NIST Interagency Report 7611

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

Use of ISO/IEC 24727

ISO/IEC 24727 Identification cards – Integrated circuit cards programming interfaces

Service Access Layer Interface for Identity (SALII): support for development and use of interoperable identity credentials

Hung Dang
Hildegard Ferraiolo
William MacGregor
Ketan Mehta
Teresa Schwarzhoff

Use of ISO/IEC 24727

NIST Interagency Report 7611

Hung Dang
Hildegard Ferraiolo
William MacGregor
Ketan Mehta
Teresa Schwarzhoff

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2009

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Dr. Patrick D. Gallagher, Deputy Director

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 analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report 7611, 25 pages

(August 2009)

Acknowledgements

The authors, Hildegard Ferraiolo, William MacGregor and Teresa Schwarzhoff of the National Institute of Standards and Technology, Ketan Mehta and Hung Dang of Booz Allen Hamilton wish to thank their colleagues who reviewed drafts of this document and contributed to its development.

Table of Contents

List of Appendices

List of Figures

1. Introduction

Major Federal Identity Management Systems (IDMS) have chosen to use Integrated Circuit Card (ICC) technology, also referred to as smart cards, for their identity credentials. Smart cards are portable and their inherent security capabilities make them well suited for identity credentials. The information and security requirements of an application on a smart card (referred to as card-application[1]) are determined by an issuing agency in support of their IT enterprise infrastructure. Information, requirements, and card-applications can vary from agency to agency, with numerous methods available to use and store information on smart cards. The legitimate variability results from differing requirements and can result in duplication of similar services and interoperability limitations. For instance, a Personal Identity Verification (PIV) Card and Transportation Worker Identity Credential (TWIC) Card may not be easily and interoperably authenticated by the same application (referred to as client-application[2]). These two cards support similar but not identical requirements and use different authentication mechanisms and security protocols.

Normalized access to information can reduce the potential for duplication of common IDMS services. Without methods that provide standardized access and interfaces, portability and interoperability of identity credentials across different client-applications is a programmatic and technical challenge.

The ability to interoperate is important to Federal government-wide initiatives. The US has led the development of an international standard for a framework that provides interoperable and secure services for identification, authentication, and digital signatures for identity credentials. The multi-part international standard, *International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 24727 Identification cards – Integrated circuit cards programming interfaces* (hereafter referred to as ISO/IEC 24727), consists of six parts, ISO/IEC 24727-1 through ISO/IEC 24727-6 [1-6]. The ISO/IEC 24727 framework allows any client-application to communicate with any card-application. This multi-part standard enables client-applications to authenticate cardholders and use card services from many different identity cards and across many client-applications.

1.1 Purpose and Scope

The purpose of this document is to describe the use of ISO/IEC 24727 in enabling client-applications to access identity credentials from different issuers. This document explores this new standard by discussing existing Federal identity credentials, such as PIV, and the PIV application demonstrations developed by the National Institute of Standards and Technology (NIST).

The scope of this document is to establish a proof-of-concept for ISO/IEC 24727 through the use and evaluation of existing PIV applications. The reader should note that this document provides a high-level discussion and strives to minimize technical details. An additional publication elaborating the technical discussion, including an ISO/IEC 24727 reference implementation, is currently under development.

The proof-of-concept applications discussed in this document are Windows Logon, Linux Logon, Email Signing and Encryption, and Web Authentication. The applications are those developed by NIST to demonstrate the use of PIV Cards in support of Homeland Security Presidential Directive 12 (HSPD-12).

---

[1] For this document, a card-application is a program running on the integrated circuit cards (ICC) that manages data storage/retrieval and its operations.

[2] For this document, a client-application is a program running in a host system which drives the execution logic.

They are available at the http://csrc.nist.gov/groups/SNS/piv/download.html. Using ISO/IEC 24727 with these applications, the proof-of-concept will demonstrate the ability to enable client-applications to accept and use cards from diverse identity credentialing systems.

This document is intended for the Federal agencies and agency officials responsible for IDMS programs. It provides program managers and system integrators with a high-level discussion of the multi-part standard ISO/IEC 24727 – Identification cards – Integrated circuit cards programming interfaces. Such information is also useful to government contractors, state and local governments, and security industry vendors implementing related systems, products, and services.

1.2 Document Organization

The sections of this document provide a high level discussion on ISO/IEC 24727, its' application environment, and use with identity cards. The structure is as follows:

- Section 1, *Introduction*, provides background information for understanding the scope of this document.
- Section 2, *ISO/IEC 24727 Discussion*, provides an overview of ISO/IEC 24727 and discusses its capabilities and uses.
- Section 3, *ISO/IEC 24727 Proof-of-Concept*, describes the proof-of-concept architecture and design considerations.
- Appendix A, *Acronyms*, provides list of acronyms used in the document.
- Appendix B, *References*, lists the specifications and standards referred to in this document.

2. ISO/IEC 24727 Discussion

ISO/IEC 24727 is the first international standard to remove identity card dependence from client-application programming. This is achieved by abstracting identity services to a set of normalized interfaces.

ISO/IEC 24727 defines an architecture consisting of standard interfaces for interoperable services[3] between a card-application and a client-application. Through such generic interfaces, client-application development can be pursued independent of card-application development. Conversely, a card-application may be designed (data elements, authentication protocols, security protocol services, etc) independent of a specific client-application. This is achieved with the following four ISO/IEC 24727 design features:

+ **High-level application programming interface (API)** — The high-level API defined in ISO/IEC 24727, referred to here as Service Access Layer Interface for Identity (SALII), enables client-applications to learn about the information and procedural facilities to be found on a card in terms of named data and computational services. Through this normative set of API functions, the client-application can perform identity related activities. This includes aligning information and procedures with the identities of individuals, storing and using such information, and using such procedures for the authentication of identities. The client-application is not required to know details of the card; this is accomplished through the cross-system interoperation. Any logical or physical access control applications can use this interface.

+ **Cross-system operation ("interoperation")** — While the SALII abstracts services for the client application, the Generic Card Interface (GCI) of ISO/IEC 24727 abstracts lower level details of card data and services. Through these distinct abstractions, client-applications can use identification services in real time, while the Generic Card Interface accommodates differences in card behavior. This feature of ISO/IEC 24727 enables developers to discover card capabilities and to write a client-application once and use it with different credential systems.

