Authentication levels

A brief description of the issue*

* This document is intended purely as a discussion paper exclusively for the internal, non-public use of the recipients. Although every effort has been made to ensure the accuracy and relevance of the contents, they do not in any way represent the official position or policy of the European Commission

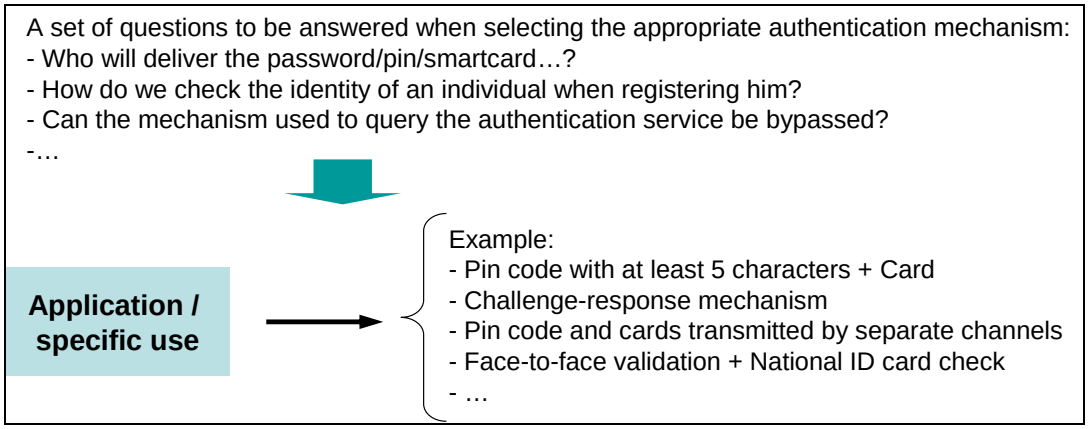
TABLE OF CONTENTS

1. The context

A good management of risks mandates the identification of potential impacts resulting from an exposure of information assets to loss, theft or destruction. This risk assessment usually results in the definition of **protection mechanisms** that will deliver a reasonable assurance that information is effectively protected and that the residual risk can effectively be accepted by the organization.

From an application standpoint, authentication is thus critical to protect the confidentiality, integrity and availability of the information assets during their entire lifecycle and to deliver adequate accountability.

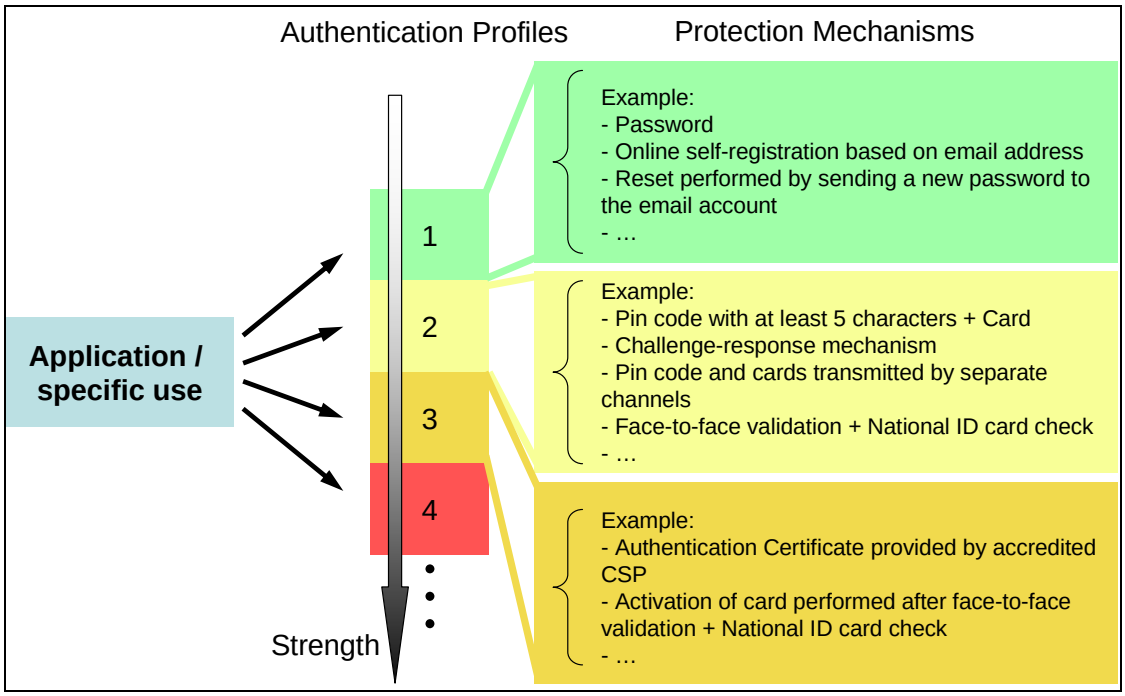
However, if the PEGS initiatives are considered has a whole, the existing protection mechanisms across MS are often heterogeneous. Each application makes its own design decisions leading to a large variety of mechanisms effectively implemented without coordination (pin code, passwords, PKI, smartcard …). Such a situation results in high implementation costs, recurring charge to maintain and operate the authentication processes and difficulties to interconnect systems.



