Supporting the PIV Application in Mobile Devices with the UICC

A Smart Card Alliance Identity, Mobile and NFC, and Access Control Council White Paper

Publication Date: June 2013

Publication Number: IC-13001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use, and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information, please visit http://www.smartcardalliance.org.

The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

TABLE OF CONTENTS

1 PURPOSE 4

2 RATIONALE 5

3 USE CASES 6

3.1 MOBILE DEVICE AS AN END-POINT COMPUTING DEVICE 6
3.1.1 Sending a Signed E-mail Message 6
3.1.2 Decrypting an E-mail Message 6
3.1.3 Using Secure Web Access to Remote Services 6
3.1.4 Encrypting and Decrypting Files 7
3.1.5 Accessing a Virtual Private Network (VPN) 7
3.1.6 Signing Documents 7
3.2 MOBILE DEVICE EMULATING A CONTACTLESS SMART CARD 7
3.2.1 Use Cases with Current FIPS 201-1: Card Physical Access 7
3.2.2 Use Cases with FIPS 201-2 Draft 2 8
3.3 MOBILE DEVICE ACTING AS A SMART CARD WITH THE CARD READER, PIN PAD AND DISPLAY 9
3.4 OTHER USE CASES 9
3.4.1 Out-of-Band (OOB) Authentication 9
3.4.2 Identity Card 9

4 INTEGRATION OF PIV WITH THE MOBILE PHONE AND UICC 11

4.1 MOBILE PLATFORM ARCHITECTURE AND COMPONENTS 11
4.1.1 PIV Applet on a UICC 12
4.2 PROVISIONING INFRASTRUCTURE 13
4.3 PIV MANAGEMENT SYSTEM CONNECTED TO THE PROVISIONING INFRASTRUCTURE 13

5 PROVISIONING AND MANAGEMENT MODEL FOR THE PIV APPLET AND CREDENTIALS IN THE UICC15

6 IMPACTS ON POLICY AND RECOMMENDATIONS 17

7 CONCLUSIONS 18

8 PUBLICATION ACKNOWLEDGEMENTS 20

9 APPENDIX A: ACRONYMS 22

1 Purpose

The increasing utilization of mobile devices such as smart phones and tablets has expanded the capability of employees to stay connected longer and be more active and efficient in their work. These connected devices are designed for the mass market often with little to no security enabled in their hardware or embedded into their applications. The mobile security requirements for a corporate or government employee are quite different, especially with organizations allowing employees to bring their own device (BYOD). Securing sensitive and confidential information within email clients and enabling secure access to remote services require an underpinning of security techniques and features.

This white paper was developed to provide guidance to U.S. Government policy makers and technologists on the key technical, business and policy considerations for supporting the Personal Identity Verification (PIV) application and credentials on mobile devices using the Universal Integrated Circuit Card (UICC).

The white paper sets out a strategy for securing mobile devices by focusing on the UICC that is present in most mobile devices; the UICC is the hardware-based "secure element" that is used for storing protected data and applications and providing a secure execution environment for those applications. Although this document is specifically aimed at the U.S. Government market and PIV credentials, the approach employs techniques and technologies that can apply to any smart-card-enabled identity credential and token and any UICC-enabled smart phone or mobile device. This strategy will enable corporations, government agencies and mobile telecommunication companies to take advantage of and achieve scale for the growing need to provide secure PKI-based services on mobile devices.[1]

[1] It is important to note that the hardware-based "secure element" can also reside in an embedded smart chip in the mobile device or in a smart microSD card. This white paper does not cover those secure element form factors.

2 Rationale

The mobile device market is rapidly evolving and ever-changing. Highly competitive market forces result in the delivery of new handsets, and new and regularly updated mobile and tablet operating system platforms (such as iOS, Android, Windows Mobile) at an ever-increasing pace. With this fluid market, the ability to undertake the lengthy cryptographic certifications required by the U.S. Government for cryptographic modules (i.e., FIPS 140-2) is extremely challenging given the lifetime of the handsets and operating systems. However, there is a secure element in most modern mobile devices that, by nature of its stable, removable and standardized form factor and interface (communication protocol), is less susceptible to changes in the handsets and the OS environment: the UICC. Furthermore the UICC already has security certifications that are driven and embraced by the telecommunications industry.[2]

Selecting the UICC allows the government to have a stable, certified form factor and managed lifecycle for the secure element containing the PIV application and credential, and provides for a logical extension for storing the PIV framework's "derived credentials" on a mobile device. This is also true for corporate usage of Commercial Identity Verification (CIV) and PIV-interoperable (PIV-I) credentials.[3] Market forces can then leverage this platform to create the various higher level services needed, such as the specific handset operating system functionality and applications to make use of the mobile PIV credential for securing email and browsers on the mobile devices.

The key characteristic of this approach is that the UICC performs the same function for the user that the smart card chip of a PIV smart card performs: it acts as a secure container to protect the user's private keys that are used for identity authentication, digital signatures and encryption. Furthermore, it protects those keys so that they cannot be copied, including in the event of compromise of the handset or physical access to the device. Finally, the secure element of the UICC acts as the *security boundary* for cryptographic operations, so that government organizations can be confident that those operations are performed properly and securely.

