


Document Owner:		Intended Reader:	
<b>Smart Card Charter</b>		<b>Smart Card Charter: TBs (EU)</b> <b>NICSS (J)</b>	
Project:			
 <p><b>GLOBAL INTEROPERABILITY FRAMEWORK FOR IDENTIFICATION, AUTHENTICATION AND ELECTRONIC SIGNATURE (IAS) WITH SMART CARDS</b></p>			
Document Title:			
<p><b>PART 2:</b></p> <p><b>REQUIREMENTS FOR</b></p> <p><b>IAS FUNCTIONAL INTEROPERABILITY</b></p> <p><b>(GIF PART 2)</b></p>			
Document type:			
<b>Blueprint</b>			
Prepared by:		Date:	Version and status:
<b>Theo van Sprundel</b> <b>Jan van Arkel</b> <b>Marc Lange</b> <b>Yvan Pirene</b>		<b>15 November 2002</b>	<b>V. 2.1</b>  <b>External</b>

**HISTORY**

Name/function	Action	Circulation	Version
Theo van Sprundel & Marc Lange	Structure of the document	Internal	v. 0.0
Marc Lange	Inclusion of applicable NICSS prerequisites	Internal	v. 0.1
Marc Lange	Update of the structure after meeting 25 January	Internal	v. 0.2
Theo van Sprundel	Update and inclusion of eESCC requirements	Internal	v. 0.3
Theo van Sprundel & Marc Lange	Review and inclusion of examples	Internal	v. 0.4
Theo van Sprundel & Marc Lange	Quality Review	External	v. 0.5
Theo van Sprundel & Marc Lange	Restructure document (in line with new DLV # 1)	Internal	v. 1.0x
Theo van Sprundel	Extended summary	Internal	v. 1.00
Theo van Sprundel Jan van Arkel	Complementary text	Internal	v. 1.01
Yvan Pirenne	Technical and quality review	Internal	v. 1.02
Theo van Sprundel Jan van Arkel Yvan Pirenne L. Den Hollander	Technical review and alignment with GIF Part 3 under preparation	Internal	v. 1.03
Theo van Sprundel	Update	Internal	v. 1.04
Marc Lange Yvan Pirenne	Update, alignment with GIF Part 4 under preparation and technical review Implementation of NICSS comments #1, 4, 5 and 6	Internal	v. 1.05
Theo van Sprundel	Update	Internal	v. 1.06
Yvan Pirenne	Update	Internal	v. 1.07
Theo van Sprundel	Update	Internal	v. 2.00
Jan van Arkel	Review	Internal	v. 2.01
Theo van Sprundel	Finalisation	External	v. 2.1

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION</b> .....	<b>5</b>
1.1	BACKGROUND.....	5
1.2	SCOPE OF GIF PART 2.....	6
1.3	REFERENCES.....	7
1.3.1	<i>Background documentation</i> .....	7
1.3.2	<i>Applicable documentation</i> .....	8
1.4	DEFINITIONS AND ACRONYMS.....	8
1.4.1	<i>Definitions</i> .....	8
1.4.2	<i>Acronyms and abbreviations</i> .....	8
<b>2</b>	<b>PRE-REQUISITES TO IOP</b> .....	<b>9</b>
2.1	INTRODUCTION.....	9
2.2	PRE-REQUISITES ON THE ROLES.....	10
2.2.1	<i>Prerequisites on CI-, SP- and CH- roles concerning the ‘active IAS process’</i> .....	10
2.2.2	<i>Pre-requisites on the CI role, concerning the ‘conditional processes’</i> .....	11
2.2.3	<i>Pre-requisites on the SP activities when delivering e-Services</i> .....	13
2.3	PRE-REQUISITES ON THE FUNCTIONS.....	14
2.4	PRE-REQUISITES ON THE DATA.....	14
2.5	PRE-REQUISITES ON THE BUILDING BLOCKS.....	15
2.5.1	<i>Smart Card layer related prerequisites</i> .....	15
2.5.2	<i>Infrastructure layer related prerequisites</i> .....	16
2.5.3	<i>Front office layer related prerequisites</i> .....	17
<b>3</b>	<b>OPERATIONAL REQUIREMENTS FOR IAS INTEROPERABILITY</b> .....	<b>18</b>
3.1	INTRODUCTION.....	18
3.2	FUNCTIONAL REQUIREMENTS.....	18
3.2.1	<i>Introduction</i> .....	18
3.2.2	<i>Functional boxes</i> .....	18
3.3	REQUIREMENTS FOR STAKEHOLDERS’ ROLES.....	20
3.3.1	<i>Card Issuer setting-up an SCC</i> .....	20
3.3.2	<i>CI ensuring trust within its SCC</i> .....	24
3.3.3	<i>Service provider setting-up an e-service community</i> .....	25
3.3.4	<i>SP ensuring trust within its e-service community</i> .....	28
3.3.5	<i>Card holder</i> .....	28
3.3.6	<i>The card holder as part of a trust system</i> .....	30
3.3.7	<i>Other stakeholders</i> .....	31
3.3.8	<i>Other stakeholder contributing in ensuring trusts</i> .....	32
<b>4</b>	<b>IMPLEMENTATION REQUIREMENTS FOR IAS INTEROPERABILITY</b> .....	<b>33</b>
4.1	REQUIREMENT FOR AN IAS/IOP IMPLEMENTATION STRATEGY.....	33
4.1.1	<i>e-Services in the centre</i> .....	33
4.1.2	<i>Which IAS /IOP is desired</i> .....	33
4.1.3	<i>Who is concerned by IAS/IOP implementation strategy</i> .....	33
4.2	THE REQUIREMENTS FOR IAS/IOP TECHNICAL INFRASTRUCTURE.....	34
4.2.1	<i>IOP &amp; PKI adapters</i> .....	34
4.2.2	<i>IOP conformance testing</i> .....	36
4.3	REQUIREMENT FOR IMPLEMENTING IAS/IOP PROCESSES.....	36

**5 APPENDIX ..... 38**

5.1 MORE INFORMATION..... 38

5.2 OVERVIEW OF GIF REQUIREMENTS (FOR PURPOSES OF RFI, RFP OR “GAP ANALYSIS” COMPARING TO EXISTING SYSTEMS)..... 39

    5.2.1 *General implementation requirements* ..... 39

    5.2.2 *Operational and implementation requirements overview table*..... 40

**TABLE OF FIGURES**

Figure 1: Four tiers in the methodology ..... 6

Figure 2: GIF Parts and the 4-Tier methodology ..... 6

Figure 3: Trust model as the basis of the GIF-concept..... 10

Figure 5: Modelling the IOP Adapters (here in scenario 1) ..... 35

**INDEX OF TABLES**

Table 1: Mandatory IAS processes.....10

Table 2: Recommended conditional processes.....11

Table 3: Functional boxes, ruled by standard interfaces .....18

Table 4: Card issuer issues .....20

Table 5: Card Issuer trust requirements.....25

Table 6: Service provider issues.....26

Table 7: Service Provider trust-issues .....28

Table 8: Card holder issues .....29

Table 9: Card holder trust issues .....30

Table 10: Other stakeholders issues .....31

Table 11: Other stakeholders trust issues .....32

Table 12: IAS processes in the three IOP scenarios .....37

# 1 Introduction

---

## 1.1 Background

This document is a product of the eEurope Smart Card Charter (eESC)<sup>1</sup>. It is the second part of the “Global Interoperability Framework for Identification, Authentication and electronic Signature (IAS) with Smart Cards for Internet Application”.

The main purpose is to present the functional requirements and operational implementation prerequisites to be used together with Part 1 for establishing interoperable smartcard communities in general, and IOP / IAS systems in particular.

eESC 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, eESC published the Common Requirements<sup>2</sup>, a document containing the action plans and deliverables of the 12 eESC 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, as well as the provision of trust in all aspects of service delivery. The overall outcome of these action plans is being consolidated in a set of eESC Specifications to be 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 vision driving GIF is the high expectation of smart cards as “**The intelligent key to e-services**” for all citizens in the domains of local and trans-national Government.

The Global Interoperability Framework is in 4 parts:

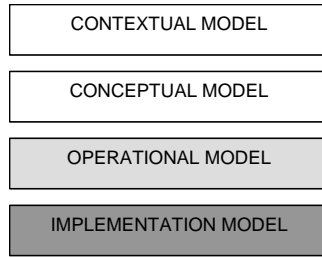
- **GIF Part 1: Contextual and conceptual modelling**  
an in-depth modelling of the smart card, its environment and interoperability issues with regards to identification, authentication and electronic signature;
- **GIF Part 2: Requirements for IAS functional interoperability** (i.e. this document)  
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**  
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.

---

<sup>1</sup> See <http://europe-smartcards.org/>

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

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



**Figure 1: Four tiers in the methodology**

**Mapping the framework with the methodology**

The mapping of the four parts of the GIF 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 with regards to the generic IAS module approach.

	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 2**

This part of the GIF (GIF part 2) addresses the requirements in the IAS-interoperability Framework for both the operational model (chapter 3) and the implementation one (chapter 4).

