eID Interoperability for PEGS

Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms

December 2007

This report / paper was prepared for the IDABC programme by:

Author's name: Hans Graux, time.lex; Jarkko Majava, Siemens

Company's name: Siemens - time.lex

Company's address (optional):

Company's logo (optional)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°3

Disclaimer

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6484/5938

Executive summary

The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable Pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovernment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

The project should conclude with several different proposals how to build interoperability without affecting member states' own existing infrastructures. One of these proposals should relate to the definition of specific authentication levels for existing authentication solutions.

This document provides a proposal for a multilevel authentication policy, and suggest a possible mapping of the existing authentication solutions observed in the Member States, Candidate Countries, and EEA Countries, into the defined authentication levels.

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY
[AD2]	A Roadmap for a pan-European eIDM Framework by 2010; see http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf
[AD3]	eID interoperability for PEGS – Draft IDABC Report on Analysis and Assessment of similarities and differences - Impact on eID interoperability

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD4]	IDABC Work Programme Third Revision http://ec.europa.eu/idabc/servlets/Doc?id=25302
[RD5]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD6]	A Roadmap for a pan-European eIDM Framework by 2010; see http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf
[RD7]	eID interoperability for PEGS – Draft IDABC Report on existing national and other authentication schemes

2 Glossary

2.1 Terminology definitions

In the course of this report, a number of context specific expressions are used. To avoid any ambiguity, the following definitions apply to these notions.

These definitions are based on the ModinisIDM Terminology paper[1]. While a few comments have been added for clarification, the definitions remain fully compatible with this paper.

Assertion ..... An assertion is synonymous with a credential.

Attribute ..... An attribute is a distinct, measurable, physical or abstract named property belonging to an entity.

Authentication ..... Authentication is the corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence.

Authorisation ..... Authorisation refers to

(1) the permission of an authenticated entity to perform a defined action or to use a defined service/resource;

(2) the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

Context ..... A context is a sphere of activity, a geographic region, a communication platform, an application, a logical or physical domain.

Credential ..... A credential is a piece of information attesting to the integrity of certain stated facts.

Digital Identity ..... A digital identity is a partial identity in an electronic form.

Entity ..... An entity is anyone (natural or legal person) or anything that shall be characterised through the measurement of its attributes.

Federated Identity ..... A federated identity is a credential of an entity that links an entity's partial identity from one context to a partial identity from another context.

Identification ..... Identification is the process of using claimed or observed attributes of an entity to deduce who the entity is.

Identifier ..... An identifier is an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context.

Identity ..... The identity of an entity is the dynamic collection of all of the entity's attributes. An entity has only one identity.

[1] See https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc

Identity Management (IDM)	Identity management is the managing of partial identities of entities, i.e., definition, designation and administration of identity attributes as well as choice of the partial identity to be (re-) used in a specific context.
Identity Management System (IMS)	An identity management system is the organisational and technical infrastructure used for the definition, designation and administration of identity attributes.
Permission	Permission describes the privileges granted to an authenticated entity with respect to low-level operations that may be performed on some resource (e.g., read, write, delete, execute, create…).
Principal	A principal is synonymous with an identifiable entity
Privacy	Privacy is the right of an entity – in this context usually a natural person – to decide for itself when and on what terms its attributes should be revealed.
Pseudonym	A Pseudonym (syn.: nym) is an arbitrary identifier of an identifiable entity, by which a certain action can be linked to this specific entity. The entity that may be identified by the pseudonym is the holder of the pseudonym.
Registration	The registration of an entity is the process in which the entity is identified and/or other attributes are corroborated. As a result of the registration, a partial identity is assigned to the entity for a certain context.
Role	A role is a set of one or more authorisations related to a specific application or service.

2.2 Acronyms

A2A ..... Administration to Administration

A2B ..... Administration to Businesses

A2C ..... Administration to Citizens

CA ..... Certification Authority

CRL ..... Certificate Revocation Lists

CSP ..... Certificate Service Provider

eID ..... Electronic Identity

eIDM ..... Electronic Identity Management

IAM ..... Identity and Authentication Management

IDM ..... Identity Management

OCSP ..... Online Certificate Status Protocol

OTP ..... One-Time Password

PKCS ..... Public-Key Cryptography Standards

PKI ..... Public Key Infrastructure

SA ..... Supervision Authority

SOAP ..... Simple Object Access Protocol

SCVP ..... Server-based Certificate Validation Protocol

SSCD ..... Secure Signature Creation Device

USB ..... Universal Serial Bus

TTP ..... Trusted Third Party

XAdES ..... XML Advanced Electronic Signature

XML ..... eXtensible Markup Language

XML-DSIG ..... XML Digital Signature

CA ..... Certification Authority

CEN..... The European Committee for Standardization

CTL ..... Certificate Trust List

ECC..... The European Citizen Card

eID ..... Electronic Identity

IAS ..... SEE PAGE 21 under CEN TC 224

IDP ..... Identity Provided

LDAP ..... Lightweight Directory Access Protocol

MS..... Member State

OCSP ..... Online Certificate Status Protocol

PEGS ..... Pan-European eGovernment services

PKI ..... Public Key Infrastructure

RA..... Registration Authority

RP ..... Relying Party

SAML ..... Security Assertion Markup Language

SP ..... Service Provider

SSCD ..... Secure signature creation device

STS..... Security Token Service

SQL..... Structured Query Language

SW ..... Software

TLS ..... Transport Security Layer

SP ..... Service Provider

IDP/IP..... Identity Provider

IA ..... Identity Attributes

FIM..... Federated Identity Model

3 Introduction

3.1 Scope and objectives of the project

The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovemment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

The project should conclude with the definition of Common Specifications for the creation of interoperability between the authentication solutions used or planned in e-government applications without affecting member states' own existing infrastructures.

3.2 Structure of the project

The eID Interoperability for PEGS project consists of 3 different phases:

- In a first stage all the main surveys, standards and research projects in the area of identity management need to be studied and evaluated.
- Secondly, accurate and up-to-date country reports need to be drafted for each participating country. These must be analysed and assessed, to determine any patterns in the national approaches and to derive a set of constraints with regard to electronic identity management for eGovernment applications.
- Then, based on the first two phases, recommendations of how to build an interoperable European wide identity management infrastructure are drafted.

This document concerns the third phase: the distillation of Common Specifications for interoperable identity management from the available national information and the resulting analysis and assessment. As a part of these specifications, a definition should be found of authentication levels which allow the participating countries to assess the security of their authentication solutions and classify them into abstract security levels; and which should also allow them to choose specific security levels required for the purposes of authentication in their applications.

3.3 Objectives of this document

As described in the eGovernment action plan adopted by the European Commission on 25 April 2006[2], and in the Roadmap for a pan-European eIDM Framework by 2010[3], one of the key building blocks for the creation of a pan-European interoperability framework is the establishment of a common multilevel authentication policy.

The reason for this is the large diversity of authentication solutions that have been deployed in European administrations, the reliability and trust levels of which vary depending on the needs of specific applications, policy preferences and socio-cultural considerations. While a certain degree of harmonisation can be expected, it is clear that many of these differences will persist because they are grounded in reasonable considerations, including the desire to choose a security level for the authentication mechanism which corresponds to the actual security needs of each application. In summary, many countries have adopted a variety of authentication solutions, which offer varying degrees of security and reliability.

The present document has two main objectives:

- First of all, to define a proposal for a multilevel authentication policy (hereafter: the Proposal), which could be used to assess the security and reliability of any authentication solution, regardless of the technology being used. While the focus is mainly on the use of authentication solutions in an eGovernment context (i.e. within eGovernment applications), the proposal should also be usable in a private sector context.
- Secondly, to propose a classification for the reported existing main authentication solutions employed in the surveyed countries (the Member States, Candidate Countries and EEA Countries.

3.4 Structure of the document

The present document contains three main sections:

- Section 4: Background information, describing the underlying information and key principles on which the document is based;
- Section 5: Proposal for a multilevel authentication policy, in which the actual policy is presented and justified; and
- Section 6: Mapping of existing authentication mechanisms, in which the reported authentication systems are mapped into the proposed security levels.

[2] See http://europa.eu.int/information_society/eeurope/i2010/index_en.htm

[3] see http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf

4 Background information

4.1 Background documents and key information

The key source documents for the preparation of this proposal were the reports prepared within the framework of the IDABC Study on eID interoperability for PEGS, and specifically:

- The Draft IDABC Country Profiles report, which bundles the information available on the electronic authentication mechanisms in use within the surveyed countries (the Member States, Candidate Countries and EEA Countries), including reference to their respective authentication policies, if any;
- The Draft IDABC Report on Analysis and Assessment of similarities and differences - Impact on eID interoperability, which analysed the aforementioned reports and identified the main trends and issues in the surveyed countries; and
- The Draft IDABC Report on existing national and other authentication schemes, which provides an in-depth overview specifically of the national authentication policies in the surveyed countries, and which also included a number of other potentially relevant authentication policies, including the IDABC Authentication policy and the NIST Guidelines.

Based on these inputs, the following policies were considered to be the most suitable as starting points for a general European multilevel authentication approach:

- The IDABC Authentication policy was the initial document of reference, as a European policy containing all of the critical elements defined above and having been drafted with cross border applicability in Europe in mind;
- The NIST Guidelines, as a more technical document that was useful to provide some further input for the elaboration of the European mechanism;
- Several of the national policies were used to enrich the final result and to validate the usability of the final outcome. In particular, the policies from France, Norway, the UK and the German proposals have been highly instructive in this regard.

