Open Smart Card Infrastructure for Europe

v2

Volume 3:	**Global Interoperability Framework for identification, authentication and electronic signature (IAS) with smart cards**
Part 3:	**Recommendations for interoperability specifications**
Authors:	**eESC GIF Expert Group**

GIF-1 TEAM: Laurent Den Hollander, Marc Lange, Theo van Sprundel, Peter Tomlinson

EDITED BY: Chris Makemson

FOR DOCUMENT HISTORY: SEE ANNEX A

Contents

Table of Figures

0 Executive Summary

The Information Society can improve and stimulate the quality of life for all European citizens. To be really useful all services must be easily accessed by any European citizens at any time, and in any place. The personalised tool to enable each European citizens to enjoy such access is their electronic Identity (eID), their "reliable key to e-services".

The document is the first part of the eESC GIF, "Global Interoperability Framework", which, in turn, is part of the "common specifications" for an "Open Smart Card Infrastructure for Europe" (OSCIE). It is also being transferred to European standardisation bodies for further elaboration. The OSCIE is the result of the eEurope Smart Card (eESC) Charter, an industry <u>and</u> government driven initiative launched by the European Commission in December 1999 following announcement of the eEurope 2002 Action Plan.

The primary objective of the GIF is to facilitate interoperability at the level of **e-Identification, e-Authentication and e-Signature** (IAS) between different smart card schemes emerging in Europe and more widely throughout the world. It provides both smart card schemes and e-service providers with necessary concepts and guidance. Topics covered by the GIF include tools required for access to e-services and securing transactions over networks (including over the Internet), implementation of the special "high-end" security requirements, preparing information systems for interoperating and organising the operation of this IAS interoperability.

The key messages of the GIF are the following:
- For setting up its business strategy, a smart card schemes can take advantage of the concept of the **value chain**, i.e. a chain of business activities and partnership, oriented to the added value of every element in the chain. The sources of value are (and / or) cost leadership, differentiation leadership andperception of value as seen by the customer.
- The functioning of smart card and e-service schemes requires a set of different **basic roles**. Some of the roles are "content" oriented and others "issuer" oriented. The issuer-oriented roles govern the business conditions (including security policy) and technical implementation means.
- In the vision of the Global Interoperability Framework, the future IAS enabled smart cards will:
  - By default be issued with a **generic IAS card application** supporting and supported by a nationally recognised scheme
  - Mainly be multi-application with **many service providers** leasing or otherwise using the facilities of the existing smart card schemes
  - Be expected to be usable in an **interoperable** way without regard to logical or physical card scheme boundaries
- When a service provider is willing to welcome a not-on-us card (i.e. a card whose specifications have been defined by another smart card scheme) for identification, authentication and electronic signature purposes, **three role interfaces** are needed and will be called upon to ensure this interoperability:
  - The interface between the not-on-us card and the access provider from the host smart card community
  - The interface between this access provider and the service provider
  - The interface between the two smart card communities concerned
- Two logical adapters or gateways (IOP-adapters) can enable interfacing between two smart card communities as follows:
  1. The **interoperability adapter or gateway**, which operates in the connectivity level and enables process interfaces between the IAS and application levels required for accessing/transferring data at card layer for the purpose of the front office application layer.

2. The **PKI adapter or gateway**, which is technically identical to the interface required for enabling certificate verification issued by two different PKI or equivalent within the same smart card community.

Part 3 contributes to developing these key messages by defining the **three role interfaces** and identifying, in their architecture and functions, requirements for supporting IAS interoperability.

1   Introduction

1.1   Overview

This document is a product of the eEurope Smart Card Charter[1].

The Smart Card Charter identifies the issues and contains an action plan for their resolution in order that smart cards can help fulfil the expectations of citizens within the information society.

This Global Interoperability Framework (GIF or "the framework") for electronic methods for Identification, Authentication and Electronic Signature (IAS), incorporating secure smart card technology and usable over the internet, is part of the Smart Card Charter Common Specifications.

Ths document is the third part of the framework, giving guidance for large scale implementation of generic IAS using smart cards. This part 3 develops further the operational and implementation models of part 2.

This document must be read in conjunction with parts 1 and 2. Terms used here (e.g. smart card community and *e*-service community) are used with the meanings and in the context defined in part 1. Assumptions made in parts 1 and 2 also apply here; they are summarised here, but parts 1 and 2 describe them in more detail and in context.

The framework's vision is for the widespread issuing of secure smart cards for use by citizens as *e*-ID tokens, together with the development of networked IAS services making use of those tokens for authentication and as tools in authorisation and electronic signature services. A general introduction to the Smart Card Charter and this framework may be found in part 1.

The vision of GIF can be illustrated with the image of smart cards as "The intelligent key to *e*-services".

The Global Interoperability Framework is in 4 parts:

- **GIF Part 1: Contextual and conceptual modelling**
  an in-depth modelling of the smart card, its environment and interoperability issues with regards to identification, authentication and digital electronic signature;
- **GIF Part 2: Requirements for IAS functional interoperability**
  a list of functional and interoperability requirements to be used together with Part 1 for establishing a set of specifications for interoperability at IAS level;
- **GIF Part 3: Recommendations for interoperability specifications** (i.e. this document)
  guidance for enabling, implementing and operating IAS interoperability;
- **GIF Part 4: Deployment strategies for generic IAS**
  an overview of business plan elements, organisation issues, and system development processes for mass deployment strategies.

The framework uses a simplified four-tiered system inspired by established software and system engineering methodologies (UML).

---

[1]   See http://eeurope-smartcards.org/

CONTEXTUAL MODEL
CONCEPTUAL MODEL
OPERATIONAL MODEL
IMPLEMENTATION MODEL
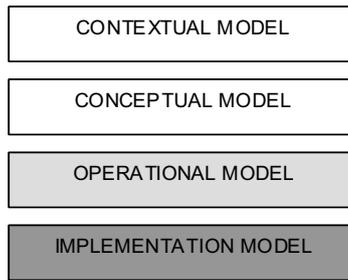
Figure 1: Four tiers in the methodology

Mapping the framework with the methodology

The mapping of the four parts of the framework with this four-tiered methodology may be interpreted as follows:

- GIF Part 1 and GIF Part 4 address respectively background (including the vision of trust systems using electronic technology) and deployment from the perspective of the first two tiers of the methodology (context and concepts).
- GIF Part 2 presents the functional requirements to be taken into account when defining the operational and implementation models by deriving them from the context and concepts defined in GIF Part 1 and some strategic decisions and assumptions
- GIF Part 3 presents operational and implementation models.

	Part#1	**Part#2**	**Part#3**	**Part#4**
Context	▨			▨
Concept	▨			▨
Operations		▨	▨	
Implementation		▨	▨	

Figure 2: GIF Parts and the 4-Tier methodology

The contextual model is an informal description of the systems and other relevant background context in which the model is being designed. It represents the "raw material" of the formal modelling process, similar to the "requirements gathering" phase in software engineering methodologies. It begins with trust scheme principles from a global perspective, and moves to focus on organised societies.

The conceptual model is the first semi-formal description of the system. It is a very high level and abstract description of the system which answers the question "What" (What is the described system supposed to do?).

The operational model refines the conceptual model by answering the question "Who" (Who is doing the job?).

Note that a conceptual model may lead to multiple operational models each presenting a different operational scenario. However, introduction of an alternative model brings the responsibility to describe how interoperability will be achieved with existing models.

The operational model is described using the following elements:

- Actors: which describe operational entities
- Functions: which enable delivery of the interactions between actors

The implementation model refines a given operational model by answering the question "How" (How are things done?).

Note that an operational model may lead to multiple implementation models each presenting a different implementation scenario. However, introduction of an alternative model brings the responsibility to describe how interoperability will be achieved with existing models.

1.2 Scope of GIF Part 3

The GIF interoperable IAS model and architecture, as described in Part 1, is designed to generically enable IAS interoperability across smart card communities (SCCs) irrespectively (within reason) of the operational and technological divergences of the smart card management frameworks (SCMFs) used.

