Business & Technical Requirements
for Identity Management
in an Interoperable & Electronic Environment

1. Purpose of this document

The purpose of this document is to collect the business requirements and technical requirements for identity management in an interoperable and electronic environment.

Ultimately this document will be presented to the TWIST Identity Management Working Group (IDWG) who will recommend next steps to the TWIST Executive Team.

The purpose of the IDWG is to deliver a framework that will enable the implementation of secure and interoperable identity infrastructures.

The goal is secure, assured and compliant electronic communication between business parties and their banks both inside and across borders.

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

This paper proposes the requirements for such architectures.

2. Terminology

For the purposes of this document, a number of key terms need to be defined. Where useful, these definitions are also complemented with a number of observations or characteristics.

Identity: An identity is the set of properties of an entity that allows the entity to be distinguished from other similar entities (identification, authentication), and /or to be authorised to engage into specific activities (authorisation). An entity can be a person, a legal entity (e.g., a corporation) or an object (e.g., a machine).

Identifier: An identifier is a set of data elements that distinguish an identity from other similar identities. Therefore, an identifier is a signifier (?) for an identity. Examples of identifiers are name, social security number, tax number, username, IP-address.

Authority: Authority refers to the right of an entity to perform specific activities.

Identification: Identification has two meanings:

it is the process by which an identity is given and registered

it is the “visualisation” of an identity, i.e. the process by which an entity is distinguished from other similar entities.

Authentication: Authentication is a process that will enable a relying party to verify two things:

the identity of an entity

the authority of an entity

Authorisation: Authorisation has two meanings:

1. it is the process by which the authority of an entity is defined (syn. habilitation)
2. it is the process by which the owner of authority is granted actual permission to engage in the activities specified under their authority.

Relying Party: A relying party is an entity that will rely on the identity and authority of an entity to allow them to perform certain activities (e.g., access to services).

Interoperability: The relying party may be “outside” the “jurisdiction” of the party that issued the identity and authority, Interoperability means that the following two conditions are fulfilled:

The identity can be read and interpreted by the relying party (technical interoperability)

The relying party will authorise the identified entity to engage in the requested activities (full operational interoperability).

Portability: an identity is portable if issued by or on behalf of a party it may be used by another party (in a different environment). Portability may be synonymous to interoperability.

Multi-acceptance: the same identity is used along a chain of different applications, possibly across company or community boundaries.

Identity infrastructure: An identity infrastructure is an occurrence of architecture, policies, operational and management activities, hardware and software, that covers the lifecycle of identities and their consumption.

Identity life cycle: The life cycle of an identity is composed by the processes that relate to the management of that identity (e.g., issuance, maintenance, revocation etc.).

3. Background

Businesses of all sizes are faced with the growing power of their customers. These customers are increasingly demanding more freedom of choice for accessing to products and services across borders, and to service providers across borders. In Europe, these requirements are supported (encouraged?) by regulation (e.g., MiFID, SEPA).

Today the growth of traffic and the number of connections on both the Internet and professional networks substantially multiplies the risk factors. Consumers, merchants, trade services providers, logistics providers and financial services providers will be able to sustain this new economic growth and reap its benefits only if technology enables them to behave in a more responsible way:

1. For individual users who are acting within their private or professional environment, anonymity is unacceptable , and
2. Users must be able to depend on real guarantees given by the providers of web services.

This means that complex networks that are taking shape on a global basis must cope with issues such as liability allocation, liability control, auditability, associability and socialisation of risks (insurability), which are all included in the modern vision of traceability.

The key to traceability is the “identity”. In the electronic world, identity is synonymous to digital identifier*(NB there should be a sign like * telling the term is defined in the glossary).

In today’s environment, corporates are having to deal with as many identity frameworks as they have trading partners and as many islands of policy and regulation as there are countries in which they do business.

It is in this context that TWIST set up the IDWG to address the critical concerns of this challenge: the assignment of risk and the assurance of trust in the context of multiple and highly-mobile trading partners across the financial supply chain.

4. Identities: the Requirement for Global Interoperability.

4.1. Introduction: Identities and identifiers in the Banking Industry

Corporates are rolling out infrastructures for the management of the identities of their employees. Today interoperability of these infrastructures with partners, suppliers or customers is still on the agenda of only a few companies. However the development of electronic trade in Asia and between Asia, Europe, North America etc. is likely to trigger a wave of secure “interconnections” across continents.

