Towards an electronic ID for the European Citizen, a strategic vision

Brussels, October 3, 2004
CEN/ISSS Workshop eAuthentication

Table of Content

Document History ***(will be deleted from final version)***			
Version #, date	*Brief Description of Delta*	*Distributed to*	*Drafted by/inputs from*
001; Feb 4, 2004	First Draft of content	Marc Lange, Henry Ryan	Jan van Arkel
002; Feb 11, 2004	Extension of content, recommendations, textual corrections	Members of expert team	Marc Lange, Henry Ryan
003; Feb 16, 2004	Incorporating and addressing comments from ML and HR	Full list of WS members for March 10 meeting	JvA
004; March 31 2004	Incorporating outcome of WS plenary on requirements, biometrics, PKI and recommendations - Delete Annexes A & C, address comments of HR on FAQ's (now annex A)	Yvan Pirenne for check on Chapter 2 (requirements) before distributing Chapter 2 to Porvoo group	JvA
005; April 13, 2004	Completion of Chapter 3, Inventory on Deployment for consideration by Porvoo Group	Secretariat of Porvoo group for upgrade of requirements and MS inventory of eID	JvA
006, April 21, 2004	Upgrade of Chapter 3 on the basis of German TAB report	--	JvA
007, May 1, 2004	Upgrade of Chapter 1, incorporating comments of ML and HR	Marc Lange, Henry Ryan	JvA
008, May 8, 2004	Updates from IDA observatory, feed back from CTST presentations, Information from Global Collaboration Forum, Info from Porvoo group Info from CEN 224 WG 15 and subgroup meetings - input from representatives from France, Austria, Belgium, Hong Kong, China, Malaysia, India - from meeting with EC official - from meeting with ISO SC 17, WG 4 TF 9 chair	--	JvA
0.09 June 10, 2004	New table of Common requirements	GCF, US/NIST, Japan/NICSS, ISO, UK NSCP Morphet, Expert team members	JvA
Special document June 14	Table of common requirements	Catherine Protic for distribution to WS eAut + participants at July 6 meeting.	JvA
0.10 June	Update on eAuthentication levels,	Expert team members	JvA

15 2004	incorporation common requirements table, corrected texts from Slovenia and Israel, comments from ISO representative M Hegenbarth on Common requirements, texts on New Zealand, US GSA cards.	in preparation of June 28 meeting.	
0.11 June 23	Comments from ML on Table of requirements	JvA, ML	ML
0.12 June 26	Update of Biometrics paragraph after CEN/ISSS Biometric Focus group meeting	Max Snijder	JvA
0.13 June 30	Incorporating comments Henry Ryan	Internal	HR/JvA
0.14 July 14	Final draft for Plenary on September 20 -Incorporating outcome of common requirements meeting of July 6 -Updates on Project descriptions -Incorporating some additional pictures of national eID cards - Updating Recommendations with outcome of GUIDE project meeting of July 12, MONIDIS tender for eID management, ideas about eEpoch dissemination activity in New East European member states	Expert team members	JvA
0.15 August 15	Update on US Visit developments, France telecom/Liberty alliance, adding some card models.	WS eAuthentication constituency via AFNOR	JvA
0.16 October 1, 2004	Addressing comments from expert of WS eProcurement, updating of national eID card descriptions of Belgium, China, Ivory coast, Japan, Oman, Russia, Switzerland, UK, US etc. .	Draft for Public comments	JvA
0.17, October 3 2004	Incorporating text suggestions and last round of comments from Henry Ryan	Final for Public comments via AFNOR	JvA

Chapter 1 The vision

1.1 Introduction

This document holds the views of the constituency of the Workshop eAuthentication on the state of the art developments, threats and opportunities in the domain of electronic identification services for the European citizen. The document is positioned in the smart card domain but heavily relies on supporting technologies as digital signature and biometrics for strong cardholder verification purposes. The focus is on high quality single and unique personal identification and verification.
The document is aimed at Central Government policy makers in the domain of electronic ID, the European Commission, the Smart Card industry and in general those organisations interested in implementing electronic ID. Their gain from reading this document will be a better understanding of the rationale for introducing electronic ID and what's even more, eID in a pan European interoperable format. Readers will be more knowledgeable on the requirements for eID, how these may be met by technology providers and they will learn about the deployment status of eID in Europe and beyond. Eventually they may lend their support to the execution of the recommendations in the final chapter of this document.

The smart card -already widely used in telephony and increasingly in public transport and epayment- is now emerging as a key building block for secure access to and convenient use of eGovernment information society services. Foremost of these at present is the drive to implement an advanced European eHealth card and national eID cards in several member states. As a safe and tamper-resistant token the smart card enables secure and convenient access to on- and off-line services. The smart card is fast, there are no orientation problems like with magnetic stripe cards and there is the perception of control for the end-user. It's the cardholder's own card which is protecting the cardholder's interest and checking the security of the system. This is different from the magnetic system set-up where the security is handled in the back offices. So the card provides its holder with increased confidence when accessing and using on-line services. In particular the elements of the Smart Card Charter developed smart card based electronic Public Identity which addresses authentication in e-government and in the private e-services domain are of major importance. Besides containing personal data elements this electronic Public ID also addresses biometrics for convenient proof of the claimed identity of a person and the digital signature to prove the positive consent of the cardholder in an e-transaction process.

An e-ID smart card can combine an electronic identity function with a physical identification function on the same support. It is hence able to address both the need for identification in the electronic ("virtual") and the real world. The electronic chip which is embedded on the card stores the personal data needed to identify and authenticate the owner in public and private on-line transactions. The plastic body contains the usual information needed to identify a person (name, photo, etc.) in the domain of border control etc.
Countries might choose for practical and financial purposes to combine the electronical and the physical function into one document as to issue 1 card is less expensive than to issue 2 separate cards. However there are also countries (see hereafter Chapter 3 on deployment i.e. Italy) that choose to have two documents alongside each other for the National electronic ID function and the National ID card

function. Nevertheless the emphasis in this vision document as well as in the CWA eAuthentication[1] is on the on-line electronic identification function for single identities.

The CWA of the Workshop eAuthentication is based on the Global Interoperability Framework of the Smart Card Charter together with the Smart Card Charter Trailblazer 1 Electronic Identity White Book which latter is positioned in the eGovernment domain. The CWA adopted and enhanced that work with specific details for multi-application smart cards and user convenience- in order to establish cornerstones for an interoperable electronic identity and authentication and electronic signature (IAS) infrastructure for European-wide usage.

1.2 Goals and Objectives of the workshop

The vision of the eAuthentication workshop is that individuals (whether as 'users', 'consumers', or 'employees') may benefit from a credentialing system for IAS that can be easily used and is widely accepted in most online interactions requiring a certain level of eAuthentication for instance on the internet. The end goal is enabling Governments to offer eGovernment services, in co-partnership with commercial uses of public e-identity. By introducing this in an efficient and cost-effective way government and commercial enterprises will benefit from economies of scale and at the same time individuals will be empowered to directly benefit from information society services and applications. For this to happen there must be a pan-European user friendly and effective set of officially recognised and accepted interoperable eAuthentication mechanisms. This equates to a pan-European infrastructure for Identity Management in support of a wide range of eGovernment services like eTax, eSocial Security, eHealth, ePermits, eInvoicing, eParticipation, eVoting etc. .

Up until now, a person has been identified from official papers, because he is known by the people he is talking or via a mutual trusted third party. The same methods do not apply to identification over the internet. At stake is how we can be sure a person is who he claims to be during an electronic transaction over a public network. In other words we need a unique single identity that can be verified in an on-line environment. This is particularly important if sensitive data is accessed or exchanged as in e-government transactional services or e-health services.

The CWA eAuthentication specifications and guidelines address three identity issues encountered in specific instances of government to citizen interactions.

- Identification:
  What exactly are the personal credentials of the requester? The response is provided from the information available on the electronic token (i.e. a smart card) which information in turn is derived from attested public records and guaranteed to be correct if the processes proposed for loading electronic identity on the token are conducted with due care and attention to the details.

[1] **CEN workshop agreement (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN/ISSS)**

This is the typical everyday scenario where citizens and government interact on a named basis. An example could be the necessary 'identity step' for a requester to get access to his 'own' personal information records e.g. tax, motor vehicle registration, payment status for local government services.

- Authentication:
  Is the rightful person presenting the token or is a different unauthorised person attempting to use it? In this process the relying government organisation wants to determine whether the claimed identity really belongs to the service requester. Authentication is considered to be achieved when it has been established that both the token and the personal credentials are valid and in addition if when for example the relying party asks for a PIN-code or a biometric template a response is received which matches with the personal PIN or biometrics of the rightful cardholder.
- Electronic signature:
  Is the service requester prepared and willing to clearly "sign" for transactions electronically thereby expressing his/her will in a way that cannot be repudiated by either party to the electronic transaction? The signature is an expression of this positive consent of the signer. An example could be an individual attesting to the accuracy of a completed electronic form.

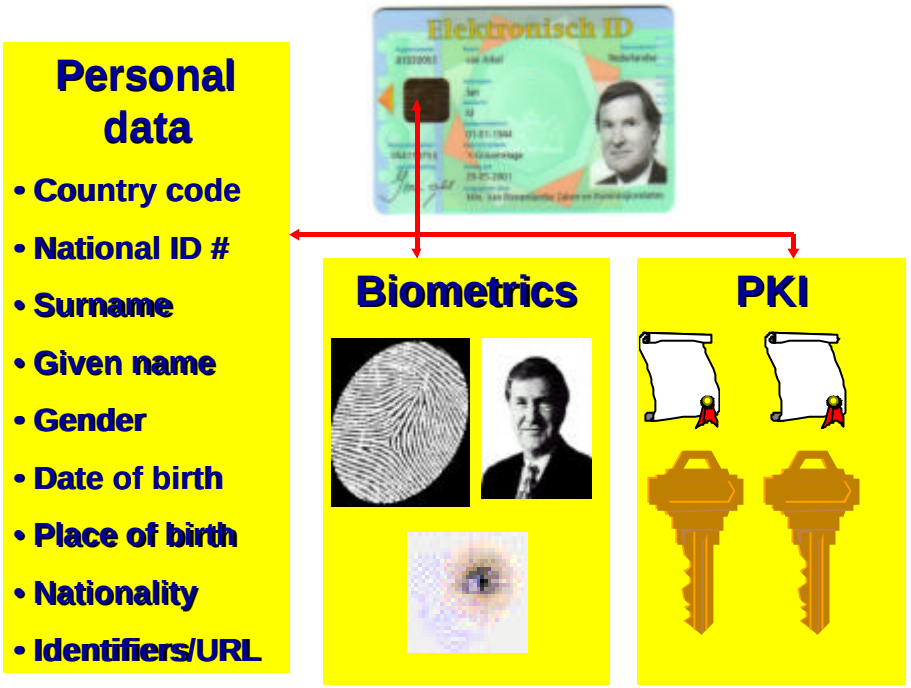


Figure 1, Example of an eID card

In summary the objective of the CWA eAuthentication is directed at the coming of age of a Europe wide –and in due time worldwide- interoperable electronic infrastructure for eID services, supporting User Identification, Authentication, and Electronic Signature services. This CWA builds on and where relevant interfaces with biometric standards as developed by ISO/IEC/JTC1 SC 37 and digital signature standards as developed by the CEN/ISSS Workshop on the electronic signature i.e. CWA 14890 (Area K).

The requirements for eID/IAS are not new. Administrations world-wide are implementing or testing eGovernment services which require IAS. However the

interoperability issue has hitherto not been very well addressed.
As several solutions are already available and being rolled out, this forms –as said in the TB 1 whitebook - simultaneously the major problem and a very challenging opportunity.

1.3 Rationale for a Common eAuthentication/eID approach

'European citizens are now familiar with the use of smart cards in their daily lives. Their use provides a secure environment for electronic transactions as well as a control on the personal information delivered through the network. However, improvement should be made to ensure interoperability of national applications and a massive deployment for the benefit of all the citizens.'
This citation is from Mr. Erki Liikanen, the former European Commissioner for Enterprise and Information Society in the eEurope Smart Cards / Trailblazer 1 "Public Identity Whitebook Version 1.0 of June 2003.

And in addition to this statement from the Commissioner it is said in the TB 1 documents: 'Achieving interoperability of e-ID card schemes in Europe is an aim shared by most European public administrations that are issuing or envisage issuing e-ID cards. This has also been underlined by the Porvoo e-ID Group in its meeting of 21 May 2003.' The Porvoo e-ID Group is an informal international cooperative network with the goal to promote and realize the potential of trans-national interoperable Electronic Public Identities using PKI and smart cards in order to help ensure secure public and private sector e-transactions in Europe.

The main drivers for this well understood need for a national eID and moreover for a pan European interoperable eID may be summarized as follows:

- *The need for a national support of e-services.*
  Smart eID cards are the ideal access tool for all kinds of e-services of any Government. They open the doors for customized service-delivery both in the public and in the private domain. Examples are dedicated access to government databases, individually customized applications, personalized access to websites and e-voting. On top of that, the European citizen enjoys free movement in the European domain and is entitled to avail of government services wherever here or she is, permanently or temporarily residing. All this will contribute to the social inclusion of the European citizen.
  Governments need to be aware of these citizens rights and needs and become proactive in -on the spot - electronic service delivery.
  Smart eID cards are proven building blocks for trust, security and convenience. In that respect there is limited possibilities for real eGovernment services without a well established electronic ID. Without eID eGovernment will not go beyond the pushing of very generic

information and e-transactions will stay out of reach.

- *The need for a common and global combating of ID Fraud*
  ID fraud is an increasing problem in today's world. A UK Cabinet report of July 2002 has estimated the identity fraud in the UK on 2 billion Euro a year. In the US similar concerns are raised. In the credit card domain the fraud problem is well understood. This is the main reason for the world wide credit card migration to EMV, in other words transferring a global magnetic stripe infrastructure into a chipcard based one. None of the credit card companies is not preparing for this transfer because they realise that the one with the weakest security system will be holding the short end of the fraud stick. The same goes for the identity fraud. The country with the weakest identity and e-identity solutions will in due time be confronted with a major fraud risk. Hence a common solution on an adequate security level is needed.

- *The need for national and as well as pan European anti-terrorism measures*
  September 11 has proven the need for world wide anti-terrorism measures. Of course verifying ID's at border crossing and in border crossing on-line service delivery is not the final solution to this problem. If the real underlying causes are not addressed then all measures will be in vain. But eID helps and is a building block to be relied upon. It has been advocated that ID's and Visa will not stop terrorists. One answer is that this might be true for the present generation of documents but not for the type of eID as envisioned in the CWA eAuthentication. On the other hand it's the procedures both for issuance and verification that really count. A near perfect document which is not verified properly has even less value in anti terrorism than a weak document.

- *The need for building a more inclusive European society*
  Providing the European citizen with an electronic-ID smart card will greatly contribute to the awareness of the European citizenship. Like with the Euro currency it helps people to understand that they are not 'just' a citizen of country X, Y or Z but belong to a greater European community of which they are a relevant and highly valued part. The eID should contribute to a citizen's general feeling of trust and security and also offer a seamless experience of entitlement to a European level of service provision whenever they are on-line, and completely independent of their whereabouts in Europe. 'I am a European Citizen and I am the rightful owner of an eID card which proves my entitlement to ……..)'. Some people might argue that such an approach stands little chance in a Europe of 25 member states and over 450 million people. In reaction one might refer to the outstanding example of India where exactly the same line of thinking of 'unifying people and offering them a new awareness of belonging to' is the rationale for a national eID card project for 1 billion people in 28 state-countries with 16 different languages.

- *The stimulation of the emergence of new intra European Union services*

Another driver is the effect of the Europe wide deployment of smart cards, smart card readers and other supporting smart card system elements as an emerging infrastructure which can support various applications at "marginal costs" and stimulate therefore the introduction of new eServices. The banking sector with its Single European Payment Area Concept for 450 million European citizens is already working on these kind of concepts.
This is exactly the rationale why the WS eAuthentication constituency has recommended its so called 'infrastructural approach', positioning smart cards and eID as something comparable to electricity, rail roads and a sewer system. It will however not be the standardisation community what can make this happen. Policy setting and regulation will.

1.4 Inhibitors to a Common eAuthentication/eID approach

One could wonder that with so many strong drivers in place and the technology being there, why are smart eIDs not already deployed widely in Europe yet? The reason for this are the following inhibitors.

- *State of the art of technology*
  Smart cards have been around for decades, however the digital signature as well as large scale implementation of biometric technologies are relatively new. The combination of the three in one package is only just emerging. There are few countries on their way of implementing this solution on a national scale, Italy and Spain taking the lead in Europe in this respect. So it is still early days on the high synergy of these three.
  Smart Card standardisation is in place and implemented, biometric standardisation is almost there but still under construction till early 2005. The smart card supported digital signature standardisation has just been accomplished but is not fully implemented by industry yet.