+ **Platform Independence** — This feature of ISO/IEC 24727 enables independence from interface devices, such as card readers, allowing compliant implementations to be used in different configurations and environments. The common device interface defined in ISO/IEC 24727 provides a generic interface for readers. This facilitates translation from a common device interface to device specific commands.

+ **Extensible architecture** — ISO/IEC 24727 includes a normative collection of basic services for authentication, signature, encryption, key establishment, and session establishment. It allows for the addition of new security protocols and authentication mechanisms to perform a variety of interoperable services. Because these services are normative, cards enabled with one or several service(s) will interoperate with ISO/IEC 24727 applications.

---

[3] Part 3 of ISO/IEC 24727 defines services as representations of action requests and action responses to be supported at the client-application interface. Essentially, it provides a high-level interface for a client-application making use of information storage and processing operations of a card-application.

Specifically, ISO/IEC 24727 provides:

- a standard set of services that allow client-applications to interact with card-applications (i.e., services provide for card-application connection, information discovery and retrieval, cryptographic operations, and identity authentication), in essence, providing a common foundation for identification systems;

- standardized authentication and security protocols (such as asymmetric internal authenticate, asymmetric external authenticate, symmetric internal authenticate, symmetric external authenticate, PIN compare, biometric compare, client application mutual authentication with key establishment, key transport with mutual authentication based on Rivest Shamir Adleman (RSA));

- standardized access to cryptographic algorithms (to include symmetric key algorithms such as Advanced Encryption Standard (AES), Triple Data Encryption Algorithm (TDEA); asymmetric, public key cryptography such as Elliptic Curve Cryptography (ECC)–based algorithms and RSA; hash functions; Message Authentication Code (MAC) and others);

- standardized mechanisms for discovery of card application(s) capabilities;

- a flexible security model that allows users of the standard to select and determine what level of security will be used by their implementation; and

- adaptable interfaces supporting a well-defined requirement for programmability and extensibility of interface devices, such as card readers.

2.1 ISO/IEC 24727 – A Multi-part International Standard

ISO/IEC 24727 is presented in logical increments. Each part was developed in concert with the other parts for optimal technical synchronization. The first part provides the overall architecture of ISO/IEC 24727. Parts 2, 3, and 4 establish the interface semantics of the architecture. Part 5 provides testing requirements for compliance to the standard. Part 6 provides registration procedures for additional authentication and security protocols, thereby allowing the standard to evolve to meet changing demands and technological capabilities. ISO/IEC 24727 thus consists of the following parts:

- ISO/IEC 24727-1 – Identification cards – Integrated circuit card programming interfaces – Part 1: Architecture. This part is discussed in Section 2.2.

- ISO/IEC 24727-2 – Identification cards – Integrated circuit card programming interfaces – Part 2: Generic card interface. This part is explained in Section 2.4.

- ISO/IEC 24727-3 – Identification cards – Integrated circuit card programming interfaces – Part 3: Application interface. This part is explained in Section 2.3.

- ISO/IEC 24727-4 – Identification cards – Integrated circuit card programming interfaces – Part 4: API administration. This part is explained in Section 2.5.

- ISO/IEC CD 24727-5 – Identification cards – Integrated circuit card programming interfaces – Part 5: Testing. This part is discussed in Section 2.6.

+ ISO/IEC CD 24727-6 – Identification cards – Integrated circuit card programming interfaces – Part 6: Registration procedures for the authentication protocols for interoperability. This part is discussed in Section 2.7.

At the time of this writing, the first four parts are published International Standards and available at http://www.incits.org/. Currently, each part is individually priced at $30.00USD. ISO/IEC 24727-5 and ISO/IEC 24727-6 are nearing completion. For the purposes of this proof-of-concept discussion, the details of parts 5 and 6 are not essential.

2.2 Part 1: ISO/IEC 24727 - Identification cards – Integrated circuit card programming interfaces – Part 1: Architecture

Part 1 of ISO/IEC 24727 specifies the architecture on which subsequent parts are based. It forms a high level description of the multi-layered ISO/IEC 24727 APIs and their interactions.

The system architecture is depicted in Figure 1. A more detailed architecture diagram can be found in ISO/IEC 24727-1. As shown in Figure 1 below, client-applications use the services and interfaces defined in ISO/IEC 24727-3. The client-application discovers the card's services, information, and other capabilities through the SALII. After discovery, the client-application can access the services that are implemented on the presented card through the SALII. The actual execution and discovery of the card services and capabilities is further explained in the following sections.

