfeiting technologies that states are using. Some are using holograms, fine-line printing, I mentioned the photos already and that's really a state decision largely based on cost.

Interoperability: We had been working on standards – X9 message format standards – which states adopted which allowed the systems to talk fairly easily to each other. There was also the issue of the retailer database that FNS&F maintains. We needed to be able to share that information with all states fairly easily and in an automated fashion - in the early days of EBT, we were using a paper system to do that. So once we had a mechanism that allowed us to share that information on a daily basis with all of the states and their processors, it made interoperability fairly easy to implement. And virtually, all states today are interoperable with the exception of the two smart card states which received a waiver from the legislation – that's Ohio and Wyoming – and Illinois which received an exemption until they implement their new contract in the fall. So, at that point, all the magnetic stripe states will be interoperable.

Requirement: In terms of performance, the regulations do set some standards for card performance. Generally, our expectation is that they be comparable to a commercial sector so that the recipients standing in retailer lines for EBT benefits receive the same level of service as those receiving those using debit or credit cards.

Lessons Learned: One of the real successes for EBT and the food stamp program has been our ability to piggyback on the commercial infrastructure. To the extent possible, we've tried to use the equipment that's out in the retailer location so that we don't have to place our own state… the government equipment out there.

SESSION: FEDERAL GOVERNMENT CARD TECHNOLOGY REQUIREMENTS

Presentation: Adding Physical Security Applications to the Common Access Card

Presented By: Gary Bruner, Department of the Navy

File Size: 1,325 KB PDF File

Transcript Excerpts:

Information: It's my office that is responsible for implementing CAC within my service.

Requirement: Today, the common access card really doesn't lend itself too well to access control. It has a magnetic stripe that many folks use, but that's a relatively insecure and legacy technology. So we were interested in trying to move ahead if we could.

Standardization: I think we're all interested in card implementation, but we have to get in sync with the functional process owners who own the stuff that the card will enable; otherwise, it's not going to work. We do a variety of innovative pilots across the spectrum of e-business within the Department of the Navy and we have the other mission of implementing the common access card program for the Navy. I've got to emphasize: we do not own the physical security domain nor do we own PKI, Information Assurance, we don't own Network Security, we don't own special security programs, force protection. Within the Navy a physical security community proceeds with developing and promulgating their standards. We have to partner with them to make sure we're in sync.

Requirement: As we use a common access card or a similar token for physical access control, there are three high level or over-arching requirements; 1) Increased security, 2) Reduced manpower requirements, 3) Reduced inconvenience to the member. We need not only to improve our security – that's probably the first goal with doing any of this stuff – you want to be more secure, but you've got to do it better, you've got to do it faster, you've got to do it cheaper as well. Reduced inconvenience is sort of an over-arching requirement. This area, I think, gets over-looked. We can come up with all these whiz-bang systems, but this area is absolutely critical because any access control system had better be pretty doggone transparent to the user or it invites work-arounds and those work-arounds compromise security.

Lessons Learned: Learn from pilots and prototype to define standards and policies.

Recommendations: If we don't do share the lessons learned, we may as well all go home because all we'll have done is roll out yet another stove-pipe system and that simply means it'll be some independent, non-integrated solution. And while it may solve a local person's immediate problem, it doesn't do anything for a wider audience or for the entire enterprise. We don't and can't afford to keep re-inventing the wheel on a "onesy" and "twosy" basis.

SESSION: FEDERAL GOVERNMENT CARD TECHNOLOGY REQUIREMENTS

Presentation: Transportation Worker Identification Credential – Stakeholder Brief

Presented By: Paul Hunter, Transportation Security Administration

File Size: 1,103 KB PDF File

Transcript Excerpts:

Requirement: TWIC visions is to improve security by establishing a system-wide common credential, used across all transportation modes, for all personnel requiring unescorted physical and/or logical access to secure areas of the transportation system. This is not just airports. This includes all modes of transportation. We're talking about mass transit, pipeline, and maritime environment. From a requirement standpoint, that's very difficult. Every mode has a different requirement and trying to collect those requirements and put them together in a single bucket is very difficult. Overall goals are 1) Improve security, 2) Enhance commerce, and 3) Protect personal privacy. Those are lofty goals but I think we can do it and interoperability will be a key in achieving those goals.

Requirement: They will be tough to establish. For example, a background check requirement in the maritime world is totally different from what might be required in the aviation world, what currently exists in the aviation world, and totally, again, for a Federal government.

Business Process: If I show up at a port or a terminal or whatever and I have a TWIC card, it's going to be the facility owners that are going to determine if I can have access - if I have a need to access. There are obviously other contingencies: I could show up at a port – a secure area of a port – and not have a TWIC, but still gain access. Do I need a TWIK? – probably not. Do I need to go through that expense? – probably not. Again, we don't define physical access – the local ports will define that. And then the last thing I want to mention is that our strategy is that we will not be installing readers at these ports.

Information: TWIC currently has many unknowns. Paul's presentation was more about the plans and their strategy than the requirements or the need for standardization.

SESSION: CURRENT CARD CAPABILITIES

Presentation: Smart Card Technology Capabilities

Presented By: Won J, Jun, Giesecke & Devrient (G&D)

File Size: 595 KB PDF FIle

Transcript Excerpts:

Capability: Current smart card technology is assess in four areas: 1) Card Operating System (COS), 2) protocol, 3) Memory capacity, 4) functionality. I would say there are two major categories 1) File structure system and 2) Java Virtual environment (Java and Multos).

Capability: COS – Java cards are trendy. Java cards are interoperable at the source level meaning you can write Java code that can be downloaded, that can be created into what's called a cat file and downloaded to the card. If you have a source code, you can tweak it a little bit here and there to download it to different smart cards.

Interoperability: Middleware and the applet software have to be tweaked because contrary to what we intended, not all Java cards are the same. I would like to say that if you plug in a vendor A card into a smart card reader with certain middleware, you can make it work just as you would with another smart card, but that's not the case. You have to make sure the middleware provider can read and communicate with a certain card and they need to program that into their middleware. And so Java cards are interoperable to a certain extent.

Capability: Protocol – And recently, you have seen the USB protocol being applied to s smart cards. And again, there are some advantages to this because it has higher speed, as well as if you can consider the card reader aspect.

Capability: Memory capacity – We typically see 32K byte EEPROM smart cards these days, as you've seen it with the contact cards. 64K is available, 120K is available to some extent -- that may be on the horizon.

Capability: Functionality – In terms of functionality again, smart cards are used for encryption as well as digital signature applications, triple DES would be used for encryption. On card key pair generation -- this is also a hot item. You want to generate public/private key pair on the card for some of your applications and perhaps store that private key on the card. On-card biometrics - that's also a hot topic. An on-card biometrics engine is where you have the matching algorithm on the card. So you would store your fingerprint template on the card, and maybe an applet or program that can do matching. When you present a live scan of your fingerprint, the host system could turn that into a template and the template would be sent to the smart card. On the smart card you would do the matching and then a yea or nay response would come from the smart card. That's what I mean by on card biometrics.

Current Trends: Again, it's Java cards, whether it be 2.1 now, or 2.2 at the end of this year. Global platform, 2.01 prime moving on to the next version: 32K to 64K EEPROM memory, and on-card key generation. Biometric on card matching has not quite caught on yet. It may catch on in the near future. There's a hybrid and composite card bodies. With composite card bodies, it's worth mentioning that I believe for some of the government applications, it was necessary that the card body had to be very durable. So there's been a lot of progress made to come up with a very durable card body. FIPS 140-2

level two or three. That's the current requirement, the current trend. Some of the reader products that you see in the market would be a small reader device with a battery and display that allows you to read a smart card. And some of the applications would be for a one-time password. Insert a smart card, based on the smart card's internals, it can generate a one-time password that can be used for network log-on or remote access user log-on. And you also see many PDAs that come with smart card readers. Some of those high capacity devices have a fingerprint sensor, as well as a lot of memory. And you can store a lot of information on those.

Requirement: I believe DoD has been leading the effort of coming up with the most refined requirements for the government application. These are some of the requirements that we've seen. They have been discussed in the past, Java card open platform, GSC-IS and 32K memory. But I think it's moving on to 64K now. Of course 3DES, RSA algorithms, and FIPS are the algorithm requirements. On card key generation - I think currently the performance requirement is for 30 seconds or less. And I think many of the manufacturers are doing much better than that. Requirements on the horizon -- it's got to be better, greater and faster. So: a 2048 bit key length for RSA operations, perhaps on-card biometric verification, - whether it be fingerprint, Iris or hand geometry, and PKI support on contact cards. That may be a little bit of a challenge for contactless technology, but is developing very fast to meet up with the requirements. Hybrid dual interface cards -- I believe currently, the Federal government is really looking at hybrid cards and not really dual interface cards. There are some issues with dual interface cards. For example, accessing different parts of the memory by using the contactless portion. And doing complex functionality using contactless.

Interoperability: The next steps would be developing new standards that can address these new requirements that are coming up, as well as maybe just updating some of the existing standards to catch up with the existing technology. And I think someone else stressed this issue, but I feel strongly that all of these new products need to be validated or tested to make sure that they conform to certain standards. Because anybody can claim to conform to certain standards, but you don't know until you test it.

SESSION: CURRENT CARD CAPABILITIES

Presentation: Ultra-High Density Barcodes

Presented By: David Young, De La Rue

File Size: 7,246 KB PDF File

Transcript Excerpts:

Capability: Ultra High Density Barcodes (UHDB) – a description adopted to identify barcodes, i.e. data stored within a machine-readable strip, which have the ability to store potentially unlimited amounts of data.

Information: New generation high-density 2D barcodes can store large amounts of data (16-32Kbytes) on printed documents and cards. They do not have constraints over aspect ratios, capacity, resolution and size and work with laser engraving, inkjet and conventional laser printers. With the latest PDB codes, any digital scanning device, including readily available office equipment, can be used and the decoder software works independently of the coder resolution hence will read all codes, however dense and however printed. As a result, it is now possible to encode ID cards, visas and passports with full biometric profiles and full color mug shots as an off-line alternative or back up to IC chips, optical laser stripes or secure networks. ICAO has recognized this potential in its recent recommendations.

SESSION: CURRENT CARD CAPABILITIES

Presentation: Optical Memory Cards in Federal Government

Presented By: Stephen Price-Francis, LaserCard Systems Corporation

File Size: 1,255 KB PDF File

Transcript Excerpts:

Capability: First, to look at the key characteristics of optical memory card, the one that stands out and the first thing usually mentioned by people is the high data capacity. The next key feature, one that is very important of course in the arena that's being discussed recently, is security counterfeit-resistance in the area of secure ID. Most important in environments where government issued documents have lives of five or even ten years is durability and reliability during that period of time. Very important where border security is concerned is the speed of transactions. And then of course, standards compliance is naturally very important.

Information: In some applications, the optical cards are recycled and some have been in use for many years. I won't say that some have been in use for ten years in this environment - I honestly don't know. But certainly some have been in use for many years. They are treated in the most inconsiderate manner in some of the most austere environments we can imagine.

Capability: And talking about the combination of optical memory with contactless technology, just so you can see it, it's a reader that actually reads the laser card optical memory card and the cubic, as it happens, contactless chip which is integrated in the card.

Requirement/Interoperability: A recent key developments in the technology of the world of optical card technology is that the optical memory has been combined with contactless technology. And as you've heard today, there's a great deal of discussion about ICAO recommendations for the use of this technology in a global interoperable system of machinery that will travel documents.