4.2 Basic principles of the Proposal

The scope of the Proposal is limited to the **remote authentication** of natural and legal entities using **electronic credentials**. For the purposes of this document, we will consider remote authentication to constitute an authentication process where there is a certain physical separation between the hosting location of the application requiring authentication and the origin of the identity information on which the authentication process is based.

While the focus is mainly on the use of authentication solutions in an eGovernment context (i.e. within eGovernment applications), the Proposal should be more broadly applicable and should be usable in a private sector context as well, as required by the Roadmap for a pan-European eIDM Framework[4].

Provisionally, the following elements are largely common to the authentication policies defined above, and should thus as a minimum be included in the Proposal:

- The definition of risk assessment criteria, typically combined with a consideration of potential damage in case of incidents; these should be the basis for determining security requirements, i.e. Authentication Assurance Levels;
- The definition of registration requirements for the issuing of tokens or credentials, which includes both identity proofing and token/credential delivery; and
- The definition of authentication requirements for the use of such tokens or credentials (i.e. proof of possession and/or knowledge of the token and/or credential).

Considering that the majority of the pre-examined authentication policies rely on a four tiered system, this is also the approach that was followed in the present proposal: four Authentication Assurance levels (security levels), corresponding to a set of requirements with regard to registration and authentication, each of which is suited for a specific risk level of the application.

It should be noted that the definition of these four levels does not preclude the definition at a later stage of even more advanced and more demanding levels. For instance, a number of trends can be expected to become more prevalent in the future, even though their role is not significant or systematic enough at this time to warrant inclusion in the definition of the authentication levels. These trends include most notably:

- The use of biometric attributes to enable/facilitate/enhance the security of the authentication process;

[4] See http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf

- The increased and systematic uptake of mandatory accreditation in accordance with specific risk and/or security related standards, such as ISO/IEC 27001/27002 and ISO/IEC 15408; and
- The use of personal interviews/cross check interviews before issuing specific credentials for highly secured authentication means.

While none of these possibilities is currently commonly used, it is likely that they will become more common in the next few years. If this is the case, it would be possible to make them a compulsory part of an additional authentication Level 5.

4.3 Authentication Process Reference Model

4.3.1 Introduction

Conceptually, as shown in Figure 1 below, the authentication of an entity requires 2 main phases:

- The Registration phase, which is the process by which a user gains a token/credential such as a username or digital certificate for subsequent authentication. The registration generally consists of the following steps:
  - The **Identity Proofing**, during which the real-world identity of the claimant is verified;
  - The claimant's details registration and the **Token Delivery**;
  - The delivery of **Electronic Credentials**;
- The Electronic Authentication phase, also called **Proof of Possession** (or PoP), during which the electronic identity of the claimant is verified.

Note: Authentication simply establishes identity, not what that identity is authorised to do or what access privileges he or she has; this is a separate decision related strictly to authorisation.

The separation of these three functions (Registration, Authentication and Authorisation) by entrusting them to separate entities can be beneficial from a privacy enhancing perspective, as it links and restricts the permissible data processing actions and the availability of personal data to the specific tasks of each actor. However, such a separation is not strictly necessary from an assurance perspective, and will thus not be commented further in this document.

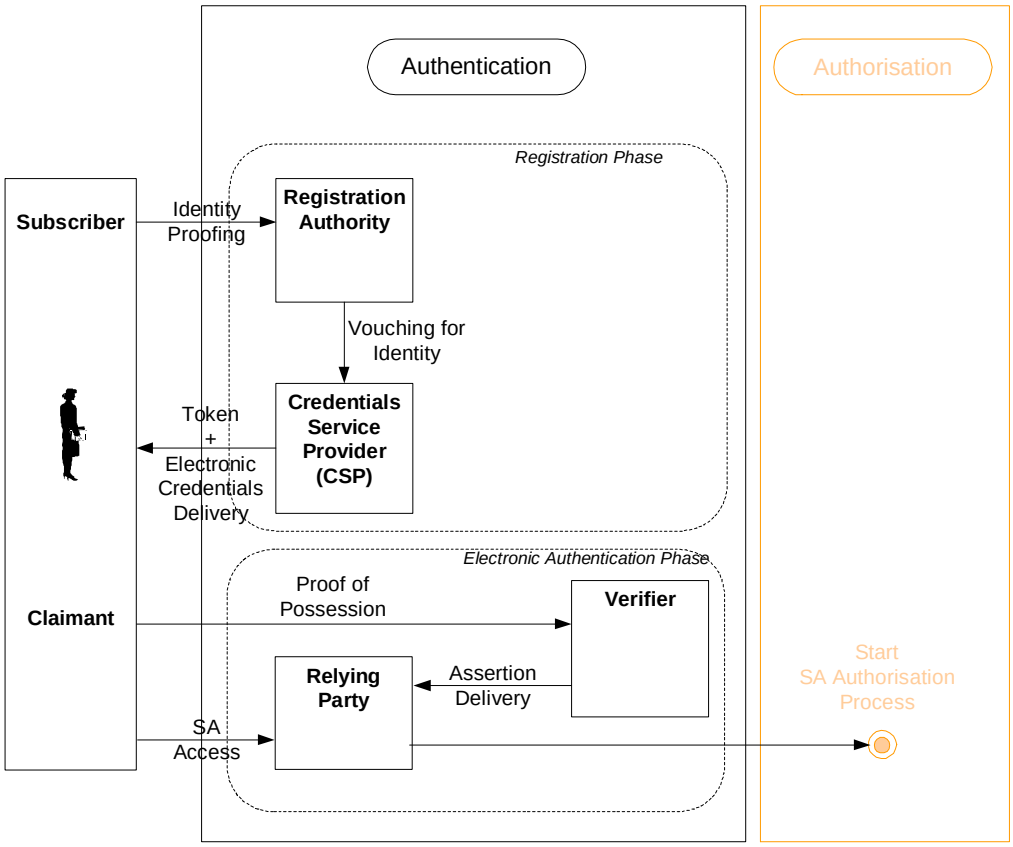


Figure 1: Authentication Process Model.

4.3.2 Actors

4.3.2.1 Subscriber / Claimant

The entity claiming an identity is called a claimant. Before an entity can claim an identity, he or she must demonstrate that the identity is a real identity, and that he is entitled to use that identity. For this reason, the claimant (in an authentication protocol) must be a **subscriber** to some Credentials Service Provider (CSP). The subscriber has a duty to maintain exclusive control of his token and/or credentials, since this is used to authenticate the subscriber's identity.

4.3.2.2 Registration Authority (RA)

The Registration Authority (RA) is responsible for verifying the identity of the subscriber, typically through the presentation of paper credentials and by records in databases. The RA, in turn, vouches for the identity of the subscriber to a CSP.

4.3.2.3 Credentials Service Provider (CSP)

The CSP registers or gives the subscriber a token to be used in an authentication process and issues credentials as needed to bind that token to the identity, or to bind the identity to some other useful attribute. The subscriber may be given electronic credentials to go with the token at the time of registration, or credentials may be generated later as needed.

There is always a relationship between the RA and CSP. In the simplest and perhaps the commonest case, the RA/CSP are separate functions of the same entity. However, an RA might be part of a company or organization that registers subscribers with an independent CSP, or several different CSPs. Therefore a CSP may have an integral RA, or it may have relationships with multiple independent RAs, and an RA may have relationships with different CSPs as well.

4.3.2.4 Verifier

In any authenticated on-line transaction, the verifier must verify that the claimant has possession and control of the token and/or credential that verifies his identity. A claimant authenticates his identity to a verifier by the use of a token and/or credential, and an authentication protocol. This is called Proof of Possession (PoP).

The verifier and CSP may be the same entity, the verifier and relying party may be the same entity or they may all three be separate entities. Where the verifier and the relying party are separate entities, the verifier must convey the result of the authentication protocol to the relying party. The electronic object created by the verifier to convey this result is called an assertion.

4.3.2.5 Relying Party

A relying party relies on results of an on-line authentication to establish the identity or attribute of a subscriber for the purpose of some transaction. The verifier and the relying party may be the same entity, or they may be separate entities. If they are separate entities, the relying party receives an assertion from the verifier.

4.3.3 Processes

4.3.3.1 Identity Proofing

Identity proofing is the process of ensuring that an identity actually corresponds to a real entity, with correctly associated attributes (which can be very limited, e.g. perhaps only a name). Increasing levels of assurance require increasing effort to establish the identity of subscribers. The entity that does the identity proofing is the Registration Authority (RA).

4.3.3.2 Token and Credentials Delivery

The CSP registers or gives the subscriber a token to be used in an authentication protocol and issues credentials as needed to bind that token to the identity, or to bind the identity to some other useful attribute.

4.3.3.3 Proof of Possession

When a claimant successfully demonstrates possession and control of a token and/or credential in an on-line authentication to a verifier through an authentication protocol, the verifier can establish the identity of the subscriber. A verifier can pass along an assertion about the identity or provide an attribute of the claimant to a relying party. The relying party can use the authenticated identity and other factors to make access control or authorisation decisions.

4.3.3.4 Assertion Delivery

If they are separate entities, the relying party receives an assertion from the verifier. The relying party is responsible to validate that the received assertion came from a verifier trusted by the relying party. Where the assertions indicate time of creation or attributes associated with the claimant, the relying party is also responsible for verifying this information.