For implementing interoperable IAS solutions, two approaches have been identified:

- Generic IAS common specifications, for the situations when, from day one, a smart card scheme includes IAS interoperability in its objectives (e.g. for opening the SCC to as many *e*-services as possible and to cards issued by other SCCs).
- Using IOP-adapters (gateways) to handle conversions when interconnecting SCMFs, for the situations when a smart card scheme already exists and wants to be interoperable with a new service offered by a service provider or another smart card scheme.

GIF Part 3 includes both approaches. In addition, it allocates firewall functions to the IOP-adapter (gateway). Part 3 describes, from a high level perspective, elements of specifications for the generic IAS functions for each of the three layers and related stakeholders.

The detailed characteristics of IOP-adapters will have to be specifically defined on a case-by-case basis depending on the technical characteristics of the SCMFs to be bridged and on the operational and legal agreements between the *e*-service communities which make use of this bridge.

1.3 Terminology

This part of GIF makes some changes in terminology compared with earlier parts:

New term	Previous term	Comments
User	Card holder	
Identity file	Card holder ID data Card data	Could be used for other entities

1.4 Acronyms

The acronyms in this section are in addition to the acronyms section included in GIF Part 1 and 2.

AID	Application Identifier
ATR file	Answer To Reset file (ISO/IEC 7816 file name)
CWA	CEN Workshop Agreement
DIR file	Directory file (ISO/IEC 7816 file name)

DTBS	Data To Be Signed
*e*Epoch	*e*Europe Smart Card Charter proof of concept and holistic solution
FINREAD	FINancial card READer
NICSS	(Japan) Next generation Ic Card System Study group
NIST	(USA) National Institute of Standards and Technology
OSCIE	Open Smart Card Infrastructure for Europe
OCSP	On-line Certificate Status Protocol (RFC 2560)
OID	Object IDentifier
PIF	Public Identity File
PP	Protection Profile
SIF	Subject Identity File
SSCD	Secure Signature Creation Device
STIP	Small Terminal Interoperability Platform
TBn	(eESC) Trailblazer group n
URL	Uniform Resource Locator

2 Two approaches to interoperability

2.1 SCMF operational model

Basic SCMF operational model
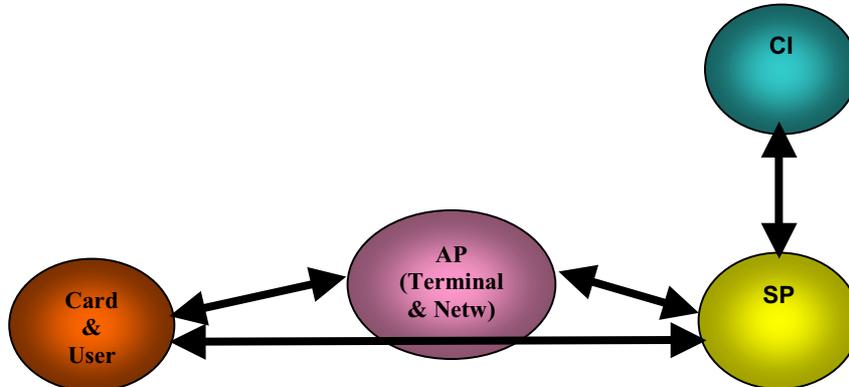
Figure 3: SCMF operational Model

The operational model of a single SCMF (smart card management framework) during the active phase of a smart card's life cycle is modelled as above.

The card and user (card holder or CH) interact through a terminal and network (managed by the access provider (AP)) with a front office application (provided by a service provider (SP)) in order to gain access to a given *e*-service.

Since the framework focuses on high-level security, the links between the entities must be secure, which includes identifying the entities by means of their certificates. In order to secure the links, the AP and SP may contact the card issuer (CI) acting as certificate authority (CA) (or acting as VA) for verification (authentication). The SP may decide not to grant access to a given *e*-service until other entities have been secured.

The SCMF is incorporated within a single smart card scheme. The scheme includes all of the elements, technical, organisational, financial and legal, required to satisfy its owners, users and partners. In terms of the models in GIF part 1, the scheme includes the smart card community (SCC) and all registered *e*-service providers. Such a scheme operates within a single security domain, and therefore the scheme's CA (or VA) can authenticate the entire network used for transactions carried out wholly within the scheme.

Interoperability in the SCMF operational model

Interoperability between schemes is required when not all of the entities involved are registered in the same security domain, which is described as one or more of the entities being "not-on-us". This requires the use of gateways between the schemes, which may be for functional and protocol reasons (IOP-adapters) and/or at PKI level (e.g. where CA/VA certificate validation methods are different in the two schemes), or may be minimal in function where the schemes are designed around agreed common specifications.

Examples of not-on-us operation are:

- a visiting card holder holding a card issued by scheme B uses a terminal in scheme A in order to access an *e*-service which is registered only with scheme B
- a government office whose terminal is part of the infrastructure of scheme A wishes to authenticate a visitor who holds a card issued by scheme B

The common specifications for the interfaces between the entities in the SCMF operational model of Figure 3 are described in the framework as Generic IAS application specifications.

However, the framework does **not** mandate a set of common interchange formats, and therefore the overall model is still one of multiple one-to-one technical conversion specifications, rather than conversions between scheme formats and a set of common interchange formats. Migration towards common interface specifications will, in time, reduces the complexity of conversions required and maximise the scope of interoperability.

Even if common interchange formats can be defined, the issues surrounding legal recognition and liability of IAS signed transactions across smart card communities still need to be negotiated or harmonised on a one-to-one basis. That is, it is still necessary for schemes to negotiate agreements based on mutual recognition of each other's security policies and processes, and thereby define the scope of not-on-us IAS trust.

Both the adapter method and the generic IAS interface method for interoperability are described in the following sections of this part of the GIF.

Mutual authentication of schemes at the SCMF level

Interoperable operation requires each SCMF to authenticate the other in order first to secure the infrastructure. Then the cards (and card holders) can be authenticated across the link between the schemes.

SCMF – or the CAs of the two schemes, assuming that they are independent (i.e. are not linked back to a common root CA) – will have previously approved each other's security policies and processes, and will have cross-certified each other. During operation, authentication may then use several routes:

- direct links between the CAs to authenticate the not-on-us CA,
- links through the infrastructure layer (via an IOP-adapter and PKI-adapter) or via a VA common to both schemes in order to authenticate infrastructure entities, user smart cards and cardholder certificates.

2.2 Adapters

Adapters are also known as gateways.

The IOP-adapters act as mediators, enabling operation across different systems to support the various on-us and not-on-us scenarios. They may act as firewalls and message routers between the schemes. They also provide drivers for different card platform types and on-card IAS applications, and thus may be found at various nodes in the SCMF (possibly within terminal equipment).

The PKI-adapters act as converters between an authentication request and the authentication (validation) formats of the different CAs. For this function, a CA (or an

associated VA), may accept direct requests using the OCSP protocol, or may offer access to the latest certificate revocation list (CRL).

Using more traditional terminology, once schemes have established that their security policies and processes are interoperable, the IOP-adapters enable the mutual recognition of interoperable schemes during operation. However, they are not sufficient to deliver mutual authentication between schemes for all the components of the three layers (infrastructure, user, application); PKI-adapters handle trust requests and responses.