Interoperability Issue: So I arrive at JFK today as a trusted traveler where they use a particular kind of fingerprint recognition and I store my template for that kind of fingerprint recognition system on the contactless chip and use it within the airport that day. If I'm enrolled in an airline's frequent flyer program, maybe it's there permanently. But I go to another airport where I'm not enrolled and they use a different kind of system, then that fingerprint can be enrolled and the template can be stored on the contactless technology.

Requirement: In the proposal that we've made to the ICAO environment, you have time-limited access, you have physical limitations on access, and you have facilitation applications. And intelligently, you can mix and match these using more or less any kind of biometric that is likely to be encountered in this environment.

Requirement: And talking about the combination of optical memory with contactless technology, it's a reader that actually reads the laser card optical memory card and the cubic, as it happens, contactless chip which is integrated in the card. It is not only the card, now you have to enable the reader / infrastructure to use the technologies on the card.

Information: But it's actually very important that you don't have a ubiquitously available technology that you can pick up off the street, buy a development kit and play with it and figure out how it works and find

people all over the place who know how to use it. This is a risk - this is a gap in your security. It's very important, there are very few people, actually, who know how a technology is put together and what the total security system is.

Information: What of course we always have to look at in this situation is the total cost of the system and the business case attached to that system. So the cost of the reader I won't say is not an issue, but it's a component that has been taken account of by some of the major users that I'm discussing here.

Information: There's very little infrastructure for optical memory card on our borders, but it's coming as I've just described. And once it comes, it will expand further, of course. And we can expect to see over time that the infrastructure for reading optical memory cards will become more and more ubiquitous.

Information: Stephan went into the details of capacity, security and durability of optical cards.

Capability: But what we're talking about here is officially issued cards with data on them. The data cannot be changed. It's an irreversible process. The medium upon which the data is stored enters a state from which it cannot be returned to its original state. This is clearly very important, because it's not possible to do, as people do with official documents today, is get an original one and change it to someone else's identity for example, by changing the photograph. It's becoming more and more difficult, of course, as time goes by. But this is still what people do. It's impossible to do that with optical memory because you cannot change the data. But there's another very important point here and that is by the nature of the memory, the optical memory, in each of the applications I've described, there is a unique matching between the physical format, the hard-coded format of the memory and the device which reads and writes the card. This is extremely important, because it's a mutually exclusive relationship which enables, for example in Italy, if someone tries to circumvent the system and use blank cards for fraudulent issuance, the encoders will mindlessly disable the card without reference to the host, without reference to an application.

Capability: One of the techniques used by all of our government customers is to laser engrave eye visible information into the memory, which you can see here. This is a feature that we call the embedded hologram. The piece of memory itself is irreversibly and permanently marked with eye-visible information that identifies the cardholder. So in those situations where electricity is out, whatever it is, the inspector can make a judgment about the person's identity by looking at this information. It helps to verify what is printed on the other side, which criminals will attempt to change. And of course, it can be verified against the person. David talked about the three-way check; we have a four-way check here. We have a printed image of the person, laser engraved image in the optical memory, which cannot be changed. And, if we're using it, the biometric match.

Interoperability: We'd like to see GSA and NIST between them get their act together on the equivalent of the IC chip inter-operability spec. We think that would be a big plus for the use of the technology in the Federal government environment. We'd also like to see NIST look at the issue of best practice for the combination of optical memory and contactless technology, with a view to looking at its use in the travel card arena. In the international inter-operability sphere, based on the fact that the smart border action plan exists. It calls for harmonization of an inspection infrastructure. It implies, at least, the controlled exchange of data. Standards are needed there and I think NIST and its equivalent in Canada, perhaps, could be looking at that. And the controlled exchange of data is a very important issue where privacy is concerned and David touched on that. He suggested that a card with a lot of data on it is potentially a privacy infringement. I have a vested interest here, which doesn't need declaring. But I have a personal preference for the idea of carrying my data and using it or allowing its use under the principle of informed

consent rather than government storing all my data on big brother databases all over the place which are inter-linked and checking, perhaps, what I'm doing wherever I go.

Interoperability: I talked about the unique relationship between the readers and the cards. It's only an authorized reader that can read the data on these cards. Not any old reader. So as long as the owner of the card is intelligent enough and has been educated well enough to understand that you give this card to a border inspector, the border inspector is entitled to look at xyz, then the privacy issue, again, can be dealt with under the principle of informed consent. Second, global inter-operability: The legislation following 9/11 called for various issues related to biometrics, tamper resistant documents. And in particular, it called on this NIST to play a part in establishing standards for storage of image, storage of biometrics and so on. We think that's very important. And the third area where we think that some standards are needed is the transportability of original biometric images. By which I mean face, fingers, irises and so on. We have the White House office to science and technology policy discussing the need for 250K of images: a couple of facial images, all ten fingers, possibly, both irises. All at a resolution that then could subsequently be used for on the spot ID verification and the generation of a template. So this might come back to the question about how much storage you need. Maybe you need 250K or more. This process is recommended both by NIST and ICAO.

Interoperability: To talk a little bit about biometric transportability, David quite rightly pointed out that really standards don't exist today for the real transportability of biometrics. So you have these proprietary systems between which there is no effective interchange. Now an awful lot of work is going on, both by NIST participating in the standards activities of insights M1. And one of those efforts is working towards an exchange standard. So you start with an image and you end up with something at the other side. And the objectives, of course, are to get inter-operability compatibility and a clean data exchange.

SESSION: CURRENT CARD CAPABILITIES

Presentation: Global Platform: a Secure Dynamic Multi-Application Smart Card Management

Presented By: Marc Kekicheff, Global Platform

File Size: 706 KB PDF File

Transcript Excerpts:

Information: And I'll try to explain a little bit that the card is not that important at the end. But I think it is more important to look at what is behind the card and how you manage the card.

Capability: So this is my case for multi-application cards here. There is a lot of cards, a lot of ID cards, all are the better and the greatest ones, including these good INS cards, which I have one of them, being a permanent resident of this country. And I have to be careful about what do I manage. And all of these have different trusts, authentication, security features, and IDs and PINs and passwords, and parametrics and this and that. So, the idea of a multi-application card is, potentially this, which is, I can pay, I can access my hotel room. I can have my house record, I can use public transportations, I can use either a mobile phone, I can have my loyalty programs when I pay and I can prove my ID to the government, this is on the net on the physical wire.

Capability: So, what is the design of this multi-application card? It will very depend on the relationship between the different actors. And this is what we call * platform * business relationships. So, a multi-application card has multiple applications on the card, not necessarily from the same issuer of that card. It is a card that can work with different applications coming from different entities. And each of these entities have their own schemes, their own security schemes, their own way of managing their data, their own way of making transactions very fine, it is really you. It is up to these different business entities to agree or not to share the same piece of hardware that will be carried by the cardholder at the end of the day.

Requirement: I need to have a card. I need to have a reader that reads that card. And I need to have a system behind that reader that needs that card.

Capability: So, again, the way you design your systems, whether you put all your security features only on the card, versus checking anything automatically with an online transaction, is a design issue. It is up to the designer of these applications to say who on this application is going to verify what, at what time, and under what conditions. It's not the card by itself that they're going to decide if you can enter the country or not. It is the fact that the card has these characteristics, these pieces of data, whether they match the security requirements, and it is being checked by someone who reads that card, reads that on that reader, and says you're okay to get in without going online on the system, or you're not okay to get in as long as you're not authorized by online.

Capability: If I have multi-application cards and if I have multi-application terminals, how I am going to know what application is on what card after I have issued that card? If I am about to add and delete applications remotely, update them, on the card and on the device, I need systems to manage that. It is a typical IT issue. Which is, how to load the applications, how to track them, how to know they're at the right level, they have the right data. So we have typically in a card, any type - any type of technology of cards - we have a typical infrastructure, IT infrastructure of systems, where the card is just the tip of the iceberg. We have distributed software. These are on the card, on the terminal, or on both. We have

hardware to track, to make sure that we're at the right level on the hardware. We have security features to enforce on the card, on the device, on the host. And we have customizations to follow up, because that card is for one cardholder, so it is personalized to that cardholder. So we have in, what I call a nice IT management, from a systems perspective, I need to think of software, hardware, security, and customization. And I need to do that in a consistent and efficient and cost-effective manner.

Capability: I need to have systems that tells me about cards - are they lost, are they stolen, are they going to expire, do they need to be re-issued, what type of applications are on them? Do I have more than one? If yes, who are the application providers? Where do I get the data to reload on that card? Whether I need to update it? Is this card being recorded as stolen, or reported as stolen? Do I need to lock it or block it when it shows up somewhere? To destroy it? It's usage? All of these issues are systems issues. They are done in the back office of the systems. And these systems are actually the most complex to manage, to set up, and to run. And these are more expensive than just multiplying the number of cards in the streets. Which is very easy, and becoming cost-effective more and more.

Interoperability: So, what we call interoperability in our world, in the world of Global Platform, isn't interoperability from the infrastructure perspective. It is how do these different pieces of the puzzles work together? How can I run my smart card or my CARD* management system, how can I run my database, how can I run my application software that I need to load on the cards? How can I personalize my cards? How can I issue them? How can I track once they're issued? How can I update them? And all of that is, as well for the card, as for the devices. And our interoperability is not to define what the credit card transaction needs to do, or what a passport ID needs to do, or any commerce, or wireless telephone conversations, or online banking, online commerce. And of those are vertical segments for us. What we provide is infrastructure for all of these people to securely do their transactions and be sure that nothing in their data, nothing in their security, is being compromised by the fact that they share the same infrastructure or part of the same infrastructure.

Capability: On the trust model, I listed a couple of them. And it goes from what we call ISSUER initial centric model, where the card issuer is controlling everything that goes on the card. Nothing can be done to the card except running a transaction, without the issuer being involved. That means when I want to add a new application on the card, it is the issuer who is going to do it.

Capability: And we have what we call an application providers empowered model, where I can share or sub-divide my cards into virtual cards, where someone can act as the issuer of that virtual card. So it is like having a physical card that is split in virtual cards. Each entity, each virtual card having its own card issuer or its own application provider, that can run this piece of virtual card like it was a separate card, and do whatever he wants on that separate card. So this is showing infrastructure on that perspective.

Interoperability: And we're trying to promote interoperability across industries, so we work very heavily with a governmental organization like NIST here in the U.S. or NIX in Japan, or Europe's * chapter in Europe, as well as with the telecom industries, with the finance industries, these are the three strongest industry players within Global Platform today.

Capability: And basically we have five basic objectives, is interoperability, and I explained what we meant by interoperability; infrastructure, management level. We have scalability; it is any number of applications. The only constraint is the size of the memory. So if the size of the memory is 1 MB, 2 MB this is the limit. The limit is the hardware from that perspective. We have flexibility - As I said, any type of applications, or any type of industries. And I gave you the three major industries we have that have implemented Global Platform technology today. Portability - because if I want to be able to have different types of applications, I cannot predict on what card they're going to be. So these applications

needs to work on different types of cards. And of course, security, because if I talk about typically smart cards, usually we have high security features on this.

SESSION: CURRENT CARD CAPABILITIES

Presentation: Contactless Card Capabilities

Presented By: Richard Smith for Marc Gartner, Cubic Corporation

File Size: 2,594 KB PDF File

Transcript Excerpts:

Requirement: Contactless technology has grown to a large extent out of the transportation over the last two decades. I think that's something most of you already know. But transit today is not just subways and rail, but it encompasses a whole new set of markets including buses and taxis, heavy rail, and even e-commerce - all with a single fare card. The other major move that's going on is from transit to security. And not just through Homeland Security, the Homeland Security Department, but in other kinds of security that we'll talk about. This has to do with not just borders, but seaports, airports, etcetera.

