Prepared for the eGovernment Unit
DG Information Society and Media
European Commission

Modinis
Study on Identity Management in eGovernment

Common Terminological Framework for Interoperable Electronic Identity Management

Consultation paper

v2.01
November 23, 2005

1. Introduction

This short document attempts to provide a common terminological framework for interoperable identity management in eGovernment. This was identified as a key issue that needs to be resolved during the first Modinis^{IDM} Workshop of 4 May 2005 in Leuven; a position which was subsequently supported by the eEurope eGovernment subgroup – Ad hoc group on Identification and Authentication. The initial version was largely written between July 6-15, 2005 by the partners of the MODINIS Study on Identity Management in eGovernment (K.U.Leuven, A-SIT and Lawfort). The document has subsequently been updated, based on feedback from Prime, Belgian Federal ICT Ministry and several Member States representatives.

The terms in this terminology paper have been influenced by the following consulted source materials:

- The final report of the first Modinis^{IDM} Workshop of 4 May 2005 in Leuven, including the presentations of Frank Robben and Reinhard Posch.
- The presentations given during the meeting of the eEurope eGovernment subgroup – Ad hoc group on Identification and Authentication on 30 June 2005 in Brussels, by Reinhard Posch and the Modinis^{IDM} Study Team (represented by Hans Graux)
- FIDIS D 2.1: Inventory of topics and clusters (and the corresponding WIKI page: http://internal.fidis.net/178.0.html?tx_a1wiki_pi1[keyword]=t2.1%20definition
- PRIME D 14.1.a: Framework V1 (http://www.prime-project.eu.org/public/prime_products/deliverables/fmwk/pub_del_D14.1.a_ec_wp14.1_V4_final.pdf)
- Lia Borthwick: Towards an Open Architecture for European eGovernment Identity Management (http://istrg.som.surrey.ac.uk/projects/guide/files/eChallenges_2004_Paper.doc)
- APES D 4: General report of the legal issues (2003, https://www.cosic.esat.kuleuven.ac.be/apes/docs/APES_d4.doc.gz)
- Alfred J. Menezes/ Paul C van Oorschot/ Scott A. Vanstone, Handbook of applied cryptography, CRC Press, 1996, downloadable at: http://www.cacr.math.uwaterloo.ca/hac/
- ISO/IEC 1st WD 24742: 2005-01-10
- ISO/IEC 21827: 2002-10-01
- ISO/IEC 11770-2: 1996-04-15
- ISO/IEC 15945: 2002-02-01
- ISO IS 15408
- ISO/IEC 15408-2:1999
- ISO/IEC 2nd FCD 18033-2: 2004-12-06
- ISO/IEC 9798-6:2005(E)
- FIDIS D 3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems"
- Regulating a European eID – A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID for the Porvoo e-ID Group by Thomas Myhr
- The Laws of Identity, Kim Cameron, Architect of Identity, Microsoft (http://www.identityblog.com)
- The definitions list of the Dutch government, available through https://www.pkioverheid.nl
- Austrian E-Government Act, Federal Act on Provisions Facilitating Electronic Communications with Public Bodies, Austrian Federal Law Gazette, Part I, No. 10/2004
- Stephen T. Kent / Lynette I. Millett: Who Goes There? Authentication Through the Lens of Privacy. The National Academies Press, 2003, downloadable at http://books.nap.edu/html/whogoes/index.html
- Liberty Technical Glossary, version 1.4 – Liberty Alliance Project
- Lexicon of the Center for Internet Society at Harvard Law School, http://www.identitygang.org/Lexicon
- The SAML glossary 2.0-os available at http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

- The identity management related terms defined by the Open Privacy Initiative, cf. http://www.openprivacy.org/opd.shtml
- http://www.faqs.org/rfcs/rfc2828.html
- http://www.itu.int/ITU-T/studygroups/com17/def005.doc
- Identity concepts and definitions of the Identity management technology thread of the Burton group, Dan Blum
- Identification and Authentication Fundamentals, Roger Clarke
- Privacy and Security, TU Dresden, Dept. of computer science, Institute of system architecture, Anon Terminology Paper, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

This document is intended as a consultation paper, and has not yet undergone a formal review by the Commission. The Modinis^{IDM} Study team is keenly aware that community consensus around the definitions is a prerequisite for success. Therefore, we hereby cordially invite all interested parties to contribute their thoughts and feedback on the terminology paper, so that it may be further refined. Any comments are welcome at modinis-idm@esat.kuleuven.be.

