Open Smart Card Infrastructure for Europe v2

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

Part 5: **Euclid and the e-Cities (Your e-key is OK, v1)**

Author: **Theo van Sprundel, eESC GIF Chairman**

Information Society

Your e-key is OK

Volume 1

euclid and the e-cities

By Théo van Sprundel

Your reliable key to e-services

Finnish Population Register Centre and in priority to the author.
Quotes from the GIF synopsis are only allowed with reference to the source.
Part one of this book
remains the intellectual property of the author; copyright Theo van Sprundel .

THE TEAM OF WRITERS HAS CONSISTED OF:

- Theo van Sprundel, the undersigned, is the author of the tale.
  He is co-author of GIF, for which his initial paper was the basis
  (SchlumbergerSema, Amsterdam).
- Marc Lange is co-author of GIF, and responsible for part 2 of this book,
  being the 'official' synopsis of the underlying GIF concepts.
  (Build-in-Europe SA, Brussels)
- Gwendolyn Ryan and Bébhinn Ryan elaborated the script of the
  conversations in the novel and edited the total novel text.
- Art Direction was assured by Advertising Systems SA/NV
  Brussels - for the EC - Euclid Project 2002-2003 .

Preface

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".
This book is a novel. It relates some weeks in the life of Mayor John. He is struggling to create an e-city program with "the reliable keys' for his citizens. He discovers and follows through on the realisation that for sustainable success the reliable key should be interoperable and self financing.

The discourse of mayors is chosen because the subject of this booklet is "strategy building for a card operator' The e-city is the metaphor for this scheme, and the mayor is the one who has to integrate the interests of e-service providers, with that of infrastructure and card base operators.

The book is based on the eESC GIF, "Global Interoperability Framework". The GIF documents are created under the responsibility of the e-Europe smart card charter. They are part of the 'common specifications' of the smart card charter, and are also being transferred to European standardisation bodies.

The situation and characters are completely fiction. Any resemblance with existing situations and persons is by coincidence. The characters represent the social types that pop up in all groups: the loyal and diligent one, the social and warm one, the cynical one, the expert, etc .The approach is inspired by Eli Goldratt's book "The goal". The central figure in this book, the virtual "Euclid", is inspired by Rupert Sheldrake, who has introduced the notion of 'morphic resonance'.

This book is the first of three. The first covers the strategy. The second will be positioned in the consultants' environment and cover the tactical and deployment questions. The third and last will be positioned in the media world and handles the discussions with consumers, and their experiences with the "reliable key". The three booklets are being published in co-ordination with the seminars of the "Porvoo eIDGroup", and with the conferences of the eEpoch IST project. The first concerns the national European electronic identity, the last a demonstrator project in 6 European countries where the electronic identity is combined with e-services. Each new book is therefore published on a cycle of 6 months.

This book consists of two parts:

1. *the novel*
2. *the 'official' synopsis of the GIF documents, in the order of the novel and a short list of references to important relevant Web-sites.*

The novel part of this book does not represent any official point of view from the eEurope Smart Card Charter, or any trailblazer, nor the Euclid-projects or GIF editing team, or any other body. The synopsis part of the book consists of extracts and quotes from "GIF". It is recommended that the complete text of the relevant parts 1-4 of GIF be consulted for full information.

DRAMATIS PERSONAE

John – Mayor of an e-City, central protagonist

Mildred - Mayor of neighbouring e-City, longstanding colleague of John

Ben - Mayor of another e-City, a Smart Card sceptic

Pete – John's consultant, chief advisor and golf partner

Brian – John's bright young nephew

Professor Rupert – custodian of the Euclid program

And, of course, Euclid…

PART ONE

EUCLID AND THE E-CITIES

THE NOVEL

BY
THEO VAN SPRUNDEL

04 december 2002
with contributions from
Gwendolyn Ryan and Bébhinn Ryan.

Contents

Chapter 1 The Rendezvous

John joins other e-City mayors at the seaside campus. With help from Euclid they discover the value-chain and learn how to add sustainable user value in their e-services.

John looked eagerly out of the window of the plane. Stretching before him was a beautiful sunny beach. To the right of the beach he could make out the tall weathered limestone buildings of the university. Since being elected Mayor of his e-City, he had been to many places on business. This was the first time, however, that he had reached a destination with no clear idea as to what would happen during his stay. Nevertheless, he did feel excited. He was finally going to meet the elusive Euclid.

It was this Euclid who had invited him to the two-day conference, where ten other mayors like himself would discuss 'a new era for e-Cities'. But, from what he knew about this Euclid figure it looked like it was going to be a conference with a difference. John was extremely curious.

“I wonder who he is?” mused John, aloud.

“Me too,” said Mildred, a colleague of John's from an e-City in a nearby state, “And I want to know who he is working for. Who is paying for all this?” She gestured with her hands at the business class cabin they were seated in.

“Yes,” agreed John, “nobody seems to know. I've asked around and I think I've heard more rumours than facts. All I know is that Euclid is somehow linked to a 'Virtual Reality' experiment being carried out by scientists in the university labs of this campus here,” he said, pointing to the college buildings on the horizon.

“Has anybody ever seen him?” pressed Mildred, “or is he just a mascot invented to provide good PR for some industry or service provider set to make millions out of the e-commerce revolution?”

John laughed quietly at Mildred's imagination, but she did have a point. Euclid had never appeared in public. “I suppose that is possible, but let’s hear what he has to say. If there is anything sinister about it, then we can question him face to face. You know, finally separate the man from the myth?”

“Anyway, how is your e-City project going, John?” Mildred asked, as they made their way across the hot tarmac to the terminal building.

"Well, as I mentioned to you on the phone the other day, in my city at this moment we have had many requests from e-service providers to participate in our e-City pilot. At the moment they can join the pilot for free. But in a year's time, they will have to pay for the Smart Card and identification services. I expect it's the same in your jurisdiction?"

"Very similar," Mildred agreed. "And, although most of them are prepared to put some money on the table, I know that the burden of responsibility will fall on me as mayor. This worries me. We can't keep going like this. There are other services we need to maintain, and we just can't keep on offering services at a loss."

"Yes, it is difficult" sympathised John. "There are some very popular services among them. Think what cancellation would do to our own popularity and prospects for re-election." John smiled wryly. " Maybe this conference will help. At least it gives us the opportunity to discuss with one another and the other invited mayors about the new problems and challenges that we all face."

"I guess so," agreed Mildred. "Otherwise, these e-services will have to go. We just can't afford them. The subsidy program from our government stops at the end of this year. And the city can't drop everything else for the sake of this project."

"Hmm" mused John, "Citizens will benefit from improved services, and I know from our focus groups that they are certainly prepared to pay something for this. You have hit the nail on the head. We need some new ways to tackle the problem of the city budget while still being able to offer these new services to all. Perhaps if we can isolate and pool the common elements we could then make it easier to introduce new services for which the users will be prepared to pay?"

"I know what you mean. Our smart projects must become less dependent on the city's coffers," said Mildred.

"Well, maybe we'll come up with something over the next couple of days," said John positively. "Maybe this Euclid will have the answer!"

Inside the airport

Inside the airport, John and Mildred made their way to the business lounge, where they were to meet the other delegates who had been invited by Euclid. John held open the door for Mildred and followed her inside. There were already quite a few of the delegates present, from Europe, both eastern and western, as well as Africa, the US and Japan. The flights from the Pacific rim, South America and

Australia had not yet landed so John took the opportunity to accept a cup of coffee and strike up a conversation with a nearby group. He was curious as to the implementation of their e-City Programmes.

“Take teleworking for example”, one of the mayors, an American, was saying. “Does it really help solve the traffic crisis? And even if it does, is there not a risk that management will lose its influence over these teleworkers, and that the workers themselves will lose out on the camaraderie that a 'real' office provides?”

John was interested, especially as many of the delegates in the room he had met only virtually up to this. There was a buzz of conversation, even a buzz of excitement, in the room. Another heated discussion was going on over by the window. A group of mayors were debating door-to-door public transport; “It sounds wonderful in theory, but is it really feasible?” That was Mildred, always asking the hard questions, smiled John. Similar conversations were happening all around - mayors from all around the globe chatted about Smart Cards for parking, libraries, and other public services, even electronic purses to eliminate the need to carry cash.

The last participants arrived, tired, but like John, looking forward to learning more from Euclid, and their fellow delegates, to improve life in their e-Cities.

The mayors streamed out into the midday sunshine, and climbed into the waiting limousines. After a short but comfortable ride, they turned in the gates of the university where the conference was being held. They pulled up in front of the main building. John looked around, taking in his surroundings. Inside the Quadrangle, in the shade of the elegant buildings, groups of students lounged on the grass, studying or chatting, some even tapping away on laptop computers.

Inside, the delegates were treated to a fine lunch in the boardroom, and welcomed by the Dean and a scientist called Professor Rupert. The Professor was a middle-aged man, friendly and enthusiastic. As the coffees were being served, he stood at the podium and addressed the group.

“Welcome! Thank you for giving your time and energy to find out more about our project. I'm sure you're all wondering what its all about, and how our work will affect this new era for e-Cities. Firstly, I would like to reassure you that this project is not tied to any specific industry. We have been funded by a scientific foundation, and thus are independent of commercial or political motivations.”

At this John sneaked a look at Mildred, and gave her a smile. She shrugged her shoulders, not yet fully convinced.

"What we have been working on", continued Professor Rupert, "is a project called the ‘Micro Resonance Presentation Program’, a new form of virtual intelligence. This is the result of ten years of cooperation between this university and centres of excellence across the world as far as India and Japan. My colleagues and I have managed to combine the best in Information Communication Technology with that of Behavioural Science. The result of our experiment is that we have created a virtual intelligence that can converse and interact with humans. The intelligence can communicate and respond to any person or group around the world, anyone involved in specific areas of problem solving. The Micro Resonance Presentation Program provides both theoretical insights and practical solutions.

“Over the next two days, we will apply this intelligence in individual situations, in an attempt to generate a framework which we can apply in our e-Cities. In the long term, in six months to be exact, we invite you to return, and report back on the implementation."

The Professor stopped speaking. After a moment, the audience spoke up. Everyone spoke at once. What are you talking about? Who or what is this intelligence? An oracle? A spirit? How does it get its information, and why should we believe this so called intelligence? Even John raised his eyebrows in confusion.

Professor Rupert smiled. “I understand your scepticism,” he said calmly. “But of course it is not a spirit, or an oracle. It is purely scientific. Unlike an oracle, this intelligence does not make vague, ambiguous statements that you interpret yourself. Everything it says is clear, fact-based and backed up by extensive research and evidence. We have documented results of experiments, verifying the intelligence of the program.”

“Why did you choose the subject of e-Cities?” asked Mildred.

“Good question”, said the Professor, nodding. “e-Cities are about to enter a new era. With the expansion in e-services, e-Cities like your own are looking for more generic solutions to the challenge of providing interactive screen-oriented services. This is a chance for you to meet together, and discuss your own current and future needs. With the aid of this intelligence, you can challenge traditional thinking and explore new methods of problem solving. The intelligence we have created is primarily a tool for problem solving, to generate questions, direct discussion, act as an intelligent sounding board. We can offer the opportunity for millions of people to enter, or more effectively explore, the world of e-services."

Mildred seemed satisfied with this answer and leaned back in her seat deep in thought. The Professor paused at the podium, ready for further questions.

'Does your intelligence have a name?' asked the American John had met earlier in the business lounge.

Rupert nodded quickly. “Yes, Bill. It does. You might have heard of it.” A murmur passed along the group. “The intelligence goes by the name of… Euclid.”

"Come with me" said the Professor, leading the way into a spacious, circular room. The lights had been dimmed, and the simple furniture - ten comfortable looking armchairs - had been arranged in a semi-circle around a large plasma screen. "All we need is beer and football", quipped one of the mayors, settling back into the cushions. Everybody laughed and made themselves comfortable. Some took out notepads, others powered up their laptops or positioned their Dictaphones. Professor Rupert stood in the centre of the room, before the still dark screen.

“Take your e-City project - now consider the goals and possible benefits of this project, and note any factors that enable or restrict the advance of the project.” He switched on the screen via his own computer.

Some of the mayors looked disappointed - "Just another talk, just another PowerPoint presentation." said one of them to John.

All of a sudden, the screen - in fact, the whole room - lit up. A soft voice filled the air. “I am Euclid" she said - for it was a she. Some of the mayors gasped. She was virtual all right, but virtually perfect!

Euclid smiled from the oversize screen, “Welcome, mayors of the e-Cities. I can share with you all the available knowledge for the identification of persons in any networked environment. I can talk with you. As long as I am on the screen, I hear the questions that you put forward. I cannot always go into details, but if you are open to my help, I can direct any work that you would like to explore.”

“But what type of knowledge do you represent? Is it information certain industries would like us to hear? Or do you represent this University? Or the government?’
The questions came from Ben, an experienced mayor known for his caution and scepticism.

Euclid replied, “I am not connected to any industry or industry branch like telecom or computers. I do not represent any single university. I am independent from any government or political movement. Once I am focussed on a particular area, I only share knowledge, insights and experiences which are applicable to that area.”

"But what about proprietary information, such as copyright and industry patents?" This was from the US city mayor.

"Each of you could benefit from existing knowledge which until now has been inaccessible to you. This still is far from violating any legal rights, patents or intellectual property."

The room had settled down, and the figure on screen took advantage of the calm to press forward. "Let's begin," she said.

"Let's start by establishing a sustainable generic basis for all e-services, that is, all services that can be delivered via screens. What services come to mind?"

"E-mail," suggested John.

"Video Clips, said a German mayor.

"Documents and Reports," said the Indian lady with the laptop.

The list appeared on the screen

- E-mail
- Video Clips
- Documents
- Reports
- Direct mail and Advertisements
- Conference announcements
- Telephone books services and other directories
- Product sheets
- Bookings and tickets
- Company profiles, including also promotions for shops and restaurants
- Economic information like stocks
- Electronic papers
- Cultural info and programs

"These are good examples of generally available services. Now think more about your own individual needs, whether personally or in a business context," Euclid prompted.

Ben was thoughtful. "I would like to be able to easily access a quick selection of news, based on a personal profile I can create. Also I'm interested in the dynamic provision of news services, for example when something happens in my city."

"Yes" said Mildred, "but I want to have access to all this information, not just at my desk, but wherever I go, whether I'm in my office or in my home. It needs to be mobile."

Now the suggestions came thick and fast. One mayor noted, "See what we have here. As we talk, our words come up on screen in written format. Can electronic services do that the other way round? For example, can my computer read texts to me while I'm in my car, on the move?"

The Indian mayor said, "I'm a busy woman. For me, it would be nice if I could handle my shopping and private bank account in the same way as I can ask my assistant to do it. Without going through all those screens and different password procedures for every service involved. But with the same level of security of course."

"I would like to see more graphics," said George, the Hong Kong mayor, "especially statistics on command. Immediate polls, analyses. I get way too much paperwork with too much 'prose'. I just like to see conclusions based on quantitative data. I like to access a wide range of sources to check information and conclusions."

"Well I think one of the big advantages of this technology is that it's not all about work," said the German mayor, Hans. "For me, I see it as an opportunity to watch some TV or a movie, in a corner of my screen, while working."

"Stop, stop," interjected Euclid, a smile on her attractive thirty-something features. "We could continue like this all day! It's enough for the moment to say that, in principle, all these technologies are either available or in development. Although, what we currently have is a series of non-connected e-services, each with different structures, different providers, and in the end, a lot of very confused users."

"Sometimes I think using e-services is like programming the video recorder," said Hans, "I figure out one model, and my wife goes and buys another, more complicated one!"

"Yes, you want a human interface; you want ease of access and use," agreed Euclid. "But the fact is, there is no comprehensive industry standard out there. As you say, it's not all about the availability of technology, it's about how we can easily and effectively use it."

"Sometimes, even when there is an electronic service available, I pick up the phone or go to the shop, because at least then there is person at the end of the line, or face to face, who can provide a service fitted to my individual needs," said Mildred.

"There are people out there, experts on every form of e-services", replied the American, "the problem is how to reach them."

"Well," said Euclid, "why not put more attention into communicating via webcams? And at the same time, we can focus on more appropriate standards in ICT." She carried on, "For example, whom would you contact "face to face" via a screen, a service you can use "any time any place"?"

As before, the mayors' suggestions appeared on the screen

- ***My assistant***
- ***My girl friend***
- ***My lawyer, who is also my consultant***
- ***My golf mates, not only for golf, but for some social talk***
- ***My travel agent***
- ***My section directors***
- ***My doctor and my diet consultant***
- ***My fitness trainer to assess my progress***

Mildred added, "For me it could be anyone; depending what activity I am involved in; it could be my garage, my estate agent, my financial advisor, my tax consultant."

Bill made another point. "These are all personal requirements and private networks. There are also some generic services that I sometimes want to consult interactively. I'd like to be able to access a 'virtual person', who will interact with me and gibe me information on the weather forecast, traffic information, stock exchange info, and so on."

"OK," said Euclid. "Next question. Does the technology used at present offer value to you as a consumer?"

"Yes," started one of the mayors, "to a certain extent."

"No" interrupted Ben. "Look at this list of services. It is obviously a minus if we cannot have real face-to-face contact. The challenge is to compensate for this by ease of access and the saving of time, energy and costs in physically getting to the other person."

"Of course, one advantage there, Ben," said John, "is that you can access multiple sources in a fraction of the time it would take to physically go and meet with even one of the services or people we have mentioned."

"Indeed," said Euclid. "Could it be that technology creates value for the user, insofar as it enables the user to more easily access services? How can we increase the user value of the technology?"

The mayors suggested two main ways this can be done.

- ***Increasing the user convenience in comparison to existing accepted technology***
- ***Lowering the costs of its use.***

"That sounds fine in theory, but how do we actually apply this in our e-Cities?" asked Mildred.

"Well, ladies and gentlemen, this bring us to the introduction of the Value Chain concept." The points came up on the screen as Euclid explained.

"The 'strategic fight' of any company should concentrate on

- ***Position against competition (ultimately to make competition moderate)***
- ***Good margins (cost leadership or leadership in value as perceived by the cus tomer)***
- ***Risks in 'mega" –forces: market entrance, technology substitution, shifts in the base of suppliers and/or customers."***

"A stable situation is reached when competition is moderate, margins are good and risks are controlled risks. Therefore, the company strategy should focus on expansion in the distribution channels. You can see this in all company strategies, and hear examples in all reports on company returns."

"Let's use a widely-accepted model here. Michael Porter's 'value chain' concept is very useful as a basis for modern business thinking. The concept moves business organisations on from an analysis of isolated specialised functions in a company, and focuses instead on the total process of value creation for the customer."

"The sources of value are:

- ***Reducing complexity on the production / supply side, for example creating eco nomies of scale. We call this cost leadership.***
- ***Innovation - to take advantage of the fact that the customer is prepared to pay a premium for a particular specialised or high quality product. This is often oriented to niche markets. This is what we call differentiation leadership.***
- ***Finally, some value, such as brand names, is created through the cultivation of a perception of value as seen by the customer."***

It was Hiro, the Japanese mayor, who raised his hand. He spoke for the first time that day. "Does the company attitude not differ widely, between, say, a 'price fight-er' and, for example, a specialised niche supplier? Or is it possible that these two attitudes can co-exist in one

Euclid smiled. “Very good,” she said. “In practice it does seem impossible to organise in one company both cost leadership for some parts, and leadership in obtaining the maximum user value through differentiation in other parts. This has consequences, which you will come across later on.

“But first let me give two typical examples, which should illustrate the ‘value chain’ concept:

Bringing the purchase prices down, say by higher volumes per order, could create extra value in a ‘supply chain’. When this action causes extra costs further on in the chain - higher stock keeping costs, more waste, or extra services - then the contribution to the total value is limited, or could even be negative. Bringing down the prices of the purchased goods is not enough; the total cost in the chain must be brought down. Information on the costs in the total chain must be shared, and used to measure the performance. And to give the right incentive to the purchaser. The production of goods could create extra value by anticipating service requirements that can be cashed later in the chain. For example, in modern cars, plugs for electronic diagnosis systems are built in; these higher costs in the production are more than compensated by lower maintenance costs later in the life cycle of the car. Information on the user benefits in the total chain must be shared, and used to assess the production costs.”

“I see” nodded Hiro. The others assented. It was starting to make sense.

Euclid continued: “The value chain is built up of ‘elements’. Each element is oriented to a phase in the real value creation or production process. Each element has a clear supply side (input) and a demand side (output). The value is always derived from its effectiveness on the demand side, applied to the whole chain. It is important that all elements in the chain maximise their contribution to the total value of the chain. Each element has to perform to the best benchmarks that are available. The consequence is that all activities that under-perform could be done better by other parties and should be ‘in-sourced.’

“Now, lets apply this value chain to our e-services. But before we can do that, we have to make some assumptions.

We assume that we use a token with a microprocessor chip to identify and authenticate its holder for access and for giving an electronic signature.

We also assume that, based on the rights that belong to the identity of the token, the user can ‘surf around’ in the infrastructure, and the connected services.

We assume that there is an operator that issues and manages a base of tokens

We assume that the consumer, being the Card Holder, can use his or her card, to access and identify for one or more services in the card base.”

"Yes, all these assumptions are correct. That's what underlies the whole idea behind e-Cities. Although, what you refer to as tokens are really our Smart Cards." Hans smiled broadly, as it all came together.

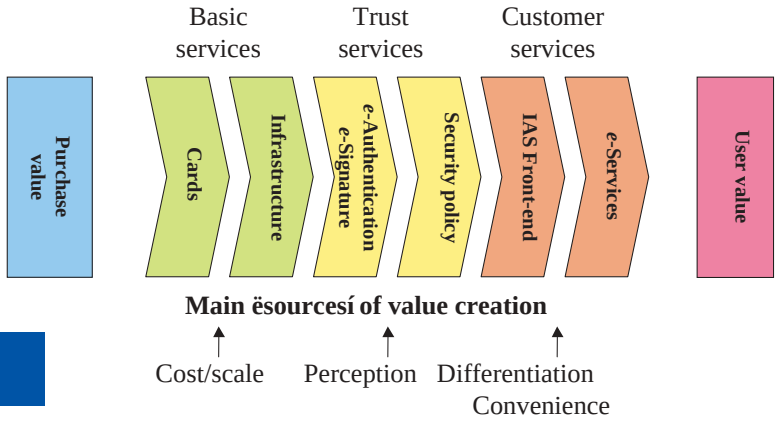
The other mayors agreed, relieved that the theory was now out of the way and they could get down to discussing the area of interest to themselves. They decided to refer to the tokens in Euclid's analysis as Smart Cards.