Capability: Cubic memory cards maintain a simple state machine with protected space, key management, and security procedures. The memory type on this particular chip is called Ferro Electric Random Access Memory. It is extremely fast. And it was selected specifically for its speed in transit applications. I think it's something like 100 nanosecond memory access time. The card itself can store up to 16 applications of the 2K variety. And there's a 32K variety of it that can actually store many, many more applications, or have ample room for biometrics.

Capability: I think the contactless SmartCards themselves provide flexibility, more memory, high levels of security, fast transactions, low maintenance. You're seeing a lot more open source issues and successes. For instance in the London transit system we have MyFareA and GoCardB working simultaneously with the same readers and turnstiles. And the bottom line to the whole thing is, I hate to coin it, but "better, cheaper, faster" is the idea behind contact-less.

Capability: And where transportation is really moving is towards the regional process. And when we talk about regional process we're seeing the combining of transit, not necessarily authorities but we're going to the point where you can use one card across for seamless travel across linked services, with consolidated ridership and revenue reporting - basically seamless travel with one card. The Federal government, we're seeing a big push in particular in federal buildings for the U.S. Visit. We're seeing borders and ports, a need for more speed in some of those applications. The same types of things that we're seeing in the security world for DOD and for the other Department of Transportation and stuff, we're also seeing applications in the commercial world for the same types of security.

Requirement: I don't necessarily mean that every driver's license and every Affinity card is going to have three or four technologies on it. But I think we're going to see standards developed and practices developed that enable the technologies to co-exist and be used where they are appropriate. And I come back to my earlier point, and I hope there are still people from NIST here. I'm making an appeal for that activity to be undertaken beyond just contact and contact-less chip.

SESSION: SECURITY AND PRIVACY ISSUES

Presentation: Ensuring the Integrity and Security of ID Documents with Digital Watermarking

Presented By: Robert Durst, Digimarc ID Systems

File Size: 1,821 KB PDF File

Transcript Excerpts:

Security: We're pretty much an additive in terms of what we bring to the party with respect to document integrity and security. And the general take-away is that this is a technique that lets us embed digital data directly into analog data that was originally derived from a digital source. So what that means is that for those of you that are new with modulation and de-modulation, is if you have a signal that is modulation of intensity of light over a space, we can basically use a spread spectrum technique to embed digital data directly in it.

Definition: What is digital water marking (DWM), what's this all about? Well, first of all, it's a set of proven software technologies that are used to covertly encode and decode digital information in digitally derived analogue in digital content.

Information: Most, if not all print that you currently see in any form including an I.D. card starts out as data. Now most people don't think of it that way. But we understand the computers are generating everything we see in a printed analogue form. Because of that, we can use that digital source signal and modulate it so that we can use, we can convey across what we call the analogue gap. We can embed the data and then re-extract it on a scanning basis and tie that element back into the digital infrastructure.

Information: How is it currently being used? Well digital water marking is not something that's just coming out of the box. It's been used extensively in both printed and electronic digital photographs.

Information: Digital water marking is a part of all the adobe sweep products if you're a free lance photographer and you're trying to put photographs out on publication sources, the Internet, you can embed digital water marking in those photographs so that you can trace back to copy right material.

Information: It's used in digital advertising, of commercials and for news feeds and for other video segments and MP3 files and a lot of other applications like that to track digital content that's converted to analogue in either broadcast, printed, or represented electronically.

Information: So it's a pretty well established working technology and I guess that's the second authors message here which is we're not re-inventing the wheel here, this is something that's actually been demonstrated and works in a variety of places. We're just applying that technology now into the identification space.

Information: And finally, we've done some work in the Defense Intelligence Agency where if you think about satellite imagery, we can incorporate digital watermarks to both track the content, analyze and also collect information together across multiple applications.

Information: So the technology itself is derived from a whole variety of disciplines including image processing, signal processing, information theory, communication theory, cryptography, color science and print technology. It's not only how do you put the data in using spread spectrum techniques, it's how you then

take that modulation once it crosses into the analogue space of print and then reconstruct it from digitalization after that, and convert it back into, into digital and extract the covert information that's in the original digital covert channel.

Limitations: Now our payloads are not large, we're not a data carriage in the sense of something that would compete against a two dimensional bar code, or an optical memory card or a smart card chip. We're about 56 bytes right now. But it's enough of a marker to put in where we can convey a lot of relevant information regarding the content.

Limitations: And one of obviously our research areas we're pushing that limit again. I've done some stuff in the lab where we can, we feel we can easily get up into the 100 byte, I'm sorry 100 bit level and probably beyond that taking out some of the constraints in terms of the print recovery with digitalization.

Security: So the concept here is you're taking information and you're embedding it in kind of modulated free space inside the spatial in case of an image, inside the spatial frequency of that image. And it's a way of smuggling information covertly in band in the signal. We can either carry fixed data or variable data.

And it can either be personalized, in other words it can be uniquely related to that particular photograph. It can either be descriptive of it. It can be age information; it can be unique identification, registration information. Or it can be serialization. For instance, in the graphic on the background of a card we can have a serial number so that we know the sub-straight word originated from what printer was used on.

Security: To find this information in the code. You have to have detailed knowledge of the algorithms that were used and the parameters and the protocols they were using. This gets back to the spread spectrum elements. You need to know a lot about how you'd actually encoded the signal in order to look for it to figure out how to extract it. You also have to compromise the encryption keys. We're not using triple DES with a 56 byte payload obviously we're below those limits. And in fact one of our goals is to get up to the point where we can use like 128 bytes and do something like a triple DES string.

Security: And we also currently use convolution coding; which they're not as secured as, as true cryptographic deciphers or cryptographic techniques. It's a slash cipher technique that has a fair degree of reliability if the content is buried is on a circular basis.

You have to also know the knowledge and location, knowledge of the location of the DMW. They can be distributed across the image by t they can also be stored and given locations. So in other words, you can have part of the content that looks like a normal photograph and part of it containing embedded data unless you know where to look you wouldn’t even know where to begin the analysis.

Security: And you have to have knowledge of the specific data contained in terms of doing the decode and this is true of any, of course in any decipher crypto cracking technique. This is the next point is very key. The presence of the DWM is not obvious to someone not looking for it. And even if you are looking for it, you may or not be able to determine whether it's in the image or not.

Information: We can also use it [*DWM]* with non-conventional printing technologies. We've done it in visible and UV inks, because it gives us the ability to again modulate in space and modulate in intensity.

Information: In fine line artwork in which are all security elements that are routinely used in currency and security documents. We can now make them data carriers as well and tie them in to the interlink structure.

Integration: And we've also done some work with OVD's which is holograms and Kinegrams®, we'll be hearing more about Kinegrams® shortly. Well since that also is an image, it's generated in a different way

that has an intensity pattern and a spatial pattern and we can actually put a digital watermark in the hologram content and in the Kinegrams® content and make it machine readable and digitally link back into the other content without having to burn holes into directly.

Information: *(continued from above requirement)* You can use it for sub straight verification serialization, identification and manufacture and printer origin. For instance, one thing we can do fairly and we have done very straight forwardly is we can have a given printer insert a watermark in what it's printing to determine its serialization of origin. So for forensics you can go back and say, well where did this come from. And say it came out of this particular production process, and this particular run, with this particular printer. So you've got a link path forensically right back to the origin point of that item and of related items.

SESSION: SECURITY AND PRIVACY ISSUES

Presentation: Enhanced Physical and Logical Security

Presented By: Wayne Tompkin, OVD Kinegram®

File Size: 702 KB PDF File

Transcript Excerpts:

Information: High-quality, secure identity documents and cards protect the governments and the issuing agencies, but they also protect and assure the rightful bearer of these documents and cards that their rights and privileges will be respected.

Information: Visual security is not only important to the issuing agency to make sure the bad guys don't come in, but also it helps give the people an assurance that their rights (for travel, entry, etc.) will be respected.

Definition: The Kinegram® security device is an optically variable device. The Kinegram® has been used for over 20 years and is a unique, high-security, non-holographic authentication feature. Primarily the Kinegram® was developed as a visual authentication feature to prevent people from copying and counterfeiting documents, banknotes and cards, yet the Kinegram® can also contain machine-verifiable and machine-readable features.

Information: The philosophy behind the Kinegram® is relatively straightforward. We make use of a very secure, unique technology. But what's important is that we don't aim for very complex features because this complexity in itself (although may be very difficult for people to counterfeit) does not ensure ease of use. The Kinegram® security device is easy to verify, easy to communicate and hard to copy.

Requirement: The first-line security features should describable in a few sentences, and it should be possible to authenticate the feature in a very short period of time-- in a second or so you should have a feeling concerning the authenticity.

Requirement: It is very important that you can incorporate the security feature onto your document or card so that they last long enough. We have over 20 years of experience and we have proven and tested ways of incorporating security features so that they stay on the documents for up to 10 years. It's important to have experience and not to underestimate the issues of durability and lifetime.

Technology: We use a diffractive feature to represent data; this data can provide a highly secure link to important data or information, for example, to the rightful bearer, document data or card data.

Trend: We notice the trend of countries moving towards chip cards as soon as the legislation permits it. And of course this is borne out by the growing number of chip cards that are in circulation now.

Information: Risks increase with incentive and hackers and thieves learn in parallel; this is borne out by the history of the chip card. Chip cards are permanently here and their use is increasing. Thieves are not going to go away; they will find ways, as they've always found, ways of attacking chip card security. Once the chip card succeeds in being implemented, the incentives for their compromise will increase.

Information: You should stay more than one step ahead of the hackers and counterfeiters. Once chip cards begin to be implemented in large numbers in the United States (e.g. following the implementation of the

TWIC cards and all the other federal programs) you will have more people trying to compromise the chip-card security while the incentives will be so great.

Recommendation: Our proposal is the Kinechip®. The Kinechip® solution uses disjunctive technologies. This means that you combine chip- card technology with a second technology which is completely different to the chip-card technology. The idea is to combine diffractive optical technology with the state of the art chip card technology.

Technology and Integration: The idea is to have a diffractive optical technology, a Kinegram®, and combine it with the state of the art chip card technology. The secret is to combine these two technologies, so that the optical technology enhances the chip-card technology. We want to impart physical security and additional logical security.

Security: Physical security is important, while it allows you to say this chip card is real, this is not a copy of the chip card.

Security and Integration: The problem is that the information on how to attack chip cards is very easily disseminated. We enhance the security measures for chip cards by adding a non-holographic diffraction technology. The Kinegram® itself allows quick and easy authentication as a first line feature and the machine-verifiable Kinechip® enhances the physical and logic security of the chip card.

Security: We can classify three main threats against the components of chip card security: data manipulation, re-engineering of chip cards and stolen secret keys.

Requirement: The Kinechip® is used to secure specific data in the chip card; this specified data will be constant over the lifetime of the card, e.g. fingerprint data or personal data. You take this constant data, apply an encryption algorithm to this data to get a digital certificate, which is then stored permanently in the diffractive linear code of the Kinechip®. This digital certificate which is in the diffractive linear code of the Kinechip® can be any length up to 1,000 bits. Typically 80 – 160 bits are used in the digital certificate of the Kinechip®.

Security: We use an irreversible process, laser ablation, to write the data. You cannot change these data bits from a ‘1’ to a ‘0’ or from a ‘0’ to a ‘1’; you can erase a data bit (e.g. by destroying it), but you can't change it. Physically different diffractive structures are used to represent a ‘0’ and a ‘1’.

