


Document Owner:		Intended Reader:	
Smart Card Charter		Smart Card Charter: TBs (EU) NICSS (J)	
Project:			
 <p>GLOBAL INTEROPERABILITY FRAMEWORK FOR IDENTIFICATION, AUTHENTICATION AND ELECTRONIC SIGNATURE (IAS) WITH SMART CARDS</p>			
Document Title:			
<p>PART 3: RECOMMENDATION FOR IOP SPECIFICATIONS</p>			
Document type:			
<p>Blueprint</p>			
Prepared by:	Date:	Version and status:	
L. Den Hollander	20 August 2002	V.0.96 (internal)	

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)	GIF	V.0.96
			

TABLE OF CONTENTS

1	INTRODUCTION	5
1.1	BACKGROUND: THE SMART CARD CHARTER	5
1.2	SCOPE OF GIF PART 3	6
1.3	REFERENCES	6
1.3.1	<i>Background documentation</i>	6
1.3.2	<i>Applicable documentation</i>	7
1.4	DEFINITIONS AND ACRONYMS.....	7
1.4.1	<i>Definitions</i>	7
1.4.2	<i>Acronyms</i>	7
2	ADAPTERS AND GENERIC IAS APPLICATION, TWO APPROACHES TO IOP	9
2.1	THE SCMF OPERATIONAL MODEL	9
2.2	ADAPTERS.....	9
2.3	GENERIC IAS APPLICATION	10
3	THE GENERIC IAS APPLICATION INTERFACES	12
3.1	OVERVIEW	12
3.2	THE CARD INTERFACE	12
3.3	THE TERMINAL INTERFACE.....	12
3.4	THE PKI INTERFACE.....	12
4	THE CARD INTERFACE.....	13
4.1	GENERIC IAS FUNCTION: ARCHITECTURE AND ROLE.....	13
4.1.1	<i>Card Application and internal interfaces</i>	13
4.1.2	<i>IAS and subjects</i>	14
4.1.3	<i>Subject Identity Files</i>	15
4.1.4	<i>IAS application and security</i>	16
4.1.5	<i>IAS application and off-card applications</i>	16
4.2	FUNCTIONAL REQUIREMENTS (HIGH LEVEL).....	17
4.2.1	<i>The Identification Function</i>	17
4.2.2	<i>The Authentication function</i>	17
4.2.3	<i>The Signature function</i>	17
4.2.4	<i>The Trusted Signature Function</i>	18
4.3	ADDITIONAL CONCEPTS:	18
4.3.1	<i>Security policy</i>	18
4.3.2	<i>Secure Channel</i>	18
4.4	THE IAS APPLICATION AND SECURITY FUNCTIONS	18
4.5	FUNCTIONAL DEFINITION (LOW LEVEL)	19
4.5.1	<i>IAS availability</i>	19
4.5.2	<i>Subjects List: IAS_SubList</i>	19
4.5.3	<i>Selection of Subject: IAS_Sel(Sub)</i>	19
4.5.4	<i>Identification: IAS_GetID()</i>	19
4.5.5	<i>Authentication: IAS_AuthGetData()</i>	19
4.5.6	<i>Authentication: IAS_IntAuth (Chal)</i>	19
4.5.7	<i>Signature: IAS_SignGetData()</i>	19
4.5.8	<i>Signature: IAS_GenSign(Data)</i>	19
4.5.9	<i>User Consent Protocols: IAS_GetCstDta()</i>	19
4.5.10	<i>User consent verification : IAS_UsrCstVerif(Data)</i>	20
4.6	IMPLEMENTATION GUIDELINES.....	20
4.6.1	<i>Asymmetric Cryptography</i>	20
4.6.2	<i>Certificates</i>	20
4.6.3	<i>Private Elements of the identity file</i>	20
4.6.4	<i>Example of a Typical Certificate Profile (Subject public ID)</i>	20
4.6.5	<i>Privacy and the issue of subject data</i>	21
4.7	GIF/IAS AND CEN/ISSS GROUP K	21
4.8	GIF/IAS AND NICSS SPECIFICATIONS	21
5	THE TERMINAL INTERFACE	22

5.1	GENERAL DESCRIPTION.....	22
5.2	DESCRIPTION OF FUNCTIONS	22
5.2.1	Capabilities: <i>Term_GetCapab()</i>	22
5.2.2	Authentication: <i>Term_AuthGetData()</i>	22
5.2.3	Authentication: <i>Term_Auth (Chal)</i>	22
5.2.4	Authentication: <i>SP_GetAuthData()</i>	22
5.2.5	Authentication: <i>SP_Auth(Chal)</i>	22
5.2.6	Secure Channel: <i>SP_Schan(Data)/Term_Schan(Data)</i>	23
5.2.7	Signature: <i>Term_GenSign(Data)/SP_GenSign(Data)</i>	23
5.2.8	User Consent: <i>Term_AskUserCst(Data)</i>	23
6	THE PKI INTERFACE	24
7	MORE INFORMATION	25

