GlobalPlatform®
The Standard for Managing Applications on Secure Chip Technology

The GlobalPlatform Value Proposition for Identity Management

White Paper
November 2007

secretariat@globalplatform.org | www.globalplatform.org

Contents

About GlobalPlatform

GlobalPlatform is a member driven organization with worldwide cross-industry representation. GlobalPlatform is the leading, international association, focused on establishing and maintaining interoperable specifications for single and multiple application smart cards, acceptance devices and systems infrastructure that deliver benefits to issuers, service providers and technology suppliers. These specifications are known as *the* standard for smart card infrastructure, thanks to their balance of technical superiority and business justification.

GlobalPlatform Specifications are freely available and have been adopted in Europe, the Americas, Asia and Australia by many public and private bodies.

For further information, visit www.globalplatform.org

Publication Acknowledgements

GlobalPlatform wishes to offer special thanks to the members of the Government White Paper Task Force, and their respective organizations, for their contributions and involvement in developing this White Paper.

Participants included:

Rien de Grijp - ACI Worldwide Inc.
Pieter Hoogendoorn - ACI Worldwide Inc.
Eric Le Saint - ActivIdentity
Gil Bernabeu - Gemalto
David Asay - IBM Global Business Services
Ian Hermon – Thales e-Security
Lynne Prince - U.S. Department of Defense / Defense Manpower Data Center

With special thanks to the GlobalPlatform Marketing Secretariat for managing the development of this White Paper.

Phil Davidson - GlobalPlatform
Kevin Gillick - GlobalPlatform
Ayse Korgav - GlobalPlatform

Executive Summary

The need has never been greater for governments worldwide to implement secure and robust identity (ID) management programs in order to control access to their physical and logical property and ultimately ensure the safety of staff and their own establishment. With countless solutions deployed in today's marketplace and new products introduced every year, however, the challenge is not finding a technology to help manage identities and secure data, but how to select a solution that is flexible, secure, cost-effective, scalable and standardized, yet which offers a minimum level of risk.

This White Paper aims to explain the value of implementing a government ID smart card program which is based on the GlobalPlatform Specifications. Many governments worldwide have already realized the benefits of deploying GlobalPlatform technology in their ID programs. Current known implementations, at the time of this White Paper's publication, include: Austrian Citizen Card, BioPass (Singapore Biometric Passport), CNS Italy, Daejeon Project (South Korea), Hong Kong National ID Card, Kingdom of Belgium ICAO e-Passport, Macau Special Administrative Region Project, Moroccan National ID Card, Polish Transport Authority Project, Qatari National ID Card, Saudi Arabia's King Fahd University ID Card, Sultanate of Oman National ID Card, Taiwan National Health Insurance Card and US Government Agency initiatives from the Department of Defense, the General Service Administration and the Transportation Security Administration.

For ease of reference, this document focuses solely on one widely recognized use-case of GlobalPlatform technology – the United States Department of Defense (DoD) Common Access Card (CAC) - and also uses the widely recognized Personal Identification Verification (PIV) standard as an example ID management framework. The case study illustrates how the GlobalPlatform Specifications can be applied across the entire smart card infrastructure to benefit the issuance and management of smart ID cards and applications in a government program. It is intended that other use-cases, originating from Europe and Asia-Pacific, will be developed and explored in future editions of this White Paper series.

This document provides a detailed overview of how and where GlobalPlatform technology is applied across an ID management program and to what effect. GlobalPlatform's impact relative to the ID card itself and different roles within a card management system are explored, and the role that GlobalPlatform plays in facilitating interfaces and data exchange between different actors in an ID management program is also outlined.

For the purpose of clarity from the outset, it is important to note that GlobalPlatform technology offers an approach to deploying smart cards and card management. It does not address the entire ID management program framework.

This White Paper is intended to be informational rather than technical in nature. This allows it to be accessible to government officials, project managers and consultants advising on the implementation of smart card based ID programs in government, in addition to more technical audiences.

Section 1: The Concept of Identity Management

There was a time when to secure a loan or join a club, a person required a sponsor. It was a banker, attorney, preacher, or someone of similar reputable standing who vouched for the person by confirming their identity (ID). Even without using smart cards, ID management systems essentially provide the same services - they establish trusted identities and securely link credentials to people using tokens.

The ID management model no longer requires a one-on-one introduction from a trusted person to enter a physical space or access a web site. Rather, the trusted ID carried on securely issued tokens empowers the credential holder. This person can use their credential to move across networks, use web applications and enter doors, gates and buildings. Simultaneously, organizations protect themselves from unauthorized access.

Figure 1 introduces a reference model of ID management, which will be used throughout this White Paper to describe the impact of smart card technology in general and to explain how the GlobalPlatform Specifications ensure an open and future-proof approach. Figure 1 depicts the situation before the introduction of smart cards:

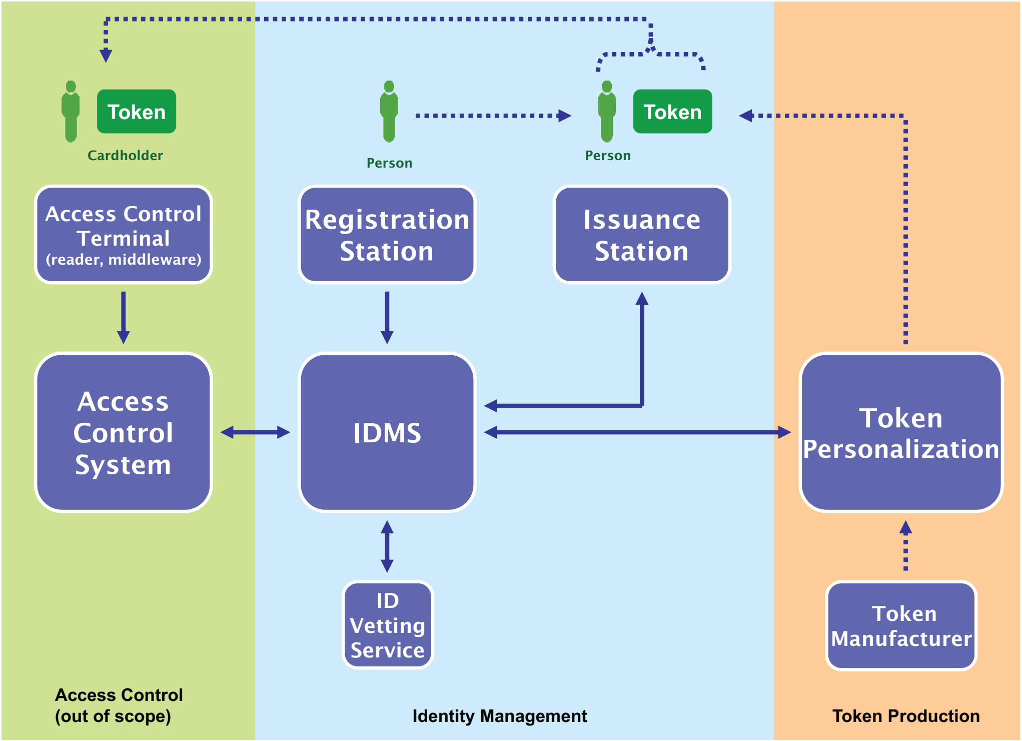


Figure 1 – Identity management overview

The secure and accurate control of access privileges (Access Control - the area shown on the left (green) in Figure 1) is the primary objective of ID management. People may be granted access to facilities or infrastructures/services when their credentials have been authenticated and they have proven to be the rightful carrier of the token, for instance by entering a PIN. The Access Control System may subsequently contact the Identity Management System (IDMS) to ensure that the presented credentials have not been revoked. As this White Paper does not discuss card reading equipment characteristics in any detail, however, the area depicted in Figure 1 as 'Access Control' is outside the scope of this document.

The middle (blue) area of the diagram, which represents ID Management, comprises all of the facilities required to actually issue and manage identities and credentials. During the first stage of enrolment on an ID scheme a person must present documents to establish his/her proper ID. Those documents must be presented to a registration station and ID vetting may occur either before or during the enrolment process. Here ID information is validated and the right of the person to obtain ID credentials is established. It is imperative that registration and ID vetting processes are performed by different people or organizations. At the issuance station, tokens will be issued in a secure way in order to make sure the ID credential can be accepted as a representation of an ID later on.

The IDMS is a core component of any ID infrastructure. The IDMS usually conjoins multiple databases that contain various ID elements. It controls the enrolment/registration process — including credential vetting — and initiates document production. It may schedule personal appointments for enrolment and issuance stations. After issuance, the IDMS plays a role in the online authentication of credentials, e.g. for building access, border control or e-government services. During its life cycle, the token may require updating, revocation or replacement, so the IDMS must also be capable of addressing these requirements as necessary.

Finally, the right (orange) area of the diagram, which represents Token Production, is concerned with the actual token production and personalization processes. These tasks can be done in central secure facilities, from where personalized tokens are shipped to issuance stations for collection, or in a distributed fashion close to the issuance stations. In all cases, production and personalization must be highly secure and stocks of blank cards must be protected from misuse.

Introducing Smart Cards to Identity Management

The key aim of this White Paper is to educate on the capabilities and benefits offered by smart cards and smart card management systems when deployed in government ID management programs. While much of this document focuses on ID management concepts and issues, this information is provided as a context for explaining the value that a smart card based solution – specifically a smart card solution based on GlobalPlatform's open technology – can bring to issuers of government ID management programs. For the purpose of clarification it has to be made clear that GlobalPlatform offers an approach to deploying cards and card management, not ID management.

