GLOBALPLATFORM

THE STANDARD FOR SMART CARD INFRASTRUCTURE

Overview

June 2004

Executive Summary

GlobalPlatform technology, managed by the GLOBALPLATFORM consortium, is an architecture and associated standards organization for the definition and management of dynamic, single and multi-application smart cards. GlobalPlatform includes not only specifications for the cards (the *GlobalPlatform Card Specification*), but also for the devices used to read smart cards (the *GlobalPlatform Device Specification*), and for the card and device support infrastructure (the *GlobalPlatform Systems Specifications*). Together, these components define a secure, flexible, easy to use smart card environment.

Smart card components to date have largely not been interoperable because applications have been built onto a proprietary card and device operating system. GlobalPlatform forms the foundation for the development and deployment of single and multiple application smart cards by any Card Issuer. With GlobalPlatform, users have total independence in choosing both smart card and device vendors, moving away from inflexible, closed proprietary systems. For existing smart card Issuers and Acquirers who have been struggling with the high cost of smart cards and smart card infrastructure, and for those new to smart cards, GlobalPlatform's standards will translate into greatly increased innovation and significantly lower smart card system costs.

GlobalPlatform works with the underlying card, device, or systems technology to provide additional security and functionality. Established open technologies, such as Sun's Java/Java Card supports GlobalPlatform, brings established bases of programmers and development tools to GlobalPlatform and to smart cards.

The combination of a flexible, easy to use development environment, results in a number of significant benefits, both commercial and technical, which are unmatched by any other available solution. The primary commercial benefits of GlobalPlatform include:

- The ability for Card Issuers to strengthen customer relationships by differentiating their products with added features and functionality.
- The ability for Card Issuers to customize their products to the cardholder level by allowing the addition of cardholder specific applications.
- The opportunity for Card Issuers and Acquirers to develop new revenue streams from new single and multiple application business models.
- The enforcement of Card Issuer control over the card and business processes.
- The reduction in cost and time to market for Card Issuers and Acquirers with new products and enhancements through post-issuance/deployment downloading of new applications and application updates.
- The protection of investment in card support infrastructure by ensuring all GlobalPlatform card and device technology can be supported by the same infrastructure.

While use of GlobalPlatform has significant commercial benefits, those commercial benefits derive from the underlying advantages of GlobalPlatform technology. The primary technological advantages of GlobalPlatform are:

- The wide selection of suppliers for all aspects of the technology, including cards, devices, operating systems, software providers and card technologies.

- The secure support of single and multiple applications that allow applications to coexist on a single card or in a device in a safe controlled manner.

- The standardization of GlobalPlatform commands that ensure card platform independence for the Issuer's support infrastructure.

- The support of existing standards such as ISO 7816, ISO 14443 and EMV that ensure backwards compatibility with existing smart card implementations.

- The strongest commercially feasible security designed to balance risk with cost and complexity.

With GlobalPlatform, a single infrastructure can support many card programs, device, and systems technologies. It is important to note that while GlobalPlatform encompasses card, device, and systems technologies, GlobalPlatform cards do not require GlobalPlatform devices and vice versa, nor do GlobalPlatform cards require GlobalPlatform systems and vice versa. GlobalPlatform device technology scope extends beyond traditional terminals to a wide array of emerging card acceptance devices making them available for new uses and applications. Examples of these devices include personal computers and kiosks as well as consumer devices such as cell phones, TV set top boxes, and increasingly popular hand-held computers and PDAs (Personal Digital Assistants). By providing a common way for smart card applications to be developed and managed for both traditional and emerging types of devices, GlobalPlatform enables extended business opportunities. GlobalPlatform's advancements in Smart Card Management Systems and related specifications contribute to the development of a seamless, comprehensive systems architecture for managing smart cards and applications throughout their lifecycle. Controlling process execution, the developments in Smart Card Management Systems define interoperability with back-office or legacy systems by standardizing critical processes such as messaging, personalization, security, key management and application loading.

2. Introduction

This document is intended to provide an overview of the GlobalPlatform initiative in order to fill the gap between industry perception and the available technical documentation. By reviewing this document, you can quickly gain insights into how you can begin to harness this powerful technology to offer unique, tailored products to your customers across industries around the globe.

Understanding the benefits of a universal smart card platform, the GLOBALPLATFORM consortium is promoting the adoption of GlobalPlatform card, device, and systems technology into many industries which will make use of smart cards, including financial services, governments, mobile telecommunications, public health care, retail and transit. Widespread cross industry adoption of GlobalPlatform will eliminate the technological barrier hindering cooperation between different industries. In this environment, Card Issuers will be able to make arrangements with potential Application Providers to enhance their cards, without having to worry about infrastructure incompatibilities or other serious technological issues. Card Issuers will be able to compete based on quality of services, product features and marketing, while application providers will have a wide selection of distribution channels.

In October 1999 management and ownership of the GlobalPlatform was assumed by the GLOBALPLATFORM consortium, making the GlobalPlatform Specifications part of a truly open cross industry effort. The GLOBALPLATFORM consortium was established to create, maintain and drive adoption of standards to enable an open and interoperable infrastructure for smart cards, devices and systems that simplifies and accelerates development, deployment and management of applications across industries. Companies participating in the GLOBALPLATFORM consortium are interested in issuing single and multiple application smart cards to their customers. The goal of the organization is to advance and drive adoption of GlobalPlatform's smart card technology. While it was founded by issuing organizations of various industries, GLOBALPLATFORM brings together the interests of issuers, vendors, public entities and technology companies to develop standards and specifications. Participants determine how different emerging smart card technologies can converge to create a global infrastructure, while still allowing competitive, unique product capabilities. The expected result is an acceleration in the implementation of static and dynamic single and multiple application smart card programs around the world.

GLOBALPLATFORM will achieve its objectives through the creation of pragmatic, actionable deliverables that will enable:

- Issuers with greater choice of technology providers resulting in: lower product costs; granting access to value added services for greater differentiation; a common platform that supports extensibility.

- Vendors to focus R&D initiatives on truly value-added capabilities that will distinguish their product from the competition.

- Application developers to expand their customer base by targeting applications that benefit multiple industries.

More information about GLOBALPLATFORM can be accessed from the GlobalPlatform website at www.globalplatform.org.

2.1. Problems with Today's Smart Cards

Before beginning a discussion of the vision of GlobalPlatform, it is important to understand the problems present in the market place that GlobalPlatform is designed to overcome. In many markets, very successful smart card systems have been built and provide ongoing value to Card Issuers and consumers, such as the worldwide GSM wireless, the French banking and the Hong Kong transit markets. Yet smart card based solutions can provide value to more industries and consumers. By promoting standard approaches to the common components of a smart card system, GlobalPlatform provides an alternative to custom designed solutions.

GlobalPlatform is designed to overcome the following major impediments to low cost smart card implementations:

- ***Lack of a Universal Card Platform***. Before GlobalPlatform each card and device manufacturer developed its own card and device solutions using their own unique operating systems. To develop applications for these cards and devices, software developers needed a thorough understanding of each card and device operating environment. Consequently, few developers were available to work with any particular type of smart card or device. As a result, there was little incentive for software companies to offer the development and testing tools programmers have learned to rely upon for more common technology, such as Windows and Java.

- ***Extended Time to Market***. Before GlobalPlatform an Issuer either developed expertise in specific card and device operating systems internally, or contracted with the few available outside smart card developers. In many cases, months were wasted in waiting for a developer to become available, or to become familiar with specific technology. Even after an Issuer manages to fully staff and train a development team, further delays are likely to result from the lack of available development tools.

- ***Difficulty in Testing***. Along with the lack of programmers, there are few tools available to assist programmers in developing and testing smart card systems. Because smart card technology is improving rapidly, and each device uses a proprietary operating system, there is little incentive for software companies to develop and provide the sort of tools that software developers in other areas of the computer industry rely upon to test their work. Lacking these tools, smart card software developers must either invent their own tools; increasing the time and complexity of development, or deliver systems which may not have been sufficiently tested.

- ***Difficulty in Dynamically Updating Cards.*** The lack of standards has led current smart cards to be programmed without enough sophistication to support post-issuance or dynamic reconfiguration throughout the card's life cycle. The internal organization of data on the card is not structured well enough to securely support adding, changing and deleting applications after the card has already been issued and used.

The problems listed above result from a lack of consistency, either in the programming requirements demanded by proprietary operating systems, or from the lack of open specifications defining critical procedures such as post-issuance application loading.

2.2. The GlobalPlatform Vision

GlobalPlatform is designed as a cross-industry standard for the entire smart card infrastructure to include card, devices, and systems technology that will increase the total market by facilitating access to and use of smart cards and decrease the costs of implementation.

GlobalPlatform is a secure and flexible technology standard that organizes and focuses the single and multi-application initiatives of the many participants in the global smart card industry. By defining the specifications for a comprehensive system architecture, GlobalPlatform enables the effective development of globally interoperable, single and multiple application smart card systems.

GlobalPlatform is supported by many key players in the smart card industry—service providers, hardware manufacturers, software companies, application developers, and systems integrators. Collectively these players have worked together to make GlobalPlatform an effective cross industry technology standard.

