eID Interoperability for PEGS

—

Multilevel authentication mechanism (WP4)

Summary of existing national and other authentication schemes

—

European Commission
Directorate General For Informatics

Brussels

—

PROJECT IDENTIFICATION	
CONTRACT NUMBER	PROGRAM
ENTR/05/58-SECURITY/SC3	**N/A**
CUSTOMER	CONTRACTUAL
DG DIGIT	**Yes**

	Name, Function	**Date**	**Signature**
Written by:	Hans Graux – Jarkko Majava	17/10/2007	
Checked by:			
Approved by:			
Authorised by:	Gzim Ocakoglu		

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 first overview of the existing definitions of authentication levels in the Member States, Candidate Countries, EEA Countries and beyond.

KEYWORDS:

DOCUMENT CHARACTERISTICS			
Number of pages	Copy reference	Dependent documents	Host system
70	N/A	None	PC
Number of figures	Recipient name		Software
N/A	N/A		Microsoft® Word 2003

Archive number	Recipient function		
N/A	N/A		

Document Change Log

Issue	Issue Date	Description	Modified paragraphs
1.0	20-August-07	First draft version	All sections
1.1	27-August-07	Technical token linking	Section 4
1.2	4-Oct.-07	Updates based on expert feedback	Section 4
1.4	17-Oct-07	Inclusion of future plans in Austria	Section 4

Contacts

Code	Name	Phone	Email
	Hans Graux	+32 479 795500	hans.graux@timelex.eu
	Jarkko Majava	+32 498 216768	jarkko.majava@gmail.com

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

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

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

	entity's attributes. An entity has only one identity.
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

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 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 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. A number of these countries have also adopted so-called authentication policies, in which a country defines various authentication security levels based on certain criteria (which are trivial in some cases, and quite detailed in others), and which allows them to categorise the authentication services currently being offered. This can provide a guideline to application owners in choosing a suitable security level for their applications, and can also be a useful instrument in summarising the key qualities of a country's authentication policies.

The main objective of the present document is to present an concrete overview of the authentication policies which have been formally or informally adopted in the surveyed counties, in addition to a number of authentication policies from other potentially relevant contexts. This overview will serve as a key input for the definition of generally applicable authentication policies in a later stage of the project.

[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

3.4 Overview of presented approach

To ensure that this document is both pragmatic and usable, it has been structured into three main parts:

- First of all, a presentation of existing authentication solutions in the surveyed countries, including a summary description of their scope and potential for extrapolation to cross-border scenarios (section 4 below);
- Secondly, a presentation of influential and potentially relevant solutions outside of these profiles (section 5 below, including the IDABC Authentication policy document[4] and the U.S. General Services Administration Draft E-Authentication Policy for Federal Agencies[5])
- Finally, a short conclusion is provided, identifying the general trends and approaches which offer the greatest potential for extrapolation to a European level (section 6 below).

Thus, sections 4 and 5 identify and describe the main examples of authentication policies, whereas section 6 provides a summary 'lessons learned' overview declaring which of these examples could be followed on a European scale and why.

Additionally, as a precursor to a further mapping exercise, in Section 4 a technical mapping is made between the authentication policies for each country and a group of authentication methods which would appear to satisfy the requirements of this level. For the purposes of this exercise, a number of abstract authentication token categories have been considered that have been reported to be used in the surveyed countries, specifically:

Authentication token	High level description
Anonymous	Access to an eGovernment service without the user authenticating and revealing his or her identity.
Username/password	A secret character string that a citizen memorizes and a static account (citizen identity) within the eGovernment service.
Onetime password (paper list) 1-OTP paper list only 2-OTP paper list and static username 3-Onetime password/username/static password	1. A personal soft token (paper list) that user possesses. A list contains "PIN" codes for use in authentication. Not often used.[6] 2.

[4] See http://ec.europa.eu/idabc/en/document/3519/5927

[5] See http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-17634.pdf

[6] Because of the lack of implementation in the surveyed countries this type of authentication token will not be included in the authentication policies linking tables below.

	A personal soft token (paper list) that the user possesses. A list contains "PIN" codes for use in authentication. The system usually relies on one-time passwords and users static account (citizen identity) within the authentication system. 3. A personal soft token (paper list) that the user possesses. A list contains "PIN" codes for use in authentication. The system usually relies on one-time passwords, user static account (citizen identity) and additional static password within the authentication system.
Mobile SMS onetime password	A personal soft token (mobile device) that the user possesses. The authentication system sends a one-time password to the citizen mobile device. The system usually relies on one-time passwords and users static account (citizen identity) within the authentication system.
Onetime password (device token)	A personal hardware based security token that generates "one time" passwords for use in authentication. The type of these devices can vary from tokens with integral entry pad to the tokens without entry pad connected to a computer with some specified link. Two main types of devices can be recognized: mathematical-algorithm-based devices and time-synchronized devices.
Soft crypto token	A cryptographic key that is typically stored on standard PKCS#12[7] file. The certificate file can then be stored on disk or some other form of storage media. The soft token is encrypted using users' PIN-code ("password"). In the authentication process the user is required to input this password to gain access to an eGovernment service.
Hard crypto token	A smartcard or mobile device that contains a protected cryptographic key. A token carrying a citizen cryptographic key and certificate needs to be security certified[8] to the predefined level. The crypto hard token system requires users to provide possession of the device and to know some predefined PIN-code ("password") to access the key. There is no possibility to export

[7] PKCS#12 standard specifies a portable format for storing or transporting a user's private keys, certificates, miscellaneous secrets, etc.

[8] Commonly agreed security certification in the surveyed countries included; Common Criteria certifications at EAL4+ and EAL5+ and FIPS 140-1 level 1 to level 3 key protections.

	authentication keys from the secured device.

Thus, the tables in section 4 below will provide an overview and description of the defined authentication levels, and will indicate how the abstract tokens above could be mapped into the authentication levels. In cases where the country actually uses a specific token type (such as a one-time password or hard crypto token) these mappings should be entirely accurate; of course, when the token is not used (i.e. a country does not use any one-time password or hard crypto token systems) a classification is proposed by the author based on the abstract descriptions above and the logical structure of the authentication policy.

The goal of this exercise is of course not to propose any kind of binding mapping system (which would be impossible due to the use of abstract definitions which keep into account the inherent properties of the defined tokens, but not e.g. the preceding registration process), but rather to get a first indication of the (in)flexibility of the authentication policies already being used.

4 National authentication policies in European countries

4.1 Summary overview

As outlined in the Draft Report on Analysis and Assessment of similarities and differences - Impact on eID interoperability [AD3], not all of the surveyed countries (Member States, Candidate Countries and E.E.A.) have adopted authentication policies. The situation has been summarised in the table below.

Please note that, for the purposes of this table, a policy is considered to be 'formally adopted' if a specific government decision has been made to embrace the policy and to use it in practice; whereas a policy is labelled as 'informally adopted' if it is occasionally quoted without any formal government support or impact in practice.

Country	Status (Formally adopted / Informally adopted / Non-existent)	Description / Details
Austria	Formally adopted	Austrian law distinguishes between unique identities and recurring identities. The former indicate that an exact person can be identified, whereas the latter only ensures linkability (i.e. that a person's interactions can be identified as having the same origin, although that origin cannot necessarily be traced back to a specific individual). As will be noted below (section 4.2.1.1.), this system will likely be abolished in the short term, and a more general policy is being considered for future adoption.
Belgian	Informally adopted	A four level system exists, but is not formally adopted by application owners.
Bulgaria	Non-existent	N.A.
Croatia	Non-existent	N.A.
Cyprus	Non-existent	N.A.
Czech Republic	Non-existent	N.A.
Denmark	Non-existent	High standardisation (through the OCES signature) makes multilevel policies irrelevant; since only one solution is formally proposed as the standard, there is little point in drafting up hierarchies with other niche systems.
Estonia	Non-existent	N.A.
Finland	Informally adopted	A four level system exists, but is not formally

		adopted by application owners.
France	Formally adopted	A three tier system has been formally adopted through the general Security framework of reference ([*Politique de référencement intersectoriel de sécurité*] (PRIS)); application owners can freely determine which of the three levels they require; this principle (gradual security principle) is also formally endorsed by the CNIL (the National Data Protection Authority).
Germany	Non-existent	No nation-wide eIDM system exists yet; the issue is therefore premature. However, preliminary work to create an extensive authentication policy has already been done. A draft document has been created, and this draft will be further discussed below. It should be noted that the document is provisional and subject to future change.
Greece	Informally adopted	An informal two tier system can be deduced, the first based on a username/password system; the second using the Syzefxis PKI system.
Hungary	Informally adopted	A four tier system has been referred to in policy documents; but there is no formal consequence to this.
Iceland	Not yet adopted.	An authentication policy is under consideration as a part of plans for introducing a PKI based authentication system.
Ireland	Non-existent	N.A.
Italy	Non-existent	N.A.
Latvia	Non-existent	N.A.
Liechtenstein	Non-existent	N.A.
Lithuania	Non-existent	N.A.
Luxembourg	Non-existent	N.A.
Malta	Informally adopted	Maltese authentication plans revolve around a four tier system: Level 1: restricted authentication (login, password and PIN); Level 3: confidential authentication (digital certificate); Level 4: maximum authentication (qualified digital certificate). However, only Level 1 is currently deployed.
The Netherlands	Informally adopted	An informal two tier system can be deduced, the first based on the DigiD username/password system; the second using the future eID card ENIK as a PKI device.

Norway	Formally adopted	A fairly detailed policy has been adopted through the "Strategy on eID and e-signature in the Public Sector" policy document. This document describes a four level security system, keeping into account registration requirements, management policies and potential risks. This system has been referred to in related legislation.
Poland	Informally adopted	An informal four tier system can be deduced from an official document „The security rules for ePUAP – WKP".
Portugal	Non-existent	N.A.
Romania	Non-existent	N.A.
Slovakia	Informally adopted	No formal system, but an informal three tier system can be deduced (username/password, qualified signature with prior personal identification, and qualified signature with a unique identifier in the certificate).
Slovenia	Informally adopted	An informal three tier system has been adopted (direct input of personal data, username/password, and qualified certificates)
Spain	Informally adopted	An informal three tier system can be derived (username/password, two factor authentication with a random password, and authentication certificate)
Sweden	Non-existent	High standardisation (through the bank issued eIDs) makes multilevel policies irrelevant.
Turkey	Informally adopted	The eGovernment Gateway project implies the recognition of a three tier system: login based on unique ID number, two factor authentication using a random string, authentication certificate.
United Kingdom	Formally adopted	The UK government's Strategic Action Plan distinguishes a number of authentication means based on damage risks through the 'Registration and Authentication - e-Government Strategy Framework Policy and Guidelines Version 3.0', but does not implement a strict hierarchy between these.

