GLOBALPLATFORM
THE STANDARD FOR SMART CARD INFRASTRUCTURE

The GlobalPlatform Value Proposition for Biometric Match-on-Card Verification

White Paper
March 2009

secretariat@globalplatform.org | www.globalplatform.org | © 2009 GlobalPlatform Inc.

The GlobalPlatform Value Proposition for Biometric Match-on-Card Verification

Contents:

Appendices:

About GlobalPlatform

GlobalPlatform is the leading, international association, focused on establishing and maintaining an interoperable and sustainable infrastructure for smart card deployments. Its technology supports multi-application, multi-actor and multi-business model implementations, which delivers benefits to issuers, service providers and technology suppliers.

GlobalPlatform Specifications are freely available and have been adopted worldwide by many public and private bodies. As of October 2008, there were an estimated 305.7 million GlobalPlatform-based smart cards in circulation across the world and an additional two billion mid range USIM/SIM cards using GlobalPlatform technology to enable over-the-air (OTA) application downloads for 3G and GSM mobile networks. These figures are expected to increase significantly throughout 2009.

GlobalPlatform is an independent, not-for-profit organization and its strategy is defined and prioritized by a Board of Directors. GlobalPlatform is currently chaired by Sebastien Tormos, Vice-President of Marketing, Datacard Group, and vice-chaired by Marc Kekicheff, Vice President Product Technology, Visa Inc. Kevin Gillick serves the membership on a full-time basis as its Executive Director.

For further information, visit www.globalplatform.org.

Publication Acknowledgements

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

Participants include:

GlobalPlatform Full Members:
- Dominic Fedronic – ActivIdentity
- Eric Le Saint – ActivIdentity
- Gil Bernabeu – Gemalto
- Patrice Plessis – Gemalto
- Emmanuel Mellery - NXP
- Marijke de Soete – NXP
- Marc Vauclair – NXP
- Jean-Loup Depinay – Oberthur

Participating Members:
- Julien Bringer – Sagem Sécurité
- Ludovic Merrien – Sagem Sécurité

Observer Members:
- Doug Black – Collis
- Jonas Andersson – Precise Biometrics

Public Entity Members:
- Shawn Elliott – US Department of Defense (Contractor Support)
- Eric Hildre – US Department of Defense (Contractor Support)
- James Hutchinson – US Department of Defense (Contractor Support)
- Chris Miller – US Department of Defense (Contractor Support)

GlobalPlatform team:
- Kevin Gillick – Executive Director of GlobalPlatform
- iseepr – PR agency and copywriter
- Alliances Management – Operations Secretariat

Executive Summary

Biometric technology has evolved significantly and has become one of the most convincing ways to confirm the identity of an individual. As the use of passwords and personal identification numbers (PINs) becomes increasingly widespread, public and private sector organizations are looking for new ways to verify an individual's identity without compromising the security of the services it delivers or the privacy of the individual; could biometric technology be the answer? Today, the technology is a fundamental element of identity management for governments, and plays a central role in government-to-citizen programs, such as ePassports and eID, and in government-to-employee schemes worldwide.

The appeal of biometric technology is that characteristics, such as fingerprints, are uniquely bound to one person. However the success of the solution depends on the strength of the whole biometric system, which includes various components and processes supplied by different organizations. The risk is that unique, private biometric material is intercepted by an unauthorized third party. Such a risk, together with the complexity of biometric technology and also the intimacy of the biometric material has resulted in society becoming apprehensive of its use.

Reluctance against biometrics usage also stems in part from the historical and strong association to criminal investigation and custodial environments. Lack of differentiation in how the technology is used will unavoidably create bad perception and confusing messages about privacy. It is crucial, therefore, to explain that valid scenarios for biometrics will offer many benefits to users who expose their fingerprints to the system, and will be issued in accordance with all legal requirements.

Biometric match-on-card technology addresses many of the privacy and security concerns if implemented correctly. This technology allows an individual's biometric template to be stored in a non-extractable manner on a smart card (or similar secure element) rather than a large central database, enabling the end user to be in control of their biometric material at all times. This enhances privacy significantly, provided the match-on-card process is properly protected by the card. As the biometric detail is not only stored within the card but also processed there, the communication between components is mostly confined to a more controlled ecosystem. This makes it possible to securely deploy an on-card verification method in environments where many 'untrusted' terminals are present, such as personal computers, however at the cost of increased card security and higher performance requirements.

Other biometrics solutions that store biometric material such as the ePassports do not perform match on the card, but on trusted biometrics terminals. Such deployment models offer good security characteristics and accuracy, but require these terminals to be secured and attended. This is the case, for example, in most ePassport applications, and is critical for national security reasons. The model is successful as the number of checkpoints is relatively low and strict procedures are defined by authorities which limits the risk of compromised inspection systems. As such, verification on the inspection system may be cost effective. This architecture, however, cannot be utilized in an open environment.

It should be noted that these trusted biometric terminals have security chips to perform their cryptographic operations. It could be argued that GlobalPlatform would provide a very useful management framework for these chips, which in many cases today are custom and proprietary. However, the scope of this white paper will focus solely on scenarios where the

‘match’ is performed on the end user’s card, as opposed to another secured chip, and the root of trust is consequently the user’s card.

This white paper explains how GlobalPlatform’s existing and proven infrastructure delivers the required security and privacy to enable the deployment of a secure, interoperable and flexible biometric match-on-card ecosystem. GlobalPlatform technology enhances privacy by specifying the necessary interfaces and requirements for cards, devices and system components to build a trusted, complete and deployable biometrics match-on-card verification solution.

The document further details the value of implementing such a solution using GlobalPlatform Specifications from research and development cost savings and improved time to market, to compliance with industry security requirements. The white paper also outlines how GlobalPlatform on-card access control technology can facilitate the delivery of multiple applications on one card, with each application able to securely utilize the match-on-card biometric in a flexible way without having to become biometric aware.

Different use cases where biometric match-on-card is central to project implementation in the areas of national and employee identity, payments and mobile telecoms are also referenced.

This white paper is intended to be informational rather than technical in nature. This allows it to be accessible to program managers and consultants advising on the implementation of biometric programs, in addition to more technical audiences.

SECTION 1: Introduction to Biometric Technologies

During the last decade, fresh challenges faced by governments and commercial organizations have made verifying the identity of individuals more important than ever before. This has been motivated by a variety of security and privacy-related factors in areas including law enforcement, access control, social security, transportation, mobile telecoms and financial services.

Biometric technology has evolved to meet this need and is now at the center of major regional, international and national identity management projects globally. Biometrics, which literally means 'life measure', involves recording and comparing a template of an individual's unique physical characteristics or behavior to verify their identity. It is also generally used in the context of a multi-factor authentication scheme, that is, one using two or more pieces of information in the verification process.

Several types of biometric characteristics can be used depending on their intrinsic reliability, security and user acceptance relating to a particular application. They include face, iris and retina (eye) characteristics, fingerprint patterns, hand geometry, vein pattern, voice patterns and signature dynamics. Despite the variety of characteristics, the systems that measure differences between people have essentially the same architecture and many factors are common across several biometric processes. A detailed examination of each characteristic and its measurement can be referenced in Appendix A.

1.1 The Biometrics Ecosystem

It is important to remember that a biometric measurement is an identity trait – it is not an authenticator. It is the whole system that transforms the identity trait into a credential that can be verified. The integrity of the credential is measured by the strength of the whole system, which in turn is only as strong as its weakest part. Therefore the level of assurance of the whole system is determined by the security and quality of each of the components and the security of the communication between those components.

A standard biometric ecosystem is shown in Figure 1. It illustrates the individual components and flow of data in a typical biometric authentication. For a detailed description of actors in a biometric ecosystem, see Appendix B.