TABLE OF FIGURES

Figure 1:	Four tiers in the methodology	5
Figure 2:	GIF Parts and the 4-Tier methodology	6
Figure 3:	SCMF operational Model	9
Figure 4:	IAS interoperability by adapters (functional model)	9
Figure 5:	IAS interoperability by adapters (stakeholder model)	10
Figure 6:	IAS interoperability by interfaces	11
Figure 7:	Generic IAS application interfaces (stakeholder model)	12
Figure 8:	The basic model of the functional boxes	13
Figure 10:	IAS application interfaces.....	14
Figure 11:	IAS subjects	14
Figure 12:	Subject Identity Files	16
Figure 13:	Case 1: Application with proprietary IAS and IAS application (Note that an “off-card” application may access the IAS application without requiring a specific “on-card” application)	16
Figure 14:	Case 2: Off-card application delegating IAS functions to IAS application (this can be achieved by two channels to the smart card OR by interapplication communication).....	17
Figure 15:	IAS and security functions.....	18
Figure 16:	Typical Representation of an Identity file.....	20

1 Introduction

1.1 Background: The Smart Card Charter ¹

This document is a product of the eEurope Smart Card Charter. It is the third part of the “Global Interoperability Framework for Identification, Authentication and electronic Signature (IAS) with Smart Cards for Internet Application”.

The Smart Card Charter identified the issues and an outline action plan for their resolution in order that smart cards can help to fulfil the expectations of citizens within the information society. At the end of 2000, the Charter published the Common Requirements², a document containing the action plans and deliverables of the 12 Smart Card Charter Trailblazer working groups. The action plan addresses both the citizens’ needs and those of the business community in terms of business cases, multi-functionality and interoperability of systems and infrastructure, and the provision of trust in all aspects of service delivery. The overall outcome of these action plans is being consolidated in a set of Smart Card Charter Common Specifications concluded at the end of 2002 and launched early in 2003.

As a part of these common specifications, a Global Interoperability Framework (GIF) for Identification, Authentication and Electronic Signature (IAS) has been developed. Its aim is to facilitate interoperability between the various IAS schemes emerging in Europe and more widely throughout the world.

The very starting point of GIF can be summarised with the image of smart cards as “The intelligent key to e-services”.

Defining the Global Interoperability Framework has been conducted in a step-by-step approach:

- **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 electronic signature;
- **GIF Part 2: Requirements for IAS functional interoperability**
a list of functional requirements and interoperability prerequisites to be used together with Part 1 for establishing a set of specifications for interoperability at IAS level;
- **GIF Part 3: Recommendation for IOP specifications (i.e. this document)**
guidance for enabling, implementing and operating IAS inter-operability;
- **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 (TINA-C, UML).

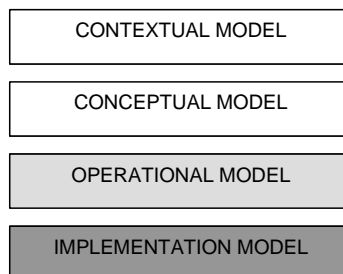


Figure 1: Four tiers in the methodology

¹ See <http://eeurope-smartcards.org/>

² See the document “eEurope Smart Cards Common Requirements: Executive summary”. Available on the website

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 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/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

1.2 Scope of GIF Part 3

The GIF IAS/IOP model and architecture, as described in Part 1, is designed to generically enable IAS interoperability across Smart Card Communities irrespectively (within reason) of the operational and technological divergences of the Smart Card Management Frameworks used.

For implementing IAS/IOP solutions, two approaches have been identified:

- The **IOP adapters**, for the situations when a smart card information system already exists and wants to be interoperable with a new service offered by a service provider or another smart card information system,
- The **“Generic IAS application”** common specifications, for the situations when, from day one, a smart card information system includes IAS/IOP in its objectives (e.g. for opening the smart card community to as much as possible e-service communities).

GIF Part 3 being aimed at providing “Recommendation for IOP specifications”, it will only cover the second approach and describe from a high level perspective the specifications of the Generic IAS application for each of the three layers and related stakeholders.

The detailed characteristics of IOP adapters are indeed 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 may benefit from this “bridge”.

More details on the distinction between these two concepts is given below under clause 2.

