ePassport for IDM in Network-Centric Citizen Life Processes

Basic Idea: Use the ePassport information for Identification in trusted Network based transactions

Focus on:

- The issue of trust and its attributes, the extensions required for deployment of the ePassport in IdM based online transactions.
- An architecture for a network-centric IdM system to support three categories of life processes: eGovernment services, high value private services, and eCommerce

Applications

- Processes and transactions:

  banking, social security, international travel, staying in hotels, high-value purchases, car rental, use of credit card, joining private clubs, admission to a school or university, seeking employment, health services, etc.

- ePassport can be used in European level:

  other identity electronic documents which are interoperable and share similar standards:

  eId card, driver's license, social security card

Today's identity cards

- Identity cards: function-specific, context-dependent
- Information on Identity cards:
  Name, Facial Photo, date of birth, signature etc.

- RFID and smartcard technology
  permits adequate information storage and processing.

- In practice they are used in different context
  (Passport for identification in a Bank transaction)

  THE ABOVE CHARACTERISTICS IMPLY

IMMEDIATE FUTURE

MOVE

MULTIPURPOSE ID CARDS

FEDERATED SERVICE PROVIDERS

Reservations over the risks on privacy and security

Electronic Passports

The European Electronic Passport

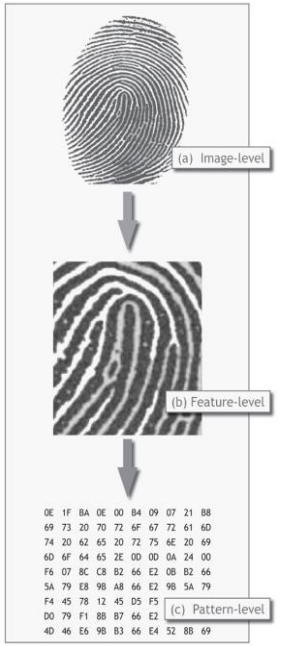
Quelle: Bundesministerium des Innern

Old

- Machine readable passport with MRZ

New

- Electronic passport with face digital image stored in the chip

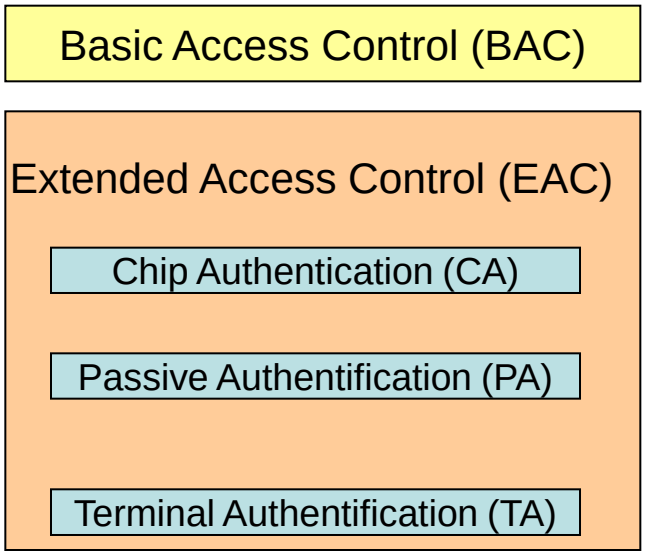


Future

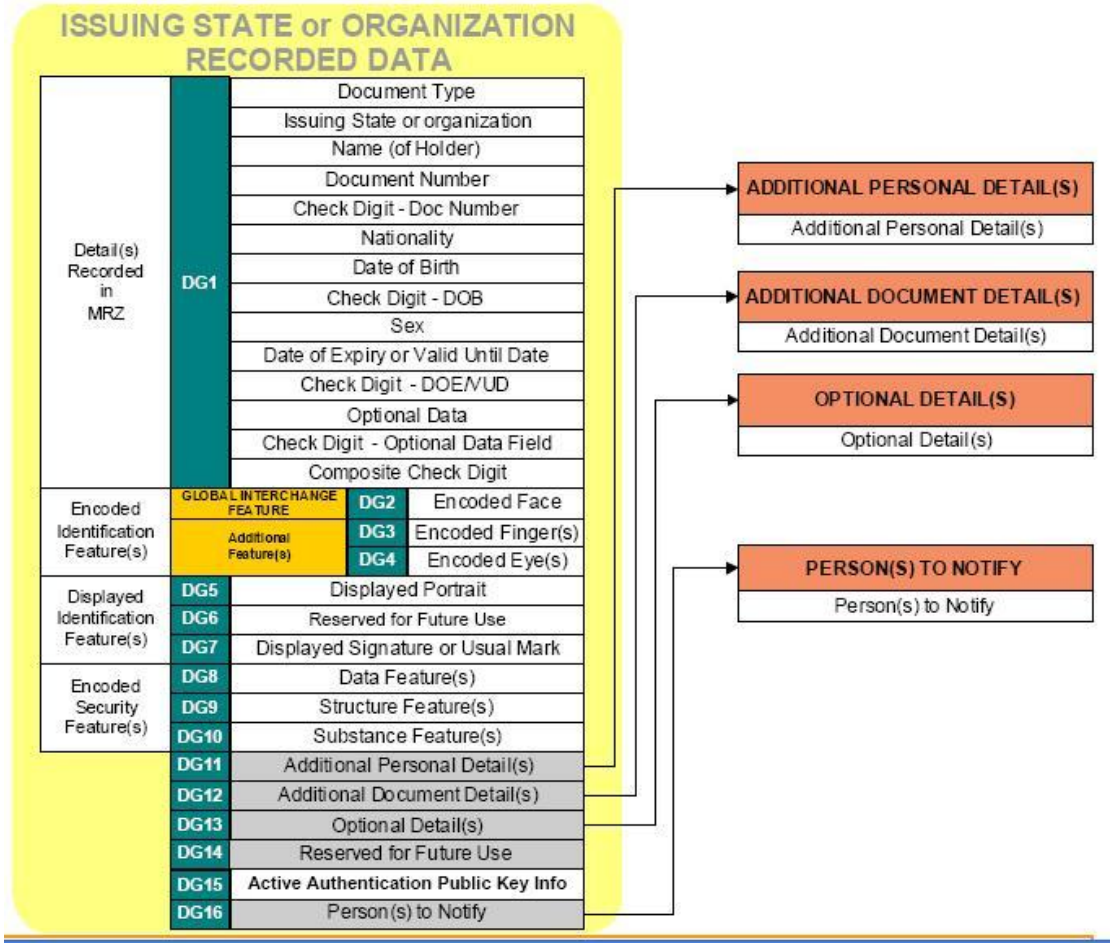
- From 2009 passport with secondary biometric information

ePassport Security Controls

Implemented in European Level



ePassport Data



BAC access control

- The purpose is to prevent a distant reading of the contact less chip without the agreement of its holder
- A key is computed from the MRZ zone reading and passed to the chip in order to obtain an only reading access to the data.
- The access code is calculated from the passport number, the date of birth of its owner and the expiration date
- Allows a dialog between the chip and the reader, preventing any external tapping of the communication.

EAC access control

Chip Authentication (CA)

- ePassport chip sends a static key
- the Terminal (reader) creates a one session shared encryption keys for further secure communication.

EAC access control

Passive Authentication (PA)