Security: The security of the Kinechip® can be added where it is needed. This is an insurance policy: the Kinechip® is a security feature which can be incorporated today and used when the need arises. You can add the KINECHIP onto your chip card and it does not alter the use of the chip card itself. You can put the diffractive linear code of the Kinechip® solution on your chip card and actually never read it should the security of the chip card never be compromised. If you have no security problems ever, you actually don't ever have a reader ever to read it. Similarly, readers for the Kinechip® can be implemented in those positions which require maximum security or in those positions which are particularly vulnerable.

Interoperability: The chip-card functions are not altered in any essential manner by the Kinechip®. The Kinechip® verifies the information of the chip card, thus the Kinechip® does not alter or impede the chip-card functions at all. A standard reader for the chip card can be upgraded to the reader for the Kinechip®. Thus, the Kinechip® solution is entirely compatible with standard chip card systems.

SESSION: SECURITY AND PRIVACY ISSUES

Presentation: The Identification Process Deconstructed

Presented By: J. Scott Lowry, Caradas, Inc.

File Size: 37 KB PDF File

Transcript Excerpts:

Information: Anyway, what we're going to talk about today is the identification process. How's that? Ok, yesterday and today, you're going to hear a lot about what we consider containers in the identification process really not identify vehicles. And we're going to try and differentiate by what we mean by that. And really that flows from the notion of doing this whole debate over the last 7 to 8 years is identification authentication a policy problem, or is it a technical problem. I think the debate largely started out as being a technical problem. I think people have come to believe that there are more policy issues related to this than technical issues, and the technical issues are probably largely solved. What are we going to talk about? Well, to get there, we're going to de-construct the identification process, and understand each of those generic parts of that process and understand where technology comes in and where policy comes in and what our expectations are of each ok.

Information: To do that, we're going to make some basic assumptions about all of this. First of all, the identification can in fact be broken down into generic phases or discreet generic phases. Secondly, that there are 3 principle players in the game. There is a subject, something or someone that needs to be identified, there's a credentialing authority, one who will do that process, and then there is a relying party, one who will in fact rely on that credential once issued.

Information: And that each of these participants in the process does in fact perform different functions, and based on those functions it creates a different set of risks attendant to those functions. And there are three types of risks we're going to talk about. Fundamental risks, activity risks, and derived risk. And given that these risks exist, we'll then also look at how do we solve or mitigate these risks, and we'll postulate that there are really are a finite set of risk management tools available to us, those will be technology tools, and those will be policy tools largely.

Security: And then finally, as we look at any identification scheme, there really are a various issues that determine the viability of that scheme. And while we sort of dream about doing this a variety of different ways, at the end of the day if these 3 or 4 issues can't be overcome, you do not have a viable identification scheme.

Information: (*Identification process*) Those phases are as I said earlier involve the activities of the various participants in that process. Those activities bring with them a level of activity risks, within applied risk management tools to those activities to mitigate those risks, then finally we look at the policy issues related to those to see if it all works.

Information: (*Identification process*) Ok, the participants, obviously the subject that's the individual or object wishing to be identified. The credentialing authority, this is the trusting, trusted organization that will do the identify proofing of the subject and create the credential, identity credential to be then used by that organization, object, or individual going forward. And then, there’s the relying party or the organization wishing to rely on that credential.

Information: (*Identification process*) Then let's look at the generic phases of the identification process. First of all it's the identity proofing by the credentialing authority. Secondly, it is the creation of an identity credential. And we really do look at these as two very, very different phases, and we'll make a very big meal of this later on in the discussion. Once you've created the identity creation then there is the presentation of the credential to a relying party and finally the acceptance of the credential by the relying party.

Security: Let's examine each of these phases in a little greater detail. Phase one, the identity by the credentialing authority. Really it begins with, "Hi I'm Scott Lowry; I'd like to get a Drivers License." So, in effect, I'm applying for a credential. At that point in time the credentialing authority will perform some sort of investigation to determine whether he really believes whether I'm Scott Lowry. And once he has made a conclusion relative to that, he is then willing to make an assertion that I'm Scott Lowry. And again, at the end of the day it's his best guess, that I'm Scott Lowry. So my Drivers License doesn't really mean that I'm Scott Lowry, it means that the State of Virginia thinks I'm Scott Lowry, based on some investigation they have in fact done.

Information: After we've, after the credentialing authority has decided is willing to make an identity assertion, it then has to make a packaging decision. And that really is essentially a form factor issue. I'll give you a password; I'll give you a letter; I'll give you a smart card; I'll give you a plastic laminated card; whatever. And the key issue here is as I say the credential is a symbol of this credentialing authority's identity assertion, it is not my identity. Think of it the same way as the flag is not freedom, but the flag is a symbol of freedom ok.

Information: So if you look at the inter-relationship between the two, it is the inner play between the strength of the identity proofing process, and the strength of the packaging process that creates your assurance of confidence levels in the identity credential.

Information: The by and large, much of the debate is focused on the wrong thing. We focus on the strength of the container without understanding at all how the initial identity assertion is created. And I think that is in fact what the challenge is.

Security: Biometrics again are not identification, they're an ability to prove that you are the same person that the credential speaks to as opposed to in it of itself identification. Secondly, he, once he has confirmed that the individual presenting the credential is in fact the rightful owner of the credential he has to understand is the credential an authentic credential, i.e., it's not counterfeit.

Information: Types of risks in the identity process. As I said earlier there's fundamental risks, activity risks and derived risks. We'll go quickly there. Look at some examples of each of these. A fundamental risk at the end of the day, for a credentialing authority, they can only get one thing wrong fundamentally. They got it wrong. From a subject stand point; the only thing that the subject is worried about is that someone doesn't steal his identity. And relying party, what can a relying party do wrong, the end of the day, he gave an unauthorized access to somebody. So these are sort of fundamentally the worse case scenarios for each of these players in the game.

Information: Some examples then of activity risks that are sort of day to day part of this process and really we've put in place technology and policies to litigate these types risks. At the end, its data is lost, stolen, or tampered with.

Information: ... Now, technology is all over this process you know we're surrounding it with PKI, we've got triple DES we've got a lot of different things, but at the end of the day, technology really introduces risks in four discreet areas. Any time we have data collection you have a chance for bad things to happen.

Information: Any time you have data communication, bad things can happen. Any time data processing, bad things, any time data storage and retrieval. Those are the only places that in this whole process, where bad things can happen. So what you want to do, what one should do rather, is look at the entire process, where are the data communication activities, bing, bing, bing, bing. Where are the data storage activities, bing, bing, bing, bing. And then look in each of those areas, what tools you're using to mitigate those risks at that point in time.

Information: Primary management tools available to you. In effect you have policies, procedures and controls, you have technologies and security assessments, and you have audits. Now, as I said earlier I think, by and large the debate over authentication, identification whatever you want to call it, over the last 5, 8, 10 years whatever, has really focused on technology.

Information: And I would submit that by and large the technology is there. What has not been figured out is the policy part of this. Whose credentials will I accept and why will I accept it.

Standardization: No one has really stood up and said they're willing to do that. The technology is all there, to package it if anybody will do that. And it really is around this policy issue of who's willing to make decisions about the identity proofing process that they're willing to do or that there was a relying party demand. We're not there yet.

Information: Key issues in determining whether this all will work. It really starts with, what is the required degree of certainty in the identity proofing process. You have to learn to live with the fact you're not going to get it right all the time. And if you can't live with that, we will never essentially move off step one.

Information: But in the sensitive but unclassified world, in the credit card industry they have said look, we have, will learn to live with the level of fraud, as long as that level of fraud is below the cost of fixing it. So if the credit industry has as a total industry has a $100 million of fraud a year, while $100 million is real money. If the cost of eliminating $100 million fraud is a billion dollars, they're not going to do it; they will live with the $100 million. So in the identity proofing process there will be a cost to getting it wrong. But we number one have to begin to understand how we're going to quantify that cost, and once quantify that cost, can we live with it.

Information: So we need to really begin to start to understand what is an acceptable credential and why is it acceptable and not kid ourselves about it. Then, relying parties need to understand and this is the old liability issue, do the relying parties really believe that they need to have recourse to you if you get it wrong.

Information: Now, in the today's real world basically the only credentials that people are willing to rely on are the GIPIDs (government issued photo Ids) and it is convenient that all GIPID issuers happen to have sovereign immunity.

Information: And then the process cost and ease of use. Again, you can make this extraordinarily complicated, extraordinarily high tech, and extraordinarily hard to use, and it will just go away. The people won't need it, won't use it at all.

Information: If we over engineer this thing, no one will ever use it. And then finally, there's the security complexity and scale-ability of it. You know, long people standing in line for in person authentication is a hard way to do 200 million people. So, it's coming to grips with this is have to going to be data base checks over web based exchanges of data to all this or again, it will be difficult to get there.

SESSION: SECURITY AND PRIVACY ISSUES

Presentation: Trusted Optical Cards

Presented By: Jack Harper, BSI2000, Inc.

File Size: 872 KB PDF File

Transcript Excerpts:

Technology: What are optical cards? Well obviously it's a card that you carry around with you, it's the same size of course as a standard credit card, but the difference is it holds somewhere around 3 to 4 megabytes of data on the card - in an optical format. And that's about 1500 type written pages.

Technology: Why optical cards, well number one is memory. It's got somewhere in the order of a thousand times a memory of most smart cards so it has all the memory in the world to do all kinds of really interesting things. Number two, it's the permanent, SmartCards you know that had problems sometimes with static electricity - things like that.

Technology: Very highly reliable technology. Ten year life, I've got optical cards, I've been carrying around for five years, and they are all scratched up and all of that you know hear the term optical card and you think good heavens, you know does this thing work, because it sounds complicated.

Integration: Because there is all the memory in the world that means you can have multiple biometrics, if you want ten fingers, ten toes, whatever it is you want, all of the above you know there is enough memory to keep all this information out there. Again it's off-line if you wish, it can be completely off-line.

Technology: When you write data to the card, realize it's not a one time write for the card, it means that every spot on the card can be written exactly one time and then you come back and read it. So we're constantly adding update records to the card. So when you use an optical card in my mind, it should be so that there's permanent audit trail that's written so that every event, every transaction, whatever it is, you go through gate, anything.

Limitation: However, there's an interesting issue with optical cards. You know with smart cards it's pretty obvious where to keep the secret key. You keep it inside the chip, where the thing is protected and not accessible from the outside world without quite a bit of headache. But with an optical card you can literally take a microscope, put the thing under it, and look at it, and you can see all the data, there it is.

Security: So where do you keep the secret key on an optical card because everything is visible, and several methods have been used in the past. Number one is well you hide it somewhere in the software. Number two is you hide it somewhere in the microcode of the optical card reader writer device which is a thing about like this about so thick that's integrated into a box.

Security: I don't like any of these things; they're in fact bad. There's a new approach needed and BSI2000, we've been working on the problem for a long time and I mean our thing is optical card systems. Number one it has to be cryptographically secured.

Requirements: In my mind, a good credibility criterion is that it certifies that FIPS 140-1 levels 1, 2, and 3. Next it has to be usable with you know normal techniques to any type of publicly encrypted or whatever it is that you want to do.

Requirements: But also, obviously you have to prevent things like clone cards, where you take one optical card and simply copy data from that to another optical card. How do you prevent that? Last but not least it has to be affordable, unless the plane for Switzerland is flying over.

Technology: (*Hardware*) Crypto 2000, again, it's a hand held module, looks like that inside. It has several functions, number one, and I guess most important is simply a secured key repository, again it answers the question, where do you keep the key. Well the answer is, and our philosophy you don't keep the key, actually on the optical as you can see it with the microscope. Rather you keep the key inside our machine that we build that reads/writes the data.