5 Proposal for a multilevel authentication mechanism

The following sections contain the descriptions for each of the building blocks of the Proposal, as well as an overview of the Proposal itself. It consists of the following components:

- A definition of four Authentication Assurance Levels, in terms of risk and potential damage in case of abuse. These are the criteria to be applied by application owners when determining a suitable security level for their application. It should be noted that this definition is not a part of the Proposal as such, which entails only the definition of authentication levels as encompassed in the following three components, since it does not relate to the authentication mechanism being used, but only to the needs of the application. None the less, it has been retained with few modifications from the pre-existing IDABC Authentication Policy as a good practice for determining the security needs of an application.
- A definition of registration requirements for solutions to be used at each of the four assurance levels; and
- A definition of authentication requirements for solutions to be used at each of the four assurance levels.
- Finally, an overview bringing the aforementioned registration and authentication requirements together in the actual Proposal.

It should be stressed that the registration requirements and the authentication requirements are cumulative to determine the classification of an authentication mechanism, i.e. in order to qualify as a level 3 qualification mechanism, the presented solution must meet all requirements for level 3 mechanisms, both with regard to registration and authentication. Therefore, the mere fact of using a specific token (e.g. a soft PKI certificate) is insufficient to decide that the presented solution is a level 3 authentication mechanism, since all other level 3 requirements (e.g. with regard to registration before a token is issued) must all be met. In summary, the assurance level of an authentication mechanism can only be determined by examining the whole of the qualities and circumstances surrounding its availability and use.

5.1 Definition of Authentication Assurance Levels

5.1.1 Authentication Assurance

Note: The authentication assurance describes the application's degree of certainty that the authenticating entity has presented a credential that refers to his identity.

In this context, authentication assurance is defined as the result of satisfying a series of requirements aiming to provide two components, namely:

- an acceptable degree of confidence in an asserted real-world identity (i.e. identity proofing)
- an acceptable degree of confidence in an electronic identity presented to a service provider by means of a credential (i.e. proof of possession)

5.1.2 Levels

Note: Our approach is to consider that authentication assurance levels should be layered according to the severity of the impact of damages that might arise from misappropriation of a person identity.

The more severe the likely consequences are, the more confidence in an asserted identity will be required to engage in a transaction.

In accordance with most authentication policies in this field, we suggest 4 assurance levels to be defined:

- **Level 1: .....Minimal Assurance**
- **Level 2: .....Low Assurance**
- **Level 3: .....Substantial Assurance**
- **Level 4: .....High Assurance**

5.2 Risk management and determining Authentication Assurance Levels

The level of risk an application owner is willing to accept depends on a number of factors. For the purposes of this Proposal, authentication requirements should be determined by:

- The possible risks for abuse of the authentication method, as defined in section 5.2.1. below; and
- The possible damages incurred by abuse of the authentication method, as defined in section 5.2.2. below.

The required Authentication Assurance Level should then be determined by assessing the likelihood of the risks occurring (section 5.2.3.) and measuring this against the nature and magnitude of the possible damages (section 5.2.4.). The outcome of this process determines the required Authentication Assurance Level (section 5.2.5.)

It should be stressed that the purpose of this document is not to provide a specific universal standard for good risk management practices in the field of eGovernment identity management. This section pertaining to risk management considerations is only intended to provide some initial guidance to application owners in determining suitable Authentication Assurance Levels in case of doubt. For more specific guidance, it is recommended to refer to generally applicable and internationally accepted standards, such as the Common Criteria (ISO/IEC 15408-1:2005), ISO/IEC 27001:2005 or ISO/IEC 27002: 2005 (17799).

This section of the proposal is thus purely an enabling guideline which does not impact the application owner's competence to choose other authentication levels than those resulting from the application of the matrix.

5.2.1 Identification of Risks

Risk is normally defined as the chance or likelihood of damage or loss. This definition can be extended to include the impact of damage or loss. That is, it is a function of two separate components, the likelihood that an unwanted incident will occur and the impact that could result from the incident.

Note: Only general risks pertaining to registration and authentication processes and those pertaining to misappropriation of credentials/electronic identity and/or real-world identity are considered here.

Risk id.	Type	Description
Risk 1	**Fictitious real-world identity**	That a client will obtain a credential pertaining to a fictitious real-world identity.
Risk 2	**False details**	That false information will be recorded against a genuine real-world identity, and subsequently given credence.
Risk 3	**Theft of access token**	That an access token containing a credential will be stolen from or while in transit to the user, and will either itself be used by an impostor or will be used to obtain information about a user for subsequent misuse.
Risk 4	**Real-world identity theft**	That a genuine real-world identity will be misappropriated at the time of registration.
Risk 5	**Interception or revelation of secret authentication information**	That secret information (such as a PIN or private signing key) will be intercepted in transmission when the credential is used, or will be revealed deliberately or inadvertently by the client or another party.

Risk id.	Type	Description
Risk 6	**Retention of secret authentication information in a non trusted terminal**	That secret information will be retained by an untrusted terminal (such as a home or office PC, PC in an Internet cafe or public kiosk). Such secret information may include for example private signing keys used to perform cryptographic functions within the terminal, and PIN numbers entered into a web-based form and subsequently held in cache.
Risk 7	**Unauthorised use of access token**	That an access token will be verified against a user other than the one issued with the token.
Risk 8	**Use of compromised credential**	That a credential will be used after it has been compromised.
Risk 9	**Use of credential after substantive change in circumstances**	That a credential will be used when a change in circumstances means that the credential would not normally have been issued
Risk 10	**Use of credential for unintended purposes**	That a credential will be used in connection with a transaction for which the issuer is not prepared to warrant it, because of the nature or value of the transaction.
Risk 11	**Withdrawal of credential without due cause**	That a credential will be withdrawn due to a false or malicious report of change in circumstances, compromise of credential, etc.
Risk 12	**Fraudulent use of credential**	That a credential holder will attempt to use their credential, either personally or through a third party, for transactions to which they are not entitled.
Risk 13	**Hacker attack**	That a hostile outsider may gain direct access to Sectoral Application's services with the objective of achieving some personal gain, embarrassment to the EU, denying access to the system or causing damage to the system.
Risk 14	**Dispersed storage of information**	That client information will be at greater risk of compromise due to fragmentation of information collected across various e-Government services.

Table 1: Inventory of Security Risks Associated to Authentication Errors.

5.2.2 Damages

Every application owner will be in charge of analysing damages resulting from a breach in the authentication process and assess their impact. To help him in this process, we suggest the possible impact of damages to be chosen among those listed below.

Damages	Comment
• **Loss of Integrity**	System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorised changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
• **Loss of Availability**	If a mission-critical IT system is unavailable to its end users, the organisation's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users performance of their functions in supporting the organisation's mission.
• **Loss of Confidentiality**	System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardising of national security to the disclosure of Privacy Act data. Unauthorised, unanticipated, or unintentional disclosure could result in loss of goodwill towards an organisation, with resultant damage to its reputation, loss of credibility and other adverse consequences, loss of public confidence, embarrassment, or legal action against the organization.
• **Risk to Personal Safety**	The unauthorised disclosure, modification or unavailability of information could lead to the endangerment of personal safety. Examples are as follows: • the unauthorised disclosure of the addresses of certain people could mean that they are targeted by those who desire to cause them harm, whether for political, grievance or other motives • the unauthorised modification of information (for example associated with manufacturing processes, travel movements and medical processes), could mean the malfunctioning of equipment or incorrect decisions being made, with resultant

	adverse effects on the safety or well-being of people • the unavailability of information from some systems (again for example associated with travel movements and medical processes), could result in incorrect or late decisions, with resultant adverse effects on the safety or well-being of people.
• **Financial Loss**	Some IT systems store and process information, which is concerned directly with financial transactions or has a bearing on the financial well-being of the organisation concerned. The consequences of unauthorised disclosure and modification, as well as unavailability and destruction, of such information could well be financial loss. Examples are loss from a reduction in share prices, fraud or breach of contract because of late or no action. Equally, the consequences of unavailability or destruction of any information could be disruptions to users. To rectify and/or recover from such incidents takes time and effort. This will in some cases be significant and should be considered. In order to use a common denominator, the time to recover should be calculated in man months and converted to a financial cost. This cost should be calculated by reference to the normal cost for a man month at the appropriate grade/level within the organisation.

Table 2: Damages.

5.2.3 Likelihood Determination

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

The likelihood that a potential vulnerability could be exercised by a given threat-source can be divided into likelihood levels as defined below.

Likelihood Level	Likelihood Definition
Almost certain	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Likely	The threat-source is highly motivated and sufficiently capable, but controls are in place that may impede successful exercise of the vulnerability.
Moderate	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Unlikely	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.
Rare	The threat-source lacks motivation and capability, or controls are in place to impede the vulnerability from being exercised.

Table 3: Likelihood Levels.

5.2.4 Impact Severity Scaling

We suggest the impact of damages to be valued according to a scale ranging below.

N	**Negligible**	The damages would be dealt with by routine operations.
L	**Low**	The damages would threaten the efficiency or effectiveness of some services, but could be dealt with internally.
M	**Medium**	The damages would not threaten the provision of services, but would mean the services of the application owner could be subject to significant review or changed ways of functioning.
H	**High**	The damages would threaten the continued effective provision of services and require top-level management or ministerial intervention.
V	**Very High**	The damages would threaten the provision of key services, causing major problems for clients and/or for administration in general.

Table 4: Scale ranging of impact severity.