1.3 References

1.3.1 Background documentation

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

#	Author	Title	Version	Issuing date
R1	TB 1 of eEurope Smart	Requirement for European Public EID-card's Issuers supporting PKI and	v. 0.14	06.02.2002

#	Author	Title	Version	Issuing date
	Card Charter	Certificate contents		
R2	TB 7 of eEurope Smart Card Charter	To be completed		
R3	NICSS	NICSS-Framework Scheme ftp://ftp.cenorm.be/public/eEurope-scc/GIF/NICSS/	v. 1.20	24.04.2001
R4	US Nist	NIST Interagency Report (NISTIR) 6887, Government Smart Card Interoperability Specification(GSC-IS) http://smartcard.nist.gov	V 2.0	

1.3.2 Applicable documentation

The following documents are endorsed by this document.

#	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

1.4 Definitions and acronyms

1.4.1 Definitions

This section complement the definition section included in GIF Part 1. Therefore, only definitions which are new to the GIF have been introduced in this section.

Generic IAS application	The " Generic IAS application " defines a set of common interfaces to be used by each layers (i.e. card, infrastructure and front office application layers) and related stakeholders (i.e. user/card holder, access provider and service provider).
Identity File	An abstract object holding all the IAS data about a subject.
Interface	A standardized technical requirement facilitating interoperability
IOP Adapters	The IOP adapters act as "mediators", enabling operation across different systems to support the various "on-us" and "not-on-us" scenarios.
Subject	An entity described and managed by IAS (similar to a principal in PKI terminology)

1.4.2 Acronyms

This section complement the acronyms section included in GIF Part 1. Therefore, only acronyms which are new to the GIF have been introduced in this section.

2 Adapters and Generic IAS application, two approaches to IOP

2.1 The SCMF operational model

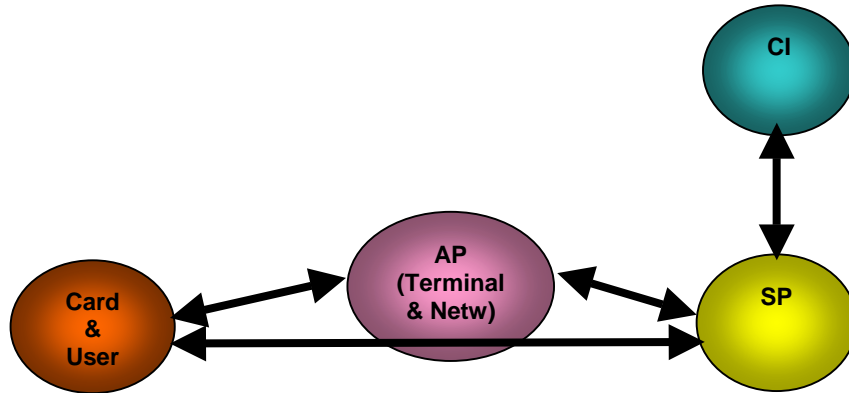


Figure 3: SCMF operational Model

The operational model of an SCMF during the “active” phase of a smart card’s life cycle is modelled as above.

The Card (User) interacts through a terminal and network (AP) with a front office application (SP) in order to gain access to a given service. In order to grant this service the service provider (SP) may additionally need to get in touch with the smart card’s initial issuer...the card issuer (CI).

2.2 Adapters

The **IOP adapters** act as “mediators”, enabling operation across different systems to support the various “on-us” and “not-on-us” scenarios.

Using more traditional terminology, the IOP adapters enable the recognition of the GIF/IAS **same** across a variety of acceptance devices and systems.

Part 1 identified the concepts and functions of the IOP adapters as follows:

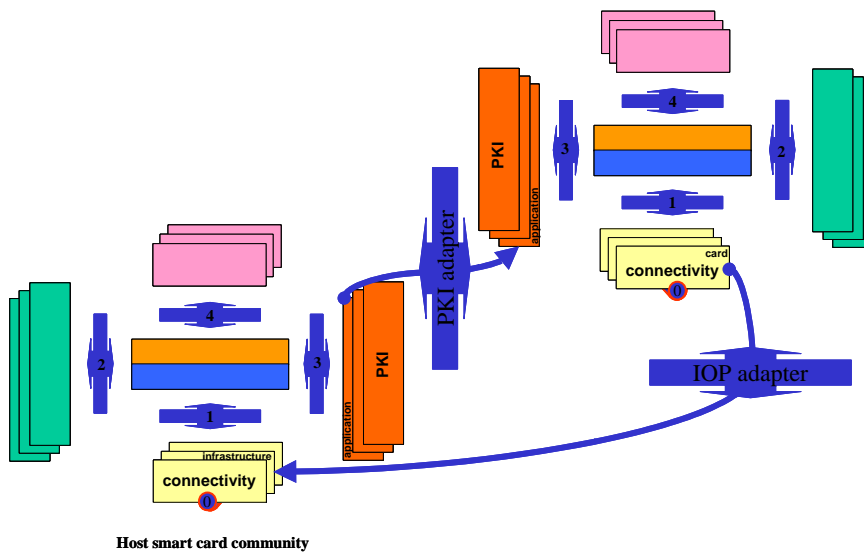


Figure 4: IAS interoperability by adapters (functional model)

Part 1 also gave a view of these adapters from the stakeholder viewpoint and the drawing below provides a simplified version of it, focused on IAS operations and in line with Figure 3.