Part 1 identified the concepts and functions of the adapters as in Figure 4 below:
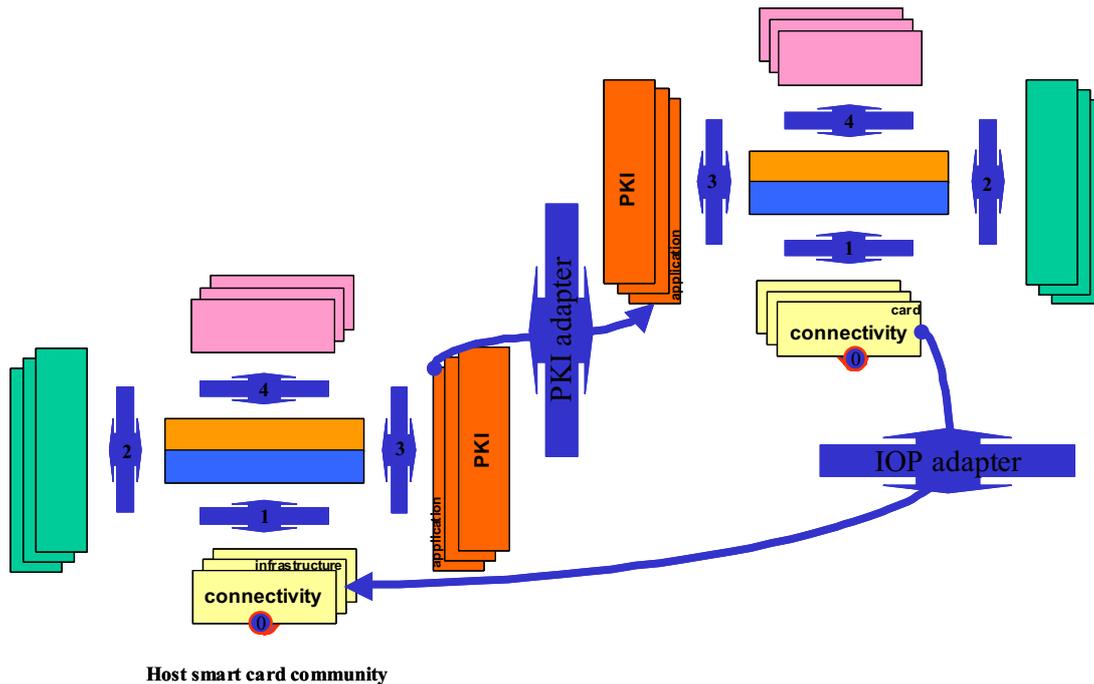
Figure 4: IAS interoperability by adapters (functional model)

Note that Figure 4 is a logical diagram. It is important to understand that in practice the PKI-adapter may be incorporated into a direct link between the PKIs, or may operate in conjunction with an IOP-adapter.

Part 1 also gave a view of these adapters (from the stakeholder viewpoint) and the drawing below (Figure 5) provides a simplified version of it, focused on IAS operations and in line with Figure 4.
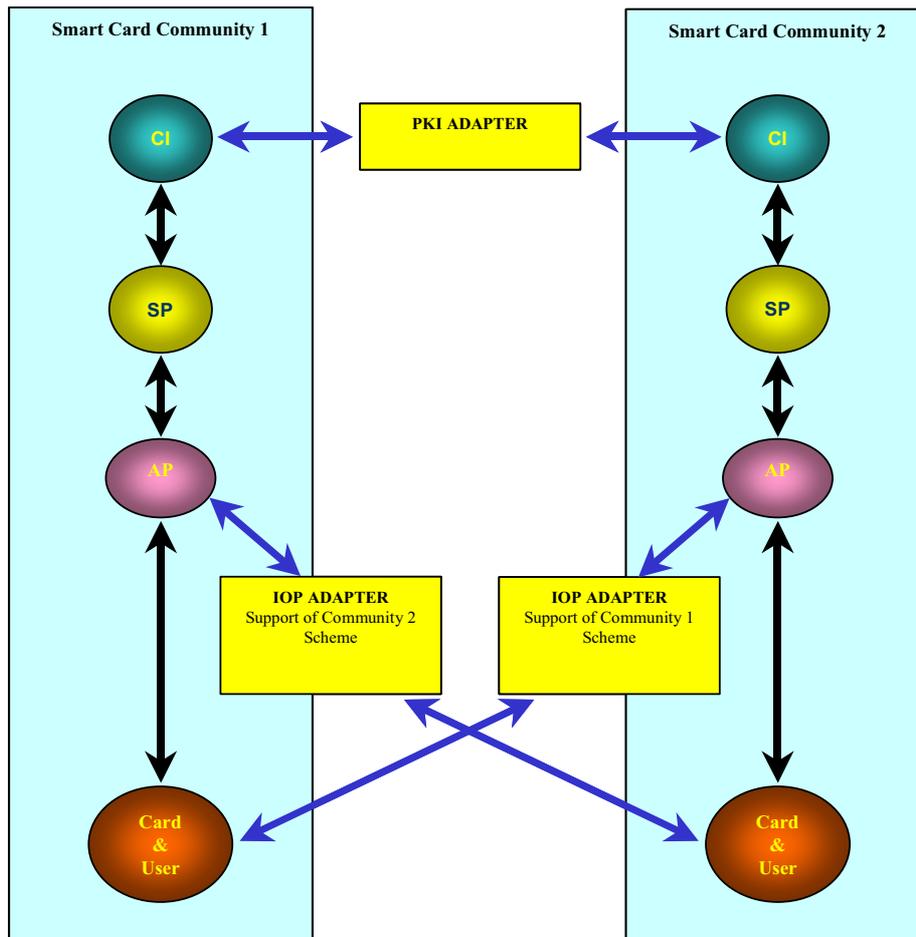
Figure 5: IAS interoperability by adapters (stakeholder model)

2.3 Generic IAS

The IOP- and PKI-adapter model requires co-operating schemes to define the interfaces that they will use for communication between schemes. The aim of the framework, by modelling a generic IAS architecture, is to guide scheme implementations towards common models, and thus to eliminate the conversions required in the adapters (and also minimise the loss of functionality when transactions have to take place between schemes).

The generic IAS common interfaces are to be used (logically) for communication at each of the three operational layers (card/user, infrastructure and front office application) and to link to the security plane. Communication through the adapters supports the operational stakeholders (i.e. user/card holder, access provider, service provider, and PKI), but adapter functions are expected to be minimised as schemes migrate towards the generic IAS architecture and interfaces.
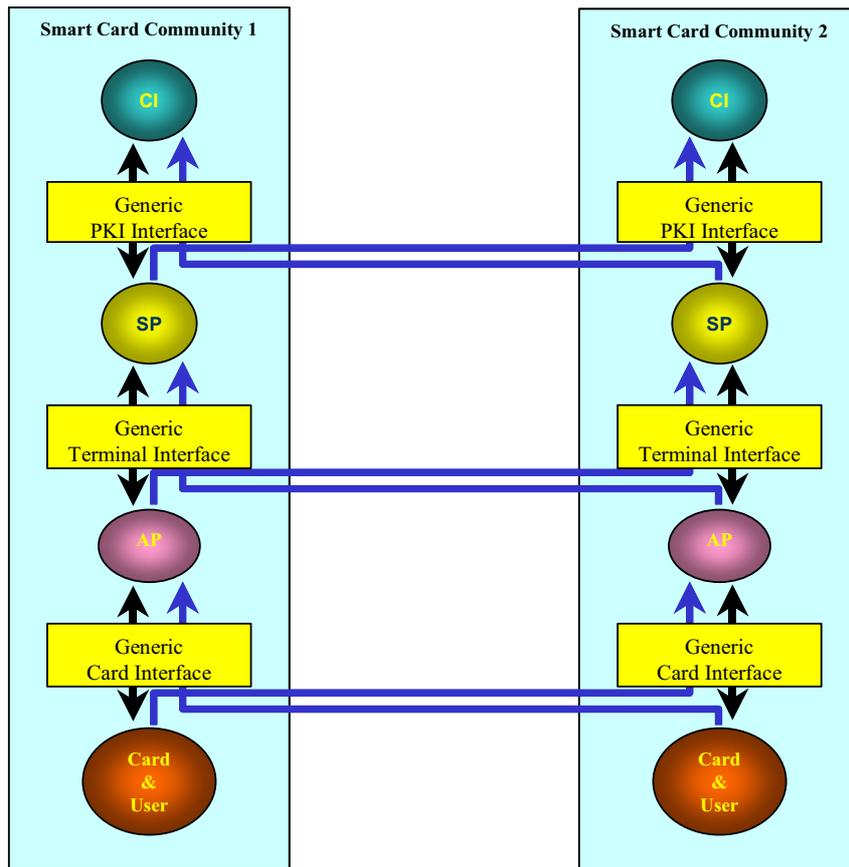
Figure 6: IAS interoperability by interfaces

3   The generic IAS application Interfaces

3.1   Overview

This section is a short introduction to the generic IAS interfaces, with later sections providing more details.