"So," said Mildred, "What does a value chain for a Smart Card scheme look like?"

Demonstrating that, as Professor Rupert had promised, she did indeed have a thorough grasp of the research, Euclid replied: "The British research company OVUM introduced a value chain for Smart Card centric services. Following this concept we divide the value creation process as follows:

1. Basic Smart Card services (Smart Cards, infrastructure)
2. Security services (strong authentication, qualified electronic signature)
3. Electronic services (generic e-services, individualised/ interactive services)

"Have a look at this diagram"



"For a deaper analysis of this point, see Part 2 Clause 2"

"Don't worry about taking it down. A copy is being e-mailed to each of you as we speak."

"The whole process of interaction is like a community, isn't it?" said John. "Yes," said Hiro, "any individual card scheme operated by a user, is a Smart Card Community." The others agreed, and decided to use the term in their discussion.

"Traditionally," continued Euclid, "the value chain in a Smart Card Community was limited to just two basic services, the Smart Cards and the infrastructure. The issuer did not offer the Card Holder any choice in the application of e-services. The Smart Card was restricted to those services chosen by the Card Issuer; this goes for:

- ***Dedicated payment schemes***
- ***Dedicated identification services (social security, health care)***
- ***Keeping track of individual / dynamic parameters (medical data, loyalty data, entitlements, including physical access).***

"The value creation chain was limited in chain elements, and mostly oriented to cost reduction in existing business processes (payments, entitlements, automatic settlement, etc.) Attempts to increase the value for this type of services by new or better services do not seem to pay off. Creating more value in the chain is oriented to lowering the cost of the smartcard and the infrastructure, by standardising and enlarging the scales.

"In the context of IAS/IOP this means making the first elements of the chain more open, and adding more value by making the value chain longer. And more sharing of the first elements through the introduction of different services.

"This is my first point," said Euclid. "Now, a second area of interest is Secure Services. Secure services are more or less card-independent services to ensure trust. How so?

- ***Generic identification and authentication of users***
- ***Electronic signature.***

There are standard or commercial services available for these types of services, directed to special groups. With the offered products and services, virtual organisations are created, such as:

- ***e-Market networks (purchasing, b-t-b ordering, etc.)***
- ***Closed subscriber groups***
- ***Secure internal company (tele-) networks***
- ***Secure e-mailing etc.***

These services are offered by commercial companies to environments with high interests and high risks. The prices for the 'trust' products are high. Mobile telecom is one segment where interoperable Identification services are applied on a large scale through the SIM card, but without strong authentication or qualified signatures. In all other segments of low priced security products (via the internet), both the offer and the acceptance of trust services seem to be fragmented.

To build more added value there is a need to disconnect the basic services from the trust services, and base the interface on open standards, or establish an industry standard."

The mayors were all in agreement.

"Thirdly", she continued, "Electronic services include payments, ticketing, loyalty, gaming, gambling, entitlements (insurance etc.), forms, etc. Currently, the

value creation process of e-services is mainly deployed by Card Issuers, and mostly with only one, often issuer oriented, service. In the context of IAS / IOP, the e-service should be disconnected from the Smart Card base with its infrastructure, and from the so-called trust services. These services should be open, and connected via an interface to the e-services. This connection will also make cost sharing among e-services possible. From the IAS point of view, there are no requirements for the application of standards in the e-Services. But when the total chain is using internet-oriented tools, it creates more opportunities to create value."

"The following table summarises these points," she finished.

Value chain for card based IAS /IOP services

Type of service	Service chain	Main basis of value
Basic services	Smart cards	Cost reduction
	Infrastructure	Cost reduction
Trust services	Strong authentication	Perceived trust
	Qualified signature	Perceived trust
e-services	High level services	Service value for customer
	Interactive expert services	Service value for customer
Total	User value	Summarised service value

"Well, we can see from this diagram," commented Mildred, "that without customer-oriented e-services, Smart Card centric services show relatively low customer value."

Euclid replied, "Well, you can state the same thing more positively. Relatively, the most substantial user value is created by the e-services. For these parties bringing the e-services all strategies are open:

- ***Large scale / cheap services, competing on cost leadership***
- ***Small scale / dedicated services, competing on differentiation leadership***
- ***Brand / image oriented services, competing on perception"***

"Also," said Hans, "Parties involved in card issuing and card access provision are probably not the best placed to maximise the user value through services. Their contribution in optimising the value creation is oriented to the cost reduction strategy."

Euclid called for some possible suggestions. The mayors suggested:

- ***Improvement in Quality / Cost ratios in large scale service provision***
- ***Cost sharing among different elements in a value chain***

"One concern I have," said Bill, "is that for the acceptance of high level services in a networked environment, the perception of 'trust' by the customers is essential."

John suggested a possible solution, "Quality and independence from commercial interests for this part of the chain could be the key. The applied technology

must be perceived as superior, and / or generally accepted."

"And," said Bill, "Don't forget. In order to get the maximum value across the total chain, every element must be maximised in its value creation capability. Assuming that there is a stakeholder responsible for every element in the total chain, it is the responsibility of every stakeholder to create a value chain for his own part in the value chain, if you get my drift."

"There are several conditions that parties have to fulfil," said Euclid, "to organise themselves in a value chain for Smart Card centric e-services. What do you think they are? Suggestions came from the floor, and appeared on the screen along with the other data.

- ***Technical (standards, interfaces, handling common data flows)***
- ***Business (cost sharing, branding, business growing strategy)***
- ***Organisational (legal entities, responsibilities, common systems) with last but not least accepted common performance indicators."***

"Of course, when it comes down to it," said John, "the value of every element in chain is calculated by its cost price and its benefit as well. In the total chain, both the cost of the inputs and the revenue from the users side, as well as the total margin, has to be assessed."

"Very well," Euclid concluded, "with this you have the basis to create a sustainable e-services system to complement your e-City policy, although there is much more to be explored."

"So, what's next?" asked Bill.

"Tomorrow you will participate in an excursion, a situation with the right conditions to help you formulate a model of roles within this system. You are free to include your own ideas as you see fit. The only requirement is that this model is in line with the value chain we have discussed today."

"But -," said Mildred, only to be silenced by Euclid. The virtual chairwoman said, firmly, "When you are back in your city, after this conference is over, you can contact me. Professor Rupert will tell you how. Good Luck."
And all of the sudden the screen went black. Euclid was gone.

The mayors were flabbergasted. They had so many questions! "Where is she gone?" exclaimed Ben.

Even Professor Rupert seemed surprised. He smiled at the group. "At least we have all the data here. Let's take a short break and meet up again at dinner. That will give us a chance to evaluate what we have heard, and come to our own conclusions.

"Dinner," he continued, "will be held in the Dunes, which you should find an interesting restaurant. Uniquely, this restaurant is located half on land and half on sea." He smiled enigmatically. "Between the worlds of sea and land, seems a good position for us."

The view from the Restaurant was amazing. There were large French doors on either side of the main area: one set of doors led to a spectacular view of the ocean, and the other overlooked the university campus, limestone buildings glowing white in the dusk. The mayors walked leisurely around the room, pausing on the balconies to admire the sunset. John took his place at the dinner table. Mildred was already seated, deep in discussion with Ben about the day's events.

"I really don't see how this value chain can help us." Ben was saying.

Mildred shook her head. "What I've taken from it", she replied thoughtfully "is that the goals and functions of the issuer are not the only criteria and in fact may not amount to much overall when considering the expectations of other stakeholders. For example when a Bank Card scheme is used the only one who is making a commission profit here in a point of sale system is the bank itself. Although it is the cashier and consumer that complete the sale the cost is entirely borne by the store and ultimately by the consumer. For me the value chain poses important questions such as *"What's in it for me? Or for the store?"* It is not sufficient that the bank takes all of the credit. After all the money stays electronic instead of cash. The Banks eliminate the need and expense for physical cash handling at the same time as holding on to the hard currency".

"I don't think you're being fair on the banks," Ben said, "They can offer credit facilities, which can be a real benefit to users. Plus, you get the convenience of always having money in your pocket, without the risks of carrying actual cash around."

"Yes but that card cost me a lot of money," answered Mildred, "Money I am only willing to pay if it ensures the type of services that we discussed this afternoon."

"What?" exclaimed Ben. "Would you really be willing to exchange your gold card for a measly blue one, just to save on banking charges?"

The other mayors at the table laughed.

"OK," said John, "you can discuss how much the payment services are worth to you. But the fact is that it is very difficult to create a business case for services where the issuer is not prepared-"

"Or even able to" George interrupted

"Exactly," agreed John "It is very difficult to create a business case for services where the issuer is not prepared - or able to - invest in the card base and infrastructure. We all have a card base in our e-Cities. We are all trying to avoid creating a 'stove pipe' of these services. Without a doubt, we have to disconnect the elements of the chain. This will create openness for basic services and the so-called 'trust elements' of all content-oriented services."

"Well, openness is one thing," said Mildred, "but you also need cost sharing over the total chain. Then you can bring down the cost of the card. By increasing the frequency of use."

The mayors at the table grew silent after this statement. Thinking it over, John added:
"And you need to solve a lot of problems in standard interfacing"

"And security", added Bill.

"And privacy", said Ben

"And legislation", said George.

The mayors looked at each other. They all seemed to be agreed on this one point. A waiter appeared with the wine, and filled their glasses. The appetisers were served. Rupert stood at the head of the table. "Let's have a toast!" he said as he lifted his glass. In Euclid's absence he stepped into the shoes of host. The mayors raised their glasses. "To Euclid!" cheered Rupert.

"To Euclid!" echoed the mayors as they settled down to the feast.

At the end of the table, John continued their earlier conversation. "The main lesson for me was that the chain leads to a split in business activities that are oriented to the service providers. This is a kind of business-to-business approach, comparable to a wholesaler. And the second activity is business-to-consumer, mainly done by service providers. This is comparable then to the retailers. They have to get the consumers in their shop. It is a two-part approach. The first part is to bring the produce to the shopkeepers, and the second is to sell it to the consumer."

"But John, when you look to the banks, they cover the whole column. Are not they successful?" asked Ben.

"Generally they are," John replied. "But the banks are an exceptional case: They are in such a strong position with payments that they can strongly push the use of cards and terminals, and the infrastructure is already there. They have the financial power to implement a card scheme, even a proprietary one. And many of them have invested in one. They can afford to host or not to host any other service on their cards.

"I am convinced that the user is willing to do much more with such a card than just some bank related financial services. But the banks are not in the position to easily develop this capability. Because of their branding, their proprietary systems, their system of issuing, their privacy. My conclusion is that you can only maximise the chain when you disconnect the responsibilities, and only make technical and financial integration arrangements. This is exactly what Euclid has said."

"I agree with you." It was Mayor Bill. " Do we look to our governments? Do they put the money on the table to provide Smart Cards for every citizen? No. They want the citizen to pay for it. The same goes for the terminals and infrastructure. They want the companies and card accepting bodies to pay for it. We only get subsidies for experiments and pilot programs. Which is good, but it's no structural solution. So what do we do?"

Mildred made some suggestions. "There are two options in my opinion:

- ***Either the government uses its position to self-finance the card base and the infra structure. I read that one of the Baltic States has made an identification Smart Card obligatory as a travel document. Or in France, as I've heard, they have made legislation making health cards compulsory for all insurance companies.***
- ***Or, alternatively, you make one card for the use of every civil service. You let the service providers pay for the use of the card. When the card is used for three or five frequently used services, the providers will break even."***

The mayors nodded. "It probably wouldn't work with one option alone. I would say you have to provide both," said George. "You have to respect the different positions and responsibilities. It is not easy to organise."

John nodded in agreement. "By the way," he asked, "do we need the same type of card, and the same identification, and verification of the link between card and the cardholder for all services? For some services you need a simple exchange of card numbers. The back office systems do the rest and there is no need for time consuming checks. And for other services checking is very critical. This means that not only do we have to integrate the card to different services but at the same time we need to create an interface that can differentiate."

"Come on now, my friends," said Hiro, "let's not make things too complicated. Of course we can solve this. But we have to do this step by step. And Euclid has asked us to concentrate first on making a model for all stakeholders involved in the value chain."

They agreed, and decided to move off the subject. Only Ben remarked: " I am not sure if I really want to return to my city with this Euclid story. Its integration will just cause so many complications. What's wrong with one card for the bus, one card for parking lot payments, one card for my city hall staff, and so on. …"

“Let us see how far we get tomorrow!” said George. “Now, where’s dessert?”

After dinner, John sat on the veranda of his hotel room, enjoying the sea air, and thinking about the value chain. He made a few notes about the topic, while the afternoons and evening’s discussions were fresh in his mind, knowing that it would help him to focus when he came back to the question in the morning.

He wrote, “The value chain concept should help to define the most strategic decisions for a e-City (or any card operator). In a mission document, this will have to cover:

- The e-City (or any other Smart Card community)
  - What type of problem / solution is addressed / basic quantities
  - Legal entity / Ownership relations
  - Mission towards e-services to be offered
  - Mission towards cardholders / branding
- Products and services: requirements / basic choices / basic quantities
  - Basic offer: cards and infrastructure
  - Trust offer: card management, PKI, e-sign
  - E-Services offer
- Marketing
  - E-services segments to be addresses
  - Product (services) / segment matrix
  - Positioning
  - Quantities
  - Pricing strategy
- Creating the technical environment: buying/ building / altering/ adapting
  - Cards
  - Infrastructure: card readers / terminals, network services /
  - Front office for card issuing / card management / RA / development and compliance testing
- Development strategies and strategic tools
  - Towards user groups: Action research yes / no
  - Towards e-service suppliers: smart factory yes / no
  - Towards technical suppliers: accelerated development
- Global financial plan
- Organisation plan
- Action plan”

John was not the only person still awake. In his lab across campus, Professor Rupert was also reviewing the day’s achievements. He looked over tomorrow’s itinerary.

Chapter 2 The Cave

John and his new colleagues explore a cave and discuss in old Greek style, how to maximise the value creation process. They identify the roles involved in value creation and realise the importance of avoiding the stove pipe role model.

The next morning, after a pleasant buffet breakfast, John made his way to the conference room. Many of the mayors were already present. They sat in the comfortable semi-circle of armchairs, waiting for Euclid to appear on screen. There was an air of expectation around the room.

'Morning, John!" called Bill, "How are you? Are you ready to meet the most beautiful woman in town?"

John laughed along with Bill. He was looking forward to meeting Euclid again too. Most of the mayors seemed to have already accepted her leadership. They all looked up as Professor Rupert entered the room.

"Good morning!" he addressed the group. "Thank you for assembling so promptly. I have to disappoint you, however. We will have to work independently of Euclid today. Keep her in your mind, though, during our excursion.

"Excursion?" asked Ben, startled.

"We will visit an ancient village, carved into the rock. We can only reach it through a cave. The only way through the cave is on foot. It is a famous and splendid walk. I know you will enjoy it."

"I didn't bring my hiking gear!" The Indian lady looked worried.

"You do not need any special clothing or equipment. There should be no major difficulties. The weather forecast is good. You will have plenty of time to rest, chat or simply to look around. Each of you will be given a pack with food and drink.

"We will divide into two groups. Each group we have maps and other documentation, a first aid kit and a mobile phone. Limousines will bring you to the cavern, but you will have to walk from there. We will all meet up again in the village. We shall leave in half an hour. Any questions so far?"

"Why do we have two groups?" asked Ben, who was also wondering why they were going on a nature walk in the first place but who thought it more polite not to ask.

"It's really just to make our area of study more group friendly," answered Rupert. "I'm asking each group to cover a different part of the value chain. What I'm hoping is that within your group you will discuss the roles of stakeholders involved in the value chain. The question you should be addressing is: What stakeholders do you need? And how do you describe their roles?

"One group will start from the left side of the chain, and the other from the right hand side. That means that one group will concentrate on the stakeholders involved in cards, infrastructure, identification management, services for authentication and for electronic signature. The other will concentrate first on e-services, and the roles of all other stakeholders touched by the e-services. Keep in mind yesterday's discussion: the card operator need not be, or probably is not, the same as the service provider."

Rupert looked around. Greeted with silence, he took that to mean they all understood. "Right," he said, "Let's divide in half…"

John joined group one, which was to focus on the Smart Card community from the Card Issuer's viewpoint.

"Do we need a name?" asked Bill.

"Why not?" said John. Together, the group choose the name The Buffalos, because it was a symbol of strength, an animal difficult to slow down.

"And don't forget, it's also the symbol for newly discovered land" added Ben, as the limos arrived at the cave entrance.

"This is definitely undiscovered land," said Bill. "It's beautiful!"

They all looked around, impressed by the flora. They started walking, deep into the cave. After a little while, the narrow passageways broadened and brightened, and they were able to walk more comfortably. John took the initiative in changing the subject from social talk to the famous value chain. "In my opinion, our mission is very simple. We can arrange it all within a few minutes, and then we are free to do what we like."

"You might be right," agreed Bill. "Well, do you have any suggestions?"

"I think," said John, "that we simply need a stakeholder for every element of the chain, plus the cardholder in its role as consumer.

Since we are asked to elaborate, as part of a group, this is how I see it

- ***The card scheme operator***
- ***The infrastructure operator, may be suddivided into smaller roles of***
  - ***The provider of the terminals***
  - ***The operator of the networks***
- ***The accepter of the cards, like the shopkeeper with the card terminal.***
- ***The Registration & certification authority to link the cardholder to the card, and the electronic signature of the cardholder to an information object that the user will want to sign.***

How about we start from this point?"

" Well I accept this as a good start," answered Ben, "but I am not sure. The card operator purchases the cards, and issues them to the cardholders. Right? But when an e-service provider wants to check the identiy data, who does he go to? The Card Issuer, which holds the personal data, or the Certification Authority, responsible for the certificates? Should these tasks be combined?"

"But what about the card supplier?" asked George, "and the supplier of the ID-data. You need secure relations with them, if you want to build up a really secure service."

They decided that you can have qualified relations, and secure procedure, but nevertheless determine them in the generic role of 'supplier' in a purchase relation with the Card Issuer.

"We are placing a lot of emphasis on the Card Issuer," commented Ben.

"Yes we are completely orientated by the Card Issuer," agreed John, "but thant's what Rupert asked us to explore. I expect that we will have to integrate what we're discussing now with the service-oriented approach of the other group. It will be interesting to see how our different approaches can be integrated."

At this, they reached a smooth and sunny circle of grass. They decided to take a break here. The midday sun shone down as they opened their packs and gulped their water bottles thirstily. Refreshed, they made their list of stakeholders responsibilites, which looked like this:

The Card Holder

The Card Holder or user is a physical person (in the legal sense, i.e. an individual human being not a company/legal structure) who has been issued a Smart Card by a Card Issuer.

The issued Smart Card is associated and issued to the specific Card Holder and to him/her only.

This association enables the card to be used by the Card Holder for IAS purposes and thus to enable him/her access to services provided by the service provider.

The Card Holder is only the user of the card and not its owner. The Card Holder has the use of the card, but the card and its contents remain controlled by and under the responsibility of the Card Issuer.

In order to be issued a Smart Card, the Card Holder must first register with the Card Issuer. In some cases, a card may be used to grant associated rights to a family or other group of persons e.g.

- ***For tax purposes***
- ***For Health care/Social security (where the children/spouse are covered under the adult's health plan)***
- ***For social services***

These cases do not contradict the fact that the Card Holder is a unique physical person. They just mean that for some specific applications the rights of the Card Holder may be extended to other people. Nonetheless, each card is strictly associated only to a unique and specific holder."

The Card Issuer

The role of the Card Issuer is to issue Smart Cards to Card Holders.

While the Card Issuer holds the legal responsibility, most of its operational tasks are likely to be delegated/sub contracted to specific entities such as a card manufacturer and/or the certificate provider.

Independently of the issuance policy deployed by a Card Issuer (this is an implementation level issue), the Card Issuer has the responsibility to:

- ***Register Card Holders: i.e. obtain sufficient proof of the identity of the Card Holder by traditional means. This RA function may be operationally delegated.***
- ***Generate IAS (data, functions): i.e. issue certificates associated with the Card Holder. This CA function may be operationally delegated to a certificate provider. Physically issue the Smart Card. This function may be operationally delegated to the card manufacturer.***
- ***Personalise the card with the appropriate software and IAS data on board.***
- ***Securely deliver the Smart Card and authentication mechanism (Pin or enrolment of biometrics) to the Card Holder.***

The Card Issuer, since it is the owner of the cards, also has the responsibility post-issuance to:

- ***Operationally manage IAS and cards (e.g. CRL, repudiation policy in case of lost, stolen or misuse of cards)***
- ***Operationally manage card security (e.g. authorize application download/activation in the case of multi-application frameworks, authorize card unlocking)***

The Buffalo group gave an example of a Card Issuer: "A government or a government related agency (e.g. Ministry of the Interior, Ministry of Health) is a good example of a Card Issuer. Today Card Issuers are essentially private companies like banks. Whether public or private, the Card Issuer roles and responsibilities are the same."

The next stakeholder they discussed was the Certificate Provider. They concluded:

The Certificate Provider

The role of the certificate provider (also known as CSP) is to issue:

IAS certificates and attribute certificates related to the Card Holder
Any other certificates used for the functioning of the Smart Card information system.

It acts under the responsibility of the Card Issuer and/or, if applicable, of the SCC Administrator or the service provider.

