

# Common requirements for (global) interoperable eID



**Jan van Arkel**, co- chair Porvoo group,  
member of the Global Collaboration Forum on eID



# Rationale for a global eID approach

- global support of eServices for the mobile citizen  
(building block for trust, security, easy access, convenience, service providing only to entitled persons)
- Building a more global (including a EU) society  
(enhancing sense of communicty, offering trust, making persons aware to be a –relevant- part of society by offering a seamless e-services experience)
- global combating of ID fraud and ID theft (causes more and more of a problem)
- global preventing of illegal work and illegal immigration
- global measure of anti-terrorism and combating organised crime
- watch the common EU payment domain!



# Global eID interoperability requirements

## Status:

- A basic set of common requirements has been defined in the context of the Smart Card Charter and the CEN/ISSS Workshop eAuthentication.
- This set was discussed and approved by a special joint meeting in Paris in July 2004 of the Porvoo group, the Workshop eAuthentication and CEN 224 WG 15.
- The set was updated and reconfirmed at Porvoo 8, circulated and posted on the Porvoo 9 website <http://porvoo9.gov.si/documents.htm>
- The set was used as input by CEN 224 WG 15 and the WS MUSSTT
- The issue is once more on the agenda of the Porvoo 9<sup>th</sup> Ljubljana meeting
- The issue is once more on the agenda of the GCF Ljubljana meeting



# Is there a need for additional activity?

## Some considerations

- Right now there is much emphasis on the ePassport developments
- In Europe the eID roadmap is under development
- eID card standardisation is (almost) complete
- eID IOP demonstrators and testing is on its way (problems encountered?)
- However the question needs to be answered: is there still a need for a joint position from the EU, the AICF, US NIST (common IOP project??)
- If yes, is there a role for the Porvoo group?



**Supporting Material,**  
only to be presented if needed for a  
discussion on the content of the  
Common eID Requirements



## High level eID requirements

<b><i>Functional requirements</i></b>	<b><i>Building blocks:</i></b> <i>Smart Card, Biometrics, PKI</i>
Mutual trust and security	Setting security environment, challenge response, trusted channels, multi-factor authentication
Identity (personal data set)	National Population Register, RA services
Authentication (proof of the claimed identity)	PIN and Biometrics
Signature (proof of consent)	Digital signature, PKI infrastructure



# Scope & general concepts

- ❑ The positioning of the system is interoperable electronic ID and eAuthentication in the on –line eGovernment domain
- ❑ The concept is based on the IC 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
- ❑ Legal basis in line with the Thomas Myhr report (for Europe)



# Basic System Functionalities

- ❑ electronic identification & authentication of the cardholder to public and private services
- ❑ electronic signature for legal proof of non repudiation

## Optional functions like:

- ❑ support of confidentiality services, enabling encryption of data transmitted over a network
- ❑ official travel document



# Overall 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.
- ❑ The system shall be future proof
- ❑ The IAS functionality shall be executed in a secure and controllable way



# Cardholder identification requirements

- ❑ The system shall support a secure and reliable cardholder identification function:
- ❑ Personal data of the cardholder shall be held in an electronic form
- ❑ The Personal data set shall contain as a minimum for interoperability:
  - (optional) national identification number
  - family name(s), given name
  - sex
  - date of birth
  - (optional) place of birth
  - (optional) nationality

This file is (optionally) PIN/Biometric protected

- ❑ The Card related data set shall contain as a minimum for interoperability:
  - card issuer name/reference
  - card number
  - country name,
  - date of issuance
  - expiration date



# Cardholder authentication requirements

- ❑ The system shall support a secure and reliable cardholder authentication function
- ❑ A Signature key for authentication purposes
  - shall be present
  - shall occur only once and shall be protected so it cannot be derived
  - shall be protected against unauthorized usage by PIN and optionally by biometrics
- ❑ PIN handling requirements compliant with ISO/IEC 7816-4
- ❑ If biometrics are included the following applies:
  - 1:1 verification compliant to ISO/IEC 7816-11
  - a Biometric OID in support of multiple biometric technologies must be present compliant to ISO/IEC 19785-1
  - Fingerprint minutia data is recommended. Implementation shall be compliant to ISO/IEC 19794-2 (CBEFF format type '0003')
  - Biometric template storage shall be on the card
  - Biometric matching on the card is recommended



# 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
- ❑ For Europe the PKI system elements of the system shall be in compliance with the qualified digital signature as per article 5.1 of the EU directive 1999/93/EC on a Community framework for electronic signatures
- ❑ The PKI system elements shall be in compliance with ETSI QCP 101456
- ❑ The PKI system elements shall be in compliance with CWA 14890 parts 1 and 2



## Electronic signature requirements (2)

- The PKI system elements shall be in compliance with ETSI QCP 101456

The main issues being:

- registration procedures
- information content of a certificate
- liability of the certificate authority
- responsibility for protecting the eID card and its content
- loading of other applications on the card
- renewal of an eID card
- prevention of use of eID card and its certificates
- cancellation of an eID card
- requirements for the supporting PKI (i.e. CWA 14171)
- obtaining and protecting the CA certificate
- obtaining certificate status information



## Electronic signature requirements (3)

- Compliance with CWA 14890 (area K) part 1 and 2:
  - key pair generation on board card
  - storage of keys on board card
  - compliance with 7816/15 (PKCS 15) and Crypto Objects
  - signing function will be PIN and/or Bio protected
  - data to be signed cannot be altered
  - the format for electronic signatures and their certificates shall be interoperable
  - secure messaging shall be supported (symmetric crypto)
  - algorithms as in EU WS eSign algo document shall be supported
  - public available certificate status verifying function for relying parties
  
- PKI shall be implemented in the following way:
  - minimum of 2 certificates (1 for signing; 1 for other functions)
  - compliant with X509 V3 minimum profile:  
name of CA, name of Cert holder, unique identifier of Card Holder /Certholder, period of validity of certificate, serial number of certificate, pointer to info on CA certificate policy