Open Smart Card Infrastructure for Europe

v2

Volume 3: **Global Interoperability Framework for identification, authentication and electronic signature (IAS) with smart cards**

Part 2: **Requirements for IAS functional interoperability**

Authors: **eESC GIF Expert Group**

GIF-2 Team: Theo van Sprundel, Jan van Arkel, Marc Lange, Yvan Pirenne

Edited by: Peter Tomlinson, Chris Makemson

FOR DOCUMENT HISTORY: SEE ANNEX A

Table of Contents

Table of Figures

Index of Tables

0 Executive Summary

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

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

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

The key messages of the GIF are the following:

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

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

Part 2 contributes to developing these key messages by deploying a **global vision** on how IAS interoperability may affects at operational and implementation level the models developed in Part 1, i.e. roles of the stakeholders, the functions required for the functioning of a SCC, the IAS-related data and the building blocks which constitute an smart card based information system.

1 Introduction

1.1 Overview

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

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

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

This document is the second part of the framework, describing the functional and interoperability requirements for large scale deployment of generic IAS using smart cards. This part 2 develops operational and implementation models for interoperable IAS systems, derived from the contextual and conceptual models of part 1.

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

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

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

The Global Interoperability Framework is in 4 parts:

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

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

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

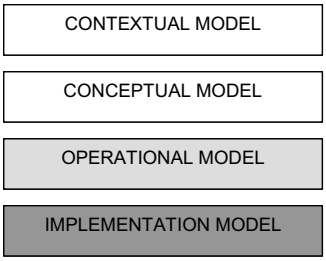

Figure 1: Four tiers in the methodology

Mapping the framework with the methodology

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

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

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

Figure 2: GIF Parts and the 4-Tier methodology

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

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

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

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

The operational model is described using the following elements:

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

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

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

1.2 Scope of GIF part 2

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

It outlines, following the models presented in part 1:

- The stakeholders' responsibilities and liabilities in organising IAS – in an interoperable manner,
- The requirements to be met by ICT 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 for all parties involved
- Applying available standards, technical specifications and relevant products
- Creating and protecting a business case for all parties
- Supporting user convenience

This document covers the requirements for smart card enabled schemes, which have been discussed in different European bodies as well as in the areas of:

- 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 the eEurope Smart Card Charter
- Decision-makers and consultants involved in preparing a smart card community with generic IAS for supporting multiple services, especially communities for *e*-government services
- Those who are involved in establishing RFIs and RFPs for multi-service and interoperable IAS
- Project leaders for pilots on generic IAS

1.3 Acronyms

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

Acronym	Term
AI	Application Issuer
AP	Application Provider
CA	Certificate Authority

CEN	Centre Européen de Normalisation
CH	Card Holder
CI	Card Issuer
CofC	Certificate of Conformance
CP	Card Provider
CRL	Certificate Revocation List
CSP	Certificate Service Provider
CWA	CEN Workshop Agreement
EAL	Evaluation Assurance Level
eESC	*e*-Europe Smart Cards
e-ID	Electronic IDentification
EMV	Europay, MasterCard, Visa
E-sign	Electronic Signature Directive 1999/93/EC
eURI	URI extended to multi-application smart cards
GIF	Global Interoperability Framework
GSM	Global system for digital mobile telephones
IAS	Identification, Authentication and Electronic Signature
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
ID	IDentification
IOP	Interoperability
ISO	International Standards Organisation
JCRE	JavaCard Runtime Environment
OCSP	On-line Certificate Status Protocol (RFC 2560)
OTBS	Object To Be Signed
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RFI	Request For Information
RFP	Request For Proposal
SAM	Secure Access Module
SCC	Smart Card Community
SP	Service Provider
SSCD	Secure Signature Creation Device
TB	Trailblazer (eESC)
TLV	Tag Length Value
UML	Universal Modelling Language
URI	User Related Information
URL	Uniform Resource Locator
VA	Validation Authority
VLA	Vulnerability Level Assurance
XML	Extensible Mark-up Language

Table 1 – Acronyms

2 Operational model for interoperable IAS using smart cards: roles, functions and pre-requisites

2.1 Introduction

The operational model in this chapter uses the conceptual model of GIF part 1 as input. Assumptions are set out, roles and functions are described in more detail, and pre-requisites for scheme components are identified. In this chapter, the model is primarily developed for a single scheme in a generic IAS environment using smart cards. This is then extended to add interoperability interfaces between schemes.

Chapter 3 develops further the operational context for both single scheme (on-us operation of functions and processes) and interconnected scheme (not-on-us operation) scenarios.

The analysis follows the classification introduced in the conceptual model:

- Basic processes and roles
- Functional elements
- Data model
- Technical building blocks

The basic assumption of the contextual model (GIF Part 1) is of an open scheme architecture to serve the smart card community. Following establishment of core IAS services, this permits extension to additional *e*-services that can make use of the IAS services.

This operational model follows the assumptions made in the development of the conceptual model in GIF Part 1. The main assumptions are:

- the model is designed to meet the requirements of *e*-government services (but is expected to provide an interoperable IAS nucleus for many business to citizen and business to business services);
- strong (high level) security is essential;
- it is most likely that a PKI will be used as the trust architecture (so that the operational and implementation models are developed for a PKI);
- the boundary of a 'smart card scheme' is co-terminus with the boundary of a single security domain; and,
- because of the *e*-government environment, responsibility for the following roles is combined in one organisation:
  - Registration authority (RA);
  - Certificate service provider (CSP), which is most likely to be a PKI certificate authority (CA) (which includes the possibility of delegating certificate validation to a Validation Authority (VA));
  - Card issuer (CI);
  - On-card IAS application issuer (IAS AI);
  - SCC administrator; and
  - IAS service provider (IAS SP)

The combined organisation is described as the 'Card Issuer' in this operational model, qualified where necessary (e.g. 'CI acting as CA').

Note that tasks associated with the above roles may be delegated to other operational entities.

Pre-requisites for this part 2 of GIF in this model for interoperable smart card communities using *e*-government services are:

- the card issuer (CI) is a central or local government administration;
- a PKI is used;
- the schemes must comply with the EC Electronic Signature Directive 1999/93/EC (E-sign) (and therefore be capable of issuing and supporting attributes in certificates in order to be able to comply with the advanced electronic signature requirement in clause 5.1 of E-sign);
- the primary set of certificates installed on the card represent the official identity of the card holder;
- the card issuer (CI), having legal responsibility for the scheme, accepts the duty to develop and maintain interface specifications for interoperability with other schemes;
- the GIF part 1 *e*-service community concept of service providers supplying services to card holders from many card communities (schemes) is implemented; and
- card holders are all real persons (i.e. cards are not held by organisations).

Note that roles held by, and responsibilities of, real persons may be indicated on the card by use of either qualified certificates or attribute certificates, but:

- the operational model assumes that qualified certificates are used (rather than using attribute certificates) where the card holder ID information in the certificates is to be extended, and.
- the combining of roles for the card issuer assumed in the model may mean that qualified certificates (or attribute certificates) are stored in a separate on-card application rather than in the on-card IAS application, but the model provides for IAS services using those certificates to use the underlying cryptographic services in the smart card.

The above assumptions and pre-requisites are not intended to exclude other models. However, it is suggested that other operational models should, where possible, use elements of the present model.

The interoperable IAS nucleus with strong security is expected to be an enabler for the business needs of third party service providers, who are invited to join the associated *e*-service community.

2.2 Roles and functions

2.2.1 Card issuer combined roles

The card issuer's first task, in the card-issuing role, is to establish security management functions (security policies and processes) across the entire scheme.

The tasks that are directly associated with issuing cards include:

- Acquiring cards to the scheme's specification;
- Personalising and initialising the cards;
- Creating the card population database;
- Delivering the cards to the card holders;
- Managing the card life cycle; and
- Maintaining the card population database (including establishing and operating card backup accounts).

The combining of roles also brings to the CI the tasks associated with other roles. These tasks include:

- Registering real persons (or re-registering, if a citizen register already exists);
- Issuing certificates (including key generation);
- Loading the IAS application onto the card;

- Providing an IAS service (a CSP/CA/VA service), and
- Establishing and operating a backup account for the on-card IAS application.

