# Listing and Scoping TWIST Standards and Projects for Identity Infrastructures

Version 0.1

November 26, 2006

## *Foreword*

In the IDWG we are looking for the underlying identity infrastructure to be serviceable for the TWIST applications/processes *e.g.* bank mandates, payments within SEPA, and supply chain.

The purpose of this paper is, following the business requirements document, to help the IDWG to focus its debates and developments on issues we are still debatable or need further developments in the Identity Working Group (IDWG).

The outline takes the point of view of processes:

- Processes to manage the identity life-cycle, and
- Processes relying on digital identities.

Identity management is becoming the battlefield for new and old solutions providers. Some of them concentrate on retail Web services while others tailored their offer to a company perimeter. The danger is the emergence of islands of non-communication while "interoperability", the ability to transact securely across open networks, is the ultimate goal.

SEPA is an opportunity to think anew the role of identities and identifiers in the finance and "adjacent" processes.

There is still a strong resistance to the implementation of PKI infrastructures, while PKI still look the most practical means to respond to the business requirements. Implementation issues should not be neglected.

Under the pressure of Governments around the world local or international identity schemes are put in place. They have to be taken into account because corporates as well as persons are likely to minimise strongly the number of identities they are will have to "carry". Furthermore these schemes will condition the way existing identities can be used in other fields, like ours.

## *History*

This version is a framework for discussion. It was written/edited by JY Gresser, cochair of the IDWG, which work is supported by InterComputer. It combines chap 2 and 3 of the "requirements" document (version 0.2, which version 0.1 had been prepared by our colleagues from IdenTrust) and elements from Nick Ragouzis' Advancing a Versatile Interoperable Identity Infrastructure for Finance and Services in the EU, 2006 Jan 19 issue.

This document should frame the IDWG's considerations and start dividing the subject matter into points that seem likely to require discussion and those(*) that may require little or none because they are thought to be rather widely accepted, and appropriate.

The current outline is largely inspired from previous work and from the emergence local or international standards. More points could be added and should be developed by the IDWG.

*Comments and contributions are highly welcome!*

**List of content**

### *Introduction: Identities, identifiers, certificates, identity infrastructures.*

In a broad sense, an **identity** is a set of elements, which will enable a relying party to recognize a physical person or a legal entity and to differentiate it from another SIMILAR entity.

An **identifier** is a character or a group of characters used to identify or to designate data and, possibly, to specify some of its properties (ISO 2382/IV). With regard to persons, we could use the word "credentials" instead of properties[1].

Social security numbers and corporate taxations numbers are identifiers. You can have parallel identifiers for the same individual, e.g. a passport number or a driving license number.

The scope and use of these identifiers may differ widely: everyone is given a social security number when born and will keep it throughout his life while or a passport number is attached to a physical document, which has a limited life span.

In the literature "identity" is often synonymous to "identifier". From a practical standpoint an identity is a set of identification elements. These elements may sometimes be wrapped up into an identifier. An identifier might or might not be "reversible" to its composing elements, while an identity MUST be.

In our context we will have to deal are with many types of identities[2] (or identifiers[3]):

- Professional identities of persons, i.e. to identities which relate to a person professional role, activity etc. in a business entity or a public body;
- Identities of legal entities (corporates or public administrations), bank accounts, financial services, machines etc. which are relevant to our context i.e. the exchange of information between companies, between companies and banks, between companies and public body where payments are involved. The exchange may take place between two persons, between a person and an application, or between two applications.

*In the IDWG, we focus on the identities of professionals (physical persons). In this area it the standardization process seems much less mature than in others.*

Still the identities of "business entities" should not be neglected, as they are required in core payment messages and have been subject to standardisation of so-called "reference data".

**Digital certificates**[4] are often referred to as *"digital identities"*, which may be misleading. They are actually data objects issued by or on behalf of a company to its employees for

---

[1] However the word "credential" or "credentials" also designate the actual support bearing the information, like a smart card or a passport with a travel visa: "please give me your credentials".

[2] (1) An *identity* is a set of information that is attributable to a given ***entity***. [Source: ***Wikipedia on Digital Identity***.] (2) *Identity* is a presentation or ***role*** of an ***entity***. [Source: ***Roger Clarke***.] (3) a set of claims made by one ***entity*** about itself or another ***entity***. [Source: ***Kim Cameron***.] (4) An *identity* is the set of the properties of an ***entity*** that allows the ***entity*** to be distinguished from other ***entities***. Identities are *owned* by their ***entities***. *Identities* have several key attributes, including: ***anonymity***, ***strength***, owning ***entity***. (R)

[3] (1) An *identifier* is information that names or indicates an ***entity*** or ***grouping*** of ***entities***. [Source: ***Stefan Brands***.] (2) An *identifier* is a signifier for an ***identity*** ; it is one or more data items that distinguishes an ***identity*** from other identities. Examples of *identifiers*: name, id-number, username, IP-address. [Source: ***Roger Clarke***.] (R.)

[4] An ITU x.509 v3 standard data structure that securely binds an identity to a public key.

A certificate is created when an entity's public key is signed by a trusted identity, a certificate authority. The certificate ensures that the entity's information is correct and that the public key actually belongs to that entity.

A certificate contains the entity's name, identifying information, and public key. It is also likely to contain a serial number, expiration date, and information about the rights, uses, and privileges associated with the certificate. Finally, it contains information about the certificate authority that issued it. (O.)

As part of the X.509 protocol (a.k.a. ISO Authentication framework), certificates are assigned by a trusted Certificate Authority and provide verification of a party's identity and may also supply its public key. (I.)

The certificate is a form of digital identification that allows you to secure exchanges on the Internet by guaranteeing authentication of the issuer, integrity of the data sent, non rejection of actions and the confidentiality of transmitted data. It is a logical data processing object that allows you to link the identity of an entity to certain characteristics of this entity intangibly.

access control to internal information or on behalf of one of the Company's banks for access to granting access to banking services under specific conditions.

A certificate includes at least "identifying information" and may include "information about the rights, uses and privileges associated with the certificate", and security information (like the public key of the entity to which the certificate is attached).

Such a certificate may be the sub-product of a corporate identity-management system, to be used within the company perimeter, for specific applications or beyond. It may be provided by business partners in a specific business environment (supply chain, treasury services).

**Identity infrastructures**[5] are occurrences of architecture, policies, operational and management activities, hardware and software, that cover the lifecycle of identities and their consumption.

## *1. Participants in an identity systems and their requirements.*

Within the context of a business application, there are multiple entities, legal entities, organizations, and persons involved. Each of these parties represents a particular interest in business transactions. Identities should be tailored to their needs.

In the following we outline these needs for the main entities to be taken into account.

### 1.1 Corporations

The corporation in the context of identity systems is the originator of identity. The corporation creates, owns, bestows, and removes identities, roles, and attributes through an identity system (it may also do so via a so-called "trusted third party").

#### *Agents*

For the purposes of this document, an agent is a person or machine (server or service) that represents a particular aspect of a business function for a corporation. The agent then would have a name, a role, and some attributes that empower the agent with authority to operate the business function on behalf of the corporation.

---

Ownership:
- It is attributed to an individual. Therefore, it is personal and can be neither exchanged nor lent.
- It is renewable automatically if no request for non-renewal or modification has been made by persons or authorities[1] authorised to do so (its period of validity is limited and subject to the nature of its use).
- It is revocable, which means that in case of theft or violation of the key, the certificate can be stopped
- Associated to its private key, it is stored on a microprocessor card, issued by SG Trust Services.