For more information about the Modinis^{IDM} Study and a continuously updated version of the Modinis^{IDM} Terminology Paper, we refer to our web site: https://www.cosic.esat.kuleuven.be/modinis-idm.

2. Table of Contents

3. Scope of the terminology document

During the first Modinis^{IDM} Workshop of 4 May 2005 in Leuven, one of the first problems identified as a barrier to the development of interoperable IDM systems in eGovernment is the lack of a common conceptual framework. This was identified by the Modinis^{IDM} Study Team as a key issue that needs to be resolved; a position which was subsequently supported by the eEurope eGovernment subgroup – Ad hoc group on Identification and Authentication during its session in Brussels on 30 June 2005.

Part of the conceptual framework – which includes every aspect of the IDM infrastructure – is made up of the terminological framework: the definitions of all concepts of the infrastructure. The lack of a common understanding of even the most prevalent IDM notions constitutes a meta-problem which obstructs a constructive dialogue on the problem of interoperable identity management as a whole. There is no common agreement on the definition of essential concepts such as identity, entity, attribute, delegation, or even entity authentication and identity management.

The current definitions vary widely, since they reflect a complete different point of view on such issues as the use of unique identifiers, who should manage identities and the scope of the definitions. As a practical example, it is nearly impossible to discuss privacy protection questions when there is no consensus about the attributes that define an entity, or if an entity can be something other than a natural person (e.g., a legal person, or even an object such as a computer system, where privacy concerns would not apply).

This paper deals with this issue by attempting to propose a series of neutral and internally consistent definitions of such IDM concepts, thus creating eGovernment IDM ontology. The definitions are based on the preparatory work done through other European projects and initiatives (such as FIDIS, PRIME and GUIDE), amended and completed by inputs from several eGovernment initiatives (such as the aforementioned subgroup, IDABC and of course the Modinis^{IDM} Study itself).

The quality of any ontology depends on three characteristics: coverage (level of completeness), consensus (agreed upon), and accessibility (ease of use). It is thus important to note that this is a consultation paper, intended to draw criticism and generate constructive feedback. As such, it should be considered provisional in its entirety.

4. Terminology

This section presents a variety of definitions regarding identity management. Beyond a short definition, further explanatory comments according to the term defined are presented.
The terms provided in this section aim to propose a shared vocabulary for common IDM terminology, taking into account the specific eGovernment IDM context. It is intended to provide all stakeholders with a common terminology, in order to facilitate further debate in this field and contribute to the further growth of a more general IDM conceptualisation. Thus, the definitions are ultimately intended to function as an enabler for the creation of a pan-European IDM architecture.

4.1 Access control

Definition: ***Access control*** *is the protection of resources with technical, regulatory and organizational measures against access or use by unauthorized entities.*

4.2 Anonymity

Definition: ***Anonymity*** *refers to the quality or state of being not identifiable within the set of all possible entities that could cause an action and that might be addressed.*

In this state, the involvement of an entity in a given process is concealed, so that a given action can not be attributed to a specific entity.
The set in which an entity is anonymous typically varies in time and decreases in size as digital systems do not "forget".

4.3 Assertion

Definition: an ***assertion*** *is synonymous with a credential.*

4.4 Attribute

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

An attribute has a type and a value. It is any piece of information about an entity, which does not necessarily uniquely distinguish the entity from any other entity in a given context. Attributes include the characteristics of an entity.
An entity has a finite, but unlimited number of attributes.

4.5 Authentication

<u>Definition:</u> ***Authentication*** *is the corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence.*

Authentication may be used during any IDM process. Authentication serves to demonstrate the integrity (i.e., equivalence to a corresponding reality) and origin (i.e., the source) of what is being pretended (the claimed information). The security and reliability of authentication mechanisms may vary dependant on the desired authentication level. The stronger the authentication, the higher the confidence that an entity corresponds with the claimed set of attributes.

Authentication is typically subdivided into two separate classes: data authentication and entity authentication. For this reason, autonomous use of the term "authentication" (without specifying the type of authentication) should be avoided, as it is subject to (mis)interpretation.

Authentication can be unilateral or mutual. Unilateral authentication provides assurance of the identity of only one entity, where mutual authentication provides assurance of the identities of both entities.