The CI is further responsible for establishing contracts (Service Level Agreements) with:

- Other card application issuers
- Other certificate issuers (e.g. of qualified certificates)
- Other service providers
- The access providers
- The content providers
- The card providers

and all contracts required for managing the security of the scheme.

2.2.2 Operating the trust model

The relationships of the major entities in the basic roles model can be summarised as follows:

- The **card issuer** in the framework model (with combined roles) is responsible for
  - Card issuing and card management tasks for card holders
  - Scheme security
  - Organising the smart card community
    - Registering card holders
    - Triggering certificate issuance, maintaining them and offering verification services to all service providers
    - Making access available to high level IAS *e*-services (including IAS on-card application load)
    - Ensuring that service level agreements are established
- The service provider is primarily oriented to
  - The card issuer with which he has made all necessary arrangements
  - The cardholders whom he welcomes to his service
- The **card holder** has his/her basic relations with
  - The card issuer (in order to belong to a smart card community)
  - A number of chosen service providers

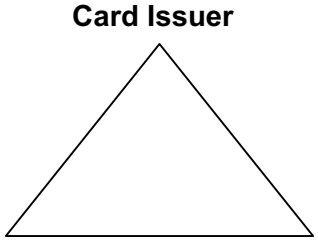

Figure 3: Trust model as the basis of the GIF concept

2.2.3 Performing the roles

Performing the roles is based upon the processes (functions) they are supporting for the delivery of common and trusted IAS services. These processes are classified as primary, secondary and tertiary, depending on the relationship that they have with the core IAS functions. A separate set of tertiary processes for interoperability is included.

Note that this sub-section lists processes only, and does not include their allocations to stakeholders.

Primary IAS processes

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

- **Connect** (contact or contactless) smart card to (modules in) terminal and secure the links
- **Identify/validate and accept/reject** the card in the infrastructure + identify/validate and accept/reject the terminal / terminal application (authenticate the building blocks)
- **Find, open and interact** with the requested *e*-service
- **Transfer ID data** to the *e*-service / make data available
- **Authenticate** card holder (if requested by the *e*-service)
- **Execute** *e*-service (IAS is a slave function)
- **Sign** an information object (if requested/required by the *e*-service)
- **Update** administrative log-files and close the IAS session

e-service service providers grant access to their services under the control of their own business rules. These service provider business rules are key to the functioning of an *e*-service community: they define the conditions under which cardholders are granted access to *e*-services. The business rules for *e*-services are, however, strongly dependent on the specifications agreed between the service providers and the smart card community in which they deploy their services. As presented in the function model defined in GIF Part 1, the business rules are technically to be considered as being implemented in service providers' applications (the "additional applications" function in the functional model).

Note that:

- *e*-service service providers do not have to use the common IAS services, although the framework only includes within its scope those e-service providers who use the common IAS services either by selecting the nucleus IAS application on the smart card or via a proprietary on-card application that has internal on card access to the nucleus IAS services; and
- access to *e*-services, whether or not those *e*-services use the IAS services, is *always* subject to the business rules of the *e*-service

Secondary IAS processes in a single scheme

The processes listed below are secondary processes aimed at ensuring that the IAS services provided by the card issuer can be trusted by service providers and card holders, that the network infrastructure is created and maintained, that commercial functions are implemented within the network, and that scheme security is established and maintained. They follow from the assumptions above, with the objective that *e*-government services are provided at the required quality and security levels, and respecting the combining of multiple roles for the card issuer.

Note that:

- secondary processes specific to interoperability between smart card communities are described after the tertiary processes below.

The CI is responsible for the processes by which the smart card community is created and maintained. These processes are required to comply with the following criteria:

- Trust and security
- Technical compatibility
- Business cases respecting all stakeholders responsibilities

- User convenience

For security purposes, the roles which in the framework model are assumed by the card issuer must be treated separately in the definition of processes.

Note that:
- The recommended processes identified in the following table and lists are not necessarily listed in the sequence in which they take place; and
- The table and lists are not necessarily a complete list of secondary functions.

1	**Creating a Smart Card Community** (Registration and internal certification)
1.1	• Register the smart card scheme (smart card community or SCC) and external secure suppliers
1.2	• Verify the compliance of SCC stakeholders with card issuer requirements and register them i.e. establish ID + URL
1.3	• Provide PKI certificates to registered stakeholders (including those roles incorporated into the CI) as a technical proof of their registration
1.4	• Verify the compliance of all secure building blocks (technical components), register them and provide them with PKI Certificates
1.5	• Develop security policies and processes
2	**Issuing and maintaining cards**
2.1	• Personalise cards with card holder details
2.2	• Issue card holder certificates
2.3	• Initialise the cards
2.4	• Download on-card IAS core application software
2.5	• Enrol (register) the card holders
2.6	• Maintain life cycles (cards, card holder ID, certificates)
3	**Registering and implementing e-services** (including at post issuance)
3.1	• Test/Accept IAS and *e*-service interface software used by the *e*-service provider
3.2	• Test/Accept on-card application software and data structures offered by the *e*-service provider (if used)
3.3	• Authorise download and/or implement download of on-card applications offered by the *e*-service provider (if used)
4	**Managing Smart Card and *e*-service Communities and scheme infrastructure**
4.1	• Agree commercial parameters (tariffs, service levels)
4.2	• Agree network infrastructure provision with access providers
4.3	• Capture and log session data: the use of cards, application load, IAS core services and the network (including maintaining card and IAS application backup accounts)
4.4	• Execute, acquire and settle transactions (between stakeholders)
4.5	• Manage security
4.6	• Manage scheme infrastructure

4.7	• Provide card holder customer services (including single point of contact help desk)

Table 2: Recommended single scheme processes

1. Creating a Smart Card Community (Registration and internal certification)

1.1 Register the smart card scheme (smart card community) and external secure suppliers

Required functions are:

- Card issuer (CI) registration and certification (in relation to the issued cards and as a basis for all other certification of stakeholders)
- Supplier registration (e.g. card providers, infrastructure providers)

1.2 Verify compliance and register SCC stakeholders

Required functions are:

- Develop compliance criteria
- Develop compliance verification process
- Develop registration process
- Verify compliance and register (including establishing ID and URL where required)

At least the following stakeholders are included:

- Certificate authority (CSP/CA/VA) and registration authority (RA) (for certificate issuance, card holder registration and IAS functionality)
- Card providers (CPs)
- Application issuers (IAS AI and all other AIs)
- Service provider (SP)
- Content provider (in relation to service providers)
- Access provider (AP)

1.3 PKI certification of stakeholders

Required functions are:

- Issue certificates to list of stakeholders in item 1.2

1.4 Compliance and certificates for building blocks

Required functions are:

- Develop compliance criteria
- Develop compliance verification process
- Card type compliance verification and transport certificate issuing (for unpersonalised cards)
- Card registration and certification for every card issued
- Infrastructure building blocks: identification, compliance verification (including terminal to card interface), certificate issuing for all building blocks, address creation and network maintenance

1.5 Develop security policies and processes

See item 4.5

2. Issuing and maintaining cards

2.1 Personalise card

Required functions are:

- Electronic card issuance (including loading card holder identification and authentication information)
- Physical card issuance (including printing card holder and scheme information on the surface of the card)

2.2 Issue certificates

Required functions are:

- Authenticate card and card holder

- (Optional) Record card holder attributes (for advanced electronic signature complying with E-sign)
- Generate key pairs
- Load certificates

2.3 Initialise cards
Required function is:
- Initialisation of the card (enable chip for operation)

2.4 Enrol the card holder
Required functions are:
- Card holder registration
- Notify card holder (scheme rules)
- Obtain card holder agreement to join smart card community (signature, which may be physical or electronic)
- Obtain confirmation of card delivery to card holder

2.5 Maintain life cycles
Required functions are:
- Card holder status
- Certificate status
- Card status
- Hot lists
- Card service management (including card replacement with card content re-instatement)