The Access Provider

The Access Provider is the entity in charge of managing the infrastructure (i.e. the card readers and necessary drivers, communication network and servers) to be used by the Card Holder accessing the offered services. This responsibility includes:

- ***Identification of the card by the card reader.***
- ***Security of the communication between the card and the reader as well as the path between the reader and the desired front office application layer.***
- ***Loading of the reader with the appropriate software for reading the card.***
- ***Initial checks (valid card, valid issuer, expiration) for accepting/refusing the card.***

They also noted that "The Card Issuer and the service provider strongly rely for IAS purposes and any of their e-transactions on the security provided by the access provider".

Satisfied by their progress, the Buffalo group shouldered their bags again and made their way to the village.

When they arrived the other group was already there, sitting at a table. George saw them first. "Hi!"he called as he walked towards them. "How did you get on?" he asked the others.

"Hi George!" answered Hiro, who was part of the second group. "Beautiful walk. Really enjoyed it. What did you call yourselves then?" he asked, taking a seat.

"The Eagles. We fly high and see all what happens in the landscape."

"Good name", said John, joining them at the wooden table. "Do you mind if we compare our lists?"

"Not at all," replied Hiro. He took John's list and his group gathered around to read it. John took Hiro's list and began to read. The Eagles group had started with the cardholder, as their ultimate 'e-valu'-ator. In content, their list was not very different from that of the Buffalo group. It read as follows:

The Service Provider

The role of the service provider is to provide business services to the Card Holder using the Smart Card as an IAS token and/or as a support for a specific on-card application.

As examples the Eagle Group gave:

- "A service provider only using the IAS function of the card = an e-commerce company. This company will use the IAS function to obtain a non-repudiable electronic signature from the Card Holder binding him to the order he has made on the Internet (Note: payment is not under discussion here).
- A service provider using a specific card application. The health service, for example, may find it useful to have a specific card application which manages the Card Holder's medical rights and which uses medical prescription details stored electronically "on card" to allow the Card Holder obtain prescription medication from a pharmacy without direct payment."

The Content Provider

The Content provider is the entity in charge of keeping the content of the service provider up-to-date. This will be in accordance with the content service requirements and agreements concerned. Note that it does not play any role in IAS interoperability.

The Buffalos asked the Eagles their opinion about the Certificate Authority. In practice they agreed that the Card Issuer is involved in certification. But there was a need for separtion of responsibilites. After discussion it was decided to add a more or less independent 'monitor' role that especially looks to the balancing of responsibilites. They called this the SCC Administrator.

The Smart Card Community Administrator

The role of the SCC Administrator is administrating, monitoring and supporting the relationships between the Card Issuer, the access provider(s) and service provider(s) in order to ensure the integrity of the Smart Card community. This responsibility includes:

- ***Definition and maintenance of IOP specifications and rules of access which are internal to the Smart Card community (e.g. IOP between the Card Issuer and a service provider),***
- ***Registration of the different stakeholders in the Smart Card community and verification of their compliance to the Smart Card community specifications and rules of access.***

John pointed out that "in a multi-application environment, this responsibility covers the specifications required for enabling and managing the coexistence of several applications on the same card. In this context, this role is also known as Multi-Application Management System (MAMS)"

John put down the notepad, as lunch was brought out to their table.During lunch they discussed the question of what strategy to follow. Each group had a different opinion.

George, John's teammate, said, "We need to develop services, and build the required card base and infrastructure bit by bit. It is the service that pulls the infrastructure"

Mildred, who had been on the other team, disagreed. "I think we need to create a card base, and offer this to service providers who can then offer profitable services. The infrastructure is what pushes the services."

Nobody was surprised that the two groups had different views, "Let's made a list of pros and cons for each view" suggested Bill.

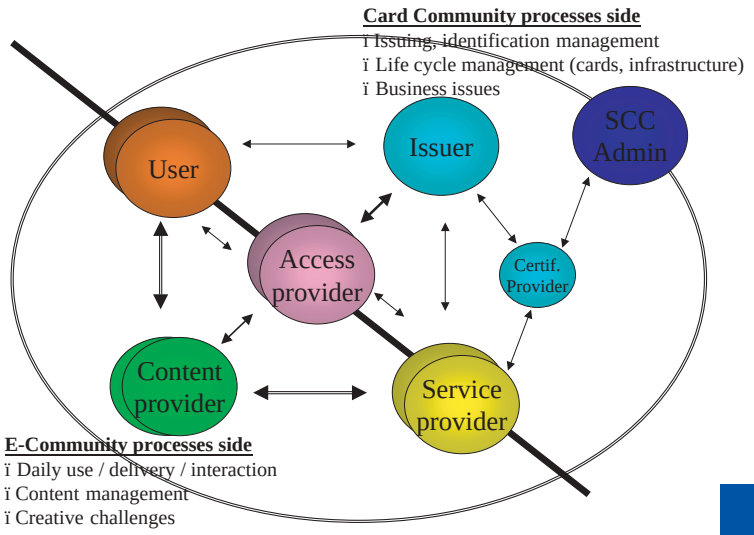
After they had done that, John summed up: "Our conclusion must be that each strategy depends on a number of circumstances, which we cannot always control. For both strategies, however, the ultimate aim should be maximum value, for the maximum of target groups."

After lunch, they were given a guided tour of the village.The guide was friendly and entertaining, and gave an interesting description of local life in the village. He explained that the village and village life were very well adapted to the nature and environment of the area.

John laughed. "Do you hear that? Here, the infrastructre shapes the content. It is PUSH, coming from the circumstances of this valley"

"Oh, yeah?" Mildred retorted "Do you think they made thousands and thousands of cave houses in the early days, just waiting for people to come and live in them? It is PULL from the desire of the people"

Later, sitting on a terrace, shaded from the afternoon sun, Rupert opened a flip chart. He drew the following model on it:



"For a deaper analysis of this point, see Part 2 Clause 3 & 4"

"Tell me," Professor Rupert asked the group: "What role would bring coherence to the stakeholders?"

"The Card Issuer arranges for the technical and business conditions and means for a number of service providers. But it does so without interfering in the content-oriented relations of the service providers. It could be a kind of 'primus inter pares' to other stakeholders, when initiating and keep track of the policy making process," suggested George.

"The Card Issuer has a stable relation with the Card Holder," said Hiro, "the service provider may not deliver his service to all Card Holders. The Card Issuer has to maintain a kind of service desk for the Card Holders."

"The Card Issuer, in the role of card scheme operator, has a stable relation to the access providers in the working area of the card base. The Card Holder has at least to stimulate the access providers to organise a kind of operational desk to solve technical problems for access providers, exploiting a kiosk or terminal. These access providers can give access to more than one service. They are distinct from the service provider because they do not care about the content, but about the terminals and the network," said Bill.

The conclusion they came to was that approaching the model like this would lead to the card operator as central.

"This terrace meeting is the closing session," announced Professor Rupert. "Always leave them wanting more," he joked.

"But don't worry," he reassured the mayors, "Euclid will be available for all of you when you are back home, be it perhaps in a limited way, but she will assist you. I will explain you how you can call her when we are back at the campus. With all the experience that you have in your city, the direction that she gave you and the assistance that she can provide in your city, you are now equipped to settle a sustainable and effective strategy of your Smart Card community.

"The steps that I advise you to make at home are:

- ***Elaborating how the key stakeholders in your city are positioned***
- ***Defining the key processes that must be organised.***

The evaluations and conclusions can be done in an informal way. I propose to do this in the lounge, before our farewell drink. Then we'll leave for the airport."

When he had packed, John made his way to the lounge, where they had met Euclid that first day. The mayors sat in the comfortable armchairs. Professor Rupert tapped at his laptop.

"OK, This is an important moment for you all of us," said Rupert. "For me the relevance is to find out how you are going to interact with Euclid when you're back home. For you, the importance lies in the content of the knowledge you can take from what Euclid gives you. Yesterday, in interaction with Euclid, you built the value chain.

The basic notion is that you need at least three levels of service that are loosely connected with standardised interfaces

- ***The basic services to create the virtual world. All entities have to be defined, and secured with a key. It is through the components of the infrastructure with which we as human beings can communicate with the services.***
- ***The services to make the components secure, insofar as this is required. Secure infrastructure boxes, strong authentication of the users and other entities using the services. Qualified expressions of the will, which means qualified electronic signatures over objects that the users want to sign.***
- ***The real user oriented services, including all 'user content' of the network services."***

Professor Rupert projected the value chain onto the screen in front of them. "Do you agree that it is difficult to make a business case, given either of the following restrictions:

- ***when you start with cards and terminals, without dynamic service; and***
- ***when you start with services, so that they must bear the burden of the total card base and infrastructure"***

"In both cases you first need to invest in the card base and the infrastructure" interrupted Ben. "I do not see how I can avoid the vicious circle problem."

At that moment Euclid appeared over the projected value chain picture. There was a sharp intake of breath.

Euclid got straight to the point. "OK, this is what could happen to you within the coming months, when you really want me to participate in your policy making process. Ben, you have described the heart of the problem. Let's evaluate these two situations:

The first is the banks and credit companies who have invested enormous amounts of money in cards and infrastructure. The parameters of their business case are:

- the relative costs of the operational process
- the new customers
- the number of transactions
- all projected against what the competition is doing. For a number of services the banks and credit companies have a business case.

The second is companies with high-risk profiles who invest in the protection of the physical access and / or their desktops. These companies are not mass oriented, but with their business parameter they also have a business case.

Try to learn from the both cases. What are the general drivers behind both types of cases?" She paused. "The answer lies in making open standards for interfacing the units of the chain. Every unit has to optimise its own business."

"I do not want to rehash today's session," Ben argued, "But in my opinion that is the whole question. I still think that banks are only prepared to invest in their own business. And companies in the protection of their own risk. They both cover the whole chain for themselves. I still do not see how we can find money and create cases for every unit in the chain itself. Even after the brainstorm today with our individual groups, which I did find quite beneficial."

"Yes," Mildred came in, "I was quite astonished to see how complementary the e-services approach and the card scheme operator approach was. At the same time, I share Ben's concerns about how to solve the policy problems that I foresee. There are a number of areas where challenges arise, I think.

- ***Operational: this concerns the issuance of a generic card that can be used and trusted by e-services parties***
- ***Technical: how to organise the interface between generic identity services and the specific e-services, with all the different elements of infrastructure***
- ***Cash flows between the stakeholders: how to involve the e-service providers in the case of the scheme operator. Do we need an accounting system, and how to make this operational?***
- ***Legal: who is responsible for what? How to organise the responsibility towards the users."***

“Well,” Ben added, “do not forget the subject of privacy. This concerns all stakeholders. But especially the citizen involved. Does he always want to give his identity? And what about the legal basis when we put, like in our city, the official population register data on the card. It is clear that we have quite a list of policy subjects after these sessions.”

“My feeling is, that we have to consider all aspects for each of the roles AND for the total chain as well.” It was more a question than a statement from Mildred.

The group looked at Euclid to hear her answer. She was gone.

After a moment of stunned and disappointed silence, Professor Rupert took a breath. “I think that we have to solve this for ourselves” he concluded. He began to explain how he hoped his lab would co-operate with the e-City program in the next six months. The mayors made appointments for conference calls and evaluation procedures. Rupert finally explained the experimental software to create the conditions for the appearance of Euclid.

Everyone had some reservations. But Ben was the only mayor who did not gave his full assent to Rupert’s plan. “I am not convinced,” he said clearly. “I am willing to try it, but please phone me when you have real results to report”.

The mayors did not try to convince Ben. They all toasted the end of the conference with a farewell drink in the bar. In six months they were to meet again. Then it would be clear if the e-City program could survive.

Chapter 3 The Dilemma

Back at home John analyses the business interests and the main target groups of his e-service providers, and those of the card scheme operator. His children help him to realise the central importance of the services component and the freedom of choice for the consumer.

John collected his car from the airport and drove to City Hall. He missed the weather he had enjoyed during the Euclid trip. And, the traffic was awful this morning. He should call his city development director and ask him about the progress in the city traffic circulation program. It sure didn't look like there was any progress happening. And without progress in these areas there would be no re-election next year. His mood was already dark when he entered the official car park. "Someone has taken my parking spot," he grumbled. But although he was angry, he decided to let it go. He had a lot of other things going around in his head, and decided to give priority to the ones that really needed his attention.

He invited his immediate circle of staff to have coffee in his office. Over coffee, he reported the content of his meeting at the university campus. His mood brightened as he settled into his position as chairman, John's favourite role.

He asked his staff, "Which of you are stakeholders in our e-City program, and what is your role?" John looked around the table.

They all looked rather astonished. "What do you mean, are not we all involved?"

"OK then, 'civil services' is doing the card issuing. 'Education and culture' is doing the content for the schools and event ticketing. 'Sports' is issuing the sport pass. 'Information and communication technology' is supporting the terminals, isn't it? And 'PR' is running a kind of help desk for the citizens."

"Yes, mayor, but you forgot one important category: the special groups using our electronic forms. The building permits, the tendering forms and databases, even hospital transfer forms."

"OK, Pete. I did not try to be exhaustive. What I'm trying to do is describe the split in responsibilities between 6 stakeholders: the card operator, the infrastructure operator, the strong authentication issuer and the qualified signature operator, the services providers, the experts involved by the service providers. And of course the consumer as card holder"

"A number of us are oriented on the support of the card scheme, and a number are oriented on the support of the content in certain areas. But everything is connected to everything. You know yourself how complicated it was to add our ticketing to the cards that were already in the field. And last month, we rejected the proposal to add the billing service for the heavy users of public transport, because our infrastructure cannot handle contactless smartcards. The conclusion was, you remember, that implementing this program means as much investment as restarting the whole existing program.

"But this is exactly what it is all about. I came to the conclusion that we have to try to unite all the money that is available in our city for any e-service, for which you need identification and or an electronic signature. We provide this service. We also provide a driver's licence, on behalf of the national body. And we provide travel papers controlled by our national ministry of internal affairs. We get money for issuing these documents. But these papers are used for all types of identity checks in services in which we do not participate. I would like to explore what we need to do with each of the services, in order to maximise the user value for the total service.

"So I ask all of you to come up with the following data in qualities and quantities:

- ***What do you need for your service?***
- ***What are you going to deliver?***
- ***What do you need as a tariff at what quantity levels?***

When you come up with some material, let's say in two days, we'll make a first overview, and we can define the direction and tune the figures. Questions?"

After two days, John met his consultant, Pete. He had made calls to all directors involved, and also to a number of service providers.

"What you're asking me to do, John, isn't very easy."

"That's why I pay you so well!" John grinned. "Right, Pete, stop teasing. Let's get down to business. What are the complications that you see?"

"I have made a report," Pete explained. " The most important thing from a business point of view is the services. You concentrated very much on e-gov related services, since they are the only ones to be allowed to used the official population register data. Theoretically, there are many other services that could use, and are willing to use, the e-City cards.

During my research, I came up with this list of constraints

- ***You need to create access to their services via your e-City infrastructure. Not only the kiosks in the city hall, and the hospital and the libraries and so on. But also via the access software which citizens may use on their PCs in private homes. People want to have software that they can integrate in their internet applications, in order to ask the user to identify themselves, authenticate or receive an electronic signature.***
- ***The majority want to pay, in principle, only for each authentication and signature, and for Smart Card oriented services that are directly related to their service. You can also apply a registration fee. Of course the tariff levels must be low enough to attract the service provider, but also high enough to balance the books at our end.***
- ***As a consequence of this, there is a need for an accounting system.***
- ***We have to organise a professional organisation to support the required qualities and uptime and so on, to check the certificates.***
- ***We need to formulate a good organisation plan to manage mutual expectations, and to arrange responsibilities and liabilities, towards the customers and third parties."***

"Well Pete, I don't say this is easy to do. On the contrary. I recognise that it is extremely challenging. "

"Yes, John, it is. Here are some of the complications".

Complication one: Not all service providers have the same requirements to connect the e-service to the generic identification etc. The regulated connection at least has to be 'pre-structured' in three levels of requirements, which the e-service can go for:

1. Only identification of the Smart Card in a trusted infrastructure. In this case only the ID-data of the card will be read, and taken at face value. In that case only the security of the technical environment (the building blocks) has to be checked.
2. Strong authentication of the parties in the session (verification of the cardholder via PIN-code or biometrics).
3. Qualified electronic signature of an (information) object.

There is a need for a mechanism to differentiate this per service.

Related to this complication, is the fact that this connection mechanism must be technology independent. Many of the e-service providers expect an explosion of new applications and service when broadband network really breaks through. Some of them expect much more interactions, with real human experts presented as e-service. Or in the background of the application handling forms while an expert or consultant

is on the screen of the user. That kind of stuff. Of course all under the assumption that there is a good payment service available, that could be integrated.

Complication two: A number of service providers require dedicated human interfaces. Some of them want to differentiate this at request of the different groups. For some, they want big characters, simple, icon-driven, with menus based on preferences of the consumer. Or, for the more experienced users, detailed graphics with many shortcuts. This is not easy to implement on a generic basis. You need widely supported standards for this.

Complication three: the target groups of the e-services are not always included in the card base. When a service provider is targeting prospects that do not have a Smart Card, he has to negotiate with card scheme operator to supply the card. When the service provider is paying for the card as a whole, the card operator is probably willing to supply the card when the prospect is using the card for more than one service. And even then, there is a complication, because someone must convince the prospect to participate in the card base. As a comparison, you do not place an advertisement in a paper that doesn't reach your target group. The person who controls the content of the paper does not always promote the paper in order to reach a certain target group. I am not excluding this possibility, when a service provider has a very dominant interest in a certain target group. But the issue does need careful analysis.

Complication four: I met a number of potentially very interesting service providers who are only interested if they can reach national and international target groups. For them the local use is only a minor link in the total chain. It is the last mile of their journey to reach their customers, to communicate with their prospects and to promote their services. That means that they require a wider network of operators, all using common models and interoperable technology.

"OK, Pete, that's enough to be going on with. I see three stakeholders: the consumer, the Card Issuer, and the service provider. The access provider and the provider of the certificates could be under the umbrella of the card operator. The bottom line is that, they operate strictly within the e-City program. The e-service provider can be anywhere, and can communicate with customers wherever they are. And the citizen can travel between cities, and use all services where they are available: all kiosks, all internet cafes, all over the world. I understand that.

"The problem is we have to find out how the three core entities match? Can you elaborate in your report what the consequences could be and what policy alternatives you see?"

“I can do what you suggest, John. Just one more thing. When you get a chance, try to consider the type of relations that exist between these three core stakeholders. You need to create trust between these three, even when they operate in a common session, via total different environments.”

Home for dinner, John joined his wife, Annie, son Charles, and daughter Wendy. The kids talked about their day at school, but they were more interested in getting away from the dinner table to the computer. They both had to use the internet this evening; Charles was working on a school project, and Wendy had to download some music for her friend Patricia’s party this weekend.

Annie wanted to ask about Patricia’s party, but John was more interested in his daughter’s computer use than her social life. “Are you going to use the city card I gave you the other day?” he asked.

The children laughed aloud. “Are you going senile, Dad? What can we do with that silly card of yours, except maybe telling the library that we want to keep our books out for another week. I’m looking for serious stuff.”

“Like music,” said Wendy

Charlie agreed with his sister. “You told us that we could use your card to read the team composition for next week’s match. Well, it doesn’t work. The team list doesn’t come up until half an hour before the game. It’s no good.”

“Sorry for all that mess that I have caused in your life, my dear children. But why do you blame me?”

“It is your e-City card scheme,” said Wendy “You are the mayor and you always say that you are responsible for what happens in city hall”.

John raised his eyebrows. “Are the services the responsibility of city hall?”

“Yes,” said his daughter, “or at least, it is your responsibility to contract out to people who know what they’re doing.”

“In your opinion, what should I change?”

Charles spoke up. “One thing I’d like is to be able to use it to buy tickets, so I don’t have to sleep on the street and queue with millions of people. And that would stop Mum worrying too. And there are other services too, not just city services. I’d like to be able to choose them, and register for free.”

"And when I'm in a chat room" said Wendy, "I don't like not knowing who I'm talking to. Maybe not always, but sometimes you want to know you can trust someone. Same with websites. Like, if you're looking for information about a school project. They could just be making it up!"

"I agree with her, John," said Annie. "Perhaps you could contract more trustworthy services, and give us more security and certainty about who our kids are interacting with?"

"Then would you be prepared to promote my card?" John teased his children.

"What's the point? What I'm interested in is the services, not the card," retorted Charlie.

"You should listen to Wendy and your mother. There is a question of trust here. How do you trust content provider's own security systems? That's where the card comes in, and why we have a separate authority to register and authenticate providers."

"OK. But I still want more of a choice in what I can access. Not just what your city wants me to see."

"Well my children, I appreciate your suggestions. You've been very frank. I will speak to my staff about this 'triangle of trust'."

"Triangle? Did we say that?"

"Yes. You, using the service and making your own choices about what you want to use. Then, the service provider you interact with. Finally me, the third party that does not know what you are doing, but who creates a secure trusting relationship between you and the service provider. That third party is the issuer of the card, that you appreciated so well"

"Yeah Dad. Can we eat now?"

"Yeah, call yourself a service provider. We're starving!"

In his study, John wished he could discuss with Euclid the direction in which his thoughts were going. He followed Rupert's instructions, and contacted her via his laptop.

She appeared on the screen, "I was wondering when you would call.

Yes, John, the mysterious triangle of trust:

"For a deaper analysis of this point, see Part 2 Clause 4"

- The Card Operator
- The Service Provider
- The consumer, the Card Holder

The card operator exploits the card base and the terminals and kiosk in his infrastructure, and he offers the trust that the service provider needs.
The consumer has a double relation:

- To the services for which he is registered
- To the service provider, that has given him the card."

"The infrastructure is used by the e-service provider and the user. The community exploited by the card operator is not the same as the community exploited by the service provider. The consumer is involved in both, but both communities do not necessarily know about the relations."

"The keyword for your policy is interoperability. Define the common models and you connect these communities…"

Was John dreaming, or was Euclid really there. He blinked. His screen was empty. He stood up from his desk and went to have a cup of coffee.

Chapter 4 Talking Action

Are all mayors working on the same goals? John consults his colleagues and finds out how to integrate the proposed processes.