4.5.1 Data authentication

<u>Definition:</u> ***Data authentication*** *is the corroboration that the origin and integrity of data is as claimed.*

Data authentication is a technical process which (in an IDM context) serves to verify that any claimed attribute corresponds to the actual attribute held by an entity.

It is worth noting that data authentication verifies origin and integrity (i.e., the correspondence of a claimed attribute to an attribute that was issued to a specific entity), but not necessarily truth (i.e., the factual correctness of the claimed attribute). E.g., an authentication token containing incorrect data (e.g., an incorrect name) could be used to authenticate data which is factually wrong. Data authentication protects against manipulation (insertion, substitution or deletion) by unauthorised parties; not against e.g., incorrect issuance of credentials or tokens.

4.5.2 Entity authentication

<u>Definition:</u> ***Entity authentication*** *is the corroboration of the claimed identity of an entity and a set of its observed attributes.*

As a part of entity authentication, entities can be identified by factors: knowledge (e.g., password), possession (e.g., token), a personal characteristic (biometrics), location (e.g., network address or phone number), etc., or by a combination of these factors. A typical example of a two-factor authentication mechanism consists of the combination of password and fingerprint authentication.

The specific case of biometrics can be considered a variation of possession (e.g., fingerprint authentication demonstrates the possession of the required fingertip). As the only difference between biometry and other forms of possession is the decreased likelihood of accidental loss of the identifying element, it does not necessitate specific attention at this point.

Entity authentication can be unilateral or mutual. Unilateral authentication provides assurance of the identity of only one entity. Mutual authentication provides assurance of the identities of both entities.

4.6 Authorisation

Definition: ***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.

Usually, authorisation is in the context of authentication. Permission is granted or denied based on the result of data or entity authentication, and on the allowed activities, as defined within the system. Once an entity is authenticated, it may be authorized to perform different types of access, each of which is referred to as a role.

4.7 Characteristic

Definition: A ***characteristic*** *of an entity is an attribute specific to a particular context.*

A characteristic does not need to uniquely identify an entity. Characteristics indicate an entity's capacity, function, and qualification, etc.

Examples:
- the prime minister of a particular country or a prime minister in a group of prime ministers;
- the Belgian national registry number of a citizen in Belgium or the same number determining a part of a computer device.

While a characteristic is a single attribute, in practice it often implies a set of other attributes, which may or may not be included in the system. E.g., the characteristic of being a doctor implies adulthood and the completion of a certain education.

4.8 Confidentiality

Definition: ***Confidentiality*** *refers to the state of keeping the content of information secret from all entities but those authorised to have access to it.*

4.9 Context

Definition: a ***context*** *is a sphere of activity, a geographic region, a communication platform, an application, a logical or physical domain.*

Practically, a context is only relevant in an interaction.

4.10 Corroboration

*<u>Definition:</u> **Corroboration** is the confirmation by provision of sufficient evidence and examination thereof that specified requirements have been fulfilled.*

The term “verification” is often used as a synonym of corroboration. However, this term is somewhat more dubious, as it is also occasionally used as a synonym of authentication (either entity or data authentication). For this reason, “corroboration” should be preferred over “verification”.

“Sufficient evidence” is determined by the Identity Management System. It is possible that the amount of evidence required is (virtually) non-existent or holds (virtually) no legal value, e.g., a simple set of claims (e.g., claiming to have a certain name or address).

4.11 Credential

*<u>Definition:</u> A **credential** is a piece of information attesting to the integrity of certain stated facts.*

Credentials are primarily used in the process of entity authentication, and are then often incorporated in an authentication token, e.g., a smart card, bank card, mobile phone, etc.

Note that credentials are not always integrated into a token: in certain systems, a password might function as a credential, despite the lack of a medium carrying the information. Certificates are a common type of credential in a PKI system, where they often take the form of so-called *attribute certificates*: a credential attesting to the integrity of one or more attribute values with identification information about the corresponding entity.

Credentials are typically revocable.

4.12 Delegation

*<u>Definition:</u> **Delegation** is the process in which an identified entity issues a mandate to another identified entity.*

From a legal perspective, the concept of delegation usually implies acceptance by the receiving identified entity. In a technical context, acceptance is usually unnecessary.

A mandate can be used to delegate authorizations of one identified entity to another.