Just like many smart ID cards today, including driving licenses and health cards, a smart government ID card body often has additional features such as text, Machine Readable Zone (MRZ) lines, a bar code and a photo. In the case of a government credential, however, standard graphical personalization is combined with highly secured printing such as Changeable/Multiple Laser Image (CLI/MLI), micro perforation for text and images, a hologram and UV color personalization, designed in a way to offer an overt and covert means of determining authenticity of the credential. The embedded chip, however, constitutes a new element which may contain a wealth of applications and data, optionally originating from different authorities. This is the value that multi-application smart cards bring to a government ID program. The information on the chip is securely stored and not retrievable without the express permission of the cardholder. Additionally, the smart card can authenticate users with a high degree of fidelity, allowing them to digitally sign documents, ensuring non-repudiation. The use of a chip, however, does necessitate vital changes to an ID management program. Token production is a key illustration of this.

Token production was traditionally seen as the subject of printing technology and key concerns were for security paper, holograms, and lamination. In the case of smart cards, however, more sophisticated programming and cryptographic processes are required to personalize the chip. It is a mistake to view chip personalization as simply an extension of the printing process. This results in the mistaken focus on the brief period during which the token is produced and ignores the need to manage the chip and its data during the entire life cycle of the token. Additionally, enhancing the IDMS to perform these new processes can result in a highly complex project, as more and more features may impact the upgrade.

So, what starts out as a simple extension to personalize chips can quickly expand to encompass all other aspects of the life cycle of the chip and its data. To avoid this situation, the following approach is recommended:

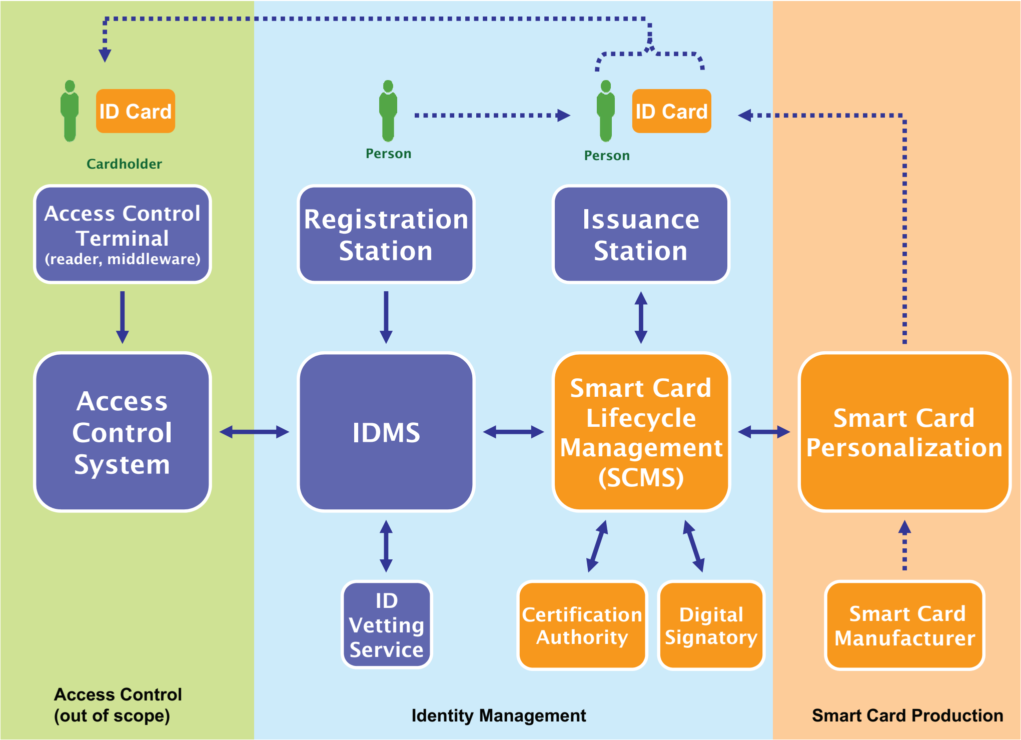


Figure 2 – Smart card enhancements (orange) to identity management

To implement the new smart card technology with minimal impact to the existing environment, a Smart Card Management System (SCMS) is necessary. The SCMS encapsulates important aspects of the life cycle of a smart card, such as data encryption, key generation and key management and allows most of the smart card specific processes to be isolated from existing systems. For instance, the IDMS is responsible for the life cycle events of the cardholder, and may continue to send token renewal/replacement requests to the SCMS as if little has changed. Triggered by the IDMS requests, the SCMS will interface with the certificate authorities, personalization bureaus and other external institutions to drive smart card issuance and post-issuance updating. When properly implemented, the personalization of a smart card can be securely outsourced to either a central facility or local (distributed) issuance bureaus or stations.

Besides the addition of an SCMS, other areas in Figure 2 may need to be upgraded to ensure that they do not become a weak link in the security chain. For instance, biometrics data may be captured at the registration desk for later inclusion on the smart card and two factor authentication may be used to ensure the person collecting the card at the issuance station is the same person who enrolled at the registration desk. Two factor authentication is a means of identification based on more than one criteria, e.g. something you have (card) and something you know (PIN). Though these critical ID management elements are imperative for a secure ID program, they are outside the scope of GlobalPlatform systems. Both ID management and GlobalPlatform systems are required to build a strong government smart card based ID scheme.

The model of ID management outlined in this section is more clearly illustrated in Section 2 by one concrete example of GlobalPlatform technology deployed in a government ID program: the U.S. Department of Defense's (DoD) Common Access Card (CAC). In addition to providing some background information on the CAC, this section will also examine the impact of smart card technology on different functions of the CAC ID management program and explain how GlobalPlatform technology facilitates and benefits the CAC implementation.

Section 2: Case Study - U.S. Department of Defense (DoD) Common Access Card

At this juncture, it is considered beneficial to showcase a successful ID management solution which uses smart cards. The U.S. Department of Defense's (DoD) Common Access Card (CAC) is the flagship model of a government smart card solution for ID management and in this section all the processes from pre-issuance to post-issuance of the ID token will be explored.

Upon reading this case study, readers may note the complexity of electronic ID schemes and how a smart card facilitates rapid authentication for both logical and physical access.

The U.S. DoD Identity Management Concept

The U.S. DoD has always had an obligation to provide an ID token to its Uniformed Service personnel and their family members. As such, the DoD ID Management Program was initiated in the early 1900s when the basic ID card was the primary form used for ID management. In the mid 1980s, the initial and current DoD ID repository, The Defense Enrolment Eligibility Reporting System (DEERS), was established and used to consolidate identities and ID cards into one database.

The DoD ID card, as it was then, served as a token of affiliation to the DoD. Additionally, for those military members serving overseas, the U.S. DoD ID card was also accepted as a Geneva Convention Card. For family members, the U.S. DoD ID card identified privileges such as commissary, medical care, recreational facilities or exchange access.

In 1999, however, the Deputy Secretary of Defense mandated a new technology for DoD ID cards. The new technology was a smart card called the Common Access Card (CAC). The smart card was considered to provide greater security against fraud tampering and counterfeiting and provided better privacy protection for the cardholder. The first CAC was issued in 2001, resulting in the DoD becoming the first U.S. Government Agency to develop an ID smart card.

The Common Access Card (CAC)

Today, the CAC is a smart card that serves as the DoD standard identification and logical access credential. It may also be used for physical access to DoD facilities. In addition to retaining the key functions of the traditional ID card it replaces - serving as an ID and privileges card and a Geneva Convention Card - the CAC is additionally used for secure authentication and network access, enabling users to securely log on to their computer, decrypt email and digitally sign documents. The CAC increases security for unclassified networks and allows the undertaking of secure transactions over the internet.

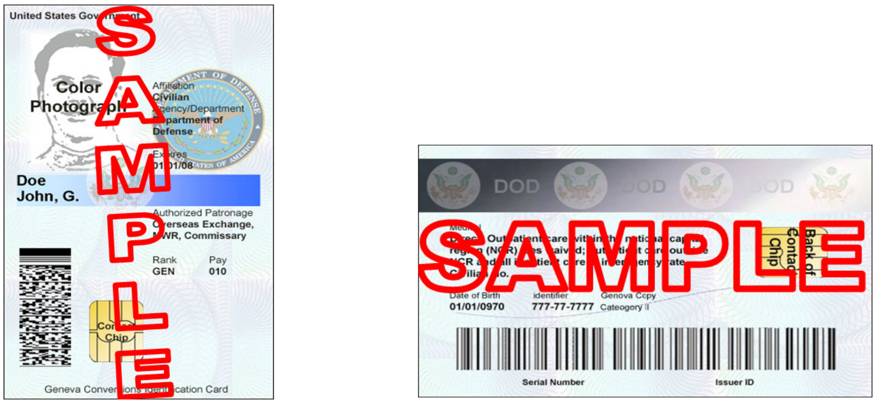
The CAC conforms to the following standards:

- Federal Information Processing Standards (FIPS) 201 – a U.S. Government standard related to the Personal Identity Verification of Federal Employees and Contractors.
- FIPS 140-2 – a U.S. Government computer security standard which specifies requirements for cryptography modules.
- ISO 7816 – an international standard related to electronic identification cards.

All members of the Uniformed Services (Active Duty, Reserves and National Guard), receive a CAC, as do DoD civilians, eligible contractors and DoD affiliated organizational members. The look of a DoD ID card is unified by external features including a digital photograph, bar codes, a magnetic strip and a contactless interface. While these features facilitate proper recognition of military, civilian and appropriate DoD contractors worldwide, the real value proposition is in the chip. The secure data on the chip enables the rapid electronic authentication which both the DoD, and the Homeland Security Presidential Directive (HSPD)-12, mandate. The CAC chip contains:

- DoD PKI certificates
- Two digital fingerprints
- Digital photo
- Personal Identity Verification (PIV) Authentication Certificate
  - U.S. Federal Government
- DoD organizational affiliation
- DoD agency code
- DoD department code

- CAC expiration date
- Cardholder unique identifier
    - available through both a contact and contactless interface



(Front of CAC)

(Back of CAC)

Figure 3 – Layout of the Common Access Card (CAC)

Highlighting the complexity of CAC issuance, there are 2000+ issuance stations worldwide and a central issuance facility which issues cards to all military recruits. Post-issuance facilities, for updating CACs, are made available at users' desktops and facility kiosks.