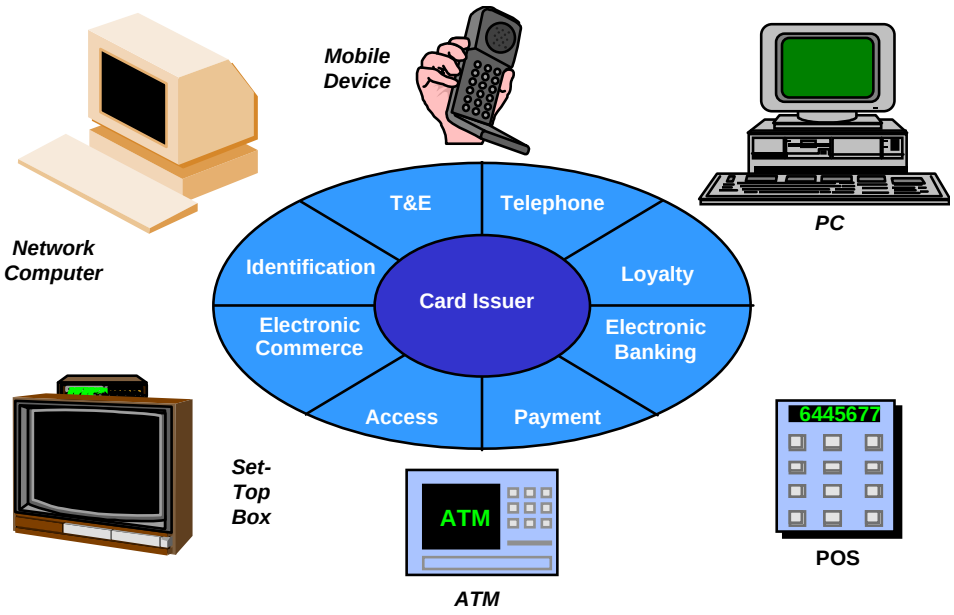


Figure 2.1: The GlobalPlatform Vision – Multiple Services available through Multiple Devices using a Single Smart Card enables the provision of differentiated services to build stronger relationships with customers.

GlobalPlatform enables the development of single and multiple application smart cards that can be tailored to the individual customer's needs through the ability to reconfigure and load new applications even after the card has been issued and used. The flexibility of post-issuance application loading gives the capability to create unique, highly valued services and products.

Facilitates 'anytime anywhere' access. GlobalPlatform supports existing standards for smart cards. Therefore, GlobalPlatform ensures compatibility with existing smart cards and devices already

installed and in use. In addition, GlobalPlatform promotes the acceptance of smart cards at a variety of consumer devices.

Maximize return on investment in acquiring infrastructure. GlobalPlatform provides a structure to enable an acquirer (e.g. a merchant) to interface with many different cards hosting different types of applications issued by different businesses.

GlobalPlatform serves to orchestrate the efforts and operations of the many players in the smart card industry to yield tangible solutions which overcome many of the prior limitations of smart card technology. GlobalPlatform is backed by many stakeholders in the smart card industry – service providers, chip manufacturers, card manufacturers, device manufacturers, software companies, application developers, and system integrators.

3. GlobalPlatform Commercial Benefits

GlobalPlatform does more than tear down barriers to smart card system development. It also offers the freedom to create single and multiple application smart cards and to customize product offerings. Unlike most of today's smart card systems, which are designed to serve a single purpose, GlobalPlatform supports the deployment of stable and secure single and multiple application cards. GlobalPlatform cards are capable of performing many different types of operations, for different purposes, in different environments.

GlobalPlatform enables Card Issuers to customize the application(s) on their cards – both before and after card issuance – to meet the specific needs of different customer segments. By providing these single and multiple application and customization options, GlobalPlatform offers Card Issuers the opportunity to extend their relationships with customers and to explore new business areas.

While GlobalPlatform is a significant advance in the technology of smart cards, its greatest significance is in the new commercial structures and partnerships it allows.

3.1. Differentiation

In a highly competitive marketplace, GlobalPlatform allows Card Issuers to strengthen their customer relationships by differentiating their products and services from their competitors with added features and functionality. GlobalPlatform allows Issuers to build combinations of applications unique to their products. Once an Issuer establishes a unique set of product features in the market, price will no longer be the primary competitive weapon.

3.2. Customization

By enabling the easy addition of applications to the card post-issuance, GlobalPlatform enables the cardholder to select applications made available by their Issuer, and create their own card. For the first time ever, card products can be customized to a segment of one. This will increase retention since the cardholder will have built their "ideal" card and will be less likely to abandon one application if it will have an impact on other applications which they value.

3.3. Additional Revenue

By enabling Issuers to offer real estate on their cards to other entities, GlobalPlatform provides an opportunity to generate new revenue streams through the introduction of new businesses. Additionally, by allowing cardholders to "build" their own suite of applications on a card, the card has greater utility and therefore is a greater potential to generate cardholder based revenue.

3.4. Enable Issuer Control to be Enforced on the Card

Within the card, GlobalPlatform enables the Issuer to maintain and exercise control through the use of an on-card agent – an application called the "Card Manager" – which logically represents the Issuer. This agent controls which applications can be loaded onto the card after it has been issued. Although GlobalPlatform allows cardholders to load new applications and delete old ones from the card post-issuance, the ultimate arbiter of card content remains the Card Issuer. External to the card, there is no central authority which controls the application loading function, nor is there any need for a Card Issuer to pay a central authority to add applications to cards.

3.5. Faster, Cheaper Development

GlobalPlatform allows Issuers to move to market faster, and at a lower cost than other single and multiple application solutions. The primary reason for this is that GlobalPlatform is based on widely employed development environments such as Java/Java Card. This popular development environment already has developers numbering into the millions, established development tools and significant worldwide marketing and support infrastructures. As a result of these factors, when a Card Issuer is ready to move to market with new partners and applications, they will be able to move more quickly and with less resources if they use GlobalPlatform Specifications. Additionally, support for post-issuance download allows new products to be distributed and existing products to be updated without incurring the expense of reissuing cards.

GlobalPlatform specifies a standard command set for personalizing the card. This provides the Issuer with the ability to utilize the same personalization process for any card manufacturer that supports GlobalPlatform. It also standardizes the process for single and multiple applications so that cards can be personalized in a single, streamlined process, regardless of the combination of applications on the card. This is significantly more efficient than today's personalization of multi-application cards, which often involves a personalization step for each application on the card or a time-consuming and expensive effort to integrate multiple proprietary personalization processes, resulting in a new process which is only applicable to one specific card series.

3.6. Protects Investment

GlobalPlatform specifies how to load and delete applications to and from cards after issuance, using existing infrastructure. Not only does GlobalPlatform eliminate the costly process of reissuing cards when new requirements arise, but it also enables a card to be automatically updated during the normal course of use. Additionally, by standardizing the commands for application and card lifecycle management, GlobalPlatform ensures that new advancements in card technology can be accommodated within the established back-end system.

4. GlobalPlatform Features

GlobalPlatform resolves many of today's smart card problems by defining a fully integrated, open environment for the development, issuance, and operation of smart cards. The intention of GlobalPlatform is not to compete with existing smart card specifications, operating systems, or standards. Instead, GlobalPlatform encourages and supports these efforts by facilitating smart card development that is compatible with existing systems and standards. GlobalPlatform builds on the existing smart card infrastructure to support a single and multiple application environment.

4.1. Issuer Choice

By defining an interface which exists on top of other technologies, GlobalPlatform allows the freedom to choose cards, devices, operating systems and applications, while enabling a single standardized support infrastructure. This choice will help drive innovation and new product development across all aspects of the industry.

Adopting widespread and popular development platforms also solves other critical smart card problems: availability of developers and time to market. With the support of commonly used software programming languages like Java/Java Card, GlobalPlatform opens up smart card application development from the few elite programmers who understand today's arcane card, device, and back-end operating systems to millions of developers around the world. By using the tools developed by the industry, these developers can become productive smart card application developers virtually overnight.

4.2. Support for Single and Multiple Applications

By defining a secure application management method, GlobalPlatform works with the different card technologies to allow single and multiple applications to coexist on a single card, and to share resources in a safe and controlled manner. The ability of the GlobalPlatform card to support single and multiple applications allows Card Issuers to tailor cards to meet the specific needs of individual customers. The GlobalPlatform Device Specification is also capable of supporting single and multiple applications, which will further expand the smart card services Issuers can offer to their cardholders.

4.3. Platform Independence

GlobalPlatform is designed to support a wide variety of smart card and device technology. This means that the investment in developing the support infrastructure is not lost when moving to a new platform. GlobalPlatform can support new smart card platforms as they become available. The design or "architecture" of GlobalPlatform and the GlobalPlatform command and response formats between the card and device/support infrastructure remain constant, and do not have to be changed.

This is important in a dynamic industry where new smart card platforms with expanded capabilities are frequently introduced to the market.

4.4 Standardization and Interoperability

GlobalPlatform provides a standardized infrastructure offering the promise of true interoperability for the complete smart card infrastructure. The standardization of smart card systems and components transforms the issuance of smart cards from a complex integration of proprietary components into a seamless smooth operation. A standardized issuance process enables a wider choice of vendors and improvement in the quality of service for Issuers.

Additionally, standardization enables an issuer to choose additional vendors or change vendors effortlessly. No longer facing the substantial time and cost penalties incurred before standardization, problems and integration costs are significantly reduced when both vendors support the standard.

An issuer's investment is protected by standardization because it does not lock them into a single proprietary system. As the market grows, the issuer can be confident that vendors supporting the standard will move to update their products and systems to incorporate any changes to the standard.

4.5. Standards Compatibility

GlobalPlatform supports the ISO 7816, ISO 14443 and EMV industry standards. This provides the capability for existing ISO/EMV terminals to accept and use GlobalPlatform cards.

When loaded with the appropriate application, GlobalPlatform cards can be used in existing ISO/EMV-compliant terminals and any EMV-compliant card currently in use can also be used in any new, GlobalPlatform compatible device. This means that cardholders that have cards from previous smart card programs can use the GlobalPlatform infrastructure and do not have to re-issue their cards. This also means that the issuance of GlobalPlatform cards does not have to be tied to the availability of GlobalPlatform compatible devices or vice versa.

By building on the ISO and EMV standards, GlobalPlatform ensures interoperability between new smart card implementations as well as interoperability with all existing card implementations that are ISO and EMV-compliant.

GlobalPlatform systems documentation uses common IT standards for portions of the systems components of the GlobalPlatform infrastructure. As an example, XML technology [W3C REC-xml-19980210]is used systematically for describing the structure of data , and ECMA script [ECMA 262] is the language selected for scripting.