Thus, in 15 out of 32 countries (47%) some form of multilevel authentication policy can be recognised; but only in 4 of these countries (10% - Austria, France, Norway and the UK) can a formal authentication policy be identified. It can be noted however that the classification of the Austrian policy as an authentication policy is debatable, as it is mainly intended as a way of integrating foreign eIDM systems into the Austrian system, rather than an internal authentication policy. However, Austria's future authentication policy plans (see section 4.2.1.1 below) will certainly qualify as a formally adopted authentication policy.

The section below will take a closer look at these fifteen countries which have formally or informally adopted authentication levels, and will examine the scope and relevance of these policies in greater detail.

4.2 Extended overview and basic principles

4.2.1 Formally adopted policies

As noted above, four countries (Austria, France, Norway and the UK) have formally adopted authentication policies. These shall be examined in greater detail in this section. In addition, the German draft proposal for an authentication policy will also be briefly examined, due to its potential impact in the future, even though the document is still in a draft stage and has not (yet) been accepted in a definitive form.

4.2.1.1 Austria

4.2.1.1.1 Description

Austrian law distinguishes between unique identities and recurring identities. The former indicate that an exact person can be identified, whereas the latter only ensures linkability (i.e. that a person's interactions can be identified as having the same origin, although that origin cannot necessarily be traced back to a specific individual).

More specifically, the Austria eGovernment Act defines two identification levels, as follows:

- *Unique identity*: "*designation of a specific person by means of one or more features enabling that data subject to be unmistakably distinguished from all other data subjects*"

- *Recurring identity*: "*designation of a specific person in a way which, while not ensuring unique identity, enables this person to be recognised by reference to a previous event, such as an earlier submission*"

The first identification level, the unique identity, is offered by Austrian citizen cards (typically but not necessarily smart cards), as the identity is linked to the unique identifiers stored in the Austrian base registers.

The second level, the recurring identity, is only relevant for the integration of foreign eIDs into the Austrian identity infrastructure. Basically, the Austrian eGovernment Act and the sourcePIN Register Authority Regulations allow the Austrian identifiers (which are required for the unique identity) to be substituted by so-called substitute sourcePINs; i.e. the unique identifier used by a foreign signature token can be accepted as a substitute for an Austrian identifier. This substitute sourcePIN is then used as a recurring identity.

4.2.1.1.2 Technical authentication method linking

As noted above, the classification in the Austrian policy is concentrated on PKI based authentications, so technically linking needs to be highly simplified.

Non mapped authentication methods	*Anonymous* *Username/password* *Onetime password (paper list)* *Mobile SMS onetime password* *Onetime password (device token)* *Onetime password/username/static password*
Unique Identity	National soft crypto token National hard crypto token
Recurring identity	Foreign soft crypto token Foreign hard crypto token

As shown in the table above, the mapping of several commonly used authentication tokens to specific authentication levels is not possible in the Austrian authentication policy model, as non-PKI based methods are not included.

4.2.1.1.3 Scope and potential for cross border generalisation

As noted above, the classification of the Austrian policy as an authentication policy is debatable, as it is mainly intended as a way of integrating foreign eIDM systems (or more accurately: foreign eSignature creation systems) into the Austrian system, rather than as an internal authentication policy. The approach is not intended to be used as a classification system for authentication solutions.

However, Austria has announced its intention to amend its E-Government Act, eliminating the recurring identity for foreigners. Under the new plans, foreign eID cards will be treated equally to the Austrian Citizen Card, provided they meet certain requirements. The amended Act is expected to be adopted by the end of 2007.

In addition, a body comprising governmental officials from all Austrian administrative levels have recently adopted an authentication policy called "Security Classes for Accessing Applications" (SecClass 2.0.0)[9], which clearly defines four categories of data processing:

Security Class 0: openly available data;

Security Class 1: access to personal data which is openly available to third parties (e.g. information from the central residence register);

Security Class 2: transactions with personal data;

Security Class 3: transactions with sensitive personal data.

[9] See http://reference.e-government.gv.at/Sicherheitsklassen_-_SecClass.1040.0.html

The paper also defines which authentication method is permissible for each security class, e.g. knowledge based and ownership based (SW-Certificate, HW-Token, Citizen Card, One-Time-Password) would be permissible up to security class 2 – but it would not be sufficient for security class 3. This policy is more generic in nature, and offers greater potential for generalisation.

4.2.1.2 France

4.2.1.2.1 Description

A three tier system has been formally adopted through the general Security framework of reference ([*Politique de référencement intersectoriel de sécurité*] (PRIS)). Application owners can use this system to freely determine which of the three levels they require. This principle (gradual security principle) is also formally endorsed by the CNIL (the National Data Protection Authority).

Specifically, article 4 of the Ordinance n°2005-1516 requires public authorities to comply with the general Interoperability and Security frameworks of reference. The general Security framework of reference (*référentiel général de sécurité*)[10], the so-called Security inter-sector framework of reference [*Politique de référencement intersectoriel de sécurité*] (PRIS), distinguished three different security levels according to the sensitivity of the data exchanged and the risk of identity theft: middle, strong/standard and strengthened. The level of security required for each service offered is defined by the public authority providing the service.

It should be mentioned that the CNIL has set up a 'gradual security principle' in its opinion on the Electronic Administration Plan[11]. It advocates for the respect of anonymity where the authentication is not required for the provision of the public service. Where authentication is required, the authentication means should also pass a strict proportionality test: security requirements should be adapted to each e-process. The use of electronic signatures should not be systematic and, according to the CNIL, does not constitute a prior condition for the implementation of e-processes.

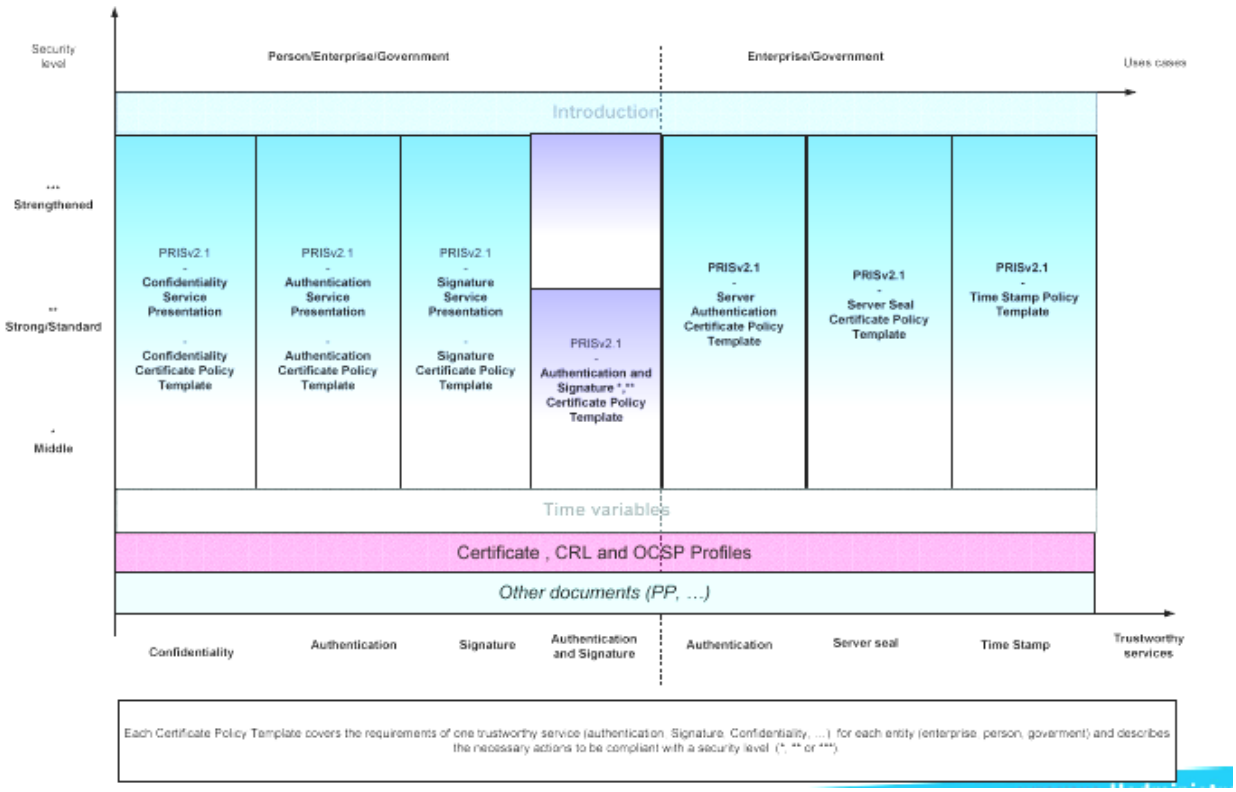
The security frame of reference (PRIS) defines security functions requirements such as electronic signature, authentication, confidentiality, timestamping and e-archiving, as illustrated in the table below[12]. This assessment is carried out by public authorities issuing the eIDM. Daily Life cards, Vitale Card and the future eID card are considered to require a high level of security.[13]

[10] Decree nº2007-284 of 2 March 2007 on Interoperability general frame of reference [*relatif au referential general d'interopérabilité*], J.O. nº 53 pf 3 March 2007, page 4060.

[11] CNIL, 26 February 2004, Op. cit.