SG Trust Services issues key authentication and encryption certificates: they satisfy the need to authenticate individuals who act on behalf of the company or to encrypt keys. These certificates can be used for remote administrative procedures.

The conditions for delivery, usage and management of these certificates are described in the Certification Policy for key authentication and encryption certificates and signature certificates (www.sgtrustservices.com/en/entreprise/pc/).

[1] Persons and authorities entitled to have an involvement in the life of a certificate:
- Subscriber,
- Certificate Manager,
- Representative of the company,
- Registration Authority,
- Certification Authority,
- Any other person authorised by the Certification Authority. (SG T.)

Oracle Advanced Security Administrator's Guide, Release 8.1.7 (O.)

Identrus System 2.0 Installation, Administration & User Guide (I.)

SG Trust Services- Digital Certification Center- Glossary (SG T.)

[5] Identity Infrastructure is that bundle of information, technology, processes and law by which "real world" identity is established, maintained (managed), propagated, shared, demonstrated, proved or disproved, expressed digitally, etc. Designed and built correctly, that infrastructure will support citizens' identity needs where, when and how they choose, and will improve individual privacy while meeting needs for access to information. The purpose of this document is to provide a thought-provoking look at current and future functional identity needs and what will be necessary to meet them.
(NECC 2003)

### *Employees*

A person who is in the employ of a corporation is an agent.

Not all employees are authorized to represent the corporation in every action. The roles and authorizations of an individual are important to the business context.

People also have personal information that must be protected from unauthorized access and sharing. This presents some challenges to identity systems particularly in proofing individuals.

### *Managers*

Managers will validate information about employee's identities and roles. During the course of a business transaction they may authorize specific operations.

### *Administrators*

Administrators will overlook and control the set-up and the operation of either the identity infrastructure or of a specific part of the applications using this infrastructure. They must be provided with the tool to manage and control the "identity life-cycle" in their specific environment.

### *Contractors*

Beyond the agent, some individuals and entities may take on an identity provided by a corporation to which they do not belong. They may use the identities provided by the partnering corporation or they many use identities that are deployed by an identity system of their own choice.

The business need is to have the identity system of the contractor be able to interact with the identity system of the corporation for a business purpose.

### *Auditors*

Auditors have a special role in business communications and transactions. They provide the underlying trust for the whole environment. They must be given the adequate tools to perform surveys of the systems and organisations build around them.

## 1.2 Banks or Financial Service Providers

Criminal use of money has become a major focus of legislatures and government regulators. Being on the path of most money transfers, banks are in a position to provide information on the misuse and inappropriate movement of money.

They are responsible on a global basis for knowing, who their customer is (Know Your Customer – KYC). Banks do this on the basis of accounts – deposits, lending, cash management.

Banks are in a good position to identify, verify, proof, and vet corporations for their identity; they can provide means to check on how they express their identity.

For the purpose of this document, financial institutions are called banks. What distinguishes a bank from a general corporation is that banks are usually regulated by some government agency. There are proscribed bounds under which the bank operates.

## 1.3 Trusted Third Parties (TTP)

Within any identity system context, there is an entity, organization, and/or system that sets identities and associates with them credentials. A trivial example is that of a standalone application, which creates its own user ID and passwords. A more robust system may provide a single-sign-on capability for a corporation using one-time-password (OTP) tokens. Another robust system may provide a hierarchical structure of PKI certificate authorities issuing smart cards.

### *IDSP[6] or Trusted Third Party-TTP[7]?*

The role of the TTP is to provide to relying parties a place of reference for trust in the statements and assertions made by an entity.

The entity may be passive in that it simply creates it credentials and makes them available. Another type of trusted third party may be active in providing attribute services and additional information about the entities that it identifies. In either case, the trusted third party associates names, credentials, and attributes with a particular identity.

A TTP is not to be confused with an ID service provider, which only provides "identity indexed" services like discovery.

## 1.4 Governments

Identity has always been a key question for governments. Public accountability, political pressure, and defence necessities – present a different set of risks than those of the commercial sector. In commerce, most situations can be leverage with controls, procedures, and even insurance. Government concerns may not always fall in that space.

Government penalties' can be more severe typically found in the commercial space. They may range from significant fines to incarceration of corporate agents.

The driving factor in our field is that public administrations are often the largest buyer in a country. Thus a solution, which a government will choose, is likely to become a de facto standard nationally and internationally for some. Business solutions will have to adapt rather than the reverse.

### *Regulators*

Regulators form a special subset in the government sector. The regulators may cover any commercial space including privacy, financial institutions, customs, and trade practice.

Key in each of these areas is the identification of the corporation and / or corporation agents involved in transactions.

Regulators are also interested in agents that file reports, customs forms, and tax records for governments. There is need for the regulators to be able to examine and conclude that the identity systems are appropriate for their area.

---

[6] **identity (web) service**

A type of web service whose operations are indexed by identity. Such services maintain information about, or on behalf of, Principals — as represented by their identities — and/or perform actions on behalf of Principals.

They are also sometimes referred to as simply identity services.

In Liberty ID-WSF, such services are both mapped on a per-principal basis and discoverable — meaning that once a Principal authenticates, the authenticating party possesses a reference to the Principal's Discovery Service instance, which it may use to discover the Principal's other identity services. See also "discoverable".

See also Discovery Service, discoverable, web service (2), and [LibertyDisco]. (L.A.)

*As identities may be embedded into digital certificates IDSP may be called CSP Certificate Sevice Provider (PSCE in French).*

[7] An organization entrusted with the keeping of cryptographic keys. The apparent idea behind the appointment of trusted third parties (TTPS) is that by holding a copy of someone's public key they can provide independent confirmation of that person's identity to other parties in an E-commerce deal.
www.research-hosting.co.uk/data/hosting-terms/web-hosting-terms-t.asp

In cryptography, a trusted third party (TTP) is an entity which facilitates interactions between two parties who both trust the third party; they use this trust to secure their own interactions. TTPs are common in cryptographic protocols, for example, a certificate authority (CA).
en.wikipedia.org/wiki/Trusted_third_party

In general, a security authority or its agent, trusted by other entities with respect to security-related activities.

In the context of Liberty, these other entities are, for example, Principals and Service Providers, and the trusted third party is typically the Identity Provider(s) involved in the particular interaction of interest (L.A.)

## *2. Managing the Identity Life-Cycle*

An Identity is a "chain". The quality of an "identity infrastructure" will derive from:

- Its build-in processes (identity management), as well as
- The processes that can be build around it. Business processes like the "Bank Mandate" may trigger identification, authentication, and authorisation. These are just examples of identity "consumption".

ID consumption assumes that valid identities are "at hand", i.e. that underlying ID management processes covering the identity life-cycle i.e. the provisioning/creation, the maintenance and the revocation of identities, wre put in place.

In this chapter we will deal with the processes directly related to the life-cycle of the identities.

The "consumption" of identities is the subject of chapter 3.

### 2.1 Capturing the Identity Life-Cycle

There are currently several attempts[8] [9] [10] to model IDM or IDLM. We will adapt these models to our own environment.

These models originate from the management life-cycle of digital keys or certificates to which specific features were added.