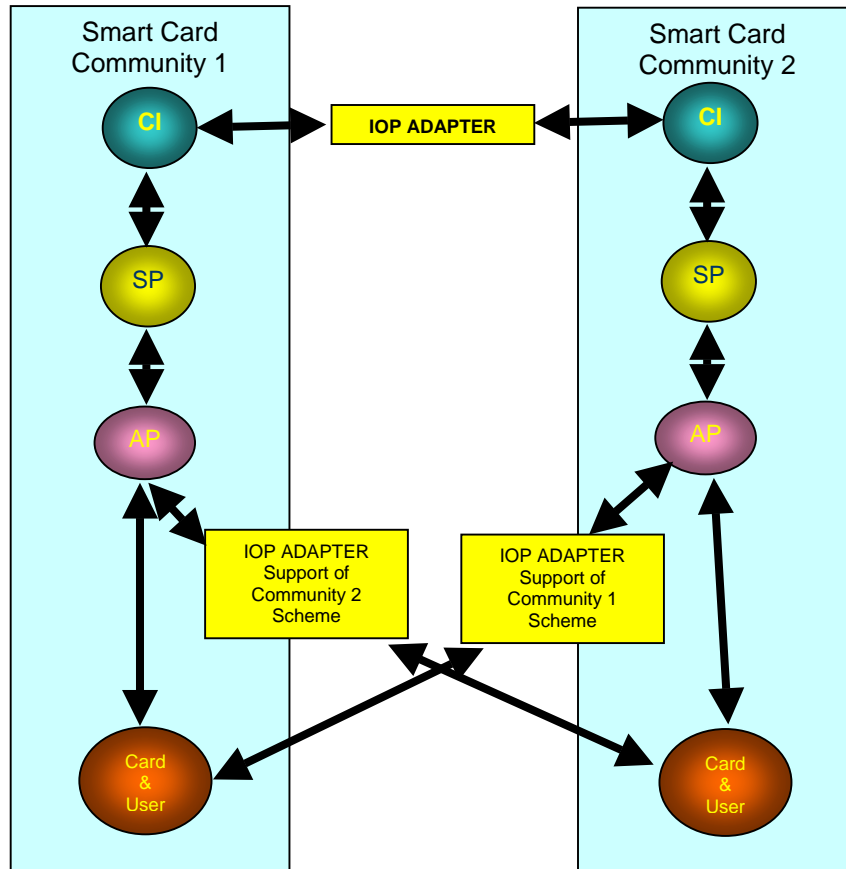


Figure 5: IAS interoperability by adapters (stakeholder model)

2.3 Generic IAS application

The “**Generic IAS application**” defines a set of common interfaces to be used by each layers (i.e. card, infrastructure and front office application layers) and related stakeholders (i.e. user/card holder, access provider and service provider).

This is a far more directive approach to interoperability than the adaptor’s one. It is based on the compliance by all participating SCMFs to a set of technical and operational requirements embodied in **IOP interfaces**.

Compliance to these interfaces enables any Service Provider to access and make use of the IAS functionalities of a smart card independently of where it was issued, hence technically removing the distinction between the “on-us” and “not-on-us” cases.

Note however that interfaces only enable a transparent **technical** interoperability of systems and that the issues surrounding legal recognition and liability of IAS signed transactions across smart card communities still needs to be negotiated/harmonised on a one-to-one basis.