It outlines, following the models presented in GIF Part 1:

- The stakeholders' responsibilities and liabilities in organising the IAS-interoperability,
- The requirements to be met by IT-functions,
- The requirements to be met by the data flows and
- The requirements to be met by the system components involved.

The basic criteria for identifying the requirements are:

- Ensuring trust to all parties involved
- Applying available standards, technical specifications and relevant products

- Creating and/or protecting a business case for all parties
- Supporting user convenience

This document covers the requirements, which have been brought up in different European bodies involved in smart cards as well as in:

- Public ID
- PKI and security
- Human interface
- Multi-application
- Card readers/terminals
- e-Government

The intended readers of this document are:

- Policy makers/advisors establishing the common requirements for eEurope Smart Card Charter
- Decision-makers and consultants involved in preparing a smart card community with generic IAS for multi services, especially communities for e-government services.
- Those who are involved in establishing RFI's and RFP's for multi service and interoperable IAS
- Project leaders for pilots on generic IAS

### 1.3 References

#### 1.3.1 Background documentation

This clause lists the main documents used as background information in the preparation of this GIF Part 2.

#	Author	Title	Version	Issuing date
R1	TB 1 of eEurope Smart Card Charter	Requirement for European Public EID-card's Issuers supporting PKI and Certificate contents	v. 0.14	06.02.2002
R2	TB 7 of eEurope Smart Card Charter	<ul style="list-style-type: none"> <li>• Current and future business models for multi application systems</li> <li>• Multi application systems architecture</li> <li>• Integration of multi application systems</li> </ul>	.	
R3	NAME-ES	Network Authentication Module for internet End-userS		
R4	NICSS	NICSS-Framework Scheme	v. 1.20	24.04.2001

### 1.3.2 Applicable documentation

Provisions in the following documents are referenced within this GIF Part 2.

#	Author	Title	Version	Issuing date
A1	CEN/ISSS WS/ESIGN-K	“Application Interface for Smart Cards used as Secure Signature Creation Devices”	V. 0.12	4 November. 2002
A2	CEN/ISSS WS/FINREAD	Technical Specifications CWA 14174	-	July 2001

## 1.4 Definitions and acronyms

### 1.4.1 Definitions

This clause defines terms introduced in this GIF Part 2. Additional terms are defined in other GIF Parts. .

Business rules	These SP business rules are key to the functioning of an e-service community. They define the conditions under which cardholders are provided access to e-Services. They are therefore strongly depending upon the specifications agreed between the service provider and a smart card community in which it deploys its services. As presented in the function model defined in Part 1, the business rules are technically to be considered as part of the “additional application” function.
----------------	--

### 1.4.2 Acronyms and abbreviations

This clause defines acronyms and abbreviations introduced in this GIF Part 2. Additional terms are defined in other GIF Parts. .

ECC	Elliptic Curve Cryptography
EID	Electronic Identifier
ICT	Information and Communication Technology
MTBF	Mean-Time Between Failure
OTBS	Object to be signed
SSCD	Secure Signature Creation Device
SLA	Service Level Agreements
TLV	Tag Length Value
VLA	Vulnerability Level Assurance

## 2 Pre-requisites to IOP

---

### 2.1 Introduction

This chapter identifies the interoperability pre-requisites on (the generic) IAS between smart card communities for each of the four models introduced in GIF part 1:

1. The (basic processes and) roles model
2. The functional boxes model
3. The data model
4. The (technical) building blocks model

These prerequisites are based on the vision how the smart card community works when applying common IAS/IOP for e-services starting from the basic assumption that the smart card community wants to apply an architecture fostering the extension to additional e-services thanks to the provision of IAS common services.

In accordance with the role model in GIF part 1, the Card Issuer is the 'primus inter pares' of stakeholders involved in offering the generic IAS process. Its primary task is to manage the smart card base and the initial set of e-services. This concerns various tasks that are directly associated with "card issuance":

- Acquiring cards
- Personalising and initialising them
- Maintaining the cards base

In GIF, the CI is also assigned responsibility for contracting or establishing Service Level Agreements (SLA) with the following stakeholders:

- Certificate Provider(s)
- Access Provider(s)
- Service Provider(s).

The responsibilities and relationships of the primary entities in the basic roles model can be summarised as follows:

- The **card issuer** as the "primus inter pares"; is responsible for
  - o Card issuing and card management tasks<sup>3</sup>:
  - o Organising the smart card community
    - Triggering certificates issuance, maintaining them and offering verification services to all (on-us and not-on-us) service providers
    - Making access available to high level e-services
    - Establishing IOP arrangements to other smart card communities
- The **service provider** is primarily oriented to
  - o The card issuer with which he has made all necessary arrangements
  - o The cardholders whom he welcomes to his service
- The **card holder** has his/her basic relations with
  - o The card issuer (in order to belong to a smart card community)
  - o A number of chosen service providers

---

<sup>3</sup> The full role model described under section 2.2.2 of GIF Part 1 distinguishes the CI role from the SCC Administrator and Access provider ones. For the sake of simplicity however, this document groups them all together since they are often, in particular in the e-Government field, assumed by the same organisation.

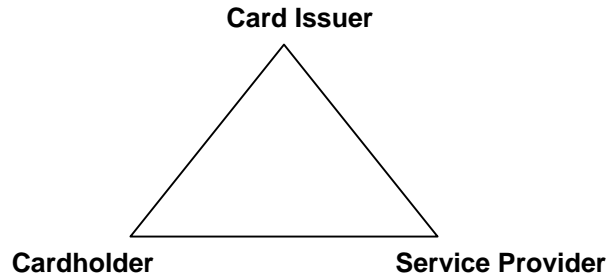


Figure 3: Trust model as the basis of the GIF-concept

## 2.2 Pre-requisites on the roles

All pre-requisites on roles are based upon the processes they are supporting for the delivery of common and trusted IAS services. These processes will be classified as primary, secondary and tertiary processes depending from the relationship they have with the IAS function

### 2.2.1 Prerequisites on CI-, SP- and CH- roles concerning the ‘active IAS process’

The processes listed below are considered as the Primary IAS processes; they are those through which the IAS services can interact with e-services.

1. <b>Connect</b> (contact or contactless) smart card to (modules in) terminal and secure the links
2. <b>Identify/validate and accept/reject</b> the card in the infrastructure + identify/validate and accept/reject the terminal / terminal application (authenticate the ‘building blocks’)
3. <b>Find, open and interact</b> with the requested e-service and read the business rules for the requested e-service
4. <b>Transfer ID data</b> to the e-service / make data available
5. <b>Authenticate</b> card holder (if requested for e-service)
6. <b>Execute</b> e-service (IAS is passive)
7. <b>Sign</b> an information object (if requested for e-service)
8. <b>Update</b> administrative log-files and close the IAS session

Table 1: Mandatory IAS processes

Note that each service provider may/may not use the technical capability of using the common IAS services for offering access to its own e-services. If it does, the SP will always provide access under the control of its own “business rules”. These SP business rules are key to the functioning of an e-service community. They define the conditions under which cardholders are provided access to e-Services. They are therefore strongly depending upon the specifications agreed between the service provider and a smart card community in which it deploys its services. As presented in the function model defined in Part 1, the business rules are technically to be considered as part of the “additional application” function.

## 2.2.2 Pre-requisites on the CI role, concerning the ‘conditional processes’

The processes listed below are the Secondary IAS processes aimed at ensuring that the IAS services provided by the card issuer can be trusted by service providers and card holders.

The CI is responsible for the processes by which the smart card community is created and maintained. These processes are considered by the GIF, although it focuses on IAS the interoperability only because they are needed to comply with the following criteria:

- Trust / security
- Technical compatibility
- Business cases respecting all stakeholders responsibilities
- User convenience

Note that the recommended ‘conditional’ processes identified in the following table do not always need to be applied in the particular sequence shown.

<b>1</b>	<b>Creating a Smart Card Community</b> (Registration and internal certificates issuance)
1.1	• Register smart card community and external secure suppliers
1.1	• Verify the compliance of SCC stakeholders with CI requirements and register them i.e. establish ID + URL
1.2	• Provide PKI certificate to registered stakeholders as a technical proof of their registration
1.3	• Verify the compliance of all secure “building blocks” (technical components), register them and provide them with PKI Certificates
<b>2</b>	<b>Issuing and maintaining cards</b>
2.1	• Personalise card
2.2	• Issue card holder certificates
2.3	• Initialise the card
2.3	• Enrol the card holder
2.4	• Maintain life cycles (cards, card holder ID, certificates)
<b>3</b>	<b>Registering e-service</b> (including at post issuance)
3.1	• Test/Accept IAS connection software offered by the e-service provider
3.2	• Test/Accept “on-card application” software offered by the e-service provider
3.3	• Authorise download or download “on-card application” offered by the e-service provider
<b>4</b>	<b>Establishing &amp; maintaining IOP</b>
4.1	• Create IOP adapter, install rules and policies
4.2	• Maintain IOP adapters
<b>5</b>	<b>Managing the SCC</b>
5.1	• Log the use of cards, IAS and front office
5.2	• Execution, acquiring and settlement (between stakeholders)

**Table 2: Recommended conditional processes**

## **1. “Registration and internal certificates issuance”**

### *1.1 Register smart card community and secure external suppliers*

Required functions are:

- CI registration and certification (in relation to the issued cards, see below under 1.2)
- CI arranges its own certificate (or the legal body of the smart card community arranges the CI certificate) as a basis for all other certification of stakeholders. .