4.6. Security

GlobalPlatform has been designed to enable the strongest commercially feasible security. Based on publicly available and widely used card technologies, the security of GlobalPlatform is well

documented and well understood, a requirement for an assurance of security. Many GlobalPlatform compliant card products have been subjected to testing under the Common Criteria standards and successfully evaluated at strong levels of security such as EAL 4, EAL 4+ and EAL 5. This standard has already been endorsed by the financial services and wireless telecom industries.

5. GlobalPlatform Technology

GlobalPlatform defines an environment for the development and operation of single and multiple application smart card programs. The principle components of the infrastructure within this environment are cards, devices, and systems. An application in this environment is split between the device, the card and back end system. That is, part of the overall application resides on the card, while another, complementary component resides in the device. Management information (profile, keys, application specific data, data generation rules) are stored in the back end systems. This distributed design is illustrated in *Figure 5.1,* which shows four applications distributed over two terminal devices and three cards; the cards and terminals each support a subset of the four applications. In order for a particular application to be activated, both a card and a device component must interact.

The application layout depicted in *Figure 5.1* is also called the application architecture. The term "architecture" refers to the internal organization of a computer or a computerized system, and generally implies that a formal definition is available.

Addressing the card and device separately, are the *GlobalPlatform Card Specification* and the *GlobalPlatform Device API Specification* (based on STIP Technology). Together with the GlobalPlatform Profiles and Scripting specification, these specifications formally define the distributed application architecture to a fine level of detail. By addressing not only the cards, but the devices, development tools and back end management systems as well, GlobalPlatform has provided the first comprehensive end-to-end approach to single and multiple application smart card systems.

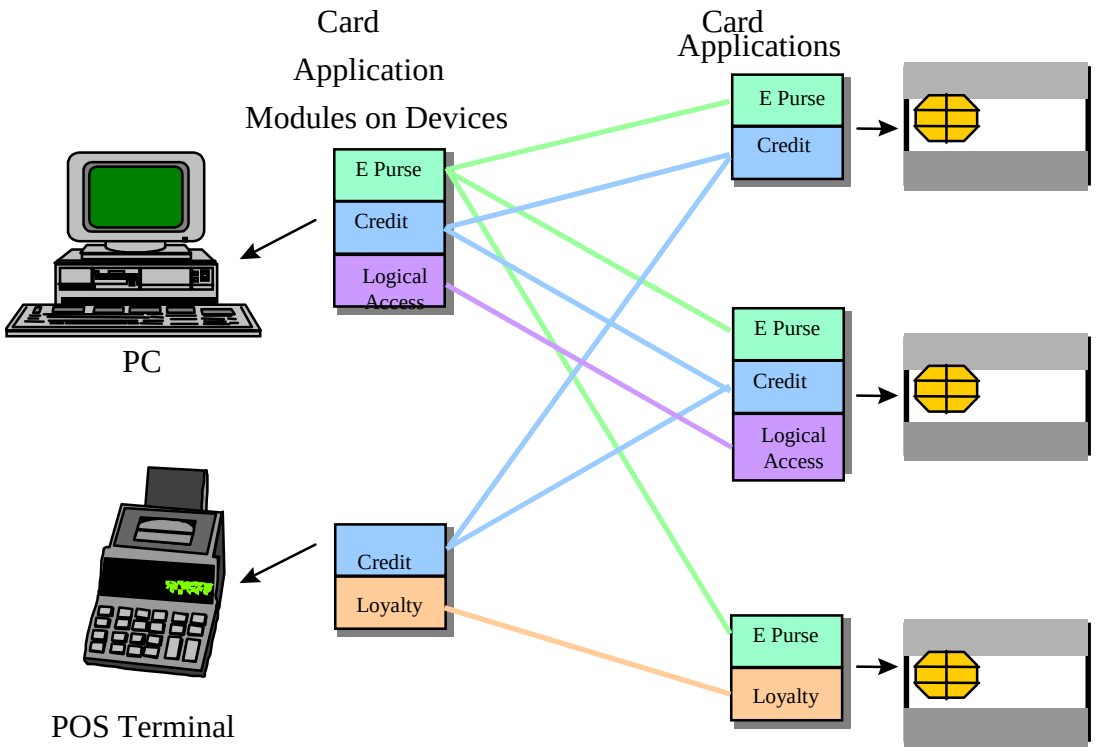


Figure 5.1: GlobalPlatform Application Architecture

5.1. GlobalPlatform Card Specification

Comprehensive card specifications are a critical component of the GlobalPlatform technology. From both the Issuer's and the cardholder's perspective, the card *is the vehicle* for providing access to a whole new array of services. From a technical perspective, it is the carefully designed card architecture that enables many of the core features of GlobalPlatform to be realized.

The *GlobalPlatform Card Specification* defines the cross-industry, non-product specific requirements for implementing a GlobalPlatform card. Its primary purpose is to define how the card itself and applications are managed by the card and by specifying the communication between an off-card entity and the card. A secondary purpose of the *GlobalPlatform Card Specification* is to define a GlobalPlatform API and explain how this API can be used by an on-card application to manage and protect itself. Another purpose is to define the security mechanisms that can be used to protect the card and its different applications. The *GlobalPlatform Card Specification* covers all aspects of application management, from initially adding the application to the card, to the application's management of its own life cycle and ultimately to the removal of the application from the card. The *GlobalPlatform Card Specification* is a broad, cross-industry specification. Today, most smart card manufacturers have developed smart card products in accordance with the *GlobalPlatform Card Specification*. This ensures ample choice of cards for Card Issuers interested in rolling out GlobalPlatform systems.

5.1.1. GlobalPlatform Card Architecture

The *GlobalPlatform Card Specification* defines the part of the GlobalPlatform application architecture that is contained within the card. The card architecture, illustrated in *Figure 5.2*, contains an operating system, a runtime environment, the GlobalPlatform API, the GlobalPlatform Card Manager and a set of applications. The GlobalPlatform components consist of specific security control mechanisms exerted over the card and applications by the Card Manager, and a GlobalPlatform API, which extends the runtime environment API being used. Because many of the necessary card components are already covered in basic card technology that specify the runtime environment and operating system, the GlobalPlatform Card Specification focuses on the new components in the card architecture.

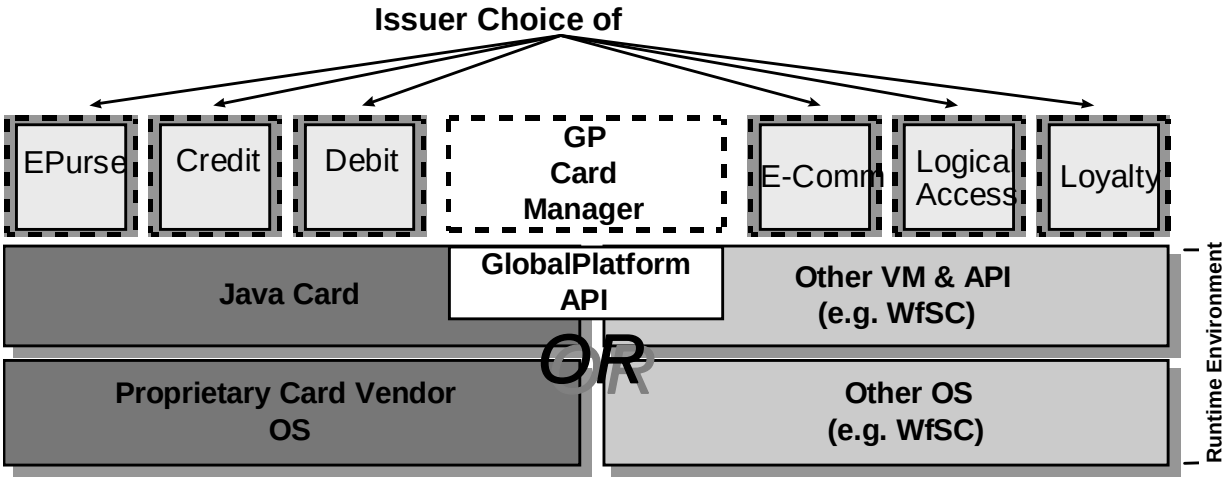


Figure 5.2: GlobalPlatform Card Architecture

The basic components of the GlobalPlatform card architecture include the following:

- ***Runtime Environment.*** The Runtime Environment consists of three basic components. These are the Card Operating System, the Virtual Machine and the Application Programming Interface (API). GlobalPlatform cards can continue to use the vendor-specific, proprietary operating systems to allow suppliers to differentiate their products. The Virtual Machine acts as interpreter between the language of the card operating system and the language in which applications are written.

  The Runtime Environment includes an API, or Application Programming Interface, which defines a way for a programmer to take advantage of (i.e. interface with) the capabilities of the card without requiring any knowledge of the underlying operating system. The API is essentially an access means to a set of tools or services commonly used by applications such as storage, communications and cryptographic features of the card.

- ***GlobalPlatform API***. While the Runtime Environment API provides generic services needed by a basic smart card application, the GlobalPlatform environment, being primarily the Card Manager, provides additional services relating to card and application management and a mechanism for securing communication between a card and an off-card entity. To assist the application programmer that wishes to use these features of the GlobalPlatform environment, a separate API is needed in the GlobalPlatform card. For example, there is a service which allows

an application to open a secure channel for off-card communications. Another service enables an application to lock the card in case of a security threat. Yet another service allows an application to verify a key check value before loading the key to the card.

- ***The Card Manager***. The Card Manager represents the Issuer's interest on the card by preventing unauthorized use of the card. The Card Manger is what enables the Card Issuer to maintain ultimate control of the card and its contents. The Card Manager supports the following four functions.

  Command Dispatch. When a GlobalPlatform card is presented to a device, the device sends commands to the card. With multiple applications on the card, there must be some way to insure each command is processed by the proper application. In other words, security problems would arise if a command intended for one application were to be seen and processed by a different application.