In the second quarter of 2007, 11 million CACs had been issued since the start of the program, and 3.3 million active cards were in circulation. The DoD's daily CAC issuance rate was 10,000 cards per day, with an annual sustainment rate of 2.2 million cards.

Testifying to the success of the CAC program, the January 25, 2007, issue of Federal Computer Weekly, referred to the CAC as 'the gold standard for rapid electronic identity authentication, online security and physical access'. The article continued by highlighting that the CAC is now actively being used by over 91% of DoD users who require logical access, as only people authenticated via their CAC are authorized logical access to DoD networks and web services. The result is that successful intrusions of DoD networks declined by over 46% between 2006 and 2007.

Evolving DoD Systems to Support CAC

This section follows the ID management life cycle of a DoD person applying for a CAC and the life cycle of the CAC itself, from registration to termination.

The ID management life cycle of a DoD person begins when they register with a DoD Human Resources (HR) System. The ID of all DoD military personnel or civilians is logged within DEERS, the central IDMS repository, together with details of their personal CAC and Public Key Infrastructure (PKI) certificates. When that person leaves or resigns from the DoD, their personal ID remains in DEERS but is marked as inactive. The CAC is terminated and their PKI certificates are revoked.

Figure 4, below, illustrates the central role of DEERS in the issuance, authentication and access processes relative to CAC:

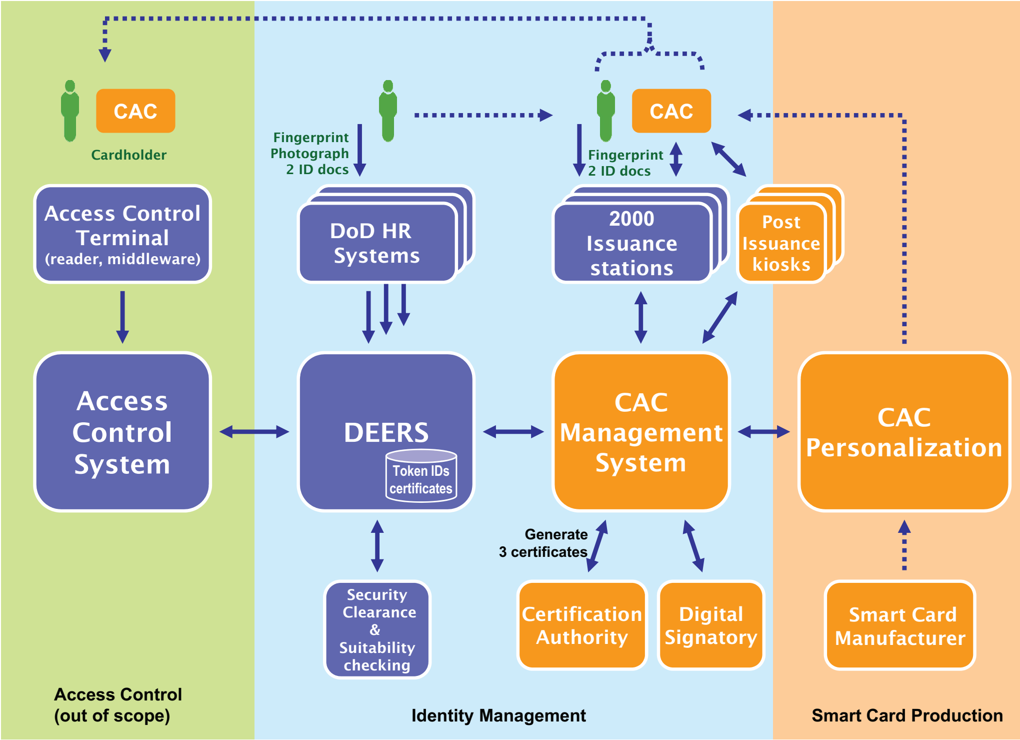


Figure 4 - A conceptual overview of the Common Access Card (CAC) system concept

As already outlined, the CAC, using the PKI keys generated by the chip, allows DoD cardholders secure logical access to DoD networks and protects DoD facilities from unauthorized physical access. The U.S. DoD CAC program therefore relies heavily on the fundamentals of a secure and robust ID management program.

So how is security maintained throughout the CAC ID management and smart card production stages (middle and right (blue and orange) sections in Figure 4) and how does the program benefit from smart card technology and GlobalPlatform's Specifications?

Stage 1) Cardholder Registration

People working for the DoD are registered to a DoD Human Resource system. At the time of enrolment, a person's fingerprints are captured and matched to the FBI master fingerprint database. Additionally, a photograph is taken and a personal background investigation or security check is initiated. To validate the ID of the person, the prospective DoD employee must provide two forms of acceptable ID documents. At least one of these documents must be a federally issued credential and contain a photograph. The documents are scanned into DEERS and in some instances, validated for authenticity.

Since the DoD is a large organization consisting of many components (Army, Navy, Marine Corps, Air Force and DoD Agencies, plus the National Atmospheric and Oceanic Agency, Public Health Service and the Coast Guard), it is imperative that each DoD Human Resource system feeds this information, taken at the time of enrolment, back to DEERS.

Stage 2) CAC Issuance

Once enrolment and the security check are completed, the person is eligible for an ID token. If the person requires logical and/or physical access to DoD networks and facilities, then they are eligible for a CAC. If no logical access is required but the person is entitled to DoD privileges, then an alternate plastic ID token is issued. The CAC issuance system is separate and distinct from the registration system. The separation of agents performing these tasks acts as a check and balance to fallacious enrolment or issuance of a DoD credential.

For the CAC issuance, a choice of centralized or decentralized model is available (see section 3 – Card Issuance Processes). At the local issuance station, the person once again provides two forms of ID documents. These documents may be the same documents presented at enrolment, in which case they can be validated against the previously captured documents. To ensure the person who registered is the same person receiving a CAC, a fingerprint is captured and checked against the DEERS database. Assuming a fingerprint match, the verifying official issues a CAC, loading the personal identification information, creating PKI certificates for rapid electronic authentication and establishing any privileges entitled to the new cardholder. The CAC itself and the new PKI certificates are also registered in DEERS.

The CAC is limited to a three year life cycle and renewal depends on the cardholder's ongoing affiliation with the DoD. As long as the person is still working with the DoD or affiliated to someone employed by the DoD after this time period, then a new ID card will be reissued. At renewal, the old PKI certificates and token instance are cancelled and new ones are registered.

Stage 3) Managing the CAC Life Cycle

The CAC Management System (the SCMS) controls the CAC life cycle from pre-issuance to termination. It is within the context of this management system that the benefits of deploying GlobalPlatform technology within the CAC program can be seen.

The stages of a CAC life cycle are as follows:

Pre-Issuance – At the pre-issuance stage of the card life cycle, the CAC management system co-ordinates the pre-initialization and delivery of CAC batches from various card manufacturers responsible for providing CACs to the DoD issuance stations. The DoD Pre-Issuance Requirements Specification describes the standard practices in key management between a card manufacturer and a card issuer (the DoD) and these standard practices follow many of the precepts outlined in GlobalPlatform's Messaging Configuration for PIV version 1.0. The DoD uses an inventory tracking system to monitor and replenish CAC stock at its issuing sites.

Issuance – During the issuance phase, there are automated safeguards to ensure that only those cards accepted by the DoD issuance site can be issued by that site. This occurs in three ways:

- The card stock number is identified to an issuance site when the issuing agent accepts card inventory.
- A specific DoD key embedded on the CAC is recognized by the issuing system so that only those cards with specific DoD keys can be referenced by the issuance system.
- The CAC information, smart card token numbers and status of the CAC (ready to be issued, terminated, destroyed) are stored in the CAC Management System.

The CAC smart card issuance system utilizes GlobalPlatform secure issuance processes to install applications and load certificates and personal information on the chip.

Post-Issuance – In the CAC program, the DoD uses a GlobalPlatform enabled capability to update the CAC after it has been issued to the cardholder. This allows replacement smart card log-on certificates, email encryption certificates and new applets to be downloaded onto a CAC from the cardholder desktop or a secure kiosk. The same GlobalPlatform Secure Channel loading mechanisms used in the issuance phase are used post-issuance to ensure the protected transmission of data.

Termination – At the termination stage, the CAC is collected and marked for deletion in the inventory system. The token is then sent to a destruction site where it is logged into the inventory system and a match marks the card as terminated. Expired cards which are not returned follow the same termination process as if they had been physically returned. All PKI certificates on CACs whether expired, lost, stolen or returned, are sent to the certificate authority for revocation.

In summary, the U.S. DoD is reliant on smart card – specifically GlobalPlatform - technology throughout its ID management and smart card production processes, to facilitate processes and exchanges, maintain security and integrity and generally aid in the management of the CAC life cycle. To produce, issue and manage the CAC, the program utilizes the secure messaging mechanisms of GlobalPlatform for exchanging key materials with card manufacturers. It also uses the GlobalPlatform Secure Channel for personalizing the PKI certificates, biometrics and demographic data on the CAC. How these and other GlobalPlatform mechanisms underlie successful ID management programs is explained in subsequent chapters.