### *1.2 Register SCC stakeholders*

Required functions are:

- CA & RA registration and certification (in relation to the card issuer for IAS functionality)
- AP registration
- SP registration
- Content provider registration (in relation to SP)

### *1.3 PKI certificate stakeholders*

Required functions are:

- CA & RA certification (in relation to the card issuer for IAS functionality) )
- AP certification
- E-Service provider certification
- Content provider certification (in relation to SP)

### *1.4 Certificate building blocks*

Required functions are:

- Card registration and certification
- Infrastructure entities/front office entities (building blocks): ID, certificate, address creation and maintaining

## **2. “Card issuing”**

### *2.1 Personalise card*

Required functions are:

- Card holder registration
- ‘Physical’ card issuance (printed on plastic)

### *2.2 Issue certificates*

Required functions are:

- Authenticate card and card holder
- Load certificates

### *2.3 Initialise cards*

Required functions are:

- Personalisation of the card (Print data)
- Initialisation of the card (Update chip)

### *2.4 Enrol the card*

Required functions are:

- Notify card holder
- Put in authentication data
- Confirmation of card “hand over”

### *2.5 Maintain life cycles*

Required functions are:

- Card status
- Hot lists
- Card service management

### **3. “e-service (post issuance) registration”**

#### *3.1 Test/Accept IAS connection software*

Required functions are:

- Register e-Service connection application
- Test e-service connection application
- Accept e-service connection application

#### *3.2 Test/Accept IAS on-card application*

Required functions are:

- Register e-Service on-card application
- Test e-service on-card application
- Accept e-service on-card application

#### *3.2 Download on-card application*

Required functions are:

- Register and certify on-card application download
- Download on-card application

### **4 “IOP establishing & maintaining”**

#### *4.1 Create IOP adapters*

Required functions are:

- Define Outgoing IOP request (‘technical’ request and PKI check request)
- Define Incoming IOP request (‘technical’ request and PKI check request)
- Implement request handler

#### *4.2 Maintain IOP adapters*

Required functions are:

- Modify implemented Outgoing IOP request (‘technical’ request and PKI check request)
- Modify implemented Incoming IOP request (‘technical’ request and PKI check request)
- Implement modification

### **5. Main process “Manage SCC”**

#### *5.1 Log/capture session-data*

Required functions are:

- Implement internal/external tariffs
- Historical database
- Statistics

#### *5.2 Execution, acquiring and settlement*

Required functions are:

- Logging on ‘inter-stakeholder’ performance indicators, statistics
- Invoice/clear internally
- Invoice/clear cardholders

The processes mentioned above are considered as the secondary processes since they are required for supporting what is to be called the primary process, those which are related to IAS.

### **2.2.3 Pre-requisites on the SP activities when delivering e-Services**

The Tertiary IAS processes are internal to the e-services and are fully and only under the responsibility of the service provider. They are securely hooked to the above-mentioned primary processes. Since they do not impact the IAS interoperability, they are not to be detailed here.

### 2.3 Pre-requisites on the functions

The prerequisites applicable to the functions of the smart card information system are presented below according to the functional boxes model (see GIF part 1).

#### IAS nucleus (IAS application and its platform)

- The parties accept to work with the generic or commonly agreed IAS nucleus application to access e-services in a trusted way. They have to support the secure integration of IAS with the e-services. The service provider can choose via business rules how he wants his e-service to use the generic IAS. This regulated connection is 'pre-structured' in three levels of requirements which the e-service can go for:
  1. Only identification of the smart card in a trusted infrastructure. In that case only the ID-data of the card will be read, and taken at face value. In that case only the security of the technical environment (the building blocks) has to be checked.
  2. Strong authentication of the parties in the session (verification of the cardholder via PIN-code or biometrics).
  3. Qualified electronic signature of an (information) object.

#### The four 'independent' functions

- The IAS nucleus application loaded on the card is interoperable with not-on-us infrastructures and front office applications thanks to the use of standardised information exchange to be applied for:
  - o Card connectivity: card readers, terminal and networks
  - o Human interface
  - o PKI handling
  - o Business rules and other information for the e-service involved.

These four categories of functions (the 'functional boxes') require an independent interface because they are all part of different type of dynamics. There is a need to change the content without influencing the rest of the system in the framework.

### 2.4 Pre-requisites on the Data

Each SCC must have a standardised set of IAS data and the conditions to be fulfilled for organising the data flows effectively and efficiently (e.g. securing and addressing the data flows between the building blocks).

The common data categories, involved in the IOP process cover (only) the data required for the minimum IAS-functions:

- Securing the building blocks
- Identifying the stakeholders
- Authenticating the users

The mandatory common minimum IAS data set contain the following categories:

- User identification
- Certificates for strong authentication and qualified electronic signature
- Stakeholder identification and authentication for creating security over an open network, within and between smart card communities

- Building blocks (entities of standardised hard-/middle-/software) identification to secure the links between the systems
- Network addresses

The minimum set of common data for IOP is the same as mentioned in the previous section, augmented with the data to make the IOP adapters function:

- Network components IOP (addresses)
- Network security

## 2.5 Pre-requisites on the building blocks

The core IAS building block the trusted token: the smart card for EID including its ( trusted) interfaces to connected services.

Because of its acceptability to the user, its PKI capable chip, on-board data storage, computing and multi-function capabilities, a smart card is an ideal trusted token. The capabilities for identification, strong authentication and the creation of a (qualified) electronic signature of the have to be exclusively placed on this token.

The main prerequisite for the interoperability of the technical components (building blocks) in an SCC is that the interfaces to the functional boxes can always be recognised and respected throughout the entire configuration.

Note that the standards identified for implementing IAS interoperability are presented below in Section 4.

### 2.5.1 Smart Card layer related prerequisites

The following card requirements should be fulfilled for preparing a SCC implementing GIF.

#### Physical characteristics

- ISO/IEC 7816 1-3
- Expected Life time not shorter than validity of ID and certificates (ISO/IEC 10373)

#### Logical interface

- Contact (ISO/IEC 7816)
- Contactless (ISO/IEC 14443)

#### Chip

- Directory/File structure for multi application capabilities
- OS:
  - Global platform
  - Java 2.1 card virtual machine and API
- Sufficient data storage capacity for the required functions (incl. certificates)
- Security concept including fraud resistance of the mask in line with functional requirements
  - Certified by a certification body, at the minimum level of EAL 4+
  - Authentication of all parties involved in card related activities by public key or public key certificate when performing other actions than reading card retained data (see below)
  - Secure data communications
  - Authentication (PIN-number or biometrics) of card holder
  - Key algorithm for operations in the smart card: for asymmetric algorithms, hashing and padding see relevant Workshop E-sign documentation.

- Card-retained information
  - o Card holder ID
  - o Card issuer ID
  - o Unique Card ID
  - o Card manufacturer data (organisation, name, card type, version)
- (Post issuing) On-card application downloading capabilities in line with mandatory GIF specifications
- On-card application deleting
- Internal card management in line with mandatory GIF specifications (\*)
- Card state search in line with mandatory GIF specifications (\*)
- The nucleus application collaborates with the access software in the infrastructure (see below under section 4.2.3). This software should support:
  - o Starting a two sided challenging (mutual authentication) between card and terminal / system
  - o Securing links (if required at lower – module- level than the terminal)
  - o General checks (card validity etc)
  - o Handling the e-service requests from the user (on-us/not-on-us)
  - o Handling the business rules requests from the e-service provider (a.o. certificate checks)
  - o Passive status during e-service session
  - o Terminating the session and logging of the required (administrative) data

## 2.5.2 Infrastructure layer related prerequisites

To implement GIF, the following infrastructure requirement list should be used as a checklist:

### Reader / terminals

- Basic requirements:
  - o Capability to read / handle all GIF accepted cards
  - o Following recommendations from eESC TB 4 (contact) and TB 6 contactless card terminals/ readers
  - o Authenticated for use in the smart card community by / on behalf of the card issuer.
  - o Handling IAS
    - Off line on-card application
    - Online with network server or e-service-application
- In general following standard as been defined by FINREAD requirements for functions and performance
  - o Secure communication between chip, keyboards, and display (In case of using the screen/display and/or the keyboard of different building block(s), the links must be secured before the interaction starts.)
  - o Displaying status / result information
  - o Human interface presentation steered by individual IAS, and minimal capable to put in numeric codes.
- Easy select of the e-service that can be accessed in a secure way
  - o Secure interaction between card and SAM
  - o Where it is allowed to apply a remote SAM, a reliable procedure must create a secure link between the card and the SAM, before any user interaction may take place.
  - o Preventing easy tap of visual PIN code input

### Network

- Basic requirements
  - o Handle secure communication between terminal / network server (as far as not integrated in the terminal)
  - o Handle secure communication between network server and
    - Front office server of requested e-service and/ or PKI server (outgoing)
    - PKI server (incoming)

The network services can be executed via secure links on the internet with internet tools

- Functions and performance
  - o Support of the terminals in presenting the accessible e-services offered to the card holder
  - o Option: network service to keep, maintain and handle some personal card holder data
  - o Option: network service to keep, maintain, and handle the session log data
- Security: see requirements for the reader / terminal
- Compatibility to network services
- Network (services) management
  - o IOP adapter
  - o PKI adapter

### **2.5.3 Front office layer related prerequisites**

To implement GIF, the following front office implementation requirements list should be used as a checklist

There are three services that must be implemented for operational use (the conditioning processes are not considered here)

- e-service front office applications (exploited by the service provider)
- Network service (exploited by the access provider, as presented above)
- PKI: certificate verification services (exploited by/under the responsibility of the card issuer)

#### **e-Service front office**

- Basic requirement:
  - o Apply certified connection module for use of generic IAS
  - o Interact with card holder, while performing IAS session
- Functions and performance
  - o Online connection to read card and card holder identification data via certified terminal
  - o Online secure connection to PKI server
  - o Generate requested secure log data
- Security: see network requirements

#### **Network services part of the front office application**

It is up to the smart card community how to organise this service. See the implementation requirements as given above.