---

[8] *ISO/IEC J1SC 27 lists the following elements as composing the identity life cycle:*

- *Identity choice, provisioning and enrolment;*
- *Identity authentication,*
- *Binding identities with attributes,*
- *Identity certification,*
- *Identity change,*
- *Unbindinding of attributes from identities,*
- *Identity revocation, and…*
- *controls.*

*See Information technology- Security techniques- A framework on Identity Management, ISO/IEC J1SC 27 N5056, ISO/IEC WD 24760, April 28, 2006.*

[9] *The US National Institute of Standards and Technology published in February 2005 a detailed document on Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS PUB 201). This document will apply to contractors in the US and abroad. IT is likely to be a key element of the Federal Bridge and of the TSCP. First applicable to the Defense industry, it will extend to pharmaceutical and… finance.*

[10] *In the line of the above, the TSCP is currently reviewing "International Proofing and Vetting Practices and Procedures" along a common so called TSCP IPV Framework process model. This models include the following concepts:*

- *Enrolment,*
- *Registration,*
- *Verification,*
- *Issuance,*
- *Publication,*
- *Revocation.*
- *Authentication,*
- *Authorization,*
- *Record retention,*
- *Approval of IDM systems.*

### 2.2 Identity Creation: Choice, Provisioning & enrolment

The following sections outline issues to be considered in the IDWG.

*Who or what are we identifying?*

Local legislations may require that the person initiating or validating a transaction be identified.

It may also require an identification of the business entities of that person.

*"From a Corporate point of view, the best solution to obtain a maximum degree of efficacy/efficiency in an advanced business platform is to use the same "counterparty identification code" used in the Customer Relationship Management (CRM), the Enterprise Resource Planning ( ERP) and the Treasury & Cash Management system.*

*Obviously, the best configuration of an electronic identification credential is one that contains the same identification code present in the business platform, especially if the same credential is also used to identify the holder of the electronic signature.*

*The best solution to manage electronic documents (invoices, payment orders, mails, fiscal declaration, etc.) is one that allows to use the same instrument, software and process for inbound /outbound flows and legal archiving." (CAST)*

*Simplicity viz Multiplication of Certificates** [11] [12] [13]

*The goal is "to reduce the cost and complexity to manage inbound and outbound authentication and digital signature creation and verification procedures."(CAST)*

It often seems easier to devise a new system rather than use an existing one. The result is an unnecessary proliferation of solutions, and often of the smart cards, applications, and other technological accoutrements of certificates.

**As much as possible, from a user perspective, a "simple identity solution" is to be preferred over a more complex one. When one certificate (and one secure device for holding a private key) will suffice, another certificate and private key should not be required.**

**However, a balance is to be found between simplicity, privacy, traceability and resilience of the ID infrastructure.**

*An alternative is "either*

- *To build from scratch a new coding system (like SWIFT in the IBEI project) with the enormous difficulty and cost of attributing and delivering codes and maintaining and managing the database, or*
- *To use existing national schemes, like tax ID's and social security numbers."(CAST)*

*Identifiers: IBAN, BIC, IBEI etc?*

EDIRA ISO was never able to define a universal company identifier. So we are faced in our context to IBEIs, IBANs, and BICs…

---

[11] *R points may not warrant much discussion; however, that may not prove to be the case. They are listed here, and could be added to the list above, if views differ from those postulated below.*

[12] *As expressed it looks very broad while there are actual issues at stake. The first question which party's needs are we trying to address. It is clear end-users call for simplicity. This may be addressed by more complexity on the service provider side.*

*While at the same time IT organization would hate putting in place several identity infrastructures.*

*So it is actually a point to be expanded and discussed.*

[13] *As expressed it looks very broad while there are actual issues at stake. The first question which party's needs are we trying to address. It is clear end-users call for simplicity. This may be addressed by more complexity on the service provider side.*

*While at the same time IT organization would hate putting in place several identity infrastructures.*

*So it is actually a point to be expanded and discussed.*

An identifier is used for identification and “localisation” like in a network or an organisation of any sort. It is then used to discover (locate) a resource and to route information to and from that resource, see for example the IBAN or the packet header in IpV6.

A danger in identifiers is that there is a temptation to use them for what they were not designed for.

### *IBAN?*[14]

There is a strong interference between personal identities and e.g. the bank account numbers. See the French "relevé d'identité bancaire" often translated into “bank ID". You may yourself have a "bank ID card" to be used as "credentials" for payments.

An account has an identity by itself, which may be separated from the “owner” or a “user”. In the business environment, a given account may change user from time to time, often at a short notice (see the BMWG requirements). This needs to be clarified, as well as the following.

In most European countries the IBAN or any other bank account number is mostly routing information, that points to a specific bank account[15]. It is used to send funds from one account to another, in the same way email-addresses are used to send emails from one address to another.

As you may use several payment means, moving information along different routes, a bank account may have several parallel addresses pointing to the same ”book”, e.g. the domestic account number (BBAN), the international account number (IBAN), card number for the card attached to the account (eg in countries using debit cards and ATM cards), phone numbers (eg in countries having mobile payments based on phone numbers) etc.

The account needs addresses so that the fund transfers can be made correctly, whichever payment mean is used.

Last but not least, customers have generally several accounts and there is a need to have “something” distinguishing these from each other.

Personal identity is something different

*Learning from the health sector?*

If we get a HEPI (Health European Personal ID) it is given to one person individually and will stay the whole life with him. Every health care institution will have access to his medical records via this identifier.

There might actually be several records for the same person, none with all his health information eg the Finnish information will be somewhere in Finland, the Swedish information somewhere in Sweden. However if somebody has the right to retrieve the information he can do it using the HEPI in all countries.

As all Finnish health care information is currently stored using the Finnish Social Security NUmber (SOTUN for short) there will be a cross reference register in future in Finland mapping the HEPI to the SOTUN so you can make a search in the registers. Still we will have a decentralised database structure in Finland and the health care information has to be searched from several databases. There will be no portability in this environment as the HEPIs and SOTUNs are fixed to given persons and all the service providers have their own fixed registers. As you don't know before hand which hospital organisation have stored information about me you have to access all to see what they have or at least a reference register with the references on all my stored information.

### *Proofing and Vetting*

The process of determining the identity of a corporation, corporate agents, or even individuals is called proofing and vetting. This is usually done through primary documents (e.g. letters of incorporation, passport, Latin notary), and through examination of public records and

[14] The issue of portable IBAN is discussed in chapter 3.

[15] Actually the BIC is used for routing within the “bank networks”. The IBAN is used for dispatching within the payee’s bank.

commercial databases. This is a relatively new area for identity management; it did not come to the forefront until identity systems began to be used between disconnected and unrelated government and business.

Banking regulators have, in recent years, increase the requirements on financial institutions to know who their customer is and be able to provide proof that the bank knows their business and where they money is moving.

Identity systems must be able to process and store documentation that originates during the proofing and vetting. If the documents and systems are sufficiently robust, the proofing and vetting may be done less frequently and therefore more economically. Having a proven, provable, automated identify may prove to be a valuable commercial asset.

Vetting of commercial institutions has long common practice in business.