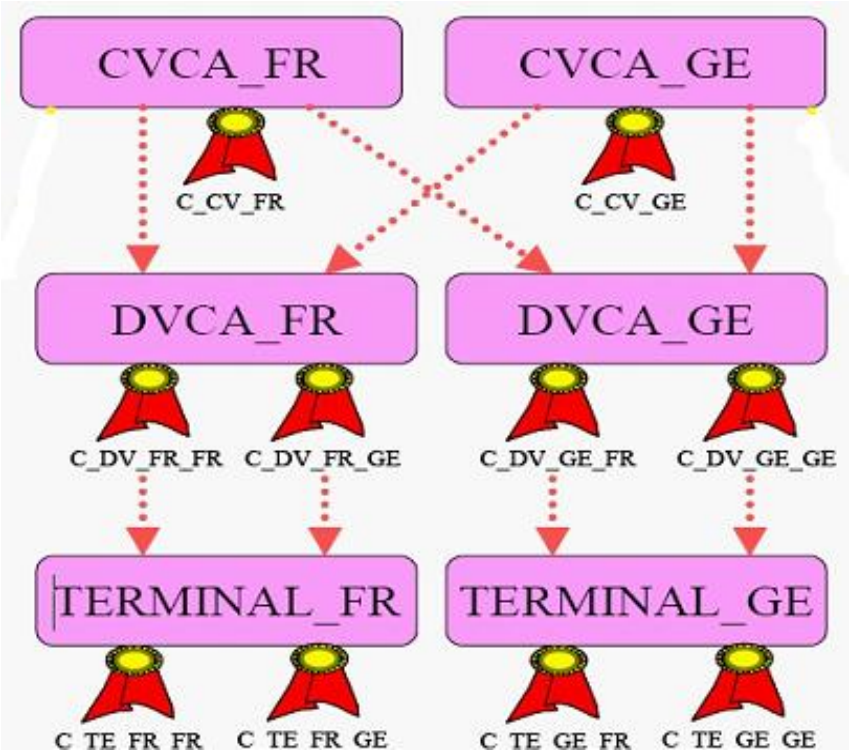
- Control Validity of the Data Group (Logical Data Structure LDS)
- Security Document (SoD) containing all hashes and a signature Document Signing Private Key checked by a corresponding Public Key (DSC)
- The DSC is signed by the corresponding country Private Key and checked with the corresponding Public Key

EAC access control

Terminal Authentication (TA)

- the Terminal (reader) sends a Private Key Certificate issued by a country CA.
- ePassport has stored a Public Key of the corresponding country CA to verify the right of the reader to access the data.

EAC Certificate Complexity



Passports

- Passport is a globally accepted identification travel document.
- ePassports –strong authentication in borders with authorised readers
- Biographical and Biometric data stored
- It is also accepted as identification document for many citizen-centric transactions.

Passport for Network

-Only authorized readers at EU borders can read the ePassport.

-With the diffusion and the maturing of the reader technology it is possible to use the existing technology

-Online services requiring network based Identification could use the ePassport infrastructure.

-This will create trust-based services with better risk control.

-With electronic identity providers we can arrive at augmented function serving other eTransactions

Trust Mechanisms and ePassport Infrastructure

Three parties:

- Beholder (person)
- Issuing state
- Border Control Authorities

(Routine control)

Can the same trust mechanisms transported to Network Identity infrastructure?

Trust relationships

Table 1. Trust relationships and constraints in ePassport infrastructure

Infrastructure Perspective	Roles & Constraints		
	Passport Holder	**Issuing State**	**Border Control Post**
IdM role	principal	identity provider	service provider
Trust relationship boot up	Provides pre-requisites (e.g. feeder documents on his identity) to the issuing authorities	Establishes the pre-requisites to the trust relationship with the principal	Establishes the pre-requisites to the trust relationship with the issuing authorities
Legacy function	Presents the passport as a traditional booklet to authenticate himself. Doesn't know how the scanned MRZ data is used, shared and retained.	Provides identity through a photo and biographic data on a printed page	Uses the visual inspection means to check the authenticity of the passport and match the printed photo with the live subject
BAC minimum scope	In addition to the printed biographical data, also provides primary biometrics (live facial image) to authenticate himself. Gives *implicit* consent to access his biometric data for the purpose of border control.	Provides facial biometric on a contactless smartcard chip, embedded in the passport booklet. Permits passive authentication to anyone with a suitable ePassport reader. Through ICAO membership, implicitly authorizes other ICAO members right to read their chips.	Uses the MRZ data on the printed page to enable access to the facial biometric on chip. May use visual means or image recognition to do the match between the facial biometric and the subject.