[2] The telecommunications industry uses Common Criteria protection profiles for security certifications.

[3] Additional information on CIV and PIV-I credentials can be found on the Smart Card Alliance web site at: http://www.smartcardalliance.org/pages/publications-a-comparison-of-piv-piv-i-and-civ-credentials.

3 Use Cases

The way someone might use PIV credentials with a mobile device can be grouped into three categories:

- Mobile device acting as an end-point computing device
- Mobile device emulating a contactless smart card
- Mobile device acting as a smart card with card reader, personal identification number (PIN) pad and display

All of these use cases describe the primary features of having PIV credentials on the UICC. Grouping the use cases into the categories is purely conceptual. The use cases are not restricted to any one of these categories nor are the use cases exhaustive. However, the use cases do require support by the mobile platform and associated applications; these areas, along with the technical implementation aspects, are covered in later sections of this white paper.

3.1 Mobile Device as an End-Point Computing Device

The mobile device increasingly has the same capabilities as a laptop or personal computer (PC) and, with that, users want to use the mobile device in similar ways to securely send and receive e-mails and establish secure connections to organizations. Federal agencies are now required to use the PIV card for accessing agency resources for compliance purposes (e.g., complying with policies specified by the Federal Information Security Management Act (FISMA) and Homeland Security Presidential Directive 12 (HSPD-12)).

In this category, the PIV use cases are similar to what is accomplished using a PIV card with a laptop or desktop PC. However, in this case, the PIV identity credential has been loaded into the UICC of the mobile device, and the PIV applet controlling access to the credentials is running on the UICC that is in the mobile device. From that point forward, the experience is seamless for the user; all of the interaction with the PIV application is performed locally from the mobile device. The following are several example use cases.

3.1.1 Sending a Signed E-mail Message

The user launches the e-mail application on the mobile phone and composes an e-mail message. Before sending the message, the user selects to digitally sign the e-mail from the e-mail application's interface. Determining that the user's PIV credentials are to be used to sign the e-mail message, the e-mail application prompts for the PIN[4]. The user enters the PIN, and the e-mail application authenticates to the PIV application on the UICC, digitally signs the message using the appropriate PIV signing credentials, and sends the signed e-mail.

3.1.2 Decrypting an E-mail Message

The user launches the e-mail application on their mobile phone and comes across an encrypted message. To read the e-mail message, the e-mail application prompts the user to enter the PIN on the mobile phone. The e-mail application uses the PIN to unlock the PIV application, which enables the appropriate PIV encryption private key on the UICC secure element to be used for decryption. Finally, the decrypted message is displayed to the user.

3.1.3 Using Secure Web Access to Remote Services

Launching a web browser on the user's mobile phone, the user visits a web page that requires authentication using PIV credentials. The user selects to logon using a PIV card and is prompted to enter the PIN. This unlocks the PIV application, which then uses the appropriate PIV

[4] In this white paper, the term PIN refers to the PIV card PIN, as defined in FIPS 201.

authentication keys on the UICC secure element to authenticate the user to the website. After entering the PIN, the user is logged into the website with a secure connection.

3.1.4 Encrypting and Decrypting Files

Files stored in a user-specified area on the mobile device are automatically encrypted and decrypted using PIV credentials from the UICC. When a user stores a file in the designated area (or sub area), the file is automatically encrypted using the public key of the designated PIV certificate. When accessing the file later, the user is prompted for the PIN to use the private key from the PIV credentials on the UICC to decrypt the file. This enables the credentials to be used to decrypt the files stored on the handset. The encryption or decryption occurs through any file-related application.

3.1.5 Accessing a Virtual Private Network (VPN)

Similar to secure web access, the organization requires authentication of the user's PIV credentials to access its network. Before accessing the corporate network, the user starts the VPN application on the mobile device. The VPN application prompts the user for the PIN to use the appropriate PIV authentication credential to authenticate. After successful authentication, the secure virtual private network communication between the mobile device and the corporate network is established.

3.1.6 Signing Documents

Similar to signed e-mail, users will need to sign documents (e.g., PDF, Word, or Excel documents) similar to the capability on a PC. In this case, a user would sign a document using the appropriate PIV signing credentials on the UICC through the file format's specific application interface.

3.2 Mobile Device Emulating a Contactless Smart Card

In this category of mobile PIV use cases, the mobile phone acts as a contactless smart card. The PIV application embedded in the UICC communicates through the Single Wire Protocol (SWP) over the Near Field Communication (NFC) interface in card emulation mode to the NFC reader that is used for physical or logical access. This use case is exactly like a PIV smart card performing operations over the ISO/IEC 14443 contactless interface.

Thanks to clever hardware design, the PIV applet and credentials function over the NFC interface even if the battery in the phone is dead, powering the chips from the reader just like a contactless smart card is powered by the reader. This is a significant benefit for use cases like physical access where the solution needs to be available under all circumstances, even when the user forgets to charge the device.

3.2.1 Use Cases with Current FIPS 201-1: Card Physical Access

With the current FIPS 201-1 implementations, the functionality of the contactless interface is limited. Consequently, the primary use case for the contactless interface is physical access.

The user simply taps the phone on the door reader and the phone and UICC emulate the contactless interface of the PIV card. The door reader authenticates the PIV credentials stored on the UICC and unlocks the door. In this case, only the subset of credentials available over the contactless interface of the PIV card is available.