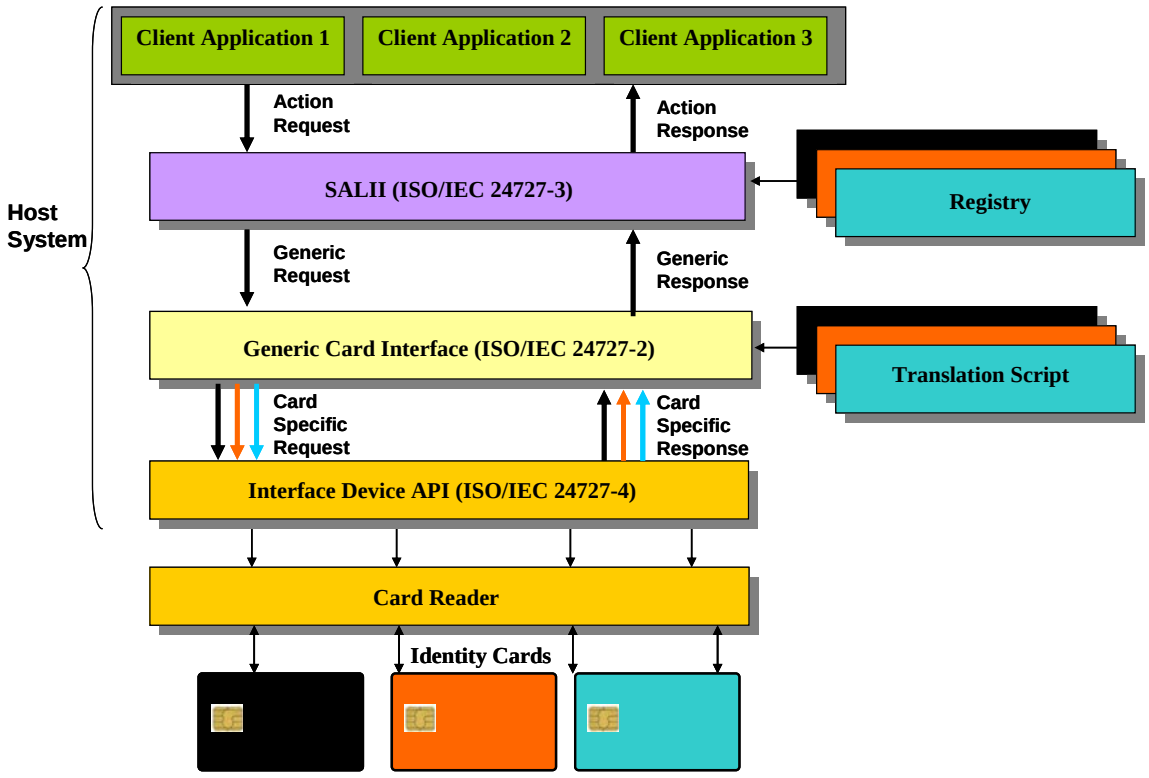

Figure 1 – Logical Architecture of ISO/IEC 24727

2.3 Part 3: ISO/IEC 24727-3 – Identification cards – Integrated circuit card programming interfaces – Part 3: Application interface

ISO/IEC 24727-3 provides high level card services that are available to the client-application through the Service Access Layer Interface for Identity (SALII). Through SALII, the client-application can request actions on the objects of the card-application. A single service request (e.g., authenticate identity) may be a one-step (e.g., Personal Identification Number (PIN) verification) or a multi-step protocol (i.e., two-way authentication). The ISO/IEC 24727-3 implementation is responsible for expanding the single service action into multiple requests to achieve the desired results. Specifically, the ISO/IEC 24727-3 implementation performs data object discovery, learns access control requirements, and organizes actions into sequences of requests as necessary through the Generic Card Interface.

For example, the SALII includes an authentication service named 'DIDAuthenticate'. This service allows the client-application to authenticate a cardholder's PIN. Instead of creating a smart card specific command, the client-application invokes the ISO/IEC 24727-3 'DIDAuthenticate' service and passes the PIN number through the interface. The ISO/IEC 24727-3 implementation then packages the PIN number into a Generic Card Interface instruction and sends it to the ISO/IEC 24727-2 implementation. The Generic Card Interface instruction is packaged in accordance with the 'discovered' data objects on the card. In order to do the discovery, an ISO/IEC 24727-3 implementation needs to come to know which key reference to use within the card-application. This mapping from the named "PIN number" to the key reference is discovered through a data structure called the registry.

2.3.1 Registry

The registry is card-application specific and can be retrieved from an on-card storage location (from the card-application's Application Capability Description (ACD) when it is activated) or from an alternative off-card storage location. The registry contains data object information, access control requirements, key references, cryptographic algorithm references, and protocol references supported by the card-application. The registry also provides associations between the objects and key references. The SALII implementation receives a service action on its interface, and with the help of the registry, translates the service into a sequence of requests/commands for the Part 2 Generic Card Interface. This is illustrated in Figure 2.

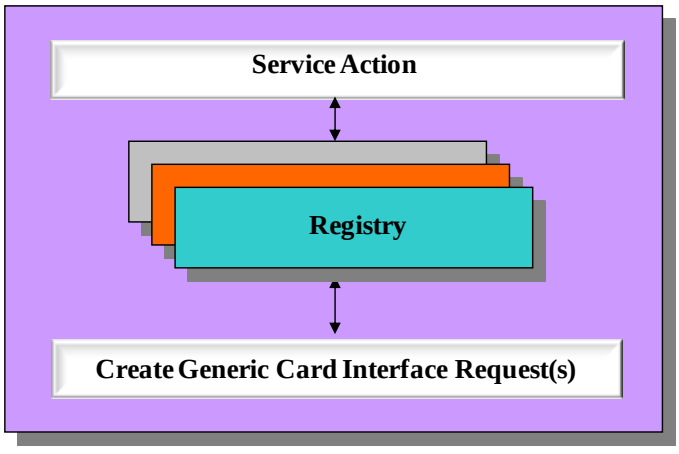

Figure 2 – Use of the Registry by ISO/IEC 24727-3

2.3.2 ISO/IEC 24727 Authentication Protocols

ISO/IEC 24727-3 provides a set of normative authentication protocols. Currently, IDMS implementations use authentication protocols to meet their requirements but the protocols may differ from implementation to implementation. For example, two IDMS implementations might use an on-card biometric comparison authentication protocol. However, it is likely they will have technical differences that make each instance unique even though both implementations are accomplishing authentication using essentially the same technology. The lack of normative authentication and security protocols introduces interoperability challenges within and amongst different identity credentialing systems. For this reason, ISO/IEC 24727-3 and ISO/IEC 24727-6 establish a set of normative authentication protocols including:

- Asymmetric Internal Authenticate
- Asymmetric External Authenticate
- Symmetric Internal Authenticate
- Symmetric External Authenticate
- PIN Compare
- Biometric Compare
- Mutual Authentication with Key Establishment
- Key Transport with mutual authentication based on RSA
- Secure PIN Compare
- Global Platform (GP) Asymmetric Authentication

2.4 Part 2: ISO/IEC 24727-2 - Identification cards – Integrated circuit card programming interfaces – Generic card interface

Smart cards use commands largely defined by a well-known international multi-part standard, ISO/IEC 7816, *Information technology — Identification cards — Integrated circuit(s) cards with contacts* [7]. However, ISO/IEC 7816 provides different methods to communicate with a smart card and often offers implementers different options for the same function. For example, two different commands support retrieval of data from a card. There is further flexibility provided through a range of command specific options. Thus, it is difficult to achieve effective interoperability among different cards, even when they each state adherence to ISO/IEC 7816.