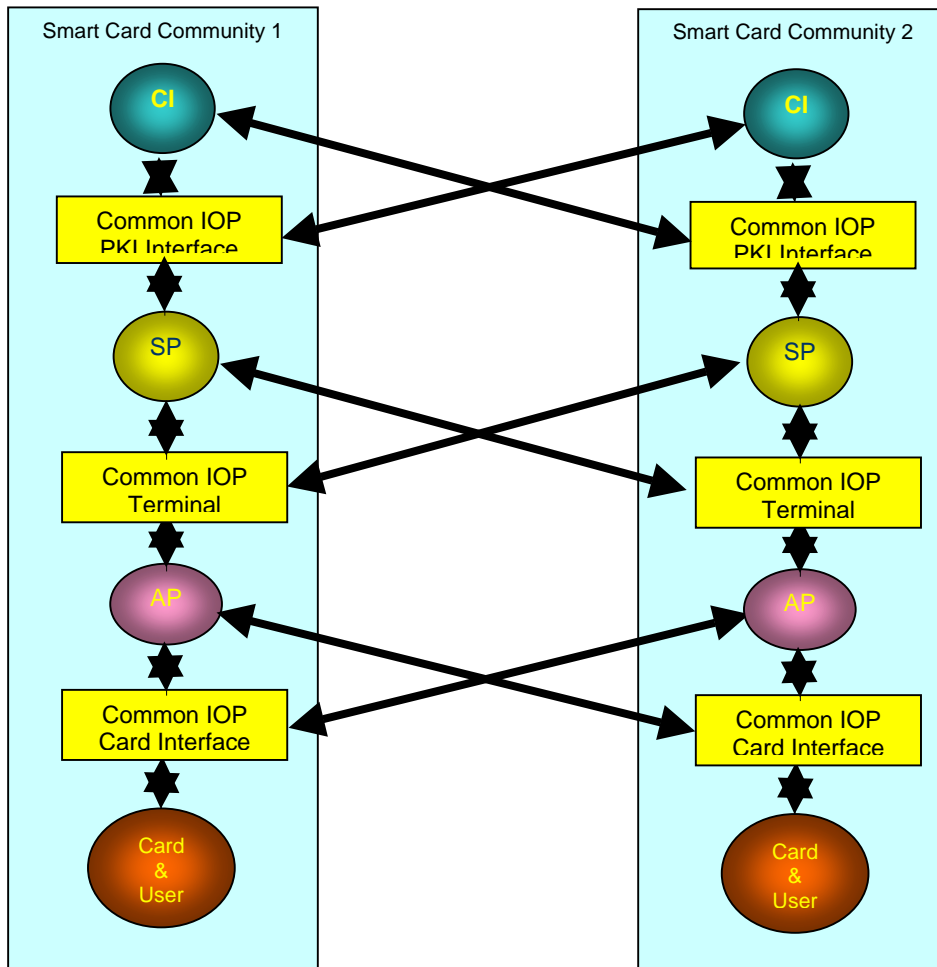


Figure 6: IAS interoperability by interfaces

3 The Generic IAS Application Interfaces

3.1 Overview

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, we first define the GIF IAS/IOP as a set of **interfaces** which plug in between these entities.

This leads to the following model:

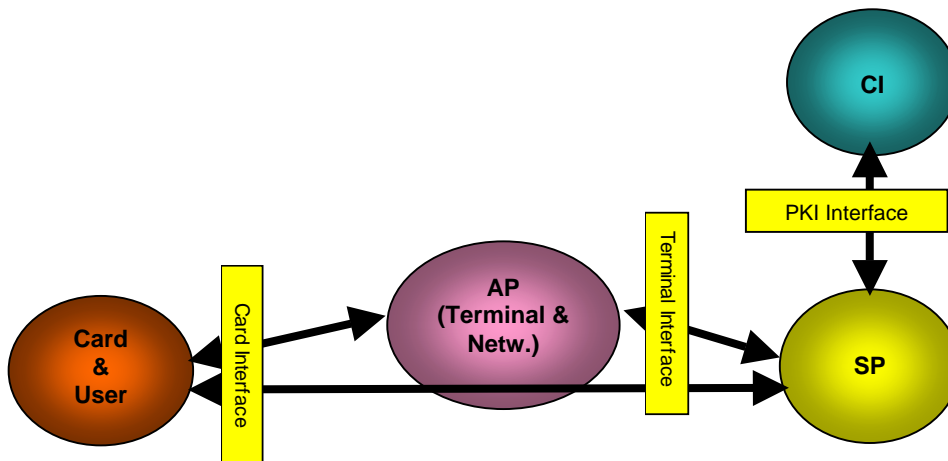


Figure 7: Generic IAS application interfaces (stakeholder model)

3.2 The Card Interface

The IAS Card Interface is the core of the GIF IAS/IOP and provides a **generic interface** to the smart card's **IAS services** 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 during authentication processes...)

4 The Card Interface

4.1 Generic IAS function: Architecture and Role

4.1.1 Card Application and internal interfaces

The below specifications are illustrated by the functional box model presented in GIF Part 1.