"Mildred, how are you?" John's voice carried clearly over the phone line to Mildred's mayoral office in the next city. "Are you busy? I'd like to talk to you about Euclid and this Smart Card project for a minute, if you have time?"

"Fire away," said Mildred, " I was going to call you soon anyway. How's it going?"

"Well, I raised the priority of my e-City program. I am working on it daily now, trying to make it self-financing before the subsidy stops. And Euclid said to me-"

Mildred interrupted "Have you spoken to Euclid since?"

"Yes, I made contact with her via Rupert's software… Amazing."

"Let me guess, Interoperability," said Mildred. "That's what she told me too."

John explained what he had started since the meeting at Rupert's campus. The names and programs were connecting to the roles. He described the complication that the card community was not the same as the service communities, and the issue of using the card for access and identification and so on. "The card operator has to manage the identities and certificates of the cardholders in his card community. And the service provider uses this card, to verify the identity and the signature of the Card Holders.

"What do you think, Mildred? I think we have to organise interoperability with other Smart Card communities, in order to offer a broad network to service providers."

Mildred agreed "It is like the saying 'think globally, and act locally'. I fully agree that we have to organise the issuing process and the management of the cards locally. Although 'local' does not always mean geographically local, it could also be a functional community that is very near to the Card Holder. And by the way should try to reach a large scale of cards. Rather more at national level than a city level"

"OK, but my question is "How can we organise interoperability, when all card communities are organising their communities in their own ways. I can imagine that there are technical standards. I will leave that subject for later, but first the non-technical issue. How do I know that I can trust you?"

Mildred was confused. “What do you mean, John?”

“Oh, I don’t mean it personally! I mean, in general, how can any one community trust another. How do we make it work for both of us? The question is what should I check when I make and agreement with another Smart Card community, to be sure that I can give my citizens the same level of trust when they want to use services that are offered elsewhere.”

“ I did not know that you were in favour of offering all kinds of services to your citizens. You wanted always to stick with your own e-gov applications. And now you seem to be prepared to offer services from everywhere.”

“Believe it or not, it was my children who convinced me that you must leave it to the cardholders to determine what services they want use the card for. There are so many services for so many target groups, we cannot imagine. We define in a brainstorm group at City Hall maybe a hundred services. The target group will use some of them and ask for a hundred others.

“I’ll have to verify this with independent research, but I’m trying to decide what policy is needed to support this new approach to services. For the moment, I’m focussing on interoperability, as Euclid advised me. So back to my question: How can I trust you?”

“John, as you know, we have already offered a number of commercial e-services in our city. And we have already addressed the subject of trust. Not for interoperability between Smart Card communities, but trust among all service providers within our city.

“Let me propose a deal. I summarise the studies and reports we have made on this subject, and send it to you. In return, what can you do for my city?”

John thought for a moment. “My concern is to disconnect and to integrate the generic process of identification, authentication and electronic signature in the electronic services. Until now, this process has been more or less woven into the e-gov processes that we support. If we want to achieve interoperability it must be clear where we put the standards. If I make a report on this subject, can you use that in your city?”

“Well, I’m sure it will be useful. We can use it to check how we are integrating the identification processes, and so on, with the commercial e-services. And, when we have our processes similarly organised, we can organise an interoperability pilot.”

"Yes, and we should be able do that within the period. We still have some subsidy funding."

"That sounds good, John. Let's do it."

Mildred did send her report. It described processes covering the establishment and management of the e-City as the Smart Card community itself. John read it with interest.

The report said that five main processes were required to control the Smart Card community:

1. Smart Card community creation
   (Registration and internal certificates issuance)
2. Issuing and maintaining cards
3. e-Service registration (incl. post issuance) registration
4. Establishing & maintaining interoperability
5. Manage smart card base (SCC) and the relations between entities in the base.

"Are these five main processes similar in every Smart Card Community, where we're looking for interoperability?" John asked Mildred over the phone. "If you want to trust another community, you have to be sure that certificates are given to and applied in the same entities, in order to create similar security."

His colleague replied, "The issuing process indeed needs to be as trustworthy as in your own community. E-services are a special case, because they're dynamic. New services, old disappearing services. This could be a risk. This needs to be carefully studied. And practical interoperability is critical," she continued.

"Yes," John agreed, "You have make, and test, practical arrangements. And there are management issues - you have a responsibility towards the end user."

"And finally, statistics are needed to monitor the cash flows between the communities," Mildred finished. "Good luck, John!"

John was impressed with the report. He was only worrying about the basic process of the cardholders. Mildred had done a good job. He could use its content not only to organise his own 'secondary processes', but also as a checklist when preparing interoperability with other Smart Card Communities.

John added some notes to complete the picture

"For a deaper analysis of this point, see Part 2 Clause 5"

1. Smart Card community creation (Registration and internal certificates issuance)

- Register Smart Card community and external secure suppliers
- Verify the compliance of SCC stakeholders with CI requirements and register them i.e. 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 them with PKI Certificate

2. Issuing and maintaining cards

- Personalise card
- Issue Card Holder certificates
- Initialise the card
- Enrol the Card Holder
- Maintain life cycles (cards, Card Holder ID, certificates)

3. e-Service (incl. post issuance) registration

- 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

4. Establishing & maintaining IOP

- Create IOP adapter, install rules and policies
- Maintain IOP adapters

5. Manage SCC

- Log the use of cards, IAS and front office
- Acquiring and settlement

Now John decided to phone Ben. He was the most cynical in the group, but John knew that he had many services in his city. Before John could put down on paper his own ideas about the generic process, which he believed should be disconnected from the e-services, he was interested in Ben's vision and solutions.

Ben was short, but not unfriendly. "No, I haven't tried to use Rupert's software yet," he told John. "Yes, I am interested in interoperability, but I don't see

much of a problem with what I'm doing here. My citizens can use all types of cards, not one for all services. They use these cards only when the user wants to give identification via a card. It is the responsibility of the service providers to issue cards for their services. But cards are not required as such. Of course, where there is a need, like for buses, they use cards. Our city buses are using contactless cards, in order to make the throughput flow quicker. Bill Gates did help us a lot," Ben concluded.

John didn't understand. "What do you mean?" he asked.

"By pushing worldwide implementation of his industry standards and tools, Bill Gates avoided many disputes. That's why I feel that Bill Gates helped us. This approach will solve a lot of problems," answered Ben. "In my opinion, we must not interfere in the process. I want the service providers to solve their own problem. And since they are using internet standards and tools, they are already on their way to interoperability."

"But how can I be sure that I can trust cards from your city?" John continued.

"It depends on the service provider who issued the card," explained Ben. "The fact that a card is used or issued in my city does not say a thing about trust. Of course I kick out any e-service provider who appears not to be trustworthy. But I guess this wasn't exactly what you had in mind when you asked me this question."

"You're right," agreed John. "What I want to know is how do you provide interoperability?"

" Well, I established a platform where the service providers in my city make arrangements. The service providers decide what they want to do in that area. I send out requests for tenders for services in my budget. Public transport, tourist passes, my city hall employees, and that's it. An example: we're currently preparing a new initiative concerning health care. It's sponsored by some insurance companies. I will wait till I see their proposal, and offer them the opportunity to participate in our e-City platform."

Ben took a breath and continued: "I appreciated the concept of the value chain, as discussed with Rupert and his crazy images. But I haven't yet seen a clear demand or need for us as a city to intervene with the e-services that want to be interoperable. And I do not see any immediate reason to propose cost sharing on card, infrastructure and identity management and so on. I am not arguing against it in principle, but it would be quite a revolution here.

"Also I do not see any huge demand among our citizens for many new

services. Once that happens, I'm more than prepared to adapt my policy. For the moment though, I'm happy with the fact that, in our e-City platform, everyone seems to be satisfied with the agreement."

Listening to Ben speak, John thought over his own approach. He had mixed feelings about Ben's focus. Although Ben had clearly followed a totally different approach, John had learned a lot. Ben's approach was not controlled by the card operator but by the service provider.

John closed his call with Ben in good harmony, agreeing that their approaches are different, but aware that both had their weak and strong points.

He made a quick cost comparison between their two approaches. On the one hand Ben's infrastructure and procedures were simple. On the other hand the sharing capabilities were restricted, and his infrastructure overlapped. John expected that the costs per access unit of the service provider-centric approach were higher, but he was not sure.

For this moment, John wanted to combine the convenience and low initial investment of Ben's approach with the high level of service, convenience and trust that his own city hall was giving to the citizens. He decided that when there was a need to disconnect the e-service and the identification, that he would influence as little as possible the application of the e-service provider. The e-service provider must continue his application as much as possible.

Perhaps it was a good idea to orient them all on internet tools, at least for the interface to the generic identification application. Perhaps even dedicated applications with proprietary elements in them, like physical access, should get an internet-oriented interface within the common identification application.

The next day John sat at his desk, with Pete. He had to fulfil his part of the deal with Mildred.

Together they defined the following primary process, which should function as a generic model

"For a deaper analysis of this point, see Part 2 Clause 5"

1. Connect (contact or contactless) Smart Card to (modules in) terminal and secure the links
2. Identify/validate and accept/reject the card in the infrastructure + identify/validate and accept/reject the terminal / terminal application (authenticate the 'building blocks')
3. Find, open and interact with the requested e-service and read the business rules for the requested e-service

4. Transfer ID data to the e-service / make data available
5. Authenticate Card Holder (if requested for e-service)
6. Execute e-service (IAS is passive)
7. Sign an information object (if requested for e-service)
8. Update administrative log-files and close the IAS session

Satisfied that they had achieved something useful, the two men decided take advantage of the unusually sunny spring morning, and go to the golf club. What with all the extra work on the e-City program, John was starting to miss his weekly informal contact with his friends on the golf course.

Strolling along the fairway, he and Pete chatted. The conversation inevitably returned to the e-City program. “It looks like the various e-Cities are not working in the same direction, Pete,” John said, and described his conversation with Ben the previous day. John told him about Ben’s approach, with the service providers in the driving seat. And Mildred’s approach, with its processes to guarantee trust. And John’s own approach, giving the model for the generic access and identification and checking process. “How can we ever create interoperability between all these e-City services?” John asked, lining up his shot.

“Do you really want to talk business now? OK, you obviously do!” Pete laughed. “You can always create interoperability between two defined situations. The question is how can you create interoperability effectively on a more or less generic basis.

“Let us first reduce interoperability to the process that you have described yourself. Identification, authentication and electronic signatures. The primary process.

“Then let us have a look to what we mean by interoperability, in an ideal situation. Card Holders being able to use their cards not only in our e-City, but also in other e-Cities. We have to elaborate on that later. It affects two levels: the card itself, and the terminal and other infrastructure where the card is offered to access a service. There is a third level too: the services that could be supported by all cardholders. We can make models or scenarios. But that’s for later.

“When you have decided what interoperability means for you, then you see that the three processes are really complementary. And you also see what you should do with it.

- The primary process, as you have described it. All participants who want to offer interoperability really must accept this process. Even when

various e-service providers, as in Ben's city, exploit the card base. You need common understanding about the steps, the data flows and the content of the interfaces. Otherwise it is impossible to organise interoperability effectively. When you are facing a dedicated system, which is able to produce the right data, in the right order and vice versa, interoperability is not excluded. But the assumption is that all parties accept what is 'the right' process'

- The secondary process, as you have received from Mildred seems to me less mandatory. It rules the conditions that have to be fulfilled to be trustworthy at a certain level. As far as I can see, it leaves room for differences in applications. Parties that want to be interoperable, where both are based on high level trust services, have to show each other their measurements. That means that these processes are required in their objectives and recommended in their appearance. It makes the organisation of interoperability much easier when the processes are mutually recognised.
- The tertiary process is simply the e-service itself. The only requirement is the interface to the primary process. In the case of Ben's city, the tertiary process is combined with the primary process. As I have stated, when his service providers are able to produce the right data and so on, a part of the interoperability can be solved.

"OK, Pete, I got it. Interoperability is based on a stairs of three steps

- the primary process with the obligatory interfaces in all e-Cities
- the recommended secondary processes, with required similarities in the e-Cities
- the free e-service process, plus the interface to the primary process in all e-Cities.

The e-Cities have more in common then I thought they had. Speaking of thinking, I think it is time to call it a day. Everyone else is at the 19th hole by now!"

Chapter 5 The Four Freedoms

John shares his ideas with his nephew Brian. Through discussion they identify four main independent dynamics, and how they can be controlled to achieve interoperability between the different service providers and card scheme operators.

John paced around his office. He looked at his watch. Ten minutes before he met his nephew. He needed to talk to someone not directly involved in the issue. Someone who could inject a clear new viewpoint on the question with which he was struggling. Brian was an engineer, well educated, with a good overview of IT. John was looking forward to picking his brains!

While walking around he reflected on the situation

- Euclid has stated that sustainability in e-City projects lies in the value chain. This value chain has to run from exploiting the IT stuff (like the smart cards and the infrastructure), via trust services to e-services. Without gaining the highest customer appreciation, no business case is sustainable. The core of the value chain seems to be that you have to disconnect the card operator from the service provider. The card scheme operator can bring down the cost per card substantially by enlarging the scales. Most of the user value comes from the services, which not necessarily must be large scale oriented. The number of services per card, or may be the frequency of utilising the card seems to be key. Even when there is not one 'killer-service' available.
- On their walk to the village, the mayors had defined the roles that are involved in this value chain. These roles were also oriented to two environments: the card and infrastructure environment to create the 'virtual space', and the content oriented environment, with the services. Both environments must be exploited, with cases for all roles. The roles do not interact directly.
- The distinction in these two 'hemispheres' is also required to create trust between parties on a generic basis. The Card Issuer authenticates the identities and the certificates of cards belonging to his 'community', towards any service provider, which the cardholder wants to access. This was the triangle of trust to which Euclid referred.
- But Euclid also referred to interoperability, for which he modelled the three categories of processes. These processes have to work together; some more, like the primary process, and some less. This means the use of open standards.

- But there was more, which is not addressed yet.
  In the campus session Euclid referred to:
  - Personalised human interfaces
  - Easy access to a personal chosen variety of services and systems
  - Guaranteed levels of trust
  - Sustainability for new technologies
    - for the broad band services
    - for new mobile cards and terminals

At this moment Brian entered. “John, how are you. You look stressed!” he exclaimed. The younger man looked relaxed and suntanned. The two men shook hands, clearly happy to see each other again.

“A little, I guess,” replied John. “Let me tell you all about it. I’ll order some coffee.”

John outlined the situation and described his worries about the e-City program

“Please John, don’t concentrate on technical problems. Maybe you’re surprised to hear that from me as an engineer. But from my experience I can say you first make a clear picture of how the main functions are to be related. Then there is time to solve the technical stuff. What makes you think, as you told me, that the identification, authentication and so on, is the heart of the matter? Why not the service?”

“I am a city governor, Brian, and when I meet new problems I often try to find a good comparison or a metaphor. In this case I compare the information and the knowledge and the images that are hidden behind television and computer screens to a city. As you also know, some e-Cities literally represent themselves on the screen with a picture of the city. And companies represent themselves with a picture of their buildings. And so on. You have access to services, which you can compare with shops. Identification enables virtual bodies that can knock on virtual doors, and enter a service. Referring to your question: ‘identification’ refers to persons. ‘Services’ refers to shops and buildings, in which people live, work, learn, meet, and what else.”

“It is always nice talking to you, John. I don’t look at computers in this way. For me they are just tools. For you, they are the mediators to a world that you see and treat like your city. Interesting.

“So, lets imagine that you put the persons in the centre, instead of the buildings. The consumers drive the infrastructure. No users, no economy, no

buildings. There is a dynamic relation between the two. Services - in your metaphor, nice shops and buildings - attract people, and more people inspire new services. So, people, or identification, is at the centre."

"And, Brian, there is another element that we have to take in consideration before going further with your functional approach. Euclid focussed me on this very explicitly. That is interoperability. In our metaphor it means that our citizens have to have access to buildings and shops in other cities, and we want to welcome citizens from other cities."

"Yes, I think so. There are four elements that immediately come to mind

- The connection of the identity function to the service. In your metaphor this translates to the windows to look through and the door to go in
- The communication to the real person, say the human interface element
- The technology for access. Here our metaphor becomes a bit difficult. In the real world, the person goes to shops, which are immobile. In the virtual world, the person can 'pull' the service to where he is.
- Fourthly, there is the 'key', comparable to the key to the room where the shopkeeper can compare my signature with the original one, in order to avoid risks of false signature.

"If you want to be interoperable, I would say that these elements need to be standardised. Shopkeepers in other cities must understand them. And your own virtual shopkeepers, John, must understand these functions from other cities."

John replied, "But suppose individuals change their preferences, which we have fixed in the human interface function. Or suppose we want to bring in new technology for access. My colleague Ben, for example, swears by contactless cards, for his public transport services. Do the standards that you mentioned allow for the possibility to change or add something to the functionality, without disrupting the whole system?"

"Yes, this can be achieved by applying standard interfaces between the functions. As long as you respect the standard interface, you limit the problems.
"So, these standards serve two important goals: Flexibility and Interoperability."

"Can we be sure that the four identification functions you mentioned are sufficient?" John asked. "How can we check that?"

"You told me that you have got the stakeholders model, derived from the value chain.

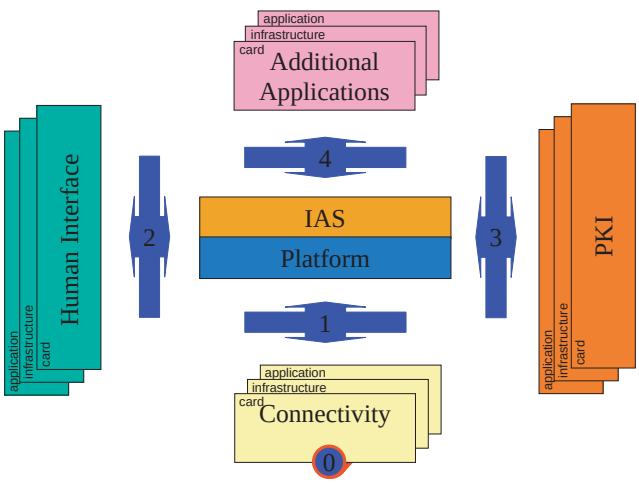
Let's follow this for a first check

- The Card Issuer is responsible for the primary basic process, to be laid down in the basic and generically used function of "Identification, authentication and electronic signature'. We have that as the core function.
- The access provider, or from the other point of view, the card acceptor, is responsible for providing and managing the terminal function. We assume that the card acceptor is not the service provider. For example the service provider could be the credit company, and the access provider could be the shopkeeper. When the shopkeeper subcontracts the maintenance of the terminals or the kiosks in his shop, this does not change this function. We defined this access function, to base it on an interface, which will be able to neutralise the different technology options.
- The service provider needs to connect his e-service to the generic IAS. That also is on the list already.
- The certificate authority is involved via the listed PKI function.
- The user's preferences are involved via the aforementioned function of the human interface.
- There is one role defined for which no function is foreseen: the experts and the dedicated interactive content provider."

John sat back in his chair, listening attentively, as his nephew concluded: "I think this role does not need a specific function. Functions were needed for independent development and for interoperability. I presume that these content providers always work via the application of the service provider. What do you think?"

"I think we are getting somewhere, Brian. But I have an idea. I told you about Euclid. I've got the software on my laptop from Professor Rupert. I'm not sure it will work. But shall we try to call her?"

After the required keyboard manipulations, and indeed the use of the e-City card, the screen lit up. Brian had high expectations of his budding relationship with Euclid. But all that came on the screen was the following picture…



They did, however, hear her voice, which was of course already familiar to John, and which did not disappoint Brian at all.

“This is the picture belonging to your discussion. It represents ‘four freedoms’ which you should create around the core function of identification, authentication and electronic signature. You are on the right track to create enough sustainability and interoperability between Smart Card communities for the coming years.

“I propose that we work together a bit to elaborate this picture.”

While talking together, they created the following text on the screen, without touching the keyboard, the mouse, or even the screen. Brian was impressed with the convenience.

"For a deaper analysis of this point, see Part 2 Clause 6"

The IAS application function

The IAS application function is the nucleus application of the whole Smart Card information system and provides three different sub-functions:

- **Identification** i.e. who is the Card Holder?
- **Authentication** i.e. determining if the Card Holder really is who he/she professes to be by using key pairs to verify the identity of the Card Holder
- **Electronic signature** i.e. has the Card Holder expressed his/her consent for committing to a particular action?

The Platform function

This function includes the operating system of the related building block.

The platform box will have no direct IOP-interface to its functional environment other than to the IAS-application that is running on this platform and the connectivity function.

The “PKI” function

The PKI set of tools related to the IAS function has two or more (bio) PIN-based key pairs. A key pair is used for authenticating the Card Holder and is required before any signatures for non-repudiation can be generated, a second one is used as a signature mechanism for expressing Card Holder consent and a third one could be used for confidentiality purpose.

The “User Interface” function

The following sub-functions are considered part of the “user interface” function of the card layer:

- Smart Card community settings
  (language, accessibility options and tools to ensure access for all)
- Individual settings (profiles, preferences)

The “Connectivity” function

The “connectivity” function is in charge of inter-connecting building blocks and includes the following sub-functions:

- Challenging the Smart Card via the reader
- Establishing a secure connection with the Smart Card

The “Applications and e-service connection” function

The following sub-functions are part of the “additional applications” function:

- Applications containing additional Personal data (if required)
- Additional functions for identification and/or card management (if required)
- General applications (on card applets) or the access to them (as far as required)
- Connection to “e-government”, “e-business” applications, based on rules given by the service provider.

Note: The downloading of a particular “additional application” onto a card remains subject to authorisation from the Card Issuer responsible for the Smart Card concerned”

Euclid spoke again: “OK, gentlemen, you have made at lot of progress. This model with functional boxes and standard interfaces is easy to understand, but not easy to implement. But it will help you in creating the flexibility you need in the value chain. And to organise the interoperability, even when you work with existing card bases”

Then the voice was gone.

“Let’s capture and print this information immediately”. Brian was a practical guy.

“It is a pity that she disappeared again so quickly,” said John. "Shall we have lunch? There's a lovely new restaurant near the lake behind city hall.”