ISO/IEC 24727-2 recognizes and accommodates these functionally equivalent but syntactically different commands by defining requirements for a procedural element, also referred to as a translation script, that translate the Generic Card Interface commands to the commands actually implemented by a particular card-application. The translation script is card or card-application specific and typically runs on the host system environment. The translation script may be retrieved directly from permanent storage on cards or may be obtained from an alternate storage location. The task of ISO/IEC 24727-2 is to use the retrieved translation script and dynamically translate the ISO/IEC 7816 commands from the entry points of its Generic Card Interface (as specified in Table 2 of ISO/IEC 24727-2) to the ISO/IEC 7816-based commands implemented by the actual card. This is illustrated in Figure 3.

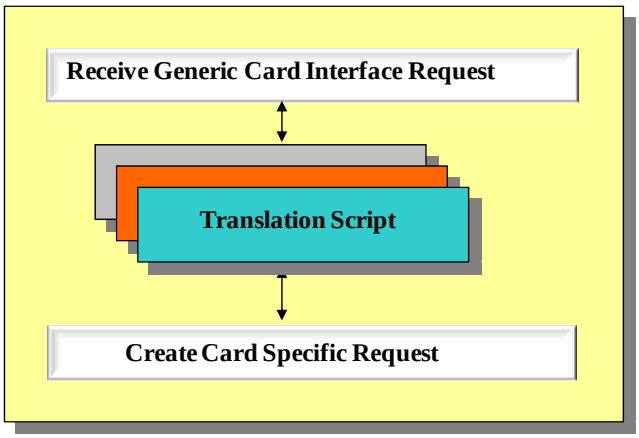

Figure 3 – Use of the Procedural Element by ISO/IEC 24727-2

An ISO/IEC 24727-2 implementation does not have prior knowledge of commands used by the card-applications. Rather, it accomplishes the translation with help from the translation script that is retrieved from the card or other alternative locations. Once the Part 2 implementation retrieves the translation script, it can dynamically respond to SALII generic requests, translate the Generic Card Interface commands as needed, and send card specific commands on to the card.

To address platform interoperability and processing efficiency of the translation script, ISO/IEC 24727-2 uses a single language, a virtual machine that conforms to ISO/IEC 20060 – Open Terminal Architecture (OTA) Specification – Virtual Machine Specification [8]. This ensures that the translation script can be interpreted and run on any ISO/IEC 24727-2 implementation in real time without requiring the implementations to support multiple languages.

2.5 Part 4: ISO/IEC 24727- 4 – Identification cards – Integrated circuit card programming interfaces – API administration

ISO/IEC 24727-4 establishes the details for different stack configurations and features that enable client-applications to interface with card-applications in different ways. Stack configuration choices range from performing all necessary services directly on a smart card to achieving the same functionality in a distributed network environment. The stacks defined are:

+ Full network stack — a configuration where the various ISO/IEC 24727 interfaces are implemented in a networked environment on different platforms.

+ Loyal stack — a configuration where ISO/IEC 24727-2 and ISO/IEC 24727-3 are implemented on the same platform.

+ Remote loyal stack — a configuration where a loyal stack is used on a platform that is remote from the client-application.

+ Opaque Integrated Circuit Card (ICC) stack — a configuration where the card-application implements and interprets the Generic Card Interface commands.

+ ICC resident stack — a configuration where the card-application accepts the SALII actions instead of ISO/IEC 7816 commands.

+ Remote ICC stack — a configuration where physical connection of the ICC is made to a different platform from the rest of the stack.

While all of the above configurations are possible, this document will focus on only two: the Loyal stack and ICC resident stack. Figure 4 provides an illustration of how the two configurations are implemented to achieve the same results.

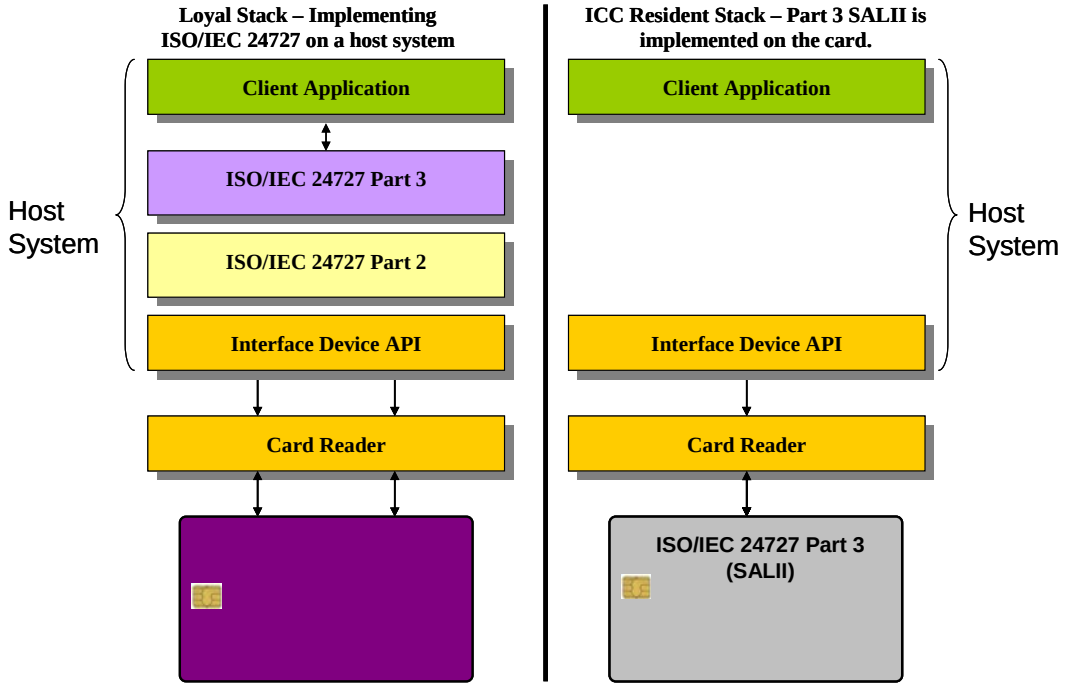

Figure 4 – Comparison of Loyal and ICC Resident Stack

2.6 Part 5: ISO/IEC CD 24727- 5 – Identification cards – Integrated circuit card programming interfaces – Testing

ISO/IEC 24727-5 defines test procedures that can be used to validate conformance assertions. The test procedures focus on testing the behaviors of interfaces for each component of the ISO/IEC 24727 architecture to ensure interoperable services, integrity reporting, and connectivity. The intent is to enable flexibility by providing for single component testing, (e.g., a Part 3 implementation), multiple component testing (e.g., a Part 3 and Part 2 implementation) or complete ISO/IEC 24727 stack testing.