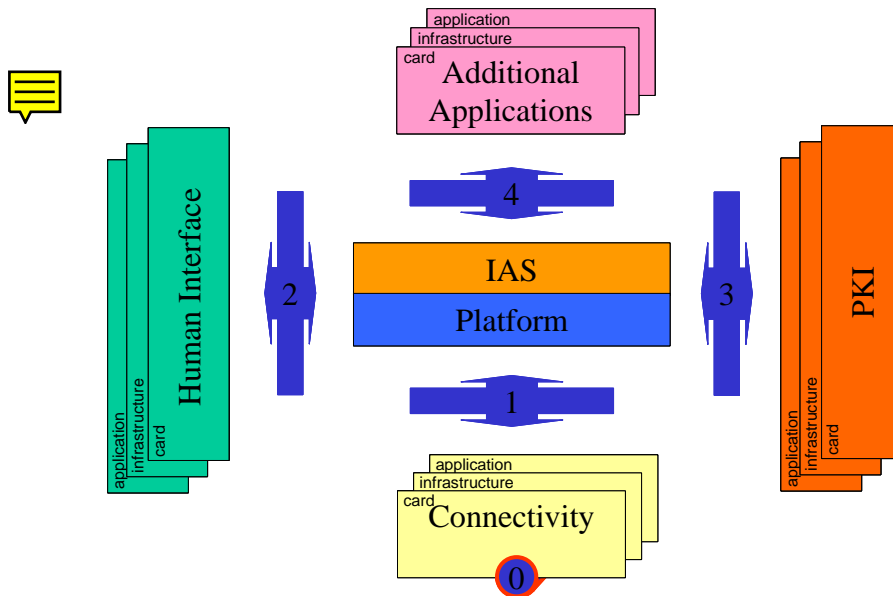


Figure 8: The basic model of the functional boxes

As a standard interface for “off-card” applications to access IAS services on the card, the IAS card interface will be essentially embodied as the interface to an IAS **card application**.

We **recommend** that the Card Interface be implemented in a **smart card application** format as opposed to as a part of the card’s run time environment/ operating system.

The IAS application **must** be accessible to off-card applications through standardized invocation methods (APDU’s for ISO 7816 cards, Java oriented solutions for Java cards.)

The IAS application **can** be made accessible to other card applications under the assumption that the smart card’s operating environment supports a secured 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.

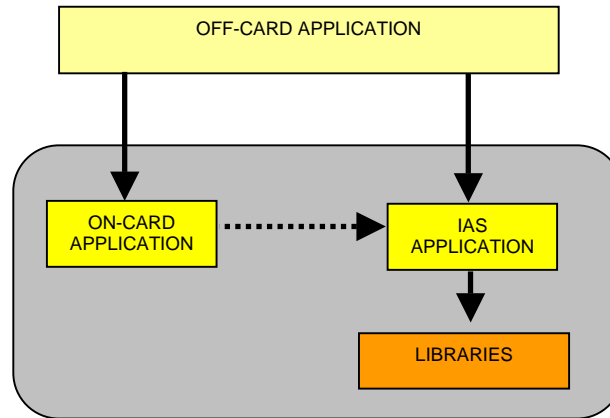


Figure 9: IAS application interfaces

4.1.2 IAS and subjects

The IAS card application provides Identification, Authentication and Signature functions for a set of subjects. Within the GIF IAS, we only recognize two subjects, namely:

- **The smart card:** The smart card as a uniquely identified and authenticated token by the card issuer.
- **The card holder’s public identity:** The public identity of the card holder authenticated by the card issuer.

An IAS card application **may** handle additional subjects as a card issuer may require but it **must** handle the smart card and the card holder’s public identity within the requirements of this document to support interoperability on the basis of the Generic IAS application” approach. The IAS application **may** provide a standardized interface to additional subjects. This however is out of the interoperability scope of this document. However, as far as they are managed by the IAS application, we consider that these subjects are **also** the responsibility of the **card issuer** (see section 0 above for example).

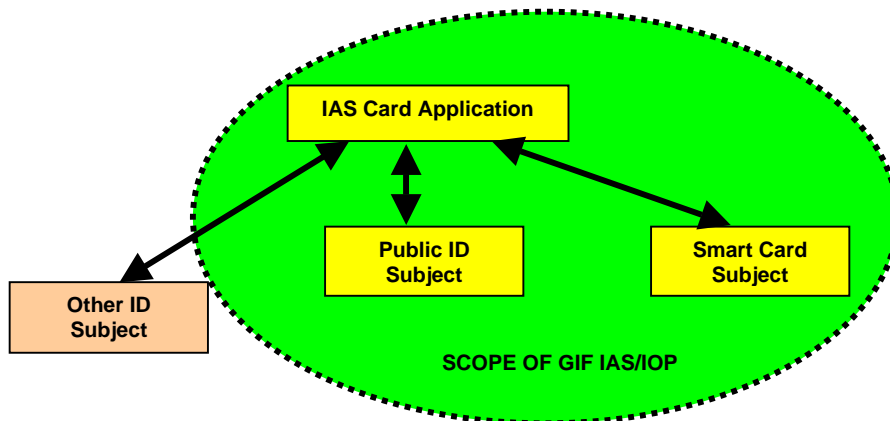


Figure 10: IAS subjects

Example: A government playing the role of Card Issuer may decide to issue smart cards with an IAS covering 3 subjects:

- The smart card: as defined above
- The card holder’s public ID: as defined above
- The card holder’s other ID subjects: Authenticated ID of the holder in relation to a certain role.