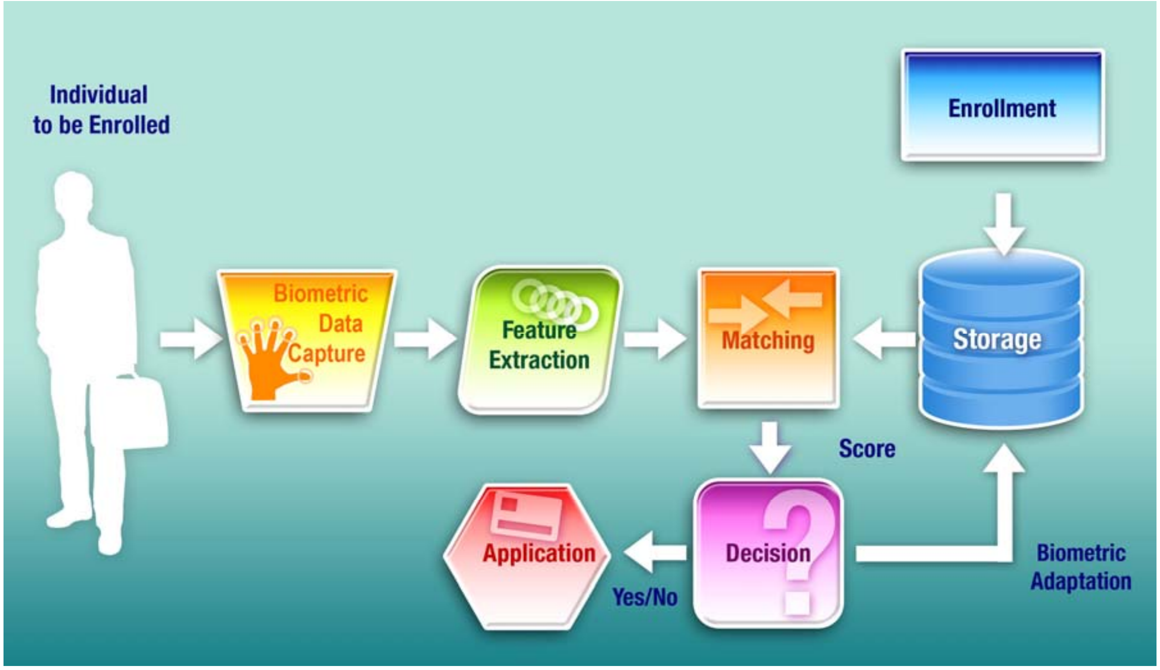

Figure 1: The biometrics ecosystem

Enrollment– The first step for any biometric authentication solution is the enrollment of the individual user to the system. The system will capture data or images specific to the type of biometric characteristic being used, extract unique features into a reference template and bind the reference template to the person’s identity. Best privacy practice requires that the reference template be stored transiently before it is stored in the end user’s smart card

Even so, the captured biometric may also be registered and the template stored in a large central database, such as a Automated Fingerprint Identification System (AFIS), to ensure the identity record is not duplicated and no identity fraud occurs. The existence of this database raises privacy concerns that necessitate additional security measures to protect the biometric data. It is therefore vital that the database is operated diligently and by a competent officer.

The enrollment process is the foundation of an identity chain of trust and therefore must be undertaken by a trusted officer using a trusted infrastructure to assure individuals that the data cannot be compromised and information is not cloned. The chain of trust requires vetting the individual’s identity from the captured biometrics, signing the biometric template by a digital signatory or registration authority, and storing the biometric reference template on the card in a confidential and private manner. This allows an individual to prove their identity quickly and efficiently in the future.

After enrollment, a biometric verification system consists of the following components:

Data capture - When verification of the individual is required, the user must present the required characteristic to a biometric data acquisition system, for example a fingerprint sensor, which captures an image.

Feature extraction – The image is presented to a component which will extract unique features from the image into a verification template according to the type of biometric methodology selected.

Storage – The reference template is retrieved from its secure storage system within a central database or within a token that is carried by the user such as a smart card or an embedded chip in a mobile phone.

Matching - A matching component will then compare the verification and the reference templates and produce a similarity score.

Decision making – The decision making component will apply pre-defined policies and business rules to the score. The result of the decision has to be communicated to the requesting application. For example, this could be a payment application or physical access to a building.

Biometric adaptation – The accuracy of the biometrics reference template slowly decays over time as the human body evolves. This means that the stored biometric reference template will periodically need to be refreshed. However, during the decision making process, a sophisticated system can record such changes to ensure the highest level of precision and reduce the need to re-capture an entire biometric template. This method is most suited to identification schemes on servers, as in match-on-card systems the high level of security afforded to the template and the trust in the initial enrollment can potentially be compromised during the process of adaptation.

1.1.1 Defining User Identification and User Verification

It is important to draw a distinction between user identification and user verification in terms of the scale of deployments and the cost of securing the biometric element. In the case of user identification, an individual simply enters a new sample of their characteristics, which is then compared to an existing database of templates to find a match (one-to-many comparison). If a match is not found, a record may be created in the database. User identification typically uses biometrics in large central database implementations, such as AFIS for civil or criminal use. These systems are designed to uncover the identity associated with a biometric template quickly and efficiently, detect record duplication and prevent identity fraud.

User verification relates to access control. An individual similarly enters a new sample of their characteristics, and this is then compared with the user’s stored reference template which would have been captured and approved during the enrollment process (one-to-one comparison). This verification can be conducted in a distributed way, for example the sample is compared with the stored template held within a chip card, or using a central database where the biometric is stored with the necessary reference / index. In either case, provided the reference template and the new sample are sufficiently similar to each other, the system will verify the user and permit access to the application.

Obviously, the one-to-one comparison for verification requires much less processing power, and constitutes the essential use case for on-card biometric.

1.2 Analyzing the Biometrics Ecosystem

1.2.1 Acceptable Tolerance Levels

The use of passwords and PINs as a verification method is based on actual values and, as a result, the outcome of any verification process gives an absolute response – either correct or incorrect. However, biometric methods – both behavioral and physiological – use variable values, and matching will be *almost* right, *almost* wrong or in many cases a scale in between.

No matter what biometric characteristic is used, it is extremely unlikely that the reference template and the new image offered by the user will produce an exact match. This is due to two factors: characteristics change over time and they record differently depending on the environment. For example, it would be virtually impossible for a fingerprint to be placed in exactly the same position, at the same angle and with the same pressure each time an individual is verified to access an application. Similarly, varying lighting conditions can greatly affect the recording of a facial image.

The biometric process therefore aims to provide a defined level of confidence that access to the system is being given to a genuine user. As the level of confidence cannot be 100%, the biometric system must incorporate a degree of tolerance. This will be established depending on the needs of the user and the environment in which the biometric is being used. As a result, biometric technology is sometimes used in a multi-factor authentication scheme in conjunction with something a person has, such as an authentication token, and/or something the person knows, such as a password.

1.2.2 The Value of Biometric Match-on-Card

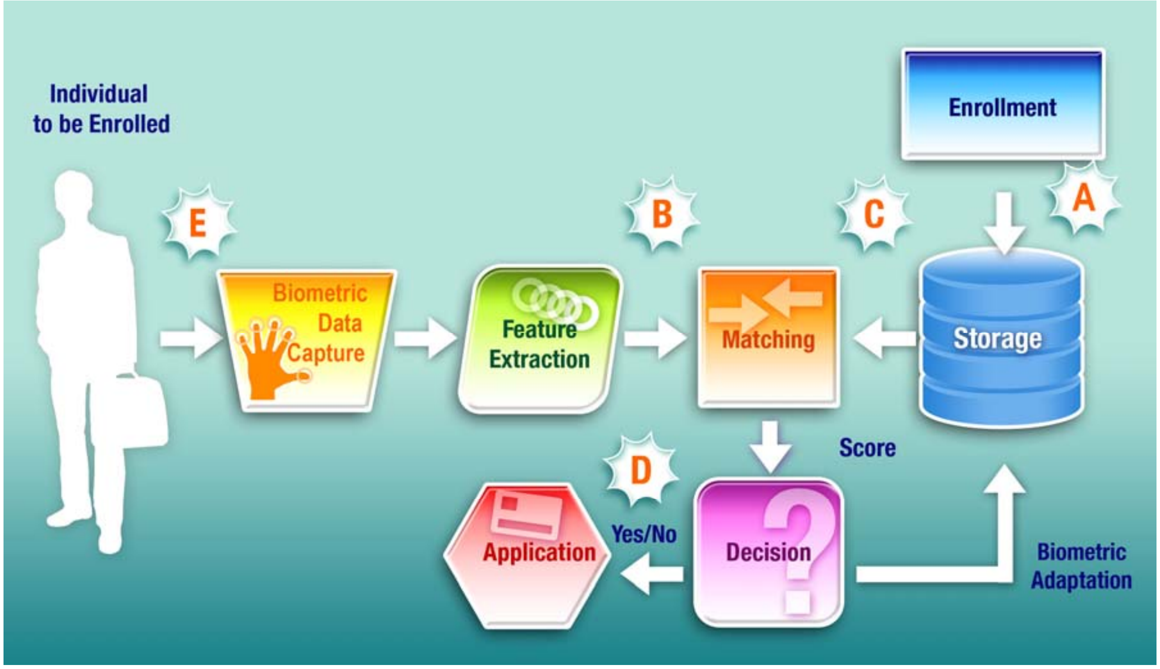

Figure 2: Vulnerabilities of a typical biometrics ecosystem

Figure 2 (above) revisits the illustration of a typical biometrics ecosystem but highlights five potentially vulnerable areas within the solution:

A. During enrollment of the biometric data. There is an immediate opportunity for two possible attacks – an image or reference template can be stolen, or a rogue image or reference template can be injected into the communication line. The key situation to be avoided here is not so much an attack against a single individual, since biometric traces are constantly being left by people as part of everyday life, but rather a situation where a large amount of biometric data and related personal information is 'stolen' in an automated or systematic way for illegal use.