**Identity systems must be able to store and manage primary documents and other proofing materials.**

**Identity systems must be able to re-use proofing and vetting systems in an automate fashion to improve economy of operation and reliability of identity.**

**2.3 Identity Change** *(to be developed)*

*Rights management*

There seem to be three options:

1) Centralised rights Management schemes;
2) Rights checked by the receiver application, value added services;
3) rights controlled internally by sending corporate …receiving bank only checks identity NB a decentralised management requires more standardisation.

…

**2.4 Identity Revocation** *(to be developed)*

**2.5 Certification, Administration & Control of Identity Infrastructures** *(to be developed)*

*Standards (to be developed)*

*Regulations(to be developed)*

## *3. Managing the Identity Based Applications*

### 3.0 Capturing the Use of Identities: Security & Beyond

The following requirements are presented in a business context. In other words, the requirements directly related to when an identity system provided identity is used to transact some monetarily important action between multiple parties.

*Trust*

Beyond the integrity needs of the IT Consumers are the concerns for trust, not the least of which is the need for a Relying Party across the Internet to know or be able to evaluate their own processing commitments, risks and liabilities. Electronic transactions are only possible if one can resolve the identity of the parties around the transaction:

- Trusting the party sending information (Representation)
- Verifying that the sending party is allowed to perform the requested task (acceptable level of verification, corroboration).

*Large corporates, SMEs & Consumers.*

Electronic payments instruments are the same ( credit transfer, direct debit etc.) for large and small corporates (and consumers). They use the same type of bank services.

SMEs will probably make more recourse to outsourcing. The difference DOES NOT lies in the instruments they use but in the different level of protection and information.

*Outline Identity "Consuming" Processes*[16]

The following are examples of processes occurring once a customer has located an application service provider.

1. Customer passes Identity, provided by Service Provider, along with electronic transaction.
2. Service Provider authenticates customer (verifies identity is valid for this Customer).
3. Service Provider gathers information from identity to perform authorization and process electronic transaction.
4. etc.

*Same Outline Process with Identity Provider*

1. Customer uses existing PKI Identity to "log-on" to Service Provider,
2. Service Provider authenticates Customer with Identity Provider.
3. Service Provider receives identity information (attributes) from Identity Provider that customer has authorized Service Provider to see.
4. Based on this information, Service Provider authorizes and processes electronic transaction.
5. etc.

### 3.1 Establishing a Relationship – Contracts and Policies *(to be expanded)*

*Business requirements are legal in nature.*

Regulatory Compliance is no less an issue, yet both require technical components which operate on validated and corroborated electronic policies—not paper policies nor legal forms which are asserted to have been in place after the fact.

[16] Other process templates are to be found in the literature (see references).

*Legal Basis for a Certification Infrastructure** [17]

Contracts provide a clear and flexible way of giving legal effect to the rules, rights and obligations of a certification infrastructure. They can also ensure that the rules remain uniform across different jurisdictions, which is a principal drawback of statutes.

Contracts need to cover liabilities and recourse.

However contracts cannot ignore the legal local framework, or international treaties. Besides government or other professional institutions are trying to establish reference framework or "standards". See for example, within the EU, the framework established in the Electronic Signatures Directive.[18]

**In TWIST enabled services, contracts are the preferred means of establishing the legal basis for an authentication infrastructure.**

*Governement regulations and policies (to be expanded, see also appendix)*

See the example of France was for payment of VAT, Italy for deposit of financial statements, tax returns.)

*2003 DG Information Society Study on Legal and market aspects of implementation of 1999/93/EC Directive in member states*

*EU Directive 1999/93/EC on Liability constraints*

### 3.2 Identification and authentication *(to be expanded)*

**Identification**[19] has basically two meanings: (a) it is the process by which an identity is given and registered, (b) the "visualization" or "materialization" of an identity. An identity may or may not be "authenticated".

In our context, **authentication**[20] is a process, which will enable a relying party to actually verify a claim about the "identity" of a person or of an other entity, including the ability of the person to perform specific tasks or activities.

Briefly stated, identification is communicating one's identity, authentication is bringing supporting elements to the proof of this identity. [from D 530]

*Identification and authentication*

In the bank account environment identification means most often that the user/customer has the right to access the account. He needs to be identified using the right **credentials**.(which differ from the address of the account).

In the corporate environment several persons may the right to access a given account (this may also be true for personal accounts). Thus identification per se is not needed. Pseudos or corporate identifiers may be used as well.

This is an area where a balance to be found between e.g. convenience, fraud detection and privacy.

---

[17] *Agreed especially in relationship with cross-certification (NB cross-certifiation is one of several options)*

[18] *Specific texts need to be referenced.*

[19] *(1) Identification is the process whereby data is associated with a particular **identity**. It is performed by acquiring an **identifier**. [Source: **Roger Clarke**.] (2) Within a designated **context**, **identifiers** enable relying parties to distinguish between the **entities** they **interact** with. This is known as **identification**. [Source: **Stefan Brands**.] (3) Identification is the act of claiming an identity, where an identity is a set of one or more signs signifying a distinct entity. [Source: **Stephen Downes**.] [See also: **Authentication**.] (R.)*

[20] *The process of verifying the identity of a user, device, or other entity in a computer system, often as a prerequisite to granting access to resources in a system. A recipient of an authenticated message can be certain of the message's origin (its sender). Authentication is presumed to preclude the possibility that another party has impersonated the sender. (O.)*

*Authentication is the process of confirming a system entity's asserted identity with a specified, or understood, level of confidence [TrustInCyberspace]. (L.A.)*

Please also take note that "personal identities", which are issued within a company framework could be used beyond the company perimeter.

### *3.3* Authorization *(to be expanded)*

Like identification, **authorization**[21] means both:

(a) A process defining what a person is actually able to do, such as access to a specific type of information or to perform a specific operation ("habilitation" in French),

(b) The process by which actual permission will be granted to the owner of a right ("authorisation" in French).

Access to Information or Services (to be expanded)

One of the key issues is how to guarantee the integrity of documents, which formats will evolve through time.

#### *Appearance of XML Documents*[22]

XML technology generally does not embed the visual formatting of the document in among the data; instead, the formatting resides in a separate file of machine-executed specifications. The appearance of the document is superimposed over the document when its data are displayed or printed. This separation of form and substance can leave room for minor variations in form, *e.g.* a user-specified preference for font size.

**TWIST enabled services must provide an approved stylesheet for the visible rendition of an XML document type, and treat minor variations in appearance as insignificant as long as they are permitted by the approved stylesheet.**

#### *Referencing in XML Documents*

XML is a referential technology in that many of the specifications applicable to a document (such as its schema, name space, stylesheet etc.) are kept external to the data file itself. References such as URIs among the data incorporate the referenced specifications into the data file. The result is efficiency through eliminating redundancy, as well as consistency in that use of a single, referenced specification helps prevent variations in the agreed specifications do not find their way into an XML system.

