Authentication Levels - Status

Aniyan Varghese

eGovernment & CIP Operations

European Commission
Information Society and Media

eGovernment

Status
A challenging situation

- Each country currently has its own way to deal with authentication.
- No alignment:
  - authentication profiles,
  - underlying mechanisms,
  - methods to identify the “right” profile
- No assurance mechanism allowing to build trust between countries.

European Commission
Information Society and Media

eGovernment

Status
Several Initiatives

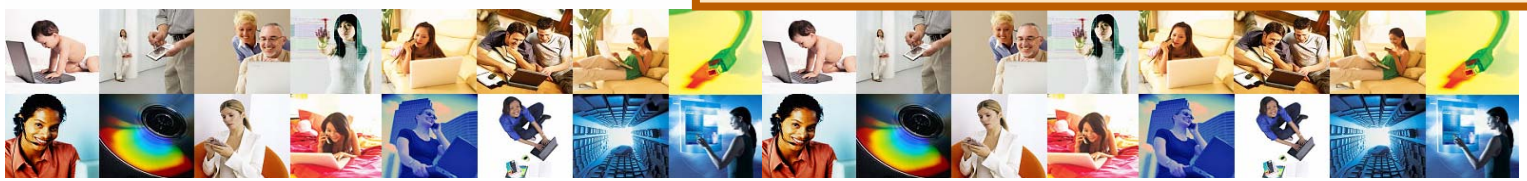
IDA	In 2004, an authentication policy has been produced in the context of IDA. This policy lists 4 authentication assurance levels.
ENISA	Recently, ENISA has initiated work on electronic authentication. Focus on a “language” allowing an adequate description of the concepts and properties underlying the authentication process.
Member States	Several MS are working on authentication levels/models. A significant diversity exists on this subject within MS. Eg. Germany recently proposed a referential based on 5 authentication levels taking into account registration, authentication and data transfer. France describes 3 security levels (PRIS).
eID roadmap	A building block includes the definition of authentication models and authentication levels.
Directive on Electronic Signatures	Even if the concepts of signature and authentication are not the same, the EU directive on Electronic Signature provides a framework for a standardisation of technological mechanisms that can also be used, in specific contexts, for authentication.
Standardisation bodies.	Several standardisation bodies are working on authentication. E.g, ISO/IEC JTC1 SC27 has produced several standards on entity authentication. ETSI has also standardised authentication facilities as part of the electronic signature standards.
Federation mechanisms	Federation mechanisms such as Shibboleth and Liberty Alliance provide facilities to put in place an interoperable federated authentication.

