Infrastructure Standards for Smart ID card Deployment

Ramaswamy Chandramouli (National Institute of Standards & Technology)
Philip Lee (Identity Alliance)

Smart Card deployment is increasing thanks to the addition of security features and improvements in computing power to support cryptographic algorithms with bigger footprints (for digitally signing and encrypting) in Smart Card Chips in the past five or six years. Typical applications are Subscriber Identification Module (SIM) cards (in Telecommunication), micropayments (in Financial Transactions), Commuter Cards (in Urban Transportation Systems) and Identification (ID) cards. Although the market share of the smart cards used for identification applications (which we shall call Smart ID cards) is relatively small within the overall Smart card market, it's one of the fastest growing segments.

The Smart ID cards control physical access to secure facilities and logical access to IT Systems (Web servers, Database Servers, Workstations) and applications. The authentication of the card and the holder takes place using a set of credentials. An organization deploying such cards must have an infrastructure for generating, collecting, storing, provisioning and maintaining credentials. The components involved in these Credential Lifecycle Management activities constitute what we'll call the *smart ID card system infrastructure*, which supports smart ID card deployment.

Not all components involved in this infrastructure have standardized interfaces. Moreover, no robust messaging standards exist for information exchange among the components. Yet, some efforts are underway to partially address the standards gap in this area.

Smart ID Card System Infrastructure

At the heart of Smart ID card system infrastructure is the *Identity Management System* (IDMS) which includes both a data repository and a software system that is increasingly used in many organizations to support all forms of identity-based applications such as Single Sign-on (SSO) and Authorization Management. Broadly, the two most common areas of identity-based applications are for physical access control systems (PACS) and logical access control systems (LACS). Despite the IDMS's versatility, no agreed-upon definition exists for its functional scope. Its canonical function as the manager of all forms of enterprise-wide credentials (identity information) is recognized, but individual product offerings vary widely in their functionality. The points of variation include the types of corporate (meta) directories to which the IDMS can interface (LDAP, for example), native DBMS support (relational or object-oriented), the expressive power of the data schemas (some IDMS systems support capture of authorization information such as roles, groups, userIDs, target IT system definitions etc) and the mechanisms they use to connect to the systems to which the credentials must be provisioned (e.g., connectors, agents etc).

We thus have a situation where a core component of an infrastructure for supporting identity-based applications in general and smart id-cards in particular, consists of product offerings with varying functionality and interfaces. Therefore, our search for identification of areas for standardization in the Smart ID card system infrastructure should start with information flows in and out of IDMS. Based upon our conceptual understanding of IDMS as the repository of all credentials, it is easy to see that it should have the following two kinds of information flow streams:

- Credential Collection stream (CCS) – this consists of all information flows needed to gather and consolidate credentials from multiple sources. Different types of credentials or credential-related information originate from these sources and flow into the IDMS.
- Credential Provisioning stream (CPS) – this consists of all information flows to various end-points (or target systems) that need to perform identity verification. Where identity verification takes place, authentication credentials (a subset of credentials stored in IDMS) flow from IDMS to the access control entities such as a door panel or an IT application systems.

When the authenticating credentials used for identity verification are long pieces of data (say 25 bytes long instead of a 4-digit ATM PINs) or the authentication process involves sophisticated transaction (such as a cryptographic protocol instead of an exchange of a simple shared secret), credential verification requires a smart card. A new component in the infrastructure is needed to securely populate the card with the credential and to track its status as to whether it is active, suspended, terminated, lost or stolen. This new component is called the Card Management System (CMS) and in a Smart ID Card system infrastructure, becomes the target of provisioning in its own right just as a PACS or LACS. Hence information flow from the IDMS to CMS becomes an important component of credential provisioning stream.