  In order to ensure that commands are routed to the proper application, the Card Manager receives all incoming commands and dispatches them to the proper application. An example of a command is the one that initially selects an application. Since all commands are routed through the Card Manager, it monitors application selection commands to keep track of the current application. It then dispatches commands to the currently selected application.

  Content Management. The Card Manager is responsible for controlling the content on the card in accordance with the Issuer's requirements. The Card Manager must grant access to the card for certain restricted operations, such as loading a new application. The Card Manager keeps track of all of the applications on the card. Through the card content management services contained in Card Manager, all applications can be created and accessed in a uniform way. This uniformity is necessary to ensure the security of the card. For example, it is only by forcing all post-issuance applications to be installed in the same way, that the Card Manager is able to provide the Card Issuer ultimate control over which applications can be loaded after issuance.

  Security Management. The Card Manager offers several security functions on the card. It provides a Global PIN (Personal Identification Number) which can be shared among applications. It also provides access to a secure channel for off-card operations which need protection, such as the loading of keys. Another role of the Card Manager is to keep track of all the applications on the card and report on both the state of these applications, and the state of the card itself, for auditing purposes. The Card Manager can also perform velocity checking to guard against "guessing" and other attempts to violate the security of the card. In addition, the Card Manager can ensure that each application is allocated only the designated amount of memory during runtime and application loading.

  Security Domain. The Card Manager acts as the Issuer's Security Domain. Each application is assigned to a single security domain, which is responsible for controlling certain operations associated with the application. The Issuer's Security Domain controls the Issuer's applications on the card. It holds the Issuer keys, provides access to secure communications and facilitates operations such as loading, removal, initialization and possibly personalization of applications under its control.

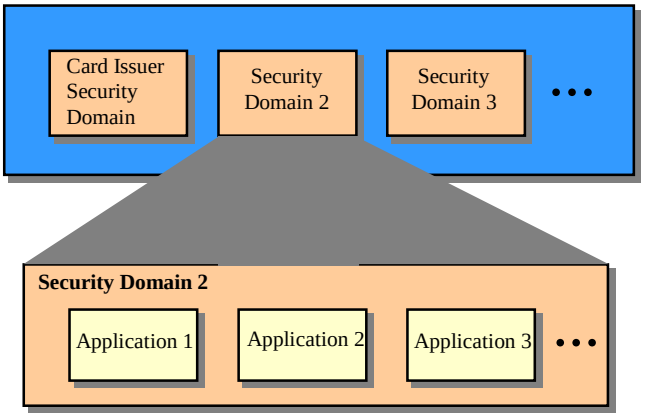
- ***Card Applications***. The applications on the card represent the differentiated and customizable services that can be offered to cardholders. There will be one or more applications on the card, and each of these applications will need to connect with a card acceptance device, or terminal, containing the complementary terminal component of the application before it can be used.

- ***Security Domains***. In addition to the Issuer Security Domain, separate Security Domains can be established on the card to protect application providers or groups of applications. Security Domains enable the applications of various providers to share space on a card without compromising the security of any particular provider or application.

  Security Domains also allow the application owner to control its applications without the Issuer having to share its keys with the provider. The use of Security Domains is ideal when the Issuer is dealing with a trusted provider who is capable of maintaining its own applications. This prevents the Issuer from incurring the administrative overhead associated with monitoring and controlling applications which are not part of its core business.

  Security Domains may be implemented such that they can perform delegated management functions. In order for a Security Domain to perform these functions, pre-authorization must be given by the Issuer. Delegated management functions of the Security Domain include loading, installation and deletion of applications. Although the Security Domain initiates delegated management activities and its keys are used in the process, the Card Manager must verify that the Security Domain has the authority to perform the function. In addition, services of the Card Manager are used to carry out each of the delegated management functions.

  As shown in *Figure 5.3*, multiple Security Domains can coexist on the card.



5.1.2. GlobalPlatform Card and Application Life Cycle

One of the most innovative and useful features of the GlobalPlatform is its dynamic nature. Unlike other card architectures developed to date, the GlobalPlatform defines stages with clearly defined roles through which the card progresses during its "life." When a GlobalPlatform card is first issued, it will contain one or more applications. It will also contain the runtime environment and GlobalPlatform components described above, which are necessary to make the applications run. All of these components are loaded onto the card before it is issued. Once a card has been issued, special security is needed to load any further applications on the card. If a security threat is detected after a card has been issued, the card can be temporarily or permanently locked by changing the life cycle state of the card.

Life cycle states of the Card Manager:

- OP_READY

- INITIALIZED
- SECURED
- CARD_LOCKED
- TERMINATED

The life cycle of an application is more complex than that of the card. Each application has its own life cycle state. The life cycle states of various applications on the card may be different at any given time. As different application may have different needs and different states in which they operate, the application is responsible for managing its own life cycle using the GlobalPlatform API.

The following life cycle states of an application are applicable to all applications and load files on a GlobalPlatform card:

- LOADED
- INSTALLED
- SELECTABLE
- Other application specific states
- LOCKED

Applications are loaded onto the card as application code ("load files" in the specification) and only become separate entities when they are installed. A loaded application resides on the card, but is not yet accessible. Once the application has been installed and made selectable, it is accessible by a terminal. It is then personalized and the cardholder can then use it.

An application can also be blocked from use by the application itself or locked by the Card Manager. The blocked or locked states, each of which is reversible, are used when a perceived security threat is detected by the application or the Card Manager. In addition, an application can be deleted from the card. If the deleted application code resides in mutable persistent memory space (EEPROM), which can be erased and written over, the memory is freed up for use by other applications.

The status of each application is independent. It is possible for several applications to reside on a card on which only some applications are actually operational.

5.1.3. GlobalPlatform Card Customization – Post-Issuance Card Content Management

The GlobalPlatform gives Issuers the power to manage and change the content of their cards while providing a mechanism to allow business partners to manage their own applications on the Issuer's cards as appropriate. However, the Issuer always has ultimate control of the card's content. Post-issuance card content management includes the ability for the loading, installation, and removal of card content. This content management and control is the responsibility of the Card Manager. Security Domains with delegated management privilege can make requests to the Card Manager for application loading, installation, and deletion, but the Card Manager decides whether or not to act upon these requests.

Secure Communication. The Card Manager and Security Domains on GlobalPlatform cards are required to implement a secure method of communication that is referred to as the secure channel protocol. This protocol uses cryptography to enable secure communication between the Card Issuer and Card Manager, between application providers and their Security Domains, and between application providers and their applications. The secure channel can ensure both integrity (that the information in the command has not been changed) and confidentiality (that the information cannot

be read by outside parties). Authentication, which is a method of positively identifying the party with whom you are communicating, is required to open a secure channel.

The Issuer's policies define the use and level of secure communication. For example, during the post-issuance phase of a card, a secure channel that performs integrity checking may be required and if the card is operating in an open network such as the Internet, a secure channel ensuring both integrity and confidentiality may be required.

Application Management by the Card Manager. All loading of new code to a GlobalPlatform card uses load files, containing application code, that are transferred to the cards. A load file that has been loaded to a card is stored in the card's memory; however, any applications contained in that load file are not yet ready for execution. An application must then be explicitly installed from its load file before it can execute. This may occur immediately following the loading phase or at some time in the future. Following installation, the Card Manager registers information in the card registry regarding life cycle status of the application. Issuers are able to remove applications from erasable memory and to logically delete application code from non-erasable memory.

Delegated Management by Security Domains. Delegated management allows application providers to load, install, and delete their own applications (load and install require pre-authorization from the Card Issuer). This pre-authorization involves digital signing of the command by the Issuer and subsequent verification by the Card Manager. The Card Manager checks the signature on the command using the Issuer's keys. Because the signed command contains a hash of the load file, the signature also ensures that the load file has not been altered. It is important to note that although the application provider's Security Domain manages this process, the Card Manager actually performs the physical loading and installation of applications into memory.

5.2. GlobalPlatform Device Specification

While the *GlobalPlatform Card Specification* focuses on the architecture within the smart card component of an application, GlobalPlatform also places significant emphasis on the device. By providing specifications for devices in addition to specifications for cards, GlobalPlatform recognizes the vital role devices play in enabling cardholders and Card Issuers to actually put their cards to use.Without devices, cardholders would have little ability to perform transactions. To ensure that the best and most appropriate devices are available for GlobalPlatform implementation, GlobalPlatform technology includes device software specifications to guide device manufacturers and application developers in programming GlobalPlatform devices. The *GlobalPlatform Device Specification* leverages the STIP specifications (initially owned and developed by the STIP Consortium and now owned and maintained by GlobalPlatform) and defines a specific Framework API to expedite device application development.

5.2.1. GlobalPlatform Device API Specification Objectives

The STIP/GlobalPlatform Device Specification is designed to meet the following core objectives:

- ***Enable Acceptance of Single and Multi-Application Smart Cards.*** GlobalPlatform's device software architecture provides a framework and an API for device software that supports single and multiple applications in a single device. This will ensure greater convenience for customers, who can use a variety of the applications on their GlobalPlatform cards at one

location, and will allow Card Issuers and Acquirers to develop a more efficient card acceptance infrastructure.

- ***Enable Coordinated Development of Card and Device Portions of Smart Card-Based Applications.*** GlobalPlatform devices are designed to support single and multiple smart card applications such as credit and debit financial applications, stored-value applications, and consumer loyalty programs. In the smart card world, these applications are split between the card and the device, which both perform critical elements of the transaction. Traditionally, device and card developers work independently to implement the device and card portions of the overall application. Using GlobalPlatform's Device Specification, in conjunction with GlobalPlatform's development and testing tools (see section 5.3), application developers can work in a more productive, coordinated manner to develop both parts of the complete application from a single functional specification.

- ***Enable Development of Portable Device Applications.*** Using the GlobalPlatform Device Specification, an application developer can write a significant portion of the device code once, and install it on any number of different GlobalPlatform devices. This application portability reduces the development cost and effort required to support the wide range of device types that will be included in GlobalPlatform systems.