[12] The graph is extracted from Schiavo M., PRIS V.2.1, A general security frame of reference, available at: http://synergies.modernisation.gouv.fr/IMG/pdf/061129_PRIS_US_ENISA.pdf

[13] Ministry of Civil Service, State Reform and Land settlement, Electronic Administration Strategic Plan (PSAE) 2004-2007, p.22



PRIS applies to security products and trustworthy service providers within electronic exchanges between users and public agencies and between public agencies. The general PRIS framework is based on standards ISO TS 101456 and RFC 3647. The authentication function is based on asymmetric keys and X509 certificates. The following table describe the different authentication requirements set up by the PRIS:

Trustworthy service providers	Strengthened	Strong	Middle
Registration phase	Face to face	Face to face	- Sending of a registration file in paper form (with certified copy of the identity papers) or in electronic form or communication of a specific element of the subscriber allowing to identify it within an administrative data base.
Delivery /acceptance of a certificate	-Delivery in person with face to face if not done during registration phase -- If AC does not generate the key, to check if the certificate is well associated with the corresponding private key -- Explicit acceptance of the certificate by the subscriber	-Delivery in person with face to face if not done during registration phase -if possible, explicit acceptance of the certificate by the subscriber or tacit acceptance starting from a sufficiently reliable handover date.	- Delivery by email - Tacit acceptance

Trustworthy service providers	***	**	*
Certificate revocation	Formal authentication of the request via a strong mechanism (ex: series of 4/5 questions/answers, use of a certificate and tool **,...) - Service : - available 24/24 and 7/7 - unavailable maximum : 2h per month. -Time between validation of the request and update of information less than 24h (7/7)	Formal authentication of the request (ex: series of 3/4 questions/answers, use of a certificate and tool *,...) - Service : - available 24/24 and 7/7 - unavailable maximum : 4h per month. -Time between validation of the request and update of information less than 24h (7/7)	- Authentication of the request by checking one or two information on the person (phone number, address, …) - Service : - available at least during working days - unavailable maximum : 4h per month. -Time, between validation of the request and update of information less than 1 working day
Certificate Revocation List	-At least, publication of CRL. - Recommendation of implementation of deltaCRL and an OCSP service. - Service : - available 24/24 and 7/7 - unavailable maximum : 4h per month.	-At least, publication of CRL. - Recommendation of implementation of deltaCRL and an OCSP service. - Service : - available 24/24 and 7/7 - unavailable maximum : 4h per month.	-At least, publication of CRL. - Recommendation of implementation of an OCSP service. - Service : - available at least during working days - unavailable maximum : 32h per month.
CA Key pair protection	-Generation and protection of the CA keys and certificates in a cryptographic module certified at a level CC EAL4+ - Key Ceremony under the control of at least two people (security responsibility) and at least two external witnesses (of which a recommended public officer). - CA Private keys controlled by at least two people with security responsibility (secret share) - Private CA keys activated by at least two people with security responsibility	-Generation and protection of the CA keys and certificates in a cryptographic module certified at a level CC EAL2+ -Key Ceremony under the control of at least two people (security responsibility) and at least one external witness -CA Private keys controlled by at least two people with security responsibility (secret share) - Private CA keys activated by at least two people with security responsibility	-Generation and protection of the CA keys and certificates in a cryptographic module compliant to the requirements in the CP Template --Key Ceremony under the control of at least one person (security responsibility) and several witnesses -CA Private keys controlled by at least one person with security responsibility - Private CA keys activated by at least one person with security responsibility
Subscriber Private key generation (if generated by CA outside the authentication device)	-Generation in a cryptographic module certified at a level CC EAL4+	-Generation in a cryptographic module certified at a level CC EAL2+	Generation in a cryptographic module compliant with the requirements in the CP Template

Authentication Key length	- RSA : 2048 b - DSA : 2048 b /q = 256	- RSA : 2048 b - DSA : 2048 b /q = 256	- RSA : 1024 b or 2048 b - DSA : 1024 b/q=160 or 2048 b/q = 256
Authentication device	- A device CC Certified at a level EAL4+ .	- A device CC Certified at level EAL2+	- Compliant to the requirements in the CP Template
Authentication application	- An authentication application CC certified at a level EAL2+ .	- An authentication application CC certified at level EAL2+ should be used	
Module to verify the authentication process	- A module CC certified at a level EAL2 should be used	- A module CC certified at a level EAL2 should be used	

The French government has set up a CA hierarchy with a general accreditation body (the COFRAC *Comité français d'accréditation*). This body accredits certifications authorities which qualifies trust service providers, according to the requirements stated in the PRIS. These certification authorities are usually constituted in GIP and sector specific (GIP-CPS, GIP-SESAM, GIP-MDS, etc.). This procedure has been developed by the Ministry of Economy, Public Finances and Industry in the year 2000 when the first e-processes were launched (e-VAT, e-Income). The DGME (ex-ADAE) has extended the procedure to all public administration in 2004 and integrated it to the PRIS.

More information is available at http://synergies.modernisation.gouv.fr/article.php3?id_article=381

4.2.1.2.2 Technical authentication method linking

The French approach is focused specifically on PKI based authentication methods. Because of that, the linking of other tokens is irrelevant.

4.2.1.2.3 Scope and potential for cross border generalisation

The French approach shows a great deal more detail than most other authentication policies, and defines a three tiered system based on (inter alia) registration requirements, and the issuance and management of PKI certificates. In addition, the French model defines a set of specific technical criteria, which means that the level of standardisation is potentially much greater.

The downside of this approach is that the PRIS is focused specifically on a PKI based approach, and a number of the requirements cannot be easily transposed to a non-PKI based authentication environment.

None the less, it is clear that the French approach is one of the most advanced in Europe, not only because of the detail of its elaboration, but also because it is one of the few policies which are actually applied in practice, rather than being a purely theoretical model.

For this reason, the model should be given strong consideration when drafting a model for European authentication policies.

4.2.1.3 Norway

4.2.1.3.1 Description

A highly detailed authentication policy has been adopted through the "Strategy on eID and e-signature in the Public Sector" policy document of March 2007. While not an officially binding policy document, the text describes a four level security system, keeping into account registration requirements, management policies and potential risks.

Risk levels for authentication are defined as follows:

	Risk level 1 None	Risk level 2 Small	Risk level 3 Moderate	Risk level 4 Large
Consequence for life and health	There is no danger of loss of life and/or health damage	There may occur minor health damage	There may occur minor health damage	There may occur of loss of life and/or major health damage
Financial loss / extra work / incur increased costs	No financial losses / extra work / incur increased costs	There may occur minor financial losses / extra work / incur increased costs	There may occur moderate financial losses / extra work / incur increased costs	There may occur major financial losses / extra work / incur increased costs
Loss of reputation (standing, trust and integrity)	No loss of reputation	Possible damage on reputation is considered trivial	Reputation may be weakened for a short period of time	Reputation may be damaged for a longer period of time, possible for ever
Obstruction of justice	No contribution to obstruction of justice	Minimal contribution to obstruction of justice	Moderate contribution to obstruction of justice	It may incur obstruction of justice
Accomplice liability / accessory to violation of the law	Accomplice liability / accessory may not occur.	Accomplice liability / accessory may not occur.	Accomplice liability / accessory may not occur.	Accomplice liability / accessory may not occur.
General problems / inconveniences	No general problems or inconveniences	There may occur some general problems or inconveniences	N/A	N/A

Each of these risk levels is proposed to be mapped to four security levels, defined as follows:

LEVEL	Requirements Regarding Authentication Factors	Issuance to holders		Assurance of authentication factors, when storing	Requirement to public registration	Requirements on non-repudiation
		Natural persons	Legal persons			
1	No requirements	No requirements	No requirements	No requirements	No requirements	No requirements
2	One factor	Mail to registered address at the Central Population Register	Mail to registered address. The name of the natural person that can sign on behalf the legal person shall be the first to receive the sending.	Both static and dynamic can be copied	No requirements	It shall be established routines and logs, that make it reasonably sure that the party you are communicating with stands behind an activity or data
3	Two factor, of which one is dynamic	Same requirements as for level 2, with the additional requirement that one ensures in one way or the other that it is the right user	Same requirement as for level 2, with the additional requirement that one ensures in one way or the other that it is the right user	Dynamic can be copied. Static cannot be copied	No requirements	It shall be established routines and logs, that make it reasonably sure that the party you are communicating with stands behind an activity or data
4	Two factor, of which one is dynamic	The requirements on registration and issuance in accordance with the ”Requirement Specification for PKI for the Public Sector”, Person-High. To meet up in person with ID-documents, at least the first time.	The natural person that can sign on behalf of the legal person, either by meeting up in person, or give a proxy to another that meets up in person. The person meeting up shall present ID-documents, and be checked against the Central Coordinating Register for	Cannot be copied.	Shall be declared in accordance with public requirements.	A party to the communication shall be able to verify that the other party stands behind an activity or data. The party shall not be able by himself to produce or alter such an evidence afterwards.

			Legal Entities. Requirements in accordance with the "Requirement Specification for PKI for the Public Sector", Enterprise.			

Security level 1

This security level gives no security. Used in open communication. There are security solutions that fall within this category, e.g.

- self-elected password and user name over the net
- identification using only a personal registration number

Security level 2

Examples:

- Static password, sent to the address registered with the National Registry
- Password calculator not protected by a password, at a minimum distributed to the address registered with the National Registry
- Lists with one-time passwords, distributed to the address registered with the National Registry

Security level 3

Examples:

- Password calculator protected by a PIN-code, where the first PIN-code is sent by a separate mail
- One-time passwords on cellular phone, where the cellular phone is registered with an own registration code distributed to the address registered with the National Registry
- Person-Standard pursuant to the "Requirement Specification for PKI for the Public Sector",
- List with one-time passwords, used together with a static password and user name.

Security level 4

On this security level only solutions based on PKI can be accepted. Pursuant to the requirements in existing regulation the solutions must be registered with the National Post and Telecommunication Authority, in accordance with the "Requirement Specification for PKI for the Public Sector", when it comes to Person-High and Enterprise. Examples:

- A two-factor solution, of which one is dynamic, of which one of the factors or registration factor is delivered personally. It is used a third party to register a log with a connection between activity/data and identity. The log shall be stored with protection against modifications.

- A two-factor solution, of which one is dynamic, of which one of the factors or registration factor is delivered personally. It is used a special program that prevents the users to generate false documentation of whom is standing behind data/activity and that prevents the provider to change the log of data/activities and identity.

In addition to the "Strategy on eID and e-signature in the Public Sector", more specific eID requirements have been defined in the "Requirement Specification for PKI for the public service"[14]. There is a significant drive in the Government, especially on the central level, to adhere to this nonbinding specification.

Rather than the Strategy's four-tiered system based on risk assessment, the Specification defines a three-tiered system which applies to signatures, eIDM and encryption solutions using PKI systems with PIN-codes. These three tiers have been designated as Personal-High, Personal-Standard (both for natural persons) and Enterprise (for legal entities).

The security levels and a selection of properties are specified in the table below:

SECURITY LEVELS	Registration and release procedure	Requirements as to name structure and content	Requirements as to protection of private keys
"Person-High"	The certificate must be a qualified certificate and the certificate issuer must fulfil the registration and release procedures that follow from this, including the requirement as to personal attendance.	The name structure and certificate content must follow the requirements in Section 4 of the Act on Electronic Signatures (e-signaturloven) [2] with the clarifications that follow from "Recommended certificate profiles for person certificates and enterprise certificates" [10].	• Access to private keys must as a minimum require two-factor authentication, where one of the factors is something in the physical possession of the user (i.e. cannot be copied electronically). • The user must approve each operation involving private keys by authenticating him/herself • Private keys must never appear in plain text in registers that might be compromised or in other ways provide a basis for unauthorised use.