Security: The idea is that if you open the crypto 2000 module, you've got to somehow get through all the many layers of very fine brittle wire. If you break that wire, then that causes the chip that's on the crypto 2000 module to instantly zap the secret key.

Integration: Secure optical cards. Well, what we build are systems that use optical cards. You can have any number of terminals on two actually, one and terminal number whatever. And any number of cards, millions of cards, all floating around these terminals and the thing is secure.

Technology/Security: But, you know, there's a little bit of difference between a secure optical card and a trusted optical card which really is the title of this talk. Crypto 2000, of course, provides data security which is not trust. Just because the data is securely written doesn't mean that it's really trusted. You don't really know who wrote it there and all those things.

Technology: So we've come up with a trust model. This is just a very brief outline of the trust model. But the idea is you have a hierarchical type organization, some sort of card issuance authority of one form or the other, commercial, government, whatever it is.

Technology: A very interesting project with change of government, suddenly there is ... years ago, suddenly there's money flowing out into the bush areas. And there's no infrastructure out there for the most part, telecommunications or anything. Therefore, how do you make an online system work ... smart code or whatever ... out in the middle of the wilds or the northern province of South Africa? And the answer is, well, you use optical cards which have enough memory to support it. And with this system and this protocol and all the rest, it's got the security for the thing to actually work.

SESSION: MULTI-TECHNOLOGY INTEGRATION REQUIREMENTS & ISSUES

Presentation: Managing Smart Card Field Returns

Presented By: Giles Lisimaque, Gemplus/Oberthur/Schlumberger

File Size: 2,858 KB PDF File

Transcript Excerpts:

Capability: *(Craig Diffie, Schlumberger during introduction***)** I should have been faster on my feet earlier when asked about the 64K dissemination in the marketplace, the 64K chip is just becoming commercially available in the ID space and has not widely been used. This is partly because of the production process, and secondarily because there hasn't been a wide call for it in the marketplace. But we fully expect that it will grow by leaps and bounds.

Issues: You may have a lot of issues when you are issuing cards, whatever cards. It could be financial cards, night stripe cards, or whatever cards, you are going to deal with. You are going to have problems. It could be passwords which are going to be forgotten. It could be cards which are going to fail. It could be terminals going nuts. We have seen that in lot of applications. It could be applications software. It could be the current personalization which has incomplete elements.

Multiple Applications: As you know, smart cards are integrated circuit plastic with a computer in it. And the problem with multiple elements on the same card, if that when one element fails, the whole card has to be replaced. So it's a very expensive process. And I am going to stress the fact that the more things you put on the same card, the more failures you will have. The whole presentation here is to say that monitoring is important, especially when you are doing something new.

Best Practices: It's not always the cards which fail. It can be the terminal which makes the card fail. And you have got to know what the terminal is doing. Even in the contactless world, some terminals can get out of the working specification range. And you've got to manage them and control when they need to be tweaked.

Multi-technology Issues: The cards combining multiple technologies as I mentioned have problems which can be created by one technology impacting on anther technology on the same card. We have seen cards used in physical access control where the max stripe was swiped and the reader was placed in the location where the card was generally bent a little. Because of the design of the magnetic stripe reader and the location of the reader that bending was stressing the chip which was breaking more often than it should. By just changing the location of the reader, it solved a cracking problem on the chip. By monitoring those failures, you can improve those little things which are part of real life.

Interoperability: Something also which is important that terminals, software, electrical wiring and ICs in the chips, do not come always from the same vendors. Smart Card manufacturers have multiple suppliers and we have multiple ways of doing things as well as developing operating systems. Incompatibilities may sometimes come from this diversity as the devil is in the details. Sometimes the problem comes from the card, its plastic body, the printing, the magnetic stripe, sometimes from the glue in the card, sometimes from the IC manufacturer and so forth.

Technology: Microprocessor cards are much more reliable than the non-microprocessor cards.

Lessons Learned: (Banking Application – Slide 9) About 30 percent of the cards which were returned and declared failing were in fact functional. It means that a lot of returns were declared bad cards for no good technical reason. And in fact, it was either the terminal or the user of the card which had the problem. That happens a lot.

And about 40 percent of the cards at the end were lost because of pin presentation. Keep that number in mind. You will see it over and over in all applications. PIN lock is a main failure problem.

Lessons Learned: (GSM – Slide 11 & Microprocessor card – Slide 12) So again, on all microprocessor cards, the main reason for card return is the PIN lock. Memory activity updating EEPROM was in the early days of GSM the second failure reason. This has been corrected since and do not show up anymore as Operating Systems are now taking care of this issue. And the third reason is mechanical features, chip broken most of the time. This last failure reason improved tremendously with customer education, asking then not to use the card to clean ice on windshields anymore.

Lessons Learned: (Payphone cards – Slide 15) We are talking here about pay phone cards. These are synchronous cards, not microprocessor cards. They are much more sensitive to their environment than microprocessor cards. And getting those chips to work into a reader is generally kind of a challenge.

Integration: I know a company in the U.S. which tried to use chips like these into a bus for fare collection. They had a nightmare problem just because of mechanical vibration creating bad electrical contacts between the chip and the reader. Such a noisy environment with a PLA protocol (synchronous contact cards) with bit protocol was just a disaster. So use microprocessor cards and you are going to be safe.

Lessons Learned: (CAC – Fort Bragg – Slide 17) The report says that there was a tremendous lack of training awareness of how to use and protect the ICC. Training has always been a very important factor in preserving cards. In all applications, the training of the user is a key element that you need to integrate in any kind of smart card deployment. The user needs to understand what the card is doing, how he needs to protect the card and why he needs to protect the card.

Lessons Learned/Standardization: (Contactless cards – Slide 18) Out of this very little number of cards *(356 out of four million contactless cards, returned and analyzed)* we have here something quite different because we are now in a contactless environment. The main failure issue, 18 percent, has to do with compliance with the specification. In this case, it means the antenna was not working correctly or the operating distance was less than the ten centimeters ISO requires. The cards were still working, but slightly out of specification. In other words, if the reader was also just at the limit of its specification, the card wouldn't work in that reader. That's something you need to monitor for contactless application. It can be a problem between cards and readers but this is improving quickly with experience now.

Best Practices: (Slide 19) Basically, we have a warranty which says that under 500 cards per million sold. Well, up to such a number, no question asked, we are going to exchange the failing cards. If it happens to go over that number, something doesn't work in the application. You've got a problem somewhere that needs to fix in a team effort, between the application developer, the system integrator, the terminal manufacturer, the card manufacturer, etc. That's really the key point to understand: five hundred card failure per million sold over three years is generally a number most applications do live with as it would generally cost more to try to get below such a number. The key is to monitor the application failures when it starts to make sure the failure rate is below this threshold.

Lessons Learned: (Why monitor – Slide 20) Education of the end user is key. For example, if you are using your contact smart card for identification, the card needs to stay in the reader during the

authentication process. But one of the failures of smart card applications in North America comes from people used to insert their credit card and remove it immediately (magnetic stripe reading process). Most users to see why it should be different between a chip card and a magnetic stripe card but habits are so difficult to change. It's just a matter of education. But that's a very hard one to overcome because of the habits we have.

Security: Monitoring also increases the security of the application. Because you have a way to get the bad cards out of the way. If you say the card doesn't work, I need to get it back, that's not only to monitor the failure, but it also gives a process for the bad cards to be collected and accounted for.

Multi-technology: One technology on the card can create a hazard for another one. Remember the magnetic stripe I was mentioning. The location of the chip is today at a given place regarding the magnetic stripe. If the reader of the magnetic stripe forces the user to bend or twist the card, this creates a hazard for the chip technology as the IC might brake. Another example has to do with cheap contact readers scratching the surface of the card, which might alter or destroy some printing secure protections on the plastic of the card. So you have got to be careful about multiple technologies.

Lessons Learned: (Conclusion – Slide 21) So in conclusion, I would say that all applications which have a PIN or a password to protect their card, must be prepared for high return rates or high management risks on how to unblock those PINs. If you do not have an un-blocking procedure as part of the application, you will get many cards with a blocked PIN which are going to be returned. That's the experience. Using Biometry might help solve this issue.

Lessons Learned: For contact cards, the more often the card is inserted into a terminal the faster it ages as this creates wearing of the golden plates contacts. The quality of the contacts or the reader is also going to be an important key element. If you use the contact card twice a day, you'd better invest in high quality contacts on the reader's side (e.g. landing contacts). Otherwise, you are going to destroy your cards rather quickly. And that's a catch 22. If you try to get cheap scratch readers, they are not going to last long and will also destroy your cards very quickly which will need to be replaced. So you won't save money at the end.

Interoperability: Mechanical and electrical interoperability between cards and readers has now tremendously improved with experience and most manufacturers have developed sophisticated tests to verify their compliance with the standards. Nevertheless any new technology will have such early tweaking requirements and adding a new technology on a card will require monitoring for a while.

SESSION: MULTI-TECHNOLOGY INTEGRATION REQUIREMENTS & ISSUES

Presentation: Migration Strategies

Presented By: Michael L. Davis, OmniTek

File Size: 227 KB PDF File

Transcript Excerpts:

Capabilities: In the access control marketplace, contactless with smart cards are the ideal medium for access control and as proof of that, we now use a technology called Prox which enjoys a very large penetration rate. But it's an older technology and it's very prevalent. But with the new contactless smart cards, we wish to talk about some migration strategies.

Lessons Learned: If you're starting from scratch, that's always a much better solution. That applies to almost any endeavor that one takes. But unfortunately, there's a lot of product out there now and we have to make it seamless for the end users and the community to move to a new technology.

Technology/Capabilities/Standards/Limitations: So Prox, as it's talked about in the United States, is actually 125 kilohertz. And it's basically, a nice technology, very reliable, very mature. But it suffers from some negatives. The biggest negative is that it's read only typically. You can write cards. But you can't do them on the fly. You can't actually present them and rewrite the data. And the security is pretty low. You can actually find the data sheets for the manufacturers, the chips used inside right on the Internet. And there's no ISO standard. And, of course, the biggest significant factor is it's not multi-application.

Comparison: So we're all experts in here about contactless smart cards. But as you can see, it shares many of the same features as Proxs, but it adds some new ones like larger memory, multi-application, very high security, true read/write and extremely high security again when compared to Proxs and it's ISO standardized.

Definition: A multi-technology card is basically a card that uses different machine-readable technologies. And that's the key, machine-readable. Human readable is okay. But for it to be an actual technology that a computer can use, it has to be machine-readable. And here are some of the ... of course, we all know about magnetic stripes. No one's mentioned debit stripes. There're a lot of debit stripe applications out there, especially at universities. That's that really thin small stripe that's read/writeable, used for vending. Bar code, optical stripe and actually barium is still very much used, believe it or not. Barium is a magnetic technology that's embedded in the card.

There are a lot of debit stripe applications out there, especially at universities. That's that really thin small stripe that's read/writeable, used for vending. Bar code, optical stripe and actually barium is still very much used, believe it or not. Barium is a magnetic technology that's embedded in the card.

Technology: So here are some reasons to migrate. So, 13.56 megahertz, which is synonymous with contact with smart cards, is much better security. The transaction speed is much, much faster. It's very much ISO standardized, has much greater memory, is multi-application, and conducts faster transactions. It actually looks like the duplicate.

And actually, believe it or not, the cards are less expensive to manufacturer. Because in 125 kilohertz, you have 200 turns of wire and you get a lot of magnetic fallout after working at a card manufacturer.

Because you have such a mass of copper in there that when you heat it up and actually begin to laminate it, when it cools down the differences in the thermal coefficient actually cause the card to look like a potato chip and there's huge internal stresses.