By meeting these objectives, the GlobalPlatform Device Specification significantly reduces the cost and complexity of implementing chip-card programs, while greatly increasing their utility.

5.2.2 GPD/STIP Compliant Device Components

The basic components of a STIP compliant device include:

- ***Device Operating System and services***. Just as each card has its own operating system, each device also has a proprietary operating system used to access the basic services provided by the device. The main difference with a usual card OS is that a device has many more services and peripherals to offer such as: cryptography, UI, storage, serial and Internet communication, smart card slots, etc.

- ***STIP Runtime Environment (STIP RTE)***. Having similar function to the Virtual Machine in the card, the device's STIP RTE is used to run the device component of an application and enable the communication between the service controls defined in the API and the actual services provided by the OS.

- ***STIP Core Framework API Implementation***. This is a fundamental framework API that allows the application programmer to deal with all services in a similar way. For this, the STIP Core Framework defines a generic notion of ***service control***. A service control is the only means of access to a service for an application, once the service control has opened a connection with the real service. Through service controls, the application communicates with services in a systematically asynchronous request/event response manner.

- ***STIP Profile APIs Implementations***. The STIP Specification defines as a ***profile*** the set of service controls interfaces to be integrated in the STIP Core Framework. Which sets of service controls are provided in a profile is related to the particular industry to which a device belongs. Currently, three STIP profiles have been defined: EFT-POS profile, Mobile phone profile and FINREAD profile (defined by the FINREAD consortium). To ease portability from one profile to the other, all profiles use the same service controls to address similar services. In particular, the

smart card slot service control is common to all profiles (and assumes the underlying slots drivers are ISO and EMV compliant).

- ***Application Management***. Just like the cards, GlobalPlatform devices can support multiple applications. The installation, life-cycle management and selection of applications are not specified in detail in the GlobalPlatform Device Specification and remain to be precisely specified on a per industry basis. However, the STIP API provides a particular API to activate applications (stiplets). In addition, an ongoing work effort is dedicated to the scripting processes to inform the platform of the rights and needs of each application. This work also defines the notion of ***protection domains***, similar in many respects to the notion of security domains for the card specifications.

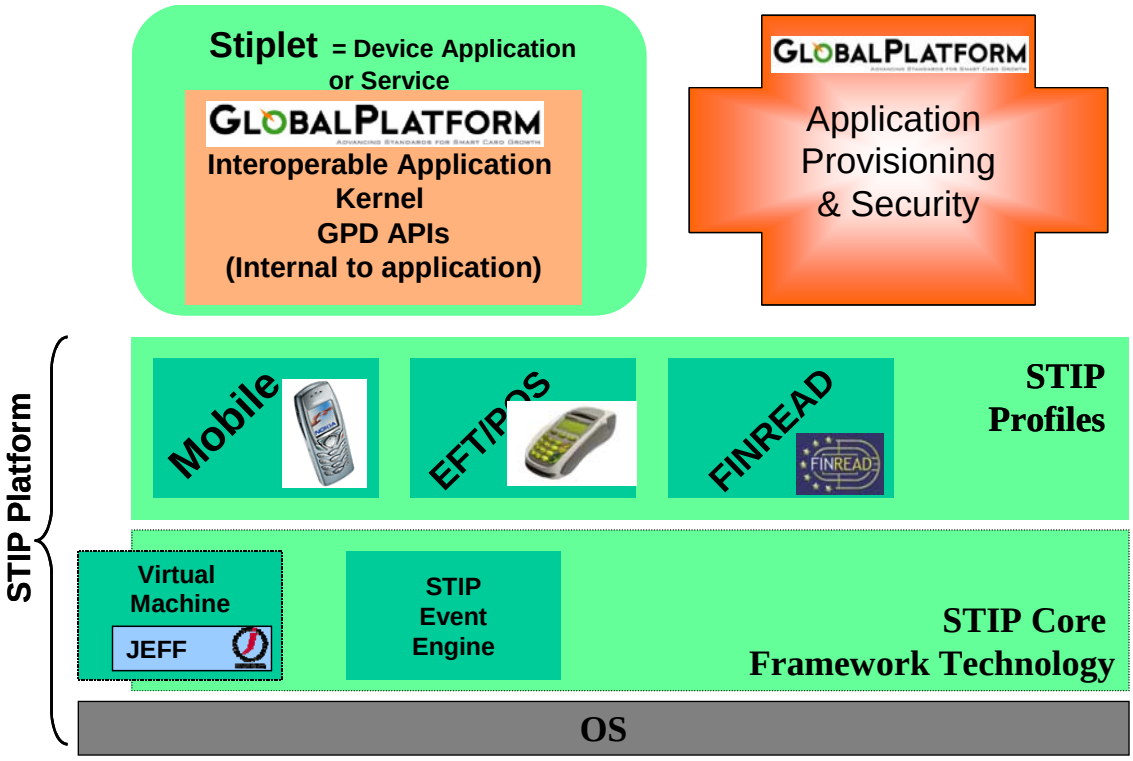


Figure 5.3: GP/STIP Device Components

Like the card specifications, the STIP/*GlobalPlatform Device API Specification* is available for application programmers to use in developing device applications. Several key device vendors are already in the process of developing GlobalPlatform devices, and more are beginning to follow. Soon there will be an adequate supply of GlobalPlatform devices in addition to the already numerous EMV compliant terminals which can be used in GlobalPlatform implementations.

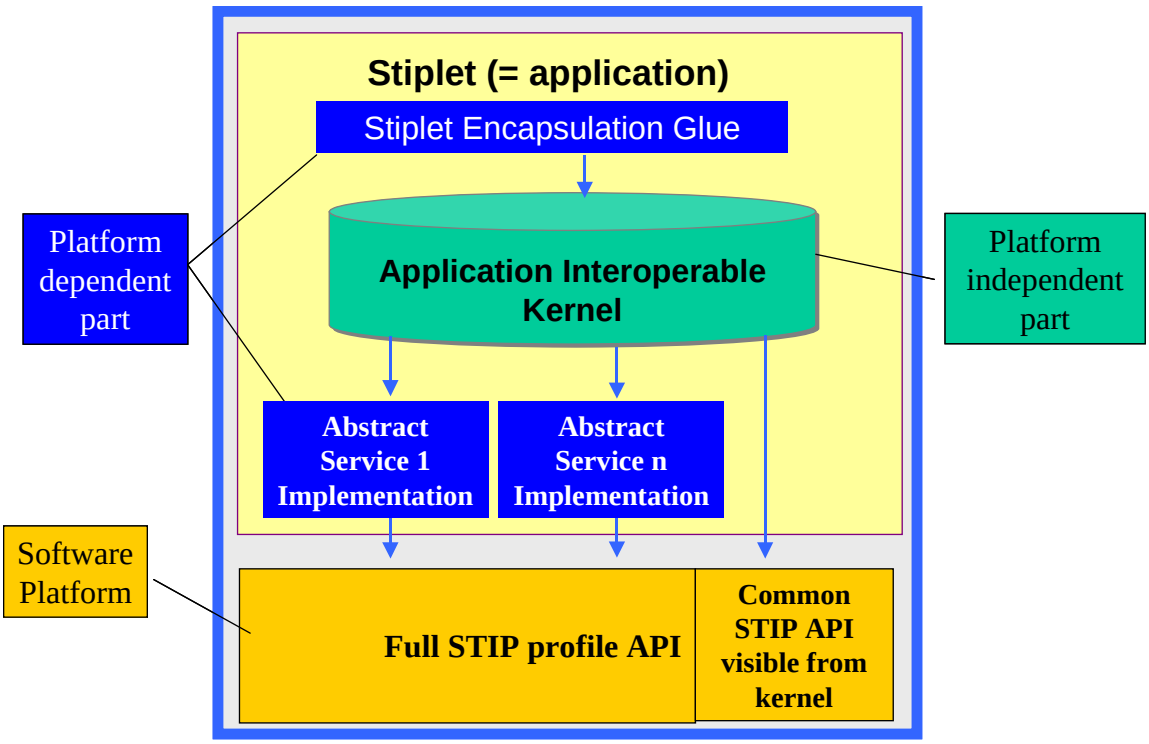
5.2.3. GlobalPlatform Device Application Architecture

In addition to the STIP Core Framework and Profiles API, the GlobalPlatform Device Specification also defines an architecture – the internal organization of the software – for the design of a device application(stiplet).

In most smart card systems, the same smart card-based application is likely to be implemented in several different places. For example, an Issuer might wish to issue e-purse cards that can be used at a wide variety of locations, from gas stations, to fast food vendors, to the cardholder's home computer. Given the differences between these various locations, each is likely to use different STIP profiles, and in each profile different features, such as communication protocols with the host or the UI preferred language.

To reflect the fact that some parts of the application software are the same in different implementations while some parts may differ, the GlobalPlatform Device architecture is composed of two main components: the *environment-dependent* component and the *environment-independent* component. The independent component is called the *Core Logic Component* (CLC), which contains all the environment-independent code. The CLC can access common STIP service control APIs and the STIP core framework API that is provided by any of the STIP profiles. The CLC also uses abstract service control APIs that are environment-dependent. The CLC is completed by the application integrator for each kind of environment with the implementation of these abstract service controls (using the actual service controls provided by the targeted STIP platform).

The basic components of an application according to the GlobalPlatform Device architecture are illustrated in *Figure 5.5*,



5.3 GlobalPlatform Systems Specifications

Smart cards provide a great deal of flexibility and utility. At the same time, however, they introduce a degree of complexity that requires that the card base be managed. The GlobalPlatform

Systems specifications, guides, and requirements documents offer a comprehensive off-the-card architecture to address these complexities. The architecture addresses requirements of software systems, defines technology to aid the smart card customization process, and a common means of exchanging information between the systems required to issue and manage single and multi-application smart cards.