[14] http://www.regjeringen.no/en/dep/fad/Documents/rapporter_planer/Rapporter/2005/Requirements-specification-for-PKI-for-the-public-sector.html?id=420380

"Person-Standard"	The certificate issuer must fulfil the requirements in Sections 10 to 16 of the Act on Electronic Signatures (e-signaturloven)[2] and Section 3 of the Regulations on requirements applicable to issuers of qualified certificates etc. (Forskrift om krav til utsteder av kvaliserte sertifikater) [4]. Verification must take place upon registration that the person is found in a Norwegian population register and that the name of the person accords with his or her national identity number. A reasonable degree of certainty must exist that keys and/or associated access codes/passwords and certificates are released to the correct person. Release must either be by postal dispatch to the registered address or electronically based on existing authentication mechanisms providing the same degree of security of correct receipt as a postal dispatch to the registered address.	The certificate must fulfil the requirements applicable to qualified certificates in Section 4 second paragraph letters b to j of the Act on Electronic Signatures (e-signaturloven) [2]. In other respects the name structure and certificate content must follow "Recommend certificate profiles for person certificates and enterprise certificates" [10].	• Access to private keys must require authentication • The user must have scope for choosing/deciding him/herself whether the individual operation involving private keys is to be approved. • Private keys must as a minimum be stored in encrypted form.

SECURITY LEVELS	Registration and release procedure	Requirements as to name structure and content	Requirements as to protection of private keys
"Enterprise"	The certificate issuer must fulfil the requirements in Sections 3 and 7 of the Act on Electronic Signatures [2] (e-signaturloven) and Section 3 of the Regulations on requirements applicable to issuers of qualified certificates etc. (Forskrift om krav til utsteder av kvaliserte sertifikater) [4]. It must be possible to identify the enterprise uniquely by equipping the certificate with the organisation number of the enterprise from the Central Coordinating Register for Legal Entities in accordance with the SEID certificate profile [10]. Safeguard must be in place to ensure that keys with associated access codes/ passwords and certificates are released to a person with the right to receive them on behalf of the enterprise. (Authorisation from an authorised signatory of the company.) Documentation of the relationship to be possible.	The certificate must fulfil the requirements as to qualified certificates in Section 4 second paragraph letters b to j of the Act on Electronic Signatures (e-signatur-loven) [2]. The name structure and certificate content must follow "Recommended certificate profiles for person certificates and enterprise certificates" [10]. The certificate must contain the organisation number of the enterprise.	• Access control to private keys must be realisable. • The enterprise must have scope for choosing/deciding him/herself whether each operation involving private keys is to be approved. • Private keys must as a minimum be stored in encrypted form.

The table below shows the intended use of the various types of certificates:

USES FOR CERTIFICATE LEVELS	Authentication	Signature (non-repudiation)	Receipt of encrypted information
Person-High	Transactions where there is a need for a high degree of certainty about the identity of the originator, for example in connection with access to particularly sensitive information or where the damage caused by a compromise would be extensive.	Transactions where there is a need for a high degree of certainty about the connection between content and the identity of the originator or where the damage caused by the compromising of the connection would be extensive.	Documents etc. containing particularly sensitive information or where the damage caused by a compromise would be extensive.
Person-Standard	Transactions where there is a need for a reasonable degree of certainty about the identity of the originator or where the damage caused by a compromise would be medium level.	Transactions where there is a need for a reasonable degree of certainty about the connection between content and the identity of the originator or where the damage caused by the compro-mising of the connection would be medium level.	Documents etc. that do not contain particularly sensitive information and where the damage caused by a compromise would not be extensive.
Enterprise	Transactions where there is a need for a high degree of certainty that the originator is/represents a specified enterprise or where the damage caused by a compromise would be	Transactions where there is a need for a high degree of certainty about the connection between content and the specified enterprise or where the damage caused by the compromising	Documents etc. containing particularly sensitive information or where the damage caused by a compromise would be

Finally, there are a number of common requirements for all three security-levels (unless expressly stated otherwise):

- The certificates shall follow "Recommended certificate profiles for person certificates and enterprise certificates", unless these are not relevant to the certificate type. If other formats are used any deviations shall be documented (4.1.6)
- The certificates should support user-specified non-critical extensions of the fields. (4.1.10)
- For Personal-Standard and Enterprise storage of keys as encrypted PKCS # 12 objects should be permitted (4.3.4 and 4.4.5).
- The Supplier shall document whether the solutions for presenting and verifying signed data comply with the requirements in CWA 14171 (7.1)
- If the Supplier supplies a signature service, documentation shall be provided of whether the solution complies with the requirements and recommendations in CWA 14170 (7.2).
- All user dialogues, help text and instructions shall be available in the Norwegian language (8.1.1 – 8.1.3).
- What the user sees shall match what she signs. The way in which this principle is satisfied shall be documented (8.1.7).
- Sufficient documentation shall be provided to allow a programmer with general expertise but no knowledge of the interface to utilise it (8.2.2)
- The solution shall not tie the user to a single platform as regards for example operating system or web browser (8.3.1).
- The CSP shall specify the operating systems that the end user may use. This shall include versions and support for "thin Clients". (Windows XP, Red Hat Linux, Citrixterminal server etc.) The solution shall as a minimum function on the three most commonly used operating systems for end-user environments (Windows, Linux and MAC). (8.3.3)
- Client interoperability (9.4)
  - Certificates should be available for running "Microsoft Certificate Store".
  - Operations with private keys should be available for applications using Microsoft CRYPTOAPI or PKCS#11.
  - The S/MIME format shall be used for encrypting e-mail.
  - The solution should support SSL Client certificates.

4.2.1.3.2 Technical authentication method linking

The Strategy on eID and e-signature in the Public Sector model allows the mapping of PKI based and non-PKI based authentication solutions.

Level1	Anonymous Username/password (self elected)
Level2	Onetime password (paper list) Username/password (centrally deployed)
Level3	Mobile SMS onetime password Onetime password (device token) Onetime password/username/static password Soft crypto token
Level4	Hard crypto token

The table above shows that in the Norwegian model, the mapping of all authentication tokens recognized by the surveyed countries is possible.

On the other hand, the three tiered Requirement Specification focuses uniquely on PKI based authentications solutions.

4.2.1.3.3 Scope and potential for cross border generalisation

The three tiered Requirement Specification is quite highly detailed, covering registration and registration requirements, name structure and content requirements and the protection of private keys. The more generally applicable Strategy serves as a useful background document in this respect, providing a list of potential risks and security responses.

However, it should be noted that the Requirement Specification is organised differently from most authentication policies, in the sense that it does not simply distinguish between security levels, but it also distinguishes between user groups (by creating two levels for natural persons and one for legal entities). While this can be an advantage because the system acknowledges the different issues between these user groups, this also makes it harder to compare it with other authentication policies.

Also, like the French model mentioned above, the Requirement Specification is focused specifically on a PKI based approach, and a number of the requirements cannot be easily transposed to a non-PKI based authentication environment.

The requirements specification does not cover the use of PKI for signing program modules or authentication/key management of processes and computers. Nor does the document define requirements for employee certificates, since it is assumed that in technical terms person certificates will in many cases cover this requirement. In such cases it will, inter alia, be the issuance procedures and rules on authorisation and use within an enterprise that will determine whether or not a person certificate can be used in a professional context.

4.2.1.4 United Kingdom

4.2.1.4.1 Description

The UK government's Strategic Action Plan distinguishes a number of registration and authentication levels based on damage risks through the 'Registration and Authentication - e-Government Strategy Framework Policy and Guidelines Version 3.0[15]', but does not implement a strict hierarchy between these.

Specifically, the document focuses on defining guidelines for effective user identification and authentication; effective user registration; effective access control; and effective user access management.

For the purposes of e-Government transactions, the document defines levels of registration and authentication that are appropriate for the different classes of transactions. However, unlike most other approaches, the UK Framework acknowledges that registration and authentication might not possess equal emphasis; i.e. it is possible for an application to require level 1 registration, but higher level authentication.

The fundamental approach recognises four tiers of access requirements:

> *"a) Anonymous or pseudonymous: Neither the real-world identity of the client nor an electronic identity in an associated credential is required to complete the transaction. In the latter case, the client provides a pseudonym (registration level: 0, authentication level: 0).*
>
> *b) Anonymous or pseudonymous with electronic identity: The real-world identity of the client is not required to complete the transaction, but the electronic identity enables the service provider to recognise the client in repeat transactions (registration level: 0, authentication level: 1, 2 or 3).*
>
> *c) Anonymous or pseudonymous with electronic identity and traceable: The real-world identity of the client is not required to complete the transaction, but the electronic identity enables the service provider to recognise the client in repeat transactions and could be used to retrieve the real-world identity via the RA, if required (registration level: 1, 2 or 3, authentication level: 1, 2 or 3).*
>
> *d) Real-world identity established – the real-world identity of the client needs to be established to some degree of confidence before the transaction can be performed (registration level: 1, 2 or 3, authentication level: 1, 2 or 3)."*

It is the responsibility of specific departments to decide which levels of registration/authentication are required for their applications.

The registration and authentication levels are defined in terms of potential damage, and recognises four tiers for both aspects:

> *"**Registration Level 0 – minimal damage***

15 http://www.govtalk.gov.uk/policydocs/policydocs_document.asp?docnum=654&topic=56&topictitle=Security+Framework&subjecttitle=

Level 0 registration is appropriate for e-Government transactions in which minimal damage might arise from misappropriation of real-world identity. In particular, misappropriation of a client's real-world identity at level 0 might result in at most:

- *minimal inconvenience to any party; or*
- *no risk to any party's personal safety; or*
- *no release of personally or commercially sensitive data to third parties; or*
- *minimal financial loss23 to any party; or*
- *no damage to any party's standing or reputation; or*
- *no distress being caused to any party; or*
- *no assistance in the commission of or hindrance to the detection of serious crime.*

No formal registration processes required, but might require issue of credentials.

Registration Level 1 – minor damage

Level 1 registration is appropriate for e-Government transactions in which minor damage might arise from misappropriation of real-world identity. In particular, misappropriation of a client's real-world identity at level 1 might result in at most:

- *minor inconvenience to any party; or*
- *no risk to any party's personal safety; or*
- *no release of personally or commercially sensitive data to third parties; or*
- *minor financial loss to any party; or*
- *minor damage to any party's standing or reputation; or*
- *minor distress being caused to any party; or*
- *no assistance in the commission of or hindrance to the detection of serious crime.*

Registration at this level is designed to prevent possible inconvenience to clients and deter casual false or misappropriated real-world identities.