4.13 Digital Identity

*<u>Definition:</u> A **digital identity** is a partial identity in an electronic form.*

For any given entity, there will typically exist many digital identities which may be unique or non-unique. A digital identity can be created on the fly when a particular identity transaction is desired.

A digital identity is, by definition, a subset of the identity, and can in effect be considered a manifestation of an entity’s presence in an electronic IDM system (i.e., it is the subset of attributes belonging to an entity that is accessible through a specific IDM system).

4.14 Enrolment

*Definition: An **enrolment** is synonymous with a **registration**.*

4.15 Entity

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

The choice was made to provisionally keep this definition open to any type of person (including legal persons, to facilitate e.g., eProcurement), but also to any other type of entity, such as objects (e.g., computers or other forms of machinery), digital resources or processes (e.g., programmes), as this allows abstraction to the largest common element and thus offers the largest number of applications.

In order for its existence to be acknowledged, an entity needs to have at leas one unique identity.

4.16 Federated Identity

*Definition: 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.*

4.17 Identifiable Entity

*Definition: An **identifiable entity** is an entity whose identity can be established.*

4.18 Identification

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

The term "identification" is also referred to as entity authentication. The identification of an entity within a certain context enables another entity to distinguish between the entities it interacts with.

4.19 Identified entity

*Definition: An **identified entity** is an identifiable entity the identity of which has been corroborated.*

The term "identified entity" is also referred to as an "authenticated identity."

As indicated below, corroboration entails that a given element has been proven to the extent required by the Identity Management System. As such, there are no fixed rules or criteria to meet before an entity can be considered identified. The only criterion is the acceptance of the identification by the IMS.

4.20 Identifier

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

For the sake of clarity, identifiers consisting of one attribute are also characteristics; they distinguish an entity from other entities.

An entity may have multiple distinct identifiers referring to it. Identifiers uniquely identify an entity, while characteristics do not need to. However, it should be noted that identifiers can consist of a combination of attributes, whereas characteristics are always one single attribute.

4.21 Identity

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

An entity has only one identity, consisting of a number of attributes that need not necessarily be unique for that entity, but which are nonetheless useful when attempting to distinguish several entities. Common examples of such attributes include name, date and place of birth, address, the identity of parents, etc.

As such, the identity is a fluid and evolving philosophical concept, rather than a practical one: as it is impossible for any one IDM system to gather all attributes of any specific entity, IDM systems must focus on a specific subset of relevant attributes.

As a rule of thumb, when people refer to **the** identity of an entity, they are referring to the essence of the entity as defined above. In contrast, when they refer to **an** identity of an entity, they are referring to the concept of **partial** identity, as defined below.

This brings us to the following concepts.

4.22 Identity management (IDM)

*Definition: **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.*

4.23 Identity management application

*Definition: An **identity management application** is a tool used by an entity to manage partial identities.*

In general, the identity management application is used to manage partial identities, e.g., for their creation, updating, revocation, etc.

4.24 Identity management system (IMS)

Definition: An ***identity management system*** *is the organisational and technical infrastructure used for the definition, designation and administration of identity attributes.*

4.25 Mandate

Definition: A ***mandate*** *(or* ***proxy****) is a revocable role or a set of revocable roles which refer(s) to one or more permissions granted by an identified entity to another identified entity to perform well-defined actions with legal consequences in the name and for the account of the former.*

Mandates are a type of characteristic, and thus also an attribute. Mandates (or proxies) must be revocable. E.g., the power of attorney or a parent's authority over its underage child.

4.26 Non-repudiation of origin

Definition: ***Non-repudiation of origin*** *is the ability to prevent an acting entity from denying at a later stage that it performed that specific action.*

4.27 Nym

Definition: A ***nym*** *is synonymous with a* ***pseudonym****.*

4.28 Partial Identity

Definition: A ***partial identity*** *is a certain subset of one or more attributes that does not necessarily uniquely identify the entity.*

While an entity has only one identity, it may have many partial identities. Partial identities are often simply referred to as "identities", which may lead to confusion when they refer to a single entity. For this reason, the term "partial identity" should be preferred.

4.29 Permission

*Definition: **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…).*

Permissions are also referred to as "access rights."