Banks have already deployed local, regional and global infrastructures. For inter-bank transactions these infrastructures are multilateral and entertain many-to-many trusted electronic communication. With respect to their corporate customers, the banks only operate bilateral models.

In the paper world, access to bank services is made possible by presenting financial credentials borne on a plastic card or in paper form. These credentials are often supplemented by

- a personal ID
- a hand-written signature
- and/or a second form of financial credentials.

When doing business electronically, obviously electronic equivalents of paper-based identifiers and identification mechanisms have to be established.

In the banking industry there is a strong relationship between personal identities and bank account numbers. Strictly speaking, an account number identifies an account and not a person. An account indeed has its own identity. Sometimes a bank account is accepted as identification of the account owner, but mostly additional means of identification are needed (e.g., electronic signature).

In some cases, account numbers are combined with “routing” information to facilitate the automated routing of instructions to the correct account. The classical example is the combination of IBAN and BIC. Given that the IBAN does not uniquely identify a bank account in some countries it needs to be complemented with routing information, in case an identifier of the account servicing institution (in this case, that institution’s BIC).

As you may use several payment means, moving information along different routes, a bank account may have several parallel addresses. For example, the domestic account number (BBAN), the international account number (IBAN), the number of a debit or cash card attached to the account, a mobile phone numbers (in the case of mobile payments. Finally, customers typically have several accounts, open new accounts often and close existing accounts.

4.2. Requirement for Multiple identities

Multiple identities are not specific to the banking industry.

Currently there is a double trend in the corporate context:

- to separate personal from professional “attributes”,
- to issue professional identities to individual employees.

This trend bears a strong relationship with Privacy & Data Protection Laws & Regulations: Personally Identifiable Information. Although one digital identity per person would be economic, it may not always be possible in the case of individuals. Data protection laws in Europe as well as privacy and safety rights generally give an individual the right to limit disclosure of their personal information. Multiple certificates, including pseudonym certificates, may be necessary where individual privacy rights leave no better way for the required protection to be realized.

Particularly with respect to personally identifiable information, the subject of the information must retain control over the dissemination of the information to third parties, including dissemination by means of certificates and other electronic means.

Multiple identities/certificates per individual are necessary in order to realize the required degree of personal and business control.

4.3. Requirement for simplicity for the end-user: extending the reach of a given identity to the whole spectrum of financial services & beyond.

Corporates, irrespective of size aim to use the same standards, processes and infrastructure with all of their financial services providers This requirement addresses the reality that even small corporates often have multiple accounts with multiple banks.

With respect to the ability to use the same infrastructure, a significant requirement is the ability to use an established identity with multiple banks. Indeed, if a corporate has established an electronic identity with a particular bank, it should be possible to use that same identity with other banks.

Whereas this may already be the case in a few European countries, it is not pervasive and certainly does not exist for cross-border transactions.

Let's look at an example: in "post-shipment reverse factoring" it is highly likely that the beneficiary of the financing is not a customer of the finance provider. If however the identity that the beneficiary has already established with another financial institution could be "re-used" by the finance provider, this would greatly contribute to manage the risks involved and to increase the efficiency of the process.

Furthermore, doing business electronically is becoming more global every day: electronic communication is not bound by geographical barriers, functional barriers or community barriers. Indeed, customers can easily engage in electronic business across geographical borders, across industries and across user communities (e.g., the connection of different e-invoicing platforms).

Communication across these borders raises questions about the "cross-border" recognition of identity and authority. Currently the solution is to establish identity and authority on a "bilateral basis" between the customer and the supplier or on a multilateral basis between a user and an electronic platform with multiple users. The requirement that TWIST is articulating is the acceptance of identity and authority across "jurisdictions". For example:

1. Is a UK certificate acceptable in another country?
2. Is identity established in one value-added network acceptable to another value-added network?
3. Is established in one e-invoicing platform acceptable to another e-invoicing platform that is connected to it?
4. Is a certificate established with Bank A in Country X acceptable to Bank B in the same country?

Of course it is so that not all identity systems must operate globally or be legally effective globally. There may be many cases where a local identity is sufficient for business purposes. However, the requirement remains for "cross-border" (geographical, functional, community) acceptance of identity and authority. In other words, what are the conditions under which identity and authority are interoperable or portable across boundaries?

Identity and authority must be interoperable across geographical, functional or community-related boundaries.

At the same time, this means that identity management systems (identification, authorisation etc) will have to be able to deal with portable identity and authority. Additionally, these systems will have to be protected from fraud and will have to comply with local and international regulation.