- *Costs and benefits*
  An EID Infrastructure is expensive despite the fact that smart card prices have come down over the years. Biometrics checking and the costs of retrieving certificates are relatively high. Moreover its not only the costs of the system components that count, it's also the organisational costs of (face to face) card issuance and enrolment of the cardholder.
  On top of that there is not an apparent business case for the Government or the private sector to carry the total of costs. It's like the early days of the fax machine, a valuable infrastructural element but if there are still limited numbers of users and service providers around yet, the costs are higher

than the benefits.
This is of course not under control by the WS eAuthentication but standardisation contributes to the opening up of the market and to economies of scale.

- *Not invented here*
  Not all Government eID programs are created equal. Domestic specifications are still dominating. Also some people feel that an eID project is complex enough on a national scale and should not be overloaded with (cross border) interoperability issues.
  The same line of reasoning left us with the legacy problem of 20 different and domestic electronic purse systems in Europe. All filled with Euros but not interoperable cross borders.
  There are some good examples. The first set of specifications was developed in Sweden (SEIS) in cooperation with the Dutch National Chipcard Platform. These specification were adopted by Finland and the Finnish documents were adopted by Estonia. The specifications are freely available on the web and royalty free. But that seems not to have been a convincing argument so far.
  Good examples of electronic ID in Europe like in Estonia (500.000 eID cards with signature capability issued, nice package of services) and Finland (50 + services related to the eID card and strong cooperation on digital signature between government and the banks) are not seriously enough investigated. Same applies for relevant projects in the Middle and Far East. These very interesting solutions are 'not invented here'.

- *no strong central leadership*
  So far there has been no strong central leadership in the domain of eID cards. National Governments are happy enough to take on eID in their own domestic domain and are not in a position to take leadership over other countries on eID. The EC has considered eID so far as a political minefield where national interest and privacy issues are dominant and has therefore not stepped in.
  The European Smart Card Charter Trailblazer 1 on Public Identity and the Porvoo group have produced good preparatory work in this domain. But they have no mandate from the card issuing bodies.
  However strong external pressure – coming from the US VISIT program- is rapidly changing this situation and has forced Europe to organise itself in the eID arena. This is already leading to the fast introduction of biometrics in passports. This will also influence the adaptation of biometrics in the national eID cards domain though not the same technical solutions need to be followed there.
  A common European introduction policy is the positive effect of such pressure. This may very well lead to a common solution. The example of the EC action on the European Health Insurance card as well as the action on the Tachograph card proves that such a EC action might very well work out well.

Nevertheless as said before the drivers are stronger than the inhibitors and the need for eID card is well understood both in Europe and the rest of the world.
In Scandinavia the eID card has already a relatively long history, Estonia, Italy, Belgium and Spain are also examples of European countries on the smart card move. However Asia is where the real action in this domain is right now, as will be elaborated in Chapter 3.
There is more evidence of the need for eID. Microsoft is showcasing how smart cards can help secure computer networks in 6 countries. And there is more underway from Microsoft in the eAuthentication domain. In the US private sector entrepreneurs are trying to fill in the gap of a secure national ID token and have deployed the Verified Identity Pass project. (See Chapter 3 under US). France Telecom is leading a consortium to develop a European wide eID solution and also some European large scale study and coordination projects are under way, the most prominent being the GUIDE project (www.guide-project.org).

So the electronic ID card is in most European countries only a question of 'when' and not so much a question of 'if' anymore.
Nevertheless the coordination of all this activity and an overall strategy are still missing.

Chapter 2 How can the vision be realised?

2.1 Conditions for mass deployment of eAuthentication/eID in Europe

The unique position of the eAuthentication CWAs are that they are based on a personal electronic token (smart card) which has for two years been studied in depth by the eEurope Smart Card Charter whose results are embodied in the OSCIE (Open Smart Card Infrastructure for Europe) documentation. This personal token surpasses from a security perspective other schemes including those which for instance store the secret signing keys of the user including PINs and biometric templates on PC hard drives.

The CWA approach covers several important features: consumer empowerment and control of the smart card, inherent storage and security of the information in the card, safe storage of biometric templates in the card (no need for a central database) and the usage under the control of the cardholder, matching of (biometric) data on the card, key pair storage and signature generation in the card, ease of use in general, simple orientation of the card in a usage mode, proven use in multi-application scenarios combining government and commercial service access.

The degree of confidence provided by existing public documents such as passports, driver's licenses, medical cards and other documents issued to the requester only after stringent face to face identification requirements has led to their use in transactions far removed from their original intention. The same principles apply to the use of the electronic ID card. A multi-application card is under the control of the user and is inherently secure. It can include features which make it easier and safer to use and introduce new governmental and commercial services. Both the issuing administration and user will also have a high level of control on the access to 'personal' information. In addition administrations may choose to levy a "real estate" charge on cards that they issue.

Central to this is increased end user acceptance and use of a trusted secure IAS environment on the basis of multi-functional e-tokens.

These issues are at the basis of and have been elaborated in the CWA eAuthentication. This Chapter summarizes:

- the minimum requirements for eID as set by Government
- the architectural model
- the legal perspective
- the standardisation issue

2.2 Minimum requirements for issuing eID

This paragraph has used the eESC TB 1 White Paper as basic input. The white paper is the result of the work carried out under the eEurope 2002 Smart Card Charter by Trailblazer 1 "Public Identity". It specifies the minimum requirements and recommendations for implementation of electronic identity by Government. This to allow member states to mutually recognize electronic identities issued by other participating member states.

The minimum requirements have been scrutinised by the eAuthentication Workshop constituency and extended and updated. Moreover the requirements have been discussed in a joint meeting of the Workshop eAuthentication, CEN 224 WG 15 and the Porvoo group on July 6 2004 at AFNOR. And also in the context of the Global Collaboration Forum on electronic ID consisting of representatives of the EU, Japan and the US these requirements have been addressed.

The following general requirements have been set for the Smart Card based eID system elements. The way in which these requirements are met have been detailed in the CWA eAuthentication.

Scope & General eID Concepts

- The positioning of the eID system is interoperable electronic ID and eAuthentication in the eGovernment domain.

-
The concept is based on the microprocessor chip (contact & contactless) as a trustworthy and convenient token for eAuthentication as well as secure signature creation device for the electronic signature.

- The concept of a Smart Card Community is supported : all smart cards issued and managed by a given card issuer Card (Issuer Centric model) where the issuer is either a Government institute or acting under the jurisdiction of a Government institute.

- The concept of an E-service community is supported: all cards from different Smart Card Communities where the IAS capabilities are recognized by a given service provider.

Basic eID System Functionalities

- Electronic identification & authentication of the cardholder to public and private services
- Electronic signatures for legal proof of non repudiation

Optional functions are:
- Support of confidentiality services, enabling encryption of data transmitted over a network

- Official Travel document

Overall eID System Requirements

- The system shall support different security profiles

- The system shall be trustworthy for the cardholder; the system as such shall be reliable and it shall protect the cardholders data present in the card

- The execution of the eID and eAuthentication function shall
be convenient and fast, it shall be executed in a secure and controllable way

- The system shall be future proof

Cardholder ID requirements

- The system shall support a secure and reliable cardholder identification function

- A set of Personal data of the cardholder shall be held in an electronic form. This file is optionally protected by PIN and/or Biometrics.

- A set of Card related data shall be held in an electronic form.

Cardholder Authentication requirements

-
The system shall support a secure and reliable cardholder authentication function

- For this purpose the card will hold support:
  - one or more PIN's
  - one or more Biometrics (bio-pin for 1:1 verification)
  - a signature key for authentication

Electronic Signature requirements

- The system shall support a secure and reliable cardholder electronic signature function for the purpose of legal validity of the positive consent of the cardholder and to guarantee non-repudiation in relation to a signed information object.

- The PKI elements of the system shall be in compliance with the qualified electronic signature as per article 5.1 of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures. In this respect there need to be compliance with the ETSI Qualified Certificate Policy document as well as the Workshop eSign Area K document on a smart card based application profile (CWA 14890). The PKI structure shall also be compliant with the documents referenced in the related Commission Decision of 14 July 2003, on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with the Directive.

2.2.1 Organization issuing e-ID-cards

The e-ID-card consists of a smart card provided by the card issuer, and containing private keys and certificates issued by a Certificate Authority (CA) on the basis of the card holder data collected or verified by a Registration Authority (RA). Although

these roles may be taken care of by different organisations, the Workshop expects that in the particular case of an e-ID-card, it will always be a central administration (i.e. central Government) that would take the ultimate responsibility for these different roles. The liabilities of and between different parties should therefore be defined according to the national legislation of the Member State of the card issuer.

2.2.2 The Authentication level

eAuthentication in the context of the CWA eAuthentication is the remote authentication of individual people (single identity) over a network, for the purpose of eGovernment and private sector services. There are different levels of eAuthentication ranging from a low level (no identity proofing required) to a high level (strong identity proofing required).

In the UK eGovernment literature there are 4 levels of authentication defined according to the potential damage if authenticity is breached in government transactions.
- level 0 minimal damage
- level 1 minor damage
- level 2 significant damage
- level 3 substantial damage.

In the US eGovernment literature (NIST Special Publication 800-63, Draft Recommendation for Electronic Authentication there is a subdivision in 4 levels of electronic ID and 4 levels of authentication mechanisms.
On level 1 eID there is no requirement to prove the identity or maintain a record of the facts of registration. Identity assertions of claimants are accepted without verification.
Level 2 identity proofing and registration provides sufficient assurance for relatively low-risk, routine business transactions.
Level 3 identity proofing requires that RAs verify substantial evidence of the identity of applicants; however, it does not necessarily require that applicants present themselves in person to register.
Level 4 identity proofing is distinct in that it requires in-person identity proofing of identity documents that contain a picture of the applicant, and that a biometric such as a photograph or fingerprint, be taken of the applicant and retained in the records. The delivery of tokens also shall be linked to the in-person appearance at the RA. This level also requires applicants to sign their application with a handwritten signature under penalty of perjury.
On the higher levels of authentication Level 3 authentication is based on proof of possession of a key or password through a cryptographic protocol. Level 3 authentication assurance requires cryptographic strength mechanisms that protect the primary authentication.
Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that “hard” cryptographic tokens are required. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or above. By requiring a physical token, which cannot readily be

copied and which shall be unlocked with a password or biometric, this level ensures good, two factor remote authentication. So far the US approach.

The CWA eAuthentication follows a somewhat similar approach and does also support the concept of multiple security environments.
The CWA offers a toolbox with the following 'levels':
- identification (just reading some cardholder data out of an open file in the card)
- authentication medium (same + PIN or Biometrics)
- authentication high (same + now a secret key is used to sign the personal card holder data), the smart card has to comply with CEN ISSS WS eSign SSCD requirements
- non-repudiation (another secret key is used to approve of the content of a certain information object, the relevant certificate is 'qualified')

Its up to an individual eID card issuer of service operator to define his own security requirements and environment. However for mutual recognition of card holder eID's in the intra Europe and Global domain its' to be expected that operators will put up a relatively high level of security requirements. In practice these may be 'negotiated' between service provider, card reading terminal and card to check what the security requirements exactly are and if they can be fulfilled in a certain practical situation. By doing so the security environment is then set. This is in line with the concept as now in study by CEN 224 WG 15.

The following factors are detailed in the CWA eAuthentication toolbox:
- a token (smart card) as proof of possession by the individual
- a password (PIN-code) as proof of knowledge by the cardholder in compliance with ISO/IEC 9654-1
- a biometric verification process that matches a life bio-template from the cardholder to a stored template in the card by an on board card operation as proof of the authenticity of the cardholder in compliance with ISO/IEC 7816-11 and ISO/IEC FCD 19794-2 (fingerprint minutiae)
- a proof of possession of a key through a cryptographic protocol (PKI), the key pair(s) having been generated on board the card. Reference to the cryptographic object on the card (keys, certificates, root-certificates) shall be conducted by means of a description application according to ISO/IEC 7816-15
- a strong cryptographic authentication of the card as well as relevant parts of the infrastructure and encryption of all sensitive data transfers between the system components shall comply with ISO/IEC 9798 (device-authentication/Secure messaging)
- on board the card generation of the digital signature (signing of the last round of hashing on board the card) for maximum security in the non repudiation process.

2.2.3 e-ID cards and qualified certificates

One basic requirement for Issuers of e-ID-cards is that the certificate(s) supporting the 'qualified electronic signature' (non-repudiation) created within/by each e-ID-card must be issued as Qualified Certificates conforming to article 5.1 of the EU directive. This means that the Issuer must comply with the ETSI Qualified Certificate Policy "QCP public + SSCD" (Secure Signature-Creation Device, specified in ETSI

document TS 101 456) which is a certificate policy for qualified certificates issued to the public, requiring use of a SSCD. For this reason the issued smart card shall be evaluated and certified as a secure signature-creation device in the sense of the EU directive.
ETSI TS 101 456 (which is now under revision) contains the requirements for an issuer of qualified certificates, defined in a technology-neutral way, regardless of the implementation platform.

2.2.4 Card holder requirements

Part 3 of the CWA eAuthentication elaborates on the interface requirements for the end-user. The clarity and simplicity of the usage of the eID function is of utmost importance for the actual take up in society. Accessibility, perceived health risks and safety, religious and ethical concerns are of equal importance. Here lies a clear task for the issuing organisations to offer the necessary transparency so pro-active dissemination activities are needed.

2.3 Architectural model

The basic objective of CWA eAuthentication is simple. To support migration from situation 1 (see figure below) where each eID card has its own infrastructure and trust services into a situation 2 where card body, microprocessor, smart card infrastructure as well as trust services may be shared between different e-service providers.

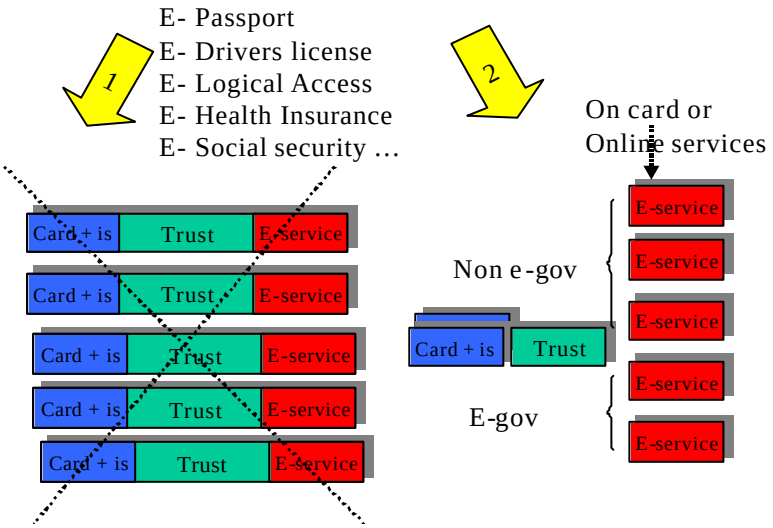
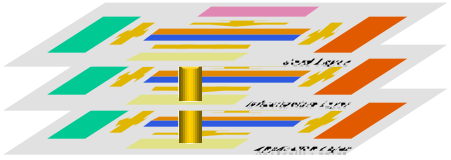


Figure 3 From many to 1

The CWA eAuthentication describes and details the overall architecture, business models, social and legal pre-requisites, and technology implementation guidelines for an interoperable eAuthentication/eID infrastructure across Europe. It makes extensive use of the following concepts:

- a Smart Card Community (SCC): all holders of smart cards issued and managed by a given card issuer
- an e-Service Community: all users of smart card enabled e-services supported by a given service provider
- functional architecture: the 3-layer architectural model comprising the smart card layer, the infrastructure layer (which includes card readers, other card interacting devices, remote servers and private or public telecommunication networks), and the front office application layer comprising the applications which deliver a service to a user with a smart card
- on-us or not-on-us: mode of operation assigned to a component of the smart card management framework referring to use in its domestic community or in a host scheme respectively.



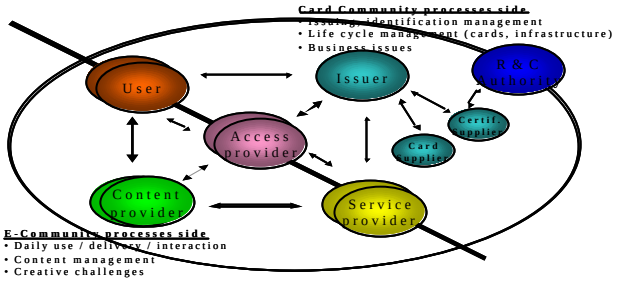


Figure 4: Basic Functional model

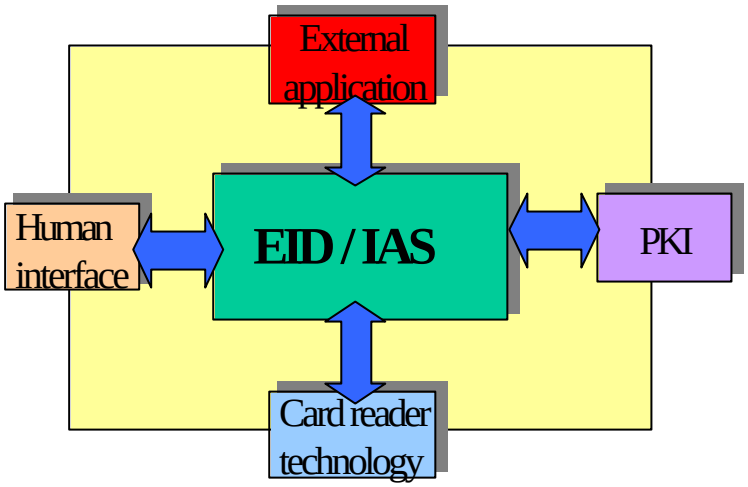


Figure 5: The interfaces

2.4 The legal issue

An architectural model (CWA eAuthentication) , standards (see next chapter) and technical specifications (eEPoch Workpackage 3) might be well in place, an eAuthentication legal regulation is still missing in the European domain.