B. Between a feature being extracted and matched. An attacker could try to capture and use biometric information to impersonate another individual, or to compromise the response of the system, by obtaining and injecting templates.

C. Between matching and storage. An attacker could attempt to capture a reference template, substitute a template to create a false reference, or more spectacularly, an attacker could compromise the database by stealing all its records.

D. Between application and decision. The whole biometric ecosystem could be compromised if there is a weak link such that a 'yes' (or 'no' if the goal of the attack is denial of service) response is always achieved.

E. Between an individual being enrolled and data capture. Finally, as with all security systems, it is important to establish an infrastructure that can deliver a sustainable level of security protection to its users. As such, the design of the system should permit isolated components and related software to be updated and refreshed without impacting the entire solution.

A secure biometric deployment must deliver a 'trusted path' between the components of the biometric solution to prevent these attacks. However, delivering a trusted path with a known and managed level of assurance can be a costly proposition as it requires:

- Every component of the system to be capable of executing cryptographic processes and hence must operate its own secure chips, so it can decrypt and validate the integrity of the data it receives and ensure the integrity and confidentiality of the data it sends.
- Secure chips to be provisioned with keys and their lifecycle must be managed.

To decrease the vulnerability of the system and reduce its cost, the number of components required in a biometric ecosystem can be reduced. This decreases deployment costs and also eliminates points of possible vulnerability, thereby providing increased security.

A conservative approach for this integration has been applied with the ePassport standards, where the biometric templates are held on-card but the match is performed by trusted readers. The operations of these readers are highly monitored, and they are deployed in small numbers when compared to the number of ePassports issued.

In comparison, implementing a biometric match-on-card solution that satisfies the required accuracy, enables for the deployment of much more cost-effective and unattended readers and provides an excellent level of privacy and security if issued following good practices.

In a match-on-card implementation, the on-card reference template is treated like a key and is non-extractable. In a biometric verification operation, a verification template extracted from the biometric measurement of a cardholder is presented to the card. The match is performed on the card and the decision is taken within the card itself. Since the biometric never leaves the card, is not stored on a central database, and all operations are executed under the control and with the consent of the cardholder, privacy is considerably enhanced.

This mode of operation significantly reduces the possibility of a systematic attack because there is no mass storage of biometric templates. Any potential breach could only occur at a single card level and this could only happen if the cardholder had lost control of the card, which the cardholder should be able to detect and report. The possession of the card is very important as one of the most complicated issues with biometric deployments is how to detect and recover from the loss of biometric data.

Biometric match-on-card technology also offers a much better alternative to a yes / no decision being made off card since the resources of the card can be used to cryptographically protect the decision transmitted to the application.

Finally, the biometric forms an organic ‘glue’ between the cardholder and their card. This enhances the value of the card by delivering a ‘proof of presence’ of the cardholder every time the card is used, making it difficult to refute a card transaction. Without match-on-card, an illicit user could deny non-repudiation by claiming their PIN and card could have been stolen.

GlobalPlatform technology can strengthen each element of a biometric match-on-card ecosystem to create a more secure, interoperable and robust solution. It can add significant value to user verification systems and facilitate multi-factor authentication. An explanation of how GlobalPlatform technology accomplishes this is detailed in the remainder of the document.

Section 2: Standardizing the Delivery of Biometric Match-On-Card Solutions

The quality and security of separate components within the biometric ecosystem have been improving, particularly through high profile government-to-citizen and government-to-employee implementations. These programs have also highlighted areas within the ecosystem that require further improvement and have led to questions being asked regarding the security and privacy of individuals' biometric data. This has encouraged the biometrics industry to specify policies and create standards with the aim of making biometric technology cheaper and easier to deploy. The industry continues to invest resources to advance the standardization of biometric technology.

In summary, standardization activities to date have focused on specifying the nature and quality of each component, the interoperability between components, and establishing security requirements. They have not addressed how these requirements can be implemented most effectively, resulting in different components being deployed in different ways. Therefore, although component security has been advancing, the biometrics industry acknowledges that the communication or 'path' between different components requires the implementation of a highly secure and consistent framework.

2.1 The Benefits of Implementing GlobalPlatform Technology

GlobalPlatform's existing and proven infrastructure provides the appropriate security requirements to ensure the necessary trust between the actors in a biometric match-on-card ecosystem, and offers many benefits when deploying a secure biometric service with smart cards or other personal devices carrying secure elements. Indeed, as GlobalPlatform concentrates on defining an open smart card infrastructure, its specifications can be applied to many other form factors including passports, access tokens, ID cards, cell phone secure elements or any object that contains an embedded chip capable of communicating like a smart card.

These benefits can be summarized as follows:

1. **Existing infrastructure.** GlobalPlatform is a proven infrastructure which covers the whole lifecycle of cards and their applications, and provides the necessary interoperability between actors such as cardholders, card issuers, application providers, identity registrars, enrollment station providers, card manufacturers, service bureaus and card acceptance device suppliers.

2. **Wide choice of secure technology**. To provide biometric authentication services, GlobalPlatform supports a wide choice of smart card, biometric and cryptography technologies compliant with a large set of open standards and policies. This allows organizations to find the best balance between cost and features without compromising interoperability and security.

   Additionally, existing GlobalPlatform technology has been evaluated by the most pre-eminent security schemes and meets the highest possible standards. For example, GlobalPlatform technology complies with the Common Criteria for Information Technology Security Evaluation (ISO 15408) which provides assurances that the process of specification, implementation and evaluation of a GlobalPlatform-compliant biometric match-on-card product has been conducted in a rigorous and internationally recognized manner.

GlobalPlatform technology also aligns with the Federal Information Processing Standards Publication (FIPS PUB 140-2), Security Requirements for Cryptographic Modules. This USA standard details the security requirements that are to be satisfied when a Federal organization specifies that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data, and maintain the confidentiality and integrity of the information protected by the module.

GlobalPlatform technology adheres to many more standards. As the organization is committed to evolving and refining its specifications to ensure continual alignment with industry regulation, implementers can be assured that it will address any changes to security requirements. This enables existing technology within the market to be updated without additional research and development costs.

As GlobalPlatform Specifications have post-issuance capabilities, any additional requirements – regulatory, functional or security related - can be made over-the-air to both cards and terminals throughout the lifecycle of the deployment. Such updates, therefore, can be issued efficiently with minimal impact on the end-user, ensuring the sustainability of the program.

3. **Proven interoperability.** GlobalPlatform is the only organization concerned with the integration of cards, devices and systems within a solution. Its compliance program validates component interfaces and behaviors to ensure interoperability between components from different providers. This proven interoperability provides flexibility for all parties involved in the ecosystem as it presents options, such as changing elements of the solution, upgrading algorithms or appointing new vendors post-implementation without impacting the entire deployment.

4. **Broad industry adoption**. GlobalPlatform Specifications are being adopted in a growing number of sectors such as financial services, government identification, mobile payment and ticketing. Biometric applications can benefit from the existing presence of a GlobalPlatform infrastructure within these markets should an issuer decide to deploy biometric match-on-card user verification systems that can be accessed by a variety of applications on one card.

Implementers of biometric match-on-card solutions can take advantage of these benefits today by implementing existing and established GlobalPlatform technology.

Section 3: Applying GlobalPlatform Technology to Biometric Match-on-Card Solutions

3.1 Creating Trust within a Biometric Match-on-Card Solution

To achieve the highest level of security, biometric match-on-card solutions must establish:

1) **An identity chain of trust.** The biometric is the ultimate binding of a person to the cryptographic credentials operated by the cards they will use to prove their identity. This only works if a complete identity chain of trust is sustained between the identity management system, which captures the biometric data and enrolls the individual, and the smart card management system (SCMS), which issues the biometric match-on-card application to the user. The core aim of this process is to establish that the user is who they say they are and the card is issued successfully.

2) **A trusted path.** Once the smart card is issued, a trusted path between components of the biometric verification system must be maintained at all times throughout the card lifecycle using modern cryptographic means.

This is shown in Figure 3 below. GlobalPlatform technology proposes a solution for both the chain of trust and the trusted path.