In order to facilitate interoperability for IAS purposes between a wide range of service providers, access providers and card issuers on the basis of the interface approach, first generic GIF IAS is defined as a set of interfaces between the entities in the SCMF operational model. This leads to the following model:
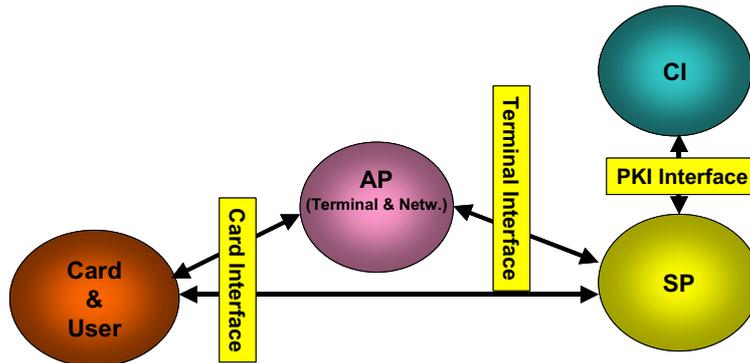
Figure 7: Generic IAS application interfaces (stakeholder model)

3.2   The Card Interface

The IAS card interface is the core of GIF IAS, and provides a generic interface to the smart card's IAS services. This card service is accessible to off-card applications, be they at the terminal level (AP) or at the front office application level (SP).

3.3   The Terminal Interface

The IAS terminal interface provides a generic interface between a terminal and a front office application to facilitate management of IAS operations requiring the physical intervention of the card holder through the terminal (signature, PIN code entry, biometrics…)

3.4   The PKI Interface

The IAS PKI interface provides a generic interface between a front office application and the certificate verification services of a card issuer (CRL/OCSP queries to CA/VA during authentication processes)

4 The Card Interface

4.1 Generic IAS function: architecture and role

4.1.1 Card application and internal interfaces

The specifications below are illustrated by the functional box model presented in GIF part 1.
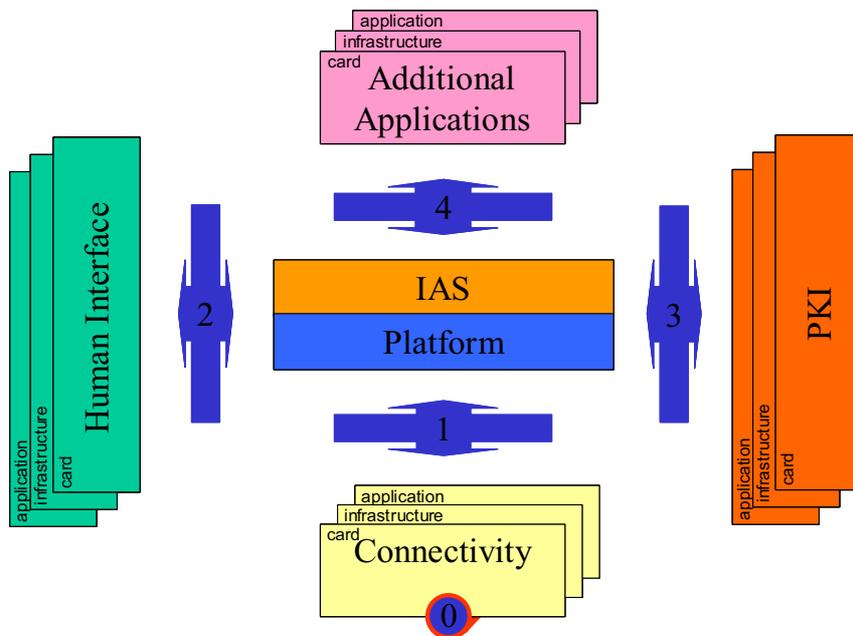
Figure 8: The basic model of the functional boxes

As a standard interface for off-card applications to access IAS services on the card, the IAS card interface will be essentially the interface to the IAS on-card application.

GIF strongly recommends that the IAS card interface is implemented in a smart card application as opposed to implementing it as a part of the card's run time environment or operating system. Primarily, this is for security reasons, but it also permits the application to be loaded onto the card at a late stage in the manufacturing and issuing process, i.e. at card issuance time. Features of this implementation method are:

- At the security level, such an application is protected by the firewall functions of the smart card platform.
- The IAS application is accessible to off-card applications through standardized invocation methods:
  - selected using the ISO/IEC 7816 Select File on AID command; and
  - accessed using ISO/IEC 7816 format APDU's

The IAS application can also be made directly accessible to other on-card applications, providing that the smart card's operating environment supports a secure inter-application communication protocol.

The IAS application must have access to the smart card's cryptographic and security libraries in order to be able to perform its tasks.
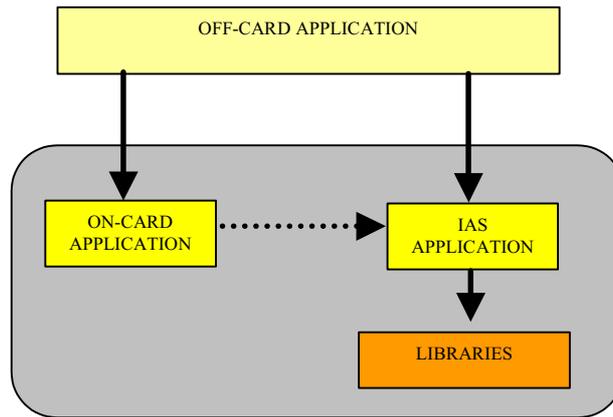
Figure 9: IAS application interfaces

4.1.2 IAS and trust subjects

The IAS card application provides identification, authentication and digital electronic signature functions for a set of trust subjects. Within the GIF IAS, there are two mandatory trust subjects, namely:

- The smart card: The smart card as a token, uniquely identified, and authenticated by the card issuer.
- The card holder's public (official) identity: The public identity of the card holder authenticated by the card issuer acting as CA/RA.

The IAS card application must handle at least the smart card and the card holder's public identity to fulfil the requirements of this framework.

The IAS application may also provide a standardized interface to additional trust subjects. This, however, is outside the interoperability scope of this document, and indeed inclusion of additional trust subjects (such as qualified certificates) in the generic IAS application's data set is subject to further study of both security and card issuer topics. But, if they are managed by the generic IAS application, these additional trust subjects are the responsibility of the card issuer.
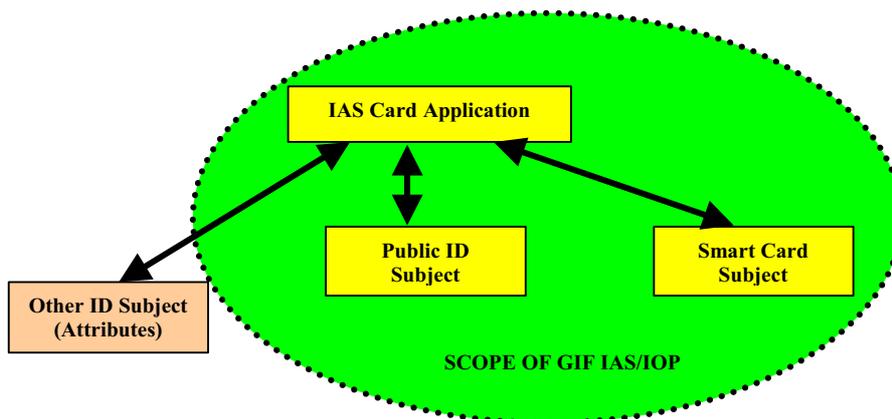
Figure 10: IAS subjects

Example: A government acting as card issuer with combined roles (see GIF part 1) may decide to issue smart cards with a generic IAS service covering 2 subjects:

- The smart card: as defined above
- The card holder's official ID: as defined above

and may also include additional subjects

- Other card holder ID trust subjects: authenticated ID of the holder in relation to certain roles (contained in qualified certificates or represented by attribute certificates linked to the official identity).