The following section presents the smart card and considerations when using smart cards as ID tokens in a model government ID management program. An explanation of how GlobalPlatform technology can be leveraged to ensure program objectives are met in a highly specified and uniform manner is also provided.

Section 3: What GlobalPlatform Offers the ID Card

It is important to note that there are a range of technology options available when building a government ID management program which uses smart card tokens. This paper explores a comprehensive smart card technology example which is modeled on the U.S. Government's recently instituted Personal Identity Verification (PIV) concept.

This section focuses on the smart ID card, which should be recognized as a central but single component of a larger ID management system. A number of considerations must be taken into account when introducing a smart card into an ID management system. Here these issues are explored and an explanation of how GlobalPlatform technology addresses them is provided. In Section 4, the paper examines the impact of GlobalPlatform technology on the various roles and actors in an ID management program, using the PIV model as an example.

In the interests of clarity, it is once again highlighted that GlobalPlatform's remit is to deliver an approach to the deployment of smart cards and card management systems within a government ID management program, regardless of business decisions taken. All references made to roles and processes outside of GlobalPlatform's scope within this section are for the purpose of scene-setting only.

Personalizing Chips and Managing Applications – Vendor (In)Dependence

Having made a decision to base an ID management system on smart card technology, the government agency issuing ID cards is presented with an opportunity to optimize this technology. At an early stage, key business decisions have to be made regarding the card's functionality. For example, will an e-purse application be required now or in the future? Will the ID card allow users to authenticate themselves for physical or logical access or to digitally sign documents?

In the case of the CAC, the DoD specified the card to be utilized for network access, physical access to DoD facilities, authentication, secure log-on, email encryption and digital signatures. Smart cards and GlobalPlatform technology were used by the DoD, as both can be implemented regardless of the business decisions that are taken. Smart cards based on GlobalPlatform technology also offer the flexibility to accommodate decisions which may arise in the future, such as for example, the decision to move card management based on symmetric (secret key) keys to asymmetric (public key) keys or the decision to move from a centralized to a decentralized model.

Technology options presented for the development of a smart card based ID program range from proprietary to open and interoperable solutions. A large number of proprietary chip operating systems have been implemented by smart card vendors. These create challenges for issuers who want to pick and choose their cards from a number of vendors. For example, the processes to personalize the chip may differ significantly between proprietary platforms, creating a problem for an issuer who needs to port their on-chip applications. These process differences also apply to security concepts and application management facilities.

Conversely, a common interoperable application management interface for ID card applications, as chosen by the DoD, promotes vendor independence by allowing card production and issuance systems from different manufacturers to personalize ID cards in a similar manner. This means a card issuer with access to different personalization devices need not have a vastly different approach to the issuance process. Moreover, uniform and well defined card and application management security policies and interoperable management use-cases enable card management interoperability. This concept is presented in Figure 5:

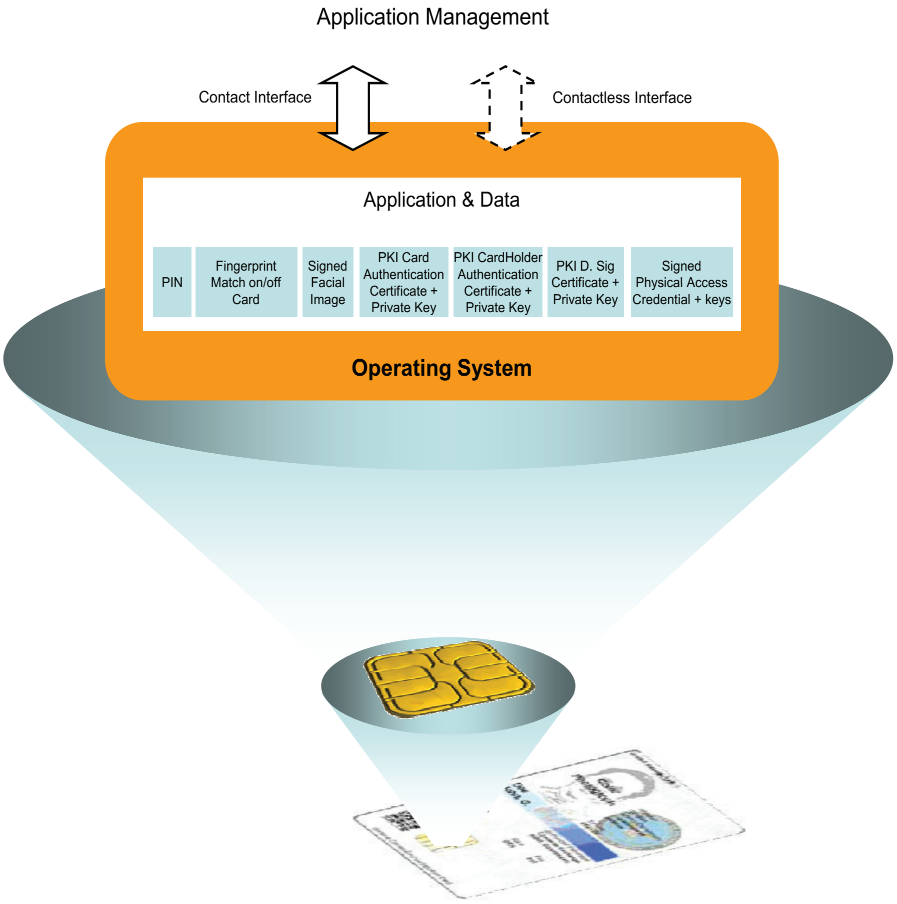

Application Management
Contact Interface
Contactless Interface
Application & Data
PIN
Fingerprint Match on/off Card
Signed Facial Image
PKI Card Authentication Certificate + Private Key
PKI CardHolder Authentication Certificate + Private Key
PKI D. Sig Certificate + Private Key
Signed Physical Access Credential + keys
Operating System

Figure 5 – Card issuers need a uniform mechanism to load, update and delete applications on the chip

GlobalPlatform's Card Specifications offer a standard, generic application management interface for cards. Using GlobalPlatform, the card issuer can leverage and benefit from the security features and the standardized approach to card and application administration interfaces. Additionally, the issuer (government) is able to accept bids from multiple card manufacturers, which reduces cost without compromising on quality. The GlobalPlatform framework is currently supported in two Operating System environments, Java Card™ and MULTOS™. GlobalPlatform ensures transparency between the two platforms in terms of application management, even if an application developed for one platform can not be used on the other.

Alternatively, if the card issuer chooses to issue cards using a proprietary operating system, they can still realize benefits by incorporating GlobalPlatform technology and specifications at the systems level. Due to GlobalPlatform technology being modular in nature, the issuer is able to pick and choose which, if any, parts of the GlobalPlatform technology infrastructure they want to implement e.g. the Profile and Scripting Specifications or the Messaging Specification. In this particular PIV implementation example, the GlobalPlatform Messaging Specification has been extended to support the necessary messaging interfaces specified in a Service Provider environment for secure ID card issuance.

A Card With More Than One Application

In order to save costs and provide added value, the government agency as the card issuer can extend the smart card capability to include multiple applications on a single ID card. Additional applications could include a payment application or electronic purse, an e-passport, or other authorized applications that meet the business needs of the issuer and/or the lifestyle needs of the cardholder.

If this is the case, these applications can be located in a secure area of the card called a Security Domain. Security Domains act as the on-card representatives of off-card authorities and enforce the security policies defined by the owner. To access a secure area the issuer uses a secure connection called a Secure Channel. Once a connection is established, the Secure Channel provides an end-to-end secure communication path between an on-card security domain and an off-card entity.

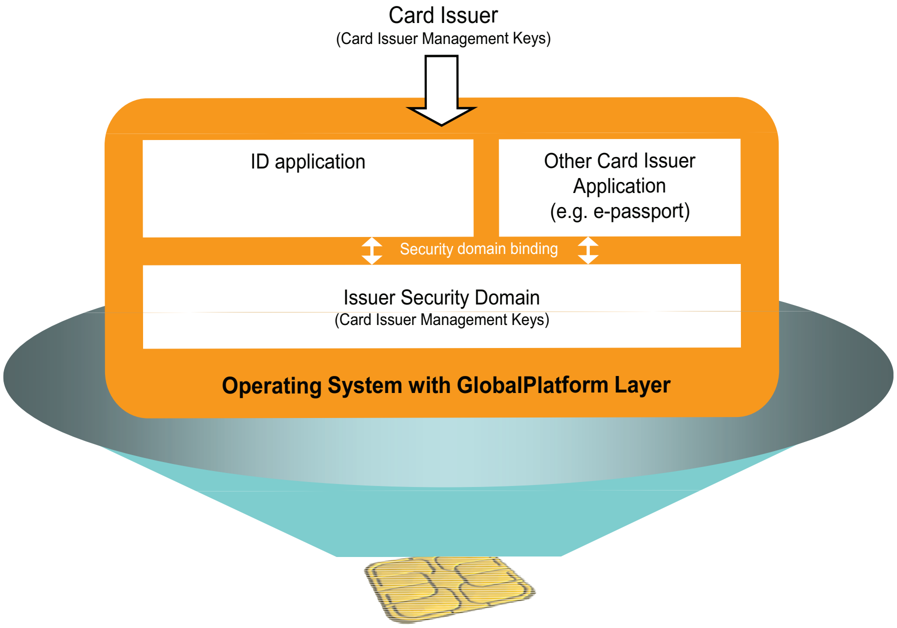

Card Issuer
(Card Issuer Management Keys)
ID application
Other Card Issuer Application (e.g. e-passport)
Security domain binding
Issuer Security Domain
(Card Issuer Management Keys)
Operating System with GlobalPlatform Layer

Figure 6 – GlobalPlatform has defined a standardized mechanism by which issuers own a Security Domain, providing them with a Secure Channel to manage applications on the chip