Trust Relationships

BAC max scope	No additional action required	Separately provides a digital certificate to authorized service providers for active authentication of chip data. These digital certificates are not highly protected.	Global scope – Needs certificate of the issuing country to authenticate the validity of data on the ePassport chip.
EAC	Also provides his secondary biometrics (fingerprints) to authenticate himself. Gives *implicit* consent to access his biometric data for the purpose of border control.	Provides certificates in a hierarchy of identity providers and service providers. Explicit authorization provided only to other EU countries.	Terminal authentication needed: Requires terminals with explicit authority from identity providers via secret cryptographic keys to enable reading of the secondary biometrics.
Organizational model	National passports / travel documents are recognized internationally as trusted credentials for identity.	National passport issuers as identity providers; implicit authorization to all ICAO states for BAC level trust; explicit authorization to the other EU States for EAC level trust.	No specific steps are required to operate at BAC level; at EAC level, the protection of private cryptographic keys is a major responsibility. Mutual recognition of passports as trusted identity.

ePassport process characteristics

- There is no provision of privacy policy of the service providers (Border Police)
- To use the EAC and additional biometrics, cryptographic keys (provided by national services) are needed assuming the consent of the beholder

Network IdM
Current Approaches

- An Identity Provider corresponds to a number of Service Providers
- Centralised IdP (e.g. Microsoft Passport)
- Federated IdPs (Liberty Alliance , OpenId)

Main Requirements for eID

Network based Identity relies on technical means

- Trust
  - Trusted credentials of the service providers
  - Trust credentials of the identity provider
  - Trusted credentials of the consumers (end users)
- Privacy and data protection
  - Data protection as required by law
  - By the IdP
  - By the SP
  - Privacy protection as civil rights
  - Unlinkability
  - Anonymization
  - Pseudonymization
  - Unobservability

Main Requirements for eID

- Security
  - Communication security – confidentiality, integrity, availability, non-repudiation
  - IdM infrastructure security
  - Protection against identity fraud (protection of identity)
    - Authenticity of breeder documents (proof of identity at the time of enrolment)
    - Binding between the user with trust credential at the time of authentication
- Interoperability
  - Between diverse identity providers
  - Between identity providers and service providers
  - Between the IdM system and the user environment (context)
- Usability
  - Ease of use
  - Accessibility
  - Efficiency
  - Adaptable to widest range of users, use cases, life processes

Risk Based Authentication

Table 2. Risk-based Authentication Options

Authentication Level	Risk assessment by Service Provider	Registration Policy of the Identity Provider	Means of User Authentication	Examples	Primary Concern
0	No risk – no damages	No proof of identity required; self-certification; Unlimited period of enrolment	None or Userid / password password strength not enforced	Chat rooms, email services; shopbot search; blog hosts	Privacy, usability
1	Low –small damages	Weak proof of identity: by referral of a trusted token or trusted identifier; Implicit identity verification through an online payment gateway; Unlimited fixed period of enrolment	Userid / password password strength may be enforced; repeated authentication attempts blocked	Online shopping; Low-value social networks	Data protection, usability; security
2	Medium – significant damages	Remote enrolment accepted; online validation of identity; off-line validation Periodic re-validation of identity and privileges	Identity tokens (software or hardware), Biometrics	Online tax filing and other eGov services; High-value social networks	Trust, Security, Data protection, Usability