In some cases, the card holder may wish to hold several sets of qualified certificates or even several entirely separate identities on the card. In general, it may be that identities other than the official identity and related certificates will be held in a separate application on the card. However, there already exist card applications which are used in a government context and are organised to hold multiple sets of certificates (e.g. Common Access Cards for the military, an application already in use on USA); these applications can support multiple identities.

Identification
- Generic technical definition: A process through which an entity (A) makes a statement about its identity to another entity (B).
- IAS Definition: A process through which the smart card provides descriptive data to an off-card application about any of the subjects managed by the on-card IAS application.

Identification may be a public function (any off card entity entitled without restriction to call the on-card identification function and obtain the identification data from the smart card), or release of the information may be subject to card holder permission, or only certain authorities may be able to obtain the information without card holder permission. The access conditions are defined by the rules of the SCC.

Authentication
- Generic technical definition: A process through which a claimed identity of entity A is successfully verified by entity B.
- IAS definition: A process through which the smart card provides an off card application with strong and verifiable electronic evidence of identity (and possibly attributes) for any of the subjects managed by the on-card IAS application.

Note that parts of the authentication process involving exchanges between the off card application and the card issuer (acting as CA/VA) are NOT covered here.

Signature
- Generic technical definition: A process whereby an authenticated entity A imposes a unique (non forgeable/non repudiable) mark on an object. For example, where the object is a contract, the signed contract is a legally binding commitment for the signing entity to comply with the terms of said contract.
- IAS definition: A process through which the smart card - triggered by the cardholder - performs a digital signature on a data object presented by an off card application on behalf of one of the subjects managed by the IAS application.

Digital electronic signatures have the property that they are linked to the signed data in a manner which ensures that they not only authenticate the data in the way that a signature on a paper document does, but also they allow detection of any changes to the data. Note that the digital signature is often not applied directly to the complete data object, but the data object may first be reduced to an electronic digest (e.g. a hash string), using algorithms which give an adequately secure method of detecting any later changes to the document; it is the digest that is then signed.
- Signature generated by the smart card subject without card holder intervention
    - o **From a legal standpoint**: The signature generated by the smart card subject has no legally binding value but can eventually be used as "corollary evidence" for non-repudiation purposes as a proof that this particular card was physically present in a

particular terminal at a particular time. As such this signature can be generated without any pre-requisites.
- o **From an operational standpoint**: The signature generated by the smart card subject will essentially be used as part of security processes such as secure channel management.
- Signature authorised by the public ID subject (trusted signature)
  - o **From a legal standpoint**: The signature generated by the public ID subject is legally binding for the card holder and thus must only be generated under strict control by the card holder him/herself.
  - o **From an operational standpoint**: The signature generated by the public ID subject under control of the card holder will be used as a legally binding digital electronic signature.

4.1.3 IAS functions and data on the card

From the preceding description it is easily seen that there is a very strong dependency between identification, authentication and signature:

- Signature is performed by an authenticated subject
- Authentication validates the identity of a subject
- Identification provides the identity of a subject

The generic IAS service on the card consists of processes and data:

- Processes to perform the authentication and signature operations
- Data about the trust subjects

From the description above, there are two mandatory identity data sets, one for the card and the other for the card holder's public (official) ID, and there may be others. A general name for these groups of data sets is Subject Identity Files (SIFs): abstract objects holding all the IAS data about a subject. Two of the data sets are in the public domain (card and public ID), and so this subset are Public Identity Files (PIFs) (Fig 11).

Since the only mandatory trust subjects in the framework are the card and the card holder's public ID, these are the only trust subjects for which interoperability across card schemes is required by the framework. Hence in Fig 11 additional PIF data sets are marked 'non interoperable'. However, the framework recognises the market requirement for other card holder IDs (held in PIFs) to be interoperable, in particular for implementing digital forms of advanced electronic signature (as defined in E-sign); the methods for delivering this form of interoperability are not yet fully determined.
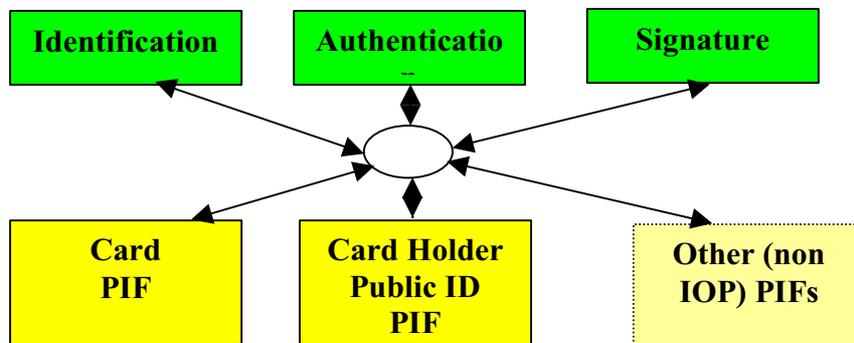
Figure 11: Subject Identity Files

4.1.4 IAS application and security

The IAS application only provides a standardized interface to a basic set of identification, authentication and signature services.

The IAS application uses security and cryptographic primitives provided by the smart card but does not control, manage or have any liability for the security of the smart card.

Within its role as a provider for a standardized interface to IAS functions, the IAS application provides a mandatory standardized interface to IAS functions relevant to the smart card and card holder public ID subjects as provided by the card issuer. The card issuer is liable for these.

4.1.5 IAS application and off-card applications

Off-card applications using the on-card generic IAS application benefit from using a service for which the card issuer is responsible, and it is recommended that off-card (front office) applications use this on-card service.

Any additional application on the smart card may have its own proprietary IAS functions and interfaces independently of the generic IAS application. The card issuer will not be liable for these additional applications.

This leads to the following possible configurations:
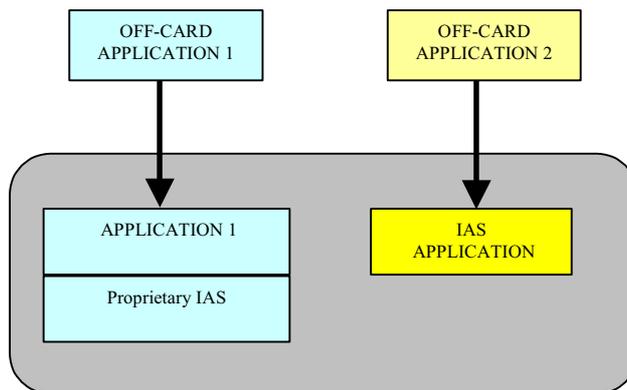
Figure 12: Case 1: Application with proprietary IAS and IAS application [2]
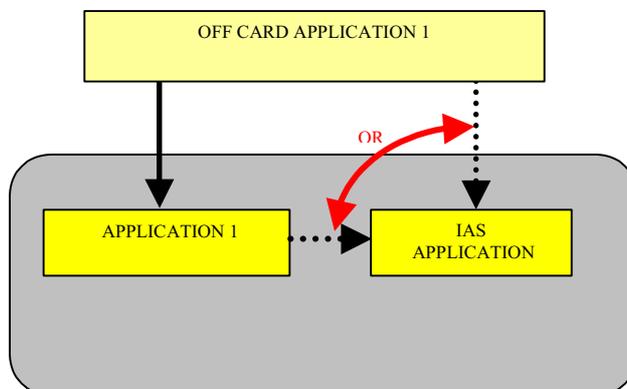
Figure 13: Case 2: Off-card application delegating IAS functions to IAS application [3]

---

[2]   Note that an "off-card" application may access the IAS application without requiring a specific "on-card" application

The two configurations may exist together on the card.