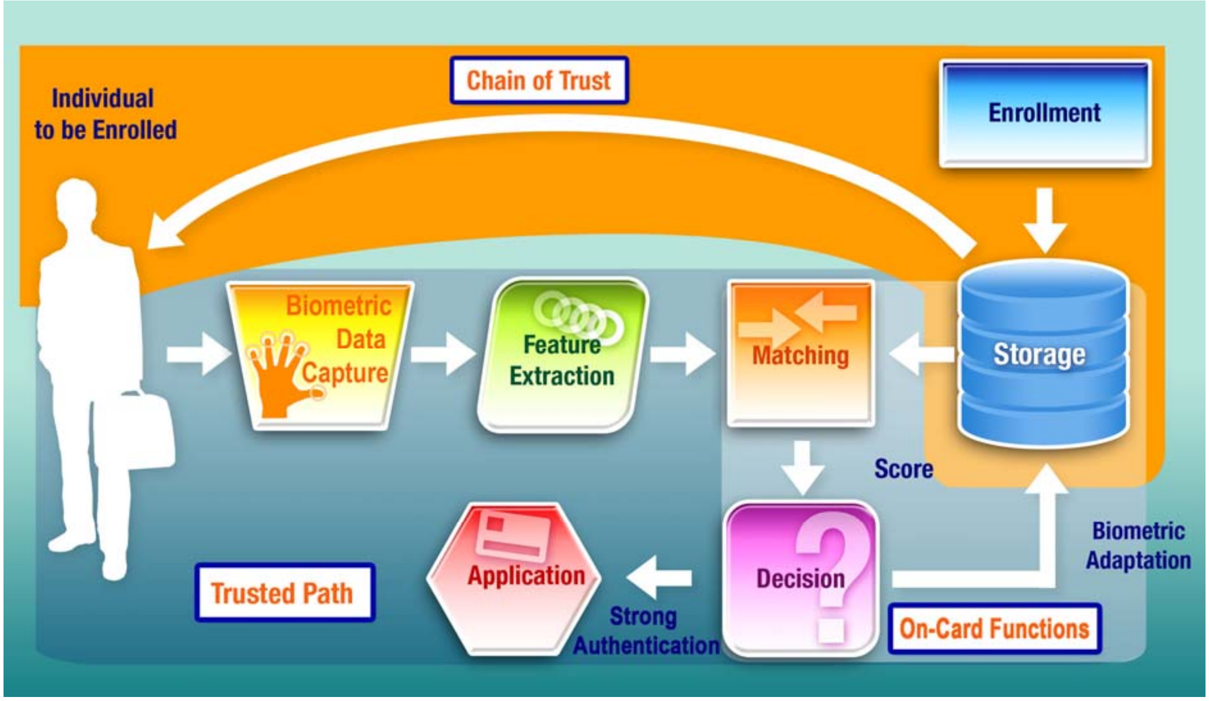

Figure 3: The chain of trust and trusted path

3.2 Increasing Security During Enrollment

The recording and storing procedure of a biometric template is highly sensitive from both a security and legal point of view. The location must be secure to prevent personal data being stolen or cloned and the operation must be conducted by an enrollment officer specifically authorized to control and secure the enrollment process. Depending on the card deployment policies the captured biometric may also be registered. This means if the individual were to misplace or damage their card, they could still prove their identity by authenticating themselves against the registered biometric. This step may allow them to obtain a new card, which is bound to the previously registered biometric information, without the need to undergo a disruptive and costly full enrollment process.

GlobalPlatform technology has been specifically designed for the secure delivery and establishment of management responsibilities throughout the card's lifecycle. Figure 4 demonstrates where GlobalPlatform technology can add value to the enrollment process.

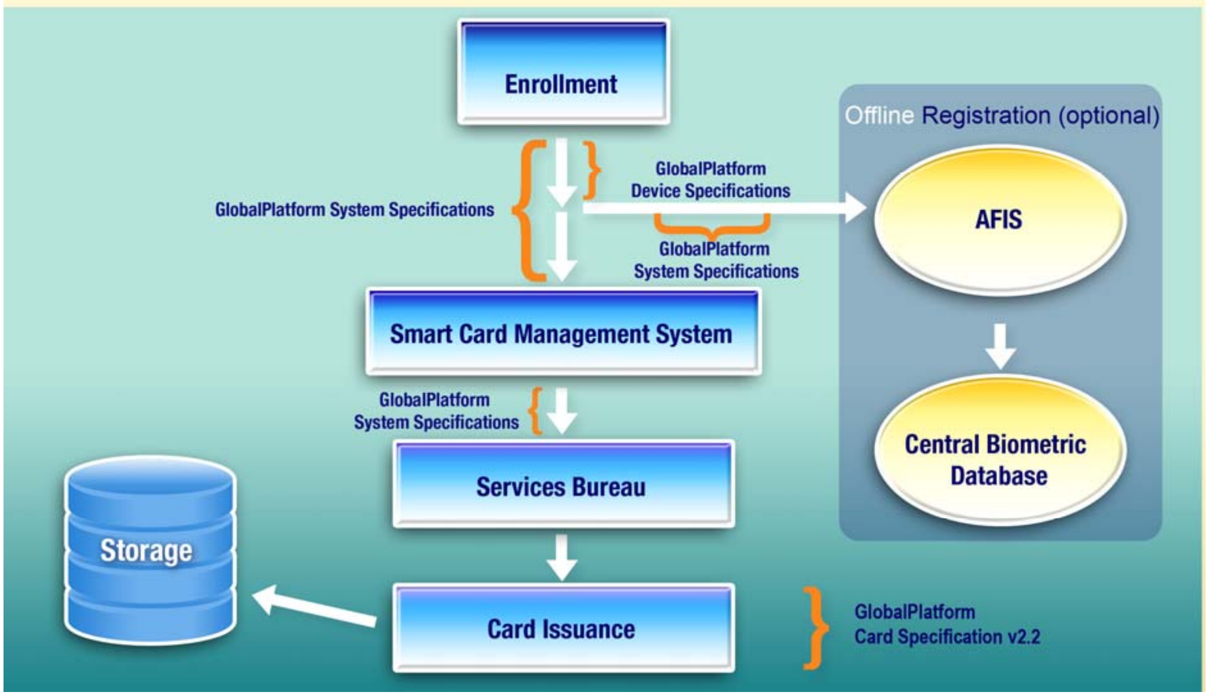
Enrollment
Offline Registration (optional)
GlobalPlatform System Specifications
GlobalPlatform Device Specifications
AFIS
GlobalPlatform System Specifications
Smart Card Management System
GlobalPlatform System Specifications
Central Biometric Database
Services Bureau
Storage
Card Issuance
GlobalPlatform Card Specification v2.2

Figure 4: Applying GlobalPlatform technology during biometric match-on-card enrollment

3.2.1 GlobalPlatform Device Specifications

At the enrollment stage, an individual's biometric sample must be captured using a trusted device. GlobalPlatform Device Specifications (GPD/STIP[1]) offers this framework. Its aim is to define an open architecture and software infrastructure for trusted terminals as well as open specifications for the management of the lifecycle of these trusted devices. Using GPD/STIP v2.3 within the device terminal, implementers benefit – at the most basic level - from the use of a common high level programming language, common platform definitions

[1] STIP is an abbreviation of Small Terminal Interoperability Platform. GPD is an abbreviation of GlobalPlatform Device. The STIP Specifications became the GPD/STIP Specifications in 2003 when the STIP Consortium transferred its intellectual property assets to GlobalPlatform. The current GPD/STIP technology provides open standards for use on smart card accepting terminals.

to achieve portability and interoperability, and a common Application Programming Interface (API) which enables the development and management of interoperable trusted applications.

3.2.2 GlobalPlatform Systems Specifications

GlobalPlatform System Specifications solve the problem of coordinating all the steps necessary to manufacture, develop, prepare, provision, personalize, distribute and maintain smart cards, smart card applications and trusted terminals within a biometric match-on-card solution. As outlined in Figure 4, existing GlobalPlatform technology supports the creation and issuance of the biometric match-on-card credential to the user by offering a trusted environment to 'transport' the match-on-card details to the SCMS, then to the service bureau prior to being uploaded onto the card and issued to the user.

Within this context, GlobalPlatform Messaging Specification provides a definition of the roles and responsibilities for all the actors within the system and how information 'messages' can be exchanged unambiguously and securely from one actor to another. This specification is key in establishing a clear framework for the enrollment system.

GlobalPlatform Profile and Scripting Specification indicates how cards and applications are configured by defining a ECMA script standard to which instructions for data generation, personalization and post-issuance instructions can be written. It also specifies all the information needed for the card customization process, including typical activities like data preparation and personalization. In other words, this specification addresses how private data will be protected from illegal use and how it will be securely stored.

GlobalPlatform System Specifications can also be used to support the offline interface between the SCMS and AFIS if registration is required as part of the enrollment process. This ensures the registration system is interoperable with the rest of the biometric match-on-card ecosystem.

3.2.3 GlobalPlatform Card Specification v2.2

GlobalPlatform proposes that personalization of the biometric match-on-card is under the control and protection of a security domain, which is an environment defined by a single set of security policies. By using a GlobalPlatform compliant card, a security domain owner can control the use of communication keys and ensure that sensitive biometric data within the security domain is never exposed and is protected from modification by unauthorized parties when transferred to the card.