**XML specifications promulgated by TWIST for inclusion by reference in document instances must be online at URIs readily accessible by TWIST users.**

**Different versions of referenced documents must have different URIs.**

**TWIST (or any other publisher of specifications for use in a TWIST enabled service) should make a digitally signed copy of a published specification available on request, together with a statement of the URI at which the specification is published.**

[21] *Permission given to a user, program, or process to access an object or set of objects. In a modern computer application, authorization is done through the role mechanism. A single person or a group of people can be granted a role or a group of roles. A role, in turn, can be granted other roles. The set of priveleges available to an authenticated entity. (O.)*

*The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access [SAMLGloss]. (L.A.)*

*The granting of permission on the basis of authenticated identification. H.235 (03), 3.3 (ITU)*

*The act of determining if a particular privilege, such as access to telecommunications resource, can be granted to the presenter of a particular credential. J.260 (05), 3.3; Y.1271 (04), 4.3 (ITU)*

[22] *At first glance technical and minor. What's more important is a0 which document are we talking abou 9an ID profile?), b) what's to be in that document.*

### 3.4 Electronic Signatures

In the European law an electronic document is to be taken as "authentic" only a) when it was electronically signed, b) when the electronic signature has been validated by an authorized person.

The electronic signature is an element of proof for the commitment embedded in the signed message or document. As such it may support "non-repudiation".

In some cases an electronic signature may be taken as a "seal" i.e. a feature supporting the "integrity" of the message or of the document to which it is attached.

*"Current situation: diversity and non-interoperability both at the national and international level.*

*Few corporates have direct experience with PKI digital signature with qualified certificates, considered by many experts the most secure system applicable to business transactions.*

*NB In the US, some large bank SSCOM members of the FSTC and the state of Michigan were ready to launch a Federated Identity Management Pilot Project involving transactions and remittance details and are seeking participation by European banks and corporates.*

*SWIFT MACUG banks in France have launched a project to define standard security and digital signature requirements on flows exchanged with corporates.*

*What has been missing in the Electronic signature debate is a pragmatic approach of experienced end users that have precise views of what is needed and what the problems are with the current schemes.*

*Legal Framework: European Directive/ Local Adaptations/ Types of Signature/ National accreditations*

*The e-invoicing Directive does not mandate electronic signature on e-invoices.*

*Each country has established its own rules… Italy, France , etc. In general, continental Europe has chosen to require electronic signature… Some countries, like Italy, require the strongest type…*

*Even worse, they have established accreditation policies and Lists that may be discriminatory and prevent foreign CAs to operate in that country or interoperate" (CAST)*

Electronic signatures & record management

Should electronic signatures be taken as records? The first answer is they should, as they are likely to appear as elements of proof for authenticity, integrity, and commitment.

However it is very unlikely that the integrity of the "signing process" be preserved over time. After a few years a check on the "signature value" itself seems out of question. Only two types of elements will be retained re. the integrity of the signature record and the trace of the original validation process. Both should be sufficient in a litigation process (to be confirmed).

Standards

The current situation is somewhat confusing.

Draft of ISO 22895 proposes a new version of the Cryptographic Message Syntax (CMS) also known as RSA PKCS #7. This is also used in S/MIME of the IETF and RFC 3269 and 3852.

ISO 22895 is derives from ANSI X9.73 (CMS) and X 9.96 (XML CMS).

In the XML representation the result is somewhat different from the one obtained by the W3C for XMLDSIG (electronic signature) and XMLENC (encryption).

In Europe the standard format originated from the EESSI (European Electronic Signature Standard Initiative), is defined in ETSI TS 101 733 and appears in XAdES (a variant of XMLDSIG).

### 3.5 Interoperability

The next stage of operation for identity systems is for them to be able to communicate levels of trust with each other. The current infrastructure is then used to generate new interaction styles and processes.

Each identity system is created with a particular threat model, risk management model, and operational model. Therefore, it is not a given or even likely that each identity system will be able to work totally within the context of another identity system. However, the goal is to re-use the infrastructures in such a way that business threats and risks are adequately addressed, and efficiency of operation is encouraged.

One of the goals of this working group is to facilitate the interaction of identity systems within a global business context.

Some examples of these mechanisms include: PKI Bridges, Cross Certification, Multiacceptance, Policy Mapping.

**Identity systems must provide mechanisms for interaction with each other. They must have ways of presenting identities and credentials in other domains.**

**Identity systems must provide means for determining the policies and practices used in their operation.**

**Interoperability** is a key issue for the IDWG. Like identity, it may be understood in many ways. For experts it is technical interoperability as for others it may include organizational and legal issues.

Technical interoperability is a prerequisite for full operational interoperability. But it is not because your neighbour's sockets are compatible with your shaver or mobile that you are authorized to use them.

An identity is interoperable if it can be read and interpreted by the party who receives it. It does not prejudge of what the receiving party will do with it, i.e. if it will authorize the person to use its services.

The technical view may define the core of interoperability. There are "views" of interoperability[23], which we might actually qualify with other words like:

- **Portability of identities**. An identity is portable if issued by or on behalf of entity X it is used by entity Y. Portability is possible if entity Y trusts the identity issued by entity X. Such trust may originate from a registry or a repository of certificates, based on an evaluation framework shared by entity X and Y. Such registries or repositories are put in place by local governments or business communities. This is a key issue for the IDWG;

[23] *The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged. ITU Y.101 (00), 35*

*The reception and presentation of applications in a vendor-, author- and broadcaster-neutral framework. ITU J.200 (01), 3.1.90*

*The ability of network management products and services from different suppliers to work together to manage communications between managed object classes". ITU M.60 (93), 2088*

*The ability for a certificate to enable functions in relationship with applications coming from different organizations and whoever is the certificate originator. (Ref. doc. Groupe des 5).*

*The ability for heterogeneous services or components to work together. One basic condition of interoperability to enable communication between these services and components is to use of common languages and protocols.*

*For example, SOAP or XML protocoles are standardized and enable different services to exchange information according to the same rules and methods.*

*(Agence de l'administration électronique)*

- **Multi-acceptance of digital certificates**[24] (Mutual recognition of certificates ref. doc. Groupe des 5). The same identity is used along a sequence of different applications across company boundaries.

  Again there are many degrees of multi-acceptance, some of which are within the scope of the IDWG like mutual authentication or digital signature, some of which are not. Defining a general framework for the management of roles, rights, credentials etc. in any B2B application is beyond our scope.

*Portable IBAN*

When the addresses are "portable" the funds can be transferred to another financial service provider without changing the address.

In some instance the address moves to the new service provider and is not prefixed to specific service providers.

*The Telephone Metaphore*

Home telephone numbers may include: telephone numbers home trunk telephone, company trunk telephone, mobile telephone, communicator telephone and PC telephone.

In some countries you can switch operator for mobile, communicator and company trunk telephone without switching numbers.

In the modern telephone systems, mobile and trunk connection have a physical and a logical number.

The logical is the one customers see. The physical number is hidden and just used by the operators.

The same concept works in Internet for domain names and IP addresses of servers.

In those countries( eg Sweden, Norway and Denmark) where you have portable account numbers (generally for corporate customers and entrepreneurs) the design is the same. There is a portable logical IBAN, which the customers tell each other. The banks (ACH) make an automated switch from the logical IBAN to the physical (absolute) IBAN i.e. the customers can open accounts in different banks and get physical (absolute) IBAN addressed, but they can also ask for one portable logical IBAN which they can attach to one physical IBAN at a time. (Of course they can also have several logical IBANs if they so wish for different purposes).

They can then switch the logical IBAN to a new physical IBAN from the start of the next business day.

The idea of the portable IBAN is that corporate customers can start to working with another bank just by attaching the portable IBAN to a new physical IBAN.

In the UK the scheme works with a different set-up. It is the ACH that takes care of the routing during the transition period.