3. Registering and implementing *e*-services (including at post-issuance)
3.1 Test/Accept IAS and e-service interface software
Required functions are:
- Register *e*-service application
- Test *e*-service IAS and network interface software
- Accept *e*-service application

3.2 Test/Accept e-service on-card application (if used)
Required functions are:
- Register *e*-service on-card application
- Test *e*-service on-card application
- Accept *e*-service on-card application

3.3 Download of e-service on-card application (if used)
Required functions are:
- Develop/acquire pre- and post-issuance application download facility
- Register and certify on-card application download
- Authorise or implement download of on-card application

4. Managing the Smart Card and *e*-service Communities and scheme infrastructure
4.1 Agree commercial parameters
Required functions are:
- Service level agreements
- Implement internal/external tariffs

4.2 Agree network infrastructure provision with access providers
Required functions are:
- Service level agreements
- Deploy and manage infrastructure

4.3 Capture and log session data
Required functions are:
- Transaction logging (for commercial purposes and card holder backup)
- Maintain historical databases (including card holder and IAS service backup accounts)
- Management reporting (use statistics, performance monitoring, etc)

Note that *e*-service providers and application issuers are expected to maintain card holder backup accounts associated with their services

4.4 Execute, acquire and settle transactions
Required functions are:
- Logging of inter-stakeholder performance indicators, statistics
- Invoice/clear internally
- Invoice/clear cardholders

4.5 Manage security
Required functions are:
- Create security policies and processes (including independent verification)
- Develop secure key distribution mechanisms (where required, e.g. for terminal infrastructure, or for distributed card issuing points)
- Monitor scheme performance for continuing compliance (including revising security policies and processes when required)

Note that registration processes must include verifying compliance of stakeholders with security policies and processes

4.6 Manage scheme infrastructure
Required functions are:
- Fault reporting and clearance
- Update card issuing systems as required
- Introduce new card types as required (including updating terminal infrastructure for compliance with new card types)
- Update terminal management as required
- Update records and network management as required

4.7 Provide card holder customer services
Required functions are:
- Implement and operate single point of contact for card holders, via several routes (phone, internet, personal contact) (including advising card holders via information printed on the card and possibly included in the card)
- Provide fault diagnosis, card replacement and customer application and data restoration services
- Include customer support provisions in service level agreements (including standards of service for two routes: direct to customer and indirect via single point of contact)

Tertiary IAS processes

The *e*-service processes other than IAS are described as tertiary processes. They may or may not be related to IAS services, because, although all *e*-services for the card holder are candidates for access to the smart card community, the use of IAS services is not mandatory. Tertiary processes internal to the *e*-services are fully and only under the responsibility of the service provider, and are not detailed here.

Secondary IAS processes for interoperability

When negotiating interoperability between SCCs, both SCCs should compare all their policies and processes for compatibility, using the primary and secondary lists

above as guidelines. The processes listed here are additional to the secondary processes listed above for a single scheme.

	Establishing & maintaining interoperability
1	• Create interoperability specifications
2	• Establish interoperability agreements
3	• Create IOP- and PKI-adapters/gateways, install rules and policies
4	• Maintain IOP- and PKI-adapters/gateways

Table 3 - Recommended interoperability processes

Note that some functions may be available without interoperability agreements. For example, a not-on-us card may be able to use a terminal pass-through service to access secure *e*-services not registered with either the on-us or the not-on-us card's SCC. Such functions will necessarily be limited, as the external *e*-service will not be able to authenticate the terminal, and the terminal will not be able to authenticate the card or card holder – however, the not-on-us service may be able to authenticate the card even though it cannot identify where the card is (this is a classic insecure network situation).

Establishing & maintaining interoperability

1. Create interoperability specifications

Required functions are:

- Define outgoing requests (certificate verification request and *e*-service request)
- Define incoming interoperability requests (certificate verification request and *e*-service request)
- Define pass-through service protocol
- Implement request handlers

This definition (specification) work should be carried out during initial scheme development, even if interoperability is not immediately required.

2. Establish interoperability agreements

Required functions are:

- Compare security policies and processes for compatibility
- Where required, create rules defining restrictions on functions and trust for interoperable transactions, and make available to *e*-service providers
- Define interoperable services and associated commercial contracts
- Agree and confirm interoperability contracts

3. Create and configure IOP- and PKI-adapters/gateways

Required functions are:

- Modify implemented outgoing interoperable request where required (technical request and verification request)[2]
- Modify implemented incoming interoperable request where required (technical request and verification request)[2]
- Determine ownership of adapter/gateway implementation
- Develop, certify and allocate ID to adapter/gateway function

4. Maintain IOP- and PKI-adapters/gateways

Required functions are:

- Each SCC to inform other SCCs when changes affecting interoperability are defined
- SCCs to implement and test any modifications required to adapters when other SCCs make changes affecting interoperability

[2] The particular case identified is where one CA offers only CRL search for certificate verification, and another offers online verification using OCSP.

- Restrictions applying to interoperable transactions to be updated as necessary and the change information distributed to *e*-service providers

2.3 Pre-requisites for scheme development

The pre-requisites applicable to the functions of the smart card enabled system are presented below according to the functional boxes model (see GIF part 1 chapter 6).

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 functions which the *e*-service can use:

- 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 for securing the primary processes concerned as far as required.
- Strong authentication of the parties in the session (including verification of the cardholder via PIN code and/or biometrics).
- Qualified digital electronic signature of an (information) object.

The four independent categories of 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 exchanges to be applied to:

- Card connectivity: card readers, terminal and networks
- Human interface
- Business rules and other information for the *e*-service involved.
- PKI handling

These four categories of functions (the 'functional boxes', for which see GIF part 1 chapter 6) have to be kept independent because there is a need to be able to change the content of each category (functional box) without influencing the rest of the system in the framework. This need for independence when implementing changes arises from a combination of internal and external influences, including:

- Technology and market developments in infrastructure components
- Standardisation of ICT human interfaces, including provision for special needs
- The commercial independence of *e*-service providers
- Developments in security methods

GIF part 1 chapter 6 shows the functional boxes intersecting the 3 layers of the conceptual model (front office application, infrastructure, smart card), illustrating that the functions may be implemented across the layers. Orthogonal connectivity (including security) functions support the functional box implementations.

2.4 Pre-requisites for IAS 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 interoperability process cover only the data required for the following minimum IAS functions:

- Securing the building blocks
- Identifying the stakeholders
- Authenticating the users
- Digital electronic signature

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

- User identification
- Certificates for strong authentication and advanced electronic signature (as defined in E-sign)[3]
- Stakeholder identification and authentication for creating security over an open network, within and between smart card communities
- Building blocks (entities of standardised hardware/middleware/software) identification to secure the links between the systems
- Network addresses

The minimum set of common data for interoperability is the same as mentioned in the previous clause, augmented with data categories to make the interoperability adapters/gateways adapters function. Data covers requirements in:

- Network components for interoperability (addresses)
- Network security

2.5 Requirements for the building blocks

The core IAS building block is the trusted token: the smart card for *e*-ID (IAS) 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 advanced electronic signatures (as defined in E-sign) have to be exclusively placed on this token.

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

Note that the requirements in this part of the framework represent the current position in the *e*-government sector, and will evolve with time. For that reason and because GIF is open to all suitable infrastructure, these requirements are not guaranteed to be complete.

Note also that interoperable operation using secure channels may require security key exchange between schemes. The model for this is not yet developed.

2.5.1 Smart card layer related requirements

The following card requirements should be fulfilled when preparing an SCC implementing GIF.

[3] The handling of attributes required in qualified certificates is not yet fully developed in the framework.

Physical characteristics

- ID-1 format as in ISO/IEC 7816 and related standards
- Expected life time not shorter than the validity of ID and certificates
- Surface suitable for printing using the required long life and secure techniques

The ISO/IEC 10373 test standard gives some assistance with test methods, but other factors include the service life of non-volatile memory.