The issuer can decide to add an application from a business partner called an application provider. In this case the separation of responsibility (who owns and controls the application or who owns and controls the platform, for example) is necessary. The role of card issuer and application provider are quite distinct, and if the card platform provides facilities to keep these responsibilities separate, then application providers may put their applications on the card platform without inflicting vulnerabilities to the card issuer or other application issuers. This is illustrated in Figure 7:

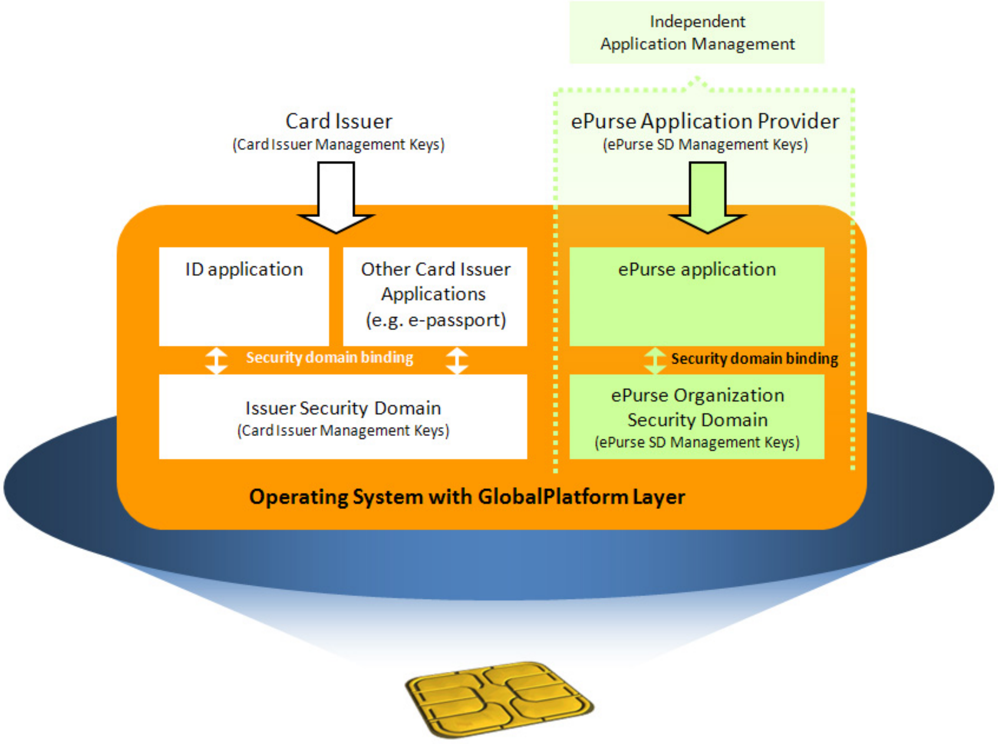

Independent
Application Management
Card Issuer
(Card Issuer Management Keys)
ePurse Application Provider
(ePurse SD Management Keys)
ID application
Other Card Issuer Applications (e.g. e-passport)
ePurse application
Security domain binding
Security domain binding
Issuer Security Domain
(Card Issuer Management Keys)
ePurse Organization Security Domain
(ePurse SD Management Keys)
Operating System with GlobalPlatform Layer

Figure 7 – GlobalPlatform offers the issuer a means to give application providers their own Security Domains on the chip, while assuring that applications, application data and application management remain totally separate

The GlobalPlatform Specifications are well suited for this type of multiple actor deployment. A card platform that abides by GlobalPlatform's Card Specifications allows an issuer to authorize an application provider to exclusively and independently occupy a Security Domain within the card, while enabling the issuer to retain control over the card and its own applications in a secure and standardized manner.

With a Secure Channel to their own Security Domain, application providers can now load, personalize and update their applications, or even operate the application services they control on the card, while meeting the necessary standards and regulation for privacy and security. GlobalPlatform's Card Specifications support symmetric and asymmetric keys and either can be used by the issuer to access a secure area and open a Secure Channel for card management. A Secure Channel can use a synchronous or asynchronous mechanism to allow the card and application providers to authenticate and transfer secure information to the Security Domain.

There is often a requirement to load new applications onto existing cards which have already been deployed, as this saves reissuing cards. GlobalPlatform supports post-issuance download in a very natural way; the application loading and activation mechanisms defined by GlobalPlatform do not make a distinction between pre and post-issuance loading as the mechanisms and Secure Channels are identical. An example is offered by the DoD CAC: cards issued by the DoD have incrementally supported additional services provided by several independent organizations within the DoD.

ID Card Security Considerations

There are a number of requirements which must be met before an ID card can be securely issued and deployed:

- The quality and integrity of the ID card software and hardware components must be ensured.
- The integrity and confidentiality of ID data must be ensured, so as to meet/exceed the control, policy and privacy requirements of the issuer.
- Proper controls over secure and trusted handling of all cryptographic keys, including card Security Domain key sets, exchange or transport keys and ID application keys must be ensured.

To satisfy these requirements, the system, infrastructure and component design must be aligned with the issuer's security policies. A well-controlled development and deployment process, that controls the life cycle of each component and securely safeguards sensitive information, is also needed.

GlobalPlatform's Card Specifications provide on-card security features, verified by the Security Domain, to reinforce the policy defined by the issuer and application providers. Such a policy could contain requirements for:

- End-to-end confidentiality and protection for the transport of data sent to an application from the application provider i.e. Secure Channel protocols.
- A mechanism to verify that the application code is authentic during the load i.e. Data Authentication Pattern (DAP).
- A cryptographic signature provided by a card issuer as proof that a card content modification (load, install…) has been pre approved by the issuer i.e. management tokens.
- Parameters to further card memory management and allow memory reservation.
- Services to provide a mechanism for a Cardholder Verification Method (CVM), including velocity checking, that may be used by all applications on the card.

GlobalPlatform's Systems Specifications are designed to support both the card features and the main requirements of an ID management system. GlobalPlatform's Systems Specifications provide the issuer and systems integrator with guidance and standards for back office development. For the purpose of clarification, 'back office' refers specifically to the smart card management system - the system that manages the card. Conversely, 'front end' systems are systems which have a direct connection with the smart card user (e.g. registration, issuance etc).

The Smart ID Card Life Cycle

A smart ID card may go through various states during its life. But in the case of a smart ID card, it is the card itself rather than items in a central database which enforces what the card can do during a specific phase of its life cycle. Although smart cards come in many (proprietary) technologies, in general they share the life cycle stages depicted in Figure 8.

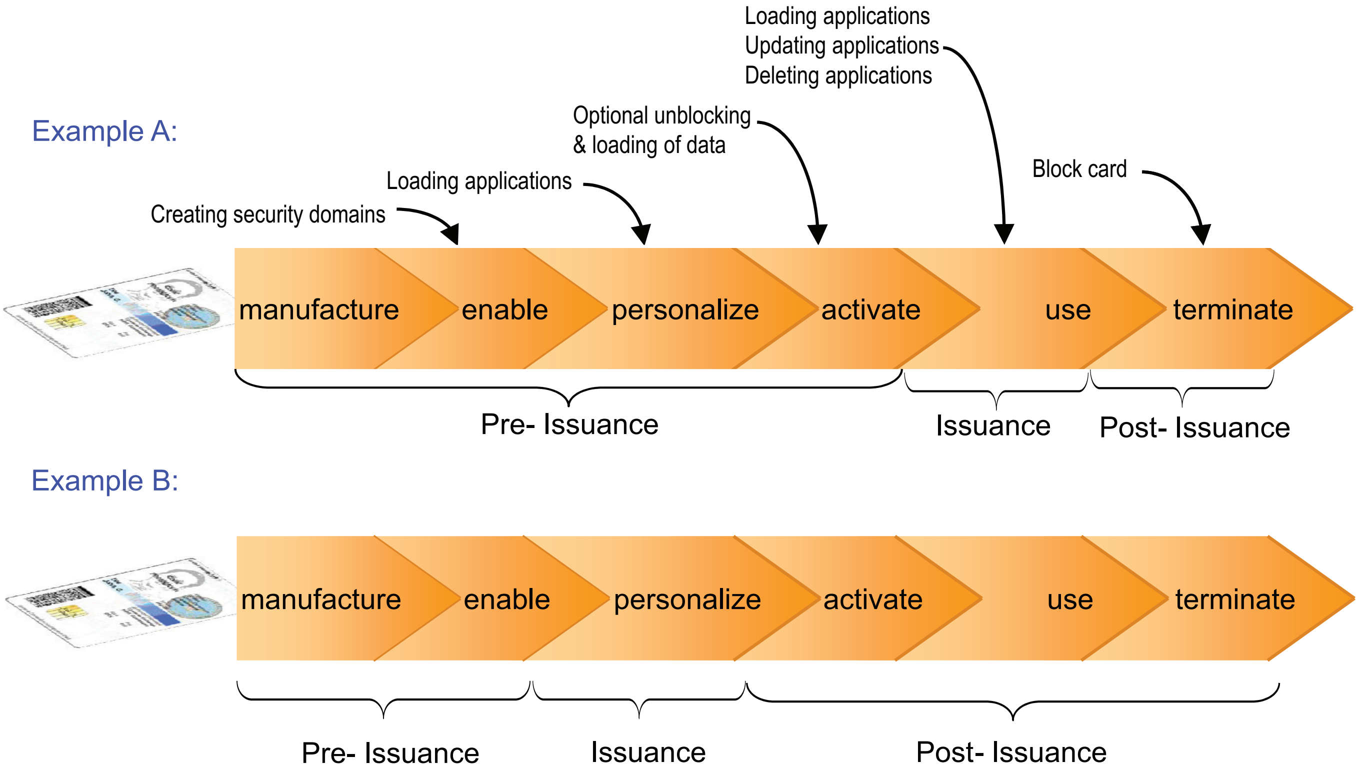


Figure 8 - Typical life cycle phases of a smart card

As mentioned previously, a smart card may contain more than one application. The figure above and explanation below give an overview of how the life cycles of the card, GlobalPlatform Security Domains and the applications are related.