In any case it seems there is always an ACH that does all the rerouting based on the cross-reference table it maintains.The banks may or may not need not to make any modification in their systems.

---

[24] *"Mutual recognition of certificates" (Ref. doc Groupe des 5)*

*At the start of the KMI , interoperability was seen as between certification authorities. But nowadays, the idea of a global root authority seems to have lost his attractiveness except in a facilitating role.*

*What counts is for applications to be able to deal with multiple certificates.*

*Users now understand that it will work in practice only if there are common acceptance policies or rules for their applications.*

*Autrans 2006 (Tutoriel et Atelier Identifiants & Identités)*

*Choice of providers*

With respect to "transferring accounts" from one bank to another. There are many more obstacles than the IBAN. First let's realize that you do not transfer an account, you transfer values from an account in bank A to another account in bank B. The ease and the cost/time of transfer will depend on the contracts you have with bank A and bank B. Theses contracts will bear the conditions applying to such transfer.

A study commissioned by the EC is underway

*Global Interoperability*

Business is becoming more global every day. No longer can the business landscape be viewed simply a city, jurisdiction, or continent – business is now global.

Identity systems have a challenge to provide a system where business can rely on the identity within the global context. Not all identity systems must operate globally or be legally effective globally. There may be many cases where a local identify is sufficient for business purposes.

However, when payments are possible and where electronic payments are encouraged, there is a real risk that particular threats can be exploited in an automated fashion. A primary risk of electronic global commerce is that it is fast and can operate without human (slow and unpredictable) intervention.

**For Identity systems operating globally, there may be local and legal controls placed on such systems, but the focus for business systems is that the identity system be useable in many business contexts.**

**Such Identity systems must operate on open networks.**

*Options for cross borders identities*

Different Digital Identity models exist in Europe…

*Examples of questions:*

*Would major CAs or Intermediaries issuing/checking validity of certificates be prepared to voluntarily validate each other's certificates cross border?*

*Do you see a need to create central policy making and policing entity or bilateral agreements are enough ?.Central policy, perhaps with national specificities, is necessary.*

*NB France is in the process of writing its acceptation policy.*

*Corporates have to deal with one or several CAs*

*Acceptance of certificate can be signed by a validation entity and not by a CA.*

*Interoperability is a problem for the verification not the issuing authority*

*The main question is one of " trust". Banks and corporates cannot trust certificates issued by "unknown: entities , like other corporates.*

*Should there be*

- *A network of trusted CAs, with cross-validated schemes?*
- *A root authority? This does not seem necessary;*

*The creation ,ex-novo, a legal liability scheme and technical interoperability between many different CA and intermediary TTPs.*

*Where to look for? Liberty Alliance?*

*If we concentrate validation why should we have a unique identification?*

*Are we talking on authentication certificates or a unique identifier like IBEI could be.*

*Certification is complex and will remain complex, but if we centralise the complexity in, for instance a validation point, then it will be easy for users and applications which is the interesting goal.*

*Regulation and Professional Standards*

Currently, especially in Europe, there exists regulatory changes, which require interoperability of identity (SEPA, MiFID). The Identity Provider model (Liberty Alliance, SAML 2) will require regulatory assistance (and support from IT security architects), when this interoperability is to occur.

*Signature Interoperability?*

*"Compared to banks, only a few large corporates have the experience and expertise with networks and electronic … " (CAST)*

**3.6 Administration & Control of "Identity-Based" Applications**

*Policy Alignment*

…

*Availability (contingency, business continuity vs attacks, thefts, loss etc.)*

…

*Traceability & Compliance: Assembling the Archive (2)*[25]

A digital signature provides proof of authentication, and it is advisable to store that proof along with the authenticated document. However, a digital signature is not the only item of evidence necessary to establish authenticity, and many general-purpose off-the-shelf products do not gather all the required evidence together. They may also not provide an efficient, easy-to-use way to archive a document with full proof of its authentication as of the time when the user relied on that authentication.

A further archiving problem occurs when certificate revocation lists (CRLs) are the means of validating certificates. CRLs are often voluminous, and may far exceed the size of the authenticated data even though most of a large CRL's content will be irrelevant to any specific signature. OCSP is an alternative validation technology that could eliminate some of the problems of CRLs.

However so far nobody so far seemed to dare implementing OCSP instead of CRLs. OCSP is a possible direction but we cannot make a recommendation without some experience of it. In any case we will have to live with CRLs for several years.

**TWIST enabled services must support certificate validation.**

**The participants in the system must have functionality for assembling and archiving the following for each instance of signed data:**

**(1) The signed data itself (including external documents referenced in the signed data),**

**(2) The digital signature on that signed data,**

**(3) The certificate necessary to verify the integrity and traceability of the digital signature,**

**(4) The response indicating that the certificate is valid,**

**(5) Any other information necessary or important in establishing the reliability of the certificate or the authenticity of the signed data.**

*Audit*

…

[25] *Need to separate the business need from the technologies.*

*Loss/ Damage Recovery*

**Recovery is an immediate need of business and recovery needs to be immediate in terms of vital business recovery:**

The ineffectiveness in terms of time during a "Due process" recovery or due to underestimated 'self-insurance' or the lack of 1st, 2nd and 3rd party commercial coverages for business processing, shows the business need in time of need. Recovery. Redundancy is a must though indefatigable infrastructure will do more.

**The integrity of Identity and ID and of Processing and process must issue intact and as independently-verifiable back, by ,not temporarily to, parties who can represent liability coverage.**

*Risks, Responsibilities & Liabilities: Tracking the Scope of the Risk[26], Variation in Trust Assurance and Risks*

In situations where a certification service provider takes a high degree of risk, the certification service provider must have a way of tracking the actual extent of that risk. Otherwise, the certification service provider's risk managers and insurers cannot assess the scope of the provider's exposure. The validation of a certificate is a fairly good indication that it is being relied on, and that a risk is thereby resulting for the certificate provider. Signing the validation request also helps ensure good data quality and makes the scope of the risk in relation to a specific relying party measurable.

**Where a TWIST enabled service requires a participant to accept a high risk of identification error, the system must provide a reasonable means of tracking the extent of that risk.** [27]

**However, the tracking mechanism must not expose confidential information to the tracker without the consent of the parties to whom the information is confidential.** [28]

[26] *A preliminary question is which risks are addressed.*

[27] *Signed OCSP is one such means.*

[28] *OCSP, whether signed or not, does not expose the content of the signed data.*

## *Conclusion and Recommendations*

This document is a basis for further discussions and detailed work. The first table is a list of recommendations complementing the list of recommendations in the "business requirements" document.

The second table starts outlining the areas where more work needs to be done.