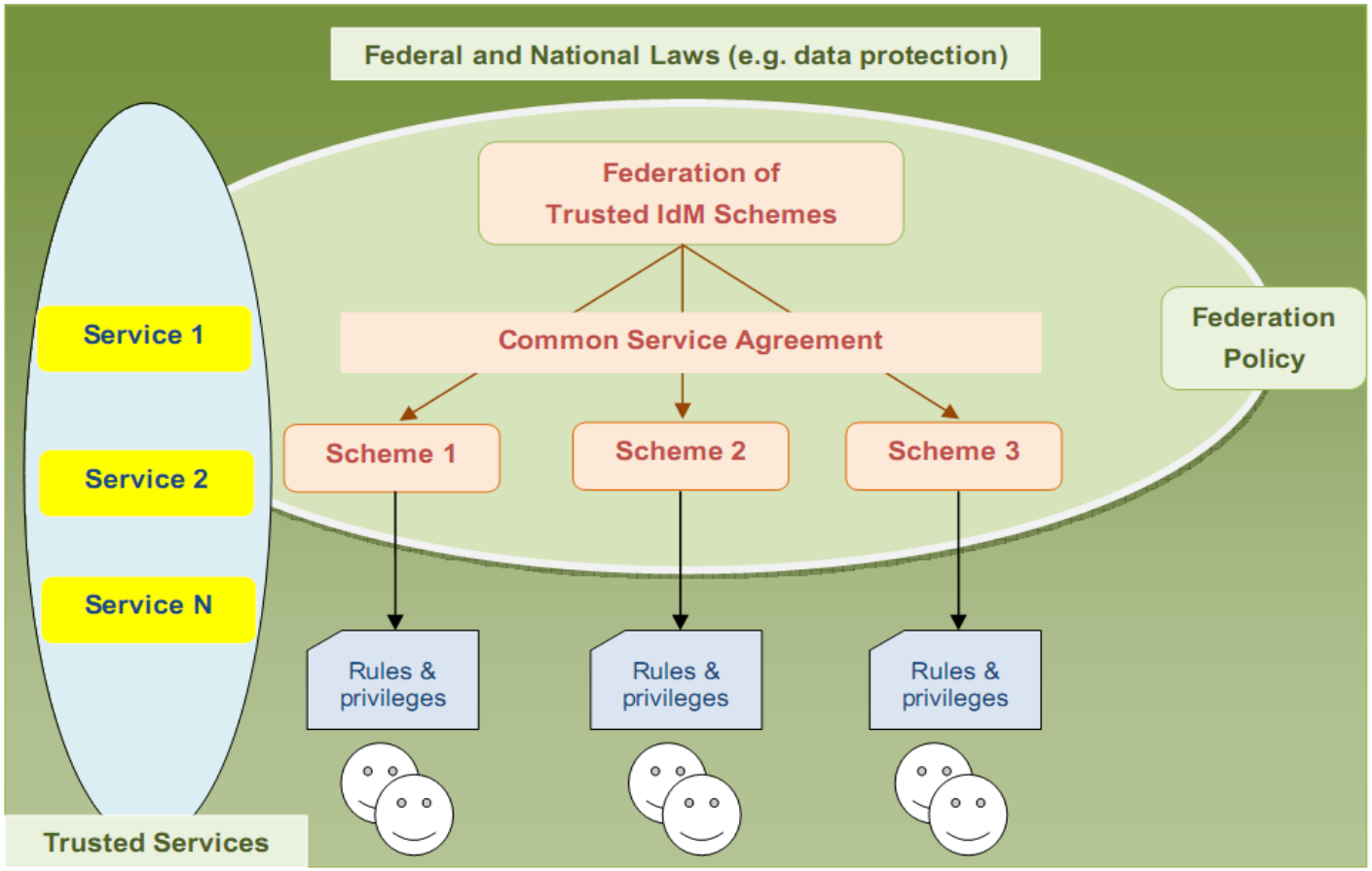
Risk Based Authentication

3	High – considerable damages	Personal presence and/or verification of claimed identity through multiple sources; security vetting; Periodic re-validation of identity and privileges	Biometrics, Hardware or software tokens; secure access; hard crypto cards	Banking, ehealth services, access to sensitive data	Trust, Security
4	Very High – unacceptable level of damages	Personal presence of the applicant is required; verification of breeder documents; security vetting; limited time enrolment; Periodic re-validation of identity, privileges and security vetting	Hard crypto cards; multi-factor authentication; Access to service only within supervised premises with physical access control Two-person authentication	National security Commercial secrets Services for high-value persons	Trust, Security