3.3 Verifying a User

Figure 5 outlines how GlobalPlatform technology can enhance the user verification model.

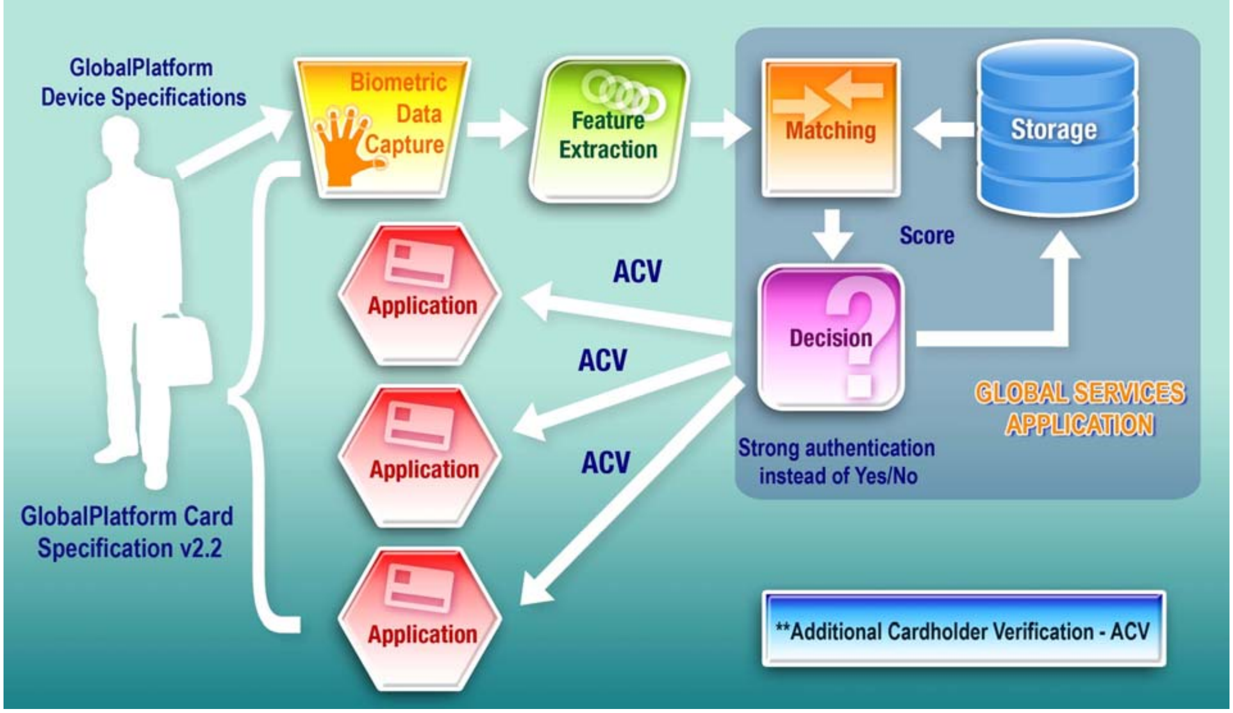
GlobalPlatform Device Specifications
Biometric Data Capture
Feature Extraction
Matching
Storage
Score
ACV
Application
Decision
ACV
Application
ACV
GLOBAL SERVICES APPLICATION
Strong authentication instead of Yes/No
GlobalPlatform Card Specification v2.2
Application
**Additional Cardholder Verification - ACV

Figure 5: Applying GlobalPlatform technology to the user verification model

3.3.1 GlobalPlatform Device Specifications

As highlighted in Section 3.2, GlobalPlatform Device Specifications can be used to define a trusted and managed biometric acquisition and feature extraction device capable of operating a trusted path directly with a smart card biometric match-on-card application.

3.3.2 GlobalPlatform Systems Specifications

The template stored on the card may need to be refreshed periodically. It is therefore vital to be able to manage the entire lifecycle of the template securely. The GlobalPlatform SCMS and Key Management Requirements provide process and security guidance on how to consistently and securely manage the lifecycle of cards, cryptographic keys and application data such as the biometric template. GlobalPlatform technology offers a secure channel protocol to transfer this data from the back-office, via a messaging protocol, from the SCMS to the card. The renewed enrollment will invoke the security access rights to the card at the same level as the initial enrollment. Methods and procedures for the secure processing of these actions, even in remote locations, are defined by GlobalPlatform.

3.3.3. GlobalPlatform Card Specification v2.2

The GlobalPlatform compliant smart card is an essential link in the chain of trust. It protects the contents of the card from being intercepted or tampered with, and ensures that secure communication is undertaken in a common language between actors throughout the card lifecycle.

GlobalPlatform secure communications and security domains also provide a basic on-card security scheme. This means that its secure channel protocols ensure end-to-end confidentiality and integrity during communication between elements on the card, while the on-card security domains restrict access to highly sensitive data, such as the biometric template, or secret keys or PINs.

This architecture, therefore, facilitates multiple applications to be securely positioned on the same card which is discussed further in Section 3.4. The technology also enables multiple actors to work together to deliver services through a single solution, and it is able to support multiple and innovative business models from different industry sectors.

In addition to providing a consistent approach to secure application management on the card, GlobalPlatform's Card Specification v2.2 post-issuance capabilities assists in managing risk, as the program will be able to adapt to future market regulations and enable the issuer to offer additional applications to the card securely throughout its lifecycle.

3.4 Global Services Application

Using GlobalPlatform Specifications, suppliers can develop commercial 'off-the-shelf' products, improving time to market and meeting the issuer's requirements. They can also avoid the expense of re-development and re-testing of proprietary solutions for individual customers, and focus instead on value-added products and services. Once the match-on-card templates have been established, GlobalPlatform technology can support two very different business models:

1. **Verification for issuer only.** This type of business model is typically the requirement of a government agency and is very sensitive in terms of privacy.

2. **Verification services open to other agencies or commercial services.** GlobalPlatform technology offers the greatest benefit to this particular business model. It allows two or more entities to share a biometric application by providing an entire system infrastrucutre that is both flexible and neutral.

GlobalPlatform Card Specification v2.2 offers a Global Services Application. When this is present on a card, an implementer can rely on GlobalPlatform's control management architecture which allows multiple applications to use the service. Within a biometric match-on-card ecosystem, this is a standard and powerful way to offer the biometric verification services to more than one organization.

> *For example, as demonstrated in Figure 5, one card could host applications from a bank for payment, transport operator for ticketing and an employer to allow access to the cardholder's place of work. Each application has access to the biometric verification service and can use it according to its access control policies.*

As mentioned in Section 1, biometric technology is often used in a multi-factor authentication scheme in conjunction with another verification procedure. The GlobalPlatform Card Specification v2.2 facilitates the use of different cardholder verification techniques to provide maximum security for each individual service.

Using the same example as before:

- *The bank's payment application could request that biometric verification and a PIN is required from the cardholder before access to funds is granted.*

- *The ticketing application may only require the biometric verification.*
- *Access to the cardholder's building might require two types of biometric verification such as fingerprint and voice recognition.*

Additionally, it also provides flexibility as to when the biometric match-on-card service is used.

> *For example, the bank could stipulate that only a PIN is required for low-value payments, with biometric verification applicable to high-value transactions.*

By locating the biometric match-on-card applet with its templates within the Global Services Application, biometric verification becomes more accessible to a wider audience as it significantly reduces the cost of developing and deploying the solution by enabling multiple providers to share this expense, and enables organizations with limited resources or awareness of biometric applications to consider its use.

> *For example, if a bank invested in developing such a solution, it may offer 'space' on the card to other application providers. The second application provider does not need to have expertise in biometrics to take advantage of the solution. Moreover, other application providers can benefit fully from the security and trust of the bank's enrollment procedure.*

3.5 A Complete and Evolving Platform

GlobalPlatform is the only organization concerned with the integration of cards, devices and systems at the component level, with committees and task forces actively pursuing the continual evolution of the technology. Ensuring technology compliance has, and will, always be central to the organization, and it will endeavor to deliver backward compatible solutions for the benefit of the marketplace.

The compliance efforts of the different committees will:

- Support future program changes
- Reduce cost through acquisition of 'open' solutions from vendors
- Reduce cost through economies-of-scale
- Simplify and accelerate the rate of new application development
- Reduce time to deploy the smart card schemes
- Provide a common framework for public/private sector initiatives.

Configuration documents are also developed and revised on an ongoing basis to provide implementation configurations consistent with the needs of users.