3.2.2 Use Cases with FIPS 201-2 Draft 2

In order to support a wider range of use cases for logical access and more secure physical access, FIPS 201-2 Draft 2[5] introduces a “virtual contact channel” that makes the full PIV data model available over the contactless interface through a secure channel.

Additional use cases that the FIPS 201-2 Draft 2 would enable are described in this section.

3.2.2.1 Card with PIN for Physical Access

The user holds the phone on the door reader and enters the PIN on the PIN pad built into the door reader. The PIN can be sent to the mobile device over the “virtual contact channel” to unlock the credentials on the UICC and these credentials are used to unlock the door. Note that this would require a reader that can communicate the PIN to the mobile device securely through the contactless interface.

3.2.2.2 Secure OS Logon

The user places the mobile phone on the laptop’s or PC’s NFC reader. The PC recognizes this as smart card insertion. For example, the user enters Ctrl-Alt-Del. The OS recognizes that the user’s PIV card is present and responds accordingly to allow the user to perform smart card logon. The OS performs the normal authentication for a PIV smart card but using the PIV credentials on the UICC. The user enters the PIN into the user interface (UI) prompt of the OS.

3.2.2.3 Secure E-mail

The user places the mobile phone on the laptop’s or PC’s NFC reader. The PC recognizes this as smart card insertion. After entering the PIN on the PC, a mail client (such as Outlook) that is configured to use certificates stored on a smart card can then read encrypted email or sign outgoing email.

3.2.2.4 Secure Web Authentication

The user places the mobile phone on the laptop’s or PC’s NFC reader. The PC recognizes this as smart card insertion. After entering the PIN on the PC, a browser configured for client-side SSL authentication using a certificate on a smart card can authenticate to a secure web site.

3.2.2.5 File Decryption

The user places the mobile phone on the laptop’s or PC’s NFC reader. The PC recognizes this as smart card insertion. After entering the PIN on the PC, the file encrypted using the PIV credentials can be decrypted.

3.2.2.6 VPN

The user places the mobile phone on the laptop’s or PC’s NFC reader. The PC recognizes this as smart card insertion. After entering the PIN on the PC, a VPN client that is configured to use certificates on smart cards can authenticate securely.

3.2.2.7 Any other PKI- or Smart-Card-Aware Application

The user places the mobile phone on the laptop’s or PC’s NFC reader. The PC recognizes this as smart card insertion. After entering the PIN on the PC, any application that is PKI aware can use the PIV certificates on the UICC of the mobile device as though they were on a smart card inserted into the laptop or PC.

[5] http://csrc.nist.gov/publications/PubsDrafts.html

3.3 Mobile Device Acting as a Smart Card with the Card Reader, PIN Pad and Display

The mobile device can also act as a PIV smart card with a reader, PIN pad and display to enable the interaction with the user. Some phones can also include a biometric entry device, such as a fingerprint scanner. This interaction requires an app on the mobile device that manages the display, PIN entry and/or biometric authentication and other user interaction, but no other functions are performed on the phone. When the mobile phone is placed on an NFC reader connected to a laptop or PC, the OS acts as if a PIV smart card was inserted into a smart card reader with a PIN pad and display. The cryptographic smart card stack and applications can access the PIV credentials coming from a mobile phone using NFC. Because the app is communicating with the UICC over the contact interface, it has access to the full PIV data model once the PIN has unlocked the card. Therefore, within policy limits, whatever a user could do with a conventional PIV smart card can be done using PIV credentials on a UICC.

All of the use cases in Section 3.2 are supported in this mode with the current generation of FIPS 201-1 components. This use case also provides the convenience of being able to use the PIN pad and display on the user's phone. Users know where to look for the interaction and are familiar with the device. There is also a potentially higher security level in using a known device for PIN entry instead of an unknown door reader.

This use case has the potential to evolve and use additional capabilities of the mobile device – for example, a fingerprint scanner for fingerprint match, a camera for facial image matching, the microphone for voice matching, or perhaps other capabilities in future devices.

3.4 Other Use Cases

Other use cases can be enabled with the PIV applet and credential on the mobile phone's UICC.

3.4.1 Out-of-Band (OOB) Authentication

A user accessing a remote service such as a web site or establishing a VPN connection from a PC could use their mobile phone and the PIV credential in the UICC for authentication. In this scenario, the user would visit a secure website from their PC and enter an identifier such as a username. The OOB authentication server would communicate with the user's associated mobile phone to perform PKI authentication over the air (e.g., through the mobile network or WiFi) using the appropriate PIV authentication credential. The user would be prompted for their PIN on the phone to complete the authentication and let the PC browser enter the website.

Similarly, the user could establish a VPN connection on their PC using the PIV credentials on the UICC in their mobile phone. The user initiates the VPN session on their PC with an identifier and the OOB authentication server performs PKI authentication over-the-air (OTA) to the associated user's mobile phone with the PIV credential. The user is prompted on the phone to provide the PIN to successfully complete the authentication and thereby the VPN connection on their PC.

This same OOB technique could be extended to more granular operations such as signing an e-mail or decrypting a message or file within a remote service when using the mobile phone as the token.