Logical and electrical interface

- Contact (ISO/IEC 7816) and/or contactless (ISO/IEC 14443 parts 1 to 4)
  Note that ISO/IEC 7816 is currently under revision, and also the EMV specification for payment cards and terminals is not entirely compliant with ISO/IEC 7816. Convergence of 7816 and EMV is an outstanding issue.

Chip

The following card requirements are a combined list of capabilities expected from the card as supplied by the CP, and from on-card software functions developed by or for the scheme.

- Directory/File structure for multi application capabilities or equivalent Java card data object storage
- OS to provide multi-application capabilities with secure firewalls:
  - Global Platform (Java or Multos with on-card security and resource management software, and with card platform recognition data structures)
  - Java 2.1 card virtual machine and API (preferred)
- Sufficient data storage capacity for the required functions (including certificates)
- Security concept including fraud resistance of the mask in line with functional requirements:
  - Certified by a recognised certification body, at the minimum level of Common Criteria EAL 4+
  - Authentication of all parties involved in card related activities by public key or public key certificate when performing actions other than reading card retained data (see below)
  - Secure data communications (secure channel capability)
  - Authentication (PIN and/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 to include:
  - Card holder ID
  - Card issuer ID
  - Unique card platform ID
  - Card manufacturer data (organisation, name, card type, version)
- (Post issuing) On-card application downloading capabilities in line with mandatory GIF specifications[4]
- On-card application deleting
- Internal card management in line with mandatory GIF specifications[4]
- Card state search in line with mandatory GIF specifications[4]
- The nucleus application collaborates with the access software in the infrastructure. This software should support:
  - Starting a two sided challenge (mutual authentication) between card and terminal / system
  - Securing links (if required at lower – module – level than the terminal)
  - General checks (card validity etc)
  - Handling the *e*-service requests from the user (on-us/not-on-us)
  - Handling the business rules requests from the *e*-service provider (e.g. certificate checks)

[4] Specifications to be developed at a later stage

- Passive status during *e*-service session (not using GSM or proposed ISO/IEC 7816 pro-active card functions)
- Terminating the session and logging of the required (administrative) data

2.5.2 Infrastructure layer related requirements

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

Reader / terminals

- Basic requirements:
  - Capability to read / handle all GIF accepted cards
  - Following recommendations from eESC TB4 for contact and TB6 for contactless card terminals/readers, and from TB-8 for human interface
  - Authenticated for use in the smart card community by / on behalf of the card issuer.
  - Handling IAS
    - Off line on-card application
    - Online with network server or *e*-service application
- In general, where secure terminals are required, following the FINREAD specification for functions and performance[5]:
  - Secure communication between chip, keyboards, and display (when using the screen/display and/or the keyboard of different building block(s), the links must be secured before the interaction starts.)
  - Displaying status / result information
  - Human interface presentation steered by individual IAS, and at least the capability to enter numeric codes.
- Easy selection of the *e*-service that can be accessed in a secure way:
  - Secure interaction between card and security access module (SAM) or other secure sub-system
  - Where it is permitted to use a remote SAM or equivalent, a reliable procedure must create a secure link between the card and the SAM, before any user interaction may take place
  - Preventing easy sensing of visual PIN code input
- Supporting eURI for configuration of human interface

Network

- Basic requirements[6]:
  - Handle secure communication between terminal / network server (as far as not integrated in the terminal)
  - Handle secure communication between network server and
    - Front office server of requested *e*-service and/or PKI server (outgoing)
    - PKI server (incoming)
- Functions and performance:
  - Support of the terminals in presenting the accessible *e*-services offered to the card holder
  - Option: network service to keep, maintain and handle some personal card holder data
  - 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:
  - IOP-adapter
  - PKI-adapter

[5] Note that FINREAD's specification is currently being merged with other terminal specifications to produce a continuum from high security to low security terminals, which will result in terminals being profiled for security, and there are other terminal architectures which also claim high security. Until a common profiling system can be worked out, FINREAD is a reference point for secure terminal design parameters.

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

2.5.3 Front office layer related requirements

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

Note that these requirements are not related to the business part of the e-Services but to the IAS primary processes. They are to be implemented in the front-end of the *e*-Services (i.e. an IAS front-end).

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 terminals, and/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 article 5.1[7]
- Security level in accordance with Common Criteria level EAL 4+ (augmented with VLA 2)

[7] The handling of attributes required in qualified certificates is not yet fully developed in the framework.

3 Operational model for interoperable IAS using smart cards: requirements for interoperability

3.1 Introduction

When considering the operational requirements, it is not enough strictly to study and describe 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 interoperability
- Content of the required ICT functions.

This chapter first presents “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?”, this clause describes the requirements for IAS as an ICT system from a functional point of view. Where possible, the functional requirements are described in terms of transformation from input to output. The nature of this clause is a checklist of required functions.

3.2.2 Functional boxes

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

Testing the interactions between the stakeholders should help in development within the functional boxes. If not required, it is then at least recommended to create a workbench where stakeholders can prototype and test their new developments. This is to support especially:

- The addition of new *e*-services (and deletion of services that are withdrawing).
- The addition of new connections to other smart card communities
- Further development in human interfaces and individual existing services.

1. Platform function

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

2. IAS function

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

- Access the on-us/not-on-us data as identified in the data meta-model of GIF Part 1
- Access the appropriate *e*-service (i.e. depending on the type of interoperability scenario)
- Call the IOP-adapter each time the IAS box has identified a not-on-us scenario.

Note that the IAS box is seen as the nucleus function and has always to keep control of, and have responsibility for, the whole process, including the interoperability

related ones. For instance, should the communication with the IOP-adapter 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 interoperability scenarios. This will be of particular importance for the following sub-functions:

- Language preference
- Individualised preferences:
  - Presentation
  - Profiles
- Notification of process progress
- Presentation of *e*-services to be accessed:
  - In on-us infrastructure
  - In not-on-us infrastructure
- Positive consent mechanism:
  - 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)
  - To express CH positive consent (sign the OTBS)
- Secure use of screen/display and keyboard eventually in combination with embedded secure modules (embedded secure tokens, which is in principle an option)

4. Connectivity function

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

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

5. PKI function

Either 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.
Or the PKI function will always be requested for certificate verification by the IAS function, whether the request is issued in the on-us or the not-on-us SCC.

The choice of method depends on the overall structure of the PKIs – respectively not linked or linked. Where PKIs are directly linked, the PKI-adapter is used (and is the responsibility of the PKIs); otherwise the IOP-adapter is called, and in turn calls a PKI-adapter to handle the security function.

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

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

3.3 SCC and *e*-service community set-up and trust management

This clause supplements the process related information in chapter 2. It is placed here in order to emphasise the importance for successful interoperability for schemes to be organised in a common manner and with common trust models.

3.3.1 The card issuer setting up an SCC

The following table lists the general issues that lead to requirements for the card issuer, with the requirements described in further detail below. Issues related to trust are separately listed in Table 6.

•	Issues concerning the smart card community	
	1.	Setting the objectives and limits of the generic IAS system
	2.	What organisation will actually issue the smart cards with generic IAS application (RA/CI relationship)?
	3.	Legal structure for SCC and CI
	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 CSP (Certificate service provider, probably a PKI CA)	
	8.	CSP arrangements
	9.	Assessment of the CSP
	10.	Obligations and liability of the CSP
•	Issues concerning the infrastructure arrangements	
	11.	Who contracts with the AP?
	12.	What should be arranged with the AP?
•	Issues concerning the *e*-services connected to the basic IAS process	
	13.	Who is responsible for the *e*-services offer?
	14.	What should be arranged with the SP?
•	Issues concerning relation to the card holder	
	15.	What is the responsibility to the cardholder?

Table 4: Card issuer issues

1. Setting the objectives and limits of the generic IAS system

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

- From the point of view of the card issuer:
  - To build and exploit a smart card base, using generic IAS
  - 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:
  - To obtain access to high level *e*-services
  - To experience optimal user convenience in using IAS for different services,
- From the point of view of the service provider:
  - To obtain the generic identification data for the (secure) *e*-service as well as strong authentication and advanced electronic signature (in line with E-sign article 5.1)
  - To make the *e*-services 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 the official ID of card holders, the purpose could be restricted to *e*-government services, at least for those *e*-services that require authentication and electronic signature. However, the framework develops an open model, in which it is expected that business to citizen and business-to-business services will benefit from the generic IAS functions.