2.7 Part 6: ISO/IEC CD 24727- 6 – Identification cards – Integrated circuit card programming interfaces – Registration procedures for the authentication protocols for interoperability

This part is intended to provide a facility for adding new authentication protocols to the normative set currently found in Part 3. Modifications to international standards are required to go through the ISO/IEC amendment process and can be protracted in nature. Part 6 will expedite this process without sacrificing ISO/IEC 24727 conformance requirements by providing a registry for protocol developers to register new protocols. The registration authority also provides an option for end-users and card issuers to register their use of ISO/IEC 24727.

3. ISO/IEC 24727 Proof-of-Concept

It is not uncommon for identity related applications and implementations to require 'tweaking' when a new card-application or service is added, identity credential attributes change, or an agency chooses to interoperate with diverse identity credentials. Configuration management of post-issuance card and card-application activities in a dynamic production and operational environment historically has offered a challenging management task. Correctly designed ISO/IEC 24727 interfaces provide a means to address these challenges.

3.1 Proof-of-Concept Applications

This section presents a proof-of-concept narrative on the applicability and use of the ISO/IEC 24727 framework. The narrative proceeds through the use of three client-applications previously mentioned: smart card logon, email signing and encryption, and Web authentication using a PIV Card. The proof-of-concept encompasses these three applications using PIV and other identity cards.

3.1.1 Application 1 – Smart Card Logon

Smart Card Logon illustrates the use of a PIV Card for Windows and Linux logon operations. The cardholder inserts the PIV Card into the card reader, enters the cardholder PIN to unlock the card, and authenticates to the host platform. The cardholder is subsequently logged on to the host platform. Figure 5 illustrates this process.

- **Alice inserts her PIV Card into the Reader**
- **At the logon prompt, Alice enters her user ID and the PIN to her PIV Card**
- **After successful authentication, involving a challenge-response and certificate path validation, Alice is logged on the machine**

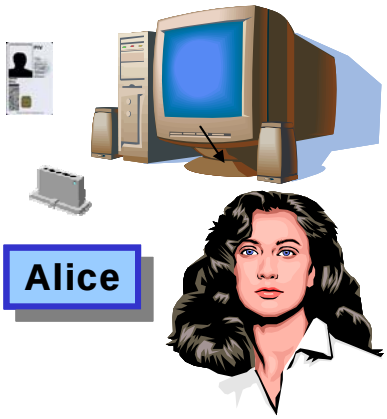

Figure 5 – PIV Card Smart Card Logon

At the present time, the PIV smart card logon application can only accept PIV Cards. Although other identity cards may have the same capabilities and features, the PIV middleware (i.e., API) is not equipped to discover different data constructs and applications that may be present on other cards. By using ISO/IEC 24727 mechanisms, the single credential use, in this case PIV, is expanded to allow the use of other identity cards.

3.1.2 Application 2 – Email Signing and Encryption

The PIV email signing and encryption application (see Figure 6) illustrates the use of a PIV cardholder's credentials for email signing and encryption. The user is required to establish accounts and configure the email client to use the PIV Card. PIV Cards allow cardholders to digitally sign and encrypt emails without the need for additional credentials. A cardholder signs the email with the on-card Digital

Signature Key or decrypts an encrypted message with the on-card Key Management Key (KMK). The process flow for email signing and encryption is depicted in Figure 6.

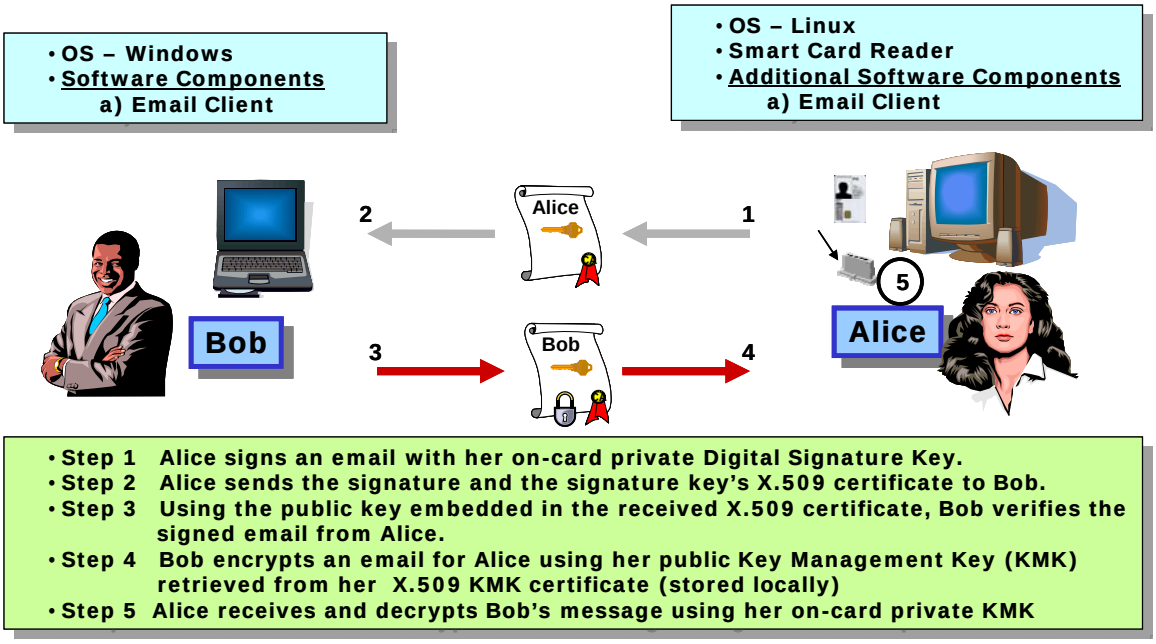

Figure 6 – PIV Card Email Signing and Encrypting

The PIV Digital Signature Key and PIV Key Management Key on the PIV Card are used to accomplish email signing and encryption. Through the use of ISO/IEC 24727 constructs, it can be demonstrated that the same signing and encryption protocol used by the PIV Card can be performed with other identity cards that hold digital signature and encryption keys.