Dedicated network management services include also (remote) management of secure terminal/s, or dedicated categories of terminals

#### **PKI: the front office for certificate check**

This function define the basic security prerequisite for the total system:

- Level of 'qualified certificates' (public with SSCD) as defined in the context of the E-sign directive art 5.1
- Security level in accordance with Common Criteria level EAL 4+ (augmented with VLA 2)

## 3 Operational requirements for IAS interoperability

### 3.1 Introduction

When considering the operational requirements, it is not enough strictly looking at the IAS processes. The operational context of the secure IAS processes must also be made explicit. From this point of view the operational requirements are focussed on:

- Responsibilities and liabilities between parties involved in IAS IOP
- Content of the required ICT functions.

We will first present “What is required from the operational perspective?” (Clause 3.2) and then “Who is impacted, or what are the operational requirements for the stakeholders?” (Clause 3.3).

### 3.2 Functional Requirements

#### 3.2.1 Introduction

To answer the question “What is operationally required?”, we give in this section the requirements for the IAS as ICT system from a “functional” point of view. Where possible we give the functional requirements in terms of transformation from input to output. The nature of this section will be a checklist of required “functions”.

#### 3.2.2 Functional boxes

The functional boxes model aims at creating room for the dynamics of the stakeholders, as indicated in chapter 2, without influencing other parts of the IAS-system.

Above the application of the functional boxes it is, in order to support the dynamism, if not required, then recommended to create a workbench where stakeholders can prototype and test their aimed new developments. This is to support especially:

1. The addition of new e-services (and deletion of not successful services).
2. The addition of new connections to other smart card communities
3. The adaptations in human interface/individualised interaction process.

Following GIF part 1 the following functions have to be generally supported in the different processes/functions presented in the next section

#	Functional box	Interfaced to box #
1	Platform	2
2	IAS function	1, 3, 4, 5, 6
3	Human interface	2
4	Connectivity	2
5	PKI	2
6	E-services (- access)	2
7	OP adapters	4 (7, 4 in not-on-us infrastructure)

**Table 3: Functional boxes, ruled by standard interfaces**

#### 1. Platform function

No additional requirements have been identified for the platform box for the purpose of supporting the IAS interoperability.

## 2. IAS function

For the purpose of supporting IAS interoperability, IAS box has to be able to:

- Access the on-us/not-on-us attributes as identified in the data meta-model of GIF Part 1
- Access the appropriate business rules (i.e. depending from the applied type of IOP scenario)
- Call the IOP adapters each time the IAS box has identified a “not-on-us” scenario.

Note that the IAS box is seen as the nucleus application and has always to keep the control and responsibility of the whole process, including the IOP-related ones. For instance, should the communication with the IOP adapters fail for any particular reason, then the IAS box should decide upon the appropriate action.

## 3. Human interface function

The sub-functions included in this box should be adapted for handling the applicable IOP scenarios. This will be of particular importance for the following sub-functions:

- Language preference
- Individualised preferences
  - o Presentation
  - o Profiles
- Notification of process progress
- Presentation of e-services to be accessed
  - o In on-us infrastructure
  - o In not-on-us infrastructure
- Positive consent mechanism
  - o To authenticate the CH (agree to open the card, which means to give the ID to the e-service that the card holder will choose)
  - o To express CH positive consent (e-sign the OTBS)
- Secure use of screen/display and keyboard eventually in combination with “embedded” modules (which is in principle an option)

## 4. Connectivity function

The sub-functions included in this box should be adapted for handling the applicable IOP scenarios. This will be of particular importance for the following sub-functions:

- Card connectivity (readers / terminal)
  - o Contact cards
  - o Contactless cards
  - o Anticipated future developments
- Activating the IOP adapters
- Data transfer in order to access + presentation of the e-service, available in
  - o “On-us” infrastructure
  - o “Not-on-us” infrastructure

## 5. PKI function

The PKI function will only be impacted by IAS interoperability in the sense that it will not be responsible for the handling of “not-on-us” certificates but will have to pass this responsibility back to the IAS function as indicated above.

Vice versa, the PKI function will be requested for certificate verification only by the IAS function, should the request be issued in the “on-us” or the “not-on-us” SCC.

**6. Additional (e.g. on-card) application function**

Since the IAS function is managing the whole IAS/IOP process, the additional application function will only be impacted by IAS interoperability as far as an IOP scenario foresees the download and usage of an on-card application.

**3.3 Requirements for Stakeholders' roles**

Note. Following the set up of this document, this clause should only cover the stakeholders' requirements as far as IOP is involved. If required without considering IOP, the prerequisites would have been presented in chapter 2. For practical reasons it is chosen to apply the distinction (between IAS applying only and IAS / IOP oriented) in the sense that only the process related prerequisites are presented in chapter 2.

**3.3.1 Card Issuer setting-up an SCC**

The following table lists the general issues that lead to requirements for the card issuer and the requirements are described in further detail below. Issues related to trust are separately listed in a Table 5.

•	Issues concerning the smart card community
	1. The purpose setting and limits of the generic IAS system 2. What organisation would actually issue smart cards (RA function)? 3. Legal structure for card issuance process 4. Who owns the cards and the data? 5. Who can apply for IAS? 6. What should be established in the card issuing process? 7. What card holder data should be collected?
•	Issues concerning the CP (Certificate provider)
	8. CP arrangements 9. Assessment of the CP 10. Obligations and liability of the CP
•	Issues concerning the infrastructure arrangements
	11. Who contracts with the AP? 12. What should be arranged with AP?
•	Issues concerning the e-services connected to the basic IAS process
	13. Who is responsible for e-services offer? 14. What should be arranged with the SP?
•	Issues concerning relation to the card holder
	15. What is responsibility towards cardholder?

**Table 4: Card issuer issues**

**1. The purpose setting and limits of the generic IAS system**

In the context of the framework, the purpose of the smart card community can be defined as follows:

- From the point of view of the Card issuer:
  - o To build and exploit a smart card base, using generic IAS
  - o To 'brand' and support a contracted mix of e-services (from e-service providers), willing to use generic IAS for access to their services
- From the point of view of the card holder/users
  - o To get access to high level e-services

- o To experience an optimal user convenience in using IAS for different services,
- From the point of view of the service provider
  - o To get the generic identification data for the (secure) e-service as well as strong authentication and qualified electronic signature
  - o To make the e-services offer accessible to a broader 'audience', than the smart card community where the SP is registered.

In the case of national smart card communities based on public ID, the purpose could be restricted to e-Government services, at least for those e-services that require authentication and electronic signature.

## **2. What organisation would issue the generic IAS on smart cards?**

In the context of the framework, as a rule of thumb, an individual organisation takes on the role of card issuer, responsible for the process of:

- Establishing the card holder identity,
- Loading the identity and other IAS components in the card
- Issuing the card to the cardholder.

The (legal) entity for the whole SCC facilitates the organisation of a complete "value chain" between the stakeholders (roles). The card issuer manages and is assigned complete responsibility for the SCC issuing process.

The Card issuer contracts the CP for producing certificates which take care of the quality of the operations.

The national "ID-document bodies" are the card issuers who apply the framework to public ID for e-services, especially e-Government services. They decide if they will establish a legal entity to handle all smart card community exploitation issues.

## **3. Legal structure**

The smart card community may be organised in any suitable legal structure. Generally speaking the legal entity may delegate power to the CI in order to deploy the "primus inter pares" – type responsibilities in the SCC.

Applying the framework to public ID, the national ID issuer will be the card issuer. It decides on the legal structure, and the conditions under which this public function must be fulfilled. In relation to this decision, the national body may contract a party to execute the CI-function.

## **4. Who owns the cards and the data?**

In the context of the framework, the ownership of the card is not relevant. The card may be owned by:

- The CI
- The SCC
- Any other entity which exploits an appropriate card base, and enables the SCC to use (a part of) the card in (a part of) the card base.

When the card is not owned by the cardholder (which might very well be the case) the cardholder is only given the right to use the card.