### *Summary Table of Recommendations*

| |
|---|
| As much as possible, from a user perspective, a "simple identity solution" is to be preferred over a more complex one. When one certificate (and one secure device for holding a private key) will suffice, another certificate and private key should not be required. |
| However, a balance is to be found between simplicity, privacy, traceability and resilience of the ID infrastructure. |
| Identity systems must be able to store and manage primary documents and other proofing materials. |
| Identity systems must be able to re-use proofing and vetting systems in an automate fashion to improve economy of operation and reliability of identity. |
| In TWIST enabled services, contracts are the preferred means of establishing the legal basis for an authentication infrastructure. |
| TWIST enabled services must provide an approved stylesheet for the visible rendition of an XML document type, and treat minor variations in appearance as insignificant as long as they are permitted by the approved stylesheet. |
| XML specifications promulgated by TWIST for inclusion by reference in document instances must be online at URIs readily accessible by TWIST users. |
| Different versions of referenced documents must have different URIs. |
| TWIST (or any other publisher of specifications for use in a TWIST enabled service) should make a digitally signed copy of a published specification available on request, together with a statement of the URI at which the specification is published. |
| Identity systems must provide mechanisms for interaction with each other. They must have ways of presenting identities and credentials in other domains. |
| Identity systems must provide means for determining the policies and practices used in their operation. |
| For Identity systems operating globally, there may be local and legal controls placed on such systems, but the focus for business systems is that the identity system be useable in many business contexts. |
| Such Identity systems must operate on open networks. |
| TWIST enabled services must support certificate validation. The participants in the system must have functionality for assembling and archiving the following for each instance of signed data: |
| - The signed data itself (including external documents referenced in the signed data),<br>- The digital signature on that signed data,<br>- The certificate necessary to verify the integrity and traceability of the digital signature,<br>- The response indicating that the certificate is valid,<br>- Any other information necessary or important in establishing the reliability of the certificate or the authenticity of the signed data. |
| Recovery is an immediate need of business and recovery needs to be immediate in terms of vital business recovery: |
| The integrity of Identity and ID and of Processing and process must issue intact and as independently-verifiable back, by, not temporarily to, parties who can represent liability coverage. |
| Where a TWIST enabled service requires a participant to accept a high risk of identification error, the system must provide a reasonable means of tracking the extent of that risk. [29] |
| However, the tracking mechanism must not expose confidential information to the tracker without the consent of the parties to whom the information is confidential. |

[29] *Signed OCSP is one such means.*

*Summary Table of TWIST ID Standards and Projects*

This table is the goal of the document. IT could be structured around formats (identifiers etc.) and process templates (discovery, authorization, electronic signature etc.).

## *References*

NB (more to be added)

Ian Dunning, Portable IBAN's -How to extract even more benefits from SEPA (given on September 18, 2006)

*,Basic Rules for Identification Systems, IEC, 2006 July 17,3_810,

JY Gresser,Short visit to FT deputy treasurer of France Telecom, 2006 June 14

* , Report on a review of international identity proofing and vetting practices and procedures, Annex A. The I-IPF Model and its application, Final 2.0.0,The Zygma partnership LLC,2006 June 10,

*Background information*

K. Rannenberg, Ch. Stenuit (acting editors),Text for ISP/IEC 1st Working Draft 24760 — Information technology –Security techniques – A framework for identity management, ISO/IEC JTC 1/SC27 N5056rev1, 2006 May 13

*Replaces N4721, N5056.*

BFG Security Committee, Contribution to TWIST IDWG, BFG, 2006 April 18

*Response toTWIST IDWG 2*

Eike Wahl (Identrus)(?),Identity Requirements, IDWG Identity Requirements, DRAFT Version 1.0, TWIST IDWG,2006 Apr 10

Roger Shell, PKI Present from FedPKIv, BFG, 2006 March 11

Richard Lee, Technology Components for E-Commerce Transactions, BFG,2006 March 11

Gianfranco Tabasso, Scoping of EACT's CAST* Projects, EACT, 2006 Jan 30

Nick Ragouzis, Advancing a Versatile Interopable Identity Infrastructure for Finance and Services in the EU, Draft, Release 10 Dec 2005, TWIST, 2006 Jan 19

Anthony Kirby, Founder RDUG/Accenture (Chair), Martin Sexton, London Market Systems, DISCUSSION PAPER Version 1.9, The Implications for Reference Data under the Markets in Financial Instrument Directive (MiFID – Directive 2004/39/EC), MiFID Joint Working Group, (JWG), Reference Data Subject Group (RDSG), 2005 Dec 7

Shashi Phoha (Director of Information Technology Laboratory), Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS PUB 201, Federal Information Processing Standard Publication, 2005 February 25

JYG, BFG-TWIST Meeting Notes, BFG, 2004 Dec 17

G. W. Bush (signatory), August 27, 2004 Homeland Security Presidential Directive/Hspd-12, Office of the Press Secretary, The white House, 2004 August 27

Policy for a Common Identification Standard for Federal employees and Contractors

[CARAT Guidelines]: National Automated Clearing House Association, *CARAT Guidelines: Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates* (2000).

[Electronic Signatures Directive]: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *Official Journal* 19/1/2000. (Appended in the Supporting Documents folder).

## *Glossaries*

### French and English

*T*he ITU Sancho data base *http://www.itu.int/sancho/index.asp?lang=en or fr*

now integrated into the ITU-R/ITU-T prototype data base, accessible via http://www.itu.int/ITU-R/index-fr or en.html under News/Terms and Definitions

### English

Liberty Technical Glossary, Liberty Alliance Project: Version: v2.0- Editors: , Jeff Hodges, NeuStar, Inc. , Original Filename: draft-liberty-glossary-v2.0-03.pdf (L.A.)

Digital Identity Glossary, Ranthoughts, Saturday, October 9, 2005, 2:45 PM PDT (updated) (R.)

Oracle Advanced Security Administrator's Guide, Release 8.1.7 (O.)

Identrus System 2.0 Installation, Administration & User Guide (I.)

SG Trust Services- Digital Certification Center- Glossary (SG T.)

### French

Dictionnaire historique de la langue française, Édition de …(Rey)

Grand dictionnaire terminologique de l'office de la langue française du Québec (GDT)

Glossaire de la DCSSI (extraits) -Termes relatifs à la sécurité des systèmes d'information Secrétariat Général de la Défense Nationale webmestre, version du 27-07-2005 (DCSSI)

Projet Adèle 121 Glossaire, Numéro de version : V0.3, Date de dernière mise à jour : 03/06/2005, et

Adele121_Glossaire_V0.3.doc, créé (en ligne) par Bruno DESCHEMPS, Dernière modification le 04/08/2005 15:18 (ADAE)

http://vitamine2.adae.gouv.fr/ministeres/projets_adele/adele_121_gestion_de/public/adele_121_-_glossair/preview_html?file=file&file_html=file_html

Glossaire EDIFRANCE du Commerce électronique etc.(EDIFRANCE)

*Autrans 2006 (Tutoriel et Atelier Identifiants & Identités)*

## *Appendices*

**Regulatory Regime, Expanded** *(to be updated)*

This appendix extends the discussion concerning regulatory necessity. Here we highlight (without much elaboration) the use cases and particular demands latent in the cited Directives, Regulations, and other actions.