The GlobalPlatform systems documentation helps the issuer or software architect in defining a stable architecture able to support the evolution:

- from a native card to a GlobalPlatform card
- from single to multi application,
- from one unique card or application profile for all the cards issued to one profile per card managed

5.3.3 High Level Description and Diagram

The key components of an off-the-card infrastructure needed to issue and manage a smart card are personalization systems, smart card management systems and key management systems. In a multi application world with multiples entities, application management systems will help the overall management regrouping application specific management. While these components may exist as standalone systems or an entirely integrated product, they are nonetheless critical to the initial production of mass customized smart cards and the ongoing management of these smart cards.

For the initial step of card issuance, cards need to be customized for a particular cardholder using a combination of data preparation and smart card personalization tools, under the general umbrella of personalization systems. GlobalPlatform Systems defines in the **GlobalPlatform Systems Profiles** and **GlobalPlatform Scripting Language** Specifications, respectively, detailed content formats and programming interfaces to enable the creation and dissemination of portable and reusable personalization instructions. While these two specifications define the technology, the **GlobalPlatform Systems Card Customization Guide** provides a set of recommendations to help facilitate the often dynamic world of personalization using the technology envisioned in these two specifications.

After the cards are issued, cards need to be managed as both issuer and cardholder needs may change. The critical system in this regard is the Smart Card Management System. As opposed to the personalization process, where precise detail is required in order to enable interoperability, the key requirement in card management systems is the presence of functionality needed to manage smart cards. The set of documents which define these requirements include the **GlobalPlatform Multi-Application Smart Card Management Systems Functional Requirements**, which offers a comprehensive view of functionality for managing true multi-application card programs.

Because security of the smart card infrastructure is closely related to the key management, a specific systems has been defined that is referred to as the Key Management System. The **GlobalPlatform Key Management Systems Functional Requirements** defines the particular key and cryptographic requirements for cryptographic keys used by both the GlobalPlatform smart card security architecture and GlobalPlatform applications.

Since each system needs to interact with systems not necessarily from the same manufacturer, the **GlobalPlatform Messaging Specification** provides a set of inter-system messages to coordinate and ease communication. In particular, this specification provides messages to facilitate the standardized exchange of data, requests and responses between the actual systems as well as the actual participants in the multi-application card program. This data exchange, and the use of requests and response messages helps fuel the smart card personalization and smart card

management tasks performed by personalization systems, smart card management systems, and key management systems.

The diagram below illustrates a sample multi-application architecture, *Figure 5.6*. Note the presence and interaction between the smart card management systems (SCMS), personalization systems (both data preparation and personalization systems), and key management systems.

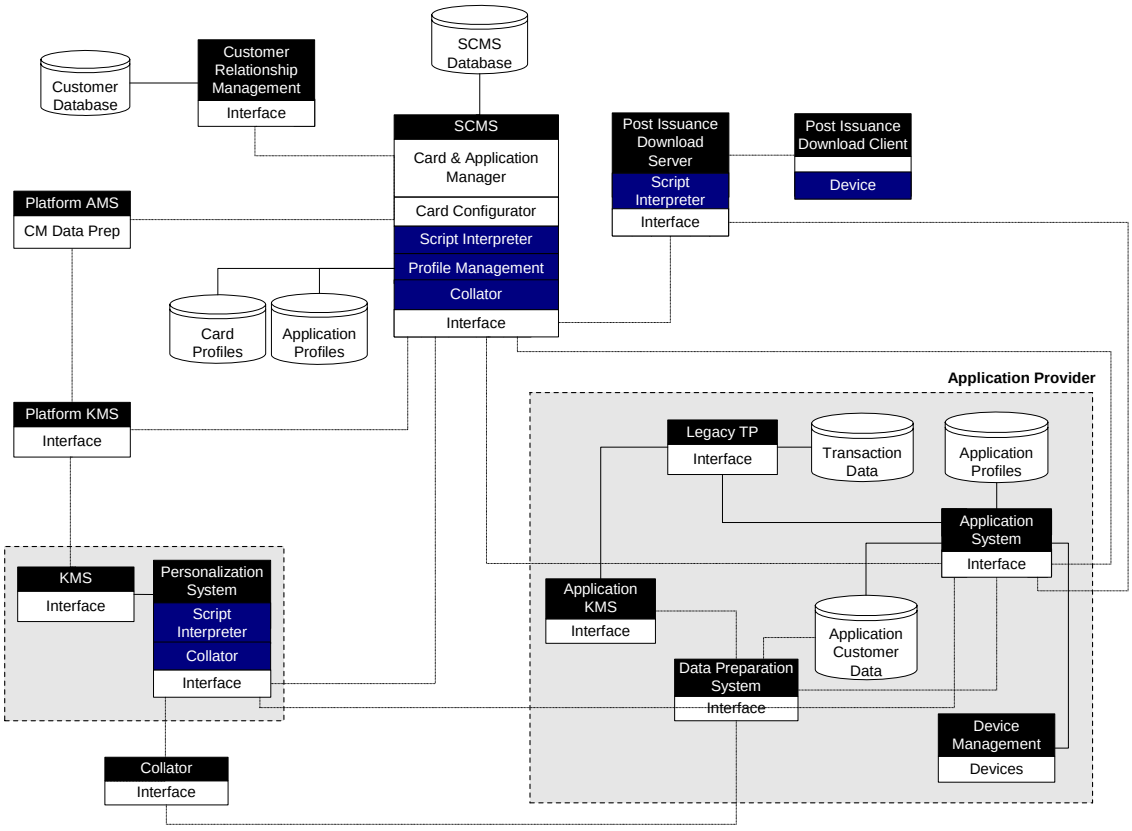


Figure 5.6: A Sample Multi-application smart card infrastructure

5.3.2 GlobalPlatform Systems Profile Specification

In GlobalPlatform multi-application smart card infrastructures, there are several systems that need to exchange information about smart cards, their applications, and the associated cryptographic and applet information which is necessary both to produce and manage an issuer's smart cards. This information, or content, will be provided in the form of separate collections of data termed GlobalPlatform Profiles for cards, applications, load files and keys. The two primary types of systems which will actively manage and utilize profiles are Smart Card Management Systems (SCMS) and Personalization Systems, as well as their related components.

The objectives of the GlobalPlatform Systems Profiles Specification focuses on the Application, Card, Key and Load File Profile:

- To define the structure and content of the data to be provided in Application, Card, Key and Load File Profiles to Smart Card Management Systems.

- To reference the scripts related to a specific profile and define the structure and content of the data to be used by scripts.

- To provide examples of potential implementation scenarios which illustrate the flexibility in which card management and card customization processes interacts, and the role of data provided by in the GlobalPlatform Scripting framework in this interaction.

- Coverage for GlobalPlatform Card Specification especially by supporting GlobalPlatform standard APDU commands and secure channel support.

GlobalPlatform Profiles possess the following properties:

- Ease of implementation, minimizing time spent on what data is sent and how it is structured;

- Supplied in a format which is easily distributable;

- Flexibility for future changes in content model or content additions per individual vendors, smart card issuers, or implementations;

- A specification supportable by the GlobalPlatform member community and actors involved in GlobalPlatform Smart Card implementations

5.3.3 GlobalPlatform Systems Scripting Language Specification

GlobalPlatform scripting is used to enable a common, portable, flexible, and extensible means of card customization. Card customization is defined in this document as the process of producing a card customized to a specific Cardholder and eventually modifying its contents after issuance to add and delete functionality. In that broad sense, card customization starts as early as application software is loaded onto a chip, ends temporarily with card issuance, and is re-enacted as soon as a new application is added (or deleted) or when some on-card data is updated post-issuance. Therefore, card customization includes loading applets, installing applets, data preparation, card issuance or pre-issuance personalization, post-issuance personalization, as well as verifying whether cards have been personalized correctly.

This work presents a choice of ECMAScript[1] and a set of objects for that language to facilitate the standardized exchange of card customization instructions for applications. These card customization operations, when designed using the ECMAScript language specified and the smart card specific scripting objects, become very portable instruction sets for use by a variety of card issuers across any number of smart card implementations.

As well, by having the language constructs of the scripting language ECMAScript at their disposal, application developers are given a flexible tool to develop scripts according to the manner in which

[1] Ecma International is an industry association founded in 1961 and dedicated to the standardization of Information and Communication Technology (ICT) Systems

they choose to prepare data and personalize smart cards. Hence, the GlobalPlatform scripting approach, as a tool for card customization, can create and personalize off of any data format as required, including CPS formats.

The objectives of this specification are:

- To provide a description of the role of GlobalPlatform scripting in card customization tasks;
- To describe the dependencies of GlobalPlatform scripting on GlobalPlatform Profiles for the creation of objects representing external data and keys;
- To identify the language used for GlobalPlatform scripting;
- To define what additional ECMAScript objects are required to implement GlobalPlatform multi-applications smart cards;
- To define the catalog of ECMAScript objects and describe the means of provisioning or instantiating such objects in order for scripts to be easily supported in environments with different processing capabilities, memory constraints, and communications bandwidth;
- To illustrate, through examples, how scripts can be packaged with GlobalPlatform Application Profiles.

The expected benefits of GlobalPlatform scripting in the GlobalPlatform card customization architecture will include overcoming all these limitations and:

- Facilitate the issuance of chip based applications by Card Issuers and Application Providers through standardization and open standards driven selection of the language to represent card customization instructions;
- Enable the accelerated deployment of smart cards, including multiple payment and value-added applications integrated into a single card, through the support of GlobalPlatform scripting through different issuance delivery channels (e.g. Personalization Bureaus, post-issuance systems);
- Facilitate high levels of security through standardized interfaces to cryptography and secure modules in the GlobalPlatform cryptographic object;
- Minimize operational impact of new applications through consistent processes, specifically the creation of scripts for a minimal set of card customization processes;
- Reduce time and costs for smart card customization through standardization of customization processes which traditionally have relied on proprietary processes and substantial systems integration efforts.