4.2 High level functional requirements

4.2.1 The identification function

- **Pre-conds**: None
- **Parameters**: Which **subject** the off-card application wants to identify
- **Returned data**: The **public identity section** of the subject's identification file (or files).
- **Post-conds**: None

4.2.2 The authentication function

- **Pre-conds**: None, could occur within a **secure channel** if required by **security policy** (for cardholder public ID only)
- **Parameters1**:
  - o Which **subject** the off-card application wants to authenticate
- **Returned data1**:
  - o **Operational data** for the authentication process (keys, algorithms)
- **Parameters2**:
  - o The **Challenge/data** to be used by IAS to prove identity (signature)
- **Returned data2**:
  - o The **signed data** to be used by off card application to authenticate subject.
- **Post conds**: None

4.2.3 The signature function

- **Pre-conds**: Could occur within a secured channel if required by security policy
- **Parameters1**:
  - o Which subject the off-card application wants to use to perform signature (if multiple signature PIFs are available)
- **Returned data1**:
  - o Operational data for the signature process (keys, algorithms)
- **Parameters2**:
  - o The data to be signed by IAS.
- **Returned data2**:
  - o The signed data
- **Post conds**: None

4.2.4 The trusted signature function

- **Pre-conds**: **That the card holder has provided proof of desiring to perform this signature (by biometrics or PIN).** This constraint is because the signature engages legally the signer and must be strictly controlled.
- **Parameters1**:
  - o Which **subject** the off-card application wants to use to perform signature (if multiple signature PIFs are available)
- **Returned data1**:
  - o **Operational data** for the signature process (keys, algorithms)
- **Parameters2**:
  - o The **data** to be signed by AIS.
- **Returned data2**:

---

[3] This can be achieved by two channels to the smart card OR by interapplication communication

     o The signed data
- **Post conds**: None

4.3 Additional concepts

4.3.1 Security policy

The notion of security policy is directly attached to that of the security file of a subject. Each function involving a subject may be associated by the card issuer with some specific security constraints in a file (part of the identity file) as part of the scheme's security policies.

This policy may, for example, state that a card holder's public authentication requires a secure channel between card and terminal and the logging of the terminal's ID on the card.

This policy is thus **enforced** by the IAS application, even though the **means of enforcement** (security functions) may not be within the IAS application.

4.3.2 Secure channel

The notion of secure channel (between card and off card application) implies that trust has been attained between the two entities through **mutual authentication** leading to the negotiation of a common ciphering scheme to protect data exchanges between them.

4.3.3 The IAS application and security functions

It becomes clear from the previous analysis that the IAS application strongly depends on underlying security features of the smart card to operate, to the point that it can be reduced to an abstraction layer defining macro functions combining elementary security functions of the smart card and data from the identity files.
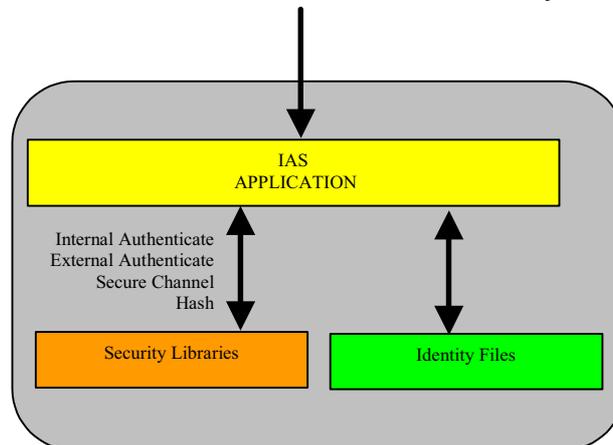

Figure 14: IAS and security functions

4.4 Low level functional definition at the card edge

Note that there are emerging standards for IAS on-card applications (e.g. ISO/IEC draft 7816-15), and these should be consulted when developing a detailed generic IAS card edge specification.

4.4.1 IAS availability

The smart card should be equipped with a standard function enabling an off-card application to determine whether or not the card is equipped with a generic IAS application.

Implementation Notes:

This should be attained by registering an AID (Application Identifier) with ISO for the GIF IAS. The answer to a Select APDU with this AID will then inform the off-card application of the availability of the application. In addition, the card may have an eURI application installed, or it may have an ATR file, or a DIR file – each of these may contain information about the available on-card applications.

4.4.2 Subjects List: IAS_SubList

The IAS application handles a minimum of two mandatory subjects but may manage more. In order to provide an off-card application with a referenced list of these subjects (which does not mean that the off-card application has rights to access them) a specific function is required.

4.4.3 Selection of Subject: IAS_Sel(Sub)

This function selects one subject which then becomes the default subject for all following IAS operations. Alternatively this function can be replaced by adding a Sub parameter to all the following functions.

4.4.4 Identification: IAS_GetID()

This function is required for an off-card application to obtain identification data from the card or from a URL about a given subject. The Identification data is returned.

4.4.5 Authentication: IAS_AuthGetData()

This function is required for an off-card application to obtain:
- The data which is to be authenticated (often identical to identification data)
- The operational means through which to perform this authentication (supported algorithms etc)

4.4.6 Authentication: IAS_IntAuth (Chal)

This function enables an off card application to authenticate a subject by sending a challenge (random value) to the IAS application. The challenge is then operated upon by the IAS application and sent back to the off card application which can verify it using the operational data/algorithms returned by IAS_AuthGetData().

4.4.7 Signature: IAS_SignGetData()

This function is required for an off card application to obtain the operational means through which to perform the signature (supported algorithms etc)

4.4.8 Signature: IAS_GenSign(Data)

This function actually performs the signature of the data (ID + hash of DTBS) provided as a parameter.

4.4.9 User Consent Protocols: IAS_GetCstDta()

This function returns the formats and protocols to be used to provide a proof of user consent from the current subject to the IAS application.

The returned data needs further formalisation and must be able to indicate for example what type of data will be used (PIN code, biometric), with what format and algorithms, etc.

4.4.10   User consent verification: IAS_UsrCstVerif(Data)

In line with the consent protocol enquiry function above, this function requires further formalisation. It is mandatory that the data is sent to the card by secure channel.

4.5 Implementation guidelines

The Open Smart Card Infrastructure for Europe (OSCIE) documents, and particularly the TB1 White Paper on Electronic Identity [R8], contain implementation information.

4.5.1 Asymmetric Cryptography

The framework assumes, at this level of the model, that the implementation of GIF IAS uses **asymmetric cryptography** and related **Public Key Infrastructures.**

GIF requires compliance with the list of European Directive Electronic Signature list of algorithms.

4.5.2 Certificates

The notion of signed certificate as specified in X509 (v3) covers most of the public fields required of an identity file.

Note that an identity file for a person will contain more than one certificate, as different key pairs shall be issued for authentication and signature. Per subject there shall be one certificate per functional key pair issued.

4.5.3 Private Elements of the identity file

The private elements of an identity file are the data elements which are NOT to leave the smart card once they are issued. These include essentially the private keys.
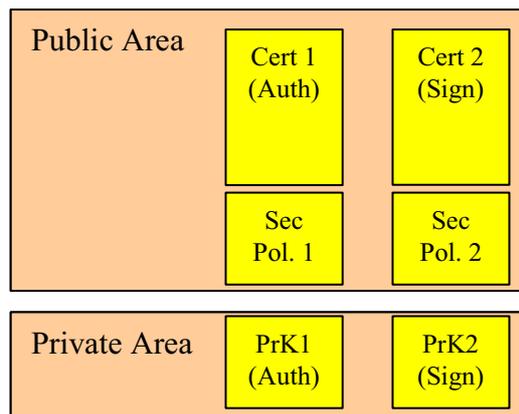

Figure 15: Typical Representation of an Identity file

4.5.4 Example of a typical certificate profile (Subject public ID)

This certificate implements the interoperable card holder public ID, and is to be formatted according to the specification X.509 v3.
- Version: Certificate version
- Issuer ID (UID)
  - o Country code: ISO Country code
  - o CA Code: Issuer code

- Issuer Access
  - o CRL/OCSP access point (where to verify revocation)
- Certificate ID: (Unique for an issuer)
- Certificate S-Alg: OID[4] of Algorithm used to sign Cert
- Certificate S-PuK: Public Key used to sign cert
- Subject ID: (unique for an issuer)
- Subject Data
  - o (See next sub-section)
- Cert Validity
  - o UTC not before
  - o UTC not after
- Subject Public Key
  - o Key usage code: Sign, authenticate….
  - o OID of Algorithm
  - o Public Key of subject for this usage

4.5.5 Privacy and the issue of subject data

The issue of privacy and subject data available in certificate is a very sensitive and political one.