On the basis of preparatory work of the Porvoo group [2] the Workshop eAuthentication constituency has discussed different elements of the legal issue and reconfirmed the Porvoo viewpoints starting with the need of avoiding over-regulation in the legal drafting. This is particularly important for e-ID, which is a relatively new field and where new technical solutions appear regularly. A balance should therefore be ensured between technological neutrality and the need to ensure legal predictability. As far as the technological neutrality is concerned it should also be considered that the CWA eAuthentication is focussed on the chipcard domain. It is important to focus only on those issues that are specific to e-ID, and to rely as far as possible on already existing regulations.

When drafting a legal framework for a European e-ID, the following issues should be covered at minimum:

1. Procedures etc. when issuing e-ID
2. The content of e-ID and its verification

[2] Prepared by Mr. Thomas Myhr, Ministry of Trade and Industry, Norway

3. Data protection
4. Liability
5. Revocation of e-ID

To have a pan European interoperable e-ID, the regulatory framework has to be at the right level, so that it can be accepted and used by all - states, national authorities, and private companies.

2.4.1 Regulations concerning procedures etc. when issuing e-ID

The link between the person/e-ID holder and the information in the e-ID must be secure, so that a 3rd party can accept the e-ID as a valid ID. This has an impact on legal requirements and is mainly a national issue (as passport issuing procedures are). For a pan-European e-ID, a homogenisation of basic procedural rules is required at least concerning the requirements for the issuing of e-ID: which documents must be presented by the holder to get an e-ID, is personal appearance required, when/at which stage of the procedure, which other evidence for proving the identity is needed, etc.
Some detailed legislation on issuance procedures is in force at European level. They have been transposed into national law within the European Economic Area (EEA), and co-exist with requirements based on internal national law. The requirements for issuing trusted visual paper based ID such as a passport should be met also for the issuance of e-ID, i.e. it should not be easier to get an e-ID than a trusted paper based ID.

2.4.2 The content of the e-ID (data quality) and the verification of the e-ID

The e-ID content issue is to be seen in the continuation of the issuing procedure: How to secure the link between the ID holder and the e-ID information? What information has to be in the e-ID certificate, and how to present the data? How can a third party verify the information given in the e-ID? Regulations exist already in this area and further regulations should rely on them. In a number of countries there exists already a unique national ID or public services number. The question is if it can / should be used to ensure the link between the holder and the e-ID. And in the countries where it does not exist, what should be used as unique personal identifier? How to solve the problem at international level?
Another issue to consider here is the range of information presented to a requesting third party, depending on the purpose for which the e-ID is used.
Regarding the signature verification, there is no formal requirement, but only a recommendation in the Electronic Signature Directive.

2.4.3 Data protection

Should the e-ID holder be given the right to control what information can/shall be presented to a third party when the e-ID is used? This could apply on a general basis or on a case-by-case basis.
There are several directives on data protection, amongst them the Directive on Electronic Signature. This Directive gives the signer the right to determine whether information in the qualified certificate shall be made public or not. This raises however the question whether this is enough for the use of e-ID.

2.4.4 Liability

Who shall be liable for any false information in the e-ID, when the e-ID is used? The Electronic Signature Directive regulates the liability of Certificate Service Providers (CSPs) issuing qualified certificates. The fundamental aspect of the regulation is that the CSP's liability is based on a reversed burden of proof. Would that be feasible also for issuers of e-ID? Will there be any CSP with such a liability potential?

2.4.5 Revocation

The impact of e-ID theft is worse than theft of paper based ID, since the use of paper ID usually requires personal appearance, which limits the use of the visual ID. In contrast, a "stolen" e-ID can be used on the Internet in many States and for an almost unlimited number of transactions in a very short period of time.
A good protection system and procedure is therefore needed. An effective e-ID revocation system would then even allow for a higher security of e-ID as compared to any visual ID, as the revocation could be made almost instantly by the holder. An enhanced security system could e.g. include a single EU contact point (i.e. a unique phone number) to revoke an e-ID.

2.4.6 Interoperability

Whereas the first 5 issues should be considered for a legal framework there is the strongly related issue of interoperability.
This could be either regulated by law or could be achieved by agreements between parties on the market, with the Government playing an active role.
Also, there is an obvious need to prevent "lawful" use of the e-ID by others, e.g. where spouses "lend" their e-ID to each other for example for voting.
However PIN and biometrics for personal verification will offer a solution to hamper such misuse of e-ID.

Recommendation:

- Existing regulations already on a European level, should be taken as starting point when drafting a new legal framework for a European e-ID.
The most appropriate solution is embedding the eID/AIS functionality requirements in the Directive on Electronic Signature.

- If this turns out to be not feasible for one reason or another a dedicated eID Directive should be developed and put in place.

- For an interim period pan European Interoperability agreements might serve.

In the context of the eEPoch project (see Chapter 3.2) such an interoperability agreement has been defined. There is also an interoperability agreement active between Estonia, Finland and Belgium.The detailed table of content of the eEpoch interoperability agreement is included in CWA eAuthentication part 1.

2.5 Standardisation

This Chapter holds some general comments on the status of standardisation on the three underlying technologies for eID/Authentication: smartcards, biometrics and digital signature. The referencing to the actual standards the CWA eAuthentication complies with, is part of the CWA itself.

2.5.1 Smart cards

Smart cards interoperability at the lower system layers has been around for a long time and smart card standardisation is well in place. The CWA eAuthentication - though positioned at the higher system levels (application level)- builds on these standards at the higher layers.

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) are responsible for international standardisation. They have installed a joint committee (JTC 1) for the standardisation of Information technology. JTC Subcommittee SC 17 is dedicated to the standardisation of personal identification and cards.
SC17 has addressed both the contact and the contactless smartcard domain. The most relevant series are 7816 for the contact domain (now a 13 part standard covering physical characteristics, electronic signals and transmission protocols, command sets, data elements etc.). In the contactless domain relevant standards are ISO/IEC 10536 (close coupled cards, working distance about 2 mm, slot or surface) ISO/IEC 14443 (proximity cards, working distance about 10 cm, wilful act) and ISO/IEC 15693 (vicinity cards, working distance about 50 cm, hands free). The ePassport recommendations mandate the ISO/IEC 14443 standard in type A as well as in type B mode. Interoperability testing of e-Passports in 2004 has however shown that some ambiguities in the standard might need to be addressed.
Standardisation of very high bit rates for communication (necessary for biometric and digital signature execution) is in progress. The CWA eAuthentication supports all of these communication modes.

A new SC 17 work item is in progress to produce a standard for application interfaces providing generic smart card services, the generic smart card services to include global interoperable eID/IAS functionality. The work item is being developed by SC17 WG4 Task Force 9, Application Programming Interface - Integrated Circuit Cards (TF 9 - API-ICC). The group is making fast progress and a draft three part standard is expected in early 2005. This standard ISO/IEC 24727 is envisioned to consist of 3parts: architectural model, high level API for services and a card edge API.

One of the standardisation elements still missing is a standard for post card-issuance application downloading and deleting. A proposal for a new work to cover this issue has been accepted by SC 17. This will lead to new dedicated part ISO/IEC 7816-13. As the CWA eAuthentication is positioned in the higher system layers this issue is transparent for the CWA eAut.

There is no ISO/IEC standard for smart card operating systems. The CWA supports different options like native cards (complying to ISO/IEC 7816) as well as a Javacard environment.

On the European level CEN (Committee European de Normalisation) is the relevant standardisation body. CEN 224 on identification cards has a number of working groups in different application areas like banking, public transport, health and also a recently (Q4 2003) installed Working Group 15 on a European Citizen Card. This group has started to work on a Technical standard for both the electronic as well as the physical aspects of the card. There are two Subgroups active one for the logical and electronic aspects and one for the physical and visual aspects. The draft standard is due in Q 1 2005. The CWA eAuthentication will be an important input document for CEN 224 WG 15.

All in all, technical standardisation in the smart card domain is well in place and offers a firm base for the CWA eAuthentication to build upon as well as to contribute to the work-in-progress.

2.5.2 Biometrics

Standardisation in the biometrics area is less advanced than in the Smart Cards or PKI domain but due to the imminent need for anti-terrorism measures is gathering speed and trying to fill in the gaps. One should also be aware that in the context of the CWA eAuthentication biometrics are also positioned as a convenient instrument to eliminate the need for the end-user remember different PINs for different purposes.

Extensive work is under construction in ISO/IEC SC 37 a relatively recently installed group dedicated to biometrics which is very active and produces draft standards at a high pace. The most relevant standards for the CWA eAuthentication are:

- ISO/IEC 19784-1 BioAPI, BioAPI specification
- ISO/IEC 19785-1 Common Biometric Exchange formats (CBEFF)
  Part 1: Data Element Specification
- ISO/IEC 19794-2 Biometric Data Interchange Format
  Part 2: Finger Minutiae Data

Most of these standards are still under development and in the stage of a FDC (final committee draft). Voting is on for a number of drafts. So at the end of 2004 /early 2005 we may expect a rather complete package of international biometric standards.

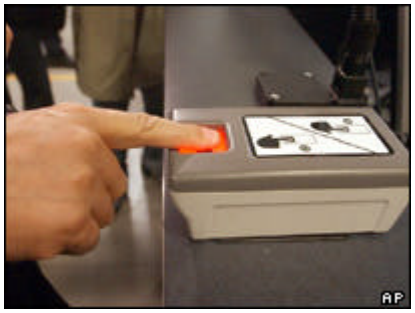
SC 37 defines generic Biometric standards. Dedicated to the smart card domain is ISO/IEC S 17. SC 17 has developed:

- ISO/IEC 7816 part 11 which addresses personal verification through biometric methods in ID's.

Another important player in the biometric standardisation domain is ICAO (International Civil Aviation Organisation). This organisation in which almost all countries participate specifies standards (multi-part ICAO Doc 9303) for international travel documents including passports, visa and ID cards for travel purposes. It's documents, the most important being document 9303 are being 'wet stamped' to full ISO standards (ICAO Doc 9303 is ISO/IEC 7501).
ICAO's new technology working group has made important decisions and defined preferred biometric solutions in the aviation and border control domain.
They made four relevant choices:
- the preferred chip technology for Machine Readable Travel Documents) is contactless (13,56 MHz)

- the preferred biometric technology for world-wide interoperability in the border control domain is facial recognition
- the chip should hold the full picture of the biometric characteristic, not the 'calculated' template (ICAO recommends 32Kbytes of memory for storing biometric images)
- the personal demographic data in the IC of the card is in principle freely accessible but a Member state may decide to make this PIN protected.

Both the US and the European Union have decided to comply with these ICAO recommendations for the border control domain. The US-VISIT program is influencing countries to implement e-Passports a fast pace. The original target date of October 2004 has since by decision of the US House of Representatives been postponed to October 26, 2005 for the 27 Visa Waiver Program countries. In September 2004 the EU Commission sought to postpone the obligation of a biometrics passport for a further year i.e. until end 2006.
Nonetheless, biometric enrolment of all persons visiting the US has commenced as from September 30 2004. These fingerprint and facial biometrics are checked against watch-lists of known terrorists and criminals. Whether this database checking is already in place is not confirmed. The proof of this will come out of the first hits and arrests. Since the deployment of US-Visit at 115 airports and 14 seaports in January 2004, more than 8.5 million non US nationals have been processed without long waits, according to US officials responsible. They insist it takes just 15 seconds per arrival.



The ICAO specifications address the data structures as well as the command sets for the communication between the ePassport and the reader/terminal. The ICAO specifications are now 'frozen' and ICAO is now concentrating on the certification issue.
A technical specification for the European ePassport is under preparation by the EC and is expected before the end of 2004.

However the Workshop concluded that the border control domain is out of scope of the workshop and moreover the requirements in that domain are different from the requirements in an on-line and un-attend e-services environment. Therefore the Workshop has come up with the following requirements/recommendations:

- Biometrics will be used for 1:1 verification

- The CWA will support different biometric technologies. An Object Identifier will be included to distinguish between different biometrics.

- The recommended biometric technology for interoperable access to e-services is fingerprint minutiae

- It is mandatory to have the biometric template on board the card

- The biometric template needs to be protected (read only) and its access may be optionally protected by a PIN.

- It is recommended to have the matching of the life bio-template and the stored template done on the card.

- Biometric 1 : n matching is out of scope of the CWA eAuthentication

2.5.3 Digital signature

The legal umbrella for the digital signature is laid down in EU Directive 1999/93/EC of December 1999 on a Community framework for electronic signatures. This –technology neutral- directive has been elaborated in a number of technical specifications from a joint CEN and ETSI activity, the CEN/ISSS Workshop eSign.

The most relevant work for the Workshop eAuthentication has been produced in Area K of the Workshop eSign leading to CWA 14890. That (2-part) document, as part of a series of standards for secure signature creation devices (SSCDs) is dedicated to smart cards as an important representation of SSCDs. The key issue of the CWA 14890 is to enable interoperability, so that smart cards from different manufacturers can interact with different kind of signature creation applications. The CWA specifies the application interface to the smart card during the usage phase, where the smartcard is used as an SSCD, to enable interoperability and usage of those cards on a national or European level. The CWA is based on the EU directive on electronic signatures and takes into account other E-SIGN documents and standards mentioned in the scope. The functionalities described in the 2 parts of the CWA map the general requirements of the EU directive to asymmetric techniques as required by the corresponding protection profile and cover additional services, useful in signature environments. In line with the CWA preferences CWA 14890 is applicable to smart cards supporting file system oriented applications (the ISO/IEC 7816 native cards) as well as for smart cards supporting object oriented applications (e.g. Java applets).

CWA 14890 has taken the following requirements into account:
• *Requirement 1: The format for electronic signatures and their certificates shall be interoperable*

Signatures will be verified in different applications and environments, unknown to the signer. Formats of signatures and certificates therefore need to be standardized in order to ensure interoperability.
• *Requirement 2: The device interface (physical, logical and application interface) shall be interoperable at least for the same device type.*
A signer should be able to use his signing device in different applications and environments, without having to install specific software drivers depending on the manufacturer of the device.

CWA 14890 consists of two parts.
Part 1 describes the mandatory services for the usage of Smart Cards as SSCDs. This covers the signing function, storage of certificates, the related user verification, establishment and use of trusted path and channel, key generation and the allocation and format of resources required for the execution of those functions and related cryptographic token information.
Part 2 describes optional services based on the same technology as available in signature devices. This covers key decipherment and client (card holder) server authentication, signature verification and related cryptographic token information

The Workshop eAuthentication has accepted CWA 14890 part 1 and 2 as the basis for the IAS signature function from a security and interoperability perspective.

This leads to the following:
- CWA eAuthentication relies on CWA 14890 for mutual device authentication (smart card and infrastructure checking vice versa each others validity and genuineness)

- CWA eAuthentication relies on CWA 14890 for the digital signature for a non-repudiation function in e-transactions

- In addition the key pair for the digital signature needs to be either PIN protected, biometric protected or both.

- CWA eAuthentication has detailed its so called PKI adapter including the functionality of cross border certificate validity check. The CWA eAut envisioned preferred solution for this functionality is a bridge Validation Authority. However this preference will be brought in-line with accepted practice as soon as a final European wide solution for this need emerges.

2.5.4 Standardisation of eAuthentication

Besides the standardisation of the above described system components, standardisation of eAuthentication as such is becoming more and more of an issue.

An example of this is the rise of new collaborative organizations and standardization groups. In recent months two very relevant industry-led organizations have emerged in the US. First the Electronic Authentication Partnership (www.eapartnership.org)

has taken on the task of developing a framework to promote authentication across boundaries of trust authorities. Recognizing that operating rules and assurance levels need to be defined before one entity can trust the credentials issued by another entity, EAP hopes to use working groups to define industry specifications and rules that will enable e-authentication between disparate parties.

A second industry group, OATH (www.openauthentication.org) is a collaborative industry initiative working to develop an open reference architecture for the universal adoption of strong authentication. The group wants to remove barriers to adoption of strong authentication technology by recommending open standards to standardization bodies. OATH partners include VeriSign, IBM, Axalto, Gemplus, ActivCard, HP, Sun Microsystems, ARM, Aladdin, Rainbow, Authentex etc. OATH had its kick-off on April 21 2004 in Palo Alto, US. Information about OATH and an OATH white paper can be found at www.openauthentication.org.