2. Authentication profiles

One solution to improve this situation is to focus on reusable authentication services that can be shared among several applications. Initiatives in this direction generally produce and get an agreement on common authentication profiles, usually organised around a “strength” increasing from one profile to another. Four difficulties must be overcome in this context:

- 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?



2.1. What is the meaning of this "strength"?

Several approaches have been used to associate a semantic to the "strength" levels and at this tage, this has not yet been settled:

- Use-cases can be regrouped into categories of similar impact.
- A mapping can be established to other frameworks (e.g. what is required to deliver a given confidentiality level: EU restricted, EU confidential, EU Secret, EU Top Secret).
- A descriptive approach, based on the underlying processes, can be used. This relies on a detailed description of the enrolment process and the authentication process.
- Assurance levels can be used as basis. As a result, a mapping to relevant authentication & enrolment mechanisms is performed to support a given assurance level.
- The quantitative economic loss due to the misappropriation of digital identities is in some cases a relevant referential.
- A combination of impact and likelihood can also be used as basis to define the scale.

2.2. How many levels should be present?

A scale including 3 to 5 levels is typically used.

- If too many levels are defined, the cost to maintain the authentication information as well as to operate the corresponding processes and the underling infrastructure goes up significantly.
- Conversely, if too few levels are defined, there is no good match between the business requirements and the potential protection mechanisms, leading either to an incomplete coverage of the risks or to an unnecessary cost burden resulting from an oversized infrastructure (e.g. Issuing smartcards where passwords would be "good enough").

2.3. How to transform an authentication profile into technical and organisational measures?

The baseline requirement in this context is the definition of a set of handling rules and assurance criteria that shall be applied consistently. The existing initiatives on this topic often have limited their scope to a subset of the items listed hereunder. This bars any comparison or even interoperability between the existing scales as no in-depth mapping can be performed.

- The issuer
- The register
- The initial user identification mechanisms (for example, face-to-face, online, shared secret)
- Issuance procedures
- The eID content related to authentication
- The eID verification procedures
- Characteristics of the equipment supporting the authentication
- The mechanisms for storing and protecting credentials (for example, smartcard, password rules)
- Data protection
- Log/Trails
- Cross sector usage of authentication mechanisms, multiplicity of the authentication mechanisms / Worn-out
- Caching of the authentication
- The authentication mechanism or method (for example, password, certificate-based SSL)
- The mechanisms for minimizing compromise of credentials (for example, credential renewal, frequency, client-side key generation)
- The revocation of credentials
- Assurance expectations of the overall process
- Ability of the holder to control the authentication / Selective disclosure of attributes

In order to reach an agreement on this subject, a potential solution is to perform a formal Threats & Vulnerabilities assessment in order to provide a reasonable coverage of the potential threats and vulnerabilities. It is likely that only this level of detail can deliver sufficient trust when the one operating the authentication service and the one using the authentication service are not part of the same organisation.

2.4. How to link the business requirements to a given authentication profile?

Once a formal certification of the authentication mechanisms supporting the authentication profiles is in place, a risk assessment can be performed, taking as input the authentication profile and the information assets handled by the application. This is however not a simple task and a methodology shall be produced in order to

- identify the most relevant authentication profile and
- identify mitigation controls for the residual exposure.

3. Interoperability aspects

Each country currently has its own way to deal with authentication. This means that neither the authentication profiles, nor the underlying mechanisms, nor the methods to identify the "right" profile are currently aligned. Furthermore, there is no assurance mechanism in place that could allow building trust between countries. 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.