Either the CI or the smart card community may own the IAS data.

The ownership of other data on the card depends on the policy statements established in the SCC. Most probably the originating party owns the data, typically the CI or the SP.

In the case of public ID, the cards and the IAS data will be owned either by the legal entity of the smart card community or by the national ID issuer.

#### **5. What customer base can apply for IAS?**

The SCC or the CI has to define the policy about the participation of customers. It can be open to all citizens or restricted to a particular group. This may be on a voluntary or a compulsory basis.

In case of public ID- involvement, it is the courtesy of the national body to make IAS participation open to all citizens that would qualify for a national passport/travel document or an ID-card.

#### **6. What should be established in the card issuing process?**

All required ID data (with data derived from or verified against a national data register) should be established and irrevocably connected to authentication data (binding the card to the cardholder).

#### **7. What card holder data should be collected?**

The data elements are to be defined according to the TLV format while being compliant with the TB1 Citizen Certificate Guidelines.

The data collection must also be arranged taking good care of the privacy aspects. A privacy code of conduct needs to be in place.

In the case of public ID, the Identification data should be derived from a reliable source, such as the national personal data register.

#### **8. CP arrangements**

The CI must make detailed arrangements with one or more certificate providers. The arrangements between CI and CP should at least cover the following issues:

- The standard to which the CP has to comply
- The types and all details of card holder and system component certificates to be issued
- The CP, CPS and terms and condition that are valid
- The organisation structure

The certification body shall include the scope description in the certificate of conformity or in an appendix of the certificate

#### **9. Content and assessment of CP's**

The certificates required should support for IAS services:

- The freedom of choice of the card issuer to sub-contact the RA function or execute this process himself. The registration process involves in any case a face-to-face registration. (in case of National ID this has to be done by qualified officers)
- Identification (in case of National ID, this will be done under the responsibility of the national personal data register)
- Establishing the binding mechanism between card and card holder
- Enrolment via face-to-face issuing of the card.

Concerning the assessment: the CA and RA functions have to comply with CWA 14172 Part 2 for guidance on:

- Requirements for independent bodies
- Qualification criteria for individual assessors
- Code of conduct for assessors

- Assessment team competence
- Use of technical experts
- Conformity assessment process

#### **10. Obligations and liability of CP**

A CP shall include an object identifier in the certificates to which CP claims conformance. This includes:

- CP Obligations
- Subscriber obligations
- Information for relying party
- Liability

#### **11. Who contracts with the AP?**

In the context of the framework, it is understood that the CI or the SCC Administrator will make contracts with (and define the conditions for) the access providers (also known as “card acceptors”).

#### **12. Arrangements with AP**

Between the CI and the AP, the following minimal specifications/requirements must be arranged:

- Card terminals/card readers + security links to other building blocks
- Human interface
  - Presentation standards, including a positive consent expression mechanism
  - Presentation of the choice/access to “on-us” e-service
  - Ditto for not-on-us services
- IOP-network services
- Transition tables (from/to concerning 1- human interface, 2- connectivity, 3- PKI and 4- e-services)
- Conformity testing
- Logging for acquiring and settlement, or other forms of cost compensation in and between the smart card communities.

#### **13. Who is responsible for e-services offer that may use IAS?**

The use of generic IAS for identification purpose only, is open to all service providers, without any control from the CI. Only the need to qualify / certify the building blocks involved must be honoured. Via a procedure for this, the basis legal arrangements (see at CI responsibilities towards cardholder) can be implemented.

The CI contracts the e-service providers who require:

- Authentication of the users
- Electronic signature.

The CI is free choosing the (high level) e-services wanting to participate in the smart card community and the type of brand that the card issuer wants to establish with the e-services.

In case of public ID, the e-service providers could be government bodies, application providers, and service providers in public or private domain.

#### **14. Arrangements with SP**

Between the CI and the SP, the following issues must be arranged:

- How the SP e-service is to be presented on the terminal (to be implemented by the AP)
- To what smart card communities the SP is connected, and from what smart card communities the SP accepts accesses? (Connectivity to the on-us and not-on-us infrastructure)
- The implementation of business rules
- The conformity tests
- The conformity of the on-card application to the specifications of the card
- Loading the on-card application on the cardholders card
- Logging for acquiring and settlement, or other forms of cost compensation
- Certificates and addresses

**15. What is CI responsibility towards cardholder / user?**

The CI is fully responsible for the card and the IAS application. The CI is the first line communication for the cardholder for any complaint, also concerning access and e-services.

The CI, (also when contracting a SCC Administrator) has to create the appropriate legal basis and bylaws including privacy arrangements for the smart card community. It has to publish and apply appropriate bylaws not only for his direct responsibility, but also the rules that apply for the e-services under contract. A privacy regulation and complaint handling process are also required.

The CI has to define a user policy, including requirements such as: convenient, easy to understand, consistent user interaction, and clear and easy to understand positive consent mechanism for all IAS use (e.g. via a defined keystroke -or use of touch screen- on standardised message, PIN, biometrics).

In case of public ID, the legal basis cannot be found in private agreements. The national ID issuer has the sole responsibility.

The CI must make such arrangements that the standards for the human interface can be respected:

- Language preference
- Same basic procedures to select a requested e-service for on-us and not-on-us infrastructure
- Presentation profiles
- Unambiguous expression of will

**3.3.2 CI ensuring trust within its SCC**

The goal of the trust concept is, for the card issuer, to protect the stakeholders in the smart card community against possible threats of:

- Illegal or non valid cards
- Leaking IAS information from the card to not secure environments
- Downloading of on-card applications and other information on the card without control of the card issuer
- Destroying cards or illegal change of card content

The trust concept is here in its requirements dedicated to ICT processes, and includes security questions

• CI Trust issues and requirements
1. Stakeholder registration, ID and certificate issuance

	2. Building blocks ID for secure processing 3. Card capabilities and security functions 4. Automated session key for immediate/pre-certificate security
--	---

**Table 5: Card Issuer trust requirements**

**1. The CI has to give ID and certificate to all stakeholders and apply this in all secured processes**

All stakeholders have to be in or controlled by a system of certificates:

- Certificate Authority
- Service provider
- Card holder
- Access Provider
- Content provider
- Smart card community administrator

The CI has to apply an appropriate issuing procedure

**2. The CI has to give “building block ID” and authentication, for each of the secure blocks**

The blocks involved concern:

- Cards and its functional components (platform, IAS application, Human interface software, reader software, on-card PKI software, on-card applications)
- Infrastructure and its components (IAS-SAM, embedded Human interface software, card communication interface software, network systems, off card application)
- Front office and its modules (platform, IAS application, Human interface software, card reader software, PKI software, applications)

**3. Card capabilities and security functions**

The following requirements are mandatory to offer adequate security level.

- Card capabilities (see at requirements for building blocks)
  - o Key generation on card
  - o Key storage on card
  - o Certificate storage on card
  - o Signature generation on card
- Secure viewing mechanism/final format OTBS
- Clear easy to use consent mechanism
- Mandatory common elements for the certificates
- Qualified level for signing
- Algorithms in conformance with European Algorithm Catalogue

**4. Session keys**

The CI has to make automated session keys applied, when non-secure card readers are applied.

**3.3.3 Service provider setting-up an e-service community**

By offering his services to the constituency of more than one smart card community the SP is by definition creating an e-services community.

The following table lists the general issues that lead to requirements for the Service Provider. The requirements are described below. All issues related to trust are listed in separate table

<ul style="list-style-type: none"> <li>• Issues concerning the e-service community</li> </ul>
<ol style="list-style-type: none"> <li>1. Who can participate in the e-services community</li> <li>2. What must the SP arrange with the CI</li> <li>3. Legal arrangements/bylaws/protecting the user</li> <li>4. Qualities of the connection between application and IAS</li> <li>5. What is compulsory or voluntary in the co-operation</li> <li>6. Who owns the data, and the use of the data</li> <li>7. Requirements for identification</li> <li>8. Where do certificates reside</li> <li>9. Responsibility in relation to AP</li> </ol>

**Table 6: Service provider issues**

**1. Which service providers can participate in the e-services community**

In principle all service providers who exploit an e-service that requires IAS, and agree with a card issuer on the use of generic IAS can participate.

In the case of public IAS, the participation could be restricted to e-government services.

**2. What must the SP arrange with the CI?**

The service provider who requires no more than identification from the cardholder just needs to be in compliance with the common security needs of the smart card communities.

For all other cases, the SP must prove to the CI that he is in compliance with the rules for the smart card community. This concerns:

- Registration
- The content of connection function from his e-service application to IAS. In this connection he has to define the “business rules” that are applicable for his e-service (as mentioned earlier, the application of the three layers: just securing the building blocks and the identification of the card [1], authentication of the user [2], and/or electronic signature [3])
- Developing, testing and accepting the (optional on-card) applications to connect the e-service to smart card and the generic IAS of the user.
- The optional on-card application can contain the business rules to access the e-service application or a complete off line application.

**3. Legal arrangements/bylaws**

The SP has to publish his specific bylaws including privacy arrangements. The SP cannot unilateral deny the general bylaws of the SCC where the SP is registered.