Firstly, during the manufacture, enable and personalize stages depicted in the diagram (pre-issuance/issuance), the card hardware is assembled and applications, application data and key materials are securely loaded onto the chip. As explained in more detail later in this section, GlobalPlatform defines duties to be performed by individual roles throughout this process, allowing these duties to be distributed across different parties without compromising security. Once personalization has taken place the card may require a separate activation process, to ensure that cards cannot be misused prior to delivery to the cardholder. During the use phase (issuance/post-issuance), the card will authenticate the credentials of cardholders to gain access to physical sites as well as networks and data. It is also possible to load new applications or update/delete existing applications. Finally, in the post-issuance stage, when a card expires or is reported lost or stolen, it may be important to deactivate the card itself rather than just registering this fact in a database. This will ensure that the card refuses to authenticate its credentials in off-line situations.

It is important to note that through the use of GlobalPlatform Specifications at both the card and systems level, the issuer can take full advantage of a highly specified manner of addressing both the card life cycle and the application life cycle. The issuer is provided with a common set of card features that allows the card itself to be followed in a back office system.

In Figure 9 below, we show how the smart card life cycle stages map onto the ID management roles defined in section 4 of this White Paper.

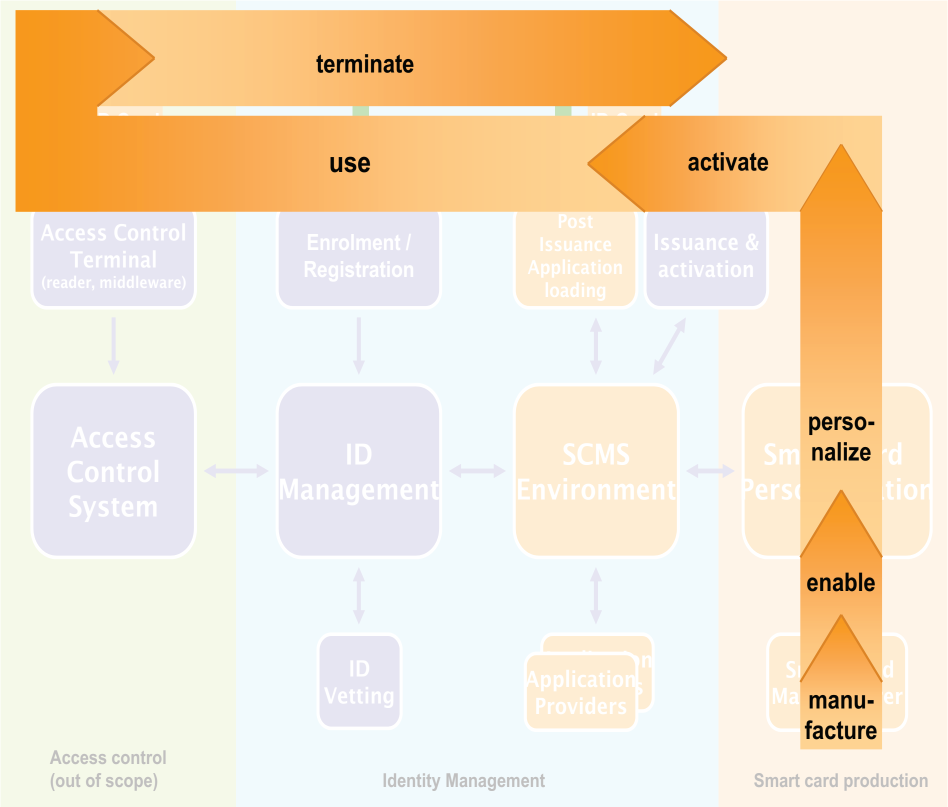


Figure 9 – The card's life cycle phases impact different parts of the identity management infrastructure

Card Issuance Processes

For the purpose of clarification, the process of card issuance can be based on a centralized or decentralized issuance model. Whichever service model is chosen, GlobalPlatform Specifications can be implemented in a common manner. They outline the duties to be performed by individual roles throughout the process, ensuring issuance is managed efficiently regardless of service model and allowing duties to be securely distributed across different parties.

In the centralized issuance scenario and during the pre-issuance stage following enrolment and ID vetting, the card issuer prepares the cardholder data to print and encode using the SCMS. Batch personalization data may then be delegated to a service bureau for the personalization of multiple ID cards. This process would occur, for example, if data is to be sent on a daily basis as a 'batch order' to an external bureau or internal department performing this service. The personalization bureau then ensures that available enabled (but non-personalized) cards have been produced by the card manufacturer, before centrally printing and personalizing the cards. Once the card batch is ready, the cards are shipped to the relevant issuance station and an audit trail is forwarded back to the card issuer. At the issuance station, upon verification of cardholder biometrics or PIN, if required, the personalization of the chip is completed (card is activated) and the card is given to the cardholder. This is the issuance stage.

The decentralized model presents a face-to-face personalization scenario. In this case, batches of non-personalized and non-printed (but enabled) cards are shipped to the issuance stations equipped with local printers. At these locations, individual cards are fully personalized and given to the rightful cardholder.

After cards have been issued (post-issuance), they can be updated via a post-issuance service provider. This allows authorized parties, such as the card issuer or application provider, to load, update or delete applications. In the case of the DoD program, replacement smart card log-on certificates, email encryption certificates and new applets can all be downloaded, post-issuance, onto the CAC. As already explained, GlobalPlatform's application loading and activation mechanisms do not distinguish between pre and post-issuance loading, as mechanisms and the Secure Channels utilized are the same. During this post-issuance phase, cards may also be terminated if the cardholder no longer works for the government agency or if it expires.

Now that key card concepts and processes have been explained, it is time to consider GlobalPlatform's contribution to the roles, actors and interfaces applicable to the PIV model.

Section 4: The GlobalPlatform Proposition

This section of the White Paper focuses on how GlobalPlatform interacts with the infrastructure of an ID management program in general, and uses the PIV model for illustration purposes. This infrastructure consists of a number of components which represent organizations as well as the systems they use to carry out their roles in the scheme. In this generalized way, these organizations and systems may be seen as 'actors'.

As the proofing, registration, issuance and production services are generally operated by independent actors in ID card programs, the communicating parties need to agree on interoperable interface specifications, such as those provided by GlobalPlatform. These define a common approach to data and file exchange formats, coherent policies and service levels.

The separation of roles is defined in FIPS for security reasons:

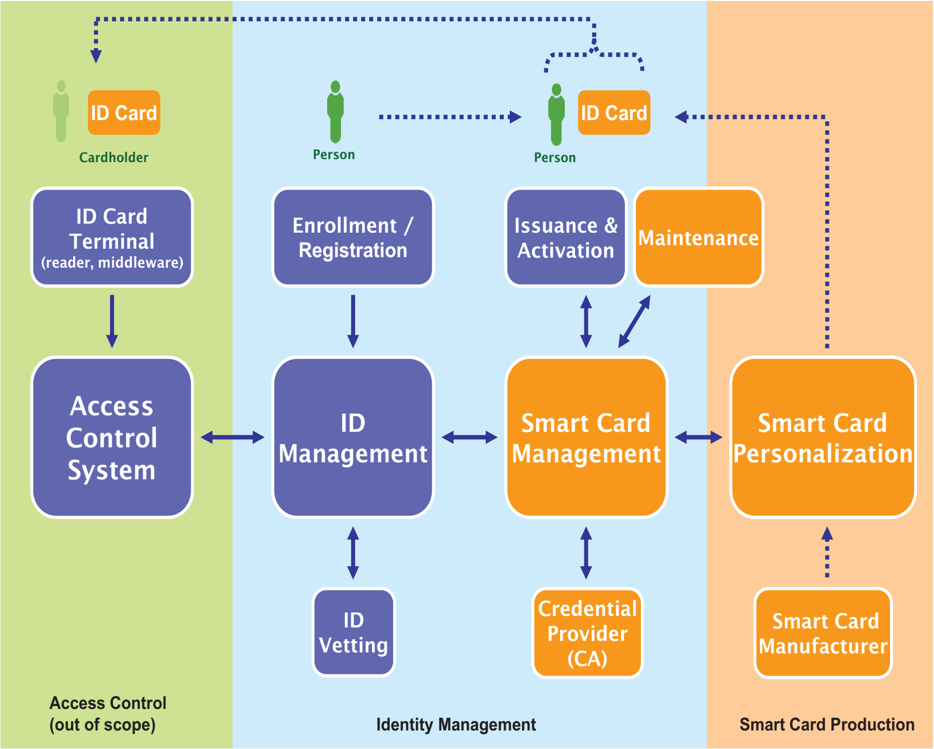


Figure 10 – Personal Identity Verification (PIV) model

In this section, the individual roles and actors within the ID management and smart card production stages are explored. A clear explanation is provided for each role and actor, making its relationship to smart card technology and GlobalPlatform explicit. By reading this section, the reader will gain an understanding of how GlobalPlatform concepts and specifications can greatly ease co-ordination among actors performing various roles associated with smart card management. The reader will also be shown that GlobalPlatform offers a modular and open approach which can be implemented across roles throughout the ID management and smart card production processes.