To design this infrastructure to an enterprise's functional and security needs, the enterprise consumer needs some market choices in the procurement of each of the components in the Smart ID Card system infrastructure. At the same time, consumer does not want to end up with a situation where integration of components that each meet the enterprise needs becomes a tedious and technically challenging task. It is in this context, that the presence of interface standards between the key components of Smart ID Card system infrastructure becomes critical. The goal of the rest of this article is to identify what those components are, and the presence or absence of interface standards between IDMS and those components. Our scope encompasses both types of interface specifications – those for program-level (APIs) and message-level (Messaging Interface) interactions.

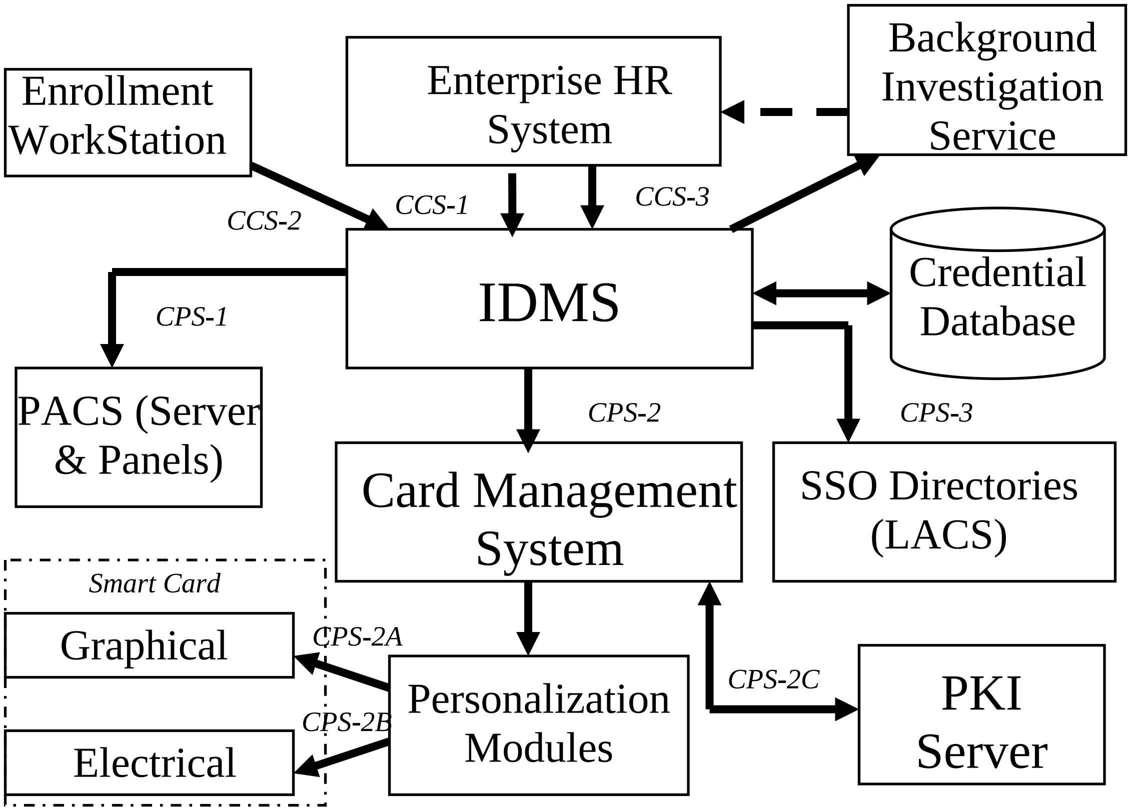

Figure 1: Smart ID Card System Infrastructure Components

The components in a typical Smart ID Card system infrastructure are shown in Figure 1 along with numbered information flows for CCS and CPS. The components from where a CCS originate are "Credential Sources" and the components from where a CPS terminate are "Credential Targets" (except for CPS-2C). Figure 1 also serves as our reference architecture.