1. **New Legal Framework** NLF, Consultation COM(2003)718:
   - removing the basis of the expense and burden objections for reporting by (especially) newcomers to banking transactions;
   - facilitating the joint satisfaction of 95/46/EC with exceptions related to Article 13(d) therein;
   - solution to the problem of non-interoperability in recognition of electronic signatures within existing context of variety in signature technologies, credentialing, and trust domains—offering an operationalization of these concerns (rather than forcing a resort to legislation) and extending current technologies while introducing a basis for innovation and competition;
   - effecting a realizable form of inspection for identity-commerce (derivative of Regulation (EC) 1/2003);
   - assisting in secure and identity-assured establishment of collateral arrangements and associated transfers expanding the form of evidence, removing procedural barriers and administrative burdens (as per Directive 2002/47/EC);
   - avoidance of single registrar solutions for unique identifier challenges, especially honouring Member state rights and controls on local identifiers (of all kinds, from natural persons to equity issues);
   - realizing objectives (including variety and responsiveness in services and vitality of competition) through removal of basis for objections seen in responses (e.g., in Oct 2002 responses MARKT/4005/2002) to number portability, and customer mobility (including handling within the identity network such concerns as standing orders—which could now also be transformed into dynamic orders) while, contrary to claims of degradation in ability to offer timely advice, improving "effective advice," the ability, in advance, to inform beneficiaries of costs, options and so on;
2. **Markets in Financial Instruments** MiFID, EU Directive 2004/39/EC (ISD2):
   - The briefing material for the recent (19Oct05) MiFID JWG make clear how challenges of meeting regulatory requirements in several areas arise when not working with an identity-aware, privacy-enabling infrastructure capable of securely managing multi-valued context-aware attributes, including for example the problem of party identification, and particularly not merely low-order and often fixed attributes (and not only at the time of initiating the business relationship), but dynamic and arbitrarily-extensible attributes, and facilitating context-dependent discovery with the ability to discern roles among other aspects;
   - the challenges of informing clients during pre-trade advice through post-trading, which when taken from at the Directive's broadest view is not merely the problem of sending the data, but of identity-enabling the exchange, to include conditioning on client's at-the-moment choice of notification mode and media, and moreover, to enable customers to insert themselves into negotiations for value-added information services (and joint social networking-style provisioning of such service), which then suggests that fully satisfying the Directive might require an identity-enabled template-based means for specifying instructions (offering options of re-use with multiple parties, perhaps with proxy options) related to selection of venue on parameterized- or fixed-value terms for best execution along with appropriate consents;

- the necessity to deliver this while remaining consistent with requirements for auditing, regulation, and the security of the markets, which touches on other requirements highlighted here;

3. **Industrial Policy**, COM(2005)474 and SEC(2005)1215 et seq:

   - The pivotal role identified for innovation and intellectual property development and protection is significantly dependent on cooperation within and among these enterprises, across sectors, and with external sources of innovation, which is, in turn, significantly dependent on secure identity-enabled services for the necessary collaborations;
   - acceleration of partnering and other enterprise reorganization and cooperation; faster integration of employees in multi-domain and multi-provider programs (e.g., training);
   - as a core feature of product and services designs, offering integration into the identity infrastructure; not solely in aerospace, defence, biotech, medical, or engineering sectors, but also in more traditionally staid domains, such as goods industries;

4. **Payer information accompanying funds transfer**, Proposal 2005/0138:

   - Removing priority to actual account numbers (vs traceable identifiers) while solving the chaining challenge, both in real time (going forward assurances) and in back-tracking;
   - removing the "technology" caveat for intermediates, while not preferring information forward-transport (which counter to suggestion impedes all-important chaining, while also increasing many other data risks);
   - including intrinsic services that enable separable, partitioned, access to elements of the records, on a rapid (near-instantaneous) access and historical basis protected through requirement for joint and multi-lateral keying; under the controlled conditions and terms, enabling chaining and mining across multiple identifiers and in preparatory and consequential transactions and activities;
   - unification with extra-Community payments;

5. **Entry and operation in credit business**, Proposal COM(2004)486 (adopted Oct05), esp. in respect to Act 1 and its annex but generally applicable throughout the discipline of regulatory capital:

   - With general attention to requirements from Basel II in respect to keeping pace with market developments and flexibility, establishing appropriate incentives for credit organizations to move toward more risk-sensitive approaches, to stimulate credit institutions to improve market strategies bringing particular attention to the necessity for real-time information flows within identity-aware and protected framework for, e.g., informing appropriate authorities of shareholder identities (in a way the authorities can directly act on such information) and significant holdings, collection and access to credit conditions of borrowers with granularity in privacy protections controlling information gathering and release (thereby removing barriers, both, to risk control and expanded perhaps innovative offerings) (more directly in CESR advice), providing secure and identity-assured means for a wide range of executory and regulatory activities such that the activities of the credit institutions can safely span the widest possible domains with capabilities for rapid action and reaction;

6. **Shareholder information and rights**, Giovannini Barrier 3, regard corporate actions, esp. in respect to investor rights and activities, including the benefits of offering shareholders effective direct voting and enhancing custodial bank proxy instructions;

   - contact with shareholders, operational on various attributes and purposes yet privacy protected; related to directing and tracking proper communication of information and disclosures in pursuit of assuring freshness (moving from passive

postings to directed active or push publication) and authenticity of disclosures conjoined while guarding against improper disclosures and uses of such information (CESR; Market Abuse Directive 2003/6/EC);

7. **Cross-Border Payments**, among other EC Regulation 2560/2001 and Commission's Consultative contribution of 19Oct05 MARKT/H3 D(2005), esp. regarding continued challenges with identifiers, marking both the need to resolve the problems in the IBAN-plus-BIC scheme beyond just Community banks (2560/2001 targeting *retail* charges as much as bank-to-bank operation), where a versatile identity infrastructure could allow essentially arbitrary customer-level identifiers, facilitating resolution to this challenge while also serving in issues of number portability, customer mobility, flexibility and further options in directing payments and settlements, providing access to delayed information, and so on;

    - as elsewhere, merely satisfying 'clear and timely' communications as compared to meeting the Directive's larger goal of using these communications to realize stronger competition for customers, and enabling customer choice and action (including seeking alternate solicitations) in such communications;

8. **Data protection**, in various respects, including directives and requirements deriving from the Data Protection Directive (95/46/EC), DPD, the Telecommunications Data Privacy Directive (96/77/EC) the Electronic Communications and Privacy Directive (2002/58/EC), including the perhaps most vexing long-standing challenge of balancing societal security with personal protections (for example the challenge of balance for DPD's Article's 6, 7, and 13) where a versatile identity infrastructure provides a way to successively move data out of the reach of inappropriate commercial uses, then a succession of types of data holding for security purposes, while also providing a de-identified yet still integral data source for managing network services; providing real-time management of unambiguous consent to directory information, including self-management and publishing of data limited only by customer choice (such choice being in any of the data dimensions, the requesting context, the automation of such as subscription to updates, customer election of data use solicitations, application of agency to such choice, and more);

    - ability to support a plurality of identifiers, including opaque or limited-time identifiers and anonymous service provision, within any context as part of a chained but not parlay-able service thereby providing further protections (in this way addressing, finally, the technical environment impediments mentioned as early as the European Commission WP6 March 1997, leading to still pervasive notions about the (im)possibilities regarding anonymity under Internet technologies, and the unhelpful embedding or direct association of extended attributes with PKI certificates);

    - beneficial reduction of the artificial distinction between natural persons and legal persons for legitimate interests, while increased protections against abuse by legal persons (the necessity of agency action on behalf of natural-person customers, for example);

    - consistent with variety in service offerings, personal choice and safety, and societal security concerns, enabling simultaneously-variable identity-conditioned (requestor, relying party, targeted identity, etc) responses to highly personal context data (such as presence, geo-location);

recognition that an identity infrastructure adds a new services layer that performs as though it is located between customer terminal equipment and any given end service, forming a new kind of data class requiring protection and that is protected under the versatile identity infrastructure.