3.4.2 Identity Card

The user is asked by a security guard to present PIV credentials for identity verification. Indicating that the PIV credentials are on the mobile phone, the user starts the PIV identification application on the mobile phone and enters the user's PIV PIN. The security guard starts the PIV ID verifier application on the guard's mobile phone and enters the guard's PIN. They touch phones to communicate over NFC. The verifier displays the "printed" picture and PIV information for the user, performs a challenge/response to verify the user as the credential holder, and (optionally) performs a revocation check on the user's certificate. The user's phone could alternately be used to verify identity with a non-transparent reader such as a handheld verifier or a transparent reader connected to a verification application. In all cases, the user's phone exhibits a high degree of versatility when being used as an identity card and being verified against traditional as well as non-traditional interfaces.

4 Integration of the PIV Application and Credentials with the Mobile Phone and UICC

Implementing any one of the scenarios outlined in Section 3 requires integration with different industry players and the mobile handset, OS and application architecture.

To support the PIV application and credentials on mobile devices in the UICC the following is needed:

(1) **Mobile platform architecture and components**: the PIV applet on UICC; the secure element access component allowing access to the UICC from the mobile applications; mobile middleware abstracting and exposing the PIV security and cryptographic capabilities (i.e., authentication, signature, encryption/decryption) to the mobile apps.

(2) **Provisioning infrastructure**: allowing the provisioning of the PIV applet and its personalization (credential delivery) onto the UICC. This is normally done using one or more trusted service managers (TSM).

(3) **PIV management system connected to the provisioning infrastructure**: the management system for PIV credentials (currently in the form of a card management system (CMS) and one or more certificate authorities (CAs) that generate the credentials for the user that will end up on the PIV card or applet) needs to be able to communicate with the provisioning infrastructure.

The following sections provide an overview of the components and infrastructure and describe how they fit together. The discussion starts at the mobile platform, then moves to the mobile operator and, finally to the government entity controlling the PIV credentials.

4.1 Mobile Platform Architecture and Components

To realize the use case scenarios described earlier, applications running on the mobile phone will need to use the PIV credentials stored on the UICC. To do this, they'll need a similar architecture to the architecture that is available on the PC. Essentially, the application will need to interface with a library to assist with cryptographic operations and with PIV middleware working through a driver to communicate with the PIV applet on the UICC. (See Figure 1.) This functionality would require an update to the device operating system to support this new cryptographic capability, similar to the "Smart Card Cryptographic Service Provider (CSP)" that is deployed on desktop and laptop computers. This update would extend the "client certificate" capabilities already present in the operating system to include client certificates that are secured by the UICC, and present them to the applications and the users in a consistent manner.

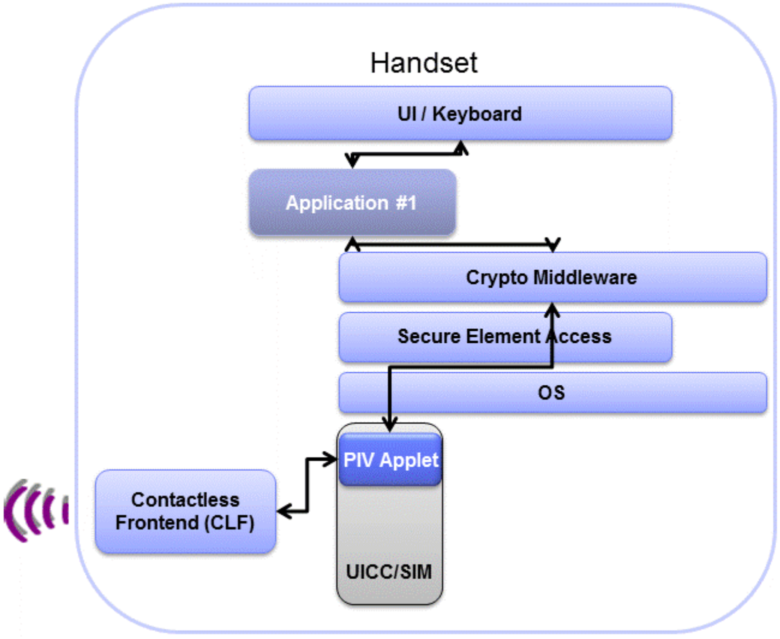


Figure 1. Interfaces to the PIV Applet Stored on the UICC

4.1.1 PIV Applet on a UICC

The mobile network operator (MNO) owns the UICC in a mobile phone with overall control of its contents. To allow use of the UICC for the PIV applet, a portion of the UICC must be "set aside" for use by the user, much as an existing Subscriber Identity Module (SIM) chip can host a user's contacts in a portion of its memory (and allow them to be ported to a new telephone).

Most UICCs in use are Java Card based and GlobalPlatform (GP) compliant[6]; they have the capability to be segregated into separate security zones called "security domains," that effectively allow security containerization between different applets. This effectively provides separation between the applets and their respective keys that are in the different domains so that the PIV applet and its keys can only be accessed by the owner of that security domain – the U.S. Government or local agency in this case.

Based on existing PIV policies and the desire to access sensitive resources with the PIV applet and credentials and in conjunction with the MNO or MNO service provider, the Smart Card Alliance proposes that a dedicated separate security domain be created in the Java Card-based UICC to contain the PIV applet. (See Figure 2.)