In September 2004 the Wireless LAN Smart Card Consortium proposed a new type of authentication that it claims will simplify secure logon to all types of wireless networks. The Consortium is endorsing a draft proposal for EAP-SC (standard for wireless access) authentication. The proposed standard would serve as a single, standardized method of logging on to Wi-Fi, WiMAX and other types of wireless networks and may also support access to GSM-based 3G networks via the SIM cards. The consortium consist of major vendors including Gemplus, Texas Instruments, Oberthur, Alcatel and also Visa International.

In the US large credential checking providers are active like Corestreet www.corestreet.com. Corestreet plays a role at certificate validity checking in large US schemes like the DOD/CAC card.

France Telecom is developing an eID management solution on the basis of the Liberty Alliance federated ID model. IST funding for this project is under negotiation.

Also non –smart card based but large scale solutions are emerging like a network based e-Authentication server in the Netherlands.(A-Select)

Overall conclusion in the standardisation domain:

The Workshop concludes that for the three domains (Smart Cards, Biometrics and Digital Signature) all the basic elements are sufficiently in place. However the combination of Smart Card, Biometric and Digital Signature Standards for the purpose of eAuthentication is still to be provided. The CWA eAuthentication is filling this gap and elaborating on the synergy of the three components.

Chapter 3 Deployment of eID in Europe and beyond

3.1 Introduction

This chapter gives basic status information on eID deployment in Europe and in the rest of the world. It is by no means a complete overview. On the website of Conference organiser Inside ID (http://www.insideid.com/ ; Id facts and figures) it says that there are at present 117 national electronic ID projects. A report from the German TAB inventories 107 projects on border control and national ID cards in 55 countries. The present inventory - in turn- holds data on 76 countries. From a content perspective it is the most comprehensive overview publicly available so far. This explains the huge interest from both Government representatives and from journalists for this material.

The inventory conducted by Smart Card Charter Trailblazer 1 on electronic ID has been of great help. Also useful information could be obtained from the IDA eGovernment News - Identification & Authentication website EUROPA - IDA Interchange of Data between Administrations , as well as the B& L ''Study on the deployment and interoperability of electronic and biometric authentication and identification'' of June 2003 and the German TAB report of early 2004. This was enriched with information out of smart card magazines, web research, feed-back of the Porvoo group members, the WS eAuthentication constituency and last but not least from various contacts with project managers from eID projects worldwide who generously provided feed back on the descriptions of their projects.

The general picture is that eID implementation is well on its way but not in all regions.
The Anglo-American regions are not very ID card minded. In the US the Bush administration is opposing national ID cards, in Canada a national ID project was withdrawn under public pressure and the same applies for Australia. On the other hand electronic ID cards are booming in the Far East (Japan, China, Hong Kong, Malaysia etc) as well as in the Middle East.
An interesting issue is that China, Japan, Korea, Hong Kong and Singapore have agreed to do a concerted action to develop a common used and interoperable smart card (Silk Road Card). One of the results of this cooperation so far is the establishment of an Asian Smart Card Forum with its first conference in June 2004 in Korea.
There is a relatively large quantity of projects in South America as well as in Africa. In Europe there is only a handful of countries engaged in the roll out phase, the majority of countries are still in the phase of getting political consent and conducting studies and pilot projects.

From a technical perspective there is a patchy situation. Though most of the projects have chosen the contact based chip as their main technology the choices in the domain of the Public Key infrastructure are various. Only very few European countries are on their way of introducing biometrics for end-user verification in combination with the national ID card. This despite the fact that worldwide more than 70 countries are applying biometrics for card holder verification purposes. However this situation in Europe might change in the near future in the slip stream of introducing biometrics in the Passport book which is very definitely on its way. In general the worldwide focus

of the projects is on the domestic market and cross border interoperability is not high on the agenda yet. Nevertheless as stated before, there is a highly promising activity in this respect between Japan, China and Korea. In Europe a pan European interoperability demonstrator is active under the name eEpoch (see paragraph 3.5) and in domains like Health (E 111 card) and Banking (EMV cards) interoperability is well under way. So it may very well be expected that interoperable eID will follow in due time.

In this Chapter we will address subsequently:

- The eID market development
- Deployment of eID in Europe
- The eID pan European demonstrator eEpoch
- eID projects in the rest of the world

3.2 eGovernment Market development

The market for electronic ID cards is expanding. Eurosmart, the umbrella organisation of Smart Card Industry and partners worldwide has published the following figures for accumulated smart card shipments in the year 2003 and has made predictions for the number of cards to be shipped in the eGovernment domain in 2004 as well as in the coming years.

EUROSMART
The Voice of the Smart Card Industry

Smart card shipment 2003

	Cards (Millions of units - Mu)	
	Memory	**Microprocessor**
Telecom	800	670
Financial Services - Retail - Loyalty	35	205
Government - Healthcare	20	40
Transport	50	12
Pay TV	-	35
Corporate Security	4	7
Others	10	10
Total 2003	**919**	**979**
	1898	

Although Eurosmart has not been able yet to distinguish between Government and Healthcare uses the fact is that in this domain 40 million cards have been shipped. It is not unrealistic to presume that 1/3 of these have probably been national eID cards.

The projections for 2004 are being even better and amount to an expected percentage growth in the range of 50% in the eGovernment and Health domain.

EUROSMART
The Voice of the Smart Card Industry

Forecast 2004

	Cards (Millions of units - Mu)		
	Memory	Microprocessor	
			growth
Telecom	730	710	6%
Financial Services - Retail - Loyalty	35	240	17%
Government - Healthcare	35	60	50%
Transport	55	20	65%
Pay TV	-	40	14%
Corporate Security	10	12	70%
Others	10	12	20%
Total	875	1094	11,7%
TOTAL 2004	1969		

The predictions of 2005 and 2006 envisage similar growth percentages.

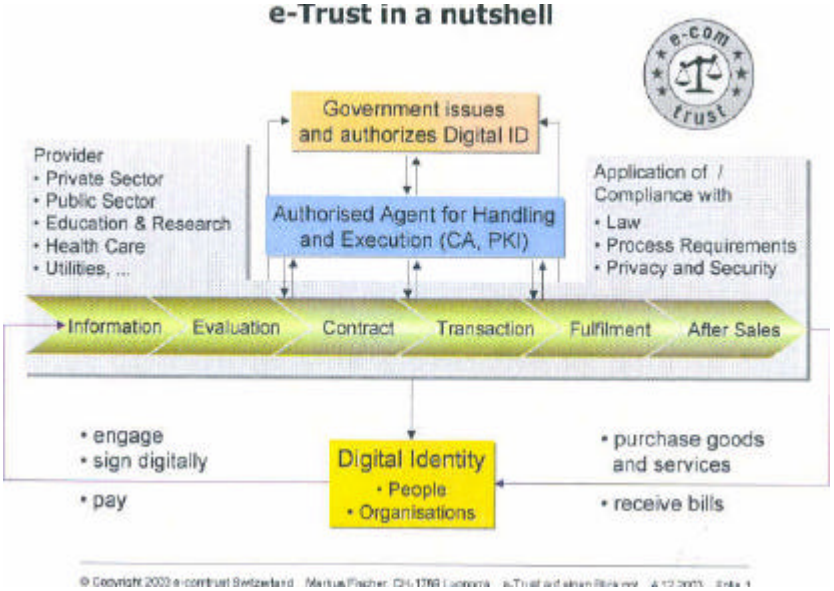
EUROSMART
The Voice of the Smart Card Industry

Smart Cards and e-Government applications

Volume of microprocesseur smart cards in Million units (*)	2003		2004		2005		2006	
	M units	%	M units	%	M units	%	M units	%
E Government applications	50	6	61	6	95	8	159	12
Wireless applications	570	66	635	62	700	60	780	57
Total applications	870	100	1010	100	1180	100	1360	100

- *Microprocessor Smart Cards in million units*
- *E-Gov applications internal or in relation with citizens: Electronic identity cards, national health cards, driver's licenses, passports, certified digital signatures, entitlement cards for public service beneficiaries, or smart cards for public service employees*

On top of the need from eGovernment side for a reliable Identity verification there is the rising demand from the private sector for reliable verification mechanisms.
An example for this is the issue of trust in e-Shops (CEN/ISSS CWA 14842 e-Trust). This activity positions a Government issued Digital ID in the centre of trust assurance. As they say it: "In tomorrow's consumer transactions over the Internet we expect a seamless integration of identity services for people and organisations, and we expect the government to issue Digital Ids that can be used throughout the world for business



transactions."

These and similar activities like the eAuthentication activities in the financial sector will even increase the demand.

3.3 Deployment in Europe

Austria
Initiated by the Austrian Government in November 2000, the citizens card concept 'Bürgerkarte' is not so much a dedicated card but a concept which defines a bundle of functions and minimum requirements from an e-Government perspective. The basic functions being the secure identification of the citizen and the digital signature function. It also offers confidentiality in communication by encryption facilities. The concepts are based on open standards and open interfaces that allows for a multitude of smart-card initiatives to operate in an interoperable way. Several private sector and public sector projects already issue cards or are planning to do so. In this way a concept has been realised that fulfils the requirements of e-Government and can be implemented in an interoperable way by several solution providers.
Some of these are:

- Membership card of Austrian Computergesellschaft OCG (operational)
- Signature card from the Certification service providers (operational)
- National ID card with chip
- Social security card e-card (contract awarded)

- Various students cards (operational)
- Bankingcards with signature capability (announced)
- Chambers of Commerce card (several Notaries)

So far 60.000 students cards have been rolled out, The roll out of 4.5 Million ATM cards is expected to start in October 2004, a contract for the Social Security Card (also know as e-Card has been awarded in June 2004). The project expects to issue 11 million chip cards which will replace the current paper-based health care voucher by the end of 2005. The chip will contain administrative data such as the cardholder's name, title, date of birth and social insurance number. A trial is scheduled at the end of 2004 in Burgenland. The digital signature is an optional function.

Up till now 30.000 cards have been issued by the private sector. All in all the national coverage is about 2% of the population in May 2004. Austria has conducted interoperability tests with the Finnish and Italian ID cards and the German signature card. There are more to come.

More information: http://www.buergerkarte.at

Belgium
In April 2003, 11 Belgian pilot municipalities started issuing a new e-ID card to the public called BelPIC, which stands for Belgian Personal Identity Card.
The municipality administration cooperates with the National Register and Belgacom, which is the Certification Authority. By May 2004 some 56.000 Belgium citizens possessan electronic ID card, the pilot had been positively evaluated and the Federal Government had decided to start the full live national roll-out in in September 2004. According to the latest schedule the large-scale distribution will be completed in 2010. . Up to early 2007 the cards will only be delivered to certain target groups (such as notaries public and doctors) and to citizens who spontaneously request them. This delay in the original distribution process is partly due to the need for a critical mass of applications to be developed before citizen demand can take off. Spontaneous requests have remained low in the pilot municipalities so far.

The basic functionalities of the system are Identification, Authentication and Digital signature. The card currently holds 2 Pin codes, and in the longer term inclusion of biometrics are envisioned. Likewise a contactless mode is expected to be added. Application areas are reliable access to e-services, e-portal functions, on-line tax declaration etc. So the citizen may apply at home for official documents from the Government or access his own civil records in the Government databases including birth certificates. Discussion with the banking sector about usage of the card for home banking purposes are ongoing. There is also discussion about integrating the functionality of the SIS social security functionality on the eID card. Universities are considering the usage of the card as a student card. The card might also very well be used as a physical token for library privileges, access to swimming pools but also as an access tool to buildings of private companies, one of the functions of an employee card. The card is finally an international travel document for the European 'Schengen' countries.

Card readers are publicly available in electronic terminals in the municipalities.

Suppliers of payment terminals have agreed to deliver 90.000 terminals which will accept the card. In the banking sector 8.000 readers will accept the card in the near future. The Belgian State Secretary for State Computerisation presented on 18 May 2004 a first set of e-ID toolkits. Targeted at cardholders as well as at IT developers, the toolkits are available for purchase online from an "eID Shop" developed and maintained by Certipost and Zetes, suppliers of the Belgian electronic identity card, under the authority of the Federal Public Service for ICT (Fedict). Among other things, the kits (starter price of 85 €) allow citizens to read their ID card contents on their computer and provide programmers with the necessary means to develop e-ID applications. The eID Shop can also provide professional users with specific training and consultancy.
Card readers and kits have to be purchased by the citizen. A price setting of about 20€ for the reader was announced. Middleware is free, downloadable from the web. The Central government charges 10€ for a card to the municipalities who do their own price setting to the citizen.
The card and certificate have a validity period of 5 years. The Government estimates that because of the card the saving in public sector, private sector and for the citizen himself will amount to 100 million € a year.

In May 2004 the Belgian Government has announced its intention to start issuing biometric passports in 2005, after an initial pilot. The passport will feature a contactless microchip that will store personal identification data including a biometric identifier. Following the ICAO recommendations facial recognition is likely to be chosen as the principal biometric technology, but also the fingerprints could be incorporated.

Bosnia-Herzegovina
Since 2002 Bosnia issues Citizen ID cards holding biometric data in the format of a 2D bar code. In 2003 this project entered a second phase. About 2.5 million cards in ID 1 card format will be distributed to all citizens over 16 years of age. The issuance process is expected to be completed by the end of 2004. The card will also contain the cardholder's photograph and signature, digitally scanned and laser-engraved in the ID card. The card will also contain the fingerprint in the form of a barcode. This biometric data will also be kept in a national electronic residents register accessible through the Internet.

At the basic of the introduction of these new documents, valid across the whole territory of Bosnia-Herzegovina, is the wish to reinforce the country's unity. Until now the two highly autonomous parts of the country, a Muslim-Croat federation and a Serb Republic, have issued their own separate ID cards.

Bulgaria

A project to issue a smart card as a national ID to each of the 8 million citizens has been developed after abandoning plans to do so on a magnetic stripe basis. The idea is positioned as a general access mechanism which may also be used in contacts with doctors and banks. The project started in June 2003 and led to an official report in November of that year. The first objective is to improve government security. In this context 10.000 data security certificates have already been issued within the administration.

Cyprus

There have been some rumours about plans in relation to participation in an eEpoch follow up activity but nothing final.

Czech republic

EID is on the list of items of political interest. The focus has however been so far on the smart card based Marcha project in the health domain.
No detailed information available.

Denmark

The implementation of electronic identification is limited to a web based solution. There are no plans for a national eID card. The national IT and Telecom agency monitors the issuance of digital signatures but there are no listed public applications so far.

Estonia

The Citizenship and Migration Board is the national eID card issuer in Estonia. The issuance process is handled by a public-private partnership. The card is contact based, holds a Personal data file and PKI certificates for identification/authentication and non-repudiation purposes. The card is PIN protected. There are no biometrics on board.
The deployment is progressing well: starting in 2002 more than 500.000 cards were issued by Q 1 2004, a penetration of almost 50% of the target population. As the card

is mandatory for the citizen this number will steadily rise by replacing the existing ID cards. The certificate is not mandatory. So far 200.000 certificates have been issued.

The beneficiary of the card is the State but the card is also used in different organisations: banks, lawyer's offices, local governments, ministries, municipality, companies, etc . New government services for the citizen are:
- on line access to one's personal data
- on line info which government employee and for what purpose has had access to one's personal data files.

On the service providing side all required software is now available, free of charge and in an operational version. Some public agencies are now equipped in order to process administrative procedures electronically (tax, migration, citizenship).
The Tallinn city government also decided to implement a virtual ticketing system for public transport relying on the Estonian e-ID card. After only 2 months there were already 78.000 users of the e-tickets. The information (rights, ticket type) for the e-ticketing function is stored in a central data base, whilst the e-ID function mainly contains the link (key) to access this information. The combination of e-ticket and e-ID allows for a large flexibility for the pricing schemes, since it facilitates the checking if the user is entitled to get a special tariff, such as a lower price for residents.
The Finnish Population Register Centre and the Estonian Certification Service Provider have signed a Memorandum of Understanding stating that they "will cooperate to make legally binding digital documents a reality within and between Finland and Estonia".

There has been a first case of court ruling concerning the validity of Electronic Signature (ES). The sentence was positive for the evolution of ES, since it confirmed that it is mandatory to process ES signed documents in the same way as paper-signed documents.

Finland
The Finnish e-ID card issued by the Population Register Centre (PRC) is a Multiapplication card used for many service applications. The Population Register Centre issued the first qualified certificates in Finland in 1999. In Q 1 2004 some 40.000 chip-cards had been issued, but the number is steadily increasing thanks to a change in the law: With the Act of Amendment from 17 February 2003 the legislation on identification cards was revised, including the extension of the validity period of the e-ID card from 3 to 5 years, the reduction of the visits to the Police to 1 visit, the

creation of an electronic identification code for everyone, the abandon of the former chipless ID card, the combination of the electronic ID card and the social security card as from 1 June 2004 and the lay-down of the term citizen certificate by law. The amended law has entered into force on 1 September 2003. Since then, about 1,000 cards per week are issued.