3.1.3 Application 3 – Web Authentication

The PIV Web application illustrates the use of PIV credentials for Web authentication by setting up user accounts on the Web server and enabling the browser to use the PIV Card. The cardholder provides his/her card PIN to unlock the card and the browser performs the necessary cryptographic challenge-response with the PIV Card's private key to authenticate to the Web server. Once authenticated, the Web application provides access to the requested Web pages based on the user's privileges. The process flow for Web authentication is depicted in Figure 7.

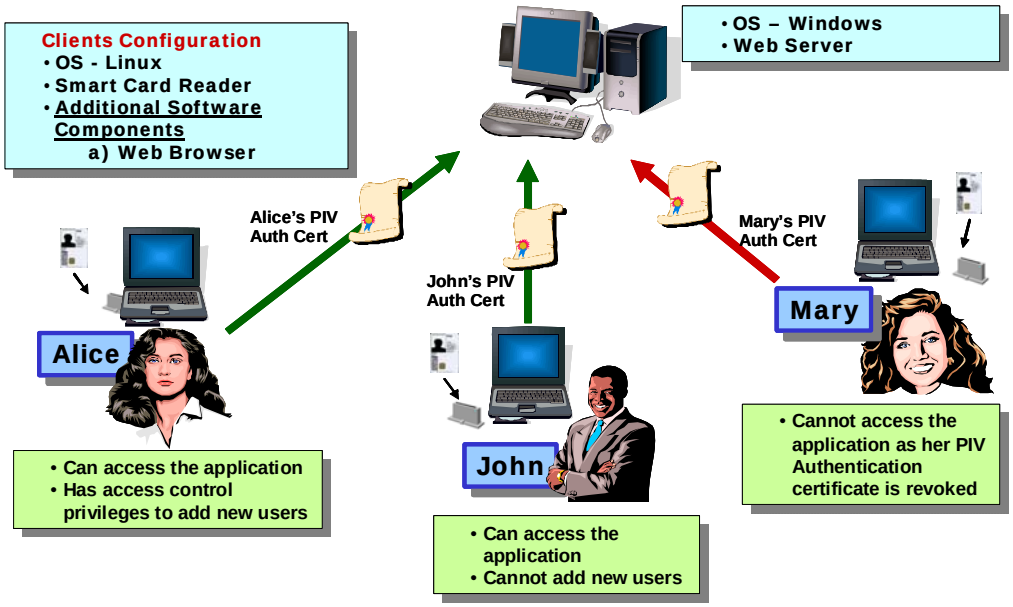

Figure 7 – PIV Card Web Authentication

The on-card PIV Authentication Key is used to enable web authentication. Using ISO/IEC 24727, it can be demonstrated that the same asymmetric authentication protocol can be used with different identity cards and that the client-application can discover the asymmetric authentication key to use for Web authentication.

3.1.4 Existing PIV Applications Architecture

The applications described in Sections 3.1.1, 3.1.2, and 3.1.3 currently use the PIV reference implementation to communicate with the PIV Card. The client-application is developed independent of the PIV Card and is encoded to use the PIV API as defined in NIST Special Publication (SP) 800-73 [9]. The NIST SP 800-73 also defines a smart card interface called Card Edge interface.

The PIV reference implementation implements the PIVAPI and Card Edge interfaces on the same platform. This configuration is equivalent to a Loyal stack in ISO/IEC 24727 (see Figure 4).

The existing architecture of the PIV demonstration is shown in Figure 8.

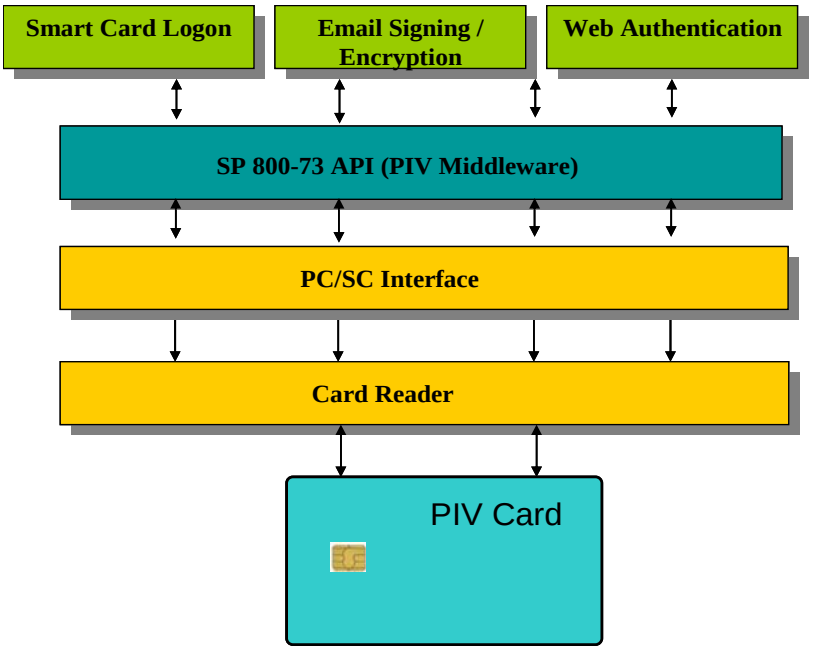

Figure 8 – PIV Implementation

3.2 Proof-of-Concept Design Considerations

An ISO/IEC 24727 reference implementation will be used for the applications described in the previous sections to authenticate identity cards from different issuers. Hypothetically, there are three potential methods of using an identity card with ISO/IEC 24727:

+ Method 1 — ISO/IEC 24727 with currently deployed identity cards

  With this method, a client-application can interact with an ISO/IEC 7816-based identity card with the help of an ISO/IEC 24727 off-card translation script and registry. When a card is inserted in the reader, the ISO/IEC 24727 implementation discovers the card, retrieves the translation script and registry off-card, and begins communication with the card. The ISO/IEC 24727-3 (SALII) implementation receives service requests from the client-application and decomposes the requests for the ISO/IEC 24727 Generic Card Interface. In turn, the Generic Card Interface receives the command/request, translates the commands using the translation script, and sends the card-specific command(s) to the card. The card produces one or more response(s) that are translated by the translation script on their way back to the ISO/IEC 24727-3, which produces a service response to the client-application.