2. What organisation will actually issue the smart cards with generic IAS application?

In the context of the framework, one organisation takes on multiple roles, including the role of card issuer, and is responsible for the process of:

- Establishing the card holder identity (RA role),
- Triggering key generation and creating certificates (CSP/CA role),
- Loading the IAS application on the card (IAS AI role),
- Loading the identity and other IAS components on the card (CI role),
- Issuing the card to the cardholder (CI role), and
- Maintaining a card backup account and providing a single point of contact for the card holder (CI role)

In the framework, this organisation is referred to as the card issuer (CI), and is the legal entity responsible for the whole SCC. Therefore the card issuer manages and is assigned complete responsibility for the SCC issuing process. The CI also facilitates the organisation of a complete value chain between the stakeholders.

The CI also contracts the CSP/CA for producing certificates for identification of scheme components.

The framework expects that national or local administrations will be ID-document bodies who establish the official identities of real persons, and they may also be the card issuers who apply the framework to public ID for *e*-services, especially *e*-Government services. Alternatively, they may decide to establish a separate legal entity to handle all smart card community exploitation issues.

3. Legal structure for SCC and CI

The smart card community may be organised in any suitable legal structure. Generally speaking the legal entity may itself be the CI, or may delegate power to a separate CI who assumes the combined roles described in part 1 of GIF.

Applying the framework to public ID, the national ID issuer is expected to be the card issuer. It decides on the legal structure, and the conditions under which this public function must be fulfilled. However, functions may be delegated to agents of the CI.

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 smart card community (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
- The card holder

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 policies established in the SCC. Most probably the originating party owns the IAS data, typically the CI or the SP. In the case of qualified certificates or attribute certificates, this framework does not yet completely specify the model.

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

5. Who can apply for IAS?

The SCC or the CI has to define the policy about the participation of citizens or others acting as customers. It can be open to all citizens or restricted to a particular group, and can include persons acting on behalf of businesses. This may be on a voluntary or a compulsory basis.

For public ID (official ID) the national body is expected 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 (possibly 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 compliant with the TB1 Citizen Certificate Guidelines. The data format on the card is expected to be TLV, but some administrations may use XML.

The data and the data collection process must be kept confidential. 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 – but the CI acting as RA still has to ensure that the real person is securely verified against that national register.

8. CSP arrangements

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

- The standard with which the CSP has to comply (including provision by the CSP of a certificate of conformance – see below)
- The types and all details of card holder and system component certificates to be issued
- The terms and condition of contract
- The organisation structure

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

For national ID, this framework assumes that the CI is also the CSP – but this does not remove the duty of the CI to prepare all the quality control information required by the list above.

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.

9. Assessment of the CSP

The CA, RA and VA 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 CSP

A CSP shall include an object identifier in the certificate of conformance (CofC). The CofC shall include:

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

Particular care must be taken with the limits of liability by the CSP (CA/RA/VA), and the obligations of the CSP to provide information about performance.

11. Who contracts with the AP?

In the context of the framework, the CI (or the SCC Administrator under delegated powers) will make contracts with (and define the conditions for) the access providers (also known as card acceptors, although their role in the framework is rather wider).

12. What should be arranged with the AP

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

- Provision and management of card terminals/card readers and secure links to other building blocks
- Human interface
  - Presentation standards, including a positive consent expression mechanism and eURI support for automatic reconfiguring of terminals
  - Presentation of the choice/access to on-us *e*-service
  - The same for not-on-us services
- Interoperable network services
- Conformance testing
- Logging for acquiring and settlement, or other forms of cost compensation within and between smart card communities

13. Who is responsible for the *e*-services offer?

The IAS *e*-service is a special case, and the framework assumes that it is controlled by the CI.

The use of generic IAS for identification purpose only is open to all service providers, without any control from the CI during operation. However, the *e*-service must be registered, the interface to the IAS service certified, and basic legal arrangements completed (reflecting the CI responsibilities to the cardholder).

The CI contracts in more detail with *e*-service providers who require:

- Authentication of the users
- Electronic signature.

The CI is free to choose 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. However, competition law and public procurement directives may apply.

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

14. What should be arranged with the SP

Between the CI and the SP, the following 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
- Conformance tests
- Conformance of the on-card application with the specifications of the card
- Loading the on-card application on the card holder's card (if required)
- Maintenance of a backup account for the on-card application (if an on-card application other than the IAS application is written to or otherwise caused to change internal data)
- Logging for acquiring and settlement, or other forms of cost compensation
- Certificates and addresses

15. What is the responsibility to the card holder?

The CI is fully responsible for the card and the IAS application. The CI is the first line of communication for the cardholder for any problem, also concerning access and *e*-services (the single point of contact).

The CI, when acting as or contracting with an 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 the 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) in response to standardised message, PIN, biometrics).

In the 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 The card issuer 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 insecure 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 dedicated to ICT processes, and includes security questions.

•	CI Trust issues and requirements
	1. Stakeholder registration, and ID and certificate issuance 2. Building block ID and authentication for secure processing 3. Card capabilities and security functions 4. Use of automated session key for immediate/pre-certificate security

Table 5: Card Issuer trust requirements

1. Stakeholder registration, and ID and certificate issuance

The CI has to give ID and certificates to all stakeholders and ensure that these are applied in all secured processes.

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

- Certificate authority (including RA and VA)
- Card issuer
- Service provider
- Card holder
- Access provider
- Content provider
- Smart card community administrator

The CI has to apply an appropriate issuing procedure.

In addition, major suppliers (in particular the card provider(s)) are also controlled by certificates.

2. The CI has to provide building block ID and authentication, for each of the secure building blocks

The blocks involved concern:

- Cards and their functional components (card platform, IAS application, other on-card PKI software, other on-card applications)
- Human interface software and other card reader software
- Infrastructure and its components (IAS SAM if used, 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 an adequate level of security:

- Card capabilities (see at requirements for building blocks):
  - Key generation on card (see note 1)[8]
  - Key storage on card
  - Certificate storage on card
  - Signature generation on card
- Secure viewing mechanism/final format OTBS
- Clear and easy to use consent mechanism
- Mandatory common elements for the certificates
- Qualified certificates for signing (conforming to E-sign article 5.1) (see note 2)[9]
- Algorithms in conformance with European Algorithm Catalogue

4. Use of automated session key

The CI has to ensure that automated session keys are used wherever communication is insecure. For example, when (as is normal) non-secure card readers are used.

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

By offering services to the constituency of more than one smart card community, the SP is by definition creating an *e*-services community. However, interoperability is only delivered when access to the *e*-service is available across SCC boundaries (see GIF part 1 clause 18).

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.

• Issues concerning the *e*-service community
1. Who can participate in the *e*-services community?
2. What must the SP arrange with the CI?
3. Legal arrangements/bylaws protecting the card holder (user)
4. Quality of the connection between application and IAS
5. Compulsory or voluntary items in the co-operation with the SCC
6. Who owns the data, and who may use the data in relation to *e*-services?
7. Requirements for authentication
8. Certificates and business rules
9. Responsibility in relation to AP

Table 6: Service provider issues

1. Who 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. Service providers not using IAS may also be permitted to participate.

[8] Key generation in an off-card secure environment may be preferred, followed by secure key distribution. Whichever method is used, key generation must take place in a secure and controlled environment to minimise threats to security.

[9] Support for qualified certificates may be included in a second IAS application on the card, and, where the card is issued by a central administration, management of qualified certificates (including certificate issuing) may be separated from the card issuer.

In the case of public IAS, the participation could be restricted to *e*-government services. However, it is expected that at least related professional services will participate (e.g. legal, accounting, tax consultants, property transfer).