Figure 11 clearly illustrates where GlobalPlatform technology is applied within the PIV framework and which roles benefit when GlobalPlatform Specifications are implemented. Though not referenced in the diagram, GlobalPlatform additionally provides Messaging Specifications which allow the various components within the PIV framework to communicate in a standardized manner.

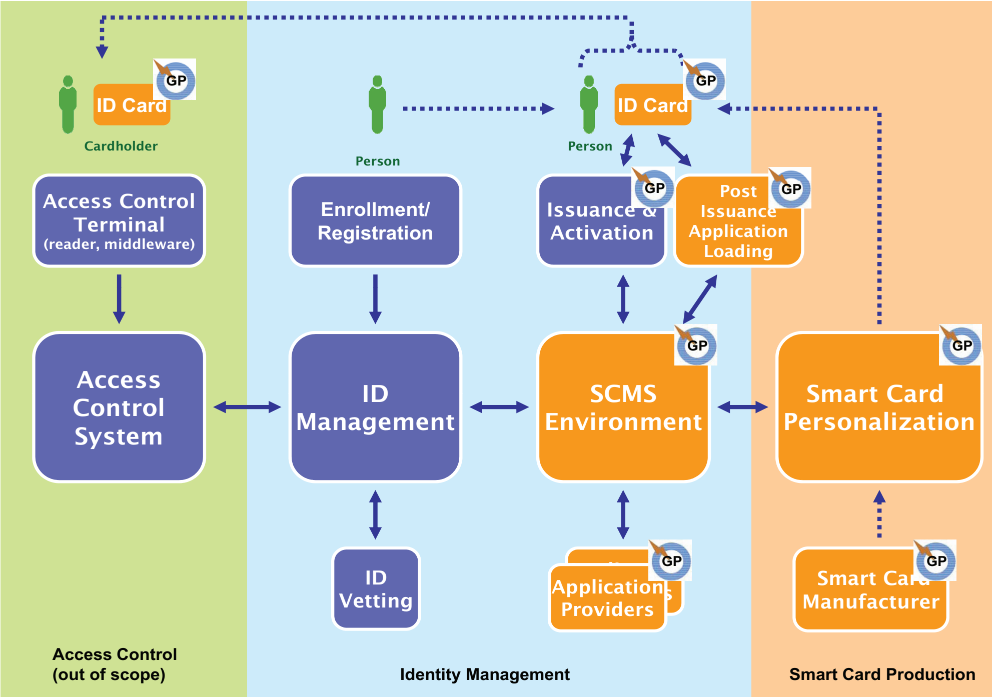


Figure 11 - The GlobalPlatform proposition for the Personal Identity Verification (PIV) model

Identity Management Roles

ID management roles establish the trust chain for a successful ID management program. They act as the foundation of a successful ID management system and should be in place regardless of the type of ID card issued. As such, GlobalPlatform assumes that ID management roles exist. They are therefore not addressed by the GlobalPlatform Specifications.

ID management roles include:

- ***Identity Enrollment Service Provider***

The Identity Enrollment Services Provider manages the process of enrollment for people applying for a smart card. Its purpose is to capture personal ID information and biometrics and store them securely in an IDMS.

- ***Identity Vetting Service Provider***

The Identity Vetting Service Provider validates the ID information provided by the employee to determine the right of a potential cardholder to obtain an ID card. The sequence of ID enrollment or ID vetting is irrelevant, however vetting and enrollment must be completed prior to loading the personal ID information onto the ID card. Ideally ID enrollment and ID vetting should be performed by different entities.

- ***Certificate Authority Service Provider (Application Provider)***

If the ID management program plans to deploy Public Key Infrastructure (PKI) then there is a Certificate Authority Service Provider. This entity is independent of both the IDMS and the Card Management System. The Certificate Authority Service uses the trusted identification data to build PKI certificates and keys which can be used for secure logical access to networks, encrypting information or digitally signing documents. From GlobalPlatform's perspective, flexibility is offered to enable a variety of application providers to load their certificates on to a card in a secure manner.

- ***Identity Management Service Provider (IDMS)***

The Identity Management Service Provider manages the IDMS which controls the life cycle of the cardholder ID. It maintains the enrollment ID data and the vetting status of the ID. It may also manage the certificate authority information associated to an ID. Clearly this life cycle is a 'cradle to grave' service provider.

Smart Card Management Roles

Now that the ID management roles have been identified, the smart card management system, and providers who interact with it, will be explored. It is in this area that GlobalPlatform has a more significant role to play.

Smart card roles include:

- ***Identity Card Management Service Provider (SCMS)***

Whereas the IDMS controls the life cycle of a card holder, the SCMS controls the life cycle of an ID card. The advantages of isolating the smart card specifics from the IDMS by locating data in an SCMS were explained in Section 1 of this White Paper. While the responsibility to manage the life cycle of the cardholder remains with the IDMS, all the processes to execute life cycle commands are delegated to the SCMS area.

Upon receiving IDMS requests, the SCMS interfaces with the certificate authorities, personalization bureaus and other external institutions to drive and co-ordinate the smart card issuance, termination, renewal and maintenance processes. This makes the SCMS the nerve center or brain for smart card technology related processes.

The GlobalPlatform SCMS Functional Requirements document states how to implement and execute all activities for managing smart cards. GlobalPlatform also specifies exchange formats to facilitate the integration of the SCMS into the entire environment. Figure 12 shows a possible configuration of a GlobalPlatform SCMS, showing a large similarity to the PIV concept:

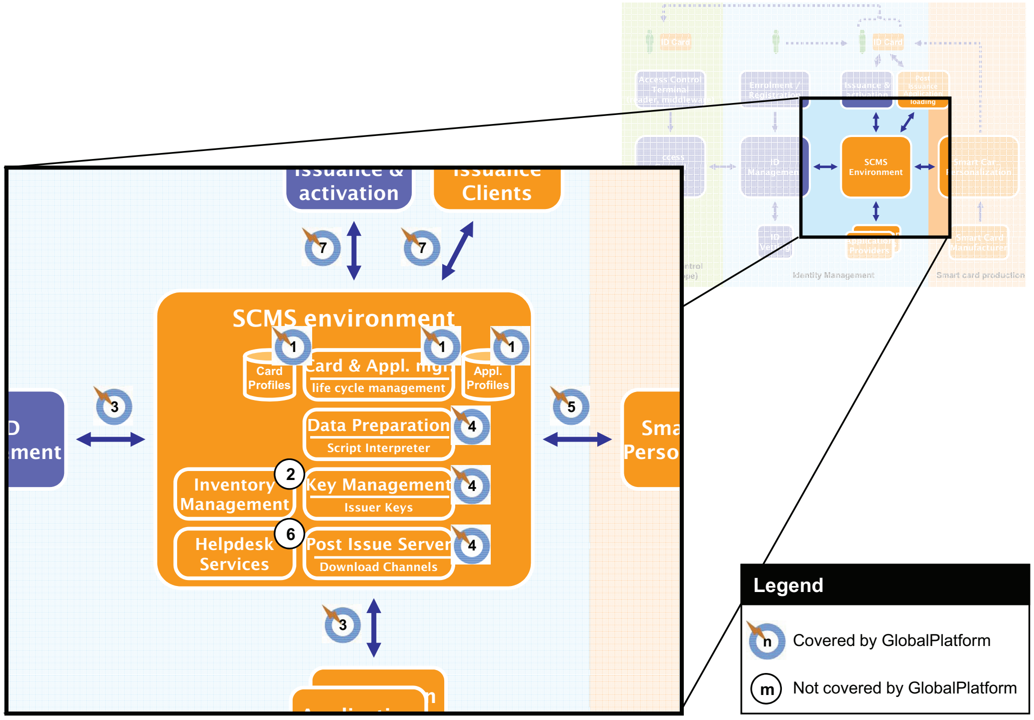


Figure 12 – The functional components of the Smart Card Management System (SCMS) environment according to GlobalPlatform

The GlobalPlatform concept for a SCMS environment is very flexible, allowing a number of functions to be distributed across roles. An important characteristic of these functions is to provide standardized building blocks with open interfaces to assemble a smart card management environment which is independent of specific systems, applications and card vendors. In this scenario, GlobalPlatform facilitates the SCMS function in the following ways:

- GlobalPlatform card and application profiles provide an easy and vendor independent way for importing new card and application definitions into the system.
- The card and application management, data preparation and post-issuance functions will use these profiles to drive the life cycle management processes for the cards.
- Key management provides a number of functions to create, manage and distribute keys securely and in a vendor independent manner.
- GlobalPlatform has also created specifications which define interfaces to other roles in the wider ID management diagram.

- ***Card Manufacturer***

The Card Manufacturer produces enabled cards centrally and in large quantities. It is in the interest of the issuer to be able to procure cards from different manufacturers. Having a standard card platform, as well as common data definitions and interfaces, ensures that personalization and further processing remain open and independent of any one manufacturer.

GlobalPlatform has defined the roles of manufacturer and enabler, and has described a number of aspects that ensure interoperability with other roles within the PIV infrastructure.

- ***Identity Card Personalization Provider***

The Identity Card Personalization Provider manages the smart card personalization process and produces partially or fully personalized but inactive cards. Depending on the scale and policies of deployment, this personalization can be done centrally and in large quantities, or in a distributed fashion at individual issuance sites.

GlobalPlatform provides an interoperable definition of the personalization process, which also extends to the post-issuance arena.

- ***Identity Card Activation Provider***

The Identity Card Activation Provider may operate distributed issuance stations equipped with biometric validation. When the Identity Card Activation Provider has verified that the genuine cardholder is present to collect the card, the personalization of the card is completed and the card is activated (unlocked) and released to the cardholder. The card management service provider can then be informed about the delivery.

GlobalPlatform specifies how activation/deactivation of cards, and the individual applications on the cards, can be carried out in a secure and interoperable manner.