How it is done now ?
A problem tackled on an adhoc basis

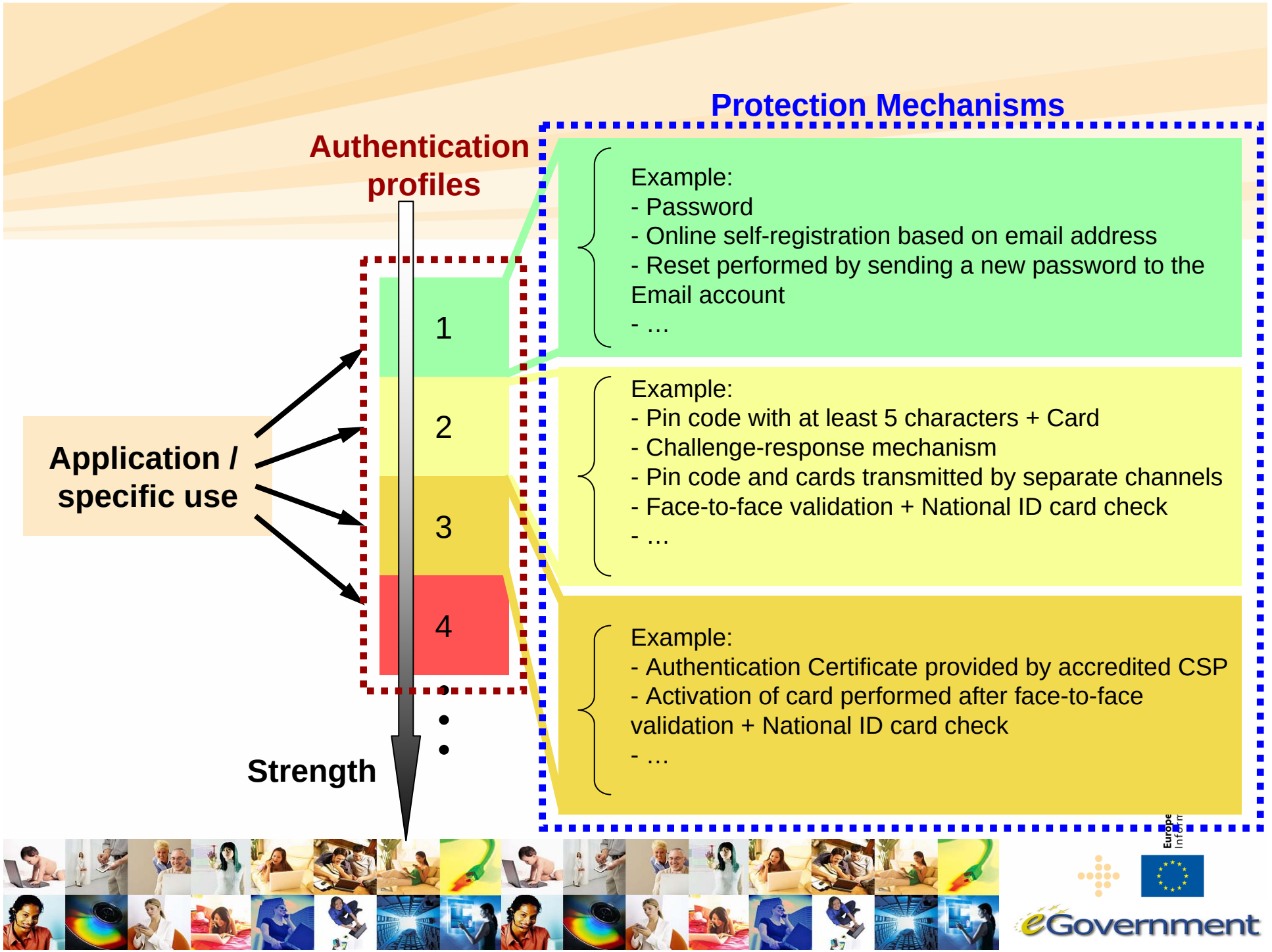
A set of questions to be answered when selecting the appropriate authentication mechanisms
- Who will deliver the password/pin/smartcard… ?
- How to check the identity when registering someone ?
- Can the mechanism used to query the authentication service be bypassed? …

Application / specific use

A selection of adhoc controls e.g.:
- Pin code with at least 5 characters + Card
- Challenge-response mechanism
- Pin code and cards transmitted by separate channels
- Face-to-face validation + National ID card check
- …



eGovernment


Protection Mechanisms
Authentication profiles
Example:
- Password
- Online self-registration based on email address
- Reset performed by sending a new password to the Email account
- …
Example:
- Pin code with at least 5 characters + Card
- Challenge-response mechanism
- Pin code and cards transmitted by separate channels
- Face-to-face validation + National ID card check
- …
Example:
- Authentication Certificate provided by accredited CSP
- Activation of card performed after face-to-face validation + National ID card check
- …
1
2
3
4
Application / specific use
Strength
eGovernment

What are the problems?

- What is the meaning of this “strength”?
- How many levels should be present?
- How do we link the business requirements to a given authentication profile?
- How do we transform an authentication profile into technical and organisational measures?

Several approaches used to associate a semantic to the "strength" levels

- **Use-cases** regrouped into categories of similar impact.
- **Mapping to other frameworks** (e.g. what is required to deliver a given confidentiality level: EU restricted, EU confidential, EU Secret, EU Top Secret).
- **Descriptive approach**, based on the underlying processes: enrolment, authentication.
- **Assurance levels**. A mapping to relevant authentication & enrolment mechanisms to support a given assurance level.
- **Quantitative economic loss** due to the misappropriation of digital identities.
- A **combination of impact and likelihood**.
- …

➔ At this stage, this has not yet been settled

A Scale including 3 to 5 levels is typically used

Too many levels

➔ cost to maintain the authentication information.

➔ cost to operate the corresponding processes and the underling infrastructure.

Too few levels

➔ mismatch between the business requirements and the potential protection mechanisms.

or

B) an unnecessary cost burden resulting from an oversized infrastructure
(e.g. Issuing smartcards where passwords would be "good enough")

A) incomplete coverage of the risks

From authentication profiles To technical and organisational measures

- Existing initiatives on this topic often have limited their scope to a subset of security measures.
- This bars any comparison or even interoperability between the existing scales as no in-depth mapping can be performed.