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 the connection function from his *e*-service application to the IAS service. In this connection the SP has to define the business rules that are applicable for his *e*-service (as mentioned earlier, the application of the three layers: securing the building blocks and the identification of the card, authentication of the user, and/or electronic signature)
- Developing, testing and accepting the (optional on-card) applications to connect the *e*-service to the smart card and the generic IAS of the user
- The optional on-card application can contain business rules to access the *e*-service application or be a complete off-line application
- Compliance with security policies and processes.

3. Legal arrangements/bylaws protecting the card holder (user)

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

The SP has to publish and apply a general registration procedure for users wanting to enter/use the *e*-service concerned. It depends also on the business rules how complex 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 prove compliance.

The SP may insist on performance guarantees by the CI, such as uptime and MTBF.

5. Compulsory or voluntary items in the co-operation with the SCC

In the GIF the compulsory elements are:

- Compliance with the basic processes and roles
- Compliance with the IOP- and PKI-adapter interface specifications, which implies application of and compliance with the IAS function and its functional interfaces (human interface, connectivity, PKI and *e*-service application connection)
- Application of the mandatory common data
- Respecting the (technical) standards for the building blocks (hard-/middle-/software) to ensure interoperability
- Compliance with SCC security policies and processes

In the case of public *e*-ID 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?

For information about the ownership of the card and the IAS-related data, see clause 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 on the card as far as the cardholder has given permission for 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, and the business rules for his own application.

7. Requirements for authentication

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. Certificates and business rules

Topics here are:

- Where do the certificates reside to be checked by the SP?,
- Where are the business rules residing? and
- How to map between two smart card communities?

The basic situation is as follows:

- Certificates of the card holder are held on the card; certificates of other entities are held in those entities (which must be identified and addressable on the network)
- The SP has to put the connection mechanism in a building block (covering the application box function) which is secured by the CI and/or certified. In addition the SP can encode business rules for the application, or the complete application, on the smart card, within an on-card application
- The certificates of a user (card holder) are always handled (issued/verified/revoked) by the CSP/CA of the user

The mapping is realised by the interoperability scenarios as presented in chapter 4.

9. Responsibilities in relation to 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 The service provider ensuring trust within its *e*-service community

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

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

•	SP Trust issues and requirements
	1. Trust requirements for registration of SP 2. Trust requirements for building blocks, especially the on-card application and/or the application module containing the business rules 3. Trust requirements for card holder authentication 4. Trust requirements for signing

Table 7: Service Provider trust-issues

1. Trust requirements for registration of SP

After demonstrating its compliance with SCC specifications, the SP has to be registered for ID and certificates with the CI, or at a SCC Administrator and CSP 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 acting as SCC Administrator the building block (or application 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 card holder authentication

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

- Mandatory: PIN or (layered) biometrics (if possible with sensing on card, and certainly with template and matching on card; if (as is normal today) sensing is not on the card, sensing and subsequent transfer to the card must be secure),
- 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
- The same for secure viewing of the OTBS (including ensuring that all of the information in the OTBS may be viewed)[10]
- Appropriate content and application of the certificates (including providing for attributes to be used with certificates in compliance with the E-sign advanced electronic signature provisions in article 5.1)
- Security mechanisms belonging to qualified signature standards

[10] In this context, application programs such as MS Word are not acceptable for high level secure *e*-signature, as they typically produce files which contain a great deal of text and related information that is not viewable.

3.3.5 The card holder in the SCC and *e*-service communities

The following table lists the general issues that lead to requirements for the cardholder. The requirements are described below. Issues related to trust are listed separately.

• Issues concerning the card holder (CH)	
	1. Participate in the smart card community (SCC) 2. Responsibilities towards the CI 3. Legal arrangements/problems/complaints 4. Registration of access to *e*-services 5. Requirements for the human interface 6. The responsibility of APs towards cardholders as member of the *e*-community

Table 8: Card holder issues

1. Participate in the smart card community (SCC)

To participate in a smart card community a user has to apply for a smart card. He or she has to go through a card registration process, is then issued with a smart card, and becomes a card holder.

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

2. Responsibilities towards the CI

The card holder has to provide all data required by the CI.

The card holder has to collect and accept the card (in direct contact with the CI's representative).

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

The card holder is responsible for offering his/her ID data to *e*-services.

The card holder has to notify the CI of loss, theft and damage of the card.

The card holder may be required to pay a fee for the card (which may be a returnable deposit)

3. Legal arrangements/problems/complaints

The card holder has to familiarise himself/herself with the rules and regulations regarding the use of his personal ID data.

The use of the data must be restricted to the situations and tasks for which they are requested. In particular, the card holder must not allow any other person to use the card (and therefore must not disclose the PIN). The cardholder must inform himself/herself about the range of services as published by the card issuer and the *e*-services for which the cardholder registers himself/herself.

Problems and complaints must be channelled via the CI, who is required to provide a single point of contact for all problems with the card and has contracts with each stakeholder. In this way the CI ensures the card holder right of protection against misuse. (See also clause 3.2.1 item 15.)

4. Registration of access to *e*-services

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

The card holder 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 card holder 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 provide 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 onto the card (downloading of an application or applet).

5. Requirements for the human interface

The human interface to *e*-service providers must include a clear method for the expression of the card holder's will concerning the application of IAS, in relation to the *e*-service.

The CH may expect:

- secure access,
- that, 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 card holder is that he/she takes responsibility for everything authenticated and signed with the card.

6. The responsibility of access providers to card holders

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.

If the card holder decides to offer his/her card to a not-on-us infrastructure, a part of the operation is carried out at the location where the card holder had offered his/her card.
The initial acceptance/rejection is done in that infrastructure, based on local interaction. In this situation, 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 card holders to:

- Avoid destroying the card or the card content
- Avoid defacing the information printed on the card
- Avoid disclosure of IAS data
- Avoid unauthorised usage of the IAS data

It is accepted that the card holder's contribution to the trust system is mainly passive: Good co-operation is expected in deploying the procedures, and taking good care of CH responsibilities.

• Card holder trust issues and requirements	
	1. Trust requirements for registration of the CH 2. On-card application downloading 3. Secure environment and free decision about ID giving 4. Binding mechanisms

Table 9: Card holder trust issues

1. Trust requirements for registration of the CH

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

Note that the framework does not fully model the use of qualified certificates or attribute certificates, but within the EC the card and IAS service is expected to comply with the advanced electronic signature provision of E-sign. Registration, storage and use of the additional IDs and certificates associated with these enhanced uses of IAS is expected to be similar to that for the mandatory single ID, but other stakeholders may be involved, and an additional application may be required on the card.

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 any necessary maintenance or upgrading of already loaded applications. The CH must read and follow carefully all instructions and bylaws of the *e*-service provider before post-issuance download of an application to 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 CH 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 CH is fully responsible for the choices that he/she makes in supplying IAS information to the *e*-service provider (plain ID data or authentication). The same goes for the CH's expression of his/her consent over an OTBS.

4. Binding mechanisms

The CH must be aware of the binding between CH and the smart 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 service 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 CI 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 prove 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 service provider: basis for action and limits

The CSP (e.g. CA) makes a contract with the CI.

The CSP has to guarantee the quality of the systems and the checks that he executes (including RA and VA functions).

The limits of liability of the CSP must be clearly defined.

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

The SCC Administrator has 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 on behalf of the CI.

4. Content provider: basis for action ant limits.

The content provider is contracted by the *e*-service provider, and has no direct relationship with the SCC.

3.3.8 Other stakeholder contributing to ensuring trust

•	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 interoperable IAS job done”.

4.1 Requirement for an interoperable IAS implementation strategy

4.1.1 *e*-Services in the centre

When considering these implementation requirements, it must be stated that interoperability and generic IAS are not goals in themselves. They are 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 makes a lot of sense to put the *e*-services in the centre of the implementation strategy.

The effective starting point for the implementation should be the concept of *e*-services. 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 any other smart card concept, but from secure *e*-services using the capabilities of the smart card as an 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 scheme 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 a card issuer having a direct business relationship with the cardholder, but this relationship is always related to the offered *e*-service(s).