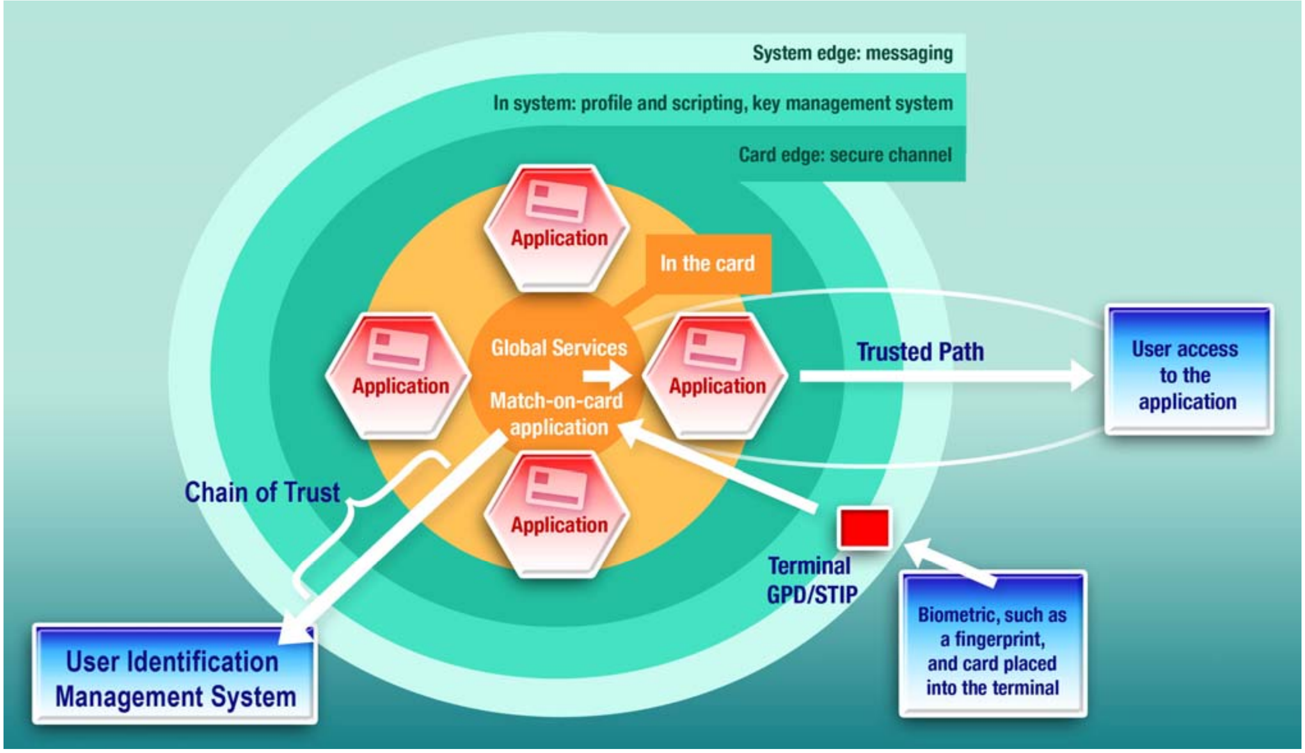
System edge: messaging
In system: profile and scripting, key management system
Card edge: secure channel
Application
In the card
Application
Global Services
Match-on-card application
Application
Trusted Path
User access to the application
Chain of Trust
Application
Terminal GPD/STIP
Biometric, such as a fingerprint, and card placed into the terminal
User Identification Management System

Figure 6: Overview of GlobalPlatform technology within a biometric match-on-card solution

SECTION 4: Use Case Scenarios for Biometric Match-on-Card

This section of the white paper introduces different use case scenarios where biometric match-on-card can play a central role in project implementations in the areas of national identity, employee identity, payments and mobile telecoms.

These are intended to provide a practical context for the previous discussion about the nature of biometric match-on-card and the need for a trusted path, which can be supported by GlobalPlatform Specifications.

National Identity Cards (eID)

National identity card schemes are by volume the biggest current application for biometric match-on-card issuance. A number of schemes currently proposed or implemented worldwide are based on fingerprint matching, a natural choice given that many countries already collect citizens' fingerprints for AFIS identification databases.

eID cards have always been linked to the person – one individual cannot delegate use of their ID card to another. Hence the use of personal biometric data supporting automated verification fits naturally into this process.

As they evolve, eID cards will have at least two different functions. One will be user identification managed by governments and the other will be for cards to simplify and secure a range of citizen services such as accessing e-government web portals and conducting financial transactions such as accessing benefits (see the Portuguese Citizen Card reference example below).

Employee ID Cards

Employee ID programs saw the first successful introduction of biometrics as a second factor of identification to the secure token. Biometric data replacing or complementing passwords in this area has progressed from smaller, high security applications to much larger deployments mainly based on ease of use, speed and economy.

Military organizations – indeed whole armies – as well as government departments and commercial organizations such as banks currently utilize match-on-card technology to provide employees with a secure and personal token for both physical access and single sign-on to IT systems. The advantages are:

- Cost efficiency – less need for password-related support/helpdesk function
- Ease of use – faster and more reliable than a password
- Improved security – users no longer write down passwords or remain logged on when absent, and sign off every transaction
- Complete off-line operation with retained security.

A specific advantage of match-on-card in this area is the ability for biometric data to be both stored and processed within the card. In many cases, this is a requirement for government approval of a biometric system in a private company (see the United States Department of State Logical Access Card reference example below).

Payment Cards

Payment cards have always been linked to a PIN for cardholder verification, and the introduction of chip and PIN has proved a highly successful initiative for the smart card industry. Biometrics can be seen as both a replacement and as a complement to the PIN in this market, and both uses are already in deployment.

In Japan, several banks have decided to complement the use of PINs with match-on-card biometric verification at ATMs due to the opportunity for crime to affect this transaction scenario. This type of application is typical of a highly developed economy where card transactions are becoming the norm and the ATM network is wide spread. Usually, the cards used are EMV compliant cards which for interoperability can only offer biometric cardholder verification at specific points of transaction controlled by the bank.

In developing economies, to date mostly in Africa, a different type of use has also been witnessed. Banks are concerned with fraud perpetrated with support from bank employees as well as identity fraud through lax issuing security for national ID cards in certain countries. In all these cases the use of match-on-card biometrics can counter the threat by physically linking the bearer to the card. At the same time it is seen as an easy-to-memorize and user-friendly process with no codes to remember or distribute.

Mobile Telecoms

Integrating biometric match-on-card into the SIM of a mobile phone is a novel use case that has been driven by the wide acceptance of mobile phone usage in Near Field Communication (NFC)-powered applications.

Any application using a smart card, and specifically a contactless smart card, can be fulfilled with the use of a SIM in an NFC-enabled phone. The advantage of this approach is that the smart card is already in the hands of the end user and hence there is no need for a separate deployment of cards, in turn reducing cost.

Match-on-card biometry is so compact that it is possible to use over-the-air (OTA) technology to activate the cards. Any suitable communication method that utilizes the GlobalPlatform secure channel protocol can be used for the transfer of biometric data to the card: OTA, SMS, Bluetooth, Wi-Fi or NFC.

It is also possible to consider the use of a fingerprint sensor integrated into the mobile handset, but the availability of such devices is limited at the present time and NFC seems a more likely candidate for integration in the near future. In any case, the integration of match-on-card delivers benefits from the availability of an existing, proven and managed secure module in the form of the SIM.

4.1 Reference Example: Portuguese Citizen Card

General Description

In April 2005, the Prime Minister of Portugal José Socrates announced that an eID card (Cartão de Cidadão) was to be launched with biometric data aimed at simplifying administration and modernizing the country’s public services as well as providing a new, highly secure identity document.

Portugal has been at the forefront of e-government projects and an early adopter of new technologies. It introduced a national electronic passport in July 2006 and launched a new integrated citizen portal (Portal do Cidadão) – a joint effort between twenty public and private entities to improve citizens’ access to e-services.

The primary goal of issuing an eID card was to revolutionize the way in which Portuguese citizens interact with the government. The card – which replaces five different physical ID documents including civil identification, taxation, voting, social security and healthcare cards – enables individuals to identify themselves both remotely and in front of officials.

The second goal was to use the card as a brand new tool for electronic signature and verification fostering the development of electronic transactions and giving citizens peace of mind in the digital age.

Above all, Portugal's e-government plan is designed to transform the public sector into an integrated and collaborative customer-oriented entity, thereby positioning Portugal as a leading country in terms of the quality of its service to citizens and businesses. The increase in citizens' satisfaction regarding these multichannel services delivered 24/7 should in time lead to a true international recognition of the quality on offer and a feeling of pride on the part of citizens for their public services.

Biometric Function in the System

The aim is to provide all Portuguese citizens with high-end cards incorporating fingerprint and facial biometric features as their national identity document by 2010. To identify and verify themselves, cardholders must enter a secret-PIN code and the card then generates a digital signature for secure declarations and e-administrative procedures.

Biometric match-on-card enables cardholders to be identified at the time of personal card delivery by letting the smart card perform biometric recognition directly on the card's chip. This technique offers both secure biometric storage and fast matching.