For face-to-face registration, the registrant is required to give a personal statement, which includes his/her full name, date and place of birth and current permanent address. At least one piece of reputable documentary evidence (e.g. passport) or third party corroboration (from a trustworthy source such as a bank or government department) is required in support.

Registration Level 2 – significant damage

Level 2 registration is appropriate for e-Government transactions in which significant damage might arise from misappropriation of real-world identity. In particular, misappropriation of a client's real-world identity at level 2 might result in at most:

- *significant inconvenience to any party; or*
- *no risk to any party's personal safety; or*
- *the release of personally or commercially sensitive data to third parties; or*
- *significant financial loss to any party; or*

- *significant damage to any party's standing or reputation; or*
- *significant distress being caused to any party; or*
- *assistance in the commission of or hindrance to the detection of serious crime.*

Personal statement as for level 1, including information that may be crosschecked against supplied documentary/third party evidence. In support are required one piece of documentary evidence that contains the registrant's signature and photograph (ideally a passport or National Identity Document) and one piece of evidence of activity in the community, such as a bank statement (two if the evidence of personal identity does not contain a photograph and signature). An item of third party corroboration may be substituted for one of the above pieces of evidence.

Registration Level 3 – substantial damage

Level 3 registration is appropriate for e-Government transactions in which substantial damage might arise from misappropriation of real-world identity. In particular, misappropriation of a client's real-world identity at level 3 might result in at most:

- *substantial inconvenience to any party; or*
- *risk to any party's personal safety; or*
- *the release of personally or commercially sensitive data to third parties; or*
- *substantial financial loss to any party; or*
- *substantial damage to any party's standing or reputation; or*
- *substantial distress being caused to any party; or*
- *assistance in the commission of or hindrance to the detection of serious crime.*

Personal statement is required as for level 2. In support are required at least one piece of documentary evidence of personal identity, two of activity in the community and third party corroboration of information asserted in the registrant's personal statement."

*"**Authentication Level 0 – minimal damage***

Level 0 authentication is appropriate for e-Government transactions in which minimal damage might arise from misappropriation of electronic identity, or no electronic identity is asserted. In particular, misappropriation of a client's credentials/electronic identity at level 0 might result in at most:

- *minimal inconvenience to any party; or*
- *no risk to any party's personal safety; or*
- *no release of personally or commercially sensitive data to third parties; or*
- *minimal financial loss to any party; or*
- *no damage to any party's standing or reputation; or*
- *no distress being caused to any party; or*
- *no assistance in the commission of or hindrance to the detection of serious crime.*

An authentication service is categorised as level 0 if no trust is put in the electronic identities asserted by the transacting parties, other than a presumption of correct operation of the underlying technology, or no electronic identity is asserted.

No authentication is required.

Access will only be permitted to publicly available information.

No management of client access is required, beyond overall technological limits on access.

Systems should be designed to prevent unauthorised access to username/password databases.

Authentication Level 1 – minor damage

Level 1 authentication is appropriate for e-Government transactions in which minor damage might arise from misappropriation of electronic identity In particular, misappropriation of a client's credentials/electronic identity at level 1 might result in at most:

- *minor inconvenience to any party; or*
- *no risk to any party's personal safety; or*
- *no release of personally or commercially sensitive data to third parties; or*
- *minor financial loss to any party; or*
- *minor damage to any party's standing or reputation; or*
- *minor distress being caused to any party; or*
- *no assistance in the commission of or hindrance to the detection of serious crime.*

Clients will authenticate themselves to the system by the presentation of a credential, which, at this level, can be a username. Clients will demonstrate their right to that credential by presenting additional (non-public) information (for example, a password) or biometric measure(s). The system will authenticate users based on the validity of this credential/private information combination.

Access is only permitted to publicly available information and information pertaining to the client that has been collected in transactions up to level 1 for which the client is enrolled, subject to the principlesof the Data Protection Act and the permitted use of the credential.

Mechanisms should be implemented to time-limit access to transactions based on a specific item of knowledge. For example, management of client access should ensure that passwords are periodically changed, and that client accounts are disabled after a defined period of disuse and/or after a specific date.

Systems should be designed to prevent unauthorised access to username/password databases.

Authentication Level 2 – significant damage

Level 2 authentication is appropriate for e-Government transactions in which significant damage might arise from misappropriation of electronic identity. In particular, misappropriation of a client's credentials/electronic identity at level 2 might result in at most:

- *significant inconvenience to any party; or*

- *no risk to any party's personal safety; or*
- *the release of personally or commercially sensitive data to third parties; or*
- *significant financial loss to any party; or*
- *significant damage to any party's standing or reputation; or*
- *significant distress being caused to any party; or*
- *assistance in the commission of or hindrance to the detection of serious crime.*

Clients will authenticate themselves to the system by the presentation of a credential (which will preferably be a digital certificate). Clients will demonstrate their right to that credential through the use of, in the case of digital certificates, a private key and using a password or biometric measure. The system will authenticate users based on validity of public key/private key pairs, and on the validity of the credential and supporting information.

Use of a username/password at level 2 is strongly deprecated owing to the significant degradation of the security provided, and only acceptable while widespread public key infrastructures are unavailable. If use of a username/password is allowed at level 2, a timescale for conversion to PKI methods must be specified.

Access is only permitted to publicly available information and information pertaining to the client that has been collected in transactions up to level 2 for which the client is enrolled, subject to the principles of the Data Protection Act and the permitted use of the credential.

Validity of the credential must be time-bounded. In addition, the revocation status of the credential must be checked at the time of the transaction.

Systems should be designed to prevent unauthorised access to username/password databases.

Authentication Level 3 – substantial damage

Level 3 authentication is appropriate for e-Government transactions in which substantial damage might arise from misappropriation of electronic identity. In particular, misappropriation of a client's credentials/electronic identity at level 3 might result in at most:

- *substantial inconvenience to any party; or*
- *risk to any party's personal safety; or*
- *the release of personally or commercially sensitive data to third parties; or*
- *substantial financial loss to any party; or*
- *substantial damage to any party's standing or reputation; or*
- *substantial distress being caused to any party; or*
- *assistance in the commission of or hindrance to the detection of serious crime.*

Clients will authenticate themselves to the system by the presentation of a digital certificate. This will be held in an access token, which would ideally be a smart card, token or mobile device. Clients will demonstrate their right to that credential through the use of a private key, and a password or biometric. The system will authenticate users based on the validity of public key/private key pairs, and on the validity of the credential.

Username/password combinations are not acceptable for level 3 authentication.

Access is permitted to publicly available information and information pertaining to the client that has been collected in transactions up to level 3 for which the client is enrolled, subject to the principles of the Data Protection Act and the permitted use of the credential.

Validity of the credential must be time-bounded, and the revocation status of the credential must be checked at the time of the transaction.

Systems should be designed to prevent unauthorised access to databases containing correct client verification information.

Validity of the credential must be time-bounded, and the revocation status of the credential must be checked at the time of the transaction.

Systems should be designed to prevent unauthorised access to databases containing correct client verification information."

The government's role lies in the definition of profiles for each registration level and for each authentication level, with separate profiles being defined for businesses and citizens (as in the Norwegian example above).

4.2.1.4.2 Technical authentication method linking

The United Kingdom authentication policy model allows the mapping of PKI based and non-PKI based authentication solutions.

Level0	Anonymous Username/password
Level1	Onetime password (paper list) Username/password
Level2	Soft crypto token Hard crypto token Mobile SMS onetime password (temporary) Onetime password (device token) (temporary) Onetime password/username/static password /temporary)
Level3	Hard crypto token

The UK approach is built to focus on both the used authentication method and the underlying registration process. As a result, the level of the specified token might change depending on the level of the registration. The table above is drafted based on the authentication levels as defined in the abstract descriptions in section 3.4.; the effect of the possible registration level is not included.

4.2.1.4.3 Scope and potential for cross border generalisation

The UK approach is interesting because it recognises that applications may be more or less demanding with regard to registration than to authentication. This allows for a more fine grained approach (although the resulting levels are less easily comparable to policies which do not make this distinction).

A second major strength is that the policy is highly goal-oriented, and leaves specific implementation details open to be defined by the application owner on a case by case basis. The requirements have been defined also with non-PKI solutions in mind. Because of this principal neutrality, the approach is more easily transposable to a European level than similar policies which are mainly or exclusively PKI oriented, such as the ones mentioned above.

However, this technological neutrality and room for appreciation and policy choices by application owners can also be perceived as a weakness, especially on a cross border scale, since this does to some extent diminish the harmonising effect of the definitions.

4.2.1.5 Germany

4.2.1.5.1 Description

While no formal authentication policy exists in Germany (due in part due to the current state of transformation of the identity infrastructure), a draft proposal has none the less been presented based on a five tiered distinction. This draft document is analysed below, on account of its potential future impact. The criteria for distinguishing between the levels should be based on:

- The quality and confidence within the enrolment / registration process for the underlying data for authentication;
- The authentication mechanism itself within a business application process where two partners (e.g. a natural person and a client software application) communicate (e.g. PIN/TAN procedure)
- The integrity and confidentiality within the whole data transfer process between the two authentication partners during the authentication (e.g. encryption via https to prevent man-in-the-middle attack)

The following draft criteria have been presented:

"Levels of Quality of the Underlying Data for Authentication

Level	Registration quality
Level 0: No	• No registration
Level 1: Weak	• Customer himself; registration of identity attributes or registration by a registration authority without a defined security level
Level 2: Medium	• Providing identity attributes based on a personal document issued by a third party with a defined security level
Level 3: Strong	• Personal registration based on an official ID document at a third party with a warranted or legally guaranteed security level
Level 4: Very strong	• Appearance in person and providing of an official ID document at an agency, which is the registration authority for government purposes

Trusted Access-Levels for Authentication Mechanism

Level	Registration quality
Level 0: No	• No authentication activities
Level 1: Weak	• Submitting of an identifier or identity attributes without check for correctness • Use of an identifier for authorised organisations

	• Use of a shared secret
Level 2: Medium	• PIN (Personal Identity Number) • PIN/TAN (Transaction Authentication Number) • Software token
Level 3: Strong	• Hardware token with PKI functions
Level 4: Very strong	• Hardware token with PKI functions – provider has to be accredited by government authorities • Biometrics – provider has to be accredited by government authorities

Levels of Integrity and Confidentiality within the Data Transfer Process during Authentication

Level	Registration quality
Level 0: No	• No technical or organisational security procedures in place
Level 1: Weak	• Use of standard software products for authentication and encryption • Technical and organisational procedures implemented by the provider and encryption of the data transfer by the authentication partner
Level 2: Medium	• Integrity secured by an electronic signature (the private key lies in a software token of the authentication sender) and secured channel encrypted based on a PKI certificate (the private key lies in a software token of the authentication receiver).
Level 3: Strong	• Integrity secured by an electronic signature (the private key lies in a hardware token of the authentication sender) and secured channel encrypted based on a PKI certificate (the private key lies in a hardware token of the authentication receiver).
Level 4: Very strong	• Integrity secured by a qualified electronic signature (the private key lies in a hardware token of the authentication sender) and secured channel encrypted based on a PKI certificate (the private key lies in a hardware token of the authentication receiver) and PKI provider has to be accredited by governmental authorities.