4.1.2 Which types of IAS services are desired

As well as government to citizen and related business to citizen services, an interoperable IAS implementation strategy should support:

- 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
- Business to business services

4.1.3 Who is concerned by the interoperable IAS implementation strategy

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

Each of these stakeholders will then have to identify their own business case for deciding when and how to join an interoperable IAS scheme. 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), costs, and the budgets available.

It must be studied and decided if revenue will be realised:

- In amounts of money per period (i.e. subscriptions)
- Tariffs by graded blocks using agreed parameters
- Statistical measurements (from samples of activity)
- By sessions

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

4.2 The Requirements for interoperable IAS technical infrastructure

The main implementation requirements for IAS interoperability are to:

- agree on mutual trust (based on secure processes), and
- implement strict procedures (which, for the purposes of this model, are assumed to be based on PKI technologies).

There are three specific implementation topics related to interoperable IAS. They cover:

- Technical infrastructure for interoperable operations, i.e. implementing the IOP- and PKI-adapter concepts, and publishing within an SCC any limitations in function and trust for interoperability with other co-operating schemes
- Requirements for testing interoperability
  - To accept new *e*-services in the schemes (including post issuance update of smart cards), because of the expected dynamics of *e*-service participation in smart card communities (introducing and withdrawing services), and
  - To open (and then maintain) new connections to other smart card communities.
- Distribution of security keys, for securing the communication channel and ensuring integrity and privacy, across scheme boundaries and selection of the correct key to use – this topic is not discussed in this framework, but is to be addressed later

It must be understood that the implementation model in this clause applies to the situation where the PKIs of the two communicating SCCs are not directly connected. Therefore requests to the not-on-us PKI are directed through the IOP-adapter, which in turn delegates to the PKI-adapter for routing through the not-on-us infrastructure to the not-on-us PKI. (Where the PKIs are directly connected, the on-us PKI will be called to verify a certificate.)

4.2.1 IOP-adapter and PKI-adapter

The core function of the adapters or gateways in this framework is to connect smart card communities for IAS purposes. The IOP-adapter also supports other communication between SCCs and between an SCC and not-on-us *e*-services.

Data and service requests flow through the adapters, which convert between the formats and protocols of the communities. Associated with the adapter concept is a mapping between the policies and processes of the SCCs, which must be taken into account in trust decisions where not-on-us processing is used. This mapping defines

restrictions in functionality and trust for the conversions carried out by the adapters, and must be available at all times to the *e*-services.

It is important to understand that the adapter or gateway concept is a logical one, and conversion related to different layers of the conceptual model (GIF part 1) may be realised at different nodes in the interconnected networks. However, in the functional box representation, it is necessary to group the adapter functions together – this is because, for security purposes, adapter or gateway implementation for IAS must be managed at the SCC level. That provision of adapter functions at the SCC level also aligns with the framework policy of providing generic services at the SCC scheme level.

These adapters are interfacing:

- Between SCC scheme infrastructures for handling IAS (in the terminals, or via the terminals in the network server and or a front office of the access provider)
- Between 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, once the card holders have been allowed to start an IAS session

These adapters are therefore modelled at the infrastructure level, including all functional boxes, acting as a link between the infrastructure layers of both smart card communities.

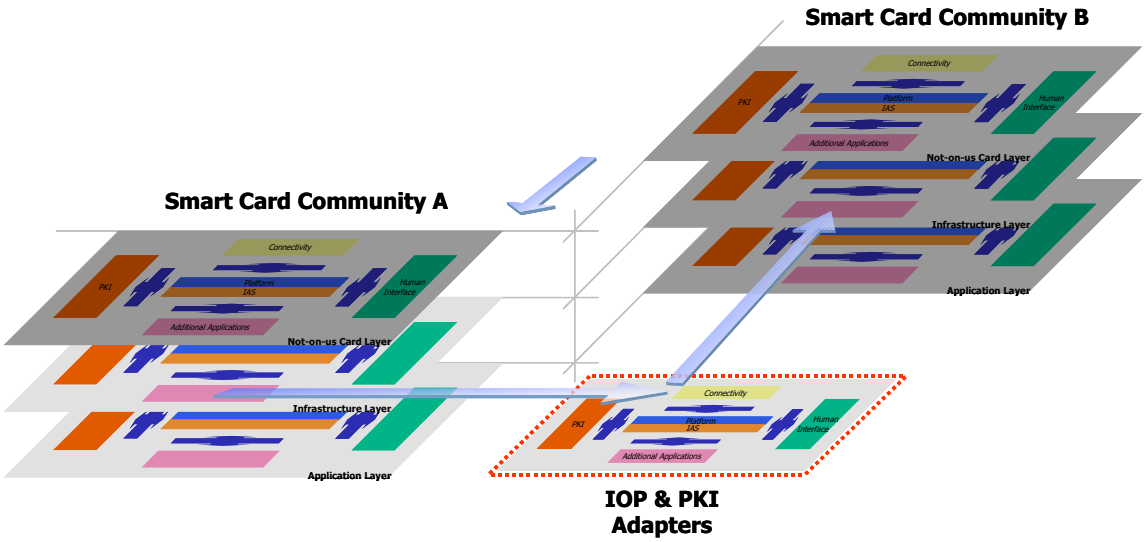

Figure 4: Modelling the IOP Adapters (here in scenario 1)

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 interoperability conversions in both directions.

Outgoing and incoming accesses include IAS requests and responses.

Service provider business rules and IAS interoperability

While each service provider may use the offered technical capability for interoperable IAS services, this is always under the overall control of the service provider's 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. However, an SP's business rules are strongly dependant upon the specifications agreed between the SP and the SCC in which it deploys its services.

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

The IOP- and PKI-adapters

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

- Make connections to services in other smart card communities
- 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 standards for technical components.

From the implementation strategy point of view, there are different ways to organise the implementation of the IOP-adapters. One of the key questions whose answer has many consequences for the types of technical solutions to be implemented, is:

- 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:
  - At the level of an industry branch (health, *e*-government, transport, banking)
  - 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?

1. The technical IOP-adapter

- In order to secure entities across the boundary between two SCCs, entity authentication requests and responses pass through the IOP-adapter.
- When a card holder requests a not-on-us *e*-service (possibly using eURI to locate the list of services available in the not-on-us SCC), the IOP-adapter acts as a gateway to the not-on-us SCC, providing format and protocol conversions if required.
- When the business rules of the *e*-service require certificate verification, then the connection to the PKI-adapter will be initiated (see below, at PKI-adapter).
- The IAS session has to be executed, with transfer of data that are exchanged according to the agreed interoperability specification.

2. The PKI adapter:

- Addresses the request for not-on-us certificate check
- Establishes the secure connection to the requested not-on-us PKI-directory or CRL
- Validates the requested PKI-directory or CRL
- Allows/Refuses continuation of the *e*-service session
- Terminates and logs (administrative) data.

4.2.2 IOP conformance testing

An interoperability conformance testing facility must be used for accepting and certifying the components of the interoperability infrastructure.

No further details on requirements will be provided here as they are out of the scope of the GIF.

4.3 Requirement for implementing IAS/IOP processes

Depending on the agreed interoperability 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:
  - 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)
  - 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.

It must be noted here that arrangements for security key distribution between SCCs are not finalised in this framework. Such arrangements will affect the processes described in the Table below.

However, the processes set out in this Table are based on the assumption that, for not-on-us cards used in the on-us environment, authentication of the card (and, if necessary as a separate function, authentication of the IAS application - i.e. the card holder - on the card) would be carried out:

- By verification of certificates read from the card (thus classic mutual authentication of card and terminal is not used – this is because the terminal function used is on-us, and therefore does not have access to any secrets (e.g. symmetric crypto keys) for not-on-us cards);
- Where identification information is to be secured (made secret) during transmission from the card, by the IAS application encrypting that information using a public key supplied by the terminal function.