The SP has to communicate and apply a general registration procedure for users wanting to enter/use the e-service concerned. It depends also on the business rules how “heavy” this e-service access registration will be.

The cardholder should in all cases be protected against other use of his identification data than stated in the SCC bylaws.

**4. Qualities of the connection between application and IAS**

The SP should follow the specifications that are applicable in the smart card community. The SP has to proof compliance.

SP may insist on performance guarantees by the CI, like “uptime” and MTBF.

#### **5. What is compulsory or voluntary in the co-operation**

In the GIF the compulsory elements are:

- Compliance with the basic process and roles
- Compliance with the IOP adapter, which implies application of and compliance with the IAS functions and its functional interfaces (Human interface, Connectivity, PKI and e-service application connection)
- Application of the mandatory common data
- Respecting the (technical) standards on the building blocks (hard- /middle-/software) to ensure IOP

In the case of public EID of citizens, it is the privilege of the national ID issuer to determine the content of the compulsory elements.

#### **6. Who owns the data, and who may use the data in relation to e-services?**

Concerning the ownership of the card and the IAS-related data: See 3.2

The SP has access to and the right to use the IAS data of the card, as far as agreed with the CI, implemented via business rules, and covered by the bylaws of the SCC. On top of this, the SP has access to the identification data of the card for as far as the cardholder has given permission to that. The human interface must foresee in a clear mechanism for this.

The SP owns and is fully responsible for the data on the card covering his own application, or the business rules for his own application.

#### **7. Requirements for identification**

The SP, who has a contract with a CI, requires means for secure messaging and encryption of data traffic, on all on-us and not-on-us infrastructure situations.

This implies authentication of card and terminal, including all components in the smart card communities.

#### **8. Where do the certificates reside to be checked by the SP, where are the business rules residing and how to map when two smart card communities are involved?**

The basic situation is as follows:

- The SP has to put the connection mechanism in a by the CI secured and/or certified building block (covering the application box function). In addition the SP can put the business rules or the complete application on the card of the end-user.
- The certificates of a user are always handled by the CP of the user
- The mapping is realised by the IOP scenarios as presented in chapter 4 (clause 4.4).

#### **9. Responsibilities in the relation between SP and AP**

The AP has a contract with the CI. Special arrangements between SP and any AP are submitted to at least the master agreement between SP and CI.

The main AP oriented subjects in which the SP is interested are:

- The span of the network, which for the SP is his channel to the cardholders
- The quality of the network

- The protection against corruption of the data flows

### 3.3.4 SP ensuring trust within its e-service community

The goal of the trust for the service provider is the protection against the following threats:

- False acceptance/false rejection of users
- Leakage/divulgement of business/privacy information
- Access attacks to his e-service systems (i.e. denial of services)

<ul style="list-style-type: none"> <li>• SP Trust issues and requirements</li> </ul>
<ol style="list-style-type: none"> <li>1. Registration of SP</li> <li>2. Building blocks, especially the on-card application and/or the module containing the business rules</li> <li>3. Authentication</li> <li>4. Signing</li> </ol>

**Table 7: Service Provider trust-issues**

#### 1. Trust requirements for registration

After its compliance to SCC specifications, the SP has to be registered for ID and certificates with the CI, or at a SCC Administrator and CP acting on behalf of this CI.

#### 2. Trust requirements for building blocks

The SP has to offer and register (for ID and certificates) with the CI, when acting as SCC Administrator, the “building block” (or module) containing the business rules to connect the e-service application to IAS.

This also includes on-card applications for after-issuance downloading or software that will be accessed in an IAS-session.

#### 3. Trust requirements for user authentication

In addition to the requirements for identification, the requirements for authentication of the user are:

- Mandatory: PIN or (layered) biometrics (if possible extraction on card; template on card; matching on card),
- Ruled by the business rules of the SP.

#### 4. Trust requirements for signing

In addition to the requirements for identification and authentication, the requirements for signing an OTBS are:

- Secure, and clear connection to the CH human interface via the generic IAS
- Ditto for secure viewing of the OTBS
- Appropriate content and application of the certificates
- Security mechanisms belonging to qualified signature standards

### 3.3.5 Card holder

The following table lists the general issues that lead to requirements for the cardholder. The requirements are described below. Another table will list separately all issues related to trust.

<ul style="list-style-type: none"> <li>• Issues concerning the e-service community</li> </ul>	
	<ol style="list-style-type: none"> <li>1. Participate in the smart card community</li> <li>2. Responsibilities towards CI</li> <li>3. Legal arrangements/complaints</li> <li>4. Registration of access to e-services</li> <li>5. Requirements for human interface</li> <li>6. Responsibility of the AP towards cardholders as member of the e-community</li> </ol>

**Table 8: Card holder issues**

**1. Participate in the smart card community**

To participate in a smart card a user has to apply for a smart card. He has to go through a card registration process.

The CH has in some cases also to apply and register with the service providers.

**2. Responsibilities towards CI**

The cardholder has to provide all data required by the CI.

The cardholder has to collect and accept the card (in direct contact)

The cardholder has to take good care of the card and use it correctly.

The cardholder is responsible for offering his/her ID data to e-services.

The cardholder has to notify the CI of lost, theft and damage of the card

**3. Legal arrangements/complaints**

The cardholder has to familiarise himself with the rules and regulations regarding the use of his personal ID data.

The use of the data must be restricted to the goals for which they are asked. The cardholder must inform him/herself about the goals as published by the card issuer and the e-services for which the cardholder register himself/herself. Complaints will be channelled via the card issuer, while he has contracts with each stakeholder. In this way the Card issuer ensures the cardholder right of protection against misuse. (Compare 3.2.1 issue 15)

**4. Registration of access to e-services**

The cardholder can request to access any e-service via the infrastructure layer of the smart card communities.

The cardholder has no automatic right to access all services; he/she must accept the service provider prerogative to decide about accepting the request for access. The cardholder has to go (once or each time) through an initial registration procedure, as deployed by the e-service provider. As a part of the (one time) registration procedure, the SP will give the business rules and conditions that the SP applies to cardholders. It is the prerogative of the cardholder to decide (if offered and if possible) to take the (access) application on card (so called downloading of applets).

**5. Human interface/Express will**

CH needs to communicate with the e-service providers including the expression of his/her will concerning the application of IAS, in relation to the e-service.

The CH may expect

- secure access,
- after accepting the card in the initial procedure in any smart card community, what he/she sees ( on the screen, concerning IAS) is correct.

The requirement for the cardholder is that he/she takes responsibility for what is authenticated and signed with the card.

**6. The cardholders responsibility towards access providers**

The e-service provider gives access to his service for on-us and not-on-us cards, via on-us and not-on-us infrastructures.

The cardholder decides to offer his/her card to an (not-on-us) infrastructure. A part of the operation is operated at the location where the cardholders had offered his/her card.

The initial acceptance/rejection is done in that infrastructure, based in local interaction.

The responsibility of the on-us card issuer for the not-on-us initial process can be limited.

**3.3.6 The card holder as part of a trust system**

The goal of the trust requirements is for the cardholders to:

- Prevent destroying the card or the card content
- Prevent unintended writing on the card
- Prevent indulgement of IAS data
- Prevent unauthorised usage of the IAS data

It is accepted that the card holders contribution to the trust system is mainly passive:

Good co-operation is expected in deploying the procedures, and taking good care of CH responsibilities.

	• CH Trust issues and requirements
	<ol style="list-style-type: none"> <li>1. Registration of CH</li> <li>2. On-card application downloading</li> <li>3. Secure environment and free decision about ID giving</li> <li>4. Binding mechanisms</li> </ol>

**Table 9: Card holder trust issues**

**1. Trust requirements for registration**

The CH must co-operate in being registered (for each CI only with one single ID).

**2. On-card application downloading**

Only the CH may decide on downloading of on-card applications after the card has been issued. This refers to new applications and not to necessary maintenance or upgrading of already existing applications. The cardholder must read and follow carefully all instructions and bylaws of the e-service provider before taking an application after issuing onboard of his/her card.

**3. Secure environment and free decision about ID giving**

In principle the CI has to guarantee to the CH that no part of the card (except the card serial number and the starting procedure) can be read, unless the infrastructure is accepted in the smart card community.

The cardholder may rely on the security of the IAS system, from the moment that the card has passed the initial procedures, and is accepted by the terminal. The cardholder is fully responsible for the choices that he makes in supplying IAS to the e-service provider (plain ID data or Authentication). The same goes for CH's expression of his consent over an OTBS.

**4. Binding mechanisms**

The cardholder must be aware of the binding between cardholder and the card. This is realised by establishing:

- The linkage “one person - one card - one identity - one record”
- Authentication data (PIN, biometrics on the card)
- Strong authentication mechanism (key pairs/certificates stored on the card)
- Reference templates stored in a database for fall back scenarios

**3.3.7 Other stakeholders**

The following table gives the issues that lead to requirements for the other stakeholders

	• Issues concerning the smart card community
	1. Access provider: basis for action and limits
	2. Certificate provider: basis for action and limits
	3. SCC Administrator: basis for action and limits
	4. Content provider: basis for action ant limits

**Table 10: Other stakeholders issues**

**1. Access provider: basis for action and limits**

The access provider makes a contract with the Card Issuer and eventually with the e-service provider for providing service infrastructure in the smart card community and e-service community.