So because 13 megahertz now is pretty mature, the price is actually just about the same. So that's one barrier.

Security: The multi-application is in my opinion the most important. And that's actually part of the migration strategy, the fact that you can have multiple applications on the same card.

Interoperability and Further Growth: So in multi-application, the way I like to describe it, is if you took 16, 32, whatever the capacity chip is, separate cards and glued them all together in one card, in effect it is 16 different cards. Each card has its own security keys. And in a sense, it's almost like a firewall. One application can't get to the other application.

So conceptually, it's just 15 cards all glued together in one convenient form factor. And here I'm showing that in each of the different application slots, you can put different applications. Access control and logical access are the two most mainstream.

And interestingly enough, this actually solves an interesting problem. This is because the physical security director of an installation never trusts the IT guy because they're sort of like rivals. And the IT guy doesn't trust the other guy.

So in the older models, they actually used separate cards. But now because each one has its own keys and can maintain its own application, they can both play in the same sandbox together. Everyone can carry the same card. Yet, the IT guy can control access to the computers. And the physical access guy can control access to the building.

Multiple Applications: One particular thing that I think is real important when you get to multiple applications is access control is typically the application. That controls the card. What I mean by that is that's typically where the card gets issued from. And if you have a vendor that doesn't tell you or won't disclose to you the keys, the unused applications, that in effect becomes a proprietary card. And you can't use the card for other applications. So that's a real important thing when selecting access control. Of course, open key strategy, which I call that an open key strategy, the vendor should not disclose the access control key. But for the rest of the card he should. Then you can actually switch vendors if you're not happy. It eliminates obsolescence because there are a lot of manufacturers making product for those standards and that actually increases the market size.

Technology: In the 125 kilohertz, there is no standardization. It is all proprietary. In the 13-megahertz contactless smart cards, there are standards. And open standards encourage broad suppliers. And then the more people making products for that particular standard, the less costly it gets. You get competition. You get all the things that are good for the user community. Of course, for the vendors, it's very bad. I am a vendor.

Migration Strategy: These are not the only strategies, but these are pretty broad. There's basically three ways to do it. You can move the data from multiple applications onto a single card using a multiple technology card. You can use your existing card and add a technology sticker to it. Or you can use multi-technology readers. Those are the there basic ways of migrating. Again, we're concentrating on migrating just from Proxs to contact with smart cards. But, of course, it applies to the other technologies as well.

So, what I did want to point out in this slide is that you may use a combination of those three strategies to achieve your goal.

Multi-technology: So what you do is to use a multi-technology card. And that was a card that I showed you before that has a magnetic stripe on it, perhaps a bar code. Just like the CAC card, you have a whole bunch of different technologies. And each legacy application still resides in its original technology.

So the advantages are you get a nice aesthetic card assuming you manage where these technologies are. Sometimes it's not a choice, because it has to be compatible with existing readers. And it's the most secure card because everything's on one card.

But the disadvantage is it is definitely the most expensive card. And there's another major disadvantage, which we've heard now from two people, from Mary Dickson on the CAC card and right here from Gil on his presentation. The more technologies you add to a card, the more likely it is to fail. When a card fails, you've got a cost to replace it.

And if you actually put, for example, the 125 kilohertz Prox ... remember, that's that 200 turns of wire ... and a contact smart card, you actually weaken the structure of the card. So it's not an ideal solution for longevity. And actually, in one of our applications over probably about ... it's not a very big sample base over 150,000 cards. We found a 16 percent failure rate from birth to field in the first three years.

What happens is when you have all this multi-technology inside the card, the price that you pay - you've already paid - for the fact that when the manufacturer made the card, he's had a whole lot of cosmetic fallouts. And every time one of the technologies doesn't work, he has to scrap the whole card, throwing out all that technology. Then when you're in the field, you have an additional failure rate. So, you'll see how I handle this or what I suggest as a solution.

So several companies make a little sticker. And basically, it's a contactless smart card and a label form. And the label itself uses a very aggressive adhesive and sets up after time and becomes permanent. And it doesn't add much to the card thickness at all. And you get an interesting package.

Migration Strategy: And the next slide will talk about the reasons why. It's a good migration strategy because you take your existing card which may already be a multi-technology card. I mean, they already have a magnetic stripe and Proxs on it. And you just add a sticker to it. So the cost of the sticker is certainly much less than replacing the entire card with all the technologies in it. So, we have to price to do this.

The second reason is that, using your existing cards, you don't have to worry about migrating the data from your legacy applications because you're still using the same card effectively. But it does have some disadvantages and it's not as aesthetic. You've got a sticker on there. You have a slightly reduced range because the antenna is inside the sticker and the sticker is smaller than a card. So you get a reduced range. You have to be careful about where you put the sticker, because, if you put it over the magnetic stripe, obviously you're going to have an issue there. Also, you've got to watch out for thickness.

SESSION: INTEROPERABILITY REQUIREMENTS & ISSUES

Presentation: Interoperability and Card Printing

Presented By: Christophe Goyet, Oberthur/Gemplus/Schlumberger

File Size: 2,103 KB PDF File

Transcript Excerpts:

Introduction: Until a few years ago, smart card visual personalization meant embossing, a technique by which mechanical pressure is applied from the back of the card to produce raised letters and numbers on the front of the card, like account number and name on a credit card. This process works on any PVC cards but is very limited in the type and amount of information that can be thus personalized. We the emergence of new technologies such as die sublimation and thermal transfer techniques, we see the development of good quality desktop card printers from multiple manufacturers, we see a migration in the card personalization business from card embossing to card printing. Card printing unleashes your creativity and offers higher flexibility in the type and amount of information you can visually personalize: text with multiple fonts, Color photos, 2D and 3D bar codes, logos etc. However if embossing produces consistent results on all PVC cards regardless of the manufacturers, card printing is more sensible to card characteristics often linked to a type of card and to some extend to its manufacturer.

Interoperability: We tried to describe the most important factors to keep in mind when you design your layout to be printed on the cards to optimize the chances of interoperability in the printing station. Key factors are:

- When to print to card (Print during card manufacturing versus card issuance)
- Causes of print problems during issuance and how to minimize them.

Issue: Card printing done during card manufacturing stage offers the highest level of quality and interoperability. However only data that are identical on a batch of cards, such as company name, logo, and data template can benefit from being printed during manufacturing. Variable data, such as cardholder name, photograph, etc. will always have to be printed during issuance (central or local).

Potential Solution: Print problems are directly linked to the type and amount of data that you print. To minimize likelihood of print issues, limit what you print during issuance to the bare minimum and have all the remaining graphics and fixed data printed by the card manufacturer using pre-lamination printing process.

Issue: The main causes of print issues during card issuance are listed on slide 8. For instance the card may not be perfectly flat, although well within the ISO specifications. It may have been contaminated by the gloveless hands of an operator. You also have irregularities in the thickness caused by the chip or the antenna and printing directly above these areas could lead to unpredictable results. If you print too close to the module, you could end up with some problems as well. Another card region that could lead to print problems is where the card structure contains delamination zones as part of the card security features. Last but not least, printer compatibilities are also a major issue. Different printers may achieve different results even with the same card stock.

Potential Solution: What we found out from experience is that if you want to print in the above-mentioned risk areas, the printer setting has to be adjusted very precisely to match the characteristics of the cards that are being printed.

Issue: What we've also found out is there is nothing like a white card. I mean, what is a white card? If you take white cards from different manufacturers, or to some extend even from the same manufacturer, depending on the batch of material and the supplier of the PVC sheets, you may end up having cards that are whiter than others. This could affect color and contrast of your printed images/pictures.

Interoperability: ISO did not address post-embedding printing. So it's not because the card is ISO that it can print well during issuance. You could have cards from two different manufacturers, each cards have been ISO certified and has gone through all the 10373 tests to make sure that it complies with the four ISO specs, but you may nevertheless end up with different print quality after embedding.

Interoperability: If you look at the ISO standard, defined in 7810, the card does not have to be perfectly flat. It can be slightly warped up to 0.06 inches or 1.5 millimeters. That means that the highest point when you put it onto a flat surface must not exceed 1.5 millimeters. The experience we've seen from the field is that there are some printers that are not as flexible as what the ISO standard specifies. And some printers would not work well for cards with a warpage value over 0.5 millimeters, despite the fact that the cards are still within ISO specifications. However, you will hardly find any specification of card flatness or warpage in the data sheet of the printer as you get it from the manufacturer.

Interoperability: The other point where ISO does not specify interoperability for post-embedding printing is on the surface profile of the contact. If you look at the ISO 7816, Part two ... I even put the exact reference if you want to look at it ... it defines that the contact plate can be between plus 50 microns and minus 100 microns below the cards surface. So that means you have some flexibility and the contact plate can be slightly above the adjacent surface of the card or slightly below. When it is below, it's not a problem for printing. But when it is above the contact plate, then you have a kind of "tent effect" that creates a no printing zone. The size of that "tent effect" zone depends on the size and geometry of your print head.

Interoperability: ISO does not define the dimension, the shape, the geometries, and the color of the module. This is purely manufacturer dependent. ISO only define a minimum zone for each electrical contact. So contact plates may have different sizes and shapes depending on manufacturer. Slide 14 gives an idea of the variety of contact plates in the field today. An artwork that is being printed a quarter of an inch from the contact plate of manufacturer A could end up being to close to the contact plate of manufacturer B and fall into the tent effect zone previously described.

Interoperability: So that's about the contact part. Now, if you want to use a card with multiple technologies like contact and contactless, the problem becomes even worse I would say. To understand the potential issues, let's look at the components of a contactless card. You have three different types of contactless cards, (slide 15). The first one is a pure contactless. In that case, there is no contact plate. It's only a single chip, contactless interface. Then you could have a hybrid contactless card. The hybrid has two chips, but no direct electrical communication in between. Or you could have dual interface card where a single chip handles both contact and contactless interface. In all three cases, you always have an antenna. Only the contact chip or module has been standardize by ISO, as its location has to be very precisely determine to allow electrical contact with a reader. Contactless by definition does not require direct electrical connection and the contactless chip can be anywhere under the card surface. The same goes for the antenna. The location of the contactless chip is not standardized. The antenna's size, its geometry, whether it's square, round or oval is not at all standardized. It's up to the manufacturer. Because of their inherent thickness, the contactless chip and/or the antenna may in some cases, create some variations of the card surface properties above them that could potentially impact printability at issuance. This depends largely on the size of the contactless chip and the technology used for the antenna.

Potential Solution: There are ways to guarantee interoperability. But you need to be aware of some constraint. And basically, you need to involve card manufacturers in the early stage of your artwork design. It's always much easier to slightly modify the layout of your design before the cards are made than to try to find a way to fix a print issue problem on cards already manufactured, when you find out that the cards are not compatible with your printer.

Potential Solution: Don't try to fill all the blanks on the card surface with printing during issuance. There's one of the comments from a speaker yesterday who said, well, since we had some space left on the card, we decided to put some more information on it. I think that's a kind of risky approach. Adding a not really needed graphical information during card issuance could increase the print reject rate and, depending on the cost of the card, the cost of adding that new information could far outweigh the overall benefit of putting it. Every new item printed during post issuance is a potential point of failure and could result in the full card being rejected.

Potential Solution: To increase your chance of achieving a good quality print during card issuance when cards come from multiple sources, we would recommend the following guidelines:

1. Involve the card manufacturers in the design of your artwork and layout of your data
2. Provide the card manufacturer with as much graphics, logo and text to be printed prior to card lamination during card manufacturing process, so you don't incur the cost of print rejects.
3. For card holder related data, that are unique to each card and have to be printed during card issuance, refrain from using the following areas:

    - Directly behind the contact chip
    - Around the printed circuit of the contact chip (contact plate).
    - Close to the edge of the card (although some new printers claim edge to edge printing capability)
    - Above the contactless chip or do some testing before.
    - Above the antenna of contactless cards or do some testing before.