5.2.5 Measure of Risks by Level

The measure of risk is determined by the relationship between both the likelihood of the event and the impact of damages, against the background of any existing risk reduction measures.

Neither impact of damages nor likelihood should dominate the determination of the level of risk

.

The greatest risks to an application are those, which have an extreme impact and are almost certain to occur. Conversely, a rare event with negligible impact may be considered trivial.

An event which occurs rarely but which has an extreme impact could be considered a significant risk.

Having taken into consideration the risks identified above, application owners may wish to develop a risk matrix enabling to deduce the required Authentication Assurance Level for their application. To help them in this process, a **reference matrix** is provided below (Table 5) that allows them to map potential risks and their impact to the minimum authentication assurance level that is required to reduce each considered risk.

In addition, Annex A contains a more extensive template derived from this summary reference matrix that allows application owners to define the required authentication assurance for their application. An example of use of this template is provided below.

		Impact of damages				
	Likelihood	Very High	High	Medium	Low	Negligible
Risk i	Almost certain	(1)	(1)	Level 4	Level 3	Level 3
	Likely	(1)	Level 4	Level 3	Level 3	Level 2
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1
(1): Not applicable to remote authentication over open networks.						

Table 5: Measure of Risk / Authentication Assurance Level Matrix.

Note: It is clear that the terminology and approach being used is to a certain extent subjective and dependent on the perception of application owners. However, this should not be considered a weakness of the system, since the application owners are the sole party who can judge the authentication needs of the application, based on its personal appreciation, local/sectoral traditions and general applicable policies. The use of risk/damage matrices is not intended to eliminate this element.

Rather, the sole purpose of this approach is to provide guidance to application owners in determining Authentication Assurance Levels in case of doubt. It is thus purely an enabling guideline which does not impact the application owner's competence to choose other authentication levels than those resulting from the application of the matrix.

Example of the application of the risk matrix to determine a suitable Authentication Assurance Level:

- Risk 12 (i.e. Fraudulent use of credential) has a **moderate** likelihood to occur. The damages that might arise from the exercise of that risk have a **negligible** impact as far as risk to personal safety is concerned, a **low** impact as far as integrity, availability, and financial loss are concerned and a **high** impact as far as confidentiality is concerned. The resulting level of authentication assurance derived from the valuation of Risk 12 is the highest value provided by the matrix, i.e. **3.**
- Risk 3 (i.e. Theft of access token) has a **rare** likelihood to occur. The damages that might arise from the exercise of that risk have a **negligible** impact as far as risk to personal safety is concerned, a **medium** impact as far as integrity, availability, and financial loss are concerned and a **high** impact as far as confidentiality is concerned. The resulting level of authentication assurance derived from the valuation of Risk 3 is the highest value provided by the matrix, i.e. **2.**

The resulting level of assurance for that case is the highest of both values, i.e. **3**. A **Level 3 Authentication Assurance** should then be implemented in accordance with the Level 3 policy guidance.

It goes without saying that not all eGovernment applications demand the same assurance level, and that a certain degree of personal appreciation by the application owner is therefore necessary.

Risk 6	Likelihood 6	Impact of damages 6: Very High	High	Medium	Low	Negligible	Highest level 6
Risk 12: Fraudulent use of credential	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	3
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3 n	Level 3	Level 2 n n n	Level 2 n	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

Risk 6	Likelihood 6	Impact of damages 6: Very High	High	Medium	Low	Negligible	Highest level 6
Risk 3: Theft of access token	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	2
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2 n	Level 2 n n n	Level 1	Level 1 n	

(1) Not applicable to remote authentication over open networks.

Resulting Authentication Assurance Level 4	**3**

n **Loss of integrity**	n **Risk to personal safety**
n **Loss of availability**	n **Financial loss**
n **Loss of confidentiality**	

5.3 Registration mechanisms

The registration mechanisms being applied for the issuing of tokens and/or credentials are a crucial first step in assessing the reliability of an authentication method. Factors such as:

- Documentation required before a token/credential is issued, including via personal appearance or registration at a distance, and the verification of specific attributes described in this documentation prior to the issuing of tokens and/or credentials;
- The issuing process, i.e. issued to the requesting party in person, or electronically or via (registered) mail to an official domicile;
- The identity/quality of the issuing authority;
- Retention of the registration information

are of critical importance.

The criteria adopted in this proposal are mainly based on the authentication policies of the UK and Germany, the IDABC Authentication Policy and the NIST Guidelines for registration as described in [RD7].

5.3.1 Documentation/identification requirements before a token/credential is issued

A key distinction must be made between registration mechanisms with or without prior personal appearance of the claimant, and mechanisms requiring the presentation and verification of official or unofficial identity documents. The official or unofficial nature of identity documents is a somewhat subjective matter, which can vary according to national legal and administrative traditions. The key criteria to determine the official character of an identity document are:

- Whether or not the task of issuing the document has been entrusted to a public sector body in accordance with a specific legal framework (i.e. its duty to issue the document is based on law, and not on a contractual relationship); and
- The fact that the attributes printed or stored on the identity document originate or are derived directly from an original identity source, such as a national register.

Based on this, examples of official identity documents include ID cards, passports, drivers' licenses and residence cards issued to foreigners, although this list is obviously not exhaustive.

With regard to evidentiary requirements, it is important to realise that all such requirements are inherently reputation based in some form or other. Any document's reliability depends on the processes observed when issuing it and on the circumstances following its issuance. For instance, issuance of a passport may require the presentation of an ID card. Issuance of an ID card may require a birth certificate. The birth certificate itself is the result of a claim made by a parent or doctor. Thus, the reliability of each document (and its value as evidence) relies on a mechanism of trust chaining,

where reliability is believed to increase as the number of reliable parties (e.g. civil servants) and reliable documents (e.g. civil status certificates) increases, and as a longer period of time passes in which the reliability of none of these documents is disputed. In summary, even highly formal registration procedures requiring the production of official identity documents are fundamentally reputation based. This should be reflected in the requirements for registration procedures.

Following existing models (e.g. the UK's authentication policy) and current trends (e.g. the rise of social networking platforms), reputation based identification relying on trustworthy third parties outside of the public sector should therefore also be permissible at lower levels. In our Proposal, level 1 is entirely claims based (which would also include registration systems where claims from the applicant are supported by a third person), and level 2 allows registration where claims are supported by documentary evidence from neutral and trustworthy sources such as a banks, insurance agencies or government departments. We have also considered the possibility of allowing level 2 registration where claims are supported by natural persons with a particular trust status (e.g. notaries public or judges), but have decided against this, since there is no clear view on how the trusted status of a specific natural person could be judged in a way that is both neutral and sufficiently reliable, and on what basis such natural persons should make their decision.

On authentication levels 2 and 3, purely on-line registration is only permitted if the attributes provided by the claimant are verified against an official identity source to ensure that they uniquely identify the claimant and that they are accurate. For the purposes of this proposal, an official identity source is defined in similar terms as an official identity document, with the key attributes being:

- Whether or not the task of managing the identity source has been entrusted to a public sector body in accordance with a specific legal framework (i.e. its duty to manage the source is based on law, and not on a contractual relationship); and
- Whether or not the information stored in the identity source is considered to be reliable and trustworthy in the country, as witnessed by the fact that other public sector bodies than the one managing the source rely on it for the performance of their functions (i.e. the source is not being kept for merely internal purposes).

The registration of biometrics data is not yet included in this model. While biometrics are being used in a few countries for match-on-card functionality, they are not yet used in actual e-government applications. For this reason, it is not yet clear how biometrics should be integrated in the current system. Therefore, no specific references to registration of biometric characteristics have been included at this point.

Finally, the hypothesis of registration in cases where an entity is unable to present valid documentation (e.g. refugees or illegal residents) has not been explicitly dealt with in this document. This is after all not a matter of eIDM interoperability, but rather a question of human rights and the right to an electronic identity (which will certainly become an important issue in the next 10 years or so), which is entirely a national competence. None the less, it can be noted that assurance levels 1 and 2 allow claims based registration and reputation enabled registration respectively, which can provide some indirect guidance. However, specific guidelines for the Member States on handling this issue is out of scope for this specific study.

The following classification can be proposed:

Documentation/identification requirements	Assurance Levels			
	1	2	3	4
No personal appearance is required; registration is done on-line based on assertions of the claimant without verification other than the validation of the e-mail address, which must be valid.	X			
No personal appearance is required; registration is done on-line based on assertions of the claimant which allow his unique identification; the assertions must undergo validation, either by cross-referencing the provided assertions (i.e. the claimed attributes which allow the unique identification of the claimant) with an official identity source or identity database from a neutral and trustworthy source such as a bank, insurance agency or government department, or implicitly (e.g. by sending credentials to the official registered domicile of the claimant or by requiring the token/credentials to be collected personally by the claimant during which identity documents must be provided to validate the assertions).	X	X		
Personal appearance is required. During registration, the claimant must present an official identity document such as an identity card, passport or drivers license, or provide third party corroboration from at least two neutral and trustworthy sources such as a bank, insurance agency or government department. **Or** No personal appearance is required; registration is done on-line based on assertions of the claimant which allow his unique identification and which are signed using a qualified signature, which the RA validates. **Or** No personal appearance is required; registration is done on-line based on assertions of the claimant which allow his unique identification, and at least one of the assertions must relate to an attribute which is only reasonably known to the claimant (such as a national register number, ID card number or passport number); the assertions must undergo validation by cross-referencing the provided assertions (i.e. the claimed attributes which allow the unique identification of the claimant) with an official identity source.	X	X	X	

Personal appearance is required. During registration, the claimant must present an official identity document such as an identity card, passport or drivers license which contains a photo and signature, and which is verified by the RA before a token/credential can be issued; **Or** No personal appearance is required; registration is done on-line based on assertions of the claimant which allow his unique identification and which are signed using a qualified signature, which the RA validates. Note that Level 4 security requires that the token/credential must be delivered to the claimant in person (see below), so that it is impossible to obtain Level 4 authentication methods without personal identification.	**X**	**X**	**X**	**X**

5.3.2 The issuing process following registration, i.e. issued to the requesting party in person, or electronically or via (registered) mail to an official domicile

Since the insecure issuing of tokens/credentials (e.g. by regular (e-)mail) can imply a security risk through the possibility of interception, this should also be factored into the assessment of the registration process. The issuing process should ensure the binding between the claimant's claimed identity and his real-life identity at higher assurance levels.