During lunch they tried to discover how you could use the model for interoperability, without developing a card scheme from scratch.

They thought quickly, inspired, it seemed, by their discussion with Euclid. Before the starters were served they had come up with an approach that would have pleased Mayor Ben. John said, "If we leave all communities as they are, but when they need to communicate, we put something in between them to translate the data flows from one to the other. A kind of additional box that simulates the use of the interfaces as defined by the model."

Brian said: ‘I do not think that this would be that easy. At the very least you need to have all required information, or more precisely the data involved in the secure identification and so on, available. This minimum set must really be mandatory, otherwise you can forget even this type of solution for interoperability’.

As they ate, they decided that this additional box, using the model as reference to simulate the standards, was probably the solution Euclid was referring to. By the time the main course arrived, they had decided that was enough for today. They relaxed and enjoyed the fine meal. Conversation turned to more social topics. As they went their separate ways after lunch, John said, “I am very grateful, Brian, you’ve helped me a lot.”

“You're welcome, John. It was my pleasure. Give my regards to Annie, and kiss the kids for me."

Walking back to the city hall, John thought about his options. Could he add some of the interfaces to the system that the e-City program was using already, or should he go for an ‘interoperability adapter’ to be interoperable with the services of other cities?

Chapter 6 No Man is an Island

John learns that no technical solution can create effective e-ID interoperability without agreement, preferably at the national level or higher, on common data for identification, authentication and signature. This agreement is recognised as perhaps one of the biggest challenges facing his program.

"It's becoming clear to me, Pete," said John over the phone, "that inter-operability leads at least to mandatory data. Whatever you exchange with another e-City, or whenever you have to operate from another e-City, if data is not available, no technology can help you. Can you do me a favour and make a quick overview of the data that should be standardised, and to find out if all e-Cities comply with this list."

"Sure," said Pete, "I'll fax it over to you soon as I can"

Pete put down the phone and got straight to work. He made a list of data and other requirements for data involved in identification cards, and travel documents that could be machine-readable. He referred to the ISO standards involved. And he phoned John's colleagues, starting with good old Mildred, as John used to call her.

Pete noted that the differences concerning some basic data were, due to the ISO standards, not too big. It covered the personal information of the citizen: name, surname, date and place of birth, etc.

Pete extended this list with what he considered the minimum information to organise interoperability, and then the differences were considerable.

He checked the following data items

1. Identification of the stakeholders, including their addresses
2. Identification of the Card Holders (Minimum)
3. Identification data of the cardholders' dates
   (Redundant for off line use, like name, address, etc.)
4. Identification of the technical components that must be secured
5. Ditto for the authentication of the user
   (certificates, to link the user to the card))
6. Ditto for the electronic signature
   (to link the signature to the users' expression of will)
7. Logging information concerning cost sharing / invoicing.

Pete found that the legislation was very different across the different cities, The subjects covered differed, but included:

- Population register
- Identification obligation in the public environment
- Travel documents
- Privacy
- Directive for qualified electronic signature
- Measurements to use strong authentication (PKI) in e-gov environment
- Legal measurement to guide the use of official ID-cards for e-commerce.

Pete added a note to this list

'It seems that national scale deployments are required to bring down the cost per e-ID-card. Investigate the legal constraints and policy in order to get structural budget that cover a part of the e-ID card costs; the rest via tariffs for the use of the cards by the e-service providers?'

List completed, Pete faxed it off to John.

John read Pete's report with interest. His consultant had defined three scenarios, covering all interoperability situations in the given role model. He introduced the term 'not-on-us' for cards, infrastructure and for e-services which are not organised in the own e-City. "If necessary, the so called "adapters" must be implemented in such a way that one or more of the following scenarios for interoperability can be carried out in the on-us infrastructure:

1. A not-on-us card is welcomed for an on-us service
2. A not-on-us card is welcomed for a not-on-us service
3. An on-us card is welcomed for a not-on-us service

"For a deaper analysis of this point, see Part 2 Clause 9"

Pete explained, "in comparing the three scenarios it becomes apparent that although they were based on the same primary processes, the scenarios differ thatas far as they have to make connections to other Smart Card Communities, which must be interoperable:

- **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.

"This comparison shows," Pete concluded, "that, to create interoperability, you also need all the data I mentioned earlier. e-Cities who do not accept that, cannot

participate in an efficient interoperability program. This has nothing to do with politics. It is just a clean technical analysis."

John decided to visit the Ministry of Interior, to see what he could find out.

The Director General received John with his full attention.

"Yes," he told John, "we are preparing new legislation and measurements

- The legal basis for e-business, which comprises much more than the identification and so on. The conditions which will be applied for trusted third parties.
- The use of population register data in connection with certificates: who might use them and for what purposes
- Application of the e-sign directive
- The new passport, with an integrated contactless chip, for authentication. The measurements to use biometrics in pilots for strong authentication. A code can easily be told to other people. To transfer a biometric is much more complicated, and this will of course reduce the problem of false identity cards.
- The experiments with the Truck driving licence, which can be used in combination with the so-called renewed 'tachograph,' a kind of speed registration box in trucks and buses.
- And last but not least the temporary measurements to support our stimulation program. You participate in the international e-City program. But we also have our smaller-scale experiments. The risk management card for trusted tele-work in our ministry, the card for the police, and a number of others."

"Do all these cards use the same functional architecture, the same technical components and the same data sets?" asked John.

"Well, this is the responsibility of the market," replied the Director General.

"Are you at least trying, with your legislation and measures to promote the use of certain standards?" pressed John.

"As a matter of fact there is no clear picture what the national policy will be, either in the ministry or in parliament. Some want to isolate one card, purely for government-controlled services, and leave all service-oriented cards, commercial and non-commercial, to the market. Others want to make the government data available to support the services that the citizens may want. Of course, legally, both arguments have their pros and cons."

With the information Pete had prepared, John was able to argue his case.

"In order to develop interoperable services, there is a need for Smart Cards, infrastructures and PKI services that could be used for any additional services. Without an active role by government towards the cards and the infrastructure, it is very difficult to create business cases for e-services. And from the finance point of view, the positive attitude towards e-services could create a cash flow to finance

the cards and the infrastructure. This means that being passive automatically means destroying real opportunities for the information society."

The director general smiled. "We've already made calculation models for this, Mayor. You could be right. I am not arguing with you. But the fact is that we need political leadership for this policy.

"And one other thing. You are very enthusiastic about the use of information technology. If your city is sucessful, you will help create and enlarge the platform of support. And when other cities follow, it would strengthen the acceptance at national level. But don't under estimate the privacy arguments."

"I hear your point", said John, "Without support from citizens there will be no political support. I feel it is my mission to contribute to that. What I would expect in return from the national government is twofold:

1. To regulate the use of data from the citizens to create a safe and trusted 'information society'. Of course with balance between the protection of the citizens' interests and proactive anticipation of expected benefits for the citizens
2. To invest not only in card and other intelligent technology for identity documents. But also to do this in such a way that the technology can be used in combination with other services. The government defines conditions for this combined use, but leaves the content of it to the citizens.

Can you advise me on how I can promote this?"

Once again the director general smiled. "Looking to the main direction of your argument we can say that in some areas, we develop steps as you propose." he said. "The legal tools and budgets are emerging step by step. At the same time we have to serve in other areas a restricted approach. This is reality. If you want more power in the policy direction that you like, I have to advice you to prioritise the political support for your ideas.

"If you want, I can introduce you to one of my directors, who can inform you more in detail about the legislation, the measurements in preparation and the projects that we support.

John accepted the offer. "Thank you very much for your time" he said, leaving the Ministry, and heading back to his office.

On his way home, John decided to organise an international meeting for his fellow politicians. His idea was to create a kind of round table. The politicians have to be more aware about the tremendous opportunities they can create, he thought, even without huge extra budgets. Huge investments would be required for mass acceptance of the information society. But that was for the creation of broadband infrastructure. Mass acceptance of identification and trust services could probably enable or ease the commercial exploitation of broadband infrastructure. Yes, we should organise a meeting," he thought. "Get together and talk."

Chapter 7 Proposals

John realises that, in the end, the technical architecture is critical. A hearing is held in the City Hall, to discuss the requirements for the technical components. Full industry support is achieved for use of open standards and specifications of where and what technologies and processes are needed.

In preparation for the meeting, John's staff, under Pete's direction, had produced a brochure. The draft was on his desk. Its objective was to inform potential industry partners about the next phase of the e-Cities project, and to call for technologies to carry this out.

In the brochure, the processes were described as a model for the next phase, the functional model, with the 'four freedom boxes" around the basic function of IAS (identification, authentication, signature). It also outlined the business context of the next phase.

The brochure ended with a call to industry to come up with proposals for usable technology.

John was proud that his staff had managed to describe a three-layer configuration model. It was a bit technical, but it seemed logical. It was in line with the Euclid models. John believed he understood it quite well, and he agreed that industry proposals were required to fit this configuration overview.

e-City configuration components overview

"For a deaper analysis of this point, see Part 2 Clause 8"

The system is made up of three architectural layers, each with their own sets of specific building blocks as follows:

- The Smart Card layer
- The infrastructure layer, including card readers and other card interacting devices, remote servers and private or public telecommunication networks,
- The front office application layer comprising
  - the application which delivers a service to a user with a Smart Card
  - An interface to the IAS generic application which needs to be integrated in the business application and connected to its counterpart on the card for IAS processes.

End of the e-city configuration overview

The discussion of this draft overview in the staff resulted in the following statements.

Note that at the implementation level, the components of the front office application layer may be distributed throughout the card information system. In an ATM, for example, some components are located in the ATM terminal itself, others distributed on various network servers.

Services are provided to the Card Holder via two separate and different roles:

- The service provider who has identified the business needs, defines the business policy and provides/manages the necessary means for accessing the desired content,
- The content provider who keeps the content of the service up-to-date or who interacts with the user. (Note: CP plays no role in IAS IOP).

This business application component is using the IAS application. How it will be structured depends on the Smart Card community:

- As an integrated part of each application, or
- As an application to which the business application is linked at a certain stage.
- The key infrastructure application
- The standards or protocols for using the human interfaces
- The standards to be used for the platforms
- The network standards.

The e-Government / e-Commerce (business-) applications and information systems could for instance include the following services:

- Secure e-mail services,
- Access to government information (generic and specific),
- Transactions (like submitting forms, applying for permits, funds transfer and settlements),
- Keeping track of procedures and getting status information on letters and complaints,
- Contracts and public procurement,
- Distribution of information,
- Ordering and delivering of goods and services.

The content will not be considered here, since from an interoperability viewpoint, it is only accessible to the user via the service providers application. From a technical point of view it is important:

- To connect to the IAS-application
- To secure the channels
- To integrate the proces of IAS and the checks of the certificates for as far as required
- To log and hand over the required management data

John had already realised that it was a drawback that he had to work alone so much for his own e-City. Yes, there was the e-City yearly meeting, and the odd conference like the Euclid one. But that was just for information exchange, PR and funding requests from other official bodies.

Seeking more intensive cooperation, John sent out the draft brochure to the other mayors, explaining his intention to organise an industry hearing about the technology to be applied.

As expected, given their longstanding rapport, Mildred supported him.

But the reactions from the others were quite neutral. He had left Ben till last.

“John, you’re making it much too difficult for yourself. Either concern yourself with your own city, or else create an all-encompassing project for all e-Cities, with contributions for all of them. And, by the way,” Ben continued, “the configuration overview in your draft brochure is much too vague for the industry.”

John called all his colleagues again, and proposed to prepare a generic white paper with ideas, concepts and proposals. They accepted.

Help arrived from a surprising source. John received an e-mail from Ben. “As I said on the phone, your configuration overview must be more tangible,” he wrote. “But please don’t think I can’t be constructive. Here are some of my thoughts on what should be in it. You may wish to consider it, and integrate it with your plans.

"For a deaper analysis of this point, see Part 2 Clause 8"

Memo to John on e-City technical requirements

The following criteria should be taken into account when deciding on the technical components for smart cards, readers/terminals, networks and front office.

1. Smart Cards

- ISO 7816 1-3
- Contact (ISO 7816) and contactless (IEC 14443)
- Directory/File structure for multi application capabilities
- PIN Authentication (number or biometrics) of Card Holder
- Key algorithm for operations in the Smart Card: for asymmetric algorithms, hashing and padding see relevant Workshop E-sign documentation.

2a. Reader / terminals

- Secure communication between chip, keyboards, and display (In case of using the screen/display and/or the keyboard of different building block(s), the links must be secured before the interaction starts.)

2b. Network

- Handle secure communication between terminal / network server (for 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)
- Support of the terminals in presenting the accessible e-services offered to the Card Holder
- Network (services) management
  - IOP adapter
  - PKI adapter

3. Front office

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

a) e-service front office applications (exploited by the service provider)
b) Network service (exploited by the access provider, as presented above)
c) PKI: certificate verification services (exploited by/under the responsibility of the Card Issuer)

End of memo

Ben's e-mail gave John a lot of food for thought. He decided to widen the base of participants in the upcoming meeting. Since the aim was to find technological solutions, the meeting included card suppliers, terminal suppliers, the chip industry, software industry, tools, and telecommunications industry, many with expert representatives.

A small group of mayors met up in a conference room in John's city hall. The surroundings were nothing like those of Professor Rupert's campus, but the big reunion was yet to come.

The meeting decided that the technology must fulfil the following requirements:

- 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

The mayors realised that these words needed to be translated into practice.

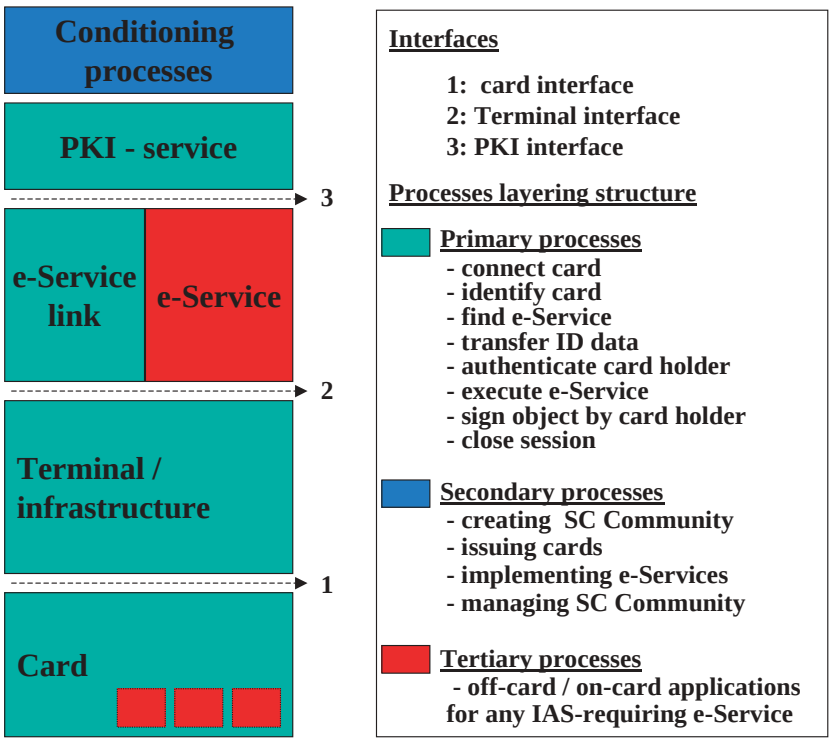
"A number of these criteria could have consequences for the use of standards," said Hiro, who had travelled from Japan. "These are portability, modularity, vendor independence. This meant that these components have to be defined very clearly in terms of input, function and output. For a number of components, this is not much of a problem, because there already exists a standard or an accepted convention."

"But," interjected John, "there are a number of components in the concepts that must be elaborated carefully, and accepted by the e-Cities. If the e-Cities want to base themselves on the cards and infrastructure supported by the governments' electronic ID, this means that co-operation in official normalisation bodies is strongly recommended."

Mildred spoke: "Let's look at the topic of the 'four freedom functions' around IAS. The problem is that the interfaces are not yet specified, and especially not as a standard." The mayors heard that in some areas, there were some standards available in the market. The industry partners did not come to a real recommendation on this.

The discussion on what components should be open and what could be proprietary did not lead to spectacular results. It was recognised that the impact on the total system, and even for the working of the role model could be considerable.

The ball was back in the e-Cities' court. But one thing they did achieve at the meeting was a first draft for the implementation. Mildred drafted this diagram.



"The grey boxes on the right hand side represent the three configuration layers," she explained to her colleagues. "They are separated by interfaces that must be defined and applied by all e-Cities. The middle box represents the service in the front office of any service provider. It must contain a connection mechanism (the grey box) to the other green boxes in the column. The top grey box represents the Smart Card management applications, which condition the total process. The arrow on the left hand side represents the primary process, handled by the boxes in the architecture."

At the close of the meeting, John felt something had been achieved. They had agreed on consulting industry experts while making the technical specifications, based on open standards "Now I'm ready to step up the programme at City Hall.". Mildred and Hiro wished him luck, and promised to keep John up-to-date on developments in their own e-Cities.

Chapter 8 SCC and the Cities

John explores and formulates policies required to set up the operational card scheme that will meet the e-City requirements for sustainability, interoperability and growth of e-services.

At City Hall, it was common knowledge that Mayor John had placed the e-City program at the top of his list of priorities. It was the conversation topic among all his closest staff. At daily brainstorming sessions, John shared with his thoughts with them. And little by little they became more and more focused in the same direction as the mayor.

One morning, during one of these brainstorming sessions, John raised the issue of a complete and balanced policy. “What statements should be decided on by our city parliament?” he asked. “What do we need to cover?”

The group made a list

- Goals of the e-City program
- Strictly IAS or more in common?
- E-gov only as it is now or adding new services dynamically
- Commercial services or not
- ROI objectives
- The target groups / customers
- Limited groups primarily determined by the scheme operator as it is now
- Groups following the e-service providers?
- The involvement of stakeholders
- Strictly doing ordered tasks as it is now
- Own responsibility for all stakeholders, with orientation on total customer value
- Nature of mutual relations
- Who and how to involve
- The security policy
    - How to secure entities involved
    - How to link persons to card
    - Link to link signature to card
    - PKI for all entities
    - Certificates on the card
    - Issuing procedures
- The legal policy
- The technical policy
    - Standards and conventions policy
    - What components that are deployed already would be continued?
    - Policy on replacement components / What should be adapted
    - Development / test bench

- ❖ Co-operation (interoperability arrangements) with other e-Cities
  - Targets
  - Required conditions
  - Test policy
- ❖ The policy toward Card Holders
  - Type / level of service
  - Privacy
  - Complaints
- ❖ Financials
  - Investors /level of investments
  - Cash flows

It was quite a list for a few minutes of brainstorming. “That’s a lot to work on,” said John. “Let’s set aside tomorrow morning to work on this exclusively. It needs to be done soon in order to prepare my proposal, but hopefully not at the expense of every other city activity!”

“So, will I finally get to meet Euclid?” Pete asked, after the others had left.

“I cannot promise anything. She is a woman.”

“I’d better not tell your wife I heard you say that!”

The two men laughed.

The following morning

The following morning, John’s core staff split into three teams; one for the Card Issuer oriented policy issues, one for the service provider and one for the cardholder and other stakeholders. They distributed the subjects. Most of the policy questions were issuer oriented.

In the plenary session afterwards, the groups met up again. The Card Issuer group presented their findings:

“Well Mayor,” said the young intern who had led the Card Issuer group. “We looked at the issue from the view point of the Card Issuer. In our discussions we discovered that the Card Issuer should be concerned with the following six areas.
One, the targeted customer base. Whether the base should be restricted or open to all citizens and whether it should be voluntary or compulsory.”

“The second major area of policy interest concerns the involvement of

stakeholders and the card Issuer's relationship with each of 3 major stakeholders: the Certificate Authority, the Service Provider and the Card Holder. In short, the CI is fully responsible for the card and the IAS application. "

"The third major point is security policy. We came up with some initial policy statements. But we are sure that we have not been exhaustive yet."

"Fourthly, legal issues. Our statements not only cover the legal entities, the contractual relations, the bylaws for the total group of stakeholders, but also ownership of cards and the different types of data."

"Five, technical policy.

"And last but not least, the final area we identified is co-operation. In other words, interoperability arrangements with other e-Cities.

The second team had focused on the Service Provider. "We have identified several area of policy importance. The first major issue is 'Who can participate?' In principle, we suggest that all e-services may participate, if they require IAS and agree with the Card Issuer on the use of generic IAS."

"That's what we think too, from the Card Issuer viewpoint," the first group agreed.

The leader of Team 2 continued. "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. When more than basic ID is required, other rules must be complied with.

"We also noted that, as there for the Card Issuer, there are legal issues involved for the SP. The SP must comply with SCC bylaws where it is registered. We must also cover areas such as ownership of data – this must be handled by the issuer."

"And there is the relationship between the SP and the AP, the Access Provider, which is principally a technical one, but nonetheless an important one."

'I agree" said John, turning to the third group for their input.

"Our focus was on the policy implications related to the Card Holder. We also looked at other stakeholders. The CH is central to the whole process, if we continue to look at smartcards as a service oriented venture. The CH also

has responsibilities – to apply for and register for the card, to use it correctly and legally. Before accessing a service, the CH must follow instructions and bylaws relating to the use of the service. This is particularly important in a not-on-us service.

"As well as responsibilities, the CH has rights. Access to a variety of e-services. Secure access. And access to quality and correct information. There must be a secure environment and free decision about ID giving. The CH must be able to 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."

"And the other stakeholders?" prompted John.

"Yes, these are the Access Provider which will make contracts with the Card Issuer and the Service provider; and the Certificate Provider, who is contracted to the Card Issuer. The SCC Administrator gets a contract from the CI. The administrator has the right to monitor all major processes against the goals and agreements

- ***Autonomously***
- ***At request/complaint of users***

The administrator takes any appropriate corrective actions."

After the three teams had completed their presentations, Pete spoke. "This is good. At last we have something which we can concentrate policy statements on."

Mayor John offered to summarise the group's findings in a strategic memo. "That's it," he said, closing the session. "Thank you."