[6] GlobalPlatform has developed specifications for managing the secure delivery over-the-air of new services with the UICC. The specifications outline the behavior of each and every actor involved in a UICC implementation, describe how they should be represented, and summarize their roles/responsibilities in a variety of business models. The specifications can be found at: http://www.globalplatform.org/specificationscard.asp. (Note that there is a charge for the specification for organizations who are not GlobalPlatform members.)

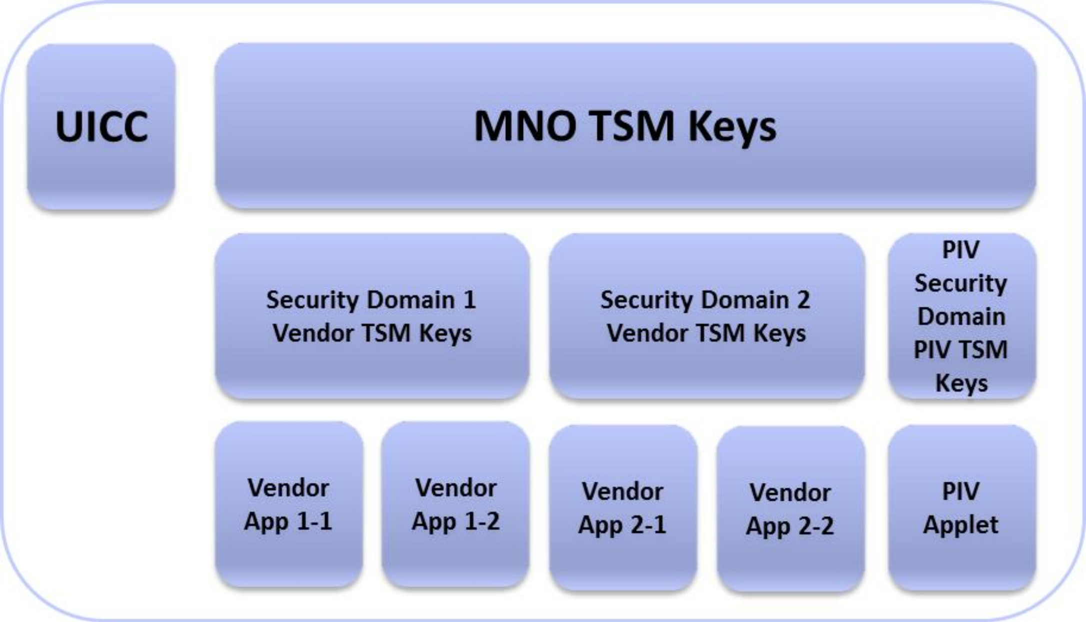

UICC
MNO TSM Keys
Security Domain 1 Vendor TSM Keys
Security Domain 2 Vendor TSM Keys
PIV Security Domain PIV TSM Keys
Vendor App 1-1
Vendor App 1-2
Vendor App 2-1
Vendor App 2-2
PIV Applet

Figure 2. Establishment of a Dedicated, Separate Security Domain for the PIV Applet

4.2 Provisioning Infrastructure

The non-personalized PIV applet[7] (without any user information or keys) could be securely preloaded into the UICC at any one of several points:

1) During the pre-personalization phase (manufacturing) by the UICC vendor in agreement with the MNO
2) By the MNO itself when delivered
3) In the field by a Trusted Service Manager (TSM) operated by the MNO or the government agency or trusted third party on behalf of the government

The TSM provisions applets onto the UICC and manages those applets while ensuring security and confidentiality. The TSM is capable of handling multiple applications, multiple MNOs, and multiple handsets and their operating systems. With these capabilities, the TSM would maintain the relationship with the MNO and have control over the separate security domain and its keys to securely manage and communicate with the PIV applet, separate from the MNO. Communication with the PIV applet could be done over-the-air (OTA) using the MNO's wireless network and/or Internet.

4.3 PIV Management System Connected to the Provisioning Infrastructure

With the PIV applet loaded and instantiated into a security domain, the managing organization or government agency's smart card management system can communicate with the applet in one of several ways to personalize it and manage the credentials. (See Figure 3.) One is through the TSM that securely delivers the command payload to the applet. Another is through the Internet initiated by an application on the mobile phone. In essence, the TSM is the transport mechanism

[7] The applet could be a dedicated PIV applet or an applet that has PIV functionality.

to communicate with the applet on the UICC, similar to the use of PC/SC is for a smart card connected to a reader in the PC.