A complete authentication model can be created by combining the requirements above (e.g. level 1 authentication would show all the qualities defined as level 1 above).

This results in the following overview:

Level	Registration data quality	Authentication mechanism	Data transfer security

Level 0: No	No registration	No authentication	No security
Level 1: Weak	Self registration	Use of a shared secret	Standard security procedures delivered by the provider
Level 2: Medium	Registration with a credential by a third party	PIN (/TAN) software token	Software token
Level 3: Strong	Personal registration with a warranted security level	Hardware token with PKI functions	Hardware token
Level 4: Very strong	Appearance in person and registration by governmental authority	Hardware token with PKI functions / Biometrics + provider has to be accredited by governmental authority	Hardware token + provider has to be accredited by a governmental authority

4.2.1.5.2 Technical authentication method linking

The German authentication policy model allows the mapping of PKI based and non-PKI based authentication solutions.

Level 0 - No	Anonymous
Level 1 - Weak	Username/password
Level 2 - Medium	OTP paper list and static username Mobile SMS onetime password Onetime password (device token) Onetime password/username/static password Soft crypto token
Level 3- Strong	Hard crypto token
Level 4 – Very Strong	Hard crypto token (qualified)

The table above shows that the German approach is generally well defined in all token levels. The table also shows that two of the highest levels are only available by using hard crypto tokens.

4.2.1.5.3 Scope and potential for cross border generalisation

The German approach shows potential for generalisation through the definition of abstract criteria which only depend on PKI solutions at the highest levels, which corresponds with common practices

in a number of countries, and which could be easier to apply universally than similar proposals which assume exclusive use of PKI solutions.

It should also be noted that the policy is only a draft paper in its current state, and that it therefore is subject to change.

4.2.2 Informally adopted policies

As noted above, eleven countries have informally adopted authentication policies (i.e. have a policy which can be deduced from administrative practices or which are occasionally quoted, but without any formal government support or impact in practice). These shall be examined in greater detail in this section.

4.2.2.1 Belgium

4.2.2.1.1 General description

There is no official authentication policy in Belgium that defines a strict hierarchy of the different authentication systems in use. However, unofficial declarations[16] show that there is a certain hierarchy which functions as a theoretical model for assessing authentication requirements. With regard to natural persons, the following hierarchy is occasionally presented[17]:

Level	Registration citizen identity	Authentication citizen identity	Applications
0	None	None	Public information and services
1	On line by entering the national register number, identity card number and SIS card number	By assigned user number in combination with a password chosen by the user	Information/services of limited sensitivity
2	Level 1 + send-out of a confirmation e-mail with activation URL to an address indicated by the citizen, and send-out of a paper token to the registered address noted in the National Register	Level 1 + entering one random letter sequence mentioned on the token (which contains 24 sequences)	Information/services of average sensitivity
3	Physical identification at the commune for the acquisition of an eID	Authentication certificate on the eID + session based password	Information/services of high sensitivity
4	Physical identification at the commune for the acquisition of an eID	Authentication certificate on the eID + signature certificate on the eID + password per transaction	Services requiring an electronic signature

[16] See e.g. the following presentation (in Dutch): http://www.law.kuleuven.ac.be/icri/frobben/presentations/20061108.ppt

[17] Translated from the original Dutch presentation referred to directly above, slide 10.

Thus, there are four levels of authentication above public access: basic username/password (after registration using official register numbers), use of the federal token (a paper card containing 24 random strings for use in a two factor login system), use of the eID card's authentication, and use of the eID card's signature and authentication.

It should be noted that, since the token will be phased out, in the future the eID will become the main tool for authentication.

While a sound national approach, the potential for generalisation is limited because the hierarchy is strictly tied to the Belgian system of authentication tokens.

4.2.2.1.2 Technical authentication method linking

The Belgian authentication policy model allows the mapping of PKI based and non-PKI based authentication solutions. It should be noted that, because of the national approach to the authentication policy, several defined authentication tokens are missing in the policy. None the less a proposal for the mapping of these missing authentication tokens can still be made, because of the clear separation from non-PKI based tokens to PKI based tokens (from level 2 to level 3).

Level 0	Anonymous
Level 1	Username/password
Level 2[18]	OTP paper list and static username Mobile SMS onetime password Onetime password (device token) Onetime password/username/static password Soft crypto token
Level 3	Hard crypto token (Authentication certificate on eID smartcard)
Level 4	Hard crypto token (Authentication and signature certificates on eID smartcard + additional password for each transaction.).

The table above shows that the Belgian approach is generally well defined in all token levels. The table also shows that two of the highest levels are only available by using hard crypto tokens. The Belgium approach can be seen as quite similar to the German approach described above. This conclusion is of course possible only when missing authentication tokens are added to the policy model.

[18] In the Belgian approach only a paper token is originally defined at this level.

4.2.2.2 Finland

4.2.2.2.1 General description

There is no official authentication policy in Finland that defines a strict hierarchy of the different authentication systems in use. However, there is a certain hierarchy deductible from the requirements of legally binding digital signatures, which functions as a theoretical model for assessing authentication requirements. With regard to natural persons, the following hierarchy can be drawn:

Level	Registration citizen identity	Authentication citizen identity	Applications
0	None	None	Public information and services
1	On line registration using address, GSM or SSN number as ID.	By assigned user number in combination with a password chosen by the user	Information/services of limited sensitivity
2	Level 1 + send-out of a confirmation e-mail with activation URL to an address indicated by the citizen, or SMS.	Level 1 + standard challenge-response authentication method	Information/services of average sensitivity
3	Physical identification at the bank for the acquisition of TUPAS credentials	TUPAS authentication certificate	Information/services of high sensitivity and requiring non-qualified electronic signature
4	Physical identification at the police station (LRA) for the acquisition of an eID	Authentication certificate on the eID + signature certificate on the eID + password per transaction	Services requiring a qualified electronic signature

Thus, there are four levels of authentication above public access: basic username/password, use of an SMS with challenge-response, use of the TUPAS authentication, and use of the FINEID card's signature and authentication.

The VETUMA authentication service is designed to support SMS challenge-response authentication (without certificates) but this is not used in any existing applications yet.

While a sound national approach, the potential for generalisation is limited because the hierarchy is strictly tied to the Finnish system of authentication tokens.

4.2.2.2.2 Technical authentication method linking

The Finnish authentication policy model allows the mapping of PKI based and non-PKI based authentication solutions. It should be noted that, because of the national approach to the authentication policy, several defined authentication tokens are missing in the policy. None the less a proposal for the mapping of these missing authentication tokens can still be made, because of the clear separation from non-PKI based tokens to PKI based tokens (from level 2 to level 3).

Level 0	Anonymous
Level 1	Username/password
Level 2	Mobile SMS onetime password Onetime password (device token) Soft crypto token
Level 3	OTP paper list and static username Onetime password/username/static password
Level 4	Hard crypto token

The table above shows that the Finnish approach is generally well suited for all token levels. It should also be noted that because of the national approach to authentication tokens the table seems to differ from the other surveyed countries token linkings, since the 3rd level only allows TUPAS (onetime password list), thus this seems strange when other similar tokens are located in level 2[19].

[19] Other OTP based authentication methods are not listed in the Finnish authentication policy, but the decision was made to link these to the second level, because at level 3 only the national solution TUPAS is allowed.

4.2.2.3 Greece

4.2.2.3.1 General description

There is no official authentication policy in Greece that defines a hierarchy of the different authentication systems in use. However, from existing applications we can deduce a formal hierarchy for authentication:

Level	Registration citizen identity	Authentication citizen identity	Applications
0	None	None	Public information and services
1	On line by entering the identity card number and other personal data + send-out of a confirmation e-mail with activation to an e-mail address indicated by the citizen	By assigned user number in combination with a password chosen by the user	Information/services of average sensitivity
2	Physical identification at the Syzefxis contractors	Authentication certificate on the smart card	Services requiring an electronic signature

Thus, there are two level of authentication above public access: basic username/password (after registration using official register numbers) and use of the smart card's signature and authentication.

It is expected, however, in the future, that a large lumber of authentication systems will be based on electronic signatures.

While a sound national approach, the potential for generalisation is limited because the hierarchy is strictly tied to the Greek system of authentication tokens.

4.2.2.3.2 Technical authentication method linking

The Greek authentication policy model allows the linking of PKI based and non-PKI based authentication solutions.

Level 0	Anonymous

Level 1[20]	Username/password OTP paper list and static username Onetime password/username/static password Mobile SMS onetime password Onetime password (device token) Soft crypto token
Level 2	Hard crypto token

The table above shows that the Greek approach is generally well defined in all token levels. This conclusion is of course only possible when missing authentication tokens are added to the policy model.

4.2.2.4 Hungary

4.2.2.4.1 General description

There is no official authentication policy in Hungary that defines a strict hierarchy of the different authentication systems in use. However, there are some documents preparing the decision making connected with a four level authentication[21]. The principle does not differ basically from internationally accepted practices as illustrated above. Considering that the documents are not final yet, the potential for generalisation is limited.

4.2.2.4.2 Technical authentication method linking

Because there is no official authentication policy in Hungary that defines a strict hierarchy of the different authentication systems in use, the creation of linking table is not possible.

[20] Only the user number in combination with a password chosen by the user is defined in the original Greek authentication policy; other classifications are decisions based on only possible location.

[21] E.g.: IHM 7147/2003 Az elektronikus aláírás közigazgatási alkalmazásának programja December 2003.

4.2.2.5 Malta

4.2.2.5.1 General description

Maltese authentication plans revolve around a four tier system:

- Level 0: no authentication
- Level 1: restricted authentication (login, password and PIN);
- Level 2: confidential authentication (digital certificate);
- Level 3: maximum authentication (qualified digital certificate).

However, there is no explicit policy document stating formal criteria for these levels, and only Level 1 is currently deployed.

4.2.2.5.2 Technical authentication method linking

The Maltese authentication policy model is still only at the planning stage, but based on the information available the following table can be presented.