Match-on-card is provided in the form of a dedicated applet that is loaded on the card. This applet will fulfill the following functions:

- Receive fingerprint templates at enrollment time (two fingers)
- Securely store templates onto the card
- Perform matching when a template is submitted at a later stage
- Supporting functions such as template deletion, updating and so on.

Actors

In 2006, Portugal's national printing office, the Imprensa the Nacional-Casa Da Moeda SA (INCM) selected GlobalPlatform Full Member Gemalto as the prime contractor to provide the solution for the national eID card. This included the secure operating system, personalization system, applications, middleware and associated helpdesk services with Zetes Burótica, the Portuguese subsidiary of Belgian Zetes Industries.

For INCM, it was an opportunity to further enhance their unique expertise after the electronic passport project and reinforce the company's experience in e-government projects.

System Overview

This application provides the required cryptographic means for secure access to e-government services portal. It allows for multi-channel identity verification when the cardholder is present or via the internet or telephone (with a one-time password generated with the card) permitting citizens to identify themselves electronically. As the Portuguese constitution forbids a single central database for names, several identifiers can be found on the citizen card including civil ID number, social security number, tax number and healthcare user number.

Platform
The Portuguese government selected a secure identification document compliant with GlobalPlatform Card Specification v2.1.1 and the IAS (Identification Authentication Signature) European standard, as defined by CEN 224 WG 15. The eID document incorporating a credit card-sized smart card will be the official ID document for Portuguese citizens and will enable them to communicate with their government administrations (Ministry of Interior, Finance, Health and Justice) in a secure, fast and simple manner.

The biometric match-on-card component is compatible with industry standards. Based on GlobalPlatform card architecture, it uses the JCF Biometry API internally which provides biometric extensions to the JavaCard Standard. Implementation of the Biometry API is provided by an extra component that is also loaded into the card.

Conclusion
A first pilot phase started in February 2007 in the Azores region, with a full roll-out continuing through 2008 amounting to more than two million cards per year. Numerous public services are now available online, and procedures that would have taken hours such as obtaining civil records/birth certificates and social security declaration now take a matter of seconds.

In the future it is hoped that the match-on-card application will be used by police to verify the identity of individuals using fixed or mobile readers.

As the solution is GlobalPlatform compliant, the issuer can be assured that the technology offers the choice to add applications easily, providing greater value to the end user. As GlobalPlatform continues to extend its specifications, it will ensure there are development choices as well.

More information - www.cartaodecidadao.pt.

4.2 Reference Example: United States Department of State (DoS) Logical Access Card

General Description
The US Department of State (DoS) has been a frontrunner in implementing and using biometrics on smart cards. In 2004, the DoS's Public Key Infrastructure (PKI) Program Office introduced a biometric logon capability, Biometric Logical Access Development and Execution (BLADE), into their global PKI deployment. BLADE utilizes a match-on-card capability for greater security and ease of use.

Biometric Function in the System
In the PKI/BLADE system, fingerprint biometrics are integrated with PKI to provide logical access to the DoS's Sensitive But Unclassified intranet. Both privacy and security concerns drove the Department's requirement for match-on-card technology, in which the biometric templates are stored on the private area of the card and do not leave it.

Actors
In 2003, the DoS chose GlobalPlatform Observer Member Precise Biometrics to supply the biometric components of the system; this included the biometric hardware, firmware, algorithms, support, training and maintenance for the BLADE program. The DoS's PKI/BLADE Program Office oversaw the implementation of the BLADE functionality and

integration into the existing Entrust PKI framework. The support of the Information Resources Management bureau staff, in conjunction with the Global IT Modernization (GITM) program, and coordination with the Bureau of Diplomatic Security in providing smart ID cards, contributed to the success of what has become the current iteration of the PKI/BLADE implementation.

As of March 2008, nearly 20,000 DoS end users can use PKI/BLADE for network logon, with BLADE having been deployed in 52 overseas locations and portions of six domestic bureaus. An additional 77 overseas locations have the software and hardware in place to implement BLADE. The PKI Program Office also worked closely with application owners to ensure their applications could optimally leverage PKI/BLADE for single-sign on (SSO) capability.

System Overview

The system uses hardware with integrated biometric fingerprint capture device and smart card reader. Only extracted templates are stored on the smart card, with room for up to four fingerprints. Biometric templates never leave the smart card, with 1:1 verification occurring on the smart card.

Platform

For the initial BLADE implementation, the DoS used existing FIPS 140-2 smart badges, file-system based, with match-on-card capability. The matching algorithm is a hybrid of pattern and minutiae matching technologies. To comply with evolving US government directives and requirements, subsequent phases involve incorporating the PKI/BLADE container and Personal Identity Verification (PIV) container on a single PIV-compliant smart card. New applications are developing to allow the use of either PIV authentication certificate or PKI/BLADE signing certificate for authentication, depending on the requirement.

Conclusion

Through the deployment of BLADE’s match-on-card capability, along with PKI and an SSO capability, the DoS has seen a significant reduction in password management costs, with an estimated US $10.2 million annual saving for a population of 45,000. Additionally, users no longer have to worry about remembering their usernames and passwords or changing their passwords periodically, their credentials cannot be shared or lost, and their privacy is optimally protected.

SECTION 5: Conclusion

Biometric technology deployment will continue to grow. This will be fuelled by the need for positive identification and verification of individuals, to bind privileges to those individuals and to do so in a secure and privacy-enhanced manner. While there are many possible biometric attributes and different approaches to match a stored characteristic to an individual, this paper focuses on the benefits of selecting biometric match-on-card technology as the best means of achieving a shortened trusted path that not only reduces deployment cost for user verification but also enhances privacy for the individual.

Implementing a biometric match-on-card solution can indeed be accomplished using application-specific and highly proprietary components. This approach, however, inextricably binds the issuer to both the technology and the vendors chosen at the onset of the program. Over time, this model will restrict the issuers' ability to:

- Expand the program at competitive prices
- Offer additional applications and services from third parties without costly and proprietary integration
- Update security measures in an industry standardized and adopted manner
- Source new and emerging technology from alternate suppliers.

In this model there is a premium to be paid - in terms of time, money and flexibility - if the issuer is compelled by technology shifts, market conditions or security concerns to implement changes to an already widely deployed scheme.

As this white paper has discussed, these concerns and limitations are considerably reduced if not entirely eliminated by implementing a solution based on GlobalPlatform's existing and proven technology. By specifying that biometric components and applications abide by GlobalPlatform Specifications, the issuer can implement a biometric match-on-card solution that:

- Encourages participation from several suppliers on a non-discriminatory basis
- Drives down cost through competitive procurement practices
- Ensures scalability and backward compatibility of the technology, thus protecting the investment over time
- Confirms component compliance to the specifications through the use of correlating tests and tools.

In summary, a biometric characteristic can be uniquely bound to an individual offering high assurance that the individual is who they claim to be. Securing the biometric is well served in a match-on-card ecosystem as it shortens the transmission path, which in turn reduces points of vulnerability and strengthens the whole biometric system while enhancing privacy for the individual. Deploying technology that abides by GlobalPlatform Specifications offers additional safeguards made possible only by the efforts of this member-driven organization.

APPENDIX A: Types of Biometric Characteristics and their Measurement

There are two distinct classes of biometric characteristics:

- Physiological – those based on measurements and data derived directly from a part of the human body, and
- Behavioral – those based on measurements and data derived from an action by a human body, thus indirectly measuring characteristics of the human body.

Physical Biometrics

Techniques that measure biological characteristics unique to individuals include fingerprint verification, retina and iris scanning, facial recognition, hand geometry and vein pattern analysis. Each will be examined in more detail below.

Fingerprint Verification

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print. These include patterns (aggregate characteristics of ridges) and minutia points (unique features found within the patterns).

Two main approaches to creating interoperability between different biometric match-on-card solutions exist today. The US National Institution of Standards and Technology (NIST) has investigated interoperability of fingerprint biometric algorithms based on a standard minutia template. The objective was to test for performance suitable for physical access systems reaching a False Acceptance Rate (FAR) of 1% and False Rejection Rate (FRR) of 1%.

According to the MINEX benchmark established by NIST, the standard representation of a minutiae set is often sufficient to achieve the required level of accuracy when using a PC-based fingerprint matching engine and the matching of two fingers from the same person. It is also necessary to know the structure and properties of human skin in order to achieve successful imaging. The MINEX 2 scheme differs from the ongoing MINEX program as it is dedicated to the evaluation of the capabilities of fingerprint minutia matches running on ISO/IEC 7816 smart cards, and aims to improve the performance and interoperability of core implementations of the INCITS 378 and ISO/IEC 19794-2 fingerprint minutia standards to eventually reach similar performance to that of the ongoing MINEX.