- ***Post Issuance Service Provider***

Post-issuance operations may be necessary on ID cards if the ID application must be upgraded and replaced on the same chip, or if digital ID information (PIN, email address, job position, or privilege, etc.) must be updated.

It has already been explained that GlobalPlatform supports the post-issuance download of applications through its application loading and activation mechanisms which do not make a distinction between pre and post-issuance loading. Additionally, because some things do not need to be done under card issuer control, GlobalPlatform allows card applications to be securely updated by multiple application providers with registered certificates. Examples of such use cases are:

- E-passport and visa management.
- Physical access across multiple independent organizations.
- Card infrastructure integration to logical access control management.

- ***Additional Application Providers***

Apart from certificate providers as discussed above, additional application providers (an electronic purse provider for example) may interface with the SCMS to allow the provisioning of application provider credentials and to exchange ID card states. The application provider will leverage the ID verification service to control and maintain the application data on the card and determine the card's validity, but this entity will generally not have any control over card issuance and revocation.

If standardized GlobalPlatform features are used on both the card and in the back office system, an application provider will be able to easily connect back office systems to the smart card infrastructure and use GlobalPlatform messaging to request card content modification. The application provider will also be able to easily deploy application life cycle in the infrastructure via GlobalPlatform profile and scripting.

Section 5: GlobalPlatform Specifications - Future-Proofing Government Identity Programs

Government ID programs are seldom static in nature and, within a relatively short period of time, the need for new features or functionality often emerges. By implementing a smart card program based on GlobalPlatform Specifications, the government issuer is choosing to deploy an open technology infrastructure which provides extensibility, ensuring that when changes to the existing ID program are needed, new features can be delivered at minimal cost and in a timely manner. The GlobalPlatform architecture also encompasses ISO and FIPS Standards.

So, what does it mean to evolve an ID program beyond a basic ID requirement? How does implementing GlobalPlatform Specifications in the first instance simplify changes to the business model downstream? The range of possible new developments is very large indeed.

The main evolution in government ID projects is related to changes in the regulation environment supporting the program. New threats can be detected that require changes to ID data management in order to provide new protection. Political changes or changing legislation can result in card changes becoming necessary and the mandatory update of the issuance process.

Since no business case is static, the issuer may be asked to add additional capabilities and privileges, such as logical access to IT infrastructure and/or the ability to digitally sign documents. Such capabilities may require additional certificates, possibly supplied by a new service provider. An issuer using proprietary technology could be confronted with extensive integration work with this new application provider. The chances are great that the systems are not sufficiently flexible to allow the new processes for key management and data preparation to be easily incorporated. Likewise, personalization processes will require updating and smart cards already issued and in the field will require the post-issuance download of new application functionality – a feature made possible only if anticipated as a feature at the time of initial issuance.

Had the issuer chosen to deploy the program using GlobalPlatform Specifications for smart card interoperability in the first instance, the government would have invested in an extendable infrastructure that permits open and competitive solutions to be developed and seamlessly integrated into the existing system. Furthermore, additional features that are required can be delivered to the cardholder without having to incur the cost of reissuing the card. GlobalPlatform specifies the manner and method to securely deliver additional applications to a card - post issuance - and manage those applications, even when provided by different service providers.

By ensuring interoperability between stakeholders, the issuer has made the transition from one technology provider to another easy, while simultaneously reducing development time and cost. As a result of collaboration (within the vendor community) multiple applications from different vendors can now reside on a single, secure platform. New smart card manufacturers can be incorporated, new card types added, additional personalization providers may be used and personalization may even be extended to the issuing stations, as depicted in Figure 13.

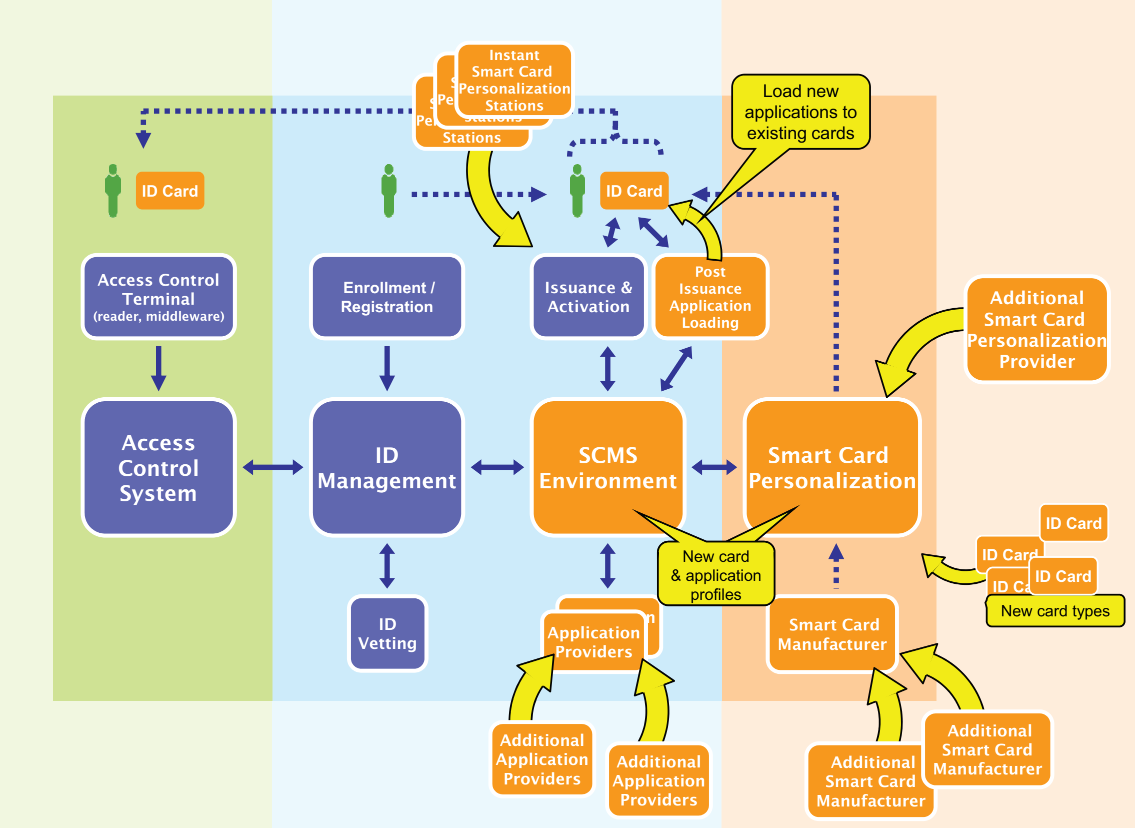

Instant Smart Card Personalization Stations
Load new applications to existing cards
ID Card
ID Card
Access Control Terminal (reader, middleware)
Enrollment / Registration
Issuance & Activation
Post Issuance Application Loading
Additional Smart Card Personalization Provider
Access Control System
ID Management
SCMS Environment
Smart Card Personalization
New card & application profiles
ID Card
ID Card
ID Card
New card types
ID Vetting
Application Providers
Smart Card Manufacturer
Additional Application Providers
Additional Application Providers
Additional Smart Card Manufacturer
Additional Smart Card Manufacturer

Figure 13 – New components can be easily added in a GlobalPlatform compliant infrastructure

Most importantly, with the flexibility to use compatible technology from different vendors, an environment is created whereby the most competitive costs can be achieved for implementations and upgrades. Adapting to changing circumstances (such as adding applications to, or changing components of, existing programs) demands that the infrastructure be open, interoperable, scalable and agile. This is accomplished though the careful selection of vendor components and solution offerings built upon open specifications created through cross-industry collaboration. In a separate document available on GlobalPlatform's website, the benefits of GlobalPlatform technology compared to proprietary solutions are captured in story format.

With GlobalPlatform Specifications as a foundation a successful, sustainable and extendable smart card program can be achieved. These specifications have already demonstrated delivery of these benefits through sixteen known real-world implementations at the time of this White Paper's publication. For further information on these implementations, please visit www.globalplatform.org

For more information about the GlobalPlatform organization and available specifications, please visit www.globalplatform.org

Appendices:

Appendix I - Acronyms

Acronym	Meaning
CAC	Common Access Card
DAP	Data Authentication Pattern
DEERS	Defense Enrollment and Eligibility Reporting System
DoD	Department of Defense
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
GP	GlobalPlatform
HSM	Hardware Security Module
IDMS	Identity Management System
IDRS	Identity Registration Subsystem
Java Card™	Smart card environment supporting GlobalPlatform card framework - Go to the following website for Java Card™ documentation: http://java.sun.com/products/javacard
MULTOS™	Smart card environment supporting GlobalPlatform card framework - Go to the following website for MULTOS™ documentation: http://www.multos.com
NIST	National Institute of Standards and Technology
O/S	Operating System
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
SCMS	Smart Card Management System

Appendix II – List of GlobalPlatform Specifications

Following is a list of GlobalPlatform Specifications and related documents which are publicly available at the time of this White Paper's publication:

Card Specifications:

- GlobalPlatform Card Specification
- Card Security Requirements Specifications
- GlobalPlatform Smart Card Security Target Guidelines

Device Specifications:

- GPD/STIP Specifications
- Device Application Security Management (DASM) Specifications

Systems Specifications:

- GlobalPlatform Messaging Specification
- PIV Configuration for Messaging
- CPS Demonstrator, a CPS Implementer Sample Package
- SCMS Functional Requirements
- Key Management Requirements Systems Functional Requirements Specification
- All Systems Profile and Scripting Specifications
- The GlobalPlatform Guide to Common Personalization

For further information on GlobalPlatform Specifications, visit www.globalplatform.org