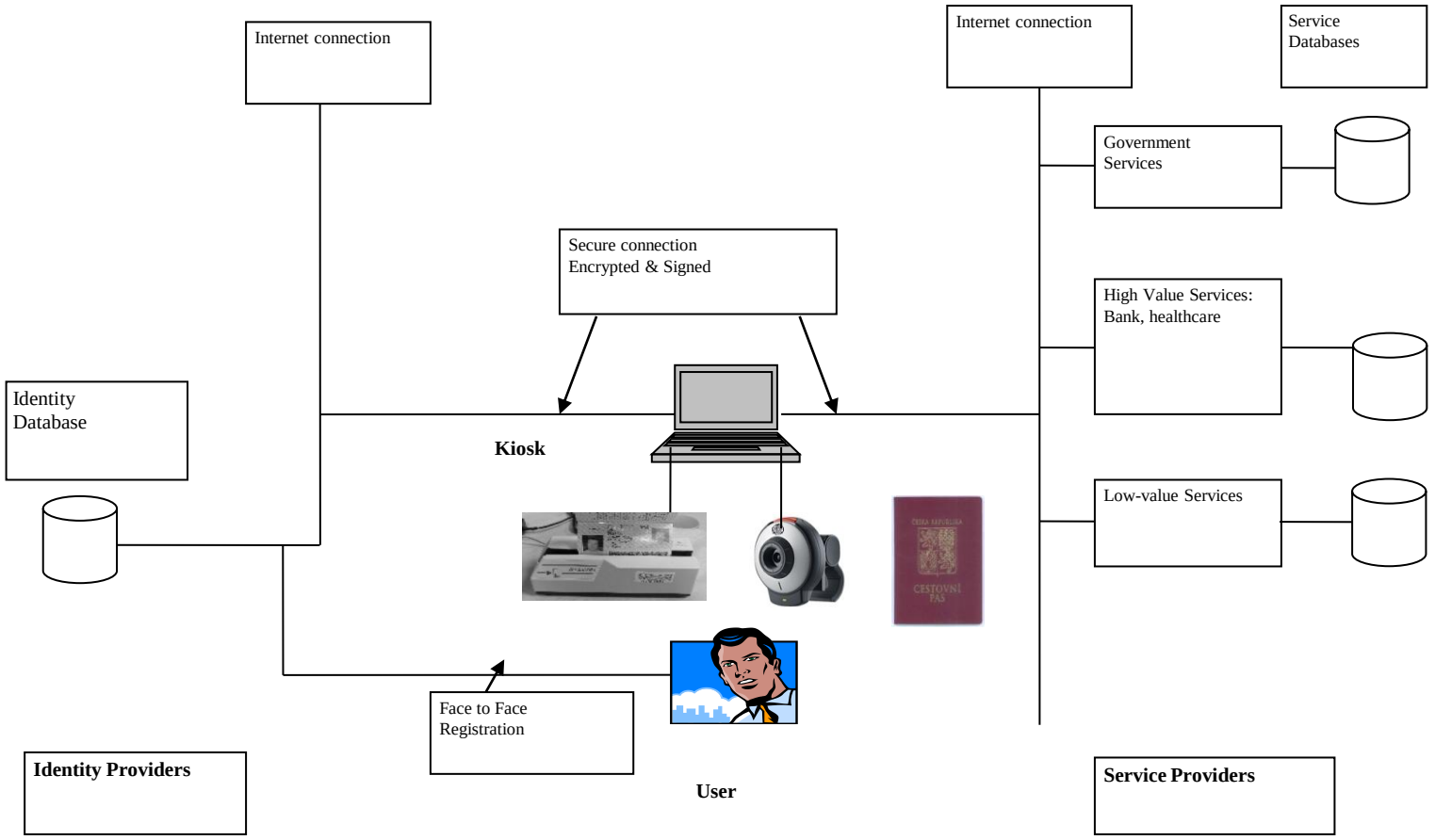
ARCHITECTURE

- Separation of the Identity Provider and the Service Provider
- In a general scheme enroll in a trusted identity provider
- Trusted network services for user verification