About 50 PKI services are now available to card-holders. A municipal application for employees with access to e-services, payment for meals etc will be ready at the end of the year 2004 (25 KB size). Since June 2004 the Finnish citizens can request to have their health insurance data included in the eID card. This combination of functions will contribute to decreasing the number of cards a person has in use. The health insurance function is only present in the visual part of the card. The mid term objective is to provide 1,000 services with e-ID authentication, and to have 35% of the citizens using the e-ID within 5 years.

The Mobile Communication Project launched by PRC and Sonera is ongoing. The necessary coordination between the Sonera mobile systems and the PRC citizen certificate infrastructure and its testing with services has started in autumn 2003. In spring 2004, the infrastructure has been opened to service providers for the development and testing of services. The service of electronic ID certification via a mobile phone with a special SIM card will become available to consumers in 2004 and offer secure access to a number of new eGovernment services based on SMS messaging.

Furthermore, the Finnish-Estonian cooperation in cross-certifying questions was continued and a Memorandum of Understanding signed. A meeting took place in September 2003, and it became clear that the cooperation has to be organised on two levels: legislation, and technical questions.

France

In February 2004, the French Prime Minister launched the ADELE program, an ambitious national plan to modernize the state infrastructure and the relationships between the citizen and the administration. The program encompasses about 140 different projects and initiatives that cover different issues in the eGovernment framework. Smart cards are a priority in this new national scheme. There are several smart card schemes under preparations.

At the basis of the national ID card is the “Titre Fondateur” now renamed “INES” (Identité Nationale Electronique Sécurisée) ; National Electronic and Secured

Identity. Under the responsibility of the Ministry of Home Affairs, the priority is to launch in the context of the CNIE project for National Identity the 'ECC' (Electronic Citizen Card) in 2005/2006. CNIE is the kernel issue in all the action lines aiming in the modernisation of State. From the beginning, CNIE is considered in the frame of the « titre-fondateur » which aims to implement a secured block of information processes allowing the citizens to get a passport or an identity card under simplified conditions.

The basic functionality of the card is to support eGovernment and to enhance the quality of public services. The citizen may use the ECC card for administrative procedures and he will be able to interact more directly with the administration. CNIE will be multi application and is envisioned to integrate an electronic signature and hold 2 biometrics: facial and fingerprint.
Procurement for the INES project is expected to begin before end 2004. The card and related database is scheduled to be developed and tested during 2005, and French citizens expected to be able to start using e-IDs from 2006. The card, containing a chip carrying the identity information of the cardholder, will provide citizens with electronic signature facilities allowing secure execution of both e-government and e-commerce services and transactions.

According to the French Government, the following services will be made available within the ADELE framework before the end of 2005:

- The '*Allo Service Public*' call centre service will be extended countrywide in October 2004. Call centre agents will have the database of the Service-Public.fr portal at their fingertips, thereby making the portal's contents also available by telephone for those users who do not have Internet access or who prefer more traditional telephone interactions. The service will thus provide a unique point of contact for information and guidance on public services and administrative procedures through a free of charge (users will only pay the normal local call rate).
- A one stop shop service for address change will be launched in January 2005. This service, which will also be available offline through traditional channels, will allow users to select the public bodies to which they want to communicate their new address. Users will then receive a confirmation message from each relevant body via mail, e-mail or text message. Initially limited to a number of public sector organisations, the service will be progressively extended to other administrations.
- All public bodies will accept tenders submitted electronically as of 1 January 2005. Some exceptions to this rule will apply, for instance for contracts below EUR 230, 000 awarded by local authorities. Public bodies will be able to adopt a central e-procurement platform or to choose a specific solution.
- A personalised public services portal ("*mon.service-public.fr*") will be launched in April 2005. Based on the Service-Public.fr portal, it will provide users with secure, personalised access to all public services available online.
- An e-service will enable civil registration certificates (birth, marriage, death certificates) to be requested online as of July 2005.
- Associations and charities will be able to apply for government funding online as of October 2005.

According to a presentation given in February 2004, the French e-government programme will be implemented through 140 concrete initiatives, representing a total investment of EUR 1.8 billion. ADELE will allow the government to consistently develop e-government services over a period of four years in a coordinated and results-oriented way. It is expected to achieve estimated yearly cost savings of EUR 5 to 7 billion as of 2007. An evaluation of the plan's implementation will be conducted annually.

In parallel, this Ministry is about to launch in 2004/2005 the CAP project being a card for civil servants. It will permit all Administration employees to access personnel data file and manage their activities. The card will be based on contact card technology and support PKI with 2 certificates. The envisioned user base is 200 K users. The total budget is estimated at 3, 5 millions euros.

The Ministry of the Civil Service, Administrative Reform and Town and Country Planning and the State Secretariat for Administrative Reform have launched in March 2003 a project for the development of the *"Carte de Vie Quotidienne"* (daily life card) in order to facilitate the life of users of proximity services. The daily life card is positioned to provide electronic access to local and national public services through an identification and/or authentication process, comprising eventually of a payment possibility. At the moment 13 pilot sites are experimenting their own CVQ during 2004/2005. Another call to extend CVQ to other local authorities will be launched in 2005.
This two tier approach is quite similar to the Italian, Belgium and German approach.

Germany
Germany has at present a paper based national ID card which is widely deployed. There are several projects with respect to electronic identification and eGovernment services under the umbrella of the BundOnline2005 program. The aim is to have 400 different eGovernment services from the Federal Government on line in 2005. At this moment 200 are already in place. For this effort Germany is spending 1.45 thousand million euros – an investment that enjoys national and international reputation.
One of the projects is a Job card to be issued to every citizen that may be expected to be economically active for on-line access to employment services and social benefits systems. The project is envisioned to start in 2007.

Germany has developed a standard for a smart card based employees card for civil servants, much like the common access card of the US Government. The Federal Ministry of the Interior also has plans for the deployment of biometrics in personal documents, like passports and non residents cards. Biometric evaluation studies have been conducted for this purpose. There are no final plans published for the transfer of the present national ID card into a smart card format.
A number of German banks including the Deutsche bank are working with the Government in the 'Signaturbundnis' to agree on a national electronic signature standards.

Greece

The government has a program to introduce eGovernment as well as a supporting electronic ID. Some evaluations have been conducted. There is however no concrete project to implement public electronic identity.

Hungary
An eID project is active. No detailed information available.

Iceland
Policy discussions are continuing on the subject of e-ID. The present paper-based card is currently being replaced by a plastic ID one, which has a place reserved for a chip but does not yet contain one. Policy decisions have been made and some small-scale pilots were conducted.

Iceland positions itself as a leader in adoption of new technologies. A survey in 2001 showed that Iceland had the highest Internet connection rate. But more importantly, Iceland has many successful real e-applications, the "killer e-Government applications" being e-tax and e-customs. In 2001, Iceland was recognized by the EC for these applications with the good practice award for e-Government. Today, over 80% of all tax returns are processed electronically.
Regarding security, software based PGP has been used until now and considered sufficiently secure for the first applications. A digital certificates pilot project has been launched in Iceland in December 2002. A workgroup comprising government institutions has been active since March 2002, with the aim to map possibilities, to estimate costs of data transactions, to proceed to a risk analysis. There are no plans at the moment to introduce a token-based PKI infrastructure.

Ireland
The mission of the Reach Agency established by the Irish government is "to radically improve the quality of service to personal and business customers of Government and to develop and deploy the Public Services Broker to help agencies achieve that improvement". In July 2004 plans were announced for the development of a Public Service Card (PSC) which could comprise a number of existing cards and new services like the social welfare card, the medical service card, revenue proposal, drivers' license, youth alcohol card and integrated transport ticketing. An expert group has been established to introduce a standard framework for the card and work out the costs and benefits of the project. By developing the card the Irish government expects to provide citizens with a convenient way of accessing public service while also significantly facilitating the secure identifications and authentication of users.

A Code of Practice for the proper use of a 'Personal Public Service Number' in accordance with relevant legislation has been established. The PPS number eliminates the possibility of confusing one person with another and makes it possible for public bodies to deal in a faster and more efficient manner with their customers. The number was introduced in 1998 but is now repositioned for a more general eGovernment support. The number will be incorporated in the PSC.

Italy
The Italian national ID card project called CIE (Carta Identità Elettronica, electronic identity card) is positioned to replace the 40 million existing paper based identity

cards. The project was launched in 2001 and the first experimental phase ended in June 2003 with about 100,000 cards issued in 83 municipalities. The second experimental phase is running in 2004 with 2 million cards in production of which 600,000 have already been dispatched to 56 municipalities. Municipal authorities are distributing them now to citizens older than 15. In the third phase (2005-2009) all municipalities will issue the cards to all citizens. The aim is to issue the cards in the next 5 years at a pace of eight million cards a year.
Instituto Poligrafico e Zecca dello Stato issues and initialises the cards but this needs to be followed by the addition of the cardholder's information and data necessary for the services by town administrations.
Technically the card is a contact smart card of 32 KB with an optical stripe on the same side of the card with a capacity of 1,8 MB. The card contains a set of personal data, including the holder's fiscal code and blood group and a template of the biometric fingerprint is embedded in the chip as well as in the optical stripe. There is one digital certificate on the card used for access to e-services. However the certificate holds no personal data. A service provider may acquire these from the Ministry of the Interior (CNSD-INA) via an on-line process. Fingerprint and certificate are only stored in the chip and not in a central or local database in accordance with Italian data protection legislation. These data can only be released and used if the holder gives his permission by inserting a PIN code.
From a functional perspective the card is a travel document, but is basically positioned as an easy and efficient access to public services. It does not support the digital signature for non-repudiation. Some active services are : age check at cigarettes machine, identification check at the polls, check of a citizen's fiscal position, access to SIM (Mountain Information System).
Under preparation (Q 2 2004) are Civil complaint filing and status control, Criminal complaint filing and status control, Payment of social charges for house servants, income tax return payment.
Some operational local services are: Payment of Waste Collection Tax (TARSU), Children school enrolment and school fees payment, City Residence and Street Residence change, Payment of fines. Examples of services in under preparations are: Enrolment to local sport centres, Booking of hospital admissions, medical visits, medical tests, Welfare requests filing (social support checks, scholarships, …), House Local Tax (ICI) variations and payment, Economical support to disadvantaged people (elders, orphans, …), etc.

The infrastructure required to access registry and demographic services and validate the card's data has in Q 2 2004 already been deployed in all of the 8.102 municipalities, with 23 million data controls and alignments already performed. Municipalities taking part in the pilots have already activated 272 services, including access to demographic and tax services, electronic payments of taxes and fines, guided self-certifications, and status checks of administrative procedures. Other functionalities are being tested, such as the payment of waste taxes in local tobacco shops, and several municipalities will also test the electronic ID cards as a way to electronically identify voters during the forthcoming European elections.

Another development in Italy is the CNS (acronym of "Carta Nazionale dei Servizi" – National Services Card). By decree of the Italian Council of Ministers in February 2004 it was laid down that all Italian citizens will be able to access all of the country's e-government services using a single smart card. The card aims at becoming an access

mechanism for all existing and future Italian e-government services. When inserted in a special reader, the CNS card will identify its holder online and allow interaction with the public authorities. In June 2004 an e- payment function has been added to the card. Due to an agreement with the Italian Bankers Association the card may be used as an access mechanism to an existing financial service for online payments called Bankpass Web. These new services will first be tested in Bologna and Verona. The Italian government believes that the implementation of the new cards will concur to the further development of the country's e-government services.

The card will be equipped with a microprocessor containing data identifying its holder, including a personal ID number. It will not hold a picture of the cardholder so it will not constitute a "proof of identity" in the physical world and will therefore complement rather than duplicate the national electronic ID card.

There is a legal arrangement that the CNS card is only complementary to the national IFD card. The Decree of the President of the Republic n.117 of 2nd March 2004, containing "Regulations on the diffusion of the National Service Card", states in Art.2, Paragraph 3: At the time of issuing or renovating the national service card, the administration, by means of the telematic services made available through the National Index of Personal Data Registries (INA – Indice Nazionale delle Anagrafi) checks the validity of personal data and verifies the person is not already a holder of the electronic identity card (CIE). If the personal data are valid and if the applicant is not holding an electronic identity card the administration issues the national service card.
So it may be expected that in due time the 2 cards will merge and only the CIE will prevail. Nevertheless the Italian Government has set a target to distribute 10 million CNS cards before the end of the current Parliament in 2006.

Latvia
There is a clear interest in eID on the Government side but so far no projects are under construction.

Lithuania
A new personalization centre for different kind of ID documents for its 4 million people has been installed in Vilnius in October 2002. A volume of 1.5 million ID cards in ID-1 card format are to be personalized in 2003 and 2004. Data capture will take place decentrally in 100 special offices from where the information is transmitted

to the personalization centre. The documents are positioned as secure documents with modern engraving technologies but do not support electronic access to services.

Luxembourg
There are no plans for a national eID card so far. Luxembourg has established a software based PKI system with registration and certification authorities for providing services for both the public and private sector.

Malta
The Maltese Government wants to provide an electronic identity to each citizen in the country, designed to enable secure access to e-government services. The eID is not smart card based but consists of a network key in the format of a confidential PIN number such as the ones used with credit or debit cards.
The electronic ID will enable Maltese citizens to access a number of interactive and transactional e-services, such as Income Tax or VAT payments, registration for social services, and access to healthcare services. Citizens will also be able to access over the Internet their personal data held by public administrations.

The concept was developed by Microsoft in cooperation with a local Maltese company.

Netherlands
The Netherlands have at present a national ID card in ID-1 card format. There are about 8-10 million cards in circulation. The legislation for introduction of biometrics in passport is in place, the introduction of a legal obligation to carry ID for every person over the age of 14 years on the basis of existing documents such as passport, national ID card, drivers license is in its final stage of approval. The Government has decided in May 2004 to introduce an overall unique administrative number for citizen/government communication called Citizen Service Number. This number is based on the present social security number and will be introduced from January 2006 on. The legislation for PKI is in place, as well as the accreditation and certification structure.
The Dutch Parliament has instigated that from 2007 on there should be only one Government issued smart card holding an eID function and replacing all other cards issued by Government. The data line of 2007 being in line with the present contract for the national passport and ID travel card which expires in 2006.
As an interim solution a network based National Authentication server is envisioned on the basis of name and password.
A pilot project for introducing contactless biometrics in passports is set to start in September 2004 till February 2005 in 6 municipalities. The applied biometric technologies will be facial and fingerprint (2 index fingers) and cover passports as well as ID cards. The testing will encompass the enrolment as well as the verification process for a target group of 15.000 persons. Two (Canadian) biometric technology providers have been selected and four suppliers of biometric devices are involved. In each municipality a verification system of two different suppliers will be installed where the adequate functioning of the Biometric Test Documents are will be checked.
Since 1993 a smart card project for asylum seekers has been in operation (access control, social benefits payments). Over 350.000 persons have been registered so far

including biometric templates (thumbprint). The central database of the system is connected with the EU Eurodac system.

Norway
Norway has no national ID card. Smart cards with an electronic ID functionality on board are used in the on-line gabling domain. 2.1 million Norsk tipping cards have been issued for this purpose.
The first public election using PKI smart cards for voting was run in 3 municipalities in Norway. The system allowed putting a voting ticket on an ID smart card, and then the smart card could be used in electronic voting booths. An "enablePKI Toolkit" provided the necessary functionalities: signing and encrypting election tickets, wrapping votes in signed and encrypted envelopes, verifying signature, and extracting (anonymous) votes from the signed and encrypted envelopes. In this way, the confidentiality of the votes can be guaranteed.
This first e-vote operation was a success with about 50% of the voters having chosen the e-voting solution. Follow up e-voting pilots are envisioned in particular the General election of 2005.
A law has been enacted on e-voting. It specifies that e-voting from home is not allowed; people have to come to public places for voting.
Norway uses 2 certificates.

A recent survey (Q 1 2004) pointed out that there is in Norway a larger need for reliable eAuthentication than for the electronic signature.

Regarding biometrics, a working group on the introduction of biometric identifiers in the Norwegian passport has been established in June 2003. It is mandated to make propositions for the implementation of biometrics in the passport. The group issued preliminary documents on the costs for 2004 for the preparation of budgets; including an implementation schedule, the establishment of the necessary infrastructure and the preparation of a tender for a new contract for the production and personalization of the new passports.
Social Security Service expects that digital signature will be widely used in the public sector shortly after. The project is developed and implemented by companies within Norway Post and Telenor. Some municipalities have chosen e-ID card deployment for their citizens for use in public services like voting.
Norway has recently developed a national standard for the physical aspects of the card (visual ID).

Poland
The country has plans to introduce an electronic ID and is closely monitoring the solutions and progress in neighbouring Hungary.

Portugal
Discussions are ongoing surrounding the policy issues of e-ID. As it stands today, the documents used for identification in the country are the national identity card or the passport. The Portuguese ID cards feature the owner's fingerprints, though not in electronic format.
Portugal has no plans for electronic and/or biometric authentication published.

Romania

In 2002 there was an announcement that Romanian electronic ID cards might soon become fact. Sources from the Romanian Ministry of Communication and IT were quoted as stating that electronic ID cards are a necessity for them. They believe that electronic ID cards will encourage citizens to make tax payments online while also stimulating Internet usage and online sales generally.
No additional information is available at the moment.