The following classification can be proposed:

Issuing process following registration	**Assurance Levels**			
	1	**2**	**3**	**4**
Token/credential is sent out by mail or e-mail without prior validation of the claimed address.	**X**			
Token/credential is sent out by two separate mailings, at least one of which must be by physical mail (not e-mail) to the official address of the claimant as shown in an official identity database in which the physical address was registered. **Or** The token/credential may be downloaded directly by the claimant following the registration procedure, by following a link which was sent to an e-mail address communicated by the claimant during the registration process; in this case, the e-mail link may not be valid for more than 24 hours.	**X**	**X**		
Token/credential is sent out by registered mail after prior validation of the claimed address against an official identity database in which the physical address was registered.	**X**	**X**	**X**	
The token/credential may only be given to the claimant in person after validation of his identity using an official identity document.	**X**	**X**	**X**	**X**

5.3.3 Identity/quality of the issuing authority

The role of the RA (Registration Authority) for authentication means is frequently assumed by a (partially or wholly) privately controlled partner. In an offline context (i.e. for traditional identification documents to be presented to public or private sector services as a means of authentication such as identity cards, passports or drivers licenses) the role of the RA tends to be assumed by public sector entities. In an on-line e-government context the quality of the RA as a public or private entity is of little importance when a suitable agreement or supervision mechanism exists between the national administration governing the private sector RAs with regard to the role, obligations and responsibilities (including liabilities) of the RA.

Since [AD3] has found that such agreements are in place for all major eIDM systems in the surveyed countries, the use of tokens/credentials originating from RAs which are not subject to an agreement or supervision mechanism from the national administration governing the RA should only be tolerated for level 1 authentication means, which operate mostly on a good faith claims basis.

It is worth noting that it would also be conceptually possible to demand formal certification of the issuing authority (e.g. ISO 27001 certification), especially when private sector entities play the role of issuers, to improve reliability and trust. However, since this requirement is to our knowledge still extremely rare in the field and would unreasonably impair the practical applicability of this document, no reference to certification requirements is presently included in the definitions of authentication levels.

Allowed RAs	**Assurance Levels**			
	1	**2**	**3**	**4**
No government agreement/supervision mechanism is in place	**X**			
Government agreement/supervision mechanism is in place	**X**	**X**	**X**	**X**

5.3.4 Retention of the registration information

Finally, there is the question of how long the RA should retain records of the facts of registration, with a view of permitting the identification of the claimant after the expiration of a given period of time, and in order to permit investigation of any claims of fraud.

The following classification can be proposed:

Retention of the registration information	**Assurance Levels**			
	1	**2**	**3**	**4**
There is no requirement to prove the identity or maintain a record of the facts of registration.	**X**			
5 years beyond the expiration or revocation (whichever is later) of the credential.	**X**	**X**		
7 years beyond the expiration or revocation (whichever is later) of the credential.	**X**	**X**	**X**	
10 years beyond the expiration or revocation (whichever is later) of the credential.	**X**	**X**	**X**	**X**

.

5.4 Authentication Methods

Extract from POLSEC:

Authentication is generally achieved through one or more of the following methods:

- **Authentication by Knowledge (a.k.a. "Something you know")**. This method is based on something the user knows. This could be a password or a Personal Identification Number (PIN). This method is based on the assumption that the value used for authenticating a certain person is only known to that person.
- **Authentication by Ownership (a.k.a. "Something you have")**. This method is based on something that the user possesses. This could be, for example, a smart card, hardware token, an identity card or a door key. The method is based on the assumption that it is difficult for an attacker to replicate the object used for authentication, and that users do not allow other persons to use their authentication objects.
- **Authentication by Characteristic (a.k.a. "Something you are")**. This method is based on the utilisation of biometrics to recognise one or more unique characteristics of the user, such as the retina pattern and fingerprints. This method is based on the assumption that certain human characteristics can uniquely identify human beings.

In electronic authentication, the claimant authenticates to a system or application over a network. Therefore, a token used for electronic authentication shall include some secret information and it is important to provide security for the token. In fact, the three methods (or "factors") mentioned above often influence the security provided by tokens. Tokens that incorporate all three factors are stronger than tokens that only incorporate one or two of the factors. However, the latter factor ("something you are") is not currently in use for the purposes of authentication in public sector applications (at least not in services open to the general public), nor is it commonly used yet in the private sector, and will therefore not be further considered in this document.

5.4.1 Token Types

In this sense, five types of tokens for authentication are presented below. Each type of token incorporates one or more of the methods (something you know, something you have, and something you are.)

Note: Only electronic tokens are considered here.

Token Type	Description
Password or PIN token	A secret character string that a claimant memorizes and uses to authenticate his or her identity.
Password list	A personal soft token (paper list) that the claimant possesses. A list contains PIN codes for use in authentication, often in combination with a static password or PIN token within the authentication system.
One-time password device token	A personal hardware device that generates "one time" passwords for use in authentication. The device may or may not have some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port). The passwords shall be generated by using a block cipher or hash algorithm to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password. The nonce may be a date and time, or a counter generated on the device, or a challenge sent from the verifier (if the device has an entry capability). The one-time password typically is displayed on the device and manually input (direct electronic input from the device to a computer is also allowed) to the verifier as a password. This may include mobile SMS onetime password systems.
Soft crypto token	A cryptographic key that is typically stored on disk, USB stick or some other media. Authentication is accomplished by proving possession and control of the key. The soft token shall be encrypted under a key derived from a password known only to the user, so knowledge of a password is required to activate the token. Each authentication shall require entry of the password and the unencrypted copy of the authentication key shall be erased after each authentication.
Hard crypto token	A smartcard or similar media that contains a protected cryptographic key. Authentication is accomplished by

	proving possession of the device and control of the key. Hard tokens shall: • require the entry of a password or a biometric characteristic to activate the authentication key; • not be able to export authentication keys

Impersonation of an identity using a hard or soft token requires that the impersonator obtain two separate things: either the key (token) and a password, or the token and the ability to enter a biometric characteristic into the token.

Therefore both hard and soft tokens provide more assurance than passwords inherently normally provide. Moreover, a hard token is a physical object and its theft is more likely to be noticed by its owner, while a soft token can sometimes be copied without the owner being aware of this. Therefore a hard token offers more assurance than a soft token.

Impersonation of an identity using a password token requires only that the impersonator obtain the password. The ability of humans to remember long and arbitrary (i.e. valuable) passwords is limited, so password tokens are often vulnerable to a variety of attacks including guessing, dictionaries of commonly used passwords, and simple exhaustion of all possibilities.

There are a wide variety of password authentication protocols that differ significantly in their vulnerabilities, and many password mechanisms are vulnerable to passive and active network attacks. While some cryptographic password protocols resist nearly all direct network attacks, these techniques are not at present widely used and all password authentication mechanisms are vulnerable to keyboard loggers and observation of the password when it is entered. Therefore password tokens generally provide less assurance than hard or soft tokens.

Based on these considerations, the use of certain token types implies a risk which is inherently incompatible which certain assurance levels. The table below provides an overview of the assurance levels for which each of the tokens can be used (i.e. the maximum permitted assurance level of each token type), independent of other technical or organisational security guarantees.

Allowed Token Types	**Assurance Levels**			
	1	**2**	**3**	**4**
Hard crypto token	**X**	**X**	**X**	**X**
Soft crypto token or one-time password device token	**X**	**X**	**X**	
Randomly generated password, PIN token or password list (but not passwords or PIN tokens chosen by the claimant).	**X**	**X**		
Password or PIN token chosen by the claimant	**X**			

5.4.2 Remote Authentication Mechanisms

Remote authentication mechanisms are basically the credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be.

5.4.2.1 Authentication Protocols Threat Model

RAs, CSPs, verifiers and relying parties are ordinarily trustworthy (in the sense of correctly implemented and not deliberately malicious). However, claimants or their systems may not be trustworthy.

Protocol threats include:

- **Eavesdroppers** observing authentication protocol runs for later analysis. In some cases the eavesdropper may intercept messages between a CSP and a verifier, or other parties rather than between the claimant and the verifier. Eavesdroppers generally attempt to obtain tokens to pose as claimants;
- **Password guessing**, especially in cases where the password is chosen by the claimant or generated in an non-random manner;
- **Replay** of a previous authenticated message to gain access to sensitive information;
- **Hijackers** who take over an already authenticated session to then:
    - pose as subscribers to relying parties to learn sensitive information or input invalid information;
    - pose as relying parties to verifiers to learn sensitive information or output invalid information.
- **Impersonation**:
    - impostor claimants posing as subscribers to verifiers;
    - impostor verifiers posing as verifiers to legitimate subscriber claimants to obtain tokens that can then be used to impersonate subscribers to legitimate verifiers;
    - impostor relying parties posing as the identity provider IT system to verifiers to obtain sensitive user information;
- **Man-in-the-middle** where the attacker poses as the verifier or relying party to the claimant, and as the claimant to the verifier or relying party and thereby learns or is able to alter sensitive information (especially passwords).