Identification

- **Generic Technical Definition:** A process through which an entity (A) makes a statement about its identity to another entity (B). Note that identification is ONLY a statement and has no xxxxxxxxxxxx something is missing
- **IAS IOP Definition:** A process through which the smart card provides descriptive data to an off-card application about any of the subjects managed by the IAS application.

Identification is a public function: Any off card entity is entitled without restriction to call onto the identification function and obtain the identification data from the smart card.

Authentication

- **Generic Technical Definition:** A process through which a claimed identification by entity A is successfully verified by entity B.
- **IAS IOP Definition:** A process through which the smart card provides an off card application with strong and verifiable electronic evidence of identity for any of the subjects managed by the IAS application.

Note that parts of the authentication process involving exchanges between the off card application and the card issuer are NOT covered here.

Signature

- **Generic Technical Definition:** A process whereby an authenticated entity A apposes a unique (non forgeable/non repudiable) mark on an object: "the contract". The signed contract is a legally binding commitment for the signing entity to comply with the terms of said contract.
- **IAS IOP Definition:** A process through which the smart card - triggered by the cardholder- performs a digital signature on an object presented by an off card application on behalf of one of the subjects managed by the IAS application.

Case of the Smart Card subject



- **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 prerequisites.
- **From an operational standpoint:** The signature generated by the smart card subject will essentially be used as part of security processes like secured channel management.

Case of the Public ID subject (Trusted signature)

- **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/her-self.
- **From an operational standpoint:** The signature generated by the Public ID subject under control of the card holder will only be used as a legally binding electronic signature.

4.1.3 Subject Identity Files

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

In other words, the IAS can be resumed to:

- Processes to perform the authentication and signature operations

- Data about the subjects including the publicly available identification data.

In the following we shall name these data sets “Subject Identity Files”.

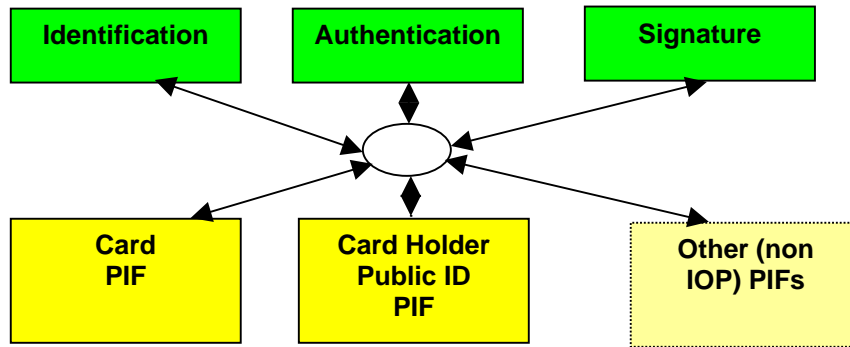


Figure 11: Subject Identity Files

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 has any liability for the smart card security.

4.1.5 IAS application and off-card applications

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**.

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

This leads to the following possible configurations:

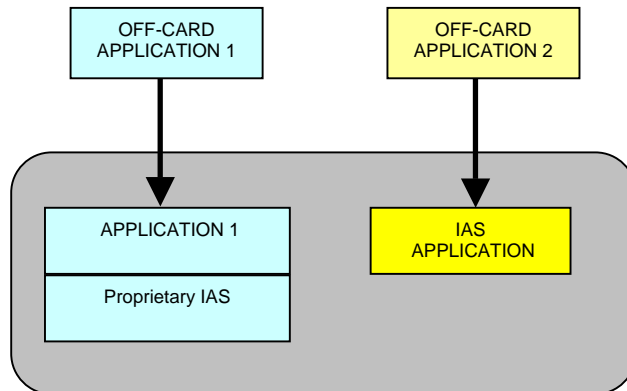


Figure 12: Case 1: Application with proprietary IAS and IAS application (Note that an “off-card” application may access the IAS application without requiring a specific “on-card” application)

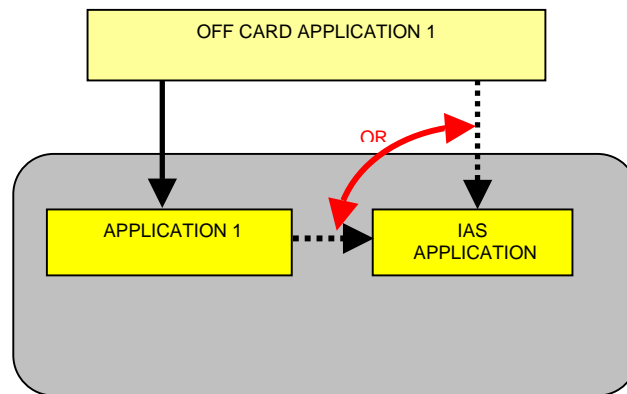


Figure 13: Case 2: Off-card application delegating IAS functions to IAS application (this can be achieved by two channels to the smart card OR by interapplication communication)

Note that case 2 is NOT exclusive of case 1!