  An example of method 1 implementation in the Federal government is the current PIV Card where the translation script and registry is retrieved off-card by the ISO/IEC 24727 implementation. With the ISO/IEC 24727 enabled client-applications and card specific translation script and registry, Federal government agencies can authenticate current PIV Cards as well as other identity cards. With this method a current PIV Card can be used with today's PIV systems and with ISO/IEC 24727 systems.

+ Method 2 — ISO/IEC 24727 with translation script and registry on identity cards

This is similar to method 1, with the exception that the translation script and registry are retrieved directly from the identity card using an ISO/IEC 24727 bootstrap procedure. The bootstrap procedure allows the translation script and registry to be discovered by ISO/IEC 24727 implementation on the host system and read from the card. The client-application uses the identity card in the same manner as in method 1. As a result, client-applications based on ISO/IEC 24727 are unaware of where the translation script and registry are retrieved and remain unchanged.

An example of method 2 implementation in the Federal government would be an updated PIV Card where the translation script and registry is retrieved from the card. With this method, the client-applications benefit from the portability and immediate access to the translation script and registry available on the card. Client-applications built on ISO/IEC 24727 are unaffected by the use of method 1 versus method 2 cards. From the PIV Card perspective, the method 2 implementation is different from method 1 because the PIV Card contains additional data objects and a bootstrap procedure. Like a method 1 PIV Card, a method 2 PIV Card can be used in today's PIV systems and in ISO/IEC 24727 implementations but the ISO/IEC 24727 systems do not need to be pre-loaded with the PIV translation script and registry because they are carried on the PIV Card.

+ Method 3 — ISO/IEC 24727 ICC-Resident Stack implemented on the identity card

  With an ISO/IEC 24727 ICC-Resident Stack, the identity card responds to service requests through the SALII (see Figure 4). The complexity of ISO/IEC 7816 card specific commands and responses is removed. Consequently, the ISO/IEC 24727-2 implementation does not exist as the card directly responds to SALII actions. Client-applications built on ISO/IEC 24727 are unaffected by the methods and remains unchanged. These client-applications could, therefore, authenticate identities using method 1, method 2, or method 3 cards.

  An example of method 3 implementation in the Federal government would be a PIV card-application using a SALII interface. From the PIV perspective, a method 3 PIV Card differs from the method 1 and method 2 PIV Card because it uses the SALII interface on-card. While method 3 impacts backward-compatibility for today's Federal Information Processing Standard (FIPS) 201 PIV systems, it increases security through the capabilities of ISO/IEC 24727 access controls and secure sessions for interconnection between the PIV Card with the ICC-Resident Stack and the applications using the card. These security mechanisms are more robust and comprehensive than those currently in use.

The methods described in this document are specific design approaches and other approaches are possible.

3.2.1 Design Improvements and Trade-offs

The three methods are hypothetical and discussions on the practical integration of PIV with ISO/IEC 24727 components are just beginning. These methods demonstrate, at a high-level, that PIV Cards can be used with ISO/IEC 24727 components in a number of very different ways. Each of the methods embodies different design improvements and tradeoffs:

+ Method 1 enables an ISO/IEC 24727 implementation to translate PIV Card commands and requires no change to existing PIV Cards while improving the ability to interoperate with other credentials. This method offers complete backward compatibility with existing PIV systems.

+ Method 2 requires the addition of two objects and a bootstrap procedure to existing PIV cards but improves the transparent use with other credentials and minimizes configuration management of post-issuance activities. The use of additional objects would impact FIPS 140-2 validation [10].

+ Method 3 provides a way forward for improvements in security and interoperability but must consider backwards compatibility with existing PIV implementations and impact to FIPS 140-2 validation. To maintain compatibility with existing PIV system, the method 3 PIV Card, can be combined side-by side with a FIPS 201 PIV Card Edge specification. "Side-by-side" means that the FIPS 201 PIV Card Edge and the ICC-Resident Stack share the same PIV data objects on the smart card. This side-by-side method 3 PIV Card can therefore project the user's credentials either through today's PIV Card Edge or through the ISO/IEC 24727 ICC-Resident Stack interface with the SALII. A side-by side method 3 PIV Card is simultaneously a current PIV Card and a consequent PIV Card that provides an innovative API for future application.

Because of the platform independence inherent to ISO/IEC 24727, the ISO/IEC 24727 implementation on the host system is constructed to read the PIV Cards as well as other smart card based credentials.

3.2.2 Proof-of-concept Architecture

For the purpose of the proof-of-concept, NIST plans to replace the PIV middleware with ISO/IEC 24727 constructs, using a method 1 PIV Card for backward compatibility. The resulting architecture after integrating PIV Cards in the ISO/IEC 24727 framework is shown in Figure 9.