5.4.2.2 Authentication Protocols by Level

Allowed Protocol Types	Assurance Levels			
	1	2	3	4
Private Key PoP	X	X	X	X
Symmetric Key PoP	X	X	X	X
One-time (or strong) Password PoP	X	X	X	
Tunnelled password PoP	X	X		
Challenge-reply password PoP	X			

5.4.2.3 Required Protection by Level

Protection against	Authentication Assurance Levels			
	1	2	3	4
Eavesdropper		X	X	X
Replay	X	X	X	X
On-line guessing	X	X	X	X
Verifier Impersonation			X	X
Man-in-the-middle			X	X
Session Hijacking			X	X

5.4.3 Assertion Mechanisms

Assertion mechanisms are used to communicate the results of a remote authentication to other parties.

In order to ensure the trustworthiness of the provided identity information, relying parties may accept assertions that are:

- Digitally signed by a trusted identity (e.g. the verifier); or
- Obtained directly from a trusted entity using an authentication protocol of the corresponding level or above;

Assertions shall expire after a certain period, defined by level (see below). They should not be accepted afterwards.

Expiration time	**Assurance Levels**			
	1	**2**	**3**	**4**
24 hours	**X**			
12 hours	**X**	**X**		
2 hours	**X**	**X**	**X**	
Immediate	**X**	**X**	**X**	**X**

5.5 Proposed Multi-Level Authentication policy

Summarising the rules above, this section will contain an overview of the requirements and possibilities for each of the four authentication levels (above public access, i.e. access to resources where no prior authentication is required).

It should be noted that all of the requirements for each of the requirements are cumulative, e.g. an authentication mechanism that fails even one of the requirements of Level 2 can at a maximum be classified as Level 1.

5.5.1 Requirements for Assurance Level 1

	Level 1
Registration Phase	
Procedure for identity proofing, user details registration, delivery of token and credentials	**Level 1 Registration** 1. Definition Level 1 registration is appropriate for application transactions in which damages that might arise from misappropriation of real-world identity would have a Negligible or Low impact. The registration is purely claims based This registration level is heavily used by lots of Internet applications (webmails, on-line, auctions, etc.). 2. Requirements The RA can be any entity whose authentication methods are accepted in an eGovernment application. There is no requirement to prove the identity or maintain a record of the facts of registration. Identity assertions of claimants are accepted. Only the e-mail address must be unambiguous and valid. 3. Delivery There is no specific requirement for delivery of the token or credential.
Retention period for registration	**None**

data	
Electronic Authentication Phase	
Authentication Protocol for Proof of Possession (PoP)	Most of the time, **Challenge-reply password PoP** However, according to risk assessment, could also be: - Tunelled password PoP - One-time (or strong) Password PoP - Symmetric Key PoP - Private Key PoP
Token Type	All token types are acceptable. Most commonly **Password or PIN tokens** will be chosen.
Requires the application owner to implement protection against	**Replay** **On-line guessing**

5.5.2 Requirements for Assurance Level 2

	Level 2 Policy
Registration Phase	
Procedure for identity proofing, user details registration, delivery of token and credentials	**Level 2 Registration** 1. Definition Level 2 registration is appropriate for application transactions in which damages that might arise from misappropriation of real-world identity would have a Medium impact. In many cases the Level 2 registration can be accomplished on-line and immediately. 2. Requirements The token/credential must be issued by a body which is subject to a specific government agreement or under government supervision. No personal appearance is required; registration is done on-line based on assertions of the claimant which allow his unique identification. The assertions must undergo a basic validation, either by cross-referencing the provided assertions (i.e. the claimed attributes which allow the unique identification of the claimant) with an official identity source or identity database from a neutral and trustworthy source such as a bank, insurance agency or government department, or implicitly (e.g. by sending credentials to the official registered domicile of the claimant or by requiring the token/credentials to be collected personally by the claimant during which identity documents must be provided to validate the assertions). 3. Delivery The token/credential must be sent out by two separate mailings, at least one of which must be by physical mail (not e-mail) to the official address of the claimant as shown in an official identity database in which the physical address was registered; **Or** The token/credential may be downloaded directly by the claimant following the registration procedure, by following a link which was sent to an e-mail address communicated by the claimant during the registration process; in this case, the e-mail link may not be valid for more than 24 hours.
Retention period for registration data	A record of the facts of registration shall be maintained by the CSP or its representative. The suggested minimum retention

	period for registration data for Level 2 credentials is 5 years beyond the expiration or revocation (whichever is later) of the credential.
Electronic Authentication Phase	
Authentication Protocol for Proof of Possession (PoP)	Most of the time **Tunelled or One-time Password PoP** However, according to risk assessment, could also be: - Symmetric Key PoP - Private Key PoP
Token Type	All tokens are acceptable except the sole use of user chosen passwords. At a minimum a randomly generated password or PIN token is acceptable; preferably a **One-time password device token** should be used.
Requires the application owner to implement protection against	**Eavesdropper** **Replay** **On-line guessing**

5.5.3 Requirements for Assurance Level 3

	Level 3 Policy
Registration Phase	
Procedure for identity proofing, user details registration, delivery of token and credentials	**Level 3 Registration** 1. Definition Level 3 registration is appropriate for application transactions in which damages that might arise from misappropriation of real-world identity would have a High impact. 2. Requirements The token/credential must be issued by a body which is subject to a specific government agreement or under government supervision. Personal appearance is required. During registration, the claimant must present an official identity document such as an identity card, passport or drivers license, or provide third party corroboration from at least two neutral and trustworthy sources such as a bank, insurance agency or government department. **Or alternatively:** No personal appearance is required; registration is done on-line based on assertions of the claimant which allow his unique identification and which are signed using a qualified signature, which the RA validates.. **Or alternatively:** No personal appearance is required; registration is done on-line based on assertions of the claimant which allow his unique identification, and at least one of the assertions must relate to an attribute which is only reasonably known to the claimant (such as a national register number, ID card number or passport number); the assertions must undergo validation by cross-referencing the provided assertions (i.e. the claimed attributes which allow the unique identification of the claimant) with an official identity source. 3. Delivery At a minimum: The token/credential must be sent out by registered mail after prior validation of the claimed address against an official identity database in which the physical address was registered.
Retention period for registration	A record of the facts of registration shall be maintained by the

data	CSP or its representative. The suggested minimum retention period for registration data for Level 3 credentials is 7 years beyond the expiration or revocation (whichever is later) of the credential.
Electronic Authentication Phase	
Authentication Protocol for Proof of Possession (PoP)	Preferably **One-time Password PoP** However, according to risk assessment, could also be: - Symmetric Key PoP - Private Key PoP
Token Type	At a minimum, Level 3 requires the use of a **soft crypto token or one-time password device token**. Preferably, a soft crypto token is used.
Requires the application owner to implement protection against	**Eavesdropper** **Replay** **On-line guessing** **Verifier Impersonation** **Man-in-the-middle** **Session Hijacking**

5.5.4 Requirements for Assurance Level 4

	Level 4 Policy
Registration Phase	
Procedure for identity proofing, user details registration, delivery of token and credentials	**Level 4 Registration** 1. Definition Level 4 registration is appropriate for application transactions in which damages that might arise from misappropriation of real-world identity would have a Very high impact. Level 4 identity proofing is distinct in that it directly or indirectly requires in-person identity proofing of official identity documents. 2. Requirements The token/credential must be issued by a body which is subject to a specific government agreement or under government supervision. The RA shall ensure that the subscriber's identity information is verified and checked in accordance with the stated registration policy. Personal appearance is required. During registration, the claimant must present an official identity document such as an identity card, passport or drivers license which contains a photo and signature, and which is verified by the RA before a token/credential can be issued; **Or alternatively** No personal appearance is required; registration is done on-line based on assertions of the claimant which allow his unique identification and which are signed using a qualified signature, which the RA validates. Note that Level 4 security requires that the token/credential must be delivered to the claimant in person (see below), so that it is impossible to obtain Level 4 authentication methods without personal identification. 3. Procedure and delivery The token/credential may only be given to the claimant in person after validation of his identity using an official identity document.
Retention period for registration data	A record of the facts of registration shall be maintained by the CSP or its representative. The suggested minimum retention period for registration data for Level 4 credentials is 10 years beyond the expiration or revocation (whichever is later) of the

	credential.
Electronic Authentication Phase	
Authentication Protocol for Proof of Possession (PoP)	**Symmetric Key PoP**, or **Private Key PoP**
Token Type	Only **Hard crypto tokens** can be accepted at Level 4.
Requires the application owner to implement protection against	**Eavesdropper** **Replay** **On-line guessing** **Verifier Impersonation** **Man-in-the-middle** **Session Hijacking**

6 Mapping of existing authentication mechanisms

6.1 Introduction

Section 5 above proposed a four tiered authentication policy, which was created to be designed in two principal ways:

- First of all, it should allow application owners to determine which type of guarantees they consider to be adequate or necessary for their purposes. They can determine an appropriate authentication level for their application using either the general risk/damage impact assessment methodology contained in section 5.2, or simply by reading the four profiles described directly above in section 5.5, and choosing the level which seems best suited.
- Secondly, the policy should allow the classification for the reported existing main authentication solutions employed in the surveyed countries (the Member States, Candidate Countries and EEA Countries), as described in [RD3], the Draft IDABC Report on Analysis and Assessment of similarities and differences - Impact on eID interoperability; and the preceding Country profiles.