Level 0 – no authentication	Anonymous
Level 1 – restricted authentication	Username/password OTP paper list and static username Onetime password/username/static password Mobile SMS onetime password Onetime password (device token)
Level 2 – confidential authentication	Soft crypto token Hard crypto token
Level 3 – maximum authentication	Hard crypto token (qualified)

The table above shows that the Maltese approach is generally well defined in all token levels. The table also shows that two of the highest levels are only available by using hard crypto tokens. The Maltese approach seems to be following a similar pattern to the German and Belgian approaches.

4.2.2.6 The Netherlands

4.2.2.6.1 General description

An informal two tier system can be deduced, the first based on the DigiD username/password system; the second using the future eID card ENIK as a PKI device. The potential for generalisation is limited because the hierarchy is strictly tied to the Dutch system of authentication mechanisms.

4.2.2.6.2 Technical authentication method linking

The Dutch authentication policy is strictly tied to the Dutch system of authentication tokens and because of this creation of the linking table is not possible.

4.2.2.7 Poland

4.2.2.7.1 General description

In Poland there is no official authentication policy. However the e-PUAP[22] project which is currently under development includes aspects of identification, authentication and authorization of citizens.

As a part of this project, four authentication methods are considered in an official document „*The security rules for ePUAP – WKP*"[23] (ver. 1.02, from August, 23th, 2006), ordered by the Ministry of Home Affairs and prepared by the Infovide company:

1. authentication with return channel – a mechanism enabling to set the channel for the reception of an information placement confirmation; such a channel does not introduce specific security mechanisms;
2. authentication with static password – an information containing an identifier and password;
3. authentication with one-time password – a user sends his/her identifier and two-part password to the system (an appropriate sequence of characters is generated by the token; additionally PIN of the user is used);
4. authentication with strong cryptographic support – based on an assumption that the person using a private key associated with a certificated public key is probably that one which is clearly mentioned in the public key certificate (in website login or electronic signature

[22] The Abbreviation e-PUAP means integrated information platform (central, regional and local portals) supporting the provision of electronic public services for administration, citizens and business (front-office); see also http://www.e-puap.mswia.gov.pl.

[23] http://www.infovidematrix.pl

procedures); an authentication can be supported by smart cards with appropriate cryptographic functionalities.

The table below shows the resulting proposed profiles:

User type	No authentication	Return channel identification	Static password authentication	One-time password authentication	Cryptographic authentication
Users with access to public information	X				
Users with one-time access		X			
Users with permanent access			X	X	X
Administrators			X	X	X

However, all of the information above is provisional and in a draft stage only.

The approach is interesting because of the distinction between user types. However, as this approach is rarely found in other authentication policies, generalisation seems problematic.

4.2.2.7.2 Technical authentication method linking

The Polish authentication policy model allows the linking of PKI based and non-PKI based authentication solutions.

Level 0 – No authentication	Anonymous
Level 1 – Return channel authentication	Anonymous (user access is provided with return channel link to eGovernment service)
Level 2 – Static password authentication	Password/username
Level 3 – One-time password authentication	OTP paper list and static username Onetime password/username/static password

	Mobile SMS onetime password Onetime password (device token)
Level 4 – Cryptographic authentication	Soft crypto token Hard crypto token

The table above shows that the Polish approach is generally well defined in all token levels. This conclusion is of course only possible when missing authentication tokens are added to the policy model.

4.2.2.8 Slovakia

4.2.2.8.1 General description

With regard to authorisation management, there is no generic policy or infrastructure in place yet. A few ad hoc solutions exist, that use one of 3 kinds of authentication/identification in a loosely hierarchical structure:

- *Basic user name and password*

In general, this kind of eIDM system is introduced in the eTendering application managed by the Public Procurement Office. Currently the system is openly accessible to anyone, and merely requires on-line registration. After registration the system is accessible to anyone, also for non-nationals. After the registration, the user receives his software certificate and password via e-mail. After this registration process the user can communicate with a public body using the requested identifier/password and software certificate.

- *Qualified certificates and prior personal identification*

The primary requirement is to have a valid qualified certificate. If the qualified certificate does not contain a unique identifier (which is currently typically the case because there is no unique identifier in place), its holder is not sufficiently identified for communication with public administrations. That is the reason why the user first has to come in person to the public administration body which provides the system/application, in order to verify the personal data of the certificate holder. During this registration process, the identity of a user is proven by using conventional identity cards which is matched with the serial number of qualified certificate. This is the way in which the eTax system, eServices of Commercial Register and several other eGovernment applications operate.

- *Qualified certificate with unique identifier*

When using this method of authentication, the person has to fill in a form containing his personal data which he/she then signs by qualified electronic signature. Its private key is stored in a secure signature creation device. The provider of an eIDM system verifies if the data in the form corresponds to the data in a qualified certificate issued by an accredited CSP (this can be done automatically or manually). If the person fills the form with incorrect identification data, this is considered an attempt to fraud and the person is responsible for it.

While the structure is more of a ranking of existing authentication solutions than a true authentication policy, the basic structure contains elements which are transposable to a broader context (in particular the signing of registration forms using trusted qualified certificates).

4.2.2.8.2 Technical authentication method linking

In Slovakia there is no generic policy or infrastructure in place yet. Creation of the linking table is not possible.

4.2.2.9 Slovenia

4.2.2.9.1 General description

There is no official authentication policy in Slovenia that defines a strict hierarchy of the different authentication systems in use. However, with regard to natural persons, four levels of authentication can be deduced:

- no authentication for public information and services
- on line by entering the personal data to register (user chooses his password and username) identity and then for authentication by assigned user number in combination with a password chosen by the user
- basic username/password (after registration using official register numbers),
- use of qualified certificates for signature and authentication.

This results in the following overview:

Level	Registration citizen identity	Authentication citizen identity	Applications
0	None	None	Public information and services
1	On line by entering personal data	By personal data entered on line	Information/services of limited sensitivity

2	Level 1 + send-out of a confirmation e-mail with username, initial password and activation URL to an address indicated by the citizen	By assigned combination of a username and password chosen by the user	Information/services of medium sensitivity
3	Physical identification at the registration authority for the acquisition of qualified certificate	Authentication/signature certificate + password	Information/services of high sensitivity and services requiring an electronic signature

While a sound national approach, the potential for generalisation is limited because the hierarchy is strictly tied to the Slovene system of authentication.

4.2.2.9.2 Technical authentication method linking

The Slovenian authentication policy model enables the linking of PKI based and non-PKI based authentication solutions.

Level 0	Anonymous
Level 1	Password/username
Level 2	Password/username (after registration using official register numbers) OTP paper list and static username Onetime password/username/static password Mobile SMS onetime password Onetime password (device token)
Level 3	Soft crypto token Hard crypto token

The table above shows that the Slovenian approach is generally well defined in all token levels. The Slovenian model is technically mostly built upon using either password/username or PKI certificates to authenticate. Using the clear separation from level 2 to level 3 based on certificates it is easy to map all non existing token models to level 2.

4.2.2.10 Spain

4.2.2.10.1 General description

There is no defined authentication policy in Spain that establishes a hierarchy between the existing authentication systems. However, in practice there is a certain hierarchy among them, fundamentally based on the sensitivity of the information which is accessed and in the security measures that each one of the authentication systems implies.

The following chart summarises this hierarchy with a number of examples:

Level	Citizen's Identity	**Citizen's Authentication**	Applications
0	None	None	Specific public services such as the downloading of forms for tax declarations
1	Online, introducing an identity number, fundamentally the ID card number (DNI) or tax identification number (NIF)	Authentication takes place inserting a user name and a password	Specific public or private services of relative importance such as e-mail services or specific requests, like the draft of the tax declaration
2	Includes level 1 and delivery of an e-mail with a URL activation or the delivery of a letter to the users address containing the data necessary to activate the service	Includes level 1 and the introduction of an random and changing combination of letters or numbers	Services of much importance that require a greater security degree such as, for example, banking services
3	Physical and in presence identity is required to obtain the user's certificate	Authentication based on the user's certificate	Highly confidential and very personal services such as access to personal information stored by the Administration: work resume, medical history

While a sound national approach, the potential for generalisation is limited because the hierarchy is strictly tied to the Spanish system of authentication.

4.2.2.10.2 Technical authentication method linking

The Spanish authentication policy model enables the linking of the PKI based and the non-PKI based authentication solutions.

Level 0	Anonymous
Level 1	Password/username
Level 2	OTP paper list and static username Onetime password/username/static password Mobile SMS onetime password Onetime password (device token)
Level 3	Hard crypto token Soft crypto token

The table above shows that the Spanish approach is generally well defined in all token levels. All recognized authentication token models are already listed in the Spanish approach.

4.2.2.11 Turkey

4.2.2.11.1 General description

The Turkish administrations are currently developing the eGovernment Gateway, in which natural persons will be able to use 4 levels for authentication purposes:

Level	Registration citizen Identity	Authentication citizen Identity	Applications
0	None	None	Public information and services
1	On line by entering the national register number, and personal information	By assigned user number in combination with a password chosen by the user	Information/services of limited sensitivity

2	Level 1 + a confirmation message that implies the USER LICENSE and send-out of an ENVELOPE with a PASSWORD to the address specified by citizens and may be checked with the one in the National Register	Level 1 + entering PASSWORD mentioned on the ENVELOPE (which contains a number of sequences)	Information/services of average sensitivity
3	Physical identification at the commune for the acquisition of a qualified eSignature.	Authentication certificate on the eSignature + signature certificate on the eSignature + password per transaction	Services requiring an electronic signature

Thus, there are three levels of authentication above public access: basic username/password (after registration using official register numbers), use of a password printed and enclosed securely in an envelope which is then delivered by the PTT (the governmental institution legally authorized to serve official communications); and use of the eSignature card's signature and authentication.

While a sound national approach, the potential for generalisation is limited because the hierarchy is strictly tied to the Turkish system of authentication.

4.2.2.11.2 Technical authentication method linking

The Turkish authentication policy model enables the linking of PKI based and non-PKI based authentication solutions.

Level 0	Anonymous
Level 1	Password/username
Level 2	OTP paper list and static username Onetime password/username/static password Mobile SMS onetime password Onetime password (device token)
Level 3	Soft crypto token Hard crypto token

The table above shows that the Turkish approach is generally well defined in all token levels. The level 2 authentication model relies on passwords; it is then strengthened by sending a confirmation letter which makes it possible to validate authorization. Thus using the clear separation between level 2 to level 3 based on certificates it is easy to map all non existing token models to level 2.