The access provider has to proof the compliance of the IAS -building blocks with the agreed CI specifications.

The access provider has to guarantee the performance of the infrastructure that he controls.

**2. Certificate Authority: basis for action and limits**

The certificate authority makes a contract with the CI.

The CP has to guarantee the quality of the systems and the checks that he executes.

**3. Smart card community Administrator: basis for action and limits**

SCC Administrator gets a contract from the CI. The administrator has the right to monitor all major processes against the goals and agreements

- Autonomously
- At request/complaint of users

The administrator takes any appropriate corrective actions.

**4. Content provider: basis for action ant limits.**

The content provider is contracted by the e-service provider.

### 3.3.8 Other stakeholder contributing in ensuring trusts

• Other stakeholder Trust issues and requirements	
1.	Registration of stakeholder
2.	Building blocks
3.	Authentication
4.	Signing

**Table 11: Other stakeholders trust issues**

The goal and issues are, with exception of the on-card application downloading, similar to the e-service provider described above.

## **4 Implementation requirements for IAS interoperability**

---

This chapter handles the requirements to get 'the IOP / IAS job done.

### **4.1 Requirement for an IAS/IOP implementation strategy**

#### **4.1.1 e-Services in the centre**

When considering these implementation requirements, it must be stated that IOP or generic IAS is not a goal in itself. It is a means to access e-services and to handle IAS securely for these services. It makes therefore no sense to base the implementation strategy on the smart card, but it make a lot of sense to put the e-Services in the centre of this implementation strategy.

The effective starting point for the implementation should be the services-concept. Technology choices will only be handled in a second step, i.e. during the implementation process. In other words, this means that the implementation does not start from a 'white card' concept or whatever card concept, but from secure e-services using the capabilities of the smart card as a IAS token for the user of these services.

When this approach is accepted, then the GIF implementation leads to key distinctions:

- Which part of the business should be organised in a business-to-business approach (between the business stakeholders in the smart card communities) for offering IAS to the e-Service providers?
- How to organise the business-to-consumer approach for the e-services?

This distinction does not exclude that a card issuer can have a direct business relation with the cardholder, but this relation is always related to the offered e-service(s)?

#### **4.1.2 Which IAS /IOP is desired**

An IAS/IOP implementation strategy should support (and/or):

- The extension of "on-us" e-services, using the common IAS
- The extension of access to "not-on-us" e-services
- Interoperability with other smart card communities, to check "not-on-us" certificates loaded in "not-on-us" cards

#### **4.1.3 Who is concerned by IAS/IOP implementation strategy**

It is also often stated that the concept of interoperable IAS has to respect the different responsibilities of the involved stakeholders, i.e. to establish a business strategy which gives a common orientation to all stakeholders concerned, possibly including stakeholders from different smart card communities.

Each of these stakeholders will therefore have to identify their own business case for deciding when and how to join an IAS/IOP agreement. There is therefore a need for establishing:

- A common denominator for the cost compensating mechanism between the stakeholders
- A mechanism that creates the relation between the realised value (revenue) and the budgets available.

It must be studied and decided if the compensations will be given:

- In amounts of money per period
- Tariffs by graded blocks in any parameters
- Statistical measurements (from taken samples)
- By sessions

These categories do not exclude each other, and can also be mixed.

## **4.2 The Requirements for IAS/IOP technical infrastructure**

The main implementation requirement for IAS interoperability is to agree on “mutual trust” (i.e. secure processes) and implement strict procedures based on PKI technologies.

There are two specific implementation subjects related to IOP/IAS. They cover:

- IOP technical infrastructure for operations, i.e. the IOP Adapters
- Requirements for testing interoperability
  - o To accept new e-services in the concepts (post issuing), because of the expected dynamism in the community (stepping in, stepping out)
  - o To open / maintain new connections to other smart card communities.

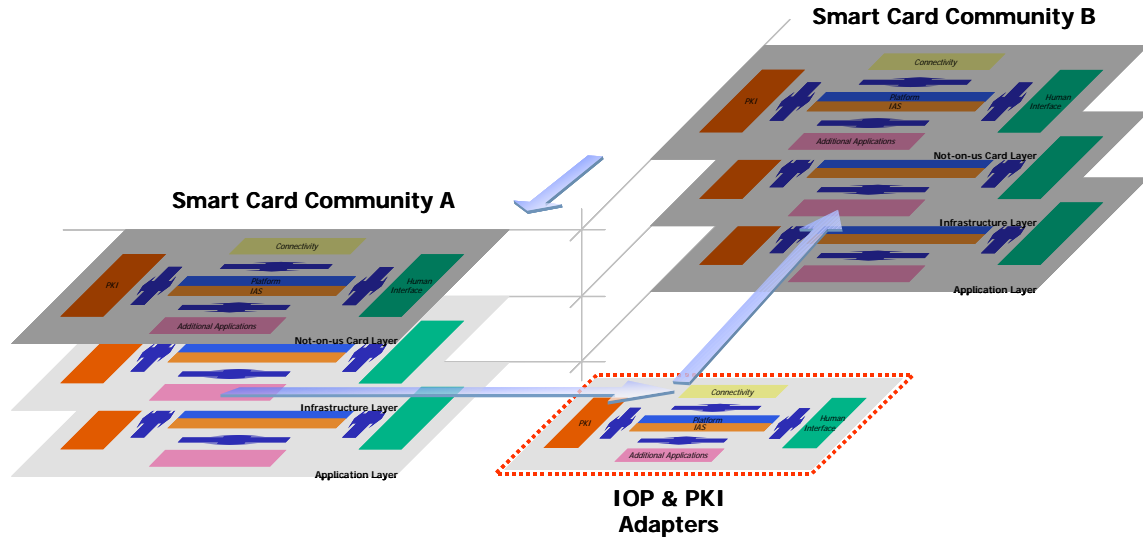
### **4.2.1 IOP & PKI adapters**

The function of the adapters is to connect two smart card communities to handle the data involved in the IAS exchange process, and to transform the flow of common data from one SCC to the other.

These adapters are interfacing:

- Both infrastructure for handling IAS (in the terminals, or via the terminals in the network server and or a front office of the access provider)
- Both PKI services for verifying not-on-us certificates
- An “on-us” card with a “not-on-us” e-service or a “not-on-us” card with an “on-us” e-service, as far as they are allowed to start an IAS-session

These adapters can be modelled as an additional infrastructure layer, including all functional boxes, acting as a link between the infrastructure layers of both smart card communities.



**Figure 4: Modelling the IOP Adapters (here in scenario 1)**

Therefore the IOP adapters have the following set of functions:

- To create **outgoing access** to the requested pre-registered “not-on-us” layers and functions
- To accept **incoming access** from pre-registered “not-on-us” layers and functions
- To invoke the appropriate IOP business rules for the (incoming/outgoing).

#### **IAS/IOP related business rules**

Each service provider may use this offered technical capability, but always under the control of its own “business rules”. These SP business rules are key to the functioning of an e-service community. They define the conditions under which cardholders are provided access to e-Services and are therefore strongly depending upon the specifications agreed between the service provider and a smart card community in which it deploys its services.

Within an e-service community, there is therefore one set of business rules for each smart card community in which a service provider deploys its services. These business rules are therefore based on the interoperability agreement between a SP and a SCC.

#### **The IOP and PKI adapters**

To realise IOP between smart card communities, connection mechanisms are required in order to:

- Make connections to services in other smart card communities
- Buffer data during the IAS data transfer process
- Transform data from conventions as used in one smart card community to conventions in the other smart card community. It is assumed that there may still be differences, even when respecting the requirements for process model, functional boxes model, the data model and the modelled standards for technical components.

#### **1. The (technical) IOP-adapter:**

- After understanding the cardholder request for a “not-on-us” e-service, AND if the business rules are not downloaded as an “on-card” application, then a call is made for the appropriate “not-on-us” business rules for

- o Identification (which only means that the secure building blocks are checked for security; the ID reading is publicly accessible)
- o Authentication (which means that the service provider wants to verify the card holder identity)
- o Signature (which means that the card holder has the intention to sign an object)
- When the business rules of the e-service require certificate(s) match, then the connection to the “not-on-us” PKI adapter will be initiated (see below, at PKI adapter).
- The IAS session has to be executed, with transfer and eventually transition of data that are exchanged according to the agreed IOP and technically laid down in the IOP adapter.

## 2. The PKI adapter:

- Addresses the request for “not-on-us” certificate check, based on the business rules
- Establishes the secure connection to the requested “not-on-us” PKI-directory
- Validates the requested PKI-directory
- Applies the business rules that are applicable for the requested certificate
- Allows/Refuses continuation of the e-service session
- Terminates and logs (administrative) data.

From the implementation strategy point of view, there are different ways to organise the implementation of the IOP adapters. One of the key questions is how far GIF can go in modelling and specifying:

- Do the smart card communities wish - and are they able - to comply with a detailed and constraining model which will be actively maintained? If this choice is considered appropriate, it can be implemented:
  - o At the level of an industry branch (health, e-government, transport, banking)
  - o At a broader level. Then a separate body must be created for active maintenance
- Do smart card communities just make bilateral arrangements based on a generic model?