The framework takes a very pragmatic view of this subject and considers that the subject data to be provided is aimed at making non-repudiable the card holder's electronically signed contractual agreements. In that sense the identification data should be similar to the data provided in order to sign and make valid a "paper" contract.

This essentially points to the following **mandatory fields** related to the subject:

- **Full Name** => As the basic Identity factor, including
  - o First name, middle name(s), last name(s)[5],
  - o "Local" representation (whatever the local script might be Arabic, Greek, Cyrillic) in compliance with ISO 10646-1
  - o "International" representation (ISO ASCII transcription, ISO 646)

The following fields are non mandatory but may be included in some schemes:
- Date of birth => For legal reasons age of "signer" can be critical, including:
  - o "Local" representation
  - o "International" representation (occidental calendar)
- Place of birth
- Gender/sex

The following field is non mandatory but is strongly recommended by GIF:

- National Identification number

4.6 GIF IAS and CEN/ISSS WS eSIGN Area K

Based on version 0 release 10 of the document [see A1 references], the SSCD application interface of CEN/ISSS WS eSIGN Area K, it clearly appears that, apart from "cosmetic" differences, all of the functions defined in GIF IAS are covered by the document. eSIGN K's latest draft is Ref A1; further comparison with eSIGN K will be required when the eSIGN K CWA is finalised, and *e*Epoch is developing this area.

---

[4]   Object Identifier (see X.509).
[5]   Spouse name or maiden names(s) as in use in card holder's country of origin

4.7 GIF IAS and NICSS Specifications

Based on the Card Interface Specification document version 1.00 issued by NICSS [see R6 references] the GIF IAS application fits in the NICSS framework as a standard card application.

In other words the Card Manager and its various functionalities as described in figure 5.2.1 of the NICSS document are essentially NON RELATED to the functionalities of IAS to the exception that the IAS application may need to access the NICSS Card Attribute and Card Key information as part of the IAS card subject identity file.

4.8 Qualified certificates and advanced electronic signature

Qualified certificates, such as for use to implement digital advanced electronic signature, contain attributes of the person identified (credentials of the card holder). The IAS application is intended for holding the official (public) identity of a real person, and therefore the mandatory subject data set does not include attributes of the person. However, other subject data sets may be stored in the card and an IAS service using them may use the IAS functions in the card, although (as noted above) these are designated non-interoperable and the CI is not responsible for them.

5 The Terminal Interface

5.1 General description

The role of the terminal to front office interface is to provide a standardized set of functions for the SP's front office application to communicate safely and efficiently with the terminal.

Terminal functions include driver modules to handle different card readers, card platforms and the on-card IAS application. These are in the infrastructure layer, and provision for interoperability between schemes at that level is in the interoperability adapters. However, the implementation models (GIF part 2) encourage migration towards generic card reader, card platform and on-card application interfaces.

Terminal functions may not necessarily be located in the physical terminal hardware used by the card holder. The physical terminal used by the card holder for transaction or session control may itself be a thin client on the network and also a router for messages directly to and from the card or via a secondary item of terminal hardware such as a secure card reader with integral PIN pad. A terminal function such as secure PIN transfer from keypad to card may be located in a combined card reader and PIN pad, in a terminal used by the card holder for transaction or session control, or at a network node. Once the infrastructure is secured and the card holder authenticated to the card, IAS-related terminal functions (such as secure interfacing with the card for signature generation) may be located either in the terminal used by the card holder, or at a network node.

Terminal management poses a very large number of issues concerning user interfaces, card platform handling and standard functionalities. The CEN/ISSS FINREAD CWA and the FINREAD consortium's linked to Global Platform and the STIP consortium are developing architectures, common specifications and protection profile (PP) methodologies for secure terminals. Further work is required to develop the GIF model in conjunction with emerging terminal architectures and secure PPs, and therefore the content of the present model in this area is limited.

The process of securing the communication between the card and the *e*-services can be achieved in two different approaches:

- End to end security, with secure (encrypted and, if necessary, signed) data channels between card and front office application (*e*-service) (or between card and a network node terminal function securely linked to the front office application), thus reducing the requirement for secure functions in the physical terminal used by the card holder to connect to the card.
- Security per interface
  - The card interface, between card and terminal (e.g. FINREAD terminal specification),
  - The terminal interface, between terminal (plus infrastructure) and off line e-service application (in the front office layer)
  - The PKI interface initiated by the e-service application and positioned between the terminal and the PKI service.

Interoperability between schemes, involving use of not-on-us cards and *e*-services makes this process even more complex by raising issues of security key management across scheme boundaries. These issues are not completely resolved in the framework, but GIF part 2 clause 4.3 introduces a model in which end-to-end communication of IAS data may be secured at the application level.

Business cases for secure services put much pressure on the terminals. On the long run end-to-end security must be preferred, because it makes the terminal infrastructure more transparent. For the short run however, solutions can be based on "secure per interface".

It is clear that the type of solution determines how the functions of the terminal have to be elaborated. Whatever the differences are, the high-level functions that have to be covered, in line with the GIF models and requirements involve:

- Secure Access Module (SAM) based on ISO 7816 protocols
- IAS handling component
- Connectivity handling component
- Human interface handling component
- E-service link handling component
- PKI handling component.

5.2 Description of Functions

We will essentially describe here the security functions which enable a smooth operation of IAS through various exchanges between the SP and the terminal in order to establish trust between the two entities.

A very large body of additional functions necessary to actually manage the operation of services between SP and the terminal is not described here (for example functions whereby the terminal indicates transaction incidents to the SP)

5.2.1 Capabilities: Term_GetCapab()

This function is essentially an "identification" function of the terminal whereby the SP will obtain not only a unique identifier for the terminal but also a complete description of the terminal capabilities such as:

- Type of input devices : Numeric, Alphanumeric, Fingerprint, etc
- Type of display device
- Security of input device
- Supported security protocols

Note that this list is far from complete or exhaustive and requires much formalisation work which is out of the scope of this document.

At this stage we shall only state that this information should be provided by the terminal in the form of one or more X509 (v3) certificates (identity and attributes of the terminal).

5.2.2 Authentication: Term_AuthGetData()

This function is required to obtain from the terminal:

- The data which is to be authenticated (might be equivalent to capability data)
- The operational means through which to perform this authentication (supported algorithms etc…)

5.2.3 Authentication: Term_Auth (Chal)

This function enables a SP to authenticate a terminal by sending a challenge (random value) . The challenge is then operated upon by the terminal and sent back to the SP which can verify it using the operational data/algorithms returned by Term_AuthGetData().

5.2.4 Authentication: SP_GetAuthData()

This function is symmetric to Term_GetAuthData() and is called by the terminal to the SP in order to obtain the SP's authentication data (certificate)

5.2.5 Authentication: SP_Auth(Chal)

This function is symmetric to Term_Auth(Chal) and enables the terminal to authenticate the SP.

5.2.6 Secure Channel: SP_Schan(Data)/Term_Schan(Data)

These two functions enable either of the parties to initiate a secure channel by generating a session key and sending it encrypted with the other party's public key (Data).

The exact protocol to be used for this secure channel is defined in the terminal capabilities.

5.2.7 Signature: Term_GenSign(Data)/SP_GenSign(Data)

These two functions enable either of the parties to ask the other one to sign a chunk of data sent as a parameter.