4.2 Functional Requirements (High Level)

4.2.1 The Identification Function

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

4.2.2 The Authentication function

- **Pre-conds:** None, could occur within a **secured 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 perform signature
- **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:**
 - Which **subject** the off-card application wants to perform signature redaction?
- **Returned data1:**
 - **Operational data** for the signature process (keys, algorithms)
- **Parameters2:**
 - The **data** to be signed by AIS.
- **Returned data2:**
 - 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 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) named the security policy.

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.

4.4 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.

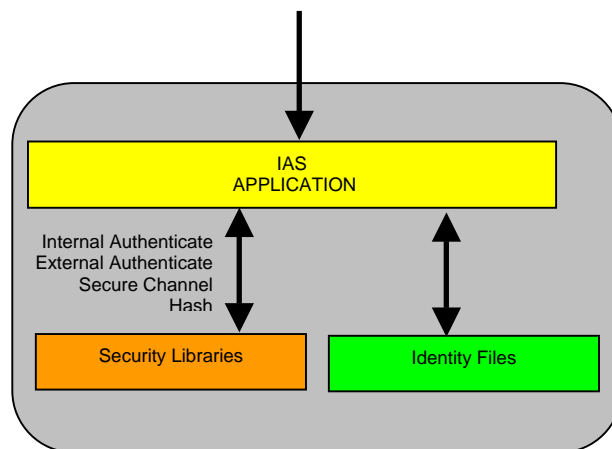


Figure 14: IAS and security functions

4.5 Functional Definition (Low Level)

4.5.1 IAS availability.

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

Implementation Note: In the case of ISO 7816 smart cards, 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.

Implementation Note: In the case of Java Cards ??? I had attached a file from Gemplus. That isn't helpful?

4.5.2 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.

4.5.3 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.

4.5.4 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.

4.5.5 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...)

4.5.6 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 AIS_AuthGetData().

4.5.7 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...)

4.5.8 Signature: IAS_GenSign(Data)

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

4.5.9 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.

4.5.10 User consent verification : IAS_UsrCstVerif(Data)

4.6 Implementation Guidelines

4.6.1 Asymmetric Cryptography

It is clear that the implementation of the AIS depends on **asymmetric cryptography** and related **Public Key Infrastructures**.

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

4.6.2 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 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.

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.

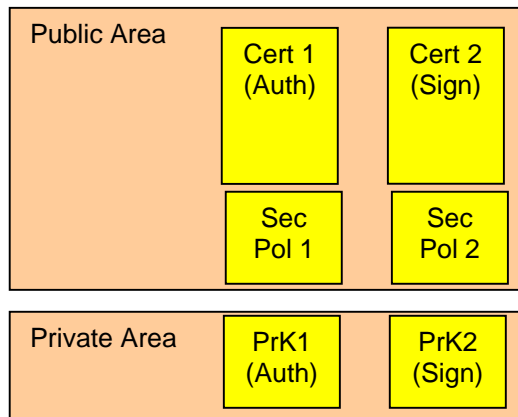


Figure 15: Typical Representation of an Identity file

4.6.4 Example of a Typical Certificate Profile (Subject public ID)

- Version: Certificate version (in compliance with X509 v3)
- 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 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 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

4.6.5 Privacy and the issue of subject data

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

We shall take a very pragmatic view of this subject and consider that the subject data to be provided are aimed at to make 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)³,
 - 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)
- **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 strongly recommended by GIF:

- **National Identification number**

4.7 GIF/IAS and Cen/ISSS Group K

Based on version 0 release 10 of the document [see A1 references], the SSCD application interface of CEN ISSS Group K, it clearly appears that, apart from "cosmetic" differences, all of the functions defined in GIF IAS are covered by the document.

(Actual mapping to be inserted here)

4.8 GIF/IAS and NICSS Specifications

Based on the "Card Interface Specification" document version 1.00 issued by NICSS [see R3 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.

³ Spouse name or maiden names(s) as in use in card holder's country of origin

5 The Terminal Interface

5.1 General description

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

Note that this is a critical issue since the terminal is the keystone of any transaction linking the Card, the card holder and the service provider!

Terminal management poses a very large number of issues concerning user interfaces and standard functionalities.

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.....
- 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 the 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, to transmit the consent data to the smart card AND to return the smart card's answer to the SP.

To be continued

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 in order to verify the validity of a given certificate.

As far as this issue is concerned, GIF entirely relies on the use of the OCSP, “de facto” protocol used in the industry.

Support of this protocol both on the CIs and SPs 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.

7 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