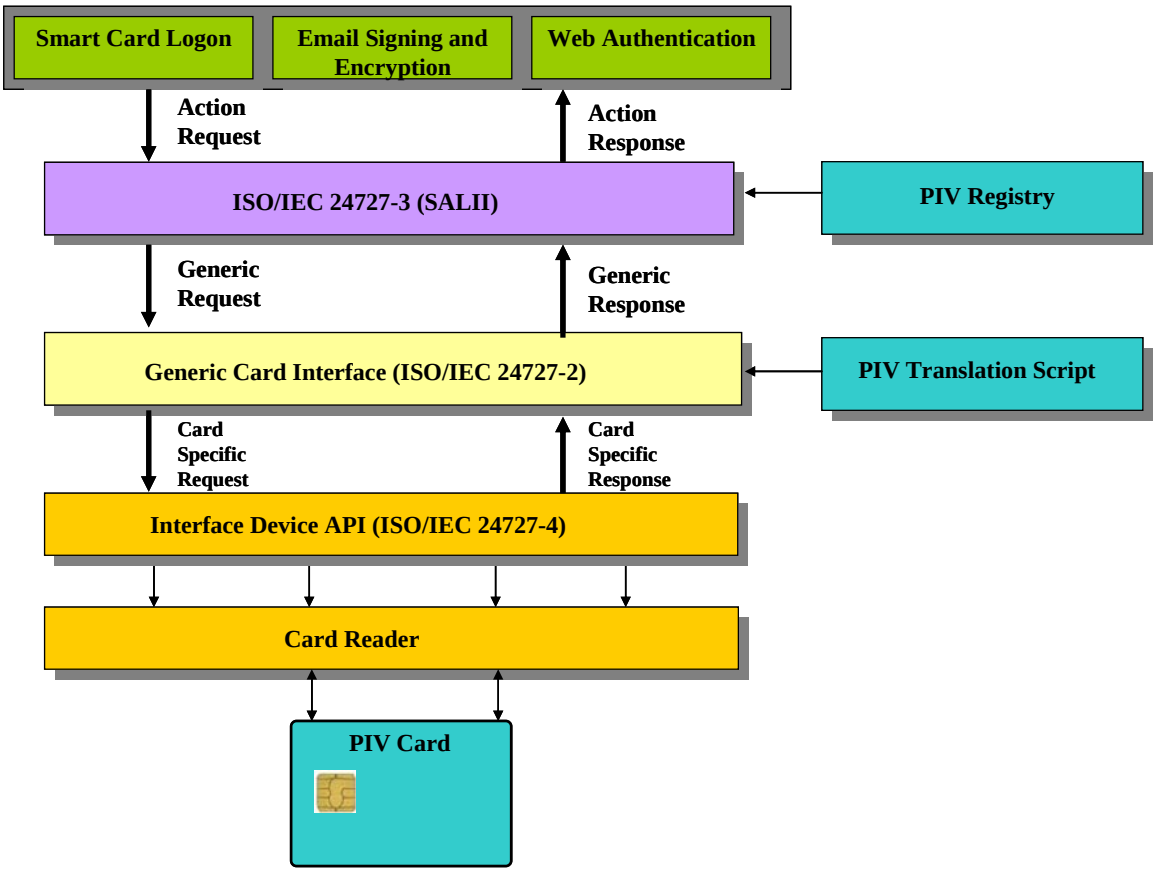

Figure 9 – Using PIV Card in the ISO/IEC 24727 Framework

Note that the client-application is completely independent of the identity credential. Also, note that the ISO/IEC 24727-2 and ISO/IEC 24727-3 implementations do not contain any PIV card specific information or logic. They do, however, use the translation script and registry to discover the properties and capabilities of the PIV Card in real-time. Therefore, it is anticipated that more identity credential cards can be added, as shown in Figure 1, to this architecture using the same methodology. A single ISO/IEC 24727 conformant implementation can be configured to authenticate various credentials, such as the Transportation Workers Identity Credential, DoD Common Access Card, Western Hemisphere Travel Initiative, and PIV identity credentials.

3.3 Summary

This document provides a high-level discussion on the technical aspects of ISO/IEC 24727. It briefly discusses each of the six parts. Design approaches and backward compatibility are considered. A discussion on normative authentication protocols is presented. The proof-of-concept presented is based on the use of ISO/IEC 24727 with the US government identity credential, PIV, PIV card-application, and other identity credentials. The presentation is done at a high-level and a follow-on document will, through the use of a reference implementation, provide the technical detailing in support of this discussion.

Appendix A—Acronyms

The following acronyms and abbreviations are used throughout this document:

ACD Application Capability Description

AES Advanced Encryption Standard

APDU Application Protocol Data Unit

API Application Programming Interface

CAC Common Access Card

CSP Cryptographic Service Provider

FIPS Federal Information Processing Standards

GCI Generic Card Interface

HSPD Homeland Security Presidential Directive

IDMS Identity Management System

ICC Integrated Circuit Card

IEC International Electrotechnical Commission

IIS Internet Information Server

ISO International Organization for Standardization

ITL Information Technology Laboratory

KMK Key Management Key

MAC Message Authentication Code

NIST National Institute of Standards and Technology

NISTIR National Institute of Standards and Technology Interagency Report

OMB Office of Management and Budget

OSI Open System Interconnection

OTA Open Terminal Architecture

PC/SC Personal Computer/Smart Card

PIN Personal Identification Number

PIV Personal Identity Verification

PKCS Public Key Cryptography Standards

RSA Rivest Shamir Adleman

SAL Service Access Layer

SALII ISO/IEC 24727 Service Access Layer Interface for Identity

SP Special Publication

TDEA Triple Data Encryption Algorithm

TWIC Transportation Worker Identification Credential

US United States

WHTI Western Hemisphere Travel Initiative

Appendix B—References

[1] ISO/IEC 24727-1- *Identification Cards – Integrated Circuit Cards Programming Interfaces – Part 1: Architecture*, June 23, 2006.

[2] ISO/IEC 24727-2- *Identification Cards – Integrated Circuit Card Programming Interfaces – Part 2: Generic card interface*, September 2008.

[3] ISO/IEC 24727-3 - *Identification Cards – Integrated Circuit Card Programming Interfaces – Part 3: Application interface*, September 2008.

[4] ISO/IEC 24727-4 - *Identification Cards – Integrated Circuit Cards Programming Interface – Part 4: API Administration*, September 2008.

[5] ISO/IEC CD 24727-5 - *Identification Cards – Integrated Circuit Cards Programming Interface – Part 4: Testing.*

[6] ISO/IEC FDIS 24727-6 - *Identification Cards – Integrated Circuit Cards Programming Interface – Part 6: Registration procedures for the authentication protocols for interoperability.*

[7] ISO/IEC 7816 (Parts 4, 5, 6, 8, and 9), *Information technology — Identification cards — Integrated circuit(s) cards with contacts.*

[8] ISO/IEC 20060 *Information technology - Open Terminal Architecture (OTA) specification - Virtual machine specification*, 2001.

[9] NIST SP 800-73-2, *Interfaces for Personal Identity Verification*, September 2008. (See http://csrc.nist.gov/groups/SNS/piv/standards.html)

[10] FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25, 2001. Available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.