5.3.4 Key Management Systems

A Key Management System is a system to securely generate, store, distribute and delete cryptographic Key Values and attributes. A KMS is part of a larger system that requires

cryptographic Key Values. A Key Management System is typically a software based system making use of a hardware based cryptographic processor for secure operations, and consists of 4 elements:

- A database for storage of the Key Values and attributes
- Services to the systems needing Key Values – typically in the form of an API
- An HSM to ensure the secrecy and integrity of the Key Values and attributes, and also provide a resource for the mathematically intensive nature of Key Value generation
- Procedures – or more accurate man/machine interface supporting procedures

Except for the requirements for security and procedural support, a Key Management System is much like any other management system e.g. a Card Management System. At the heart of the system lies a Database storing the Data and an API giving access to that Data and the services associated with it.

The GlobalPlatform Key Management Functional Requirements define the minimum functional requirements required for the support of keys within the Security Architecture of GlobalPlatform and GlobalPlatform applications. Specifically, it expands the requirements for key management to include the requirements for cryptographic services.

The intention of GlobalPlatform KMS Functional Requirements is to serve as input to the GlobalPlatform Key Profile Specification, GlobalPlatform Messaging Specification and GlobalPlatform Scripting Specification providing a means to unambiguously identify the Key Values, the cryptographic services and the messages containing cryptographic methods, used within GlobalPlatform.

Furthermore it provides a GlobalPlatform view of the roles and responsibilities of the entities handling these keys.

5.3.5 Messaging Specification

Since each system needs to interact with systems not necessarily from the same manufacturer, the **GlobalPlatform Messaging Specification** provides a set of inter-system messages to coordinate and ease communication. When talking about entities involved in the different production life cycles of smart cards, it is important to define a common terminology for these entities (various roles and responsibilities). The objective of the first part of the **Messaging Specification** is to present a coherent Systems Architecture and its components in a simulated real world environment, while being able to distinguish these roles even though they are played by the same actors. This objective serves to define the information that they need to exchange with each other. The objective of the second part of the Messaging Specification is to standardize the format and data requirements when various components or actual participants of the single or multi-application Systems infrastructure are required to communicate.

The first part of the specification defines:

- Roles and responsibilities
- Information to exchange between these roles

- Dynamic of the exchanges

There are various actors involved in the production, distribution and maintenance of a multi-application smart card program. The first sections of the specification define a simple model describing the roles necessary in such programs. Actors are the entities responsible for playing roles (i.e., taking actions). Roles are the functions to be performed. Responsibilities describe more specifically the actions and the scope of actions that are performed.

An actor may perform dual or even multiple roles. For example, a Card Issuer could conceivably also be the Application Provider as well as the Loader. At a high level, an actor can also perform roles that appear similar or that may be identical. At a lower level of detail, the specific responsibilities of actors distinguish the roles they play.

In addition, several actors may combine responsibilities to accomplish a certain function. For example, while there may be only one actor responsible for application loading, the Application Provider or the cardholders have responsibilities that result in the initiation of application loading.

For each role, the specification defines the data that should be provided by other roles as well as the data to provide to other roles. The specification also defines the dynamic of the exchanged data between roles.

The following diagram, *Figure 5.7* depicts the various roles and the interaction between these roles as per GlobalPlatform Systems Architecture.

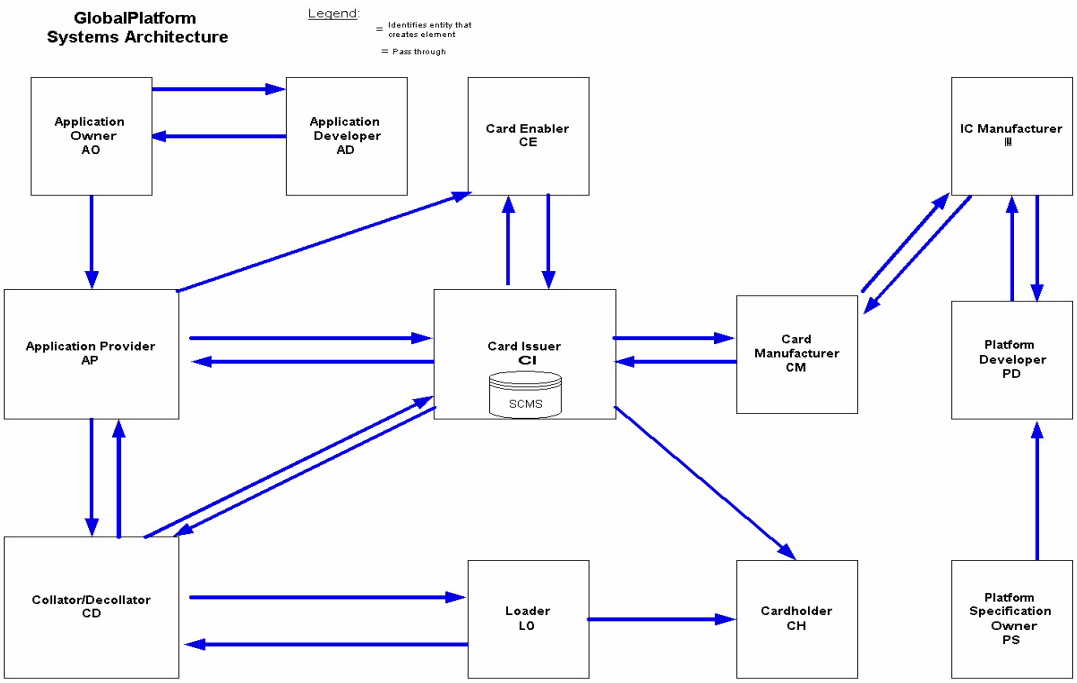


Figure 5.7: Messaging Specification Roles and interaction between these roles within the Systems Architecture.

The objective of the second part of the specification is to standardize the most common messages that will be exchanged between disparate systems in a GlobalPlatform smart card environment from a range of suppliers. By creating standards for these fundamental messages, the intention is to reduce systems integration impacts typically associated with constructing a "Systems architecture" from a variety of solution providers**.**

The messages can be characterized into two different categories:

- Messages for GlobalPlatform Profiles. These messages focus on card, application and key management interchange.

- Messages for GlobalPlatform Card Customization. These messages focus on personalization data preparation and personalization enablement including post issuance delete, load, install and personalization. This category includes audit trail messages.

The messages defined at this point are the ones that carry the following data:

- Message Header
- Application Profile
- Card Profile
- Card Profile Changes
- Key Profile
- Key Profile Exchange
- Load File Profile
- Profile Request
- Application Data Notification
- Application Data Request
- Card Customization
- Batch Card Customization
- Application Audit Trail
- Batch Audit Trail
- Card Audit Trail
- Error

Most of these messages could be used in pre-issuance as well as post issuance life cycle of the card and some of them are mostly used only in pre-issuance scenarios.

Extensible Markup Language (XML) is the language of choice to structure messages. XML provides the flexibility and standards based approach that messages require in order to be unambiguous, support different versions of messages as they evolve, and be conducive to ease of information parsing and maintenance. XML as a choice to represent messages is an open approach that should be tenable to everyone involved in smart card implementations.

5.4. GlobalPlatform Solutions

A framework of solutions has been developed to assist Issuers, Acquirers, card manufacturers and application developers in developing, testing, issuing and accepting GlobalPlatform cards. These solutions are summarized below.

- ***Application Development Tools***
- ***GlobalPlatform Device Tools***
- ***GlobalPlatform Card Compliance Tools***
- ***GlobalPlatform Card Production Solutions***

5.4.1. Application Development Tools

Application development tools are available to assist programmers in coding, debugging, loading and testing new applications for GlobalPlatform cards. Sources of application development and testing tools are as follows.

- *Card platform developers* offer development kits for applications being developed for use on GlobalPlatform cards. For Java Card, compatibility with the *Java Card 2.1* or *2.2 API* is mandatory to ensure application portability. These development kits typically include a software environment for application development, a compiler, test cards, an application loading tool and a diagnostic tool.

- *Commercially available software* is offered to facilitate development in the environments supported by the GlobalPlatform. These tools can be used by GlobalPlatform application developers because the GlobalPlatform utilizes common development platforms, such as Java. Information on Java development tools can be obtained from Sun Microsystems' web site at http://industry.java.sun.com/solutions.

- *Developer Guidelines.* GlobalPlatform provides an application developer's guide and sample GlobalPlatform code for Java Card based GlobalPlatform cards.

- *Card Compliance Program*. GlobalPlatform in conjunction with ICC Solutions provides a comprehensive Card Compliance Test Kit that provides debugging and testing for new GlobalPlatform card products.

Together these tools can be used to facilitate development, debugging and basic testing of GlobalPlatform applications.

5.4.2 GlobalPlatform Device Tools

In addition to the specifications, GlobalPlatform provides the following tools and documentation for help in programming stiplets and CLC modules: A comprehensive user's guide with examples and a PC implementation of STIP is available and can be used as a pedagogical tool to understand and test stiplets. Full-fledged development environment are also available from third-party providers. A Device compliance test-plan is under development, which will open the way to third-party provided compliance testing tools.

5.4.3 GlobalPlatform Card Compliance Tools

GlobalPlatform cards are currently provided by the world's leading card manufacturers, providing a choice of suppliers and card functions.

A GlobalPlatform Card Compliance Program is available for debugging and testing new GlobalPlatform card products. This Compliance Program comprises the following components:

- **Compliance Packages**: A document providing information on the core functionality that must be supported by all card products claiming compliance to GlobalPlatform Card Specification and information on the optional features of the specification that a card product may support.
- **Test Plan**: A detailed test specification describing the testing scenarios that verify the functionality of a GlobalPlatform card.
- **Test Suite**: A comprehensive set of Test Scripts, Configuration Files, Batch Files and Test Applets implementing the different test conditions and test scenarios defined in the Test Plan.
- **Test Tools and Test Environment**: Software and any specialized hardware required to execute the Test Suite as well as to capture and make available for review the test results.