Federation of Trusted Identities



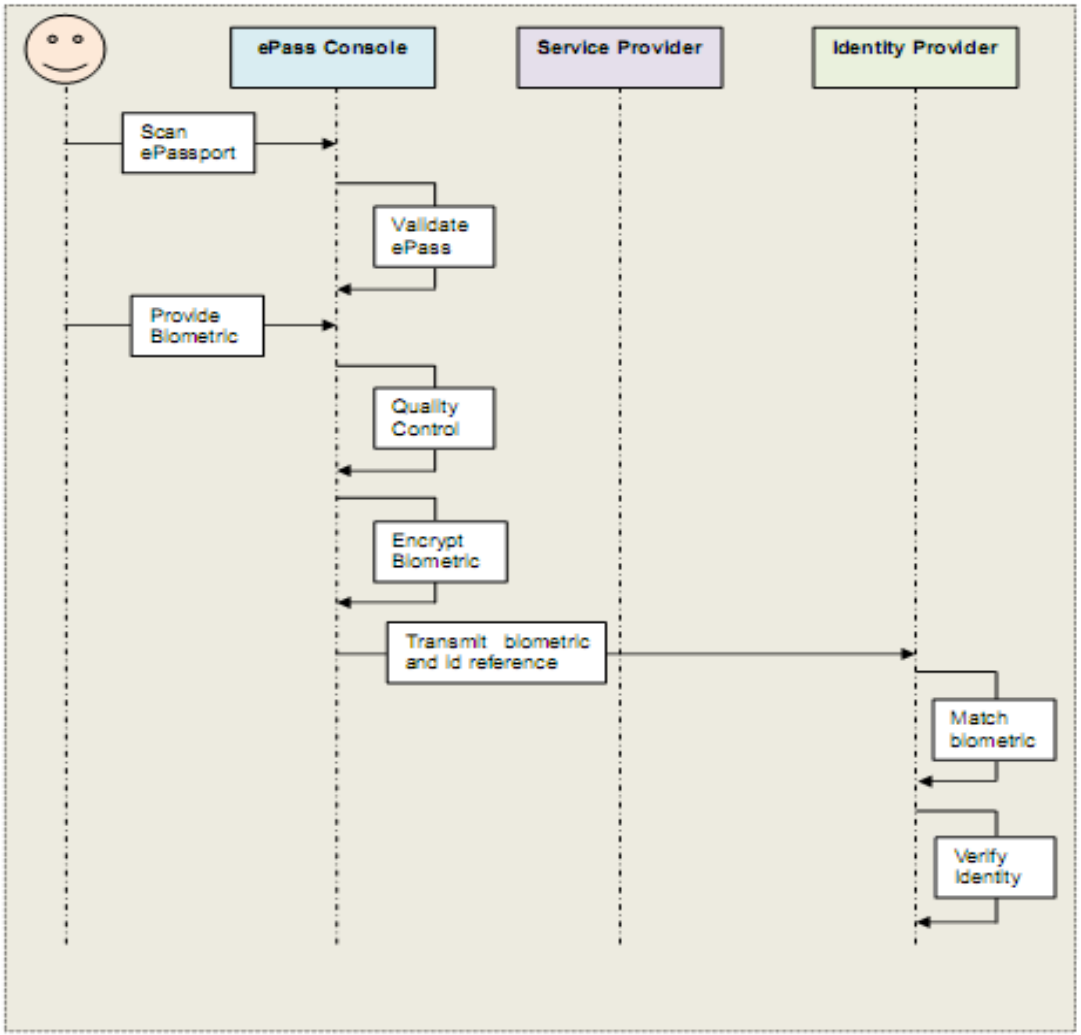
Services for Trusted Identities



Service Categories

- Public/eGov services
- High-value private services (trusted organizations Banks, Hospitals)
- Low-value private services (e-shops social networks)

Two remote identification scheme binding to ePassport information



Two Models

- Direct real time identity verification (kiosk) with the ePassport mainly for eGov services (Kiosk belongs to government)
- Indirect model based on ePassport:

  smart card carrying certificates (Banking, eHealth).

  Pseudonyms or certificates of limited scope for e-shop and other activities

Discussion

- The passport provides the first international PKI system
- The Kiosk is an extended passport reader
- ePassport infrastructure considers risks associated with traveling not market
- Increases the complexity of certificate supply

Discussion

- Id provider should be controlled and evaluated by authorities to obtain trusted status regarding privacy and security (e.g. no fingerprint retention)
- Who is ranking services to high or low value and the associated risks
- Extend kiosk to mobile or PC devices

END

THANK YOU

QUESTIONS ?