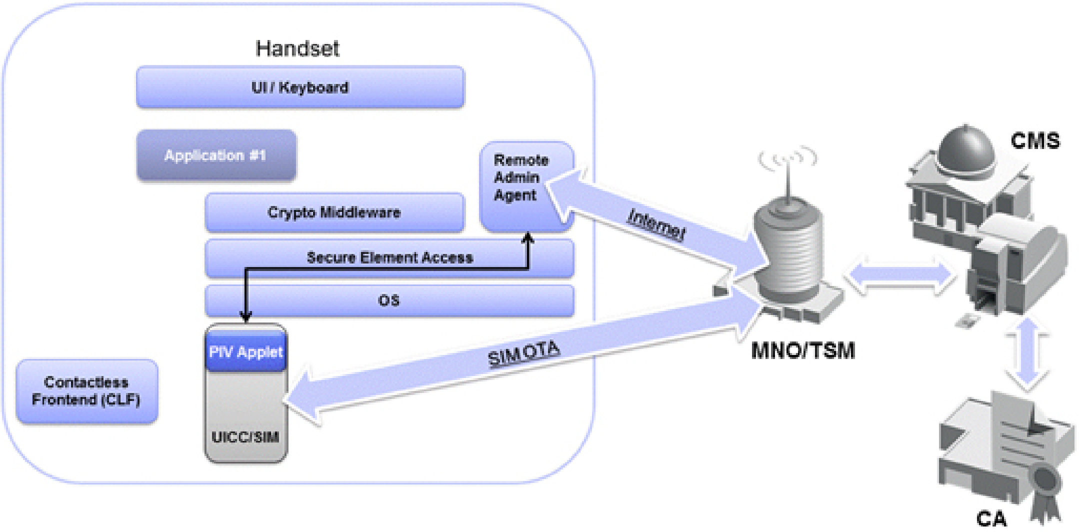


Figure 3. PIV Provisioning Infrastructure

5 Provisioning and Management Model for the PIV Applet and Credentials in the UICC

A benefit of using the UICC for PIV credentials is that the remote provisioning, activation and lifecycle management of the PIV applet and credentials may be done OTA from the issuing authority via the mobile network systems. Figure 4 shows a possible scenario for the relationship between a government agency and an MNO with respect to security domains and key management. It includes the concept of a controlling authority to manage the security domain.

This model illustrates a U.S. Government owner for all remotely configured PIV functionality via a GSA service and corresponding control of a U.S. Government Security Domain on the UICC. This provides a single point of contact between the government and each MNO. Once the security domain is created in the UICC, the MNO can no longer control the applets in this security domain or access the data within it. Only the GSA has the keys to access the Government Security Domain.

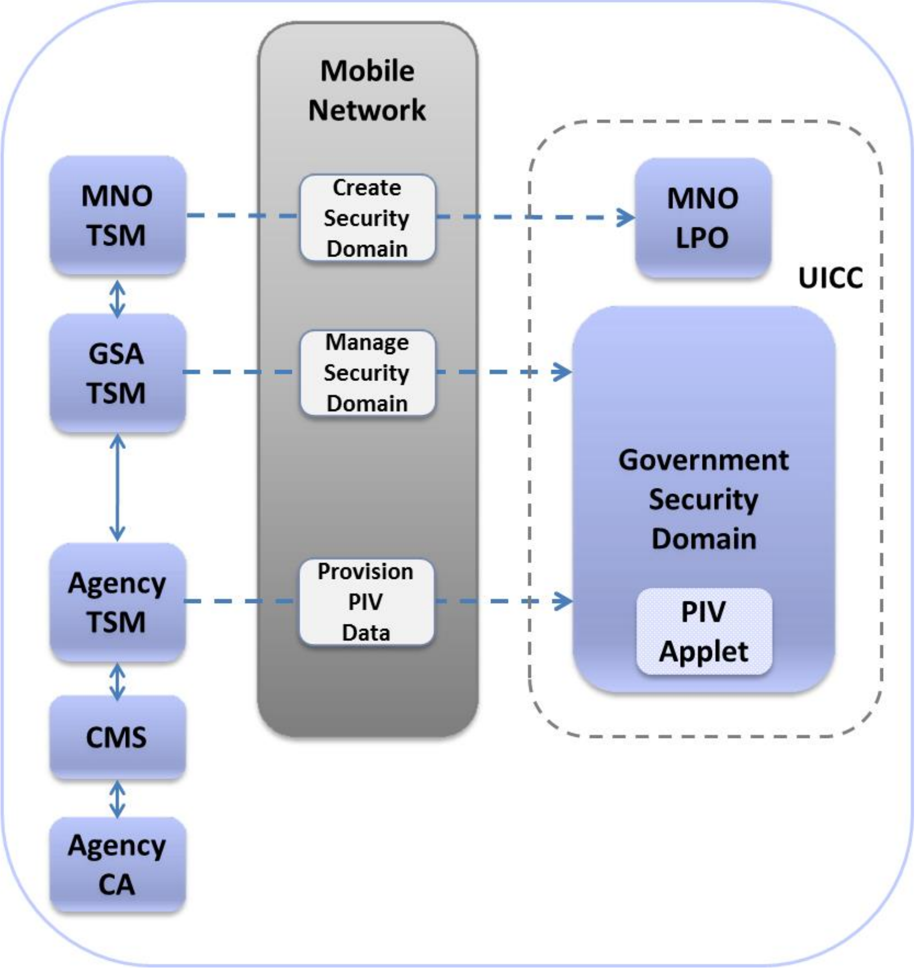
The GSA can then work with every Federal agency to provision a PIV applet within this security domain that is configured to meet that agency's requirements. This can be done on a centralized basis, or it may be delegated to one or more agencies. TSMs, hosted by the GSA or an agency, or contracted out, can manage the provisioning.