Chapter 9 The Rapids

Privacy is raised as a major concern. John facilitates an open meeting to debate the issue. Guided by the European directive, he succeeds in getting agreement on how to manage shared responsibilities to control the storage, processing and use of personal data in his e-City program.

Work proceeded on the policy statements, but in the meantime, the subject of privacy came up in a very real and urgent way. John chose to handle this subject pro-actively, in order not to destroy the chances for his proposals when they were brought before the parliament.

A letter to the editor of the local paper started the controversy. One of the citizens had recently gone abroad to another city, where he used a local city service card. In that city, cards were offered per service or group of services, all under the authority of the e-City program of that city. The letter writer had had some problems with the card. Most critically, his personal data appeared to be available to companies he had never had contact with.

"This was bad enough," the letter read. "Naturally, I wanted to complain. But what was the procedure? I contacted the local mayor's office, since the mayor, a mayor Ben, was the board advisor of the e-City program. But the mayor did not have the power to do anything for me. The service provider had hidden itself behind unclear bylaws. Now, back in my home city, and being confronted with an even more intensive use of e-City cards, I would like to ask publicly what the risks are. Is the same – or worse – going to happen here?"

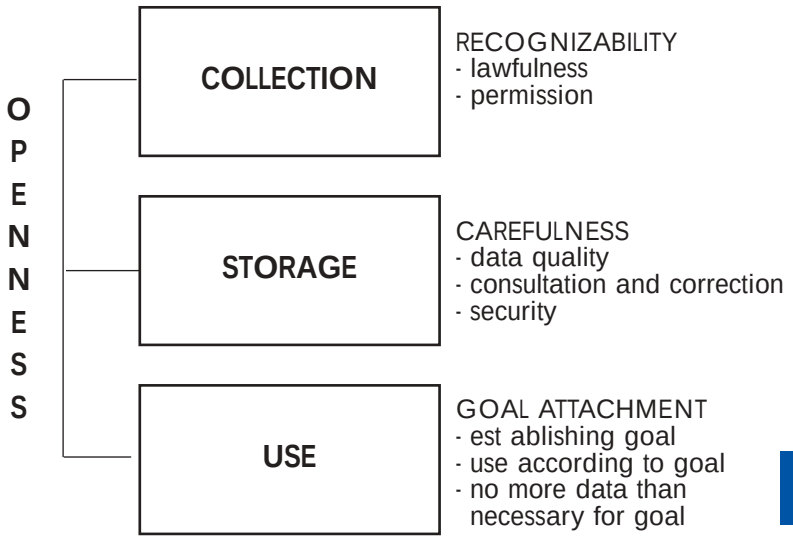
The next day, there was a report on prime time TV about electronic banking. "The banks use their Smart Cards and a dedicated encryption box to protect the home-banking process. When this process is executed via computers in a private network, then there are conditions under which users of the same network can tap into the clearly readable information flow." The reporter concluded: "Smart Cards do not protect you. Smart Cards are a danger to your privacy."

Although the two issues were not directly linked, John's citizens were worried. Calls flooded into the mayoral office. Every time John turned on the radio, he heard the same questions and concerns. The problem snowballed. The issue reached parliament and official questions were tabled. And mayor John was the one who had to answer them.

But John saw this as an opportunity, not a crisis

He decided to open communication with all his citizens. First, he called a press conference. He knew he was sure to get a lot of attention, but he had nothing to hide. On the contrary, he believed he had a lot to gain.

He had prepared a diagram, to help him visualise some of the issues, which he was sure, would be raised at the press conference.



"For a deaper analysis of this point, see Part 2 Clause 10"

All sections of the media were present: newspapers, radio, local and national television.

John spoke. “Recent discussions have put a question mark over the use of Smart Cards. It has been said that they are not secure and that they violate the privacy of our citizens”.

“This is not true. And I’ll tell you why.’

“First this. The e-City program in this city is focussed on specific groups: doctors, nurses, patients who need post-operative care, parents concerned with the education of their children. But the program is also there for our convenience, for example ordering concert tickets online. The card is beneficial to every group. And the range of services available is being expanded all the time.

Secondly. Let me tell you about the security measures we have taken. Anyone can see and check that we do not take risks with your interests.

The measures cover two areas:

- ***The technical and organisational measures that must prevent the disclosure of any information between you and the service provider with whom a contract is made***
- ***The contractual and legal measures that prevent the service providers and any other stakeholders from doing anything with the data that they received from you, which are not agreed with you, or which is not in line with the objectives that he has communicated to you. This area also includes open and fair compliant handling."***

Here the mayor stopped and looked around.

"Can you guarantee that in this city secret information will never be tapped?" It was a young television reporter, looking at his own camera, not at the mayor.

The camera zoomed to the mayor again. "We have taken very serious measures in order to give our patients and doctors and parents better service than they had before, with all available security. At the core of these security measures is an individual certificate that is given to all stakeholders. Including of course the citizens themselves. This certificate is stored on the Smart Card of the citizen. It is issued in a secure way. And protected during its life cycle. That certificate protects all data flows. I have got documentation here for your experts to check, and discuss freely the capability of this PKI-technology.

"The rest of the measures have to do with the use of data. We apply a code of conduct for all service providers. This exists already, but I am working on a new release. The new version will now be based on and backed by the latest legislation. Their definitions will comply with the new legislation. This concerns several issues and includes the principle of the citizen's right to know about his data."

"How does this work, Mayor?" another journalist called.

"The processes are related to

- ***The data collection: recognisability (permission, lawfulness)***
- ***The data storage; carefulness (quality, security, consultation and correction)***
- ***The area of use: goals to which all service providers and other stakeholders have to aim.***

"Again, for this, I have documentation available. Ladies and gentlemen, as you know, the city parliament is preparing a new code of conduct."

"Mayor how can this code really guarantee that citizens will not be tricked by some bad service provider, who goes and sells all the data to a crook?" It was the talk show host from the local radio.

Major John smiled. “We only accept first class service providers in our program, as you know. But, of course, the user will soon be free to choose other services for which he or she wants to use the card. These services are not under my control. If the new policy is accepted, all e-Cities will follow the same policy in compliance the legal constraints in all countries. The keyword, in my opinion, is ‘openness’.

“Any Service provider must publish the information about their goals, the data they stored about the citizens and the use that they intend. We can enforce that openness by law, backed by procedures that we will establish.”

“So, you introduce this so-called PKI technology and a new code of conduct, and then you sit back and see what happens?” It was the young TV presenter again.

“In our new program we oblige all service providers to present a consumer notification on the screen when the user wants to register for the service. We have prescribed what information must be published, as I indicated already. This means that the user always knows what he is doing and can decide if he wants to continue or not. To ease this process we have developed a logo for those services which apply the qualified standard, which really are consumer friendly.”

“Does that mean that you always have to register for a new service?” It was the turn of the newspaper journalist.

“There are services that only require your name and address, without checking if you are really the person the card belongs to. For these services you can avoid repeatedly filling in forms, with the same range of data every time. And always making the same mistakes in typing as I do!”

People laughed.

“Compare it with giving your passport to the hotel, to fill in the forms. Or your driver’s licence to the car rental agency. It is your choice to allow the service provider to take your name and address from the card. If you do not want to do so, you must not give the card. It is primarily your own responsibility. The good thing is that the legal requirements for the protection of privacy apply. The receiver is not free to share or sell this information, and you as a citizen can check that.”

“To be honest, mayor, this doesn’t sound very well controlled!” the talk show host interrupted loudly. “Anyone can easily read your name and address. Crooks can tap simple computers, in which the easy to get names are stored. Compared to traditional documents with names, which of course also can be stolen, the scale of this new type of fraud could be much higher!”

"In principle this is not a difficult problem to handle. But it is a serious issue, in which you have to make a decision. You can say: the fact that I offer my card is my positive consent to take my name and address from the card. All additional positive expressions of will need additional positive actions of the Card Holder of course. But you can also say: the name and address data in my card are always hidden, and just open with a positive action via the human interface. This can be a variety of things: a simple keystroke, or a pincode, or even a biometric. This last method requires additional equipment of course. We made the choice for the most simple solution at the level of name and address. But we are open to alternatives, if that is what our citizens, via their representatives, want. It is a question of measuring and balancing the benefits."

"Can't you be anonymous when you use the card?" It was a reporter from a computer-oriented magazine who asked this. The mayor smiled again.

"A very interesting question. In fact the Smart Card is the only tool with while the service provider can still be sure that he can trust you. This procedure can be studied and elaborated when society really requires it. We do not have the budget to consider it now in our e-City program.

"Another advantage of the cards is that you can afterwards reconstruct your transactions, if you suspect that the transaction was wrongly handled. For example they charge you, via an indirect procedure for 5000 Euro instead of 50,00. Unlike a face-to-face transactions, it's all there to prove or disprove. It can actually enhance transparency."

The press conference ended with the usual practical things: photos, quotes for radio and TV, the distribution of press packs filled with information on Smart Cards.

The next day

When the morning's stack of papers landed on his desk the next day, John was rather pleased. The story had been widely covered and was in general very positively handled. The same was true of the radio and TV. Some journalists had made extra investigations. They informed readers, listeners and viewers about the European directive, and made comparisons of the legislation in the member states.

Some focused on measures in particular branches, others on future developments that had to be anticipated. And others called on experts to determine where the risks are, what benefits can be reached, and how the legislation can rapidly be adapted to changing circumstances.

What had started as a crisis had turned out to be a PR man's dream.

Chapter 10 The Round Table

John, Mildred and Ben meet Euclid again via video and audio conference. John gets a clear picture how to direct the mission document that he had first drafted at the campus, to vitalising his e-City program.

John was busy at his desk when the phone rang. It was Mildred. “Hi John. How are you getting on?”

“Yes, indeed,” replied John, “we’re coming up to our deadline now.”

“Here as well,” said Mildred, “I have to prepare a plan for the card base, and for the terminal infrastructure in my city. As far as I can see, I’m going to have to triple the number of cards, and to double the number of access points in order to raise the frequency of use per card. And I must reach these goals within one or two years, in order not to lose more money than I can raise from local sponsors.”

“Remember what Euclid said the last time we contacted her?” John suggested. “She said that by studying the range of e- services, we might find the solution to this question of growth. The more units are produced, or the more each is handled, the better the results per unit are, or the lower the costs per unit could be. All big companies base their strategy on these type of notions.”

“Or in reaching such a scale that they can dictate their prices and conditions to the market,” Mildred put in.

“Yes I know your argument there. But I really think that what Euclid has in mind is that combining all services leads to accelerating the learning curve. In the conversation I had with her she emphasised the importance of interoperability. I am beginning to see a relation between these two interventions. And we are far from controlling any market. In the contrary, our problem is to get the market started.

“For the moment we are really focussing on people who enjoy the pioneering with advanced technologies. They are interested in all sorts of subjects. Health care, education, culture.”

“And, in our city we just have some niche groups who have a real business based attitude towards the e-services. I’m sure it’s the same in your city, Mildred. Real estate agents are a good example. They are using the e-City card to get online land register information, based on strong authentication on the requester. This is because this database is not public, at least not for all

information. We must define a strategy to stimulate the growth. I think the way forward is via interoperability and learning from the results with the services over all e-Cities."

"I'm looking forward to seeing the results of this overview of services. I'd like to share with you our part of the analysis. As you remember, we also include commercial services in our city, which you have always refused. I am curious to compare results, and I'm sure you are too."

"Yes, I'll have that ready by this afternoon, Mildred. Listen, I have an idea. I'd like to organise a conference call on this subject for next week and include Ben. He has been extremely helpful, especially for a Smart Card sceptic. He sent me one very useful document by e-mail. Do you remember, I forwarded it to you? And as his approach is very service provider oriented, I think his point of view will enrich our analysis."

Mildred agreed, but suggested they try a videoconference. "I'd like to include my whole team. And, remember, the use of webcams as an e-service was one of the first things we discussed back at the Euclid meeting at the campus?"

"Yes," recalled John. "That's a great idea. I'll get going on it today."

John arranged a videoconference between the three city halls, with three professional webcams. It was less complicated than he had expected. It appeared that the internet tools supported this quite well. And the experience curve with WEB technology was apparently so far developed that not only was it easy to install and use, it was also quite cheap.

John initiated the call. Ben appeared on screen first, sitting at his oak table in his prestigious modern office, surrounded by huge glass windows.

"Welcome, Ben, All OK with you and your city? We are going to contact Mildred now."

On screen, there appeared a complete meeting room. Mildred and seven of her action team sat around an oval table. The antique appearance of the woodwork contrasted effectively with the array of modern technology arranged around the room.

"Wow!" Ben exclaimed. "What is this? A surprise party? I thought we were here to simply talk about a list of services that we could share, and assess the results."

"Yes, Mildred said, "Sorry you did not expect us. I always involve my 'combine and connect team' when the direction of our e-City is involved."

"And we welcome you all," John said, "I appreciate that you are prepared to spend time in sharing your insights with other e-Cities. I hope it will be advantageous to all of us. And I have to apologise to you, Ben. It was a mistake not to inform you that Mildred was going to bring in her team."

"OK. I don't want to be rude to Mildred's people. I was just surprised."

"Let's start. Mildred, could you briefly introduce the people at your table?"

"Well, going in the circle from left you see our experts in:

- E-services business issues
- ID-issues and legal issues
- ICT and infrastructure issues
- policy making issues (my direct assistant,)
- human resource and organisation issues
- change management and innovation issues."

She named her staff as she went along. "All these people belong to the initiative group for our e-City participation. They cover a range of disciplines, which in our opinion are needed for good consideration of the direction in our policy. Two members of this team participate in the high level board that we have at the top of our functional organisation. Of course the city parliament has the final say in everything. In our city we bring commercial and e-gov services to the citizens, based on one common card, which contain the ID-data of the cardholder, plus some additional data for authentication."

It was Ben's turn to speak. " My city works very well without all these complications. When there is a service provider that wants to participate in our e-City program, I introduce them to the others, put them on the list of cards and services, and off he goes. The newcomer issues his cards, co-ordinates the eventual co-use of terminals from other existing service providers, pay to other parties for that co-use, and off he goes."

John spoke: "In my city we just have one type of card. This is something we have in common with Mildred's city. Our services are all related to e-gov, and sectors where we as government are directly responsible.

"As discussed with you, the goals of this meeting are:

1. Missions of e-City and determining how far 'interoperability' is involved
2. Strategy, especially what we could offer to services when we could be interoperable
3. Technological consequences when we would be interoperable
4. How to approach financial challenges, when going interoperable.

Let's try to find the direction and the determining elements.

"OK, the first mission then. You all have the list of potential services. No sector was excluded. We defined our mission after a first investigation of demands and needs for services.

- Entertainment
- Teleshopping
- Teleworking for small companies
- Services for elderly and disabled people
- Health care
- Transport
- Tele-education
- Sport information
- Telemagazines

Mildred took up the discussion. "A self-investigation questionnaire was developed by the pioneering team. In that questionnaire were built in some assumptions about the price the e-service provider has to pay for the use of the identification and authentication plus the infrastructure. When the service in question filled in its own parameters, it became clear whether the service provider could have a business case. If yes, the service provider became a prospect for the use of the common card, infrastructure and generic identification data. For these prospects we made business opportunities plans. And then we started our mission definition."

Ben interrupted. "I'm sorry to interrupt, Mildred, but this is not what I would expect from a mission. In my city it is simple: I have to maximise the services for my citizens, with the minimum of city budget."

John spoke. "Ben, I don't think that your mission approach is that different from Mildred's. You simply wait to see who comes to you, whereas Mildred's team contacted all the possibilities they had identified. For the rest, both of you are very much business oriented.

The chief difference, if you will allow me to bring this forward as chairman, seems to me that Mildred's mission includes the common card and infrastructure platforms, whereas yours does not."

"And what is your mission then, John?" asked Ben

"My mission is to serve targets groups which are related to the task areas of the city hall, and I have to do that with a common card and common access technology. I cannot go outside the groups that are direct subject of city hall

responsibility. I am now developing a new vision for the services and I will try to adapt the policy in order to continue to offer the services our citizens want. Otherwise, there is a danger that I may have to close down my e-City project after the subsidy stops.

"Any more questions on this subject, guys? Or are the elements of our different missions clear enough without going into further detail? We really have to wait until the statistics are on the table: Per service segment, number of registered users, starting level, growth figures, level of promotion, value for the users, tariffs, and so on. My staff has started a quick investigation, and will send around the results. I hope you will find them useful."

John paused. "Next: strategy. Mildred can your team give us some insights in your 'bottom up approach?"

Mildred spoke, drawing on a document provided by one of her team. "We defined the framework for the common identification, authentication and electronic signature function. Also for the access infrastructure. The town hall is the Card Issuer, and we use population register data for the official identification data. We have made contracts with access providers, based upon one leading party per segment: health care, public buildings, education etc. We have one contract with a PKI tool provider, which is based on open software. We do the PKI certificates ourselves, in the city hall. We have made contracts with a number of service providers, as mentioned. "

" And Ben?"

" Well, I suppose you need quite a large dedicated staff to support the common card, and co-ordinate the access providers? Could you tell me how your financial policy can cover this, which I expect is a rather heavy burden? "He turned to John. "And John, what is your strategy?"

"My strategy is not too different to your own, Ben. It is directed to bringing down the costs per unit of use. As far as I am concerned, this goes for the common parts like the cards, the issuing and other elements of card service, for the certificates check, and the use of terminals, the operational management of the terminals. Within the limits that my city council gave me, I try to make the card be used as much as possible."

"And have you managed to make your program self-financing?"

"No, not yet, and not within the limits of my target groups."

"This is what I thought already. Allow me to say bluntly what I think. Your strategy looks too much to communist central planning. You want to control every thing." Ben stopped. Looked in the web cam, nodded his head for emphasis,

and continued: “Leave it all free. That is much easier, and more effective. The market does the work.”

There was a buzz of astonishment and anger from Mildred’s conference room as they all started talking excitedly. After a moment, Mildred calmed her team. “Now it’s my turn,” she said firmly. “I’d like to pose a question: Ben, do you think that your citizens would like to take advantage of the US business news clipping services, which we offer in cooperation with Nascorp. Inc?”

“Yes, probably there will be an interest in this. Send them to me and they can issue cards in my e-City program.”

“Well, Ben, this is exactly what they don’t want. Their business is news clipping. Of course they would welcome your citizens, but they don’t want to issue cards. It makes no sense to ridicule John’s work with your pseudo polarisation of successful capitalism against caring but misguided communism. Do you see the interoperability problems that arise when you only apply some common technology standards? It would be much easier to persuade the service providers to exploit their e-service in your program if you could offer them the use of cards, infrastructure and certificates, based in standard interfaces. Both are business cases which we must develop if we want to successfully exploit the capability of interoperability.”

After this little scrimmage they went through a fruitful exchange of views on technologies. They agreed that they all wanted to reach two objectives:

“Firstly,” said John, “we want to make different categories of cards, not primarily based on the requirements as defined per service provider, or per segment but per level of identification and verification of the user and the electronic signature belonging to the card (so called authentication). Probably two levels of cards can cover all services in the e-City:

- Low level cards, for identification of the card only, for access to those e-services that require no further identification
- High level cards for access to high level services, requiring strong authentication and/or qualified electronic signature.

“Secondly, we want to neutralise the type of card reader technologies in the infrastructure. Create interoperability for contact and contactless cards, and other technologies that may be applied. Of course with the restrictions of the infrastructure involved. You cannot put a contact Smart Card in a contactless reader. But you should be able to access any e-service with either type of card.”

“Interoperability strategy also concerns the financial relations between e-Cities,” Mildred added.

Ben proposed: “Why not apply the telecoms principle of ‘sender keeps all’? This means that you charge extra money to the user who wants to access a

'not on us' service, or use a 'not on us' infrastructure. And you keep the money yourself, in order to cover the extra costs that you incur by serving users that access services you handle in your e-City. This is simple and effective."

John disagreed: "This is only feasible when the mutual traffic flows are more of less balanced. In skewed patterns there will be a problem. I am not sure if it can work out when you have a variety of card operators running their own services, and other card operators who exploit a multi-application card scheme, based on common identification, authentication, and electronic signature. We can sort out how this can be handled in practice, but can we agree on a kind of business account per level of service?

"I suggest the following"

- Cost per issued card, preferably even per service for which the card is registered by the Card Holder.
- Costs of the infrastructure, preferably per access
- Cost of the authentication certificate in the card, preferably per check of any certificate
- Ditto for the electronic signature
- Cost per unit of e-service
- Cost per interactive expert service"

The list came up on the computers in each of the mayoral offices. John continued, "These distinctions can also be expected in an interoperability situation. The e-Cities could make arrangements to compensate their costs."

"Let's make a more detailed study," suggested Mildred and her team, "in order to cope with interoperability between the different policies in the different e-Cities."

"I think we should get Euclid on the screen. She's obviously turned your head, John," said Ben. "I suppose I should listen to what she has to say!"

John managed to connect to her, and her features lit up the screens in three cities scattered all over the world. John, Ben, Mildred and her team all looked at her in anticipation. The web cam did not register the faces of the meeting in Mildred's office. But you could hear them whistling.

"John," she began, "if the others agree, I would like to invite you to present a generic mission document. At the next meeting with Professor Rupert, we will use the document as a discussion text. In it, you should integrate all common policy elements among the e-Cities. I hope you will find the following points useful. And of course you will have the valuable input of your colleagues."

The text came up on the screens simultaneously

"For a deaper analysis of this point, see Part 2 Clause 11"

The Smart Card community

- What type of problem / solution is addressed / basic quantities
- Legal entity / Ownership relations
- Mission towards e-services to be offered
- Mission towards cardholders / branding

Products and services: requirements / basic choices / basic quantities

- Basic offer: cards and infrastructure
- Trust offer: card management, PKI, e-sign
- E-Services offer

Marketing

- E-services segments to be addresses
- Product / segment matrix
- Positioning
- Quantities

Creating the technical environment: buying/ building / altering/ adapting

- Cards
- Infrastructure: card readers / terminals, network services
- Front office for card issuing / card management / RA / development and compliance testing

Development strategies and strategic tools

- Towards user groups: Action research yes / no
- Towards e-service suppliers: smart factory yes / no
- Towards technical suppliers: accelerated development

Global financial plan template

Organisation plan example

Action plan template

Then she disappeared.