This section 6 specifically concerns the second goal. Below, we will present a mapping of the main reported authentication solutions from the surveyed countries, first ranked according to country (section 6.2) and then according to security level (section 6.3). It should be noted that sections 6.2 and 6.3 thus contain the same information presented in a different way.

Note: The classification below is a proposal for classification based on the available information as collected through the national profiles and analysed in the aforementioned draft report. However, it is possible that certain circumstances of a specific authentication method were underreported, misrepresented or simply misunderstood, which can cause a solution to be ranked too highly or too lowly. Thus, there is a clear need for verification and validation of the proposal before it should be considered final.

6.2 Classification of authentication solutions per country

The table below provides an overview of the main reported authentication solutions sorted by country along with its security level classification in accordance with the criteria defined above.

Country	Authentication solution	Maximum Assurance level
Austria	Citizen card (Bürgerkarte)	4
Austria	Citizen card concept implemented through mobile phones from recognised mobile phone providers	4
Belgium	National eID card	4
Belgium	Qualified soft signature certificates from recognised CSPs	3
Belgium	Federal token - Two factor authentication, using username, password and random string from a paper token	2
Bulgaria	Qualified soft signature certificates from CSPs registered at the Bulgarian Communications Regulation Commission	3
Croatia	FINA eID card	4
Cyprus	TAXISnet - a username/password system based on prior personal identification before a local office	2
Czech Republic	Qualified soft signature certificates from recognised CSPs	3
Czech Republic	Qualified signature certificates on a smart card from recognised CSPs	4
Czech Republic	Username/password system where credentials are issued after signing an application form with a qualified certificate, used in communication with applications from the Czech Social Security Administration, Ministry of Agriculture, etc.	2
Denmark	OCES advanced electronic signature	3
Estonia	National eID card	4
Estonia	Two factor authentication, using username, password and a random string from a paper token, issued by Estonian banks.	2

Estonia	PIN calculators generating live passwords, issued by Estonian banks.	3
Finland	FINEID card	4
Finland	TUPAS: Two factor authentication, using username, password and random string from a paper token, issued by Finnish banks that belong to the Finnish Bankers' Association authentication service	2
France	Daily Life card	4
France	Vitale card	4
Greece	Syzefxis signature certificates on smart cards	4
Greece	Syzefxis soft signature certificates	3
Greece	TAXISnet - a username/password system based on on-line identification using the tax number and ID card number	2
Greece	E-KEP platform - a username/password system based on on-line identification	1
Hungary	Education cards containing signature certificates	4
Hungary	The Client Gate – a username/password system based on prior personal identification or identification through an electronically signed[5] document	2
Iceland	Soft authentication certificates from public administrations, including the Tax Revenue Directorate and the Directorate of Customs	3
Ireland	Reach Services portal – a username/password system based on electronic registration using the PPS number, which is then authenticated against the PSI	2
Italy	Authentication/ attestation certificate in the eID card	4
Italy	Authentication/ attestation certificate in the CNS card	4
Italy	Authentication or signature certificate in the CMD (public servant card)	4
Latvia	Authentication and qualified certificates in private sector smart cards from the State Revenue Service	4

[5] Using an advanced administrative certificate signature. According to the report, registrations using an advanced signature (rather than personal appearance) accounted for 68 out of 520.000 cases, or around 0.01%.

Latvia	eProcurement system - two factor authentication, using username, password and random string from a paper token	2
Latvia	Electronic Declaration System (EDS), username/password system relying on an electronic signature for requesting credentials	2
Lithuania	Qualified signature certificates on a smart card from the recognised CSP	4
Lithuania	Qualified soft signature certificates from the recognised CSP	3
Lithuania	Two factor authentication, using username, password and random string from a paper token issued by one of nine Lithuanian banks	2
Lithuania	PIN calculators generating live passwords issued by one of nine Lithuanian banks	3
Luxembourg	eTVA username/password systems, available after prior registration using hand written forms which are validated by the receiving administration.	2
Malta	The eID system, two factor authentication using username, password and a PIN-code, issued after identification in person	2
Norway	Qualified soft signature certificates from a number of private sector partners, including certain banks (the BankID conglomerate)	3
Norway	Altinn, a username/login system based on registration using government provided temporary credentials	2
Norway	Min Side, a username/login system based on registration using government provided temporary credentials, and allowing the user to change to a self selected password	1
Norway	State Educational Loan Fund using Din Side, a username/login system based on registration using government provided temporary credentials, and allowing the user to change to a self selected password	1
Poland	Qualified signature certificates on a smart card from recognised Certification Authorities in Poland: Certum (www.certum.pl), Sigillum (www.sigillum.pl.com.pl) and Szafir (www.kir.com.pl).	4
Poland	Qualified soft signature certificates recognised Certification Authorities in Poland: Certum (www.certum.pl), Sigillum (www.sigillum.pl.com.pl) and Szafir	3

	(www.kir.com.pl)	
Portugal	Authentication certificate in the national eID card	4
Portugal	Qualified soft signature certificates for lawyers, solicitors or notaries public.	3
Portugal	Citizen's Portal (Portal do Cidadão), a username/password system based purely on electronic registration	1
Slovakia	Qualified soft signature certificates from accredited private sector CSPs	3
Slovakia	Central Portal of Public Administration: basic username/password system	1
Slovenia	Qualified signature certificate on a smart card from the CA at the Ministry of Public Administration	4
Slovenia	Qualified soft signature certificate from accredited private sector CSPs	3
Slovenia	Qualified soft signature certificate from accredited CSP	3
Spain	National eID card	4
Spain	Authentication certificate on a smart card from recognised private and public CSPs	4
Spain	Soft qualified signature certificate from private and public from recognised CSP	3
Spain	Username and password	1
Spain	Password list (mostly in the banking sector)	1
Sweden	Authentication certificates on a smart card from recognised banks	4
Sweden	Soft authentication certificates from recognised banks	3
The Netherlands	DigiD – Username/password system; requires a Social Security Number (or CSN after its introduction). Other levels have been defined but are not yet in use.	2
The Netherlands	DigiD using mobile phone for two factor authentication. Other levels have been defined but are not yet in use.	3
Turkey	Soft authentication certificates from the Ministry of Justice	3
Turkey	Qualified signature certificates on a smart card from accredited CSPs	4

Turkey	Various applications use a basic username/password system based on simple electronic registration	1
United Kingdom	Soft qualified signature certificates from British Chamber of Commerce and Equifax	3
United Kingdom	The Government gateway uses a username/password system; both username and password are self-chosen	1

The overview above shows a total of 68 principal authentication mechanisms over 32 countries, i.e. an average of 2.1 authentication solutions per country. This is an important working number, since the table above shows only the main authentication solutions being used in a country (without focusing on highly specific or niche solutions), and thus is a reasonable first estimate of the number of authentication mechanisms per country that an interoperability model can be expected to support.

6.3 Classification of authentication solutions per level

The table below provides an overview of the main reported authentication solutions sorted by level along with its security level classification in accordance with the criteria defined above.

Country	Authentication solution	Maximum Assurance level
Austria	Citizen card (Bürgerkarte)	4
Austria	Citizen card concept implemented through mobile phones from recognised mobile phone providers	4
Belgium	National eID card	4
Croatia	FINA eID card	4
Czech Republic	Qualified signature certificates on a smart card from recognised CSPs	4
Estonia	National eID card	4
Finland	FINEID card	4
France	Daily Life card	4
France	Vitale card	4
Greece	Syzefxis signature certificates on smart cards	4
Hungary	Education cards containing signature certificates	4
Italy	Authentication/ attestation certificate in the eID card	4
Italy	Authentication/ attestation certificate in the CNS card	4
Italy	Authentication or signature certificate in the CMD (public servant card)	4
Latvia	Authentication and qualified certificates in private sector smart cards from the State Revenue Service	4
Lithuania	Qualified signature certificates on a smart card from the recognised CSP	4
Poland	Qualified signature certificates on a smart card from recognised Certification Authorities in Poland: Certum (www.certum.pl), Sigillum (www.sigillum.pl.com.pl) and Szafir (www.kir.com.pl).	4

Portugal	Authentication certificate in the national eID card	4
Slovenia	Qualified signature certificate on a smart card from the CA at the Ministry of Public Administration	4
Spain	National eID card	4
Spain	Authentication certificate on a smart card from recognised private and public CSPs	4
Sweden	Authentication certificates on a smart card from recognised banks	4
Turkey	Qualified signature certificates on a smart card from accredited CSPs	4
Belgium	Qualified soft signature certificates from recognised CSPs	3
Bulgaria	Qualified soft signature certificates from CSPs registered at the Bulgarian Communications Regulation Commission	3
Czech Republic	Qualified soft signature certificates from recognised CSPs	3
Estonia	PIN calculators generating live passwords, issued by Estonian banks.	3
Greece	Syzefxis soft signature certificates	3
Iceland	Soft authentication certificates from public administrations, including the Tax Revenue Directorate and the Directorate of Customs	3
Lithuania	Qualified soft signature certificates from the recognised CSP	3
Lithuania	PIN calculators generating live passwords issued by one of nine Lithuanian banks	3
Norway	Qualified soft signature certificates from a number of private sector partners, including certain banks (the BankID conglomerate)	3
Poland	Qualified soft signature certificates recognised Certification Authorities in Poland: Certum (www.certum.pl), Sigillum (www.sigillum.pl.com.pl) and Szafir (www.kir.com.pl)	3
Portugal	Qualified soft signature certificates for lawyers, solicitors or notaries public.	3
Slovakia	Qualified soft signature certificates from accredited private sector CSPs	3
Slovenia	Qualified soft signature certificate from accredited private sector CSPs	3