Slovenia
The initiative for a national e-ID project was launched in 2002. The framework for this decision has been prepared for several years starting with the Electronic Communication and Electronic Signature Act, adopted in September 2000. In the same period the governmental certification authority was established, which issues qualified digital certificates SIGOV-CA (Slovenian Governmental Certification Authority) to governmental employees and SIGEN-CA (Slovenian General Certification Authority) both to natural and legal persons (http://www.gov.si/ca/eng/).

The scope of the Slovenian eID project is to provide citizens –on a voluntary basis- with identity card holding a chip with two digital certificates, one for holder authentication and one for the digital signature. In addition, the chip contains personal data and has been prepared to upload biometric data, which will be defined in compliance with the EU ePassport regulation, once available. Recently also the addition of contactless technology has been considered.

The Slovenian national e-ID project is divided into three phases. The first phase, which is in progress is a pilot project. This will be followed by the second phase which is to include the tender and the production of a national eID. In parallel to the two phases, a third phase, which is already in progress, is focussing on interoperability and e-services. The interoperability issue comprises an ongoing discussion with the banks about possible cooperation and usage of web kiosks as well as the interoperability issues related to eID projects within EU member states. E-services resulting from the third phase comprise already available services such as e-tax return, e-access to personal data in state registers, e-forms, e-invoices. On top of that there is a plan to launch numerous additional governmental e-services which will offer real value and enrich the usage of the national e-ID.

Slovakia
No information available

Spain
After a number of years of preparation the Spanish Council of Ministers approved in February 2004 the creation and distribution to Spanish citizens of new electronic national ID cards. This allows citizens to access sophisticated e-government services. The switch to electronic ID fulfils the first measure announced in the Spanish e-government action plan of May 2003, which aimed at facilitating the access to transactional public e-services for all citizens with the introduction of an electronic ID card. It is anticipated that the new cards will provide secure identification and authentication for a wide range of online transactions, from e-government services to e-commerce and Internet banking.
The smart card based electronic ID cards will contain the following information stored in the chip:

- An electronic certificate to authenticate the identity of the cardholder
- A certified digital signature, allowing the holder to sign electronically
- Keys for its use
- A biometric identifier (fingerprint)
- A digitised photograph of the holder.
- A digitised image of the holder's handwritten signature.
- All the data that is also printed on the card (date of birth, place of residence, etc.)

According to the Spanish Government, the new card will be a secure identification tool both in the physical and the digital worlds. The polycarbonate card will contain several physical security features such as optically variable ink and a security thread. Moreover, security will be enhanced by cryptographic methods and bi-dimensional bar codes. The electronic certificates that will authenticate a holder's identity will be issued by a certification authority, a public body still to be appointed by the Spanish Government.

There are currently 29 million ID card holders in Spain, with approximately 6 million cards being renewed each year. The new electronic card will be implemented in phases, with 100,000 cards to be distributed during several pilot tests to be held in 2004. Large-scale issuance and distribution will then be carried out: 500,000 cards in 2005, 2 million cards in 2006, and 6 million cards in 2007.

From a legal perspective, since the approval in December 2003 of the electronic signature law by the Spanish Parliament, an electronic signature is equivalent to the traditional handwritten signature. The law, which established a legal framework for the development of a national electronic ID card, has among other things introduced a digital signature for legal entities such as companies.

In order to authenticate themselves or to sign electronically online, cardholders will only need their PIN code, a card reader and specific software that will be downloadable from the Internet. The new electronic ID card is meant to become a universal digital signature instrument, valid for all types of transactions.

The total cost estimate is EUR 148.9 million spread between 2004 and 2007 – of which almost EUR 100 million will cover the cost of the pre-printed cards.

Sweden

Sweden has no general plans for the issuance of a national eID card at present. Nevertheless PKI is used in the Swedish public sector to achieve a 24-hour 'one-stop-shop' to government services. With one e-ID, issued by the national post agency, by

BankID, by Nordea bank AB or by Telia AB, which covers electronic identification for eGovernment applications, citizens can communicate with all government and some private sector e-services. So there are basically two channels, which are used by both central and local government: the banks ID-service and the Certificate Service Provider/Swedish Post/Telia/Nordea selling "e-ID and services".
More than 150.000 certificates have been issued in this way.
There are no plans for implementing biometric authentication processes in the near future.

Switzerland
Swiss legislation is the same as in most EU member states regarding e-ID. There is some regulation for private certificates, but in regards to the e-ID card, it's the task of the State to issue certificates. A plastic ID card has existed for the past 10 years, and the certificates will be added to this card. Only basic ID information will be stored on the card. Discussion on the identification is ongoing. In Switzerland, there is no unique ID number; therefore a new number has to be created for the e-ID card. The corresponding law is under preparation.

On 15 September 2004 the Swiss Government gave the green light to a five-year pilot project during which citizens travelling to the United States will be able to request a biometric passport. Under the pilot project, which should start by the end of 2005 and last until 2010, Swiss citizens who need a biometric passport (for instance to enter the United States without a visa) will be issued with a new high-tech travel document on a voluntary basis. All other passport applicants will receive the regular version without biometrics.

UK
A draft Bill to establish a national ID card scheme in the UK was published on 26 April 2004 by the Home Secretary. The proposed Bill, which sets out the legal framework for the incremental introduction of biometric ID cards, is subject to public consultation until 20 July 2004.
This draft bill is another step in the ongoing political debate in the UK on the issue of national ID cards. During both the First and Second World War an ID card system was introduced but abandoned directly after the war. And there is still a strong opposition in the UK against introducing such a token on a compulsory basis once again. Privacy International published in May 2004 research by YouGov http://www.egovmonitor.com/links?124d saying that 1 million people would go to jail rather than carry an ID card, 3 million were prepared to break the law, and 5 million would demonstrate. Privacy International announced the formation of the No2id http://www.no2id.net coalition to stop ID cards, supported by the Liberal Democrats, Plaid Cymru and the Green Party.
A further report into ID Cards published on 30 July 2004 by the Home Affairs Select Committee, gives broad backing for UK Government plans to introduce identity cards but criticises implementation plans and proposed draft legislation
Although the plans are not fully detailed the idea is to have a smart card including biometrics and with the capabilities of a digital signature. An earlier suggestion has been made to position the card as an 'entitlement' card. A public consultation phase on this idea ended in January 2003 but did not bring much result. Another survey, showed however that 80% of UK citizens support the introduction of ID cards and

most people have little or no concern about any potential negative impact on their civil and human rights. This contrary to the Privacy International survey. It seems that the outcome of surveys on this subject in the UK are somewhat linked to the background of the organiser.

One of the main problems for the implementation is that the UK holds no reliable National Personal Data register. The plans foresee the setting up of such a national identity register including biometric data.
The envisioned plans encompass a kind of card-family with a common look and feel consisting of Drivers license, Entitlement card and Passport card.
The basic functionality of the card is the key to provide proof of a unique identity to access public services, to help to ensure the security of the UK, help tackle crime, terrorism and illegal immigration, and make sure that public services can only be used by those who are entitled to them.
It is expected that the card will hold basic personal data such as name, age, validity date, entitlement to work, and a unique identification number will appear on the face of the card. The card will feature a secure encrypted chip that will contain a unique personal biometric identifier. The issuance fee charged to citizens will reach about GBP 35 (EUR 53) for a 10-year identity card.

A first pilot for biometric passports opened to the public in London on April 26 2004, with further locations in Leicester, Newcastle and Glasgow. The Government expects to see ten thousand volunteers across the country sign up. The passports will have a chip on board holding biometrics. The pilot will test facial, iris and fingerprint recording and recognition. Each volunteer receives a personalised smart card carrying both printed and electronic information. Results from the trial will help inform the Government's plans to introduce biometric passports and driving licences, and build a base for the national identity card scheme.

3.4 State of the Art of the eEpoch project

The eEpoch project (eEurope Proof of Concept for a Holistic approach) is positioned to develop and provide a practical demonstration of interoperable and secure smart card based digital identification systems in seven pilot sites over Europe.
eEpoch has a specific activity dedicated to the non-technical knowledge research on pan-European interoperability on Identification, Authentication, and Signature (IAS) based on smart cards. Each pilot site participates in this interoperability demonstration. Every pilot defines its interoperability in relation to each of the other pilots. The eEpoch project assists the pilots in structuring the relations and has set-up a dedicated web based portal to manage the information on interoperability provided by the pilot sites (www.eepoch.net).

From the technical side eEpoch has specified in its Workpackage 3 documentation on an interoperable smart card application that provides Identification, Authentication and Electronic Signature services based on the Global Interoperability Framework. So by definition this eEpoch specification is in conformity with the content of the CWA eAuthentication. This application has been used by the different eEpoch pilot sites. Both a 'Generic IAS Application / System package based on CWA 14890 (Area K) and a 'LOAD of APPLETS protocol' are available.
The pilot site Sheffield (UK) is implementing the WP 3 specifications using available Open Source software which will lead to full eEPoch compliant solutions.
In 2004 the Pilots have demonstrated IOP feasibility in specific test cases leading to encourage governments and authorities to provide IOP on IAS framework at organizational and legal levels. Only the Spanish site is applying biometrics in the system.
The eEpoch project has its final dissemination and end-of-project conference in November 2004 in Brussels.

3.5 eID projects world wide

Argentina
In 1998 a smart card project with fingerprint biometrics was under construction. However the project was stopped due to legal and financial issues and never heard of again.

Australia
Plans for a national smart card based ID project including biometrics have been proposed by the Government but were withdrawn under heavy public pressure.

Australia is very active in the domain of ePassports and works close with ICAO. It is to be expected that Australia will be one of the first countries to implement the ICAO compliant passport (see also Malaysia)

Bahrain
In late 2003, the Kingdom of Bahrain released a RFP for a smart card based national ID card. Bahrain has been selected by the GCC countries to lead a common GCC smart ID card initiative and plans to spearhead this initiative with the launch of its national ID card program. The intent is to deploy a Global Platform based multi application smart card to all the citizens and residents of Bahrain. This card will carry four applications at launch. These applications are eID, Driver's license, Immigration and PKI. The project is on target to launch its first cards by end June 2004. There is an option to include an e-purse into the card.

Botswana
Since July 1998 Botswana has issued 800.000 ID's with biometrics (thumbprint) in a chipcard. Botswana is on its way to a complete national roll out (1.5 M people) . (www.face.co.za)

Brazil
The Secretaria da Fazenda (Finance secretary of Sao Paulo) has started to introduce a smart card for its 9000 employees. The card which includes fingerprint verification serves as a personal identification to guarantee that only authorized personnel have access to buildings and the network. Taking it from there 500.000 users in all States of Brazil will be equipped with such a facility in support of electronic transactions and communication.
The State of Rio de Janeiro is issuing personal ID cards since November 2000 with biometric (fingerprint) in the form of a 2 D bar code. There is no smart chip involved.

Brunei
Brunei is the first country to have implemented a smart card based national ID card including PKI and biometrics (2 thumbprints and photograph) to its complete population. The project started in July 2000 with an 8k smart card and is enrolled to the 400,000 inhabitants.
Former civic registries were replaced by a central database that includes passport and visa information. Foreign residents and frequent visitors are also registered. The biometric data are both on the card and in the central database.

Brunei is presently concluding discussions with Malaysia to integrate its national ID card and Malaysia's MyKad for use in border crossing facilitation; within the common borders between the two countries, using automatic immigration 'autogates'.

Burma (Myanmar)
A National eID project is in progress

Cambodia
A National ID project is in progress. 8 million cards with fingerprint have been issued so far. It is unsure but also unlikely that this project is chipcard supported.

Canada
There is no national eID project for citizens in progress. A plan by the Ontario government for a multifunction citizen ID card (including health information, hunting and fishing licenses, school records and driving license) has been shut down due to budget constraints and strong opposition from among others the Ontario Data Privacy Commissioner.
However Canada has announced plans for s smart card based ID for 130.000 workers at 29 major airports. This is in line with the US activities. In this domain.
The chipcard will hold two biometrics (fingerprint and iris) to identify the workers before giving them access to restricted areas.
Also Canada issues a Permanent Residents card in ID-1 card format with an optical stripe on the back. On December 31, 2003, the PR card became the required proof of status document for every permanent resident returning to Canada on a commercial carrier (airplane, boat, train or bus).
The card has a laser engraved photograph and signature, as well as a description of the physical characteristics (height, eye colour, gender) of the cardholder printed on the front.
The card's optical stripe contains all the details from the cardholder's Confirmation of Permanent Resident form or Record of Landing document. This encrypted information is accessible only to authorized officials (such as immigration officers) as required to confirm the status of the cardholder. The card cannot be used to monitor the activities or track the movement of the cardholder.

Chile
According to information from Eurosmart this country is tendering a national eID program or is already in the deployment phase.

China

On June 28 2003, the Third Plenary Meeting of the 10th National People's Long-standing Committee approved "The National Citizen ID Law of the peoples republic of China", becoming effective on January 1, 2004. By now the Chinese government has officially kicked off the world largest National Citizen eID system issuing ultimately contactless chips card to 900 million citizen over the age of 16 to be completed by the end of 2008.
These numbers might even raise as Chinese infants are now entitle to ID cards that they previously could not get until turning 18.

Nationwide distribution of the new electronic ID cards will begin in 2005 – when the traditional paper ID card will stop being issued. Since the mid 1980s when China began using ID cards 1.3 billion cards have been issued. 900 million people actually hold ID cards at present.
A limited distribution scheme of the new card was kicked off on 29 March 2004 in the cities of Shenzhen. There is also information that in 2004 cards 200.000 cards will be issued to residents of Shanghai's Jiading and in the Chongming districts. Later information showed that the take up by the Citizens was less then expected. In April 2004 only 30K cards had been issued at the time.
Personal identification data are printed on the cards and stored both in the card's microchip and in government databases. These includes name, gender, date of birth, address, 18-digits identification number, colour photograph, issuing authority, validity period.

The core of the new ID cards is an embedded microchip storing an individual's personal information, which can be read electronically and checked against databases kept by China's security authorities. Residents of most major cities also will carry other chip-based cards that control access to social services.

In their public justification for the new cards, Chinese officials have focused on how the cards can help solve a major law-enforcement problem: Paper IDs can be forged easily, contributing to fraud and financial crime. The contactless smart ID card should be much harder to counterfeit.

The amount of information to be stored on the new ID card is dwarfed by the data on social-security cards coming into use in many of China's big cities. These conveniently link account information for all the government services that a person receives, including medical care, welfare benefits and employment assistance.

The introduction of the cards will be accompanied by a major upgrade of the security ministry's databases and computer systems

The card material is PET which is environment friendly and durable for more than 10 years according to the Chinese authorities. The centralized ID card production will be applied in each province respectively.

The Smart Card Forum of china has a website at http://www.scfc.org.cn/

Columbia
4 million ID cards have been issued with biometrics (fingerprint). No information if the project is smart card supported.

Costa Rica
Costa Rica's new ID card is positioned for voting purposes for 2.3 million voters of its 4 million population. It is an electronic ID card but not chipcard based.
The card can be used for many types of transactions within the public and private sector, from obtaining driver's licenses and passports to banking and paying taxes. The cards include the person's photograph, signature, two fingerprints and a bar code containing all the minutiae associated with the fingerprints. The electronic information ensures that there are no duplicate cards issued. When a citizen enrols to obtain a new card, there is a check of the persons live fingerprint against a database containing all the existing images and records.

Egypt
Since January 2001 Egypt has issued 42 Million ID's with a supporting biometric fingerprint technology. There is no smart card involved. (www.gdm.de)

Guatemala
In July 1999 Guatemala awarded a contract for a national ID card project including fingerprint biometrics in a 2D bar code format. The card has the function of a travel document. In 2004 1 million cards are expected.

Hong Kong
In August 2003 the government of Hong Kong (Immigration Department) began issuing new multi application eID cards (SMARTICS) to its citizens.

The replacement of the present paper based ID cards – in use since 1987- to all those over 11 years old of the 6.9 million residents of the city is expected to be completed in 2007.

The card contains a contact chip, has the Multos Operating system on board and carries besides personal data biometrics (facial image and two thumbprints). Cardholders can opt to have a digital certificate loaded into the chip.

The government began issuing smart cards to new arrivals, children eligible for a juvenile ID card on reaching age 11, 18 year olds eligible for an adult ID, individuals applying for replacement cards and those changing data on their ID cards.
Existing ID card holders have been called up through public announcements to attend the Smart ID Card Centres in groups, in accordance with their year of birth.
Nine Smart ID Card Centres have been opened to accept applications under the replacement exercise. Residents must attend in person to have their ID cards replaced.
So far 1.2 million cards have been issued.

The card supports the following functions:
- Immigration applications (deter illegal immigration, automated passenger and vehicle border crossings including the busy crossing with the rest of China)
- various government and commercial services like eGovernment (change of address, online voter registration services), Library services (more than 60 participating libraries) and Driving Licence-related functions (from 2006 on). The inclusion of non-immigration applications is optional. Cardholders have a free choice to decide whether to include the applications in their smart ID card or not. Hong Kong residents are also given the option to apply for one year's free use of the Hong Kong Post e-Cert which will be embedded in the chip. Having a year's free use of e-Cert will promote awareness and growth of the service. Hong Kong expects this will also encourage and drive industry initiatives to develop new business applications or services relating to the use of e-Cert on smart ID cards. There are plans to add electronic cash in the future.
In the introduction phase much effort was put to address the public concerns of privacy. As a result of these efforts the project now has broad support.