GlobalPlatform defines the mandatory functions of the GlobalPlatform Card Specification that must be supported by all compliant card products as well as the optional features that may be supported by a particular card product. The GlobalPlatform Card Specification is not specific on mandatory features; therefore they are defined in the document: *GlobalPlatform Card Specification 2.1 Compliance Packages*.

5.4.4. GlobalPlatform Card Production Solutions

Systems developers have developed commercially available system solutions for application loading, application messaging, application load and personalization, post-issuance card updates, and card management using concepts presented in the GlobalPlatform specifications. These solutions can accommodate card issuance quantities ranging from moderate sized pilots to large-scale rollouts.

- GlobalPlatform defines a standardized process for *Application Loading*. Once a solution is developed according to this process, it can be utilized to load all types of applications. Currently, solutions for pre-issuance application loading utilizing the most popular personalization equipment and post-issuance application loading over the Internet have been developed.
- The *Card customization guidelines* of GlobalPlatform describe a standardized approach to card issuance and personalization. Using several example systems, this approach is diagrammed below for pre-issuance personalization.

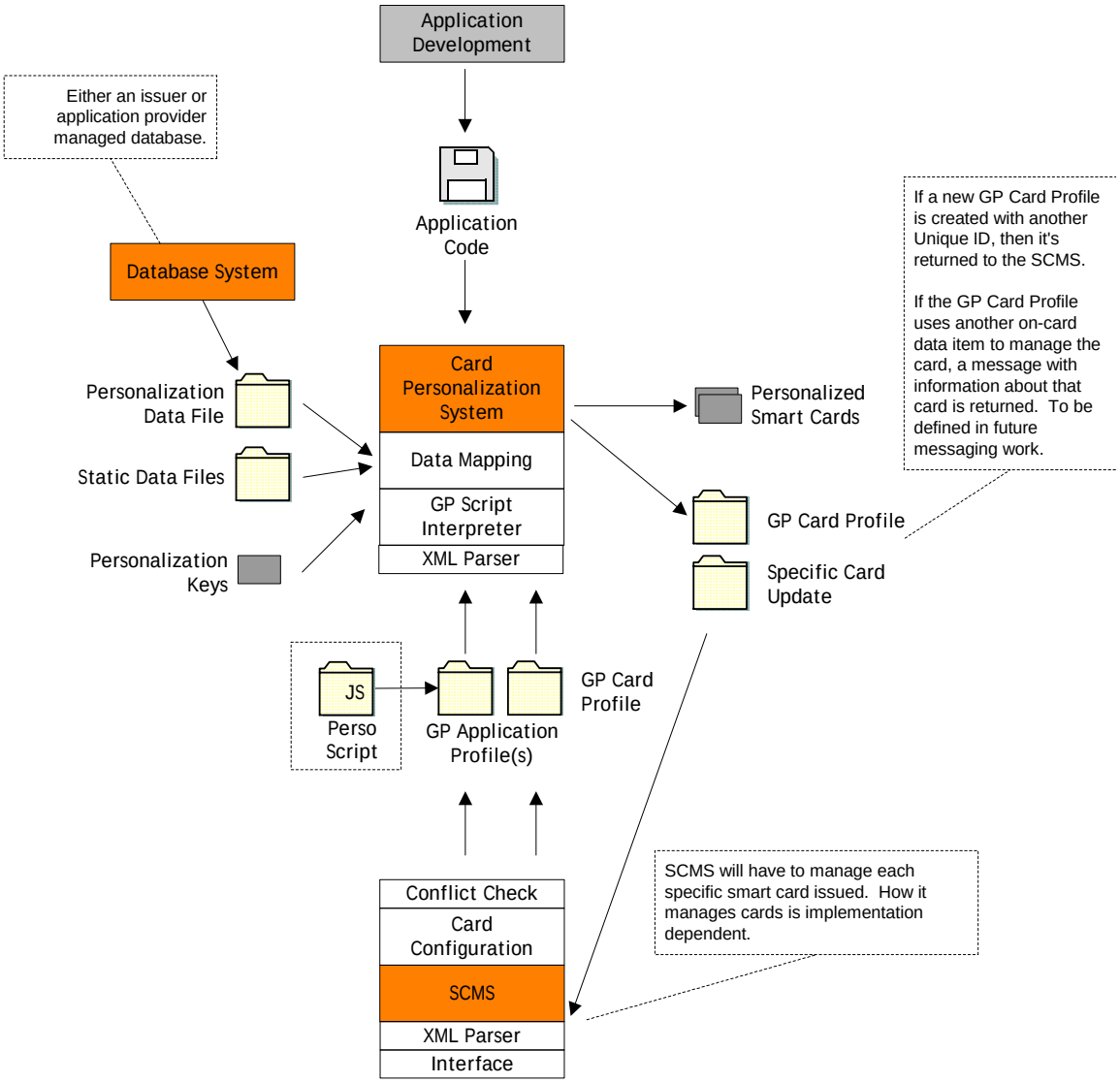


Figure 5.8: Pre-Issuance Personalization Process

In this process, two primary types of profiles, application profiles and card profiles, are used to design cards. The application profiles contain information about applications, such as code size, data size and security requirements. The card profile defines the characteristics of the card, including memory capacity, communication protocol and cryptography supported. Standard XML tools which allow the application provider and card manufacturer to easily create application and card profiles in a consistent format are readily available.

The application profiles contain personalization scripts. However, prior to executing a script, the card and application profiles are compared to ensure that there are no conflicts. The personalization scripts specify the cardholder specific data provided by the card Issuer to the personalization system.

The personalization process using GlobalPlatform system standards described here is standardized, so that application providers and card manufacturers have an open and predefined method to provide inputs to personalization. The process is flexible enough to accommodate single and multiple applications.

- *Post-Issuance Loading Tools* are available to support multiple distribution channels, including personal computers, mobile phones and public kiosks. Several suppliers will offer post-issuance loading tools as a product and some will offer it as a service.

- *Card Management Systems* are available to support cardholder bases with a high degree of variability. This variability can result from cards being tailored to individual cardholder needs at the time of issuance by placing the applications most relevant to that cardholder on the card. It can also result from post-issuance updates to the card which result in applications being added, upgraded or deleted. Card Management Systems interface to critical Issuer systems such as Cardholder Information Systems and Customer Services Systems, allowing the Issuer to always know the current status of the card at critical points in its cardholder processes. There are numerous card management systems available on the market which support GlobalPlatform smart cards and varying degrees of GlobalPlatform systems technology.

6. Getting Started Today

Developing applications for the GlobalPlatform is flexible and simple. It can be done very inexpensively because there are no license fees for developing applications for GlobalPlatform cards. Developers can download a sample GlobalPlatform implementation from GlobalPlatform's web site at (http://www.globalplatform.org). This sample implementation simulates the functionality of a GlobalPlatform card, and can be used by application developers to debug and test their applications during development, without needing to have an actual card available. There is also a *Developer's Guide* which can be downloaded from the site to assist programmers in developing applications for GlobalPlatform cards. In addition, the specifications for GlobalPlatform cards, devices, and systems are available.

7. Glossary

APDU (Application Protocol Data Units)	Standard communication messaging protocol between a card acceptance device and a smart card.
API (Application Programming Interface)	A standardized set of methods for a programmer to take advantage of (i.e. interface with) the capabilities of the card or device. The API is essentially a set of tools or services commonly used by applications on a card or device.
Application Provider	Entity that owns an application and is responsible for the application's behavior.
Business Logic	Business Logic Layer exercises the highest level of control over the operations of the terminal. The Business Logic Layer is principally responsible for selecting an appropriate application to activate, both in the card and in the terminal. The Business Logic Layer is also responsible for implementing local policies. Split tender purchases, for example, may be an accepted practice in some places, but not allowed in others.
Card Manager	An on-card agent within the GlobalPlatform card which enables the Issuer to maintain and exercise control over the card. This agent controls which applications can be loaded onto the card after it has been issued.
Chip Logic Component	The Chip Logic Component (CLC) Layer contains all the environment-independent code. The CLC Layer includes a module for each application the terminal supports. It is in the CLC Layer where the device component of each application resides.
Common Criteria	A public shared security standard, on which card industry leaders are cooperating. This will be the standard to which most smart cards will be tested in the future.
EEPROM (Electronically Erasable Programmable Read-Only Memory)	Memory that can be erased and reused, but does not require electrical power to maintain data. It is used primarily to store information that will change, such as transaction counters.
EMV	Technical Specifications developed jointly by Europay, MasterCard International, and Visa to create standards and ensure global interoperability for use of Chip technology in the payment industry.
Environment Services	These services provide a consistent interface to a set of resources commonly found on many chip-card terminals.
ISO 7816	The ISO (International Standards Organization) standard which governs contact based integrated circuit cards.

ITSEC	A regional security evaluation scheme. Based on assurance levels against private targets. Will be superseded by Common Criteria.
Java Card®	The smart card runtime environment developed by Sun. Based on Java.
GlobalPlatform	The industry standard for managing a smart card based single and multiple application program. Includes card specifications, device specifications, and systems specifications.
GlobalPlatform API	Through the services contained in the GlobalPlatform API, all applications can be created and accessed in a uniform way.
Post-Issuance Loading	The loading of applications to a card after the process of personalization and card issuance has taken place.
Runtime Environment	The Runtime Environment consists of three basic components. These are the Card Operating System, the Virtual Machine and the Application Programming Interface (API)
Security Domain	Security Domains can be established on the card to protect application providers or groups of applications. Security Domains enable the applications of various providers to share space on a card without compromising the security of any particular provider or application.
Virtual Machine	A Virtual Machine acts as a translator, converting instructions of the application into unique commands understood by a specific type of card. A Virtual Machine enables application portability.
Windows® for Smart Cards	The smart card runtime environment developed by Microsoft. Based on common Windows/Visual Basic tools and principles.