5 Influential authentication policies outside of the surveyed countries

Apart from the authentication policies in the surveyed countries summarised above, there are a number of other relevant initiatives in this field, including specifically the U.S. E-Authentication Policy for Federal Agencies, and the IDABC Authentication Policy. Similar to the approach above, these authentication policies will be described in the sections below.

5.1 Noneuropean national authentication policies

5.1.1 U.S.A. E-Authentication Policy for Federal Agencies

5.1.1.1.1 Description

The General Services Administration published an RFC regarding a draft E-Authentication Policy for Federal Agencies on 11 July 2003[24], describing a technology neutral authentication policy for authentication solutions in U.S. federal agencies, and providing these agencies with certain guidelines for choosing an appropriate authentication level.

The policy describes four profiles, based on the certainty needs of the applications and on the scope of risks in case of abuse:

> *"**2.3. Assurance Levels: Descriptions and Examples***
>
> *This section describes the four assurance levels. The levels represent ranges of confidence in an electronic identity presented to an agency by means of a credential. The levels are numbered from 1 to 4, with 1 being minimal assurance and 4 being the highest level of identity assurance.*
>
> *For each level, there is a description and examples. The description and examples will assist the agency in identifying the appropriate level of assurance required to authorize a transaction. The key part of each description is a risk profile. This is a description of certain consequential risks that may ensue to participants in a transaction when there is an authentication error.*
>
> ***Level 1—Minimal Assurance***
>
> *At level 1, little or no assurance is placed in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 1 might result in at most:*
>
> *• Minimal inconvenience to any party; and*
>
> *• No financial loss to any party; and*

[24] See http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-17634.pdf

• Minimal distress being caused to any party; and

• Minimal damage to any party's standing or reputation; and

• No risk of harm to agency programs or other public interests; and

• No risk of civil or criminal violations; and

• No release of personal, U.S. government sensitive, or commercially sensitive data to unauthorized parties; and

• No risk to any party's personal safety.

[...]

Level 2—Low Assurance

Level 2 is appropriate for transactions in which it is sufficient that, on the balance of probabilities, there is confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 2 might result in:

• Minor inconvenience to any party; or

• Minor financial loss to any party; or

• Minor damage to any party's standing or reputation; or

• Minor distress being caused to any party; or

• Minor risk of harm to agency programs or other public interests; or

• A risk of civil or criminal violations of a nature that would not ordinarily be subject to agency enforcement efforts; or

• A minor release of personal, or commercially sensitive data to unauthorized parties; and

• No release of U.S. government sensitive data to unauthorized parties; and

• No risk to any party's personal safety.

[...]

Level 3—Substantial Assurance

Level 3 is appropriate for transactions that are official in nature, and for which there is a need for high confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 3 might result in:

• Significant inconvenience to any party;or

• Significant financial loss to any party; or

• Significant damage to any party's standing or reputation; or

• Significant distress being caused to any party; or

• Significant harm to agency programs or other public interests; or

• A risk of civil or criminal violations that may be subject to agency enforcement efforts; or

• A significant release of personal, U.S. government sensitive, or commercially sensitive data to unauthorized parties; and

• No risk to any party's personal safety.

[...]

Level 4—High Assurance

Level 4 is appropriate for transactions that are official in nature for which there is a need for very high confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at level 4 might result in:

• Considerable inconvenience to any party; or

• Considerable financial loss to any party; or

• Considerable damage to any party's standing or reputation; or

• Considerable distress being caused to any party; or

• Considerable harm to agency programs or other public interests; or

• A risk of civil or criminal violations that are of special importance to the agency enforcement program; or

• A damaging release of extensive personal, U.S. government sensitive, or commercially sensitive data to third parties; or

• A risk to any party's personal safety."

As such, the document is thus quite useful for the assessment of risks in authentication mechanisms, but is less focused on presenting tangible requirements for meeting the needs of these risk levels.

5.1.1.1.2 Scope and potential for cross border generalisation

As noted above, the E-Authentication policy should rather be considered as a authentication risk assessment policy, and in this function it is quite useful. However, as an authentication policy per se, it offers insufficient guidelines for the choice of specific authentication solutions.

The NIST Electronic Authentication Guideline discussed directly below is more concrete in this regard.

5.1.2 NIST Electronic Authentication Guideline

5.1.2.1.1 Description

The NIST (National Institute for Standards and Technology) has published its Electronic Authentication Guidelines in April 2006[25], following the publication of the Federal Information Security Management Act (FISMA) of 2002. While the guideline was prepared for use by U.S. federal agencies, its provisions are sufficiently universal to be applied outside of this context. The document defines technical requirements for four levels of assurance in the areas of identity proofing, registration, tokens, authentication protocols and related assertions.

In particular, the document states specific technical requirements for each of the four levels of assurance in the following areas:

- Tokens (typically a cryptographic key or password) for proving identity;
- Identity proofing, registration and the delivery of credentials which bind an identity to a token;
- Remote authentication mechanisms, that is the combination of credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be; and
- Assertion mechanisms used to communicate the results of a remote authentication to other parties.

The technical requirements for each of the four levels are summarised as follows:

> *"**Level 1***
>
> *Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3, or 4. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.*
>
> *Plaintext passwords or secrets are not transmitted across a network at Level 1. However this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. In many cases an eavesdropper, having intercepted such a protocol exchange, will be able to find the password with a straightforward dictionary attack.*
>
> *At Level 1, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.*
>
> ***Level 2***
>
> *Level 2 provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A*

[25] See http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 3

Level 3 provides multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: "soft" cryptographic tokens, "hard" cryptographic tokens and "one-time password" device tokens.

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 4

Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only "hard" cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. The protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks are prevented. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session

(temporary) shared secrets may be provided to independent verifiers by the CSP. Strong Approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process."

More detailed guidelines are also contained in the document with regard to registration requirements, token levels and authentication mechanism requirements, although there is no clear mapping of these requirements to the levels defined above.

5.1.2.1.2 Scope and potential for cross border generalisation

The NIST Electronic Authentication Guideline is fairly detailed and contains very useful inputs on most aspects of authentication management. It has the added benefit over the solutions presented in section 4 of being written with cross border user in mind. For these reasons, the document can provide instrumental inputs to the creation of a similar European document.

However, as noted above, the mapping of specific requirements (such as registration and tokens) to specific security levels may have to be made somewhat more rigid, especially given the large variety of electronic authentication solutions in Europe and the existing national authentication policies.

5.2 Non-country specific authentication policies – IDABC Authentication Policy

Finally, this section will take a closer look at the IDABC Authentication Policy, as an example of an authentication policy which was drafted as a non-country specific document, and which has the added benefit of being drafted from a European perspective, albeit for use in IDABC sectoral networks.

5.2.1 Description[26]

The IDABC Authentication Policy Document was published[27] in July 2004 and contains a series of recommendations and guiding principles for the establishment of appropriate authentication mechanisms for the participants (member state administrations and EU institutions) in IDABC sectoral networks. It aims at providing an instrument that helps managers of IDABC sectoral networks and horizontal security-related projects to assess and establish appropriate authentication mechanisms for their projects.

Principally, the document contains a methodology to develop a customised authentication policy which suggests the use of the following steps:

- Step 1: Conduct a rapid risk assessment of the sectoral application or network.
- Step 2: Map Identified risks to the applicable Authentication Assurance level.
- Step 3: Select procedures and technology.
- Step 4: Sign a Mutual Recognition Agreement.
- Step 5: Validate that the implemented system has achieved the required assurance level.
- Step 6: Periodically reassess the system to determine technology refresh requirements.

It also includes suggestions for the distribution of responsibilities for the registration and electronic authentication phases of the authentication process of a given sectoral project between the Commission, the relevant member state administration and, when applicable, a third party.

The document foresees a Certificate Practise Statement that describes different policies for the four levels of assurance defined –Minimal, Low, Substantial and High. These policies relate to both, registration and electronic authentication phases, as well as to the choice of token type and authentication protocol for each level of assurance.

In order to facilitate the application of the suggested methodology and in particular of the above mentioned steps, the IDA(BC) Authentication Policy Document provides in an Annex, an Authentication Policy Framework that contains a number of important elements, such as how to define and select the appropriate assurance levels - and the available procedures and technologies for achieving the registration and electronic authentication per level, including token types (hard

[26] Source: http://ec.europa.eu/idabc/en/document/3519/5927

[27] See http://ec.europa.eu/idabc/en/document/3532/5585

crypto token, soft crypto token, one-time password, PIN) and authentication protocols (private key, symmetric key, tunnelled password).

5.2.2 Scope and potential for cross border generalisation

The IDABC Authentication policy is ideally suited as a starting point for the definition of a common European authentication policy, as it is technology neutral (i.e. it allows but does not assume the use of PKI), contains all of the common elements seen in the policies above (including the definition of risk and damage levels, token types, registration procedures, and authentication processes), and has pre-defined high level 'Common Practice Statements' for each of the four identified authentication levels.

Because of this, the Authentication policy appears to be compatible with most of the approaches above, and will likely only require moderate updates or modifications.

6 Conclusions and findings

While specific recommendations will be included in future deliverables within this project, a number of provisional conclusions can none the less be identified based on the overviews above.

6.1 General lessons

While the overview above has shown that the availability of European national authentication policies vary from country to country, it is clear that an increasing number of countries are recognising the importance of this issue through the definition of authentication policies. Four countries have officially adopted authentication policies, with the French, Norwegian and UK policies in particular showing elements that could prove useful and beneficial for the definition of a common authentication policy. Countries where such policies are informal and implicit (i.e. can only be derived from administrative practices) are less instructive in this regard, as their policies are generally only classifications/rankings of existing authentication solutions and contain no specific criteria or definitions that can be generalised.

Outside of these European national policies, the IDABC Authentication policies and NIST Guidelines have shown to be highly informative and suitable for the creation of a broader European consensus.

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

- The availability of risk assessment criteria, typically combined with a consideration of potential damage in case of incidents;
- The definition of registration requirements for the issuing of tokens or credentials; and
- The definition of authentication requirements for the use of such tokens or credentials.

Apart from these common elements, a number of policies also define additional elements which should be given due consideration, such as:

- token requirements, e.g. by the definition of token levels as in the NIST Guidelines; often such requirements are implicitly or explicitly included in the general authentication requirements;
- a distinction between natural persons and legal entities (such as in the Norwegian example).

6.2 Key policies

With a view of drafting the next deliverable in this study (specifically D4.2., a proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms), the following policies described in this document seem most suitable as inputs for a general European multilevel authentication approach:

- The IDABC Authentication policy should be the starting point, 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 can be useful to provide some further input for the elaboration of the European mechanism, if required;
- Several of the national policies can be 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 can be highly instructive in this regard.