Information Flows in Credential Collection Stream (CCS)

The primary sources from which all credentials originate are the Human Resources (HR) systems or equivalent (Personnel Management Systems, Contractor Registries etc) in the organization. The human being to be issued a smart ID-card is called an Applicant till the time the smart ID-card is physically issued and thereafter called the Card Holder. The first credential collection stream (marked as CCS-1) is called the pre-enrollment package and may consists of the following information:

- Applicant Demographic Information (Name, Address, SSN, Gender, DOB etc)
- Applicant Affiliation Information (Organization, Dept/Division, Status (Employee or Contractor), Country of Citizenship etc)
- Sponsorship Information (seal of approval from a sponsor attesting that the applicant is eligible to receive a smart ID-card).

Once the pre-enrollment package arrives and entered into IDMS, the applicant or the enrollee is notified (either by IDMS or by the sponsor) to go through the enrollment process at an Enrollment Work Station (see Figure 1). The applicant's biometric information (Facial Image, Fingerprint etc) is collected and identity proofing or vetting takes place through examination of the breeder documents such as Birth Certificate, Passport, Driver's License, Residency/Work Permits etc. The outcome of the enrollment process results in generation of enrollment package (second credential collection stream marked as CCS-2) that flows from Enrollment Work Station to IDMS. The enrollment package consists of the following information:

- Biometric Information (Facial Image, Fingerprint and/or Templates)
- Scanned Copies of Breeder documents

The applicant demographic information along with subset of enrollment package (especially fingerprints) are sent for background investigation to verify whether the applicant was/is a law-abiding citizen. An example of background investigation is the FBI Criminal History Check in the United States.

Interface Standards with "Credential Sources" Components

Based on the process flow described above, it is clear that the Smart ID Card system infrastructure involved in the credential collection function consists of the following components (and interfaces) (also called "Credential Sources" Components):

- Enterprise HR Systems to IDMS Interface
- Enrollment Work Station (EWS) to IDMS Interface

Enterprise HR Systems are generally legacy IT systems (or customized HR modules of ERP offerings) with heterogeneous database management systems. IDMS though of relatively recent origin do not have standardized APIs or Messaging Interfaces. In the absence of these interface specifications, web interfaces are built for HR Systems and IDMSs (all IDMSs come with web interfaces) and the following requirements are specified to standardize interaction or information flow between enterprise HR systems and IDMS:

- Secure Network Protocols
- Data and Messaging syntax
- Message-Level Protections

In the area of Secure Network Protocols, HTTPS (at the session level) and TLS (at the transport level) are generally specified. If a web service interface supporting a service-oriented protocol is specified, then the associated secure version of application protocols such as SOAP 2.0 must also be specified. The messages in both directions (HR Systems to IDMS and IDMS to HR Systems) must be identified. With reference to our chosen reference architecture for the Smart ID Card system infrastructure, the following are the messages:

- Pre-Enrollment Package Upload (HR Systems to IDMS)
- Pre-Enrollment Package Response (IDMS to HR Systems)
- Adjudication Package Upload (HR Systems to IDMS)

The machine-independent transfer syntax (e.g., XML) must be specified and XML data elements and their organization (e.g., XML Schema) should be specified for each of the messages. It must be noted that there may be some variations in the set of credentials that each smart ID-card deployment uses and hence a common messaging schema (in our case XML Schema) cannot not be used. However it is possible to define a generic XML Schema that is inclusive of all possible credential elements, facilitating selection of a subset of this generalized XML Schema for each deployment scenario.

Continuing with our process flow analysis of credential collection, we find that the enrollment package is the credential collection stream flowing from Enrollment Work Station (EWS) to IDMS. An important aspect to remember with respect to EWS to IDMS interface specification is that an EWS could be an in-house system or be located at an enrollment service provider site (and hence under a different IT administration domain) if the organization had outsourced this enrollment function due to economy of scale or the geographic dispersion of the organization's operating units. Even the in-house EWS system could be a remote system that uses the public network for communication. Taking into account the nature of interaction between EWS and IDMS (described above) and the fact that IDMS does not have a standardized programming or message-level interface specification, the same standardized set of requirements as specified for HR Systems to IDMS interaction must be specified. Further the message-level protections assume an added importance in EWS to IDMS interaction as described below:

- The Enrollment Package contains privacy-sensitive information (Biometrics and Breeder (Identity Proofing) Documents)
- The Enrollment Service Providers will be using cryptographic modules from different vendors. It is necessary to ensure that those cryptographic modules are certified for certain strength requirements required by the organization's policy for transmitting privacy-sensitive information.