4.30 Persona

*Definition: A **persona** is a pre-existing digital identity that an entity can select and use to represent itself in a given context.*

A persona is something put forward by an entity, but how it is perceived, recognized, accepted, rejected, trusted, used, etc. by another entity cannot be specified or in any way implied. It is often used when the set of credentials of the entity represents a role or has a virtual character animated by the entity.

4.31 Personally identifiable information

*Definition: **Personally identifiable information** is any data that identifies or refers to a particular natural or legal person.*

4.32 Principal

*Definition: A **principal** is synonymous with an identifiable entity.*

4.33 Privacy

*Definition: **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.*

Privacy can alternatively be described as the freedom of a natural person to sustain a "personal space", free from interference by other entities.

In an IDM context, privacy is mostly used as a synonym of "informational privacy", i.e., the interest of a natural person to control, or at least significantly influence the handling of data about themselves, also taking into account the nature of the applicable attributes and the entity in charge of data management.

4.34 Privacy enhancing technology (PET)

Definition: *A **privacy enhancing technology** is hardware or software which increases the ability of a natural person to actively influence the availability of information about and exposure of itself.*

4.35 Profile

*Definition: A **profile** of an entity or a group of entities is an organized set of attributes that characterizes the specific properties of that entity or entities within a given context for a specific purpose.*

4.36 Profiling

*Definition: **Profiling** is the practice of collecting and analysing data related to an entity with the aim of creating its profile.*

4.37 Proxy

*Definition: A **proxy** is synonymous with a **mandate**.*

4.38 Pseudonym

*Definition: 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.*

A pseudonym is typically a fictitious name that can refer to an entity without using any of the entity's identifiers. In effect, the pseudonym is an additional attribute of a given entity's identity, which allows it to form a set of partial identities which can not necessarily be easily traced to the originating entity.
As identifiers, pseudonyms are context-bound, and one pseudonym is not necessarily valid across multiple identity management systems.
An entity is pseudonymous if it relies on a pseudonym as identifier.

4.39 Registration

*Definition: 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.*

In other words, the registration of an entity is the process of linking a (partial) identity to the identity of an entity, by corroborating a specific set of attributes, which do not necessarily need to include identifiers.

Successful completion of the registration procedures results in the granting of a means (e.g., a credential) by which the entity can be authenticated in the future.

Quality assurance criteria (with various degrees of liability attached) can be imposed on the registration process.

4.40 Resource

*Definition: a **resource** is either data related to some identity or identifiers, or a service acting on behalf of some identity or group of identities.*

The set of technical, regulatory and organizational measures intended to protect system resources against access by unauthorized entities.

4.41 Role

*Definition: A **role** is a set of one or more authorisations related to a specific application or service.*

4.42 Token

*Definition: A **token** is any hardware or software that contains credentials related to attributes.*

Tokens may take any form, ranging from a digital data set to smart cards or mobile phones.

Tokens can be used for both data/entity authentication (**authentication tokens**) and authorisation purposes (**authorisation tokens**).

4.43 Trust

*Definition: **Trust** is a quality of a relationship between two or more entities, in which an entity assumes that another entity in the relationship will behave in a fashion agreed beforehand, and in which the first entity is willing to act on this assumption.*

Whether or not to trust depends on a natural person's decision. It is possible, but not necessary that several entities trust each other mutually in a certain context. Trust decisions of legal persons depend on the decisions made by the legal person's responsible natural persons.

Trust may be limited to one or more specific functions, and may depend on the fulfilment of one or more requirements.

4.44 Trusted third party (TTP)

*<u>Definition:</u> A **trusted third party** is an entity trusted by multiple other entities within a specific context and which is alien to their internal relationship.*

4.45 Unique identity

*<u>Definition:</u> A **unique identity** is a partial identity in which at least a part of the attributes are identifiers.*

Since at least some of the attributes (or combinations thereof) are identifiers, the entity can be uniquely identified through the unique identity within a certain context. A unique identity is an identifier such as a unique number or any set of attributes that allows one to determine precisely who or what the entity is.

Prepared by:

The Modinis IDM Study Team under the Service Contract 29042 from
DG INFSO, EUROPEAN COMMISSION

For further information about the eGovernment Unit

European Commission
Information Society and Media Directorate-General
eGovernment Unit

Tel (32-2) 299 02 45
Fax (32-2) 299 41 14

E-mail EC-egovernment-research@cec.eu.int
Website europa.eu.int/egovernment_research