This model provides each agency with a PIV applet within the Government Security Domain. The credentials in this applet can be provisioned and managed directly by the Agency. They may also elect to use a managed service for these functions. These credentials are then available for use as described in the use cases in Section 3.

The relevant GlobalPlatform specifications for the UICC were designed to enable this delegated authority model. In this specific example, the U.S. Government with the GSA plays a central role for multiple Federal agencies. The same structure can be used for a large corporation, with a central IT department playing the role of the GSA, and individual divisions in the organization in the role of the agencies. It will also work where an independent organization may need to provide central management for multiple third parties.

In all of these cases, the MNO simply establishes a relationship with one organization and creates a security domain under their control. All of the details and complexity of the usage within that security domain are hidden from the MNO. This structure has business benefits, as it lowers the cost and complexity of managing the different relationships. In addition, it has security benefits to meet requirements for privacy and independent control.

Figure 4. Example of Provisioning and Management Model for PIV Applet on UICC



6 Impacts on Policy and Recommendations

The following U.S. Government policy issues need to be addressed to incorporate and use the PIV credential in the UICC.

- If there is the requirement to expose full PIV cryptographic services over the NFC interface in card emulation mode (e.g., for digital signatures), FIPS 201 would need to allow for cryptographic services over the mobile device's NFC interface. Recommendation: This requirement should be addressed in the FIPS 201-2 definition for the "virtual contact interface."
- The credential to be utilized on the mobile device should be a "derived credential" from the original PKI credential. Policy is needed to define how to create and use derived credentials. NIST SP800-63-1 *Electronic Authentication Guideline*[8] and the upcoming SP800-157 *Guidelines for Personal Identity Verification (PIV) Derived Credentials* are expected to provide further details and the opportunity for industry to make recommendations.
- A policy decision is needed that states what data elements (mandatory and optional) are included in the PIV applet on the mobile phone UICC. The UICC has the ability to support all of the mandatory and optional PIV data elements.
- Government should state policy surrounding security domains (e.g., PIV credential must be in a separate security domain). SP800-157 is expected to be released for public comment shortly. Industry will have an opportunity to make recommendations as required to achieve optimal security.
- In order to provision the PKI credentials remotely to the PIV applet in the UICC over the air, supporting U.S. Government PKI policy must be extended to allow for this mechanism. Methods for securing OTA provisioning need to be considered in defining the policy.
- Several modes are available in the TSM framework for provisioning and managing applets. The government needs to consider the security implications of those modes and provide guidance on possible mode configuration and policy.
- We suggest that agencies address policies for wireless and wirelessly connected smart card readers (e.g., defining the protection that is required over the wireless interface).
- The definition of the card configuration model and interoperability test suite should be considered as a follow-on project with industry actively involved in the definition.
- The GSMA is presently embarking on the definition and specification for enabling PKI credentials on the UICC. This will be an international standard supporting the approach outlined in this paper.

It is important to note the following about cryptographic certifications. In order to be able to supply a high level of assurance, it is expected that the UICC will be required to be certified to FIPS 140-2 for use of government-approved cryptographic services, or an exception will need to be granted to authorize this deployment. With the UICC-based architecture for the PIV credential and application, where all cryptographic services are performed in the UICC, there is no specific requirement for FIPS 140 certification of the handset. This will be consistent with the current trends in the mobile marketplace, and provide handset makers with the agility that they require to continue fast-paced innovation in the space, much like how the use of a PIV card with middleware on a PC only requires that the PIV card have cryptographic certification.

[8] http://csrc.nist.gov/publications/PubsSPs.html

7 Conclusions

Incorporating the PIV credential in the UICC is a cost effective and beneficial solution for the U.S. Government as there are already well-deployed mechanisms to control the content of the UICC over the air. These mechanisms can ensure the secure activation of the credential functionality on the UICC along with its provisioning from the U.S. Government's issuing authority. The UICC-based credential can then be made available through mobile PIV middleware for local mobile applications for a range of use cases (e.g., remote authentication, signature, encryption and decryption of data in transit and at rest).

This innovative approach effectively balances the need for flexibility by handset makers with the need for security to protect government and commercial online identities. This architecture provides an approach that is interoperable with the current PIV infrastructure, leveraging the investment that has already been made.

In order for the approach to work, efforts from several parties are needed. These efforts include the following for the different industry stakeholders.

Mobile Operator(s)

- Assign space in the UICC for a subordinate security domain and applet.
- Determine how to manage the security domain keys with the U.S. Government's TSM platform.
- Utilize the MNO TSM to configure the UICC for PIV.
- Provide a network service via the MNO TSM to the U.S. Government issuing authority's TSM to allow the PIV applet to be securely configured, provisioned and activated directly by the U.S. Government on a UICC.
- Provide network services for remote use of the mobile PIV credential by U.S. Government applications.

UICC Manufacturers

- Design and manufacture FIPS140-2 certified UICC devices for each MNO that support the PIV applet and services. Allow for the PIV applet to be pre-installed at manufacture or to be loaded remotely via collaboration between the MNO TSM and the U.S. Government TSM.

Handset Application Providers

- Modify handset applications to utilize the PIV credential in the UICC (e.g., email and browsers).