One last aspect of process flow in the Smart ID Card system infrastructure related to credential collection is the flow of information from IDMS to Background verification systems. At least one background verification system, we know of, namely the US Visit/IDENT system provides complete message interface specification as follows:

- Secure Network Protocols (SOAP 2.0 Protocol with client-side SSL Authentication)
- Data and Messaging syntax (XML, 12 Message Types with XML Schema for each)
- Message-Level Protections (Client-Side Authentication)

Information Flows in Credential Provisioning Stream (CPS)

All the information flows in Credential Provisioning Stream originate from an IDMS and the number and information content of these flows depends upon the type of authentication application. The exact modules in the authentication application to which credentials are provisioned are called "Credential Targets". The various information flows that are part of CPS are:

- Physical Access Control Information (Card Holder Name, Facial Image, Unique Credentialing Number, Expiration Date and/or Status (Active, Suspended, Revoked etc)– between IDMS and PACS (marked as CPS-1)
- Logical Access Control Information (Card Holder Name, A Unique Identifier such as UPN, Organizational Role (e.g., Accountant) and/or Clearance Level)– between IDMS and a LACS module (e.g., SSO Directory) (marked as CPS-3).
- Card-Resident Credential Information (All Credentials that will eventually reside on the card)– between IDMS and CMS (marked as CPS-2)
- Digitally signed Third-Party Attestation of Identity and Credentials (The PKI certificates provided by a Certificate Authority (CA)) – between CMS and a PKI Server (marked as CPS-2C)
- Card Personalization Information – Graphical – CMS to Card Printers (CPS-2A)
- Card Personalization Information – Electrical – CMS to Smart ID-card (CPS-2B)

Interface Standards with "Credential Targets" Components

Based on the process flow described in the present section, the components (and the interfaces) involved in credential provisioning function in the Smart ID Card system infrastructure (also called "Credential Targets" Components) can be identified as follows:

- IDMS to PACS Panel Interface
- IDMS to Corporate Directory Interfaces (for supporting logical access control through Single Sign-on mechanism)
- IDMS to Card Management System (CMS) Interface
- CMS to PKI Servers

The information flows from CMS to the end-point of the provisioning (i.e., the physical Smart Card) are also considered as part of credential provisioning stream and hence the following additional interfaces are also considered part of the Smart ID Card system infrastructure:

- CMS to Card Printer Interface
- CMS to Card Interface (through the Card Reader device)

Like enterprise HR systems, most PACS are stand-alone (very rarely connected to enterprise network), legacy systems with no standardized APIs or messaging interfaces. They consist of two primary components: PACS Server (which is the main data repository containing physical access control information) and PACS Panel which contains a cache of the data required (in the form of a lookup table) for restricting physical access and which activates a door lock for opening doors or turnstiles once the match of the data sent by the smart card reader (called PACS reader) with the lookup table occurs. The deployment of PACS systems predates smart card deployments (they were connected to work with magnetic stripe cards) and even IDMS deployments. Hence the traditional approach for getting access control data into PACS server is through customized data downloading scripts which perform periodical batch transfer of data from relevant authorized sources (HR Systems, Physical Security Office databases etc). Because of the huge investment in PACS systems (even a single large organization has PACS systems from different manufacturers), a middleware-oriented approach for interfacing with multiple PACS systems from IDMS systems is under development under an effort sponsored by Department of Homeland Security (DHS) in USA. Under this approach, there will be a PACS Proxy with a standardized messaging interface that can be made use for IDMS to PACS integration. The components of this messaging interface are the following:

- Secure Network Protocols – SOAP over HTTP
- Data and Messaging syntax – XML Syntax, Two Main Message Types and XML Schemas for message format for each of the types.
- Message-Level Protections – Mutual authentication between IDMS and PACS.