	IOP Scenario #1 (not-on-us card and on-us *e*-service)	**IOP Scenario # 2 (not-on-us card and not-on-us *e*-service)**	**IOP Scenario #3 (on-us card and not-on-us *e*-service)**
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 of, and recognise, *the not-on-us card*	Activate identification of, and recognise, *the not-on-us card*	Activate identification of and recognise, the on-us card
3	Activate call for on-us application access and determine the IAS functions required IF AUTH/E-SIGN IS REQUIRED: ACTIVATE A CALL FOR ACCESS TO THE not-on-us ***PKI***	*Activate call for not-on-us application access* IN THE not-on-us SERVICE ENVIRONMENT[11] and determine the IAS functions required IF AUTH/E-SIGN IS REQUIRED: ACTIVATE A CALL FOR ACCESS TO THE not-on-us ***PKI***	*Activate call for not-on-us application access* IN THE not-on-us SERVICE ENVIRONMENT and determine the IAS functions required IF AUTH/E-SIGN IS REQUIRED: ACTIVATE A CALL FOR ACCESS FROM THE not-on-us ***PKI***

[11] The *e*-service may not be available to the card holder if the e-service is not registered with the SCC in which the card is registered

	IOP Scenario #1 (not-on-us card and on-us *e*-service)	IOP Scenario # 2 (not-on-us card and not-on-us *e*-service)	IOP Scenario #3 (on-us card and not-on-us *e*-service)
	ENVIRONMENT where card is registered	ENVIRONMENT where card is registered	ENVIRONMENT where card is registered
4	Make secure connection for the not-on-us card in the on-us infrastructure and transfer the ID data	Make secure connection for the not-on-us card in the not-on-us infrastructure and transfer the ID data	Make secure connection for the on-us card in the not-on-us infrastructure and transfer the ID data
5	Authenticate Card holder via the secure connection IN THE not-on-us ***PKI*** ENVIRONMENT (also uses secure local connection for PIN entry to on-card IAS application)	Authenticate Card holder via the secure connection IN THE not-on-us ***PKI*** ENVIRONMENT (also uses secure local connection for PIN entry to on-card IAS application)	Authenticate Card holder (if required) via the secure (local) connection (also uses - possibly different - secure local connection for PIN entry to on-card IAS application)
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 secure connection (if E-SIGN required) IN THE not-on-us ***PKI*** ENVIRONMENT	Use signature data via the secure connection (if E-SIGN required) IN THE not-on-us ***PKI*** ENVIRONMENT	Use signature data via the secure connection (if E-SIGN 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

Care must be taken during development of interoperability specifications to determine where terminal functions are to be implemented, particularly when the physical terminal infrastructure may include insecure components (e.g. a standard PC with keyboard, mouse and screen).

Note that where the card, infrastructure and *e*-service are registered with different SCCs and secure messaging is required, end-to-end secure methodology could be used at application level. This would allow for insecure networks (links and nodes) to be used. The suggested method between the IAS application and the e-service (or to a secure terminal function connected by a secured link to the e-service) is:

- The two entities to exchange public keys (contained in verifiable certificates) so that information can be encrypted using the public key of the recipient,
- For the sender to sign the information using its private key (and send with the information its public key contained in a verifiable certificate),
- For all the messages in a transaction sequence to carry sequence numbers so that the recipient can verify that all and only all messages from the sender are received, and
- For an acknowledgement and (if required) re-transmission protocol to be used.

5 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
- Theo van Sprundel theo.vansprundel@bull.nl
- Marc Lange marc.lange@build-in-europe.be
- Yvan Pirenne yvan.pirenne@build-in-europe.be

6 Overview of GIF Requirements (for purposes of RFI, RFP or "gap analysis" comparing to existing systems)

6.1 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

6.2 Operational and implementation requirements overview table

Subject	Specification	Description	Prerequisite for IAS or Required for IOP (= add on) *[p / r]*	Avail-able ? *[y / n]*
General				
Work/test-bench				
Processes				
Create / Register smart card community	• Register smart card community and external secure suppliers • Verify the compliance of SCC stakeholders with CI requirements and register them (establish ID + URL) • Provide PKI certificate to registered stakeholders as a technical proof of their registration • Verify the compliance of all secure "building blocks" (technical components), register them and provide the with PKI Certificate			
Card/cert. Issuing	• Personalise card • Issue card holder certificates • Initialise the card • Enrol the card • Maintain life cycles (card, holder ID, certificates)			
Post issuing application	• Test/Accept IAS connection software offered by the *e*-service provider • Test/Accept "on-card application" software offered by the *e*-service provider • Authorise download or download "on-card application" offered by the *e*-service provider			
IOP – Net-work	• Create IOP adapter, put rules and policies in • Maintain IOP adapters			
Community management	• Log the use of cards, IS and front office • Billing			
IAS process	• Connect smart card to (modules in) terminal and secure the links • Identify/validate and accept/reject the card in IS + identify/validate and accept/reject the terminal/terminal application (authenticate the 'building blocks') • Interact with the requested *e*-service and find the business rules for the requested *e*-service • Transfer ID data to the *e*-service • Authenticate card holder (if requested for *e*-service) • Execute *e*-service (IAS is passive) • Sign an information object (if requested for *e*-service) • Update administrative log-files and close the IAS session			

Subject	Specification	Description	Prerequisite for IAS or Required for IOP (= add on) *[p / r]*	Avail-able ? *[y / n]*
Functions				
IAS function.	• Connect smart card to (modules in) terminal and secure the links • Identify/validate and accept/reject the card in IS + identify/validate and accept/reject the terminal/terminal application (authenticate the 'building blocks') • Interact with the requested *e*-service and find the business rules for the requested *e*-service • Transfer ID data to the *e*-service • Authenticate card holder (if requested for *e*-service) • Execute *e*-service (IAS is passive) • Sign an information object (if requested for *e*-service) • Update administrative log-files and close the IAS session			
Human interface	• Language preference • Notification of process progress • Positive consent • Presentation of *e*-services • Individualised preferences • Security (remote display, keyboard, SAM)			
PKI	• Qualified certificates e sign directive art. 5.1 • Security EAL 4 + (augmented with VLA)			
Card connectivity	• Contact card interface:			
e-service connection	• Address to access • Business rules • Object to be signed • On-card application			
IOP adapters	• Technical adapter • PKI adapter			
Data				
Common data management	• IAS card holder data • Stakeholders data • Building blocks (certificates, addresses)			
Redundant data management				
Building blocks/modules				
Card	• ISO/IEC 7816 • Global platform / Java • Security concept • On-card application ability			
Readers + security modules	• Finread compliant			
Secure terminals	• Finread compliant			
Network modules				
Front office Server modules	• Access module			

Table 13: Operational and implementation requirements

Annex A Document 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
Peter Tomlinson	Edit and add new material 2003/1/13 redlined text	Internal to editing team	v.3.01
Chris Makemson	Consolidation of Peter's changes	Internal to editing team	v.3.02
Peter Tomlinson	Edit and add new material 2003/2/03 redlined text	Internal to editing team	v.3.04
Chris Makemson	Consolidation of Peter's changes	Internal to editing team	v.3.05,06
Peter Tomlinson	Consistency review, resolve editorial notes, incorporation of comments from Marc Lange and Théo van Sprundel	Internal to editing team	v. 3.07
Marc Lange	Final Review	Public	v.3.10

Table 14: Document History

Annex B References

B.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	Current and future business models for multi application systems Multi application systems architecture Integration of multi application systems	v. 2.1 v. 0.9 v. 2.0	November 2002
R3	NAME-ES	Network Authentication Module for internet End-userS	v. 02	21 June 2002
R4	NICSS	NICSS-Framework Scheme	v. 1.20	24.04.2001

Table 15: Background Document References

B.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	CWA 14174	-	July 2001
A3	CEN/ISSS	CWA 14172		
A4	ISO/IEC JTC1/SC17	ISO/IEC 7816		
A5	ISO/IEC JTC1/SC17	ISO/IEC 10373		
A6	ISO/IEC JTC1/SC17	ISO/IEC 14443		
A7		Global Platform		
A8	JavaCard Consortium	JavaCard 2.1		
A9	JavaCard Consortium	JavaCard Run Time Environment (JCRE)		

Table 16: Applicable Document References