Handset Operating System Providers

- Modify handset operating systems to provide an interface (secure element access) to the UICC PIV applet services for handset applications.
- Provide PIV mobile middleware providing abstract PIV cryptographic services to the handset applications.

Middleware Providers (Optional)

- Provide PIV mobile middleware providing abstract PIV cryptographic services to the handset applications

Government Agencies

- Connect the existing PIV management systems (e.g., CMS and PKI) to a U.S. Government TSM(s) and connect to the MNO TSM(s) to securely configure and manage the PIV credential in the Government Security Domain on the UICC.

The technology to support the approach described in this white paper is available today. The Smart Card Alliance invites the government to define clear policy and to identify any potential gaps to move the industry forward for implementing PIV on the UICC.

8 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Identity Council, Mobile and NFC Council and Access Control Council to provide guidance to U.S. Government policy makers and technologists on the key technical, business and policy considerations for supporting the Personal Identity Verification (PIV) application and credentials on mobile devices using the UICC.

Publication of this document by the Smart Card Alliance does not imply endorsement by any of the member organizations of the Alliance.

The Smart Card Alliance thanks the Council members for their contributions. Participants involved in the development of this white paper included: Bell Identification B.V.; Booz Allen Hamilton; CH2M HILL; Deloitte & Touche LLP; Gemalto; General Services Administration (GSA); HID Global; Identification Technology Partners; IDmachines; Intercede Ltd; IQ Devices; NXP Semiconductors; Oberthur Technologies; SafeNet, Inc.; SAIC; SecureKey Technologies; XTec, Incorporated.

The Smart Card Alliance thanks **Neville Pattinson** (Gemalto) and **James McLaughlin** (Gemalto) for developing the first draft of the white paper, and **Peter Cattaneo** (Intercede), **Frazier Evans** (Booz Allen Hamilton), **Philip Hoyer** (HID Global), **Bryan Ichikawa** (Deloitte & Touche) and **Chris Williams** (SAIC) for contributing content to the white paper during the review process.

The Smart Card Alliance thanks the following Council members who participated in the development and review of this document:

- **Mike Ash**, SAIC
- **Rene Bastien**, SecureKey Technologies
- **Peter Cattaneo**, Intercede Ltd
- **Stu Cox**, Oberthur Technologies
- **Sal D'Agostino**, IDmachines
- **Doug Deckert**, CH2M HILL
- **John Esser**, Oberthur Technologies
- **Frazier Evans**, Booz Allen Hamilton
- **Todd Freyman**, Bell Identification B.V.
- **David Helbock**, XTec, Incorporated
- **Philip Hoyer**, HID Global
- **Bryan Ichikawa**, Deloitte & Touche LLP
- **Gurpreet Manes**, SafeNet, Inc.
- **James McLaughlin**, Gemalto
- **Cathy Medich**, Smart Card Alliance
- **Neville Pattinson**, Gemalto
- **Raj Pillai**, GSA
- **Steve Rogers**, IQ Devices
- **Brian Stein**, CH2M HILL
- **Lars Suneborn**, Oberthur Technologies
- **Chris Williams**, SAIC
- **Mike Zercher**, NXP Semiconductors
- **Rob Zivney**, ID Technology Partners

About the Identity Council

The Identity Council is focused on promoting best policies and practices concerning person and machine identity, including strong authentication and appropriate authorization across different use cases. Through its activities, the Council encourages the use of digital identities that provide strong authentication across assurance environments through smart credentials—e.g., smart ID cards, mobile devices, enhanced driver's licenses, and other tokens. The Council furthermore encourages the use of smart credentials, secure network protocols, and cryptographic standards in support of digital identities and strong authentication on the Internet.

The Council addresses the challenges of securing identity and develops guidance for organizations so that they can realize the benefits that secure identity delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organizational resources to bear on addressing the challenges of securing identity information for proper use.

Additional information on the use of smart card technology for identity applications can be found on the Smart Card Alliance Web site at http://www.smartcardalliance.org.

About the Mobile and NFC Council

The Smart Card Alliance Mobile and NFC Council was formed to raise awareness and accelerate the adoption of payments, loyalty, marketing, promotion/coupons/offers, peer-to-peer, identity, and access control applications using NFC. The Council focuses on activities that will help to accelerate the practical application of the technology, providing a bridge between technology development/specification and the applications that can deliver business benefits to industry stakeholders.

The Council takes a broad industry view and brings together industry stakeholders in the different vertical markets that can benefit from mobile and NFC applications. The Council collaborates on: educating the market on the technology and the value of mobile and NFC applications; developing best practices for implementation; and working on identifying and overcoming issues inhibiting the industry.

About the Access Control Council

The Smart Card Alliance Access Control Council is focused on accelerating the widespread acceptance, use, and application of smart card technology for physical and logical access control. The group brings together, in an open forum, leading users and technologists from both the public and private sectors and works on activities that are important to the access control community and that will help expand smart card technology adoption in this important market.

9 Appendix A: Acronyms

BYOD	Bring Your Own Device
CMS	Card Management System
FIPS	Federal Information Processing Standard
GSA	General Services Administration
MNO	Mobile Network Operator
NFC	Near Field Communication
OOB	Out of Band
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
TSM	Trusted Security Manager
UI	User Interface
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
VPN	Virtual Private Network