The next interface that is required is between IDMS and corporate directories for the purpose of transferring credential information for logical access control. This is one of the few areas where standardized interfaces are available with the help of secure directory access protocols such as LDAP etc.

Perhaps the most important interface in a Smart ID Card System Infrastructure is the IDMS to CMS interface. CMS is the system that performs the task of populating the smart card with credentials by establishing a secure session and maintains lifecycle data such as the card status, credential status etc. A CMS is a complex software module that has only a few vendors. As could be seen from the figure, a CMS communicates with a number of systems such as PKI servers, card printers and the smart card to be populated. CMS communicates with the following entities to perform the associated functions:

- PKI servers to request and obtain digital identity certificate to create bindings between cards and credentials.
- Cryptographic libraries (not shown in Figure 1) to generate public-private key pairs and digitally sign some credential objects that will go on the card.
- Card printers to print card holder names, photographs, security features such as holographic patterns and so on; and
- Smart cards for electrical personalization of credentials in a card’s data objects or containers.

The most notable feature with respect to integrating CMS with other components in the smart ID card infrastructure is that almost all CMS vendors provide their own proprietary software development kits (SDKs) consisting of programming interface libraries for uploading information to and extracting information from the CMS. These SDK libraries facilitate the task of transferring card-resident credential information (CPS-2) from the IDMS to the CMS, as well as transferring graphical card-personalization information (CPS-2A) from the CMS to card printers. The downside is that these SDKs are useful only for integrating specific, designated CMS products; organizations must deploy new SDKs and develop new sets of data transfer programs if the CMS product in the smart ID card infrastructure changes. That said, the following platform- and product-neutral specifications are available for integrating CMS with PKI servers (for transferring CPS-2C) and smart cards (for transferring CPS-2B):

- Public Key Cryptography Standard (PKCS) #10 is a messaging specification for requesting digital certificates from PKI servers run by different certificate authorities.
- Global Platform Messaging and API specifications (published by the Globalplatform.org industry consortium) enables a CMS to electrically personalize smart cards in a secure way.

After a smart ID card is issued, various components perform the actual authentication functions. These include the host application and the service-provider middleware that provides specialized functions, such as financial transactions and telecommunications, related to the smart card’s application area. Because these components technically form part of the smart card user interface architecture, rather than the infrastructure architecture, we didn’t consider their interfaces in this article. Even restricting our focus to infrastructure components in smart ID card systems, we find that the process is still in the early stages of transitioning from the use of customized data upload and download scripts and communication sockets to the use of standardized application and network-layer protocols (that include security) using partially defined messaging specifications. Upgrading this process to one with standardized procedures can occur only when the components in the smart ID card system infrastructure have standardized APIs or message-level interface specifications. An alternate path toward this goal would be to employ middleware with standardized APIs for connecting to each of these components. Organizations planning to deploy smart ID cards, therefore, will have to take into account the direction and progress of standardization efforts in both these approaches (i.e., Message-Level Specifications & Component APIs and Middleware APIs) while formulating their overall strategy.

In summary, we find that there are gaps in standards that prevent seamless integration of components participating in Credential Collection Stream (CCS) as well as in Credential Provisioning Stream (CPS). Based on the nature of the information flows and the functionality and evolutional history of components, the following are the “Standards Gaps” must be addressed in Smart ID card system infrastructure:

- Message-Level Specifications between components participating in CPS such as Enterprise HR Systems, Credential Enrollment Workstations, Background Investigation Services and IDMSs.
- Middleware API specification for interacting with Physical Access Control Systems (PACS).
- API specifications for interacting with Card Management Systems (CMS)