But basically, if you can limit what you print during this stage to variable data and only what is necessary for your application. There's no point to print during card issuance a logo that's going to be the same on all the cards. Also do some tests with printers and cards from multiple manufacturers. If you know that you're going to need cards from multiple manufacturers, get some samples from each of the manufacturers during the stage of your artwork design to make sure that your layout is compatible with both cards, especially in case of contactless cards where chip location can vary between manufacturers. And last but not least, don't forget to clean your print heads. It's something that is often missed during the print process during card issuance.

Potential Solution: Also some tests with printers and cards from multiple manufacturers. If you know that you're going to need to have cards from multiple manufacturers, get some samples from each of the manufacturers during the stage of your artwork design to make sure that their contactless chip is not at two locations that's going to cause a problem for you. And last but not least, don't forget to clean your print heads. It's something that is often missed during the print process.

SESSION: INTEROPERABILITY REQUIREMENTS & ISSUES

Presentation: Security and Interoperability in Contactless Smart Card Systems

Presented By: Ray Freeman, Assa Abloy ITG

File Size: 104 KB PDF File

Transcript Excerpts:

Interoperability: What sometimes we struggle with is exactly what interoperability means. Clearly, interoperability means ... or common expectation of it ... is that these systems made by different manufacturers, both cards and readers, should work together interchangeably, seamlessly. I should be able to take a card from supplier A. And it should work with readers from Supplier B, C and D. And when I say reader, I mean reader/writer mostly. A reader from supplier A should also work with cards from supplier B, C and D.

For us in the access control industry and the contactless card industry at large, there is some room to play here I guess. Interoperability can be achieved by licensing the IC technology. That is integrating the IC customer needs in the card form factor.

Interoperability: Chip level – If the reliance on a single IC technology or chip operating system is acceptable, then interoperable systems are available. And that would typically be available through a licensing scheme. My impression though is that that's not acceptable. However, if a large entity were to select a single system from a single technology, then these systems are available.

Interoperability: Reader level – Also available are interoperable contactless card systems that will work with different IC suppliers that are built around multiple chip technologies by incorporating these different technologies into a single reader. A good example of that is the reader currently available through Cubic Transportation Systems. They've incorporated the Go Card technology and Mifare. I believe they also have the capability to read 14443 Type A and Type B. Plus, I'm not sure, but I think 15693 may be on the way or is currently available, the ISO standard 15693. These are not common reader platforms probably because of the cost. You have to put many things inside it to make it work including the firmware to make everything work together.

Interoperability: Card Operating System level – Interoperability of card ICs from different manufacturers that have a microprocessor can also be achieved through the use of a common operating system. Even to the point where it's certainly technically feasible to port the operating systems from the contact card world to a contactless card IC. The protocol obviously, the transmission protocol, has to be different. Currently, these microprocessor based ICs are available that conform to all four parts of ISO14443 or they're becoming available.

Interoperability: There are current limitations here for contactless memory card systems. First of all, conformance to all parts of ISO14 443 does not ensure interoperability. The fact is that ISO 14443 has no provisions for implementing security. So at least in the contactless memory card world all of the security systems currently are proprietary. Also, there's no provision within ISO 14443 for having a standard command set for access to the memory of the IC. These commands in all existing systems would be proprietary today. Point to drive home is that security as it's implemented is the major reason that contactless cards and readers that conformed to ISO 14443 are not necessarily interoperable. For me, this is a big limitation. I'm not a big believer in security by obscurity, having secret algorithms. Currently, all

of the fixed logic memory cards that are available on the market depend on encryption algorithms that are neither published nor disclosed.

Interoperability: Moving forward, I think these systems to become interoperable will have to depend on cards with microprocessor ICs. And cards and readers will be based on all four parts of ISO 14443.

Interoperability: Secure and interoperable contact with systems in the future will probably be based on strong published encryption algorithms that are embedded in the operating system of the microprocessor card. Again, you can rely on the algorithms that are currently available in the contact card world. My proposal will be mostly to port these already mature operating systems to these platforms, to these ICs, giving choice, giving familiarity. Also the portability of many of the applications would be assured as well through the use of middle ware. Secure interoperable contactless card systems of the future will be based on simple secure tamper-proof readers. In the access control world, this is very important. Readers need to be stand alone if they're broken into, they need to have tamper proof features. Key management procedures and components built on best practices.

Interoperability: In conclusion, I would say that these lower cost memory contactless card ICs are cards based on and could gain traction if an open securities standard were to emerge for this class of card. That could come from any number of sources.

SESSION: INTEROPERABILITY REQUIREMENTS & ISSUES

Presentation: APTA Universal Transit Farecard Standards Program

Presented By: Thomas Parker, APTA Farecard Standards Task Force

File Size: 2,544 KB PDF File

Transcript Excerpts:

Requirement: One of the things that was very important to committee was regional interoperability. That's really the buzzword for transit. It's taking one card and having it work seamlessly throughout a region, being able to ride bus, rail, boat, train, commuter rail, whatever you want, with the same vehicle.

Interoperability: We're trying to develop standards for all of our transportation to use one card or a combination of cards that work in an interoperable way. The first thing we needed was the standards. Because there were so many different card platforms out there. As you heard earlier, 14443, parts one, two, three and four, just not that alone would give you interoperability between cards or readers. When we looked at this problem between the card and the reader, we kind of broke it up into two parts. We kind of broke it up into what we call the front end as the card to reader and what standards were there. We did adopt the ISO standards 14443; which says that basically we're going to use two types of cards in our system. We're going to use a type A card and a type B card. I won't get into the differences, but there are other cards out there, C, D, E and so forth. But we've chosen to use two card types, A and a B. Now, those cards have to be interoperable. And the thing that stops them from being interoperable on the card and the reader after you get past parts one, two, three and four is what they call the application protocol interface. And then basically, understanding what the data elements are and understanding what the format file structure is basically like if I'm going to talk to you, I've got to use the same words. We've got to agree to the words. We've got to agree to how to put these words in a sentence. And then when I put these words in a sentence, you're going to understand my communication. The same is true with cards. So everyone's going to use the same data file structure and data elements. 14443 does not address that. 7816, on the other hand, did give us an application. But in transit, we needed something to be very quick. 7816 was more for a contact environment. Our environment needs to be contactless.

Standardization: In the Bay Area, one of the things that we've done is that we've developed a standard for printing on the card and we share that with our vendors.

SESSION: TECHNOLOGY ROADMAP AND GAP ANALYSIS

Presentation: Smart Card Technology Roadmap for Secure ID Applications

Presented By: Randy Vanderhoof, Smart Card Alliance

File Size: 558 KB PDF File

Transcript Excerpts:

Interoperability: Security is not something that we can blankly say that every application for identity requires something beyond simply a visible identity or authentication. But when it does because the thing that you're protecting is more important, we need to go to the next level and the next step. So there are levels of security (something you know, something you have, and something you are) and its (level of security needed) appropriateness depends on the application needs and the department policies and regulations.

Interoperability: How strong do we need to bind the identity of the card holder with the information that is being presented on the card is a subjective matter. Once a card is created and it's issued, if I'm going to trust that card in the future, then I'm assuming that because the person in front of me is presenting that card or the person in front of me knows an access code that goes along with that card. But that means that everything else about that card is current and accurate and associated with the individual presenting that card. Maybe that's good enough. If it's not, then I need to go to another level to bind that card to the individual, which could be a biometrics step in the process.

Requirement: I think that the slide (in transaction time) that I saw was if you add nine seconds to each transaction at the San Isidro entry point, it resulted in eleven hours of additional delay in getting through the line. So those are types of decisions that have to be made in terms of making sure that the solutions we propose also are addressing the needs in terms of speed as well as convenience.

Interoperability: The overall challenge is managing scalable ID solutions that need multiple technologies with security and privacy, both from the point of when the card is issued to all the way out to everywhere and place that the card may be needed. You know if the IT community and the physical access community can solve that problem, then now they've got a truly working secure identification credential. But to get to that point, requires you to go back through this entire process that we've heard about over the last two days.

Interoperability: The point I want to make here is the building blocks are in place to support interoperable systems. But it's rarely a technology decision that limits interoperability as much as it is a business and policy decision on if we interoperate with other systems, are we weakening the security that we're providing? Are we allowing for others to penetrate the system and therefore create risk that it will weaken the overall solution that we're providing? And how are we going to manage interoperability when we have multiple entities now sharing and making the decisions on how the card is used and issued. So there's technology decisions and obstacles certainly that have to be overcome. But it takes the will of the implementation to overcome them. And in many cases without the will to overcome those limitations or obstacles for interoperability, we remain with very good, very secure, very reliable solutions that do not interoperate for good business decisions.

Industry Needs: Our industry today is still fairly young, particularly in the area of microprocessor-based functions for security applications, that in the overall evolution of the technologies, it's not unusual that

we have separate inoperable systems on the marketplace today. But there is a demand for it from the issuer's side that we move towards more interoperability. So that we lower costs and we increase the number of suppliers and we have more choices to be offered in the industry.

Appendix E—Standards Bibliography

STANDARDS MATRIX Version 1.0 Standard or Recommendation - S = Standard; R = Recommendation Technology Types - Anti-counterfeiting, Biometric, Barcode, Magnetic Media, Smart Cards, Optical Card			
			TECHNOLOGY
Standard	FIPS 140-2	Security Requirements for Cryptographic Modules	Anti-counterfeiting
Standard	FIPS 186-2	Digital Signature Standard (DSS)	Anti-counterfeiting
Standard	ISO 1073-1	Alphanumeric Character Sets for Optical Recognition Part I: Character Set OCR-A Shapes and Dimensions of the Printed Characters	Anti-counterfeiting
Standard	ISO 1073-2	Alphanumeric Character Sets for Optical Recognition Part II: Character Set OCR-B Shapes and Dimensions of the Printed Characters	Anti-counterfeiting
Standard	ISO 1831	Printing specifications for optical character recognition	Anti-counterfeiting
Standard	PKCS#1	RSA Encryption Standard (Version 1.5)	Anti-counterfeiting
Standard	PKCS#11	Cryptographic Token Interface Standard (Version 1.0)	Anti-counterfeiting
Standard	ANSI/AIM-BC1	1995 Uniform Symbol Specification - Code 39	Barcode
Standard	ANSI/AIM-BC2	1995 Uniform Symbol Specification - Interleaved 2 of 5	Barcode
Standard	ANSI/AIM-BC3	1995 Uniform Symbol Specification - Codabar	Barcode
Standard	ANSI/AIM-BC4	1995 Uniform Symbol Specification - Code 128	Barcode
Standard	ANSI/AIM-BC5	1995 Uniform Symbol Specification - Code 93	Barcode
Standard	ANSI/AIM-BC6	1995 Uniform Symbol Specification - Code 49	Barcode
Standard	ANSI/AIM-BC7	1995 Uniform Symbol Specification - Code 16K	Barcode
Standard	EAN International	European Article Numbering (analogous to the UPC codes used in the US)	Barcode
Standard	ISO TC 204	Transport Information & Control Systems (RF ID)	Barcode
Standard	ISO TC 122	Packaging (proposed Shipping Label home)	Barcode
Standard	ISSN	International Standard Serial Number	Barcode
Recommendation	Uniform Symbol Specification	PDF417 (1994)	Barcode
Recommendation	Uniform Symbol Specification	Code One (1994)	Barcode
Recommendation	Uniform Symbol Specification	Data Matrix (1995)	Barcode