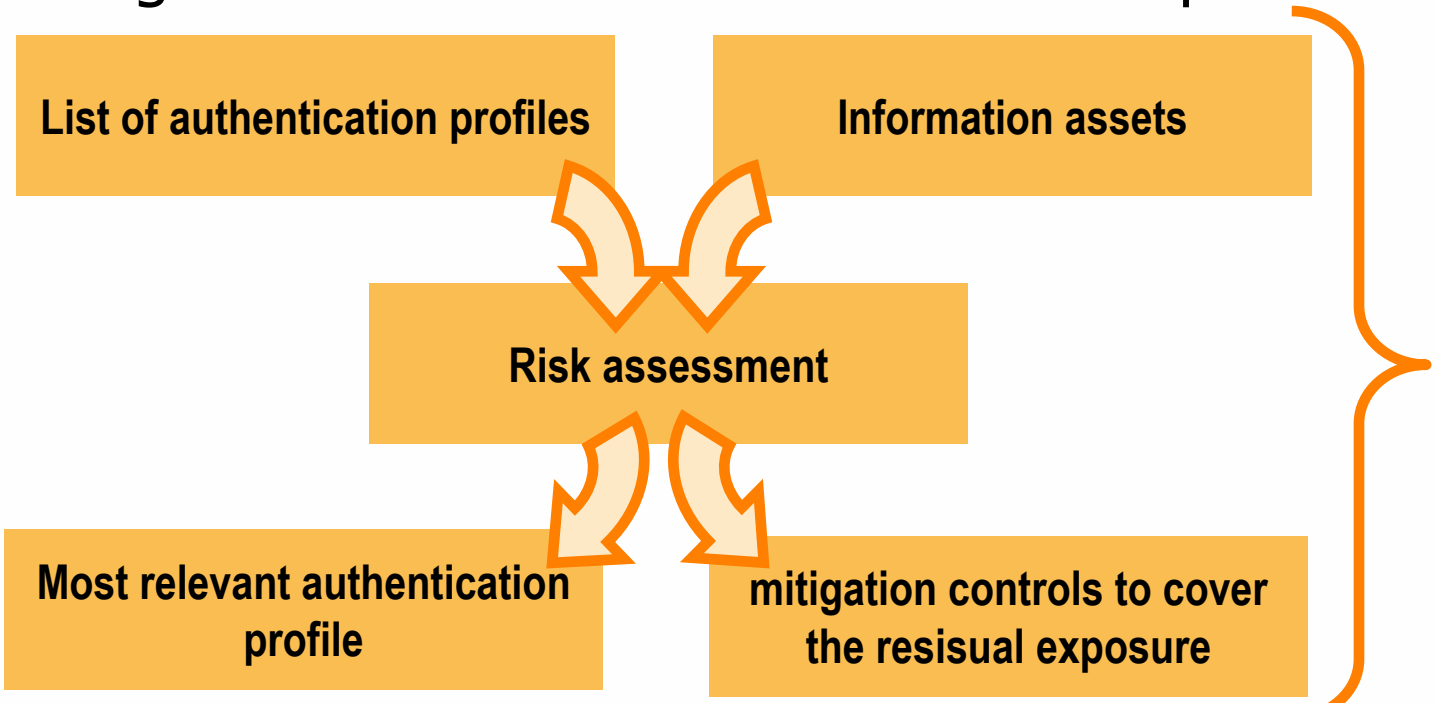
Some examples…

•The issuer and Issuance procedures •The register •The initial user identification mechanisms (eg. face-to-face, online, shared secret) •The eID content related to authentication •The eID verification procedures •Characteristics of the equipment supporting the authentication (eg. reader) •The mechanisms for storing and protecting credentials (eg., smartcard, password rules) •Data protection •Log/Trails	•multiplicity of the authentication mechanisms (Cross sector vs. per sector) •Worn-out •Caching of the authentication •The authentication mechanism or method (password, SSL/certificate…) •The revocation of credentials •Control the authentication by the holder of the credentials / Selective disclosure of attributes •Assurance expectations of the overall process

eGovernment

Linking the business requirements to a given authentication profile

- A topic to investigate once there is an agreement on the authentication profiles.



European Commission
Information Society and Media

eGovernment

Way forward?

- The setup of a common set of authentication profiles would support interoperability and trust in a similar way as decision 2001/844/EC has supported the adoption of a common security classification scheme.