Ben leaned back in his leather chair and grinned. “She does enjoy playing hard to get, doesn’t she? It’s a pity she is only virtual reality…”

“If she were real, would she have anything to do with you?” asked John, in a rare moment of levity.

“Why not?” said Ben, looking more positively at the whole issue than he had ever done before. “Smart Cards could be the best thing that ever happened to me!”

The End

Bilthoven (The Netherlands), November 3, 2002.

PART TWO

SYNNOPSIS OF GIF

By Marc Lange
04 december 2002

TABLE OF CONTENTS

Purpose of the document

This document is complementary to Part 1 and establishes a direct and easy link between it the novel "EUCLID and the e-Cities – A fable for decision makers" and the formal "Global Interoperability Framework for Identification, Authentication and Electronic Signature (IAS) with Smart Cards" as issued as part of the "Open Smart Card Infrastructure for Europe" (OSCIE) which defines the common specifications necessary to accelerate and harmonise the development and usage of smart cards across Europe.

The "fable for decision makers" is the fiction of some weeks in the life of Mayor John. He is struggling to create an e-city program with "the reliable keys' for his citizens. For sustainable success the reliable key should be e interoperable and self-financing. The scene of mayors has been chosen because the subject of this

booklet is “strategy building for a card operator” The e-city is the metaphor for this scheme, and the mayor is the one who has to integrate the interests of e-service providers, with that of infrastructure and card base operators.

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.

Since this document includes all key elements required for understanding the essence of the Global Interoperability Framework, it can also act as an executive summary of it.

1. Introducing GIF and eESC

The Smart Card Charter is an activity within the European Commission's eEurope initiative. For more information, see http://eeurope-smartcards.org/.

The e-Europe Smart Charter (eESC) initiative intends to have a decisive impact on the harmonisation of the European "smart card landscape", to allow for economies of scale and most of all to boost citizen confidence in IT. Card applications have developed in various different areas and are foreseen to become the intelligent key to a quality of life in the information age. The scope of the eESC initiative is correspondingly vast. It encompasses the use of smart cards in secure public identification and authentication, e government, e-payments, health, transportation, etc. considering technical issues such as interoperability, security certification, card readers, multi-application, contactless cards and consumer requirements for easy to use services

The **"Global Interoperability Framework for Identification, Authentication and Electronic Signature (IAS) with Smart Cards"** is part of the eESC Common Specifications to be concluded at the end of 2002 and launched early in 2003. Its aim is to facilitate interoperability between the various IAS schemes emerging in Europe and more widely throughout the world by providing the following guidance:

- **Preparing information systems for interoperating**
  i.e. providing the rules and standards which should be used within information systems in order to be able to guarantee IAS interoperability for internet transactions;
- **Organising the operation of this IAS interoperability**
  i.e. the ability of a smart card community to verify the identification and the validity of the authentication and electronic signature of a member from a different smart card community.

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

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

2. The Value Chain

"For a deaper analysis of this point, see GIF, Part 4 Clause 2.3"

For setting up a business strategy, a smart card community can take advantage of the concept of the value chain. It can be defined as a chain of business activities, oriented to the added value of every element in the chain. The sources of value are (and /or):

- Reducing complexity, creating higher scales … (cost leadership)
- Innovation / to gain the premium that the customer is prepared to pay, often oriented to niches (differentiation leadership)
- Perception of value as seen by the customer.

The value chain can be modelled as follows:

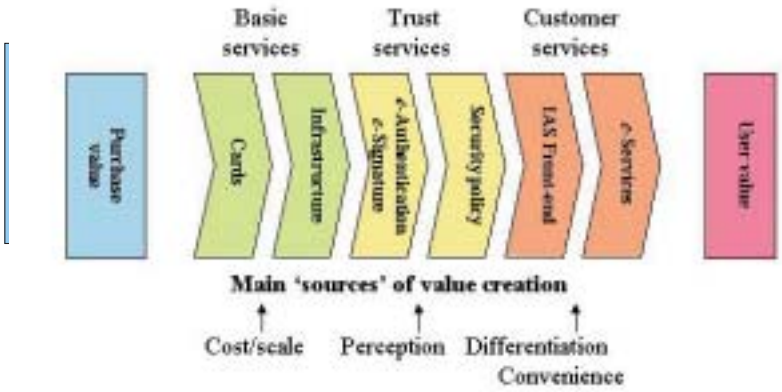


Figure 1: The Value Chain

- **Basic services**

  Traditionally the value chain was limited to smart cards and infrastructure. The issuer does not offer to the card holder any choice in the application or e-service. The application is ultimately aimed at providing benefits to the card issuer, for its own benefit (e.g. payment, social protection or health insurance identification and entitlement, loyalty programmes). The value creation chain is mostly oriented to cost reduction for the card issuer and *"creating more value"* in this chain often means *"lowering the cost of the smart card and the infrastructure by standardising and enlarging the scales"*.

- **Trust services** (i.e. Generic identification and authentication and electronic signature)

  These services are currently often directed to special services with a limited amount of users, e.g. e-Market networks (purchasing, b2b ordering, etc.), closed subscriber groups, secure internal company (tele-) networks, secure e-mailing. They are indeed rather expensive and targets environments with high interests and high risks. Mobile telecom is the only segment where

some trust services (with the SIM-card) are applied on a large scale, but they are limited to
identification without strong authentication or qualified signatures. In ALL other segments with low priced security products (via the internet), the offer and the acceptance seem to be fragmented. Therefore, “creating more value” in this context requires
“disconnecting the trust services from the basic services”
(e.g. on the basis of interfaces to OPEN standards).

- **High-end Customer services**

  These services come at the end of the chain and are therefore expensive to implement. In a large number of situations, this is a solid barrier to their deployment! Currently, they are to be paid either by the customer (i.e. the card holder) or a card issuer which has a solid business case
  (e.g. governments). Therefore, similarly to the previous case, “creating more value” in this context requires *“disconnecting the customer services from the trust services”*
  (e.g. on the basis of interfaces to OPEN standards). This would indeed open the door for sharing costs between all those who offers e-services to the same card holders.

3 Roles model

"For a deaper analysis of this point, see GIF, Part 1 Clause 4.2.2"

The figure below models the basic roles required for the functioning of smart card and e-service communities. Some of these roles are “content” oriented and others “issuer” oriented. The latter roles govern the business conditions and technical implementation means. Note that these roles may be fulfilled by the same entity. This is an implementation issue which does not impact the roles model.

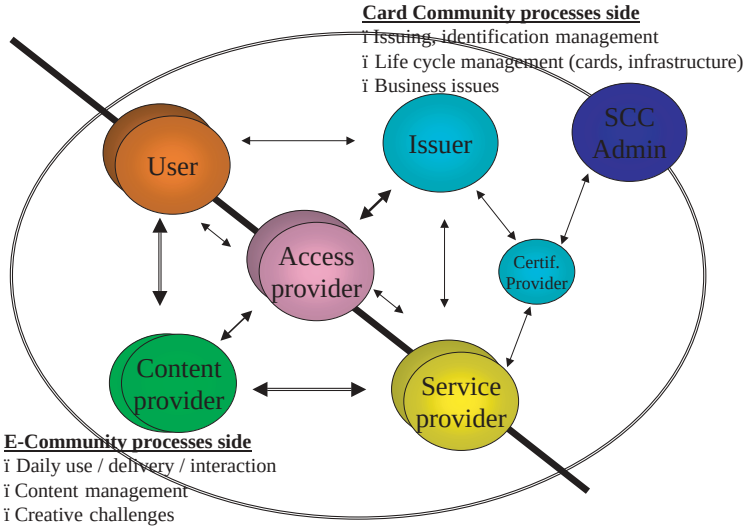


Figure 2: Stakeholder' roles

❖ The Card Holder

The Card Holder or user is a physical person (in the legal sense, i.e. an individual human being not a company/legal structure) who has been issued a smart card by a card issuer. The issued smart card is associated with and issued to the specific card holder and to him/her only.
This association enables the card to be used by the card holder for IAS purposes and thus to enable him/her to access services provided by the service provider

❖ The Card Issuer

The role of the Card Issuer is to issue smart cards to card holders. While the card issuer holds the legal responsibility, most of its operational tasks are likely to be delegated/sub contracted to specific entities such as a card manufacturer and/or the certificate provider. The card issuer has the responsibility e.g. to:

- Register card holders: i.e. obtain sufficient proof of the identity of the card holder by traditional means. This RA function may be operationally delegated.
- Generate IAS (data, functions): i.e. triggers the key generation and issue certificates associated with the card holder. This CA function may be operationally delegated to a certificate provider.
- Operationally manage IAS and cards (e.g. CRL, repudiation policy in case of lost, stolen or misuse of cards)

✥ The Service Provider

The role of the service provider is to provide business services to the card holder using the smart card as an IAS token and/or as a support for a specific on-card application. When the provision of business services to the card holder requires the card to be loaded with additional applications or data, then the Service Provider, acting as Card Application Provider, delivers the “on-card” application or data to the card by any appropriate mechanisms.

✥ Access Provider

The Access Provider is the entity in charge of managing the infrastructure (i.e. the card readers and necessary drivers, communication network and servers) to be used by the card holder accessing the offered services.

✥ SCC Administrator

The role of the SCC Administrator is to administer, monitor and support the relationships between the card issuer, the access provider(s) and service provider(s) in order to ensure the integrity of the smart card community.

✥ Content provider

The Content provider is the entity in charge of keeping the content of the service provider up-to-date. This will be in accordance with the content service requirements and agreements concerned. Note that it does not play any role in IAS interoperability.

"For a deaper analysis of this point, see GIF, Part 1 Clause 4.2.3 - 4.3 - 4.4"

4. Smart Card and e-Service Communities – Triangle of Trust

4.1 Smart card communities and e-service communities

The Global interoperability Framework makes extensive use of the following concepts:

- **A Smart Card Community**

  A Smart Card Community is made up of all smart cards issued and managed by a given card issuer.

- **An e-service community**

  An e-service community is made up of all smart cards recognized by a given service provider. (Note: Card recognition does not imply access to the service. Assuming it can "talk" to the smart card, the service provider will grant or deny the service based on its business rules).

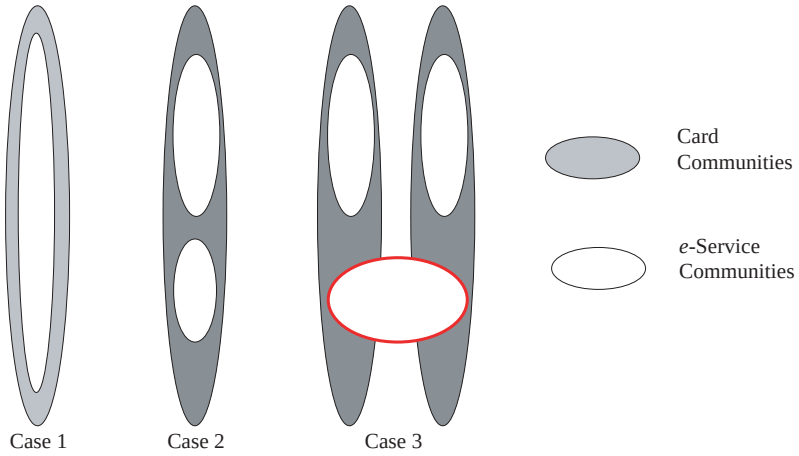


Figure 3 : Relationship between Smart Card and e-Service Communities - 3 cases

- **Case 1: The Basic Situation – 1 card issuer /1 service provider**

  This is the basic situation of a large number of SCMF today where the smart card community exactly equals the e-service community.

  EXAMPLES:

  - Banking debit cards which only work with ATMs of the issuing bank.
  - Health cards which only work for the services of the health service issuing them.
  - Transport cards which only work for services provided by the issuing operator.

- **Case 2: Multi-application Frameworks - 1 card issuer / N-service providers**

  These frameworks enable a smart card community to support multiple e-service communities. Most of the existing or emerging multi-application services propose a range of preset or dynamically modifiable services (post issuance) on a given card.

EXAMPLES:

- Multi-application city cards for transportation/ e-purse/access to public facilities
- Joint credit cards/loyalty schemes (airlines).

❖ **Case 3: Scheme Recognition - n card issuers / N service providers**

This is the case where groups of service providers agree to mutually recognize each others' cards independently of the card issuers involved. This can be achieved on a "one to one" basis between service providers or by the definition of a common scheme within a specific industry.

EXAMPLES:

- In the financial industry, where credit companies strive to get their "schemes" to be recognized by as many banks as possible, e.g. in order to be recognized in a large number of ATMs throughout the world.

4.2 The triangle of trust

All social interactions are implicitly based on achieving some mutually acceptable level of trust between the parties. Trust between the requester (of a service) and the decider (who will grant or deny the service) is achieved by reference to a common third party already trusted by the decider.

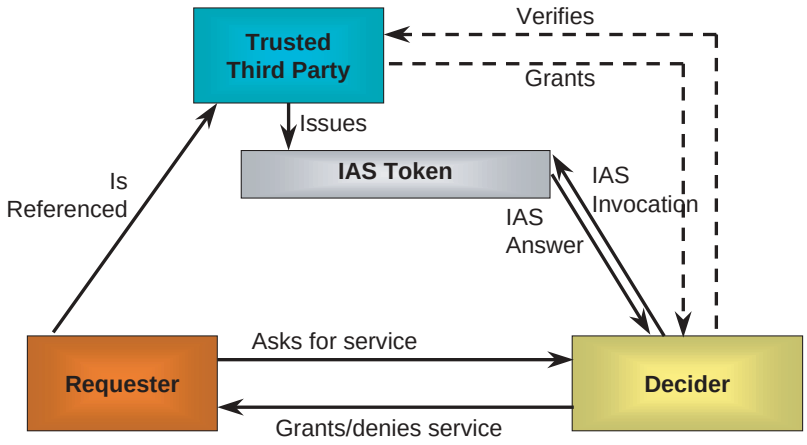


Figure 4: Trust model

4.2.1 What is IAS?

IAS is the set of processes, data and technology agreements required in a given environment to provide Identification, Authentication and Signature services. It includes the following functions:

❖ **Identification** is the process of obtaining information about whom the requester claims to be without considering the "trustability" of this information.

❖ **Authentication** is the process through which a decider can obtain

trustable proof through a trusted third party about whom the requester claims to be (identification) OR what the requester is capable of or authorized to do (attributes).

- A **Signature** on a contract is a material proof of an agreement between two (or more) parties to avoid repudiation of obligations by any of the parties.

4.2.2 Electronic IAS and Generic IAS Application

In a smart card and e-service communities' context, "Electronic IAS proof" is becoming a new buzzword. However, in most cases today, IAS is strongly embedded in proprietary smart card applications and is not considered a "generic" functionality of the smart card. This reflects the fact that up to now, the role of trusted third party and decider (i.e. card issuer and service provider in a smart card and e-service communities context) are often held by a single commercial entity (e.g., bank, transport company, telecommunications operator).

In the vision of the Global Interoperability Framework, the future IAS-enabled smart cards would be issued by institutional card issuers (government based or, in any case, recognised within the national legal system) clearly separated from the service providers.

- They will by default be issued **with a generic IAS card application** supporting a nationally recognised scheme;
- Most of them will be multi-application with many service providers leasing or otherwise using the facilities of the existing smart card information systems for providing access to what has been called their Front Office Application.

In general, recognised IAS schemes are expected to generate:

- Large smart card communities (nation-wide in the case of nationally supported schemes) containing many e-service communities;
- e-service communities interacting simultaneously with several smart card communities.

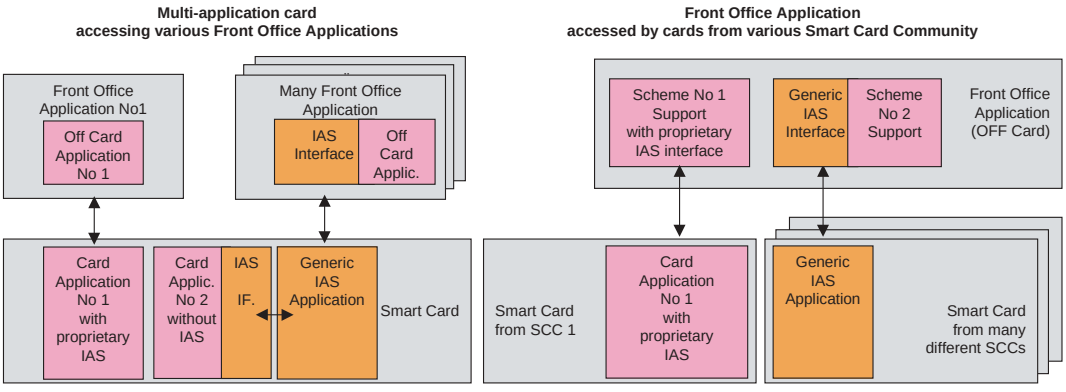


Figure 5: Implementing generic IAS

5. Processes

(primary, secondary, tertiary e-service process)

"For a deaper analysis of this point, see GIF, Part 2 Clause 2.2.3"

A number of processes are required before it can be considered that IAS services are generic and interoperable remaining trustable.

Primary IAS processes

The processes listed below are those through which the IAS services can interact with e-services. They really must be accepted by all participants to an inter-operability agreement and they have to have a common understanding about the steps, the data flows and the content of the interfaces.

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

Table 2: Mandatory IAS processes

Secondary IAS processes

The processes listed below are aimed at ensuring that the IAS services provided by the card issuer can be trusted by service providers and card holders. They rule the conditions that have to be fulfilled to be trustworthy at a certain level. On the contrary of the primary process, ths secondary ones have room for differences in applications. That means that these processes are only required in their objectives and recommended in their appearance.

1. Creating a Smart card community	
1.1	✦ Register smart card community and external secure suppliers
1.2	✦ Verify the compliance of SCC stakeholders (with a particular attention to the access provider(s) which play a key role in the trustability of IAS services) with CI requirements and register them i.e. establish ID + URL
1.3	✦ Provide PKI certificate to registered stakeholders 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 Certificate

2. Issuing and maintaining cards
2.1 ✦ Personalise card
2.2 ✦ Issue card holder certificates
2.3 ✦ Initialise the card
2.3 ✦ Enrol the card holder
2.4 ✦ Maintain life cycles (cards, card holder ID, certificates)
3. Registering e-service (including at post issuance)
3.1 ✦ Test/Accept IAS connection software offered by the e-service provider
3.2 ✦ Test/Accept “on-card application” software offered by the e-service provider
3.3 ✦ Authorise download or download “on-card application” offered by the e-service provider
4. Establishing & maintaining IAS/IOP
4.1 ✦ Create IOP adapter, install rules and policies
4.2 ✦ Maintain IOP adapters
5 Managing the SCC
5.1 ✦ Log the use of cards, IAS and front office
5.2 ✦ Acquiring and settlement

Table 3: Recommended conditional processes

Tertiary IAS processes

These processes are internal to the e-services and are fully and only under the responsibility of the service provider. They are securely hooked to the above-mentioned primary processes. Since they do not impact the IAS interoperability, they are not to be detailed here. The only requirement for enabling interoperability at this level is indeed their interface to the primary processes.

6. Functional boxes

"For a deaper analysis of this point, see GIF, Part 1 Clause 6"

Six clusters of functions (called functional boxes in GIF) are required for the functioning of a smart card information system.

✥ The IAS application function

The IAS application function is the nucleus application of the whole smart card information system.

- It uses the personal data set required to identify the card holder for authentication and electronic signature purposes in an e-government context. This data set is available to be read without restriction by any service provider to whom the card holder proffers the card. However, the definition of its content is under the responsibility of the card issuer.
- Additional personal information (e.g. social security identification number, membership number of a specific association) may be required by a particular front office application domain subject to particular access rights. This additional personal information does not belong to the IAS application function. Instead, it is specific to an additional application function (see below). It is stored and accessed separately from the minimum personal data set of the IAS nucleus and has its own protection mechanisms.

✥ The Platform function

This function includes the operating system of the related building block. The platform box will have no direct IOP-interface to its functional environment other than to the IAS-application that is running on this platform and the connectivity function.

✥ The “PKI” function

The PKI set of tools related to the IAS function has two or more (bio) PIN-based key pairs. A key pair is used for authenticating the card holder and is required before any signatures for non-repudiation can be generated, a second one is used as a signature mechanism for expressing card holder consent and a third one could be used for confidentiality purpose. The following sub-unctions are part of the “PKI” function:

- Key loading and or n-card key generation,
- Key storage
- Digital signature generation,
- Calling the PKI directories i.e. to check on policies
- Handling the PKI settings
- Verifying certificate validity.

- **The "User Interface" function**

  The following sub-functions are considered part of the "user interface" function of the card layer:

  - Smart card community settings (language, accessibility options and tools to ensure access for all)
  - Individual settings (profiles, preferences)

- **The "Connectivity" function**

  The "connectivity" function is in charge of inter-connecting building blocks and includes the following sub-functions:

  - Challenging the smart card via the reader
  - Establishing a secure connection with the smart card

- **The "Additional Applications" function**

  The following sub-functions are part of the "additional applications" function:

  - Applications containing additional Personal data (if required)
  - Additional functions for identification and/or card management (if required)
  - General applications and/or connection to "e-government", "e-business" applications (as far as required).

The figure below models the functional boxes and their relationships.