The other approach is typified by ISO 7816-11 and all existing national ID card implementations at this time. Here the handshake procedure of the ISO 7816-11 is used to ensure interoperability between not only different fingerprint algorithms but also between different and possibly multiple biometric capabilities on the side of the card as well as the terminal. This approach also has the advantage of providing for the use of standardized raw images of fingerprints (ISO 19794-4) which ensures the constant availability of the maximum relevant information for matching.

A fingerprint sensor is used to capture a digital image of the fingerprint pattern called a live scan. A number of vendors incorporate additional features such as checking the print of a live finger. This live scan is digitally processed to create a biometric reference template as a collection of extracted features. A number of different fingerprint sensor technologies exist including optical, ultrasonic and capacitance. The ability to read a fingerprint depends on a variety of work and environmental factors including age, gender, occupation and ethnic origin. The standardized image is transformed into a template by software on the terminal. Established sensors are capable of providing quality images in standard format suitable for both enrollment and verification. Use of software accepting standard images makes the supply of readers and terminals competitive and cost effective.

Enrollment takes only a few seconds. The resulting template tends to be one of the largest in the field of biometrics, ranging from several hundred bytes to over 1000 bytes, but its stability and uniqueness is well established. The matching or verification can be conducted online by a backend server or offline, for example by means of a smart card.

Fingerprint verification is one of the most widely used biometric technologies today and about 20% of laptops can integrate a fingerprint sensor. The International Civil Aviation Organization (ICAO) has selected this technology for Extended Access Control (EAC) e-passports, while in India it is being considered for banking applications. Fingerprints are almost always the only biometric solution retained for national ID cards.

Retina Scanning

Retina scanning provides a unique basis for identification. To obtain a reading the user is required to focus on a small target while looking through a binocular style lens. An infrared light, directed through the pupil to the back of the eye, then takes a 45 degree circular image of the blood capillaries which is reflected back to a camera capturing the image. The template for eye retina data is comparatively small and the verification process is very fast. For verification, the retina pattern is scanned in a few seconds and compared with the stored retina data. To date the main usage of eye retina scanning has been restricted to high and medium security areas within military, space and police institutions although some prisons also use this method. There has been a general opinion that the public, if given the option, would prefer not to use retina scanning due to its invasive character.

Iris Scanning

The iris scan uses standard video optics to capture an image of the subject’s iris. Infrared light is used instead of natural light, allowing a clearer image of the iris to be captured. The enrollment method requires the user to place one eye to a telescopic-style lens. The user sees a reflection of the eye and is required to hold still for a number of seconds. The image is then displayed on a monitor, analyzed and the iris pattern is mathematically encoded into a database. It operates successfully with or without glasses/contact lenses. As well as eye patterns being unique they also remain stable from early infancy throughout a person’s life, only being affected by a few rare diseases. The technique is already used today within prisons or for border controls, for example the Iris Recognition Immigration System (IRIS) tested by the UK Government for certain frequent travelers at Heathrow. The identification and verification speed is quick due to the low number of bytes stored on the template and gives one of the best levels of accuracy producing almost zero error rates. The method is therefore highly appropriate for user identification.

Facial Recognition

Most of the facial recognition systems currently available require the user to be looking straight into the camera although very minor deviations, such as head movement, are acceptable. Other factors also need to be considered such as the person’s distance from the camera which can vary depending on the specific manufacturer’s design. As these systems first have to locate the face within the image and then locate such features as the eyes, mouth and nose, the need to capture a high quality image is imperative. The high quality image capture is dependent on highly consistent lighting conditions. The size of the template stored by facial recognition systems can vary depending on the supplier. A new trend, claimed to achieve previously unseen accuracies, is three-dimensional face recognition. Another emerging trend uses the visual details of the skin as captured in standard digital or scanned images. This technique, called skin texture analysis, turns the unique lines, patterns, and blemishes on a person's skin into a mathematical space. Facial recognition systems are commercially available and are used at airport border controls as well as governments. For example, the US Department of State operates one of the largest face recognition systems in the world with more than 75 million photographs actively used for visa processing.

Hand Geometry

Hand geometry systems operate by looking at the length of the fingers, hand thickness and palm shape. There is also a version whereby the geometry of just two fingers is measured. These systems are relatively easy to use, mostly incorporating guide posts to ensure the hand is placed correctly. They are not affected by environmental factors such as dirt and grease although rings with large stones or structures may need to be removed or positioned downwards if they were not worn at the time of enrollment. Since hand geometry is not thought to be as unique as fingerprints or irises, it is not suitable for user identification in which a user is identified from their biometric without any other identity information. The prime application areas for hand geometry devices have traditionally been for access at military, nuclear and other high-security locations such as prisons, but they are now increasingly being used for lower-security services. The technique was also used for the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) in the US during the late 1990s and early 2000s, the purpose of which was to facilitate the entry of pre-screened, low-risk travelers through immigration and customs at certain airports. The program was discontinued in 2002.

Vein Patterns

This system compares the vein tree pattern, formed from the subcutaneous blood vessels on the back of the hand or a finger. This pattern is picked up by a video camera when the skin is held tight. It utilizes infrared cameras to capture only the blood vessels and ignore the rest of the hand. This system is currently being used in similar areas to hand geometry biometrics. Many vein recognition deployments have been in the Asia Pacific region. The adoption rate has been especially high in financial institutions in Japan where hand palm vein recognition is used for ATM transactions.

Behavioral Biometrics

Behavioral biometric systems monitor the way in which an individual performs a particular action. Techniques include voice verification and dynamic signature verification.

Voice Verification

This techniques focus on characteristics of speech patterns formed by a combination of physical and behavioral factors rather than sound or pronunciation. They depend on the dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanisms of the body. As a result, voice verification systems are safe from mimics but not from high quality digital tape recordings. To overcome this, most voice systems build in a random factor whereby words or numbers may be picked randomly by the system from a selection stored at the time of enrollment.

Signature Dynamics

Special devices record the way in which a signature is written rather than its appearance. This is measured by either a special pen, a sensitive tablet upon which the signature is written with an ordinary pen, or with a tablet and stylus purchased as a standard computer peripheral.

The data and measurements obtained from the signature writing process vary between different systems but usually include factors such as speed, direction, pressure, thickness, the number of line segments crossed, total writing time, overall height and width, time taken to each of the turning points, and the number of times the pen is on and off the paper. When all the measurements have been taken, the results are used to calculate how close the offered signature is to the pre-stored enrollment template. Some systems are however unable to cope when a signature changes radically each time it is written, which affects around 2% of people.

APPENDIX B: Actors in a Trusted Path

Biometry authentication requires many actors including cardholders, identity enrollment entities, registration authorities, application providers, device and system providers. All of these actors play a role in the overall security scheme.

Cardholder
The individual who is being identified / verified and owns the card (or other secure element) to which the biometric template is bound.

Enrollment Officer
This actor is specific to biometric data flow. The cardholder must enroll one or more biometric parameters such as fingerprint, iris scan or facial image to be stored on the card as a template.

Biometrics System Manager
The biometrics system manager supervises the provisioning, configuration management and operation of the biometrics devices and software and holds a key role in terms of security, having the main responsibility for the user phase of the card lifecycle.
They are responsible for:

- Consistency of the trust chain, ensuring security and privacy during the deployment of the products. Considering its business model, the rules and laws, and security recommendations, the manager's role is to enable all the devices, readers or cards within the system.
- Enrollment of biometric and card readers. For every new reader introduced into the system, the system should be able to provide all the technology and messaging needed for secure communications with the biometric match-on-card. This includes not only the keys required for authentication and encryption, but also the identifier data (application identifier, keyset number and so on) used by the card and the reader to open the secure communication.
- Enablement of biometrics services on card. Depending on the business model, the biometric verification may be provided as a Global Service Application, and available to numerous applications on the card. The system manager must ensure that relationships on the card are the strict reflection of the external business relationships. This management must also be in accordance with the laws and the security rules.

Application Providers
Application providers must implement their applications in accordance with the recommendations of the system manager, in particular, providers of biometric authentication services.

Verification Station Manufacturers (Device Providers)
Reader providers must ensure that a secure element in the architecture can control the communications between the biometric sensor and the card.

System Providers
All system providers, including card management providers, key management providers, card manufacturers or personalization bureaus must ensure the security of their environment, facilities, personnel, operating system, and GlobalPlatform infrastructure components as well as the confidentiality, privacy, integrity and availability of application keys, code and sensitive data they provide and communicate. This effort must follow the Smart Card Management System (SCMS) and Key Management requirements, and must be

continuously maintained and improved according to new context and associated risks. If such precautions are not taken the security of the biometric application may not be ensured and the trust chain becomes ineffective.

APPENDIX C: 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

Device Specifications:

- GPD/STIP Specifications

Systems Specifications:

- GlobalPlatform Messaging Specification
- 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.