STANDARDS MATRIX Version 1.0 Standard or Recommendation - S = Standard; R = Recommendation Technology Types - Anti-counterfeiting, Biometric, Barcode, Magnetic Media, Smart Cards, Optical Card			
			TECHNOLOGY
Recommendation	Uniform Symbol Specification	MaxiCode 16K (1995)	Barcode
Standard	UPC-A	Uniform Code Council: Universal Product Code - A. UPC-A is used for marking products which are sold at retail in the US.	Barcode
Standard	UPC-E	Uniform Code Council: Universal Product Code - E. The UPC-E code is a compressed barcode which is intended for use on small items. Compression works by squeezing extra zeroes out of the barcode and then automatically re-inserting them at the scanner. Only barcodes containing zeroes are candidates for the UPC-E symbol.	Barcode
Standard	ISO/IEC 7811-1	2002 Identification Cards – Recording Technique – Part 1: Embossing	Magnetic Storage
Standard	ISO/IEC 7811-2	2001 Identification Cards – Recording Technique – Part 2: Magnetic Stripe – Low Coercivity	Magnetic Storage
Standard	ISO/IEC 7811-3	1995 Identification Cards – Recording Technique – Part 3: Location of Embossed Characters on ID-1 Cards	Magnetic Storage
Standard	ISO/IEC 7811-4	1995 Identification Cards – Recording Technique – Part 4: Location of Read-only Magnetic Track – Track 1 and 2	Magnetic Storage
Standard	ISO/IEC 7811-5	1995 Identification Cards – Recording Technique – Part 5: Location of Read-only Magnetic Track – Track 3	Magnetic Storage
Standard	ISO/IEC 7811-6	2001 Identification Cards – Recording Technique – Part 6: Magnetic Stripe – High Coercivity	Magnetic Storage
Standard	ISO/IEC 8484	1987 Magnetic Stripes on Savingbooks	Magnetic Storage
Standard	ISO/IEC 10373-2	Identification Cards – Test Methods – Part 2: Cards With Magnetic Stripes	Magnetic Storage
Standard	ISO/IEC 10373-5	Identification Cards – Test Methods – Part 5: Optical Memory Cards	Optical Data Storage
Standard	ISO/IEC 11693	1993 ID Cards - Optical Memory Cards	Optical Data Storage
Standard	ISO/IEC 11694-1	1994 ID Cards - Optical Memory Cards Linear recording method Part 1: Physical Characteristics	Optical Data Storage
Standard	ISO/IEC 11694-2	1994 ID Cards - Optical Memory Cards Linear recording method Part 2: Dimensions and location of the accessible op	Optical Data Storage
Standard	ISO/IEC 11694-3	ID Cards - Optical Memory Cards Linear recording method Part 3: Optical properties and characteristics	Optical Data Storage
Standard	ISO/IEC 11694-4	ID Cards - Optical Memory Cards Linear recording method Part 4: Logical data structures	Optical Data Storage

STANDARDS MATRIX Version 1.0 Standard or Recommendation - S = Standard; R = Recommendation Technology Types - Anti-counterfeiting, Biometric, Barcode, Magnetic Media, Smart Cards, Optical Card			
			TECHNOLOGY
Recommendation	CEPS	The Common Electronic Purse Specifications (CEPS) define requirements for all components needed by an organization to implement a globally interoperable electronic purse program, while maintaining full accountability and auditability. CEPS, which were made available in March of 1999, outline overall system security, certification and migration.	Smart Cards
Standard	G8 - format	Raw graphics (one byte per pixel) plane three (PicLab)	Smart Cards
Recommendation	GSC-IS	Government Smart Card Interoperability Specification	Smart Cards
Standard	ICAO 9303	ICAO – International Civil Aviation Organization - Standard for Machine Readable Travel Documents (MRTD)	Smart Cards
Recommendation	ICMA	International Card Manufacturers Association	Smart Cards
Standard	ISO 1177	1995, Information processing - Character structure for start/stop and synchronous character oriented transmission.	Smart Cards
Standard	ISO/IEC 7501-1	1997 Identification Cards - Machine Readable Travel Documents – Part 1: Machine Readable Passport	Smart Cards
Standard	ISO/IEC 7501-2	1997 Identification Cards - Machine Readable Travel Documents – Part 2: Machine Readable Visa	Smart Cards
Standard	ISO/IEC 7501-3	1997 Identification Cards - Machine Readable Travel Documents – Part 3: Machine Readable Official Travel Documents	Smart Cards
Standard	ISO/IEC 7810	1995 Identification Cards – Physical Characteristics	Smart Cards
Standard	ISO/IEC 7812-1	2000 Identification Cards – Identification of Issuers – Part 1: Numbering System	Smart Cards
Standard	ISO/IEC 7812-2	2000 Identification Cards – Identification of Issuers – Part 2: Application and Registration Procedures	Smart Cards
Standard	ISO/IEC 7813	2001 Identification Cards – Financial Transaction Cards	Smart Cards
Standard	ISO/IEC 7816-1	1998 Identification Cards – Integrated Circuits With Contacts - Part 1: Physical Characteristics	Smart Cards
Standard	ISO/IEC 7816-2	1999 Identification Cards – Integrated Circuits With Contacts – Part 2: Dimensions and Locations of the Contacts	Smart Cards
Standard	ISO/IEC 7816-3	1997 Identification Cards – Integrated Circuits With Contacts – Part 3: Electronic Signals and Transmission Protocols	Smart Cards
Standard	ISO/IEC 7816-3	1997/Amendment 1:2002 Electrical Characteristics and Class Indication For Integrated Circuit(s) Cards Operating At 5 V, 3 V, and 1.8 V	Smart Cards

STANDARDS MATRIX Version 1.0 Standard or Recommendation - S = Standard; R = Recommendation Technology Types - Anti-counterfeiting, Biometric, Barcode, Magnetic Media, Smart Cards, Optical Card			
			TECHNOLOGY
Standard	ISO/IEC 7816-4	1995 Identification Cards – Integrated Circuits With Contacts – Part 4: Interindustry Commands for Interchange	Smart Cards
Standard	ISO/IEC 7816-5	1994 Identification Cards – Integrated Circuits With Contacts – Part 5: Numbering System and Registration Procedure For Application Identifiers	Smart Cards
Standard	ISO/IEC 7816-5	1994/Amendment 1:1996	Smart Cards
Standard	ISO/IEC 7816-6	1996 Identification Cards – Integrated Circuits With Contacts – Part 6: Interindustry Data Elements	Smart Cards
Standard	ISO/IEC 7816-6	1996/Correction 1:1998	Smart Cards
Standard	ISO/IEC 7816-6	1996/ Amendment 1:2000 IC Manufacturer Registration	Smart Cards
Standard	ISO/IEC 7816-7	1999 Identification Cards – Integrated Circuits With Contacts – Part 7: Interindustry Commands For Structured Card Query Language (SCQL)	Smart Cards
Standard	ISO/IEC 7816-8	1999 Identification Cards – Integrated Circuits With Contacts – Part 8: Security Related Interindustry Commands	Smart Cards
Standard	ISO/IEC 7816-9	2000 Identification Cards – Integrated Circuits With Contacts – Part 9: Additional Interindustry Commands and Security Attributes	Smart Cards
Standard	ISO/IEC 7816-10	1999 Identification Cards – Integrated Circuits With Contacts – Part 10: Electronic Signals and Answer to Reset For Synchronous Cards	Smart Cards
Standard	ISO/IEC 7816-10	1999 Identification Cards – Integrated Circuits With Contacts – Part 11: Personal Verification Through Biometric Methods	Smart Cards
Standard	ISO/IEC 10202	Architecture of the systems that utilize financial transaction cards.	Smart Cards
Standard	ISO/IEC 10373-1	1998 Identification Cards – Test Methods - Part 1: General Characteristics Tests	Smart Cards
Standard	ISO/IEC 10373-1	1998/Correction 1:2002	Smart Cards
Standard	ISO/IEC 10373-3	2001 Identification Cards – Test Methods – Part 3: Integrated Circuit(s) Cards With Contacts and Related Interface Devices	Smart Cards
Standard	ISO/IEC 10373-6	2001 Identification Cards – Test Methods – Part 6: Proximity Cards	Smart Cards
Standard	ISO/IEC 10373-7	2001 Identification Cards – Test Methods – Part 7: Vicinity Cards	Smart Cards
Standard	ISO/IEC 10536-1	2000 Identification Cards – Contactless Integrated Circuit(s) Cards – Close-Coupled-cards – Part 1: Physical Characteristics	Smart Cards
Standard	ISO/IEC 10536-2	1995 Identification Cards – Contactless Integrated Circuit(s) Cards – Close-Coupled-cards – Part 2: Dimensions and Locations of Coupling Areas	Smart Cards
Standard	ISO/IEC 10536-3	Identification Cards – Contactless Integrated Circuit(s) Cards – Close-Coupled-cards – Part 3: Electronic Signals and Reset Procedures	Smart Cards

STANDARDS MATRIX Version 1.0 Standard or Recommendation - S = Standard; R = Recommendation Technology Types - Anti-counterfeiting, Biometric, Barcode, Magnetic Media, Smart Cards, Optical Card			
			TECHNOLOGY
Standard	ISO/IEC 14443-1	2000 Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 1: Physical Characteristics	Smart Cards
Standard	ISO/IEC 14443-2	2001 Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 2: Radio Frequency Power and Signal Interface	Smart Cards
Standard	ISO/IEC 14443-3	2001 Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 3: Initialization and Anticollision	Smart Cards
Standard	ISO/IEC 14443-4	2001 Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 4: Transmission Protocol	Smart Cards
Standard	ISO/IEC 15457-1	2001 Identification Cards – Thin Flexible Cards – Part 1: Physical Characteristics	Smart Cards
Standard	ISO/IEC 15457-2	2001 Identification Cards – Thin Flexible Cards – Part 2: Magnetic Recording Techniques	Smart Cards
Standard	ISO/IEC 15457-3	2001 Identification Cards – Thin Flexible Cards – Part 3: Test Methods	Smart Cards
Standard	ISO/IEC 15693-1	2000 Identification Cards – Contactless Integrated Circuit(s) Cards – Vicinity Cards – Part 1: Physical Characteristics	Smart Cards
Standard	ISO/IEC 15693-2	2000 Identification Cards – Contactless Integrated Circuit(s) Cards – Vicinity Cards – Part 2: Air Interface and Initialization	Smart Cards
Standard	ISO/IEC 15693-2	2000/Correction 1:2001	Smart Cards
Standard	ISO/IEC 15693-3	2001 Identification Cards – Contactless Integrated Circuit(s) Cards – Vicinity Cards – Part 3: Anticollision and Transmission Protocol	Smart Cards
Standard	ISO/IEC 20060	2001 Information technology – Open Terminal Architecture (OTA) Specification – Virtual Machine Specification	Smart Cards
Recommendation	PC/SC	Personal Computer Smart Card (PC/SC) Specification	Smart Cards
Recommendation	Visa Cash	Visa's specification for "electronic purse". A microchip embedded in each plastic card stores monetary value. Each time you use Visa Cash to pay for something, your purchase amount is automatically deducted from the balance. Available in disposable and reloadable formats.	Smart Cards
Recommendation	Visa Cash CEPS	Electronic purse business requirements and specifications of a CEPS compliant version of Visa Cash.	Smart Cards
Standard	ISO/IEC 7816-4	1995/Amendment 1:1997 Secure Messaging on the Structures of APDU Messages	