The answer has many consequences for the types of technical solutions to be implemented.

### 4.2.2 IOP conformance testing

An IOP conformance testing facility must be used for accepting and certifying the interface software with which new “not-on-us” e-services will be connected to the “on-us” IAS nucleus.

It is recommended to use a test / work bench system for these purposes.

No further details on requirements will be provided here as this goes too far in the details with regards to the ambitions of the GIF.

## 4.3 Requirement for implementing IAS/IOP processes

Depending from the agreed IOP strategy, the IOP and PKI adapters are to be implemented in such a way that one or more scenarios for interoperability can be carried out.

- **Scenario 1:** the “not-on-us” cardholder connects his/her card to the “on-us” smart card community and accesses the “on-us” e-service, for which it may be required to authenticate the certificates and/or the cardholder in the “not-on-us” environment.

- **Scenario 2:** the “not-on-us” cardholder connects his/her card to the “on-us” smart card community and accesses the “not-on-us” services. Here two network connections have to be made:
  - o One to the “not-on-us” smart card community, where the card is issued, in order to check the certificates (if required; see scenario 1)
  - o One to the “not-on-us” e-service (if not directly connected to the on-us infrastructure; see scenario 3)
- **Scenario 3:** the on-us cardholder connects his/her card to the on-us smart card community, and accesses a not-on-us service. The connection is made to the not-on-us environment, where the e-service is available.

	<b>IOP Scenario #1</b>	<b>IOP Scenario # 2</b>	<b>IOP Scenario #3</b>
1	Connect smart card to terminal and secure the link	Connect smart card to terminal and secure the link	Connect smart card to terminal and secure the link
2	Activate identification and recognise the not-on-us card	Activate identification and recognise the not-on-us card	Activate identification and recognise the on-us card
3	Activate call for on-us application access and determine the business rule  IF AUTH/E-SIGN IS REQUIRED: ACTIVATE A CALL FOR <b>PKI</b> ACCESS IN not-on-us ENVIRONMENT	Activate call for not-on-us application access IN THE not-on-us <b>SERVICE</b> ENVIRONMENT and determine the business rule.  IF AUTH/E-SIGN IS REQUIRED: ACTIVATE A CALL FOR <b>PKI</b> ACCES (if e-service is registered in third smart card community) IN not-on-us ENVI- RONMENT	Activate call for not-on-us application access IN THE not-on-us SERVICE ENVIRONMENT and determine the business rule
4	Make safe connection (local) for the not-on-us card in the on-us infrastructure and transfer the ID data	Make safe connection for the not-on-us card in the ‘not-on-us’ infrastructure and transfer the ID data	Make safe connection for the on-us card in the ‘not-on-us’ infrastructure and transfer the ID data
5	Authenticate Card holder via the safe connection (if required) IN THE not-on-us <b>PKI</b> ENVIRONMENT	Authenticate Card holder via the safe connection (if required) IN THE not-on-us <b>PKI</b> ENVIRONMENT	Authenticate Card holder (if required) via the safe (local) connection
6	Execute e Service (IAS is passive)	Execute e Service (IAS is passive)	Execute e Service (IAS is passive)
7	Use signature data via the safe connection (if required) IN THE not-on-us <b>PKI</b> ENVIRONMENT	Use signature data via the safe connection (if required) IN THE not-on-us <b>PKI</b> ENVIRONMENT	Use signature data via the safe connection (if required)
8	Update log files and close	Update log files and close	Update log files and close

**Table 12: IAS processes in the three IOP scenarios**

## 5 Appendix

---

### 5.1 More information

GIF is part of the e-Europe 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](mailto:arkel@cardlife.nl)
- Theo van Sprundel [theo.vansprundel@bull.nl](mailto:theo.vansprundel@bull.nl)
- Marc Lange [marc.lange@build-in-europe.be](mailto:marc.lange@build-in-europe.be)
- Yvan Pirenne [yvan.pirenne@build-in-europe.be](mailto:yvan.pirenne@build-in-europe.be)
- Laurent Den Hollander [laurent.den.hollander@sharp.co.uk](mailto:laurent.den.hollander@sharp.co.uk)

## **5.2 Overview of GIF Requirements (for purposes of RFI, RFP or “gap analysis” comparing to existing systems)**

### **5.2.1 General implementation requirements**

For the technical building blocks the following categories of criteria should be considered and elaborated:

- Easy to program
- Secure card operating system
- Sufficient processor speed
- Sufficient data storage capacity
- Scalability
- Portability
- Flexibility
- Modularity
- Secure/fraud resistant
- Robustness
- Durable (5-10 years)
- Cost effective
- Vendor independent
- Testable

**5.2.2 Operational and implementation requirements overview table**

Subject	Specification	Description	Prerequisite for IAS or Required for IOP (= add on) [p/r]	Available? [y/n]
General				
Work/test-bench				
Processes				
Create / Register smart card community	<ul style="list-style-type: none"> <li>• Register smart card community and external secure suppliers</li> <li>• Verify the compliance of SCC stakeholders with CI requirements and register them (establish ID + URL)</li> <li>• Provide PKI certificate to registered stakeholders as a technical proof of their registration</li> <li>• Verify the compliance of all secure "building blocks" (technical components), register them and provide the with PKI Certificate</li> </ul>			
Card/cert. Issuing	<ul style="list-style-type: none"> <li>• Personalise card</li> <li>• Issue card holder certificates</li> <li>• Initialise the card</li> <li>• Enrol the card</li> <li>• Maintain life cycles (card, holder ID, certificates)</li> </ul>			
Post issuing application	<ul style="list-style-type: none"> <li>• Test/Accept IAS connection software offered by the e-service provider</li> <li>• Test/Accept "on-card application" software offered by the e-service provider</li> <li>• Authorise download or download "on-card application" offered by the e-service provider</li> </ul>			
IOP – Net-work	<ul style="list-style-type: none"> <li>• Create IOP adapter, put rules and policies in</li> <li>• Maintain IOP adapters</li> </ul>			
Community management	<ul style="list-style-type: none"> <li>• Log the use of cards, IS and front office</li> <li>• Billing</li> </ul>			
IAS process	<ul style="list-style-type: none"> <li>• Connect smart card to (modules in) terminal and secure the links</li> <li>• Identify/validate and accept/reject the card in IS + identify/validate and accept/reject the terminal/terminal application (authenticate the 'building blocks')</li> <li>• Interact with the requested e-service and find the business rules for the requested e-service</li> <li>• Transfer ID data to the e-service</li> <li>• Authenticate card holder (if requested for e-service)</li> <li>• Execute e-service (IAS is passive)</li> <li>• Sign an information object (if requested for e-service)</li> <li>• Update administrative log-files and close the IAS session</li> </ul>			

Subject	Specification	Description	Prerequisite for IAS or Required for IOP (= add on) [p/r]	Available? [y/n]
Functions				
IAS function.	<ul style="list-style-type: none"> <li>Connect smart card to (modules in) terminal and secure the links</li> <li>Identify/validate and accept/reject the card in IS + identify/validate and accept/reject the terminal/terminal application (authenticate the 'building blocks')</li> <li>Interact with the requested e-service and find the business rules for the requested e-service</li> <li>Transfer ID data to the e-service</li> <li>Authenticate card holder (if requested for e-service)</li> <li>Execute e-service (IAS is passive)</li> <li>Sign an information object (if requested for e-service)</li> <li>Update administrative log-files and close the IAS session</li> </ul>			
Human interface	<ul style="list-style-type: none"> <li>Language preference</li> <li>Notification of process progress</li> <li>Positive consent</li> <li>Presentation of e-services</li> <li>Individualised preferences</li> <li>Security (remote display, keyboard, SAM)</li> </ul>			
PKI	<ul style="list-style-type: none"> <li>Qualified certificates e sign directive art. 5.1</li> <li>Security EAL 4 + (augmented with VLA)</li> </ul>			
Card connectivity	<ul style="list-style-type: none"> <li>Contact card interface:</li> </ul>			
e-service connection	<ul style="list-style-type: none"> <li>Address to access</li> <li>Business rules</li> <li>Object to be signed</li> <li>On-card application</li> </ul>			
IOP adapters	<ul style="list-style-type: none"> <li>Technical adapter</li> <li>PKI adapter</li> </ul>			
Data				
Common data management	<ul style="list-style-type: none"> <li>IAS card holder data</li> <li>Stakeholders data</li> <li>Building blocks (certificates, addresses)</li> </ul>			
Redundant data management				
Building blocks/modules				
Card	<ul style="list-style-type: none"> <li>ISO/IEC 7816</li> <li>Global platform / Java</li> <li>Security concept</li> <li>On-card application ability</li> </ul>			
Readers + security modules	<ul style="list-style-type: none"> <li>Finread compliant</li> </ul>			
Secure terminals	<ul style="list-style-type: none"> <li>Finread compliant</li> </ul>			
Network modules				
Front office Server modules	<ul style="list-style-type: none"> <li>Access module</li> </ul>			