The overall project cost are estimated 250 million Euro.
More information on www.smartid.gov.hk.

India

In August 2003 India has started it smart card based multi purpose National ID card project. The Office of the Registrar General (Ministry of Home Affairs) has launched its first tender for the enrolment of 3.1 million citizens in 13 districts.
The card will hold personal data like name, sex name of the father, date of birth, place of birth, address and biometric features. It supports PKI and will have digital signature capabilities.

One of the reasons for the national eID project is in the immigration and border control domain. The use is to identify Indian National Citizens in sensitive border districts, which are suffering infiltration from bordering countries bringing both socio-economic and security risks.
A second consideration is the fact that India with its population of 1 billion people has some of the largest welfare programmes in the world with over 100 million registered people for which smart cards and biometrics are already in use. National standards have been mandated for smart cards. India has developed its own multi application smart card operating system for the transport domain but wants to apply this as part of its general smart card platform.

Israel

In 2001 a tender for a smart card based national eID card was issued and concluded in 2002. Due to legal problems this is however still in procedure so there are no cards deployed yet. The eID card is part of a wider approach, geared to allowing people to receive most government services on-line by creating a government administration that works better and more efficiently and costs less to the public. The Government on-line system will serve as a one-stop shopping gate for the citizen, enabling electronic access to information and Government services. For this purpose most government sites will be connected and brought on-line. The Israeli government portal currently provides access to about a hundred sites, which includes information from all government ministries and agencies. The sites include data and information about various aspects of the scope, responsibilities and activities of all offices as well as information on the economy and the social aspects of the country and offer the possibility of filling forms and applications online.

Another smart card project is that of an employee card for government employees. It is expected to distribute up to 150, 000 cards in the long run, and about 10, 000 cards in short term. The employee card will be multi-functional, providing physical access to parking and government buildings, interfacing to time and attendance systems, providing a “login” functionality and digital signature.

The Israeli approach is that there should not be much data on the card, and that any such data will be “constant” data.

B2B applications in government (procurement) are being tested, as well as the interoperability of card readers and cards from different vendors.

There are 2 registered commercial CAs. A complete PKI architecture including the realisation of a government “root CA” is in progress.

An Israeli Government Standard for the Implementation of National ID-documents based on PKI Smartcards was published in February 2002. It is positioned to ensure that all government applications that include smart cards will be interoperable.

Ivory coast
In Ivory Coast the Caisse d'Epargne et des Chèques Postaux de Côte d'Ivoire (savings bank) is issuing smart cards holding biometrics for strong authentication of its customers. So far financial transactions are conducted on the basis of signature verification only. A pilot of 5000 cards has been completed and the roll-out has started. The problem is that there is no usable national ID document. The roll- out will cover some 500 K cards. The card is a 32 Kb Java 2.2 card compliant to Global Platform 2.1.1. The biometrics is ID-3 with on card matching.
The Government has already issued 9 million paper based ID cards with fingerprint.

Japan
A smart card based national eID card (Japan Resident registration card or JUKI card) is in its deployment phase. In accordance with a new personal authentication law, all local governments have started to offer RA services to their residents from January 29, 2004 on. Cards as well as certificates are issued on a voluntary basis. Because of the needed assurance of the secret key the authentication law supposes the use of smart cards, i.e. the resident registration card.
The card enables the cardholder to receive on-line e government services. It is positioned as a multi application card but different applications need the official approval by government of municipal law.
The card has different memory areas for basic information (resident registration code), and for the applications where the following services are supported: personal authentication, certificate issuance, library, facility reservation, health care, payment.
In an earlier stage (2003) the cards were successfully piloted by 21 municipalities with a total number of 1,2 smart cards deployed.
The take-up by the Citizens is so far much less then expected. From August 2003 to September 2004 about 250K cards were issued on request of the citizens while the expectations had been in the order of 3Million cards. The background for this is that the card services of e-ID and digital signature are not considered convenient enough at the moment. Also additional applications are strongly needed. Areas such as healthcare and payment services are envisioned. The strategy remains that all e-Government services should be concentrated on one card.

Japan strongly favours the contactless technology. The card is positioned as a Multi-application card with post issuance download capabilities. The card is PKI enabled. There are no biometrics involved, the user authentication is PIN based.
The personal data on the card are derived from the National Population registration system (national ledger) .

Japan intends to start issuing ICAO compliant ePassports from March 2006.. The first tests using ISO/IEC 14443 type B compliant technology will take place at Narita airport starting in February 2005. Calls for participation have already been issued.

Korea
The Korean Government did a feasibility study in 1996 for a smart card based national ID card holding personal data, a national ID number, health insurance

information and also a credit card as well as a public transport function. Due to privacy concerns from the general public the project was stopped.
However – following the developments in other Asian countries the Ministry of Information and Communication is looking once again into the possibilities.
Korea is very active in the chipcard domain. In Seoul a smart card based public transport program is active. In summer 2004 this card will be replaced by a multi application card which supports beside public transport the functions of cash card, credit card, mileage program etc. Nearly 20 Million cards will be issued around that time.

Kuwait
According to information from Eurosmart this country is tendering a national eID program or is already in the deployment phase.

Macau
Macau (a former Portuguese dependency, since 1999 part of the People's Republic of China) started in 2002 to issue a smart card based electronic ID card to its 540,000 citizens. In Q 1 2004 around 60.000 cards have been issued. Macau expects to have the roll-out completed in a 4 year time span.

The Macau eID card issued by the government's identification department (DSI) is the cornerstone of the modernisation of government administrative processes. It supports the new Macau e-government to operate with high efficiency and intelligence. Faster and more effective border-control (eGate) is one of the first targets. Moreover the multi application card will provide card holders with convenient access to public services and secured channels for electronic transactions. Cardholders will in the future be able to download additional applications (e.g. student card, medical card, social security card, e-purse functionality) to the cards via public kiosks or the Internet.
The smart ID card comprises biometric identification (dual fingerprint) and a digital signature function. The card issuing process takes approximately twelve working days. The card is supported by a web-based card management system that operates according to Global Platform standards, featuring integrated public key infrastructure (PKI), post-issuance application downloading, authorisation control and key management.

Malaysia
The Malaysian multi purpose electronic ID (MyKad, internet extension for Malysia + Malaysian word for card) is the most advanced and largest eID project in the world. The Government Multi Purpose Card project is part of the Malaysian Multi-media Super Corridor initiative. This project is one of seven flagship applications deployed by the Malaysian government to attract leading edge technology development to Malaysia. Conceptualised back in 1997 the MyKad project was awarded to a consortium in May 1999 with an official launch in July 2001. In May 2004 the card has been issued to 11 million people. It replaces the present paper based identity card that is issued to every Malaysian citizen over the age of 12 years. It is mandatory for all Malaysian citizens (above 12 years old) to be in possession of an identity card. There are 17 million paper based identity cards in circulation on a total population of 21 million. The government expects to have issued 18 million eID cards by the end 2005. This scheme is on target.

The MyKad incorporates the Malaysian national identity card as one of its primary functions. This application is the foundation for the project and forms the basis for it being accorded such high priority by the government. Fraud is fairly high with the old paper based cards. By introducing chip cards the risk of fraud is largely reduced. Also the Malaysian Passport application, owned by the Malaysian immigration department is being incorporated in the MyKad. This should allow cardholders to pass through passport control desks more quickly, and will also eliminate the requirement of manually processing the cardholders entry or exit. However the card does not replace passports for overseas travels.
The Drivers License application is also integrated in the card. A data file in the MyKad has replaced the existing paper based driving license. The Government wanted to realise a better management of driver records and more accurate tracking of errant drivers. There are currently approximately 7 million paper card-based driver licenses in the country. Both the immigration and driver's license application are automatically loaded into the eID chip at the time of card application.

The card is also positioned as a national health card, which enables Malaysian citizens the access the free or subsidized health care provided by the government. Personalised medical emergency data (allergies, medications, medical history) is also stored on the cards.

A second (contactless) Electronic Purse was recently added on the card. This complements the existing contact Proton purse and allows payments for retail transactions, tolls on the highways and parking. An upcoming use would be the payment on the urban transport networks. This will add to the convenience of the cardholders.

The card supports an Automatic Teller machine (ATM) application for cash withdrawal, e-debit transactions to pay for government services and to conveniently reload the e-purses. This is a bank controlled application, the Malaysian government having developed a convenient methodology for the banks to capture and control this application on the MyKad.

A PKI based digital signature application to enable users to conduct secure transactions and encrypt data over the Internet using the same PKI infrastructure.

In 2004 the Malaysian Inland Revenue board (RIB) will launch an tax e-filing and stamping system. This will allow tax payers to apply for their tax returns and also get tax forms officially stamped in an on-line process. For this they have to use the digital signature facility on board the MyKad in the communication with the IRB.

For cardholder verification the card holds the face (digital colour photograph) and a pair of thumbprint templates (500 bytes per print) of the cardholder. These are captured during the card application process using a specially designed system.

The chip used in the MyKad was recently upgraded from an ATMEL 32K Bytes EEPROM micro controller device, to a compatible 64K device, both masked with a proprietary multi application Operation System. The card also holds a Mifare contactless chip for public transport purposes, this being the 2nd e-purse.
Chipcard readers has been extensively deployed to police personnel (50,000 units) for checking driver's license and ID. Banks, with the Malaysian government's

permission, are also deploying devices to read and capture information from MyKad as it allows for the paperless registration of new account holders, the capture of the ATM application (and MEPS Cash e-purse) as well as the easy registration of new credit card holders.
At its launch the card cost Malaysians about US $ 5, but this fee was dropped in January 2003.

One of the big advantages in support of the project was that the Malaysian government had already a very effective National Registration Department that was charged with the issuance and maintenance of a paper based national identity card. It was this agency that was chosen to lead the deployment of the MyKad project. From the onset of the project, the guiding rule was that, as much of the business processes for the existing identity card system would be retained as possible. This was a crucial element in the success and rapid deployment of the project.

Malaysia is also very active in the domain of e-passports. 5 million passports have been issued since 1998 of different generations but all including biometric templates (2 thumbs). Malaysia is now on its way of adapting to the latest ICAO specifications and might very well become the issuer of the first fully ICAO compliant ePassport world wide.

Mauritania
Mauritania is in the process of issuing a national ID card to its 1.1m citizens. The card uses fingerprints for verification purposes.

New Zealand
The year 2004 Budget endorsed a phased approach to all-of-government online authentication (referred to as Initial Implementation). This Initial Implementation consists of five discrete work components of which two are of relevance for this report.
Firstly accredited standards are being created which will support all-of-government authentication by standardising data, processes and systems. This will include standards around Keys (i.e. access codes such as user name/passwords) that will be used to support agency applications and all-of-government online authentication.
Secondly (and using these standards where appropriate) a trial is likely to be run to use centralised infrastructure to support selected agencies sharing a Client Key (for instance a name/password).
These are however no smart cards involved at this point in time in NZ.

Nigeria
Nigeria has an active project for its population administration and National ID card. The creation of the citizens database started in 2002 following a 2 step approach, enrollment throughout the country and identity data processing with card delivery. For the first stage 60.000 mobile registration units have been deployed throughout the country. For verification purposed a centralized date base has been constructed holding personal identity data, photograph and fingerprints for the 60 million people population. The ID card is in an ID-1 format and holds personal data, photograph and fingerprint. The latter is also coded in a 2D barcode. There is no embedded chip in the card.

Oman (Sultanate of)
The Government of Oman (Royal Police Department) awarded a contract in October 2001 to issue eID cards to its 2.7 million population of which 0.5 million are non-residents. The first cards were issued in a pilot phase during January 2004. The results of this pilot were positive and the full roll-out has since started. The personalisation is decentralised with the support of a centralised national database which can be decentrally accessed. . The complete enrolment, personalisation and issuance process takes 30 minutes and is conducted in a convenient 'ready while you wait' mode. The card which is mandatory for all citizens over 15 years old is expected to be fully deployed by the end of 2006. Non residents pay 30E for the card, citizens pay less.

The card will be used initially for personal identification and authentication, immigration purposes, and as a driver's license. It will subsequently be used as an emergency health card.
The smart card contains the personal identification data, a digital photo and uses a biometric (thumbprint) for cardholder authentication. The chip contains an eID applet in addition to a PKI applet. The on board PKI application is restricted toGovernment employees only during the first phase. The system components are evaluated to Level EAL5+. ?

Philippines
The Philippines Bureau of Immigration plans to issue a smart card carrying biometric data to identify foreigners entering and leaving the country.
Bids for the ID card system have been evaluated. The plans are to issue as a first step cards to 85.000 registered foreigners.

Peru
A national ID card projects has been active in issuing cards to 13 million people. The project includes fingerprints for verifications purposed. These are however stored as a 2D bar code)

Puerto Rica
According to information from Eurosmart this country is tendering a national eID program or is already in the deployment phase.

Quatar

According to information from Eurosmart this country is preparing specifications for a national eID program

Russia
The City of Moscow is issuing contactless social security chipcards to Moscow residents. So far 1.5 million cards have been issued. Many more millions of cards are envisioned as a large percentage of the Moscow population is on social security. The card stores social benefits details, health insurance information, metro ticketing and retail discounts. The cards have identifiers (templates) but in accordance with privacy protection hold no direct personal data.. There is, however, some discussion on introducing a national identifier. An e purse (supported by VISA) is also envisioned to be added to the functionality.
A contactless electronic Transport card (but also without a strong Authentication function) has been issued in Moscow and Petersburg to more than 1 million students.
In September 2004 it was announced that biometric identifiers would be introduced into new Russian passports issued after 1 January, 2006. A special working group is preparing the legal and technical basis for phasing in the new passports. The project will take a number of years to introduce fully in this large country with a population of 144 million.

El Salvador
A national large scale eID project is in progress. 2 million cards have been deployed so far. The card holds a biometric identifier.

Saudi Arabia
According to information from Eurosmart this country is tendering a national eID program or is already in the deployment phase.

Singapore
The Ministry of Home affairs of Singapore has developed a national eID mainly positioned as an immigration express system in order to react to a growth in the visitor arrival and departure volumes In the border control domain. The Ministry aims to address issues like: combat visa and passport forgery, protect against terrorism, deter illegal immigration and worker entry, prevent criminals from escaping from the country.

The system consist of a smart card holding encoded information, photograph and fingerprint (thumb) for 1:1 verification. The system is in place and offers fast (5-10 seconds) border passage clearance.

South Africa
The SA Government is in the process of converting the existing paper based biometric records of its citizens into an electronic database, ensuring uniqueness of records using an AFIS system. The SA Government is also planning to replace the existing paper based ID book (a personal data booklet) issued to citizens by a smart card. The electronic database will offer online verification against a scanned fingerprint, while the smart card ID will offer both off-line and on-line verification. The Smart Card ID will give citizens access to a number of Government services, e.g. social security. The card will be contact based and will hold the personal data and biometric data of its citizens. At present biometric data of more than 30 million people are held

by the Government in a paper based form. The process of transferring these into a central database is in process and the database is already filled with data of approximately 2 Million persons. The PKI requirements in relation to the card are still under consideration. The total population/card base of SA is about 43 million. The card system is expected to be tendered in Q1/Q2 of 2004.

Taiwan
A smart card based national health cards project is active and 2 million cards have been issued. No information yet on a national ID card project.

Thailand
The Thai Government has started in November 2003 the issuance of a smart card based multi-application national ID card to its citizens. The card is positioned as a communication tool between the Government and the citizen. It supports services from 34 Government bodies. The main purpose of the card is to bring the level of fraud down. Thais have now separate cards for tax, health, social security and the divers license. The current plastic ID card is mandatory for all Thais over 15 of age. The new combination is called the 'e-card'.
The card electronically holds the citizens' personal data, insurance information, healthcare data, social security details from the Labour Ministry, tax information from the Inland Revenue Department and drivers license information. All 61 million citizens of Thailand from the age of 1 year will receive the card, but the first batch of 16 million goes to farmers, government employees and citizens renewing their old ID cards.
The Thai Bureau of Registration Administration as the principal went for an 'open platform' card, including Java Card, to allow to add applications post issuance. They choose Java-based chip cards with 52 kilo-bytes of free memory for applications. The cards include digital fingerprints for biometric verification of the cardholder. Nevertheless a government official has said that the first batch of cards did not cost more than 100 Thai baht apiece (US$2.40).

Trinidad and Tobago
According to information from Eurosmart this country is tendering a national eID program or is already in the deployment phase.

UAE (Union of Arabic Emirates)
The UAE has started in March 2003 a project for the development, integration and deployment of the issuance and deployment of electronic ID cards to its citizens. The card is positioned to support all communication between the Government and its citizens.
In August 2001 the UAE has launched a project to keep deportees from re-entering the country. This project is holding data of 250.000 registered persons and uses iris scan as biometric verification technology.