5.2.8 User Consent: Term_AskUserCst(Data)

This method is used by the SP to tell the terminal to ask the user to signify his/her consent to an operation.

The contents and format of the data parameter needs to be formalized but non-exhaustively and should include:

- Method of consent to be used
- Data to be displayed to user (critical if it is a trusted signature)

Note: The terminal is trusted to securely deploy this operation, transmit the consent data to the smart card AND return the smart card's answer to the SP.

6 The PKI Interface

The role of the PKI interface is to facilitate calls by the front office application of an SP to the verification services of a CI (acting as CA/VA) in order to verify the validity of a given certificate.

As far as this issue is concerned, GIF strongly recommends the use of the OCSP de facto protocol used in the industry. Support of this protocol both on the CI's and SP's side constitutes the definition of the PKI interface.

For the support of other methods and protocols (such as CRL), specific interfaces will need to be constructed, and the PKI-adapter is used for protocol conversion.

7   Implementation architecture summary

The figure below summarises the implementation architecture as defined by the framework. It provides a mapping between the building blocks (i.e. the layers), the generic interoperability interfaces and the processes.
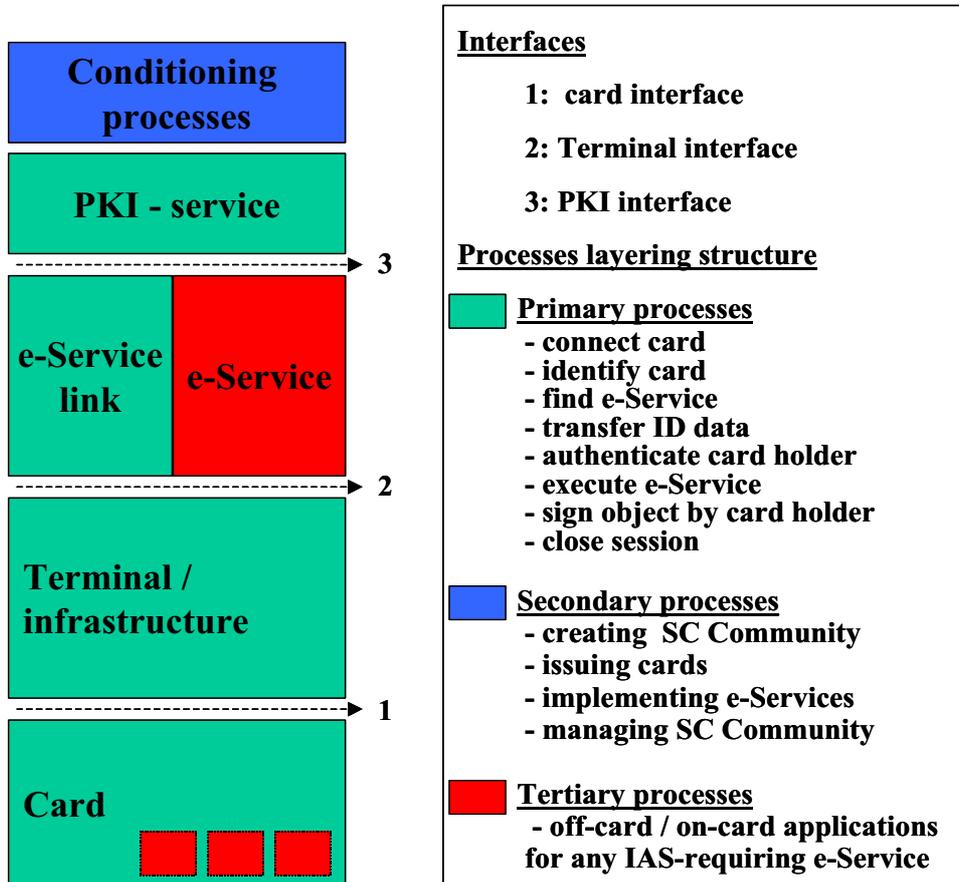
Conditioning processes

PKI - service

3

e-Service link | **e-Service**

2

Terminal / infrastructure

1

Card

Interfaces

1: card interface

2: Terminal interface

3: PKI interface

Processes layering structure

Primary processes
  - **connect card**
  - **identify card**
  - **find e-Service**
  - **transfer ID data**
  - **authenticate card holder**
  - **execute e-Service**
  - **sign object by card holder**
  - **close session**

Secondary processes
  - **creating SC Community**
  - **issuing cards**
  - **implementing e-Services**
  - **managing SC Community**

Tertiary processes
   - **off-card / on-card applications for any IAS-requiring e-Service**

Figure 16: GIF Architecture Summary

8 More information

GIF is part of the eEurope Smart Card Charter Common Specifications.

For more information on the Global Interoperability Framework (Parts 1-4) and its relationship to the eESC Common Specifications and Demonstrators you are invited to contact any of the following persons:

- Jan van Arkel   arkel@cardlife.nl
- Théo van Sprundel   theo.vansprundel@bull.nl
- Marc Lange   marc.lange@build-in-europe.be
- Laurent Den Hollander   laurent.den.hollander@sharp.co.uk
- Peter Tomlinson   pwt@iosis.co.uk

Annex A Document History

Name/function	Action	Circulation	Version
LDH	Initial Summary	GIF	V.0.5
LDH	Integration of ext sources	LDH	V.0.6
LDH	First Draft	GIF	V.0.7
LDH	Second Detailed Draft	GIF	V.0.8
Theo van Sprundel Jan van Arkel Marc Lange L. Den Hollander	Technical review and alignment with GIF Part 1 and 2 under preparation	Internal	V.0.9
LDH	Alignment and completion of document : Adapter/Interface, PKI interface, Terminal Interface	GIF	V.0.95
Jan van Arkel Marc Lange	Technical review, scope of document and adapter/generic IAS (section 2)	Public	V.0.96
Peter Tomlinson	Edit task 1st draft	Internal	V.0.97
Chris Makemson	Edit task 2nd draft	Internal	V.0.98
Peter Tomlinson	Edit task final technical draft	Internal	V.0.99
Peter Tomlinson	Edit task final draft, based on comments from Marc Lange	Internal	V.0.991
Marc Lange, Theo van Sprundel, Jan van Arkel	Technical review, Clause 5	Internal	V.0.992
Marc Lange	Final Review	Public	v.1.00

Annex B References

The following references are additions to the references listed in GIF Part 1.

Ref #	Author	Title	Version	Issuing date
R1	ISO/IEC	ISO/IEC 7816		
R2	ISO/IEC	ISO/IEC 7812		
R3	ISO/IEC	ISO 10646-1		
R4	ISO/IEC	ISO 646		

Background documentation

The following documents have been used as background documentation for the preparation of this document.

Ref #	Author	Title	Version	Issuing date
R4	TB 1 of eEurope Smart Card Charter	Requirement for European Public EID-card's Issuers supporting PKI and Certificate contents	v. 0.14	6 Feb. 2002
	TB 7 of eEurope Smart Card Charter	Current and future business models for multi application systems Multi application systems architecture Integration of multi application systems	v. 2.1 v. 0.9 v. 2.0	November 2002
R6	(Japan) NICSS	NICSS-Framework Scheme ftp://ftp.cenorm.be/public/eEurope-scc/GIF/NICSS/	v. 1.20	24 April 2001
R7	(USA) NIST	NIST Interagency Report (NISTIR) 6887, Government Smart Card Interoperability Specification(GSC-IS) http://smartcard.nist.gov	V 2.0	
R8	TB 1 of eEurope Smart Card Charter	White Paper: Open Smart Card Infrastructure for Europe (OSCIE) Vol 4 Part 1: Electronic Identity White Paper	V 0.5	15 Nov. 2002

Applicable documentation

The following documents are endorsed by this document.

Ref #	Author	Title	Version	Issuing date
A1	CEN/ISSS WS/ESIGN-K	"Application Interface for Smart Cards used as Secure Signature Creation Devices"	V. 0.8	12 March 2002
A2	CEN/ISSS WS/FINREAD	Technical Specifications CWA 14174		July 2001