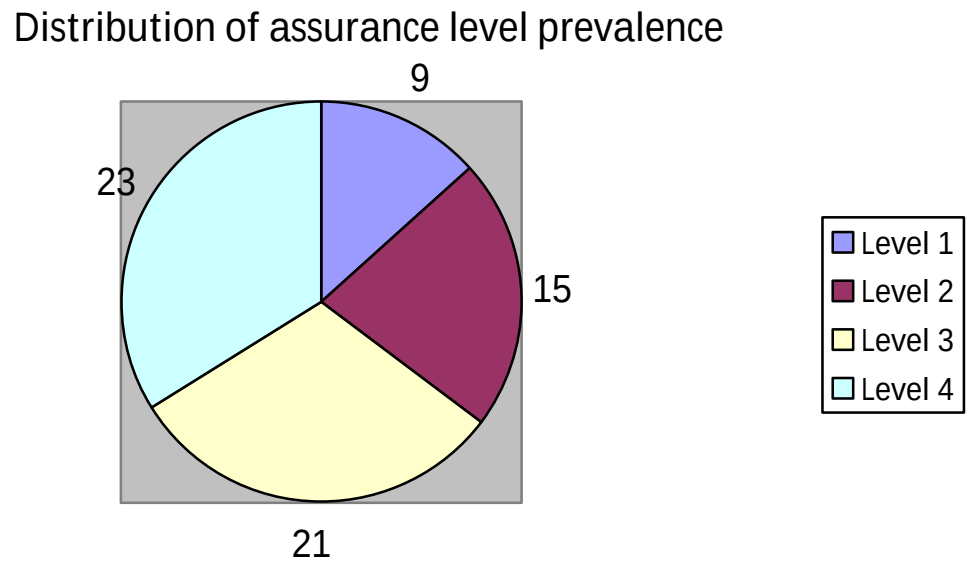
Slovenia	Qualified soft signature certificate from accredited CSP	3
Spain	Soft qualified signature certificate from private and public from recognised CSP	3
Sweden	Soft authentication certificates from recognised banks	3
Turkey	Soft authentication certificates from the Ministry of Justice	3
United Kingdom	Soft qualified signature certificates from British Chamber of Commerce and Equifax	3
The Netherlands	DigiD using mobile phone for two factor authentication	3
Denmark	OCES advanced electronic signature	3
Belgium	Federal token - Two factor authentication, using username, password and random string from a paper token	2
Cyprus	TAXISnet - a username/password system based on prior personal identification before a local office	2
Czech Republic	Username/password system where credentials are issued after signing an application form with a qualified certificate, used in communication with applications from the Czech Social Security Administration, Ministry of Agriculture, etc.	2
Estonia	Two factor authentication, using username, password and a random string from a paper token, issued by Estonian banks.	2
Finland	TUPAS: Two factor authentication, using username, password and random string from a paper token, issued by Finnish banks that belong to the Finnish Bankers' Association authentication service	2
Greece	TAXISnet - a username/password system based on on-line identification using the tax number and ID card number	2
Hungary	The Client Gate – a username/password system based on prior personal identification or identification through an electronically signed[6] document	2

[6] Using an advanced administrative certificate signature. According to the report, registrations using an advanced signature (rather than personal appearance) accounted for 68 out of 520.000 cases, or around 0.01%.

Ireland	Reach Services portal – a username/password system based on electronic registration using the PPS number, which is then authenticated against the PSI	2
Latvia	eProcurement system - two factor authentication, using username, password and random string from a paper token	2
Latvia	Electronic Declaration System (EDS), username/password system relying on an electronic signature for requesting credentials	2
Lithuania	Two factor authentication, using username, password and random string from a paper token issued by one of nine Lithuanian banks	2
Luxembourg	eTVA username/password systems, available after prior registration using hand written forms which are validated by the receiving administration.	2
Malta	The eID system, two factor authentication using username, password and a PIN-code, issued after identification in person	2
Norway	Altinn, a username/login system based on registration using government provided temporary credentials	2
The Netherlands	DigiD – Username/password system; requires a Social Security Number (or CSN after its introduction)	2
Greece	E-KEP platform - a username/password system based on on-line identification	1
Norway	Min Side, a username/login system based on registration using government provided temporary credentials, and allowing the user to change to a self selected password	1
Norway	State Educational Loan Fund using Din Side, a username/login system based on registration using government provided temporary credentials, and allowing the user to change to a self selected password	1
Portugal	Citizen's Portal (Portal do Cidadão), a username/password system based purely on electronic registration	1
Slovakia	Central Portal of Public Administration: basic username/password system	1
Spain	Username and password	1
Spain	Password list (mostly in the banking sector)	1
Turkey	Various applications use a basic	1

	username/password system based on simple electronic registration	
United Kingdom	The Government gateway uses a username/password system; both username and password are self-chosen	1

The table above shows 23 level 4 solutions (34%), 21 level 3 solutions (28%), 15 level 2 solutions 25%), and 9 level 1 solutions (13%).



7 Annex A: Authentication Assurance Level Definition Template

For each identified risk, Sectoral Application owners must determine the authentication assurance level implied and allocate the highest of these to the application.

Damages
n **Loss of integrity**
n **Loss of availability**
n **Loss of confidentiality**
n **Risk to personal safety**
n **Financial loss**

A **Risk** 6	**B** **Likelihood** 6	**C** **Impact of damages** 6					**D** **Highest level** 6
		Very High	High	Medium	Low	Negligible	
Fictitious real-world identity	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	
(1) Not applicable to remote authentication over open networks.							

Risk 6	**Likelihood** 6	**Impact of damages** 6 Very High	High	Medium	Low	Negligible	**Highest level** 6
False details	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	

	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Theft of access token	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Real-world identity theft	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

Risk 6	Likelihood 6	Impact of damages 6: Very High	High	Medium	Low	Negligible	Highest level 6
Interception or revelation of secret authentication information	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

Risk 6	Likelihood 6	Impact of damages 6: Very High	High	Medium	Low	Negligible	Highest level 6
Retention of secret authentication information in a non trusted terminal	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

Risk 6	Likelihood 6	Impact of damages 6: Very High	High	Medium	Low	Negligible	Highest level 6
Unauthorised use of access token	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	

	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Use of compromised credential	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Use of credential after substantive change in circumstances	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	

Use of credential for unintended purposes	Almost certain	(1)	(1)	Level 4	Level 3	Level 3
	Likely	(1)	Level 4	Level 3	Level 3	Level 2
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Withdrawal of credential without due cause	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Fraudulent use of credential	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					Highest level 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Hacker attack	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					Highest level 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Dispersed storage of information	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

Resulting Authentication Assurance Level 4
(highest value of column D)

8 Annex B: Authentication Assurance Level Definition Template

For each identified risk, Sectoral Application owners must determine the authentication assurance level implied and allocate the highest of these to the application.

Damages
n **Loss of integrity**
n **Loss of availability**
n **Loss of confidentiality**
n **Risk to personal safety**
n **Financial loss**

A **Risk** 6	**B** **Likelihood** 6	**C** **Impact of damages** 6					**D** **Highest level** 6
		Very High	High	Medium	Low	Negligible	
Fictitious real-world identity	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

Risk 6	**Likelihood** 6	**Impact of damages** 6					**Highest level** 6
		Very High	High	Medium	Low	Negligible	
False details	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	

	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					Highest level 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Theft of access token	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					Highest level 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Real-world identity theft	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

Risk 6	Likelihood 6	Impact of damages 6: Very High	High	Medium	Low	Negligible	Highest level 6
Interception or revelation of secret authentication information	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

Risk 6	Likelihood 6	Impact of damages 6: Very High	High	Medium	Low	Negligible	Highest level 6
Retention of secret authentication information in a non trusted terminal	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

Risk 6	Likelihood 6	Impact of damages 6: Very High	High	Medium	Low	Negligible	Highest level 6
Unauthorised use of access token	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	

	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Use of compromised credential	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Use of credential after substantive change in circumstances	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	

Use of credential for unintended purposes	Almost certain	(1)	(1)	Level 4	Level 3	Level 3
	Likely	(1)	Level 4	Level 3	Level 3	Level 2
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1

(2) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Withdrawal of credential without due cause	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					**Highest level** 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Fraudulent use of credential	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					Highest level 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Hacker attack	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

		Impact of damages 6					Highest level 6
Risk 6	**Likelihood** 6	Very High	High	Medium	Low	Negligible	
Dispersed storage of information	Almost certain	(1)	(1)	Level 4	Level 3	Level 3	
	Likely	(1)	Level 4	Level 3	Level 3	Level 2	
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2	
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1	
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1	

(1) Not applicable to remote authentication over open networks.

Resulting Authentication Assurance Level 4
(highest value of column D)