Uganda
A National eID project is active with face recognition as biometric verification mechanism.

US

There is no active national eID project for citizens in the US and the Bush administration is not in favour of such an approach. The driver's license issued by the federal states act as a de-facto ID but this is very fraudulent prone and has rather weak issuance procedures. (Report: License to Hide, Security Implications of America's Lax Driver's Licensing Laws, April 2004).
This leads to initiatives such as the private sector Verified Identity Pass, Inc, where the control mechanism for identity proof of the US Citizen comprises a screening process with database search and a face-to-face in person interview leading to an issued 'secure' smart card with biometrics on board. .

There is however a high profile smart card based eID project active under the label of CAC, Common Access Card. This card was originally developed by the Department of Defence for the military domain under the name MARC. The CAC is now standardized by NIST and will be deployed for all of the military as well as all the Federal employees. The numbers of issued cards by September 2004 is 5.5 million cards (for 4 million cardholders). . Each day 10-12.000 new cards are issued by 1500 real time automated personnel identification system issuance systems (RAPIDS). The card is a 32 KB Java card which is Global Platfo rm compliant, GSC IS version 2.1 compliant, and Bio API 1.1 compliant.
The main functionalities of the card are strong authentication for accessing computer networks (single sign-on) and physical access to secure areas. The infrastructure supports secure communication and transactions and holds certificates for encryption and decryption of email and to digitally sign email for 2.5 million desktop computers. The card also supports medical benefits and other entitlements of the cardholder and may in due time be upgraded with other personnel and logistics management functions. The card holds personal data, digital photograph, biometric templates and digital certificates. The usage of the card is also PIN protected.

Technically the CAC it is a chip based multi-application card, incorporating biometric verification (matching on card fingerprint) as well as digital signature capabilities (certificates on board). Requirements for the CAC were a Java and Global Platform compliant card with at least 32 K of EEPROM and FIPS 140 evaluated.

Like in Malaysia one of the components for success was the existing database with personal data as well as a personnel enrolment system (DEERS) which was already in place.
US based firm Corestreet Ltd updates the certificate status in cooperation with US Akmai Technologies which maintains a global network with 17.000 servers.

The Common Access Card concept might also be implemented by the Transportation Security Administration for 12 – 15 million transport workers in US airports, seaports, railroad and trucking terminals. This will be conducted in the context of the US Home Security Program. The decision has been made that the TSA card will carry a chip. Also other Government institutes (State department, Homeland Security department, Department of the Interior, Department of Treasury, Department of Veterans affairs, NASA, GSA, Western Governors Association) are considering or conducting smart card projects.

The U.S. General Services Administration (GSA) has recently selected a vendor (Oberthur) for production of new contact and contactless ID cards. The GSA cards

will be issued to employees, contractors, and visitors using facilities nationwide. The GSA announced that 18,000 of the new credentials will be issued.

A Federal Identity Cross Credentialing system is under construction under the acronym FiXs. This would cover public as well as private sector use.

There is also a high level Smart Card Interagency advisory board active (including participants form the White House) to help in coordinating all the different Government smart card activities. Basic High level goals being:
•Establish machine-readable credentialing token as platform of choice
•Adopt interoperability standards
•Require enterprise wide implementation of standards-based credentials
•Safeguard privacy.
A US Government smart card handbook is available at
http://www.estrategy.gov/information/smartcardhandbook.doc

In August 2004 the Homeland Security Presidential Directive/Hspd-12 mandated NIST to develop a Federal Standard for e-secure authentication mechanism and subsequently mandates all Federal Government institutes to implement smart cards for physical and logical authentication complying with this new standard. A Draft of the New Standard will be released for public comments by early November 2004. www.CSRC.nist.gov/piv-project.

Venezuela
According to information from Eurosmart this country is tendering a national eID program or is already in the deployment phase.

Vietnam
A National eID project is active.

Yemen
Yemen plans to issue 5 million national ID cards in a 5 –8 years period. The document will basically serve as a travel document as well as for social security purposes. It will have a coded fingerprint on board.

Chapter 4 Recommendations

This Chapter holds the recommendations of the Workshop eAuthentication constituency. They are directed at the smart card industry, the European Governments in process of deploying smart card based eID systems as well as the European Commission. Although the subject might not be high on the list of 'RealPolitik', for the benefit of Europe these issues should nevertheless be addressed in an appropriate way.

Recommendation 1
e-Authentication, and more specifically smart card based electronic ID, should be considered as a necessary European wide infrastructural element for enabling the information society.

The rationale for this first recommendation is that eAuthentication is an indispensable building block for eGovernment as well as for the e-society. The effect of such a positioning would be that each Member State would have to participate in the European wide implementation of the infrastructure and fill in its respective part of the overall structure covering both the card base as well as the other needed infrastructural elements such as a national personal data register, setting the necessary administrative procedures and having relevant agencies for a face to face issuance process in place.
From a financial point of view the costs would have to be covered directly from the Member States' national budgets, as is already the case for other infrastructures like roads, electricity networks and sewer systems.
Once fully installed and in the exploitation phase the usage of the infrastructure may of course be price-tagged to get a return on investments by Governments. However the pricing should not raise high barriers for mass deployment of eID based services from 3rd parties.
This recommendation addresses the Member States as well as the Smart Card Industry who should look upon this development as a possible break-through in the market that they should favour and consider in their price-setting.
The EC should therefore initiate a study on the exact implications of this recommendation both from the financial and from a responsibility perspective.

Recommendation 2
A legal system for cross border acceptance of e-Authentication/eID should be installed in the European domain.

For the usage of the Digital signature there is a European directive which establishes the legal acceptance and validity of such a signature between all parties concerned. A similar solution is needed for eAuthentication i.e. for the pan European legal acceptance of the on-line verified personal identity. The Member States should support such an action and the EU should take the lead.

Recommendation 3
Participation from European experts in eAuthentication/eID related standardisation activities i.e. in the fields of Smart Cards, Biometrics, Digital signature and eAuthentication/eID as such should be encouraged and supported by all necessary means.

European participation in international standardisation bodies is relatively thin. Only the large smart card industry players take part, send their people to meetings and allow them to invest time in the drafting of documents. European government officials are scarce to find in the standardisation process. Member States and the EC should contribute to the organisation and coordination of this process and instruct CEN to be pro-active in this field and offer CEN the necessary means of support. A good example of such a proactive approach is the recent (Q 1 2004) CEN/ISSS initiative to coordinate standardisation input in the biometrics domain (SC 37 biometrics focus group).
CEN/ISSS should be mandated to organise the distribution of financial support for European participation in the eID standardisation process (CEN 224 WG 15, ISO SC 17 WG 4 Taskforce 9) with a focus on participation by SMEs and Government officials.

Whereas lack of travel budgets can form a barrier for their participation, an extra effort is needed to involve representatives from the 10 Member states that recently joined the European Union

Recommendation 4
A European wide e-Authentication pilot project should be conducted.

As a proof of concept for the validity of a European wide eAuthentication infrastructure, a cross Europe pilot project should be defined and deployed. A relevant number of the Member States should participate in such a project to have hands-on experience with the cross border as well as the domestic constraints.

It should be considered to extend this pilot to include interoperability testing with Japan and the US. The Global Cooperation Forum on Interoperable IAS could be the carrier for this testing.

The eEpoch project with its 7 pilot sites in six Member States could be the starting point or anyway be a reference for the set-up of the eAuthentication infrastructure project. eEpoch should however enlarge its scope to the new member states.
Other EU funded projects like Netc@ards, INSPIRED and GUIDE, could be interfaced with. As such a project should be considered as the first phase of a Europe wide implementation and deployment process, the eTen program of the EC seems the appropriate vehicle for a (low-financial threshold) start of this approach. The initiative should come from Member States and Smart Card Industry partners jointly.

Recommendation 5
European Coordination on eID development is needed

On top of the suggested legal, infrastructural and pilot project as nucleus for EU wide implementation, strategic coordination is needed. Such an activity should keep track of the major developments in the domain and generate more synergy between the activities. The activity should not only address the issues mentioned above but also the activities of the Identity Management related IST projects like GUIDE, PRIME, FIDES, etc. More over it could build on results from completed projects like RAPID and EUCLID. In July 2004 a number of relevant projects were considering a clustering activity to generate more synergy between the projects.

There is a clear example here to follow being the US high level Smart Card Interagency advisory board active (including participants form the White House) to coordinating all the different Government smart card activities (see Chapter 3 World Wide Inventory. In this way a European Identity Management Coordinating strategy might just arrive in time to be at the basis of a common European position on eID and eAuthentication and also arrive in time to prevent eID legacy problems due to National eID implementations as are under way right now in a number of European member states.
The workshop has noted that the EU tender for the Framework to Reinforce the Exchange of Good Practices in eGovernment, i.e. Part 3 Study on Identity Management in eGovernment aims to set up an eGovernment Identity Management working group with representatives from the Member States. This might be a good starting point for this coordination function.

Annex A Frequently asked questions on e-ID cards

What is electronic identity (e-ID)?

Electronic identity (e-ID) is the answer to the need of personal identification for the access to electronic services, such as electronic services provided by government agencies on the Internet ("e-government services").

In the real world a person is identified with official papers or simply because s/he is known by the people s/he is talking to. But how to make sure that a person is who s/he pretends to be during an electronic transaction over a public network? This is particularly important if sensitive data is accessed or exchanged during an electronic transaction as in certain e-government or e-health services.

Electronic identity solutions have the aim to guarantee the identity of a person (or a legal entity, e.g. a company) during the access to e-services and in order to provide the trust to the parties involved in the electronic transaction.

What is e-ID needed for?

E-ID is needed to securely identify a person who is accessing to electronic services, such as e-government services. Secure identification is not required for all electronic ("on-line") services. For example if person XYZ wants to buy a book on Amazon.com, the service provider (Amazon) must be ensured that XYZ will pay for the delivery of the book, but does not in principle need to know the real identity of the buyer.

How is identification handled in the real (physical) world? When do you need to identify yourself? Not when you purchase a book in a shop for example. But when you want to vote, ask for specific certificates in a public administration, request a building permit, etc. the public servant must make sure s/he knows to whom s/he is talking.

The issue of e-ID is basically the same in the context of on-line services. When these services are directly related to a person or a legal entity, as in on-line banking or when accessing to certain public administration services (tax, social security, etc.), there is an need to make sure the person who is accessing the service is really the one s/he pretends to be.

What is an e-ID card?

The e-ID card is a smart card which contains an electronic identity feature, i.e. the data that identifies the card holder and the logical functions to manage this information in a secure manner.

The e-ID card can combine an electronic identity function with a physical identification function on the same support. It is hence able to address both the need for identification in the electronic ("virtual") and the real world. In this case the electronic chip which is embedded on the card stores the personal data needed to identify and authenticate the owner in public and private on-line transactions. The plastic body contains the usual information needed to identify a person (name, photo, etc.).

An e-ID card can be public, i.e. issued by a government or public administration and serve as national ID card, drivers license, social security card; or private, i.e. issued for a "closed" environment, such as e.g. a university (student card) or a company (corporate card).

What information is contained in a public e-ID card?

The CWA eAuthentication defines a common set of data that should be stored in the card to meet the minimal requirements for interoperability. This information can be subdivided into public and private or secret elements, as well as into mandatory and non-mandatory elements. Basically a public e-ID card contains the same information as a traditional ID card. In addition to the information given visually on the card, the data is stored on the microchip together with the necessary functions required to identify and authenticate the cardholder electronically, and to give him the possibility to sign documents electronically. It is however up to the Government bodies in the Member States to implement the CWA eAuthentication.

What are the benefits of an e-ID card?

E-ID cards can provide an extremely high level of security for both real and virtual (on-line) world applications:

1. In the real world the e-ID card, thanks to the combination of physical (plastic card with photo, holograms, special printing, etc.) and electronic (secret information stored on the e-ID card chip) functions, attains an extremely high level of counterfeit-resistance. The means to produce a fake e-ID card are – a priori - out of reach of non authorised institutions since complex industrial equipment and access to secrete information are needed to produce them.
2. In the virtual world (on-line transactions) the e-ID card offers a very high security level thanks to the PIN, biometrics and PKI (Public Key Infrastructure) based functions. Identity theft is much more difficult because only the combination of the physical element (the e-ID card) AND the knowledge of a secret information (the PIN code) AND the verification of a biometric template gives access to a specific e-service.

The smart card is highly resistant against attacks of all types. Furthermore, thanks to the embedded electronic chip the smart card can hold several applications that can share the smart card system resources and infrastructure in a secure environment. Finally the e-ID card is "machine readable", i.e. the verification process can be automated and be done much faster with a higher level of security (e.g. during a check-in operation at an airport).

Which are the benefits for the citizen?

The main benefits are a higher level of security against identity theft, an e-ID card being almost impossible to counterfeit. A single card can provide the security functions for multiple applications and environments in both the real and the virtual ("on-line") world. e-ID supports a reliable (in the sense of "secure") and convenient (personalised) access to on-line services and in particular to e-government services.

The interest of e-government services for the citizen is that they are available 24/24 hours 7/7 days. It is not necessary anymore to go to public administration offices

losing your time in queues – thanks to e-ID it is possible to access a service from any place (e.g. when travelling) at any time. Furthermore a higher level of "dematerialisation" (electronification) will allow reducing paper work and reduce delays for administrative procedures.

What are the benefits for businesses?

The benefits for businesses are similar to the ones for the citizen. Administrative procedures with the government can be handled electronically in a secure manner, reducing time and money for paper handling and physical presence in the government offices.

What are the benefits for the government?

The main interest for governments is first of all the higher security level against counterfeit public documents and the possibility to deploy e-government services. e-government services will provide improvement of service quality, reduction of operational cost and closer relationships with the citizen.

What is the relation of biometry and electronic identity?

Similar to most smart card applications, an e-ID card is protected by a secret code, the PIN code (Personal Identification Number). The e-ID card is hence linked to its owner thanks to secret information that only the owner is supposed to know. But remembering passwords and secret codes is a constraint for the user and the information might get lost or get to the knowledge of some unauthorised person. It's also possible that there is a conspiracy and that the PIN holder is willingly transferring the knowledge of this PIN.

Biometrics allows a person (the card holder) to be identified by her/his physical characteristics, e.g. the iris, the face or hand geometry, the voice, a fingerprint. A biometrics reference pattern is stored on the smart card when the e-ID card is issued. During a verification process (e.g. at check-in at the airport) the biometrics pattern of the card holder is captured again and compared with the pattern stored on the card. The verification might take place in the card itself (preferred) or in some other part of the system. So biometrics are a more secure and more convenient alternative to the PIN solution.

Are e-ID cards a threat to privacy?

There is a risk regarding privacy in each ID system because the data stored in the system might be more easily accessed, once put in a system, and then misused. Therefore security aspects and respect of privacy regulations are at the basis of all ID system design, including e-ID card schemes. The risk is the higher the more information is stored in central data bases.
Nevertheless there is also another side. As Amitai Etzioni, head of the US Institute for Communication Policy studies formulates it: 'There is always a balance between privacy, security and trust. The more reliable the card is, the more privacy you have, both in the off-line as in the on-line environment. Once the identity is verified there is no need for alternative searching in databases, archives etc.' For having our personal data embedded in a card we get trust or anyway a feeling of trust in return.'

Nowadays, people are using on-line services every day and as soon as they log into a website offering a specific e-service (e-commerce, e-banking, etc.), they will need to identify themselves with a user/login name, the most basic form of electronic identity. In the information society, the question is hence not anymore "electronic identity – yes or no?" but: "how is electronic identity managed?"

In principle e-ID cards reduce privacy threats because of their decentralized set-up and since the need for central storage and processing of personal information is reduced. Furthermore the activation of a transaction is under the control of the card holder / the citizen. S/he must present his/her card to a card reader and in general enter a secret code to enable a transaction. Last but not least, the card contains a chip able to carry out security checks itself and e.g. make sure the user can trust the on-line service.

An example of how the central storage of data can be avoided, thanks to a smart card, is an e-ID system using biometrics for user verification: a traditional solution without smart cards stores the biometrics pattern of the user in a central database, where it could be exposed to attacks. In a smart card based e-ID system the card holders' biometrics pattern can be stored on the card and the verification can be carried out in the card or locally, only the result of the verification being transferred to the central system.

Are public e-ID cards mandatory?

There is no European level policy yet for the introduction of e-ID cards. Currently practices vary from one country to another. In some countries public e-ID cards are supplied on demand only, e.g. in Sweden and Finland. In other countries a national deployment to all citizens that have reached the age where carrying an ID document is mandatory, e.g. Belgium, Estonia. In those countries the public e-ID card is considered as replacement of the former paper based identity card and a preparation for the introduction / extension of e-government services in the future.
There is also the consideration from privacy experts that the sheer fact of an eID card being in place will in practice lead to an identity lift, where one has to identify himself in each and every situation. There is also the fear –like in the UK- that if voluntary systems will fail in practice, this will in the end lead to a mandatory system.

The legal framework for eID in Europe will eventually hold the answer to the question mandatory or not.