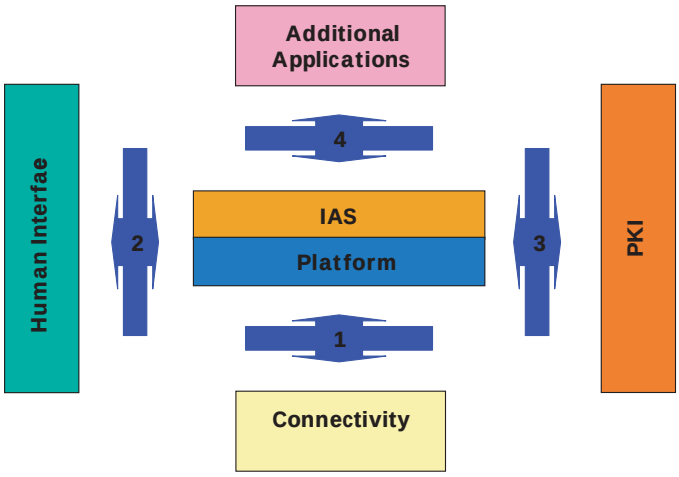


Figure 7: (simplified) Functional box model

The functional input/output interface between the central boxes and the peripheral boxes is labelled as the "IOP-interface" (interoperability interface). Four IOP-interfaces are defined:

- #1. From nucleus to (external) connections,
- #2. From nucleus to human interface,
- #3. From nucleus to PKI application,
- #4. From nucleus to front office applications when IAS functionality is required.

7. Data model

"For a deaper analysis of this point, see GIF, Part 1 Clause 5.5"

Since the meta-model of the framework is aimed at supporting IOP between applications or services within and between smart card communities, it is limited to the identification and authentication of each of the entities participating in the inter-operable IAS business process and includes three types of entity-related data:

- The entity identifier,
- The smart card community identifier
- The certificate with associated key pairs (public/private) for authentication and electronic signature.

From the data relationship viewpoint and business process, these entities may act as sender or receiver of a message/transaction authenticating the card holder.

A proposed summary of the data modelling is provided in the following table:

	ID	SCC ID	Certificate
Smart card	X	X	X
Card application (including IAS)	X	X	X
Card reader	X	X	X
Network	X	X	
CA directory	X	X	X
Front office application	X	X	
User card holder	X		X
Access provider	X		X
Card issuer	X		X
Service/application provider	X		X
SCC administrator	X		X
Smart card Community	X		
Sender			
Receiver			

Table 4: Data model

8. Building blocks model

"For a deaper analysis of this point, see GIF, Part 1 Clause 6, GIF, Part 2 Clause 2.5"

The Smart card information system is made up of three architectural layers, each with their own sets of specific building blocks.

The below figure combines the architectural layer with the functional box model.

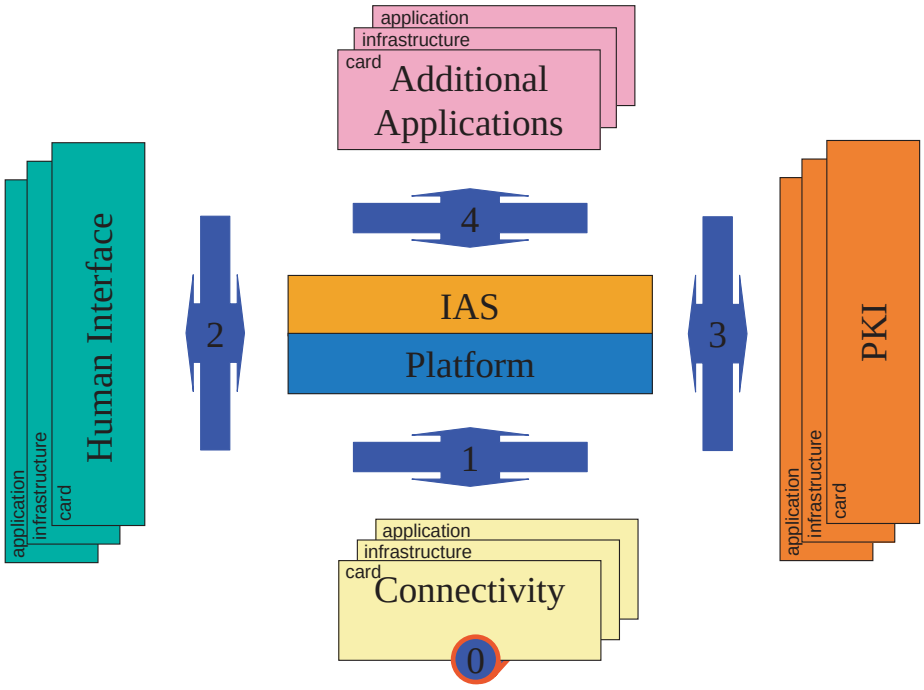


Figure 8: (Full) Functional box model

8.1 Smart Card Layer

A smart card, as considered by the framework is an electronic trusted token with capabilities to securely store and operate IAS functions. It focuses on processor based contact smart cards (ISO/IEC 7816-X) and on processor based contactless smart cards (ISO/IEC 14443-X). One reason for this form factor is the expressed need for eye readable text and images on the ID card.

The smart card functions as a component of an information system. It acts as a server in a client-server relationship because it never proactively generates an action/process. It can only respond to the requests from external “client” software. Within this client-server context, the concepts of “off-card” and “on card” applications are introduced and defined as follows:

- The “On Card” application(s) as the software, which needs to be present on the card to make this service operational.
- The “Off-Card” application(s) as the software, which resides in the infrastructure (terminal, front and back-office servers) to make this service operational.

Technically speaking, this implies that the smart card layer fit with the following standard requirements:

- Physical characteristics
  - ISO 7816 1-3
  - Expected Life time not shorter than validity of ID and certificates (IEC 10373)
- Logical interface
  - Contact (ISO 7816)
  - Contactless (IEC 14443)
- Chip
  - Directory/File structure for multi application capabilities
  - OS:
    - Global platform
    - Java 2.1 card virtual machine and API
  - Sufficient data storage capacity for the required functions (incl. certificates)
  - Security concept including fraud resistance of the mask in line with functional requirements
    - Certified by a security body, as required for EAL 4+
    - Authentication of all parties involved in card performance by public key or public key certificate when performing other actions than reading card retained data (see below) Secure data communications
    - PIN Authentication (number or biometrics) of card holder
    - Key algorithm for operations in the smart card: for asymmetric algorithms, hashing and padding see relevant Workshop E-sign documentation.
  - Card-retained information
    Card holder ID
    - Card issuer ID
    - Unique Card ID
    - Card manufacturer data (name, card type, version)
  - (post issuing) On-card application downloading capabilities in line with mandatory GIF specifications
  - On-card application deleting
  - Internal card management in line with mandatory GIF specifications
  - Card state search in line with mandatory GIF specifications
  - The nucleus application collaborates with the access software in the infrastructure. This software should support:
    - Starting a two sided challenging
    - 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 (a.o. certificate checks)
- Passive status during e-service session
- Terminating the session and logging required (administrative) data

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

8.2 Infrastructure Layer

Typically, the infrastructure layer comprises entities which:

- Recognise the presented smart card layer and invoke the IAS application as well as other on-card applications as required
- Create, as appropriate, the secure communication channel for processing the IAS application.
- Offer tools and services for the purpose of the human interface
- Support several networking standards for linking the two other layers.

Technically speaking, this implies that the infrastructure layer fit with the following standard requirements:

8.2.1 Reader / terminals

- Basic requirements:
  - Capability to read / handle all GIF accepted cards
  - Following recommendations from eESC (contact and contactless card terminals/readers
  - 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 following standard as in development by Finread Requirements for functions and performance
  - Secure communication between chip, keyboards, and display (In case of using the screen/display and/or the keyboard of different building block(s), the links must be secured before the interaction starts.)
  - Displaying status / result information
  - Human interface presentation steered by individual IAS and minimal capable to put in numeric codes.

- Easy select of the e-service that can be accessed Security
  - Secure interaction between card and SAM
  - Where it is allowed to apply a remote SAM, a reliable procedure must create a secure link between the card and the SAM, before any user interaction has taken place.
  - Preventing easy tap of visual PIN code input

8.2.2 Network

- Basic requirements
  - Handle secure communication between terminal / network server (for 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)
  - The network services can be executed via secure links on the Internet with internet tools
- 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

8.3 Front Office Application Layer

The front office application layer of a smart card information system includes all off card components required to deliver a service to the card holder. It is in charge of invoking as appropriate on-card applications (i.e. located in the smart card layer).

Note that at the implementation level, the components of the front office application layer may be distributed throughout the card information system. In ATM for example some components are located in the ATM terminal itself, others distributed on various network servers.

The following front office implementation specifications list should be used as a checklist. There are three services that must be implemented for operational use (the conditioning processes are not considered here):

8.3.1 e-Service front office

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

8.3.2 Network services part of the front office application

It is up to the smart card community how to organise this service. Dedicated net work management services include also (remote) management of secure terminal/s, or dedicated categories of terminals

8.3.3 PKI: the front office for certificate verification

- Basic requirements:
  - Give certificates to stakeholders
  - Apply certificate check
- Functions and performance:
  - Secure connections
  - Read business rules of *e*-Service for IAS
  - Execute business rules for IAS

9. IOP scenario's IOP adapter

"For a deaper analysis of this point, see GIF, Part 1 Clause 7, GIF, Part 2 Clause 4.2 - 4.3"

For the purpose of modelling interoperability scenarios, a new attribute is assigned to each component of the SCMF (i.e. the members of a Smart Card Community as well as the technical components such as cards, certificates, reader). This attribute "On-us" or "Not-on-us" is assigned to each component of the SCMF depending on whether it is being used respectively in their domestic community (i.e. in the community for which they have been primarily produced - e.g. on-us card or certificate) or in a host scheme (i.e. in a community other than their domestic one - e.g. not-on-us card or certificate).

Keeping the Infrastructure Layer constant (i.e. "on-us") and assuming the certificate and card layers are at same level (either "on-us" or "not-on-us"), four IOP scenarios are possible. Based on the above described models, these IOP scenarios can be modelled as follows:

Scenario ID	Card layer	Infra. layer	Applic. layer	Certificate
IOP #0	On-us	On-us	On-us	On-us
IOP #1	Not-on-us	On-us	On-us	Not-on-us
IOP #2	Not-on-us	On-us	Not-on-us	Not-on-us
IOP #3	On-us	On-us	Not-on-us	On-us

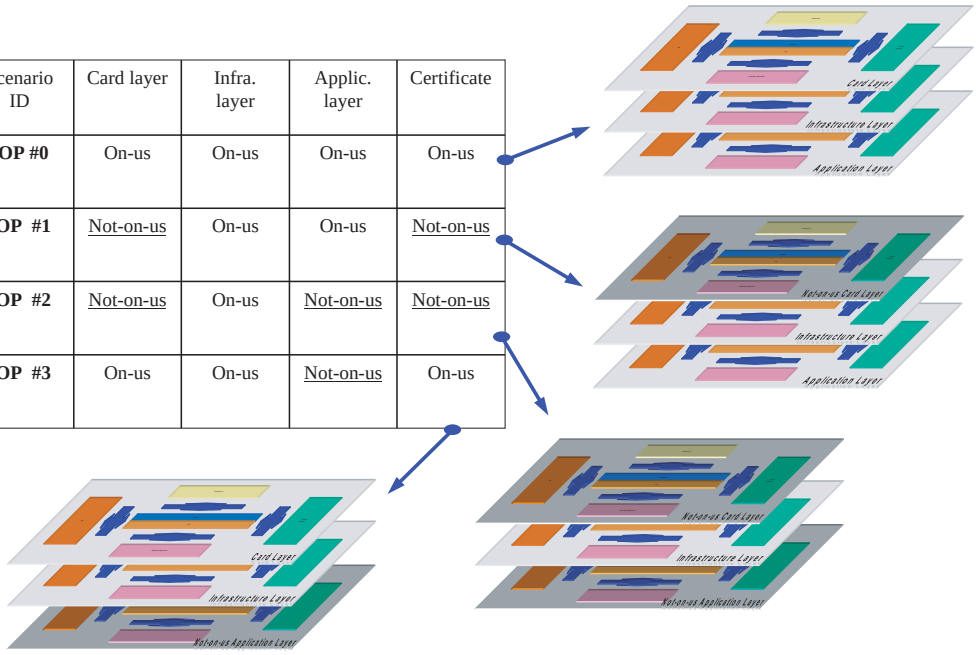


Figure 9: Typology of IOP scenario

For each interoperability scenario the primary processes should be adapted as follows:

IOP Scenario #1	IOP Scenario # 2	IOP Scenario #3
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 on-us card	Activate identification of and recognise the on-us card	Activate identification of and recognise the on-us card
3. Activate call for on-us application access and determine the AS functions required IF AUTH/E-SIGN IS REQUIRED: ACTIVATE A CALL FOR ACCESS TO THE not-on-us **PKI** ENVIRONMENT where card is registered	*Activate call for not-on-us application access* IN THE not-on-us **SERVICE** ENVIRONMENT and determine the AS functions required IF AUTH/E-SIGN IS REQUIRED: ACTIVATE A CALL FOR ACCES TO THE not-on-us **PKI** ENVIRONMENT where card is registered	*Activate call for not-on-us application access* IN THE not-on-us SERVICE ENVIRONMENT and determine the AS functions required IF AUTH/E-SIGN IS REQUIRED: ACTIVATE A CALL FOR ACCES FROM THE not-on-us **PKI** 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 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 5: Primary prosses in the three IOP scenarios

There are two approaches for setting up IAS interoperability in support of the above scenarios:

- The **"Generic IAS application"**

  It defines a set of common interfaces to be used by each layers (i.e. card, infrastructure and front office application layers) and related stakeholders (i.e. user/card holder, access provider and service provider). This is a far more directive approach to interoperability than the adaptor's one, as described below. It is based on the compliance by all participating SCMFs to a set of technical and operational requirements embodied in **IOP interfaces**.
  Compliance to these interfaces enables any Service Provider to access and make use of the IAS functionalities of a smart card independently of where it was issued, hence technically removing the distinction between the "on-us" and "not-on-us" cases.

- The **IOP adapters**

  They act as "mediators", enabling operation across different systems for supporting the various "on-us" and "not-on-us" scenarios. Using more traditional terminology, the IOP adapters enable the recognition of the GIF/IAS scheme across a variety of acceptance devices and systems.

  - The IOP adapter 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.
  - The PKI adapter which is technically identical to the interface required for enabling certificate verification issued by two different PKI within the same smart card community.

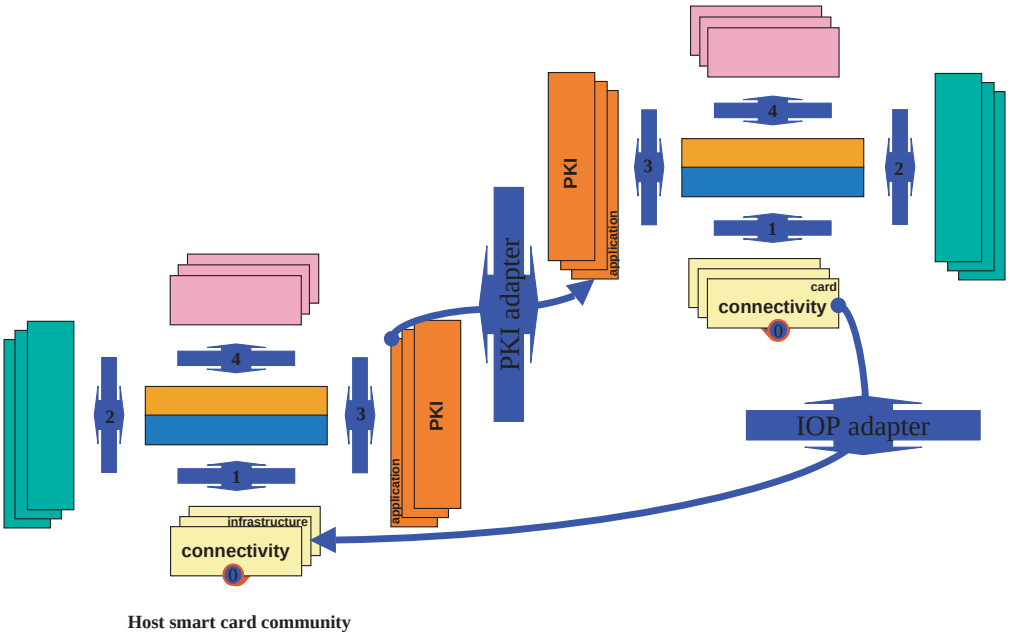


Figure 10: IAS interoperability by adapters

"For a deaper analysis of this point, see OSCIE Volume 2 Rules of Conduct for Privacy and Card Integrity

10. Privacy: summary of privacy proposal

The e-Europe Smart Card Charter proposes a set of inter-sectoral "Rules of conduct for Privacy and Card integrity" for complementing the European Directive 95/46/EC and national legislation on privacy protection in the Member States with a view to ensure that:

- Specific measures are taken for certain branches
- Future developments are anticipated
- A flexible instrument is realised, which can be rapidly adapted to changing circumstances.

These rules are based on the following privacy-related elements:

- Personal data mean any information relating to an identified or identifiable natural person.
- Privacy can be described as the right to self-determination - within certain limits(*) - of one's own environment, one's own body and one's own data. The Privacy Rules of Conduct prepared by the e-Europe Smart Card Charter and applicable to the GIF are for obvious reasons limited to informational privacy: privacy with regard to the information operation process.
- The first prerequisite the Privacy Rules of Conduct address with regard to protection of privacy is the principle of openness: all aspects of the information operation process should be transparent to the cardholder. Only then can it be explained to the cardholder "why data are needed in certain situations", "why his privacy cannot remain 100% uninvaded" and "what freedom of choice he himself has in this".

The figure below summarises the concerned processes and the applicable rules.

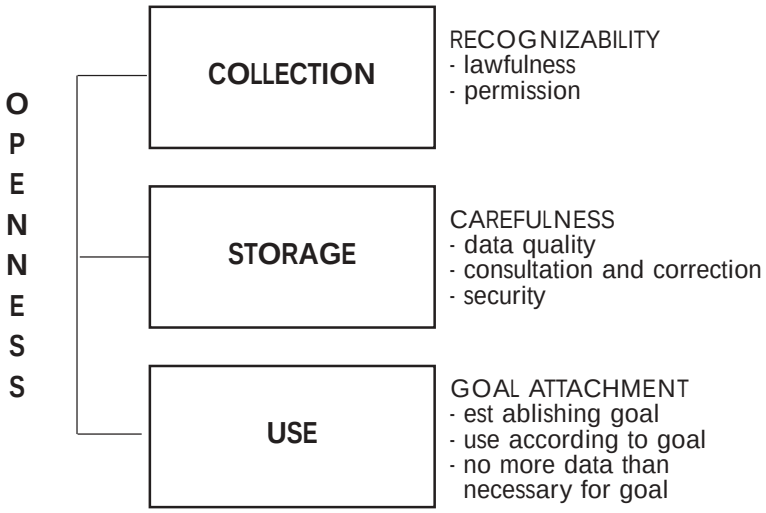


Figure 11: Privacy principle and derived rules

(*) The reservation "within certain limits" indicates that this right to self-determination is always weighed up against other interests, e.g. public interest.

When defining the privacy protection policy of a SCC, the data usage is the most crucial aspect to be considered. The starting point is use limitation. However, it is necessary to prevent card issuers and service providers from (tacitly or not) expanding the number of objectives of the card in an unlimited and uncontrolled way. This possibility does exist, especially for multi-application and multi-service cards.

Another point of attention is the so-called profiling. If no arrangements are made against this, it is possible to make an individual blueprint of the cardholder for a multi-application card with many “user” data. All the person's data are then brought together, e.g. payments, medical data and activities. The card can also stimulate the possibilities of linking if a common feature, for instance a personal registration number, is incorporated in several independent registers of personal data. Of course, only if the use of that number is permitted. The card can also be used to rapidly verify data in existing data bases. It is these forms of use that can evoke fear of invasion of privacy from the cardholder. A set of arrangements between card issuers and service providers that co-operate in a smart card community are required to prevent uncontrolled and undesired use of personal data.

11. Strategy: mission document / strategy document

"For a deaper analysis of this point, see GIF, Part 4 Clause 3"

The question GIF is willing to answer on the basis of a CI centric approach, is:

- "How a SCC can offer IAS/IOP to a still undefined organisation, should it be SCC or SP?" or
- "How can two SCC or one SCC with one external SP build IAS/IOP?"

Answering one of these questions is a complex and expensive process, involving several stakeholders, each with their own objectives and constraints, as well as heterogeneous information systems or sub-systems. This requires therefore the setting up of a comprehensive IAS deployment strategy, based for instance of the "value chain" concept and including two key documents to be supported by each of the stakeholders concerned by the IAS/IOP project.

11.1 Mission Document

This document is based on a SWOT [3] analysis and defines objectives, identifies constraints and available resources for pursuing the objectives. It would include e.g.:

- Objective and scope of the IAS/IOP project
  - Target groups / customers
  - Business case driven or not or partly
  - Type(s) of services to be offered
- Key elements and limits of a business strategy
  - Stakeholders and their contribution
  - Budgets / investment requirements
  - Basic offer to customers
  - Business development strategy
- Key Technological decisions
  - Cards and infrastructure
  - Systems and tools
  - Development / adaptation processes
- Key Financial policies
  - Investing
  - Cost compensations
- Key Policy statements
  - Public ID
  - PKI
  - Privacy
  - Stakeholder missions and constraints

11.2 The strategy document

On the basis of the mission document, the strategy document takes care of defining action plan and methods for actions at business, technical and operational levels. It should address individually each stakeholder concerned and would include e.g.:

✥ The business strategy

For each value chain element, the following has to be defined

- Input value (strategy, expected quantities)
- Added value (mission, strategy, assigned quantities, qualities)
- Output value (targeted quantity, quality)

SWOT stands for "Strenghts, Weaknesses, Opportunities and Threats"

✥ The technical strategy

The purpose of the technical environment (generic IAS or IOP adapters) is to offer the systems, tools and building blocks for accessing the considered e-services. A technical strategy would include the following steps:

- Project Initiation (API)
- Requirements Methods (ARM)
- Technical feasibility Assessment (AFTA)
- Risk reduction planning (ARP)
- Project planning (APP)

✥ The operational strategy

The objective of the IAS/IOP project is to prepare for mass deployment. A project-type organisation would be most appropriate for ensuring

- Security for all operations
- Learning by experience
- Flexibility for quick reaction on success and failure
- User acceptance for success in target groups