5. Managing Identities: the Requirement for Trust across Domains and Systems

5.1 Introduction

In the perspective of "truth in what happens", the rapid rise of Internet functionality and demands for "openness" often stand in the face of propriety, prudence and common sense. Loss of control, attacks, failures etc. expose any business to:

- Inconvenience, distress or damage to standing or reputation,
- Financial loss or liability,
- Harm to persons, facilities, activities or interests,
- Unauthorized release of sensitive information,
- Civil or criminal violations.

"Identities" are key tools for:

Better controlling ones operations or practices (assigning and controlling roles/responsibilities, business continuity etc.),

Building trust with business partners (via a better liability allocation and control etc.)

Complying with laws and regulations.

5.2 Control of operations and practices

5.2.1 Assigning and controlling roles/responsibilities in Corporations

The business entity of particular interest to TWIST is the corporation. The corporation creates, owns, bestows, and removes identities, roles, and attributes through an identity system.

Identity systems must recognize the central role of a corporation in managing its identity resources.

Identity systems must provide and protect corporate identities.

5.2.2 Employees

A person who is in the employ of a corporation needs some identification for operation within a business context. People by nature have many aspects to their lives; one of those aspects is as an agent of the corporation acting in a role within the enterprise.

Not all employees are authorized to represent the corporation in every action. The roles and authorisations 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.

Identity systems must provide identities appropriate to employee function and roles within the corporation.

Identity systems must acknowledge the personal privacy of individuals in their operation.

Identity systems must prove the identity of an individual in the context of the corporation and his role in the corporation.

5.2.3 Business continuity

5.2.3.1 Reliability

Businesses need reliable processes in the IT space—processes with *verifiably correct operations*. This is not true today. In the abstraction between pen-and-paper business processes and electronically mediated business processes an entire new universe of exposures and vulnerabilities have just started to surface.

"Open" commercial exchanges, especially those of value, need to be given effective and measurable protections.

5.2.3.2 Confidentiality

Business' information flows need to be treated with confidentiality. This means that procedures and mechanisms must be in place to guarantee this confidentialityinside the business community as well as outside. Unauthorised individuals must be barred from unauthorised access to information flows.Systems and applications that process the information flows must be protected.

In this context, information has to be understood in its widest possible sense. Consider the following non-exhaustive list of examples:

- Documents;
- Transaction data;
- Static data;
- Business process and procedures documentation;
- User manuals;
- Passwords and access codes;
- Cash and stock records.

Procedures and mechanisms must be in place to guarantee confidentiality of information internally as well as externally…

5.2.3.3. Integrity

In addition to confidentiality, integrity of information must be guaranteed too. This is achieved by putting procedures and mechanisms in place that

Prevent unauthorised access to systems and data

Prevent unauthorised creation of and modifications to data

Procedures and mechanisms must be in place to guarantee integrity of information.

5.3 Trust between Business Partners: Accountability, Liability Allocation and Control.

5.3.1 Trust

A relying party across the Internet needs to know or to be able to evaluate its own processing commitments, risks and liabilities as well as those of the other participants in a business transaction.

5.3.2 Accountability

Businesses that are transacting with each other need to understand respective accountabilities and how liability is allocated. For the allocation of liability, the identity of both individuals and processes needs to be verified. Additionally, mechanisms need to be put in place, which produce verifiable liability allocation.

Procedures and mechanisms must be in place to produce verifiable liability allocation.

5.3.3 The Role of Banks

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 government agencies. There are proscribed boundaries under which banks operate.

In the current political climate, criminal use of money has become a major focus of legislatures and government regulators. As banks play a major role in the movement of money, they are an ideal candidate to exert control on the flow of funds. Consequently, they are responsible on a global basis for knowing who their customer is (Know Your Customer – KYC).

Furthermore, corporations of any size will have accounts with banks. Therefore, banks are also in a good position to establish, verify, proof, and vet the identity of corporations.

There is a role for banks in the establishment, verification, proofing and vetting of the identity of corporations (including their agents and contractors)…

5.3.4. Auditability

Auditors have a special role in business communications and transactions. They provide the underlying trust for the whole environment.

Identity systems must be auditable. Identity systems must provide mechanisms for the auditing of transactions at every stage of their lifecycle.

5.3.5. Loss/ Damage Recovery

In case of damage to or loss of identity, a recovery process must be used. The recovery process itself must be independently verifiable by parties who can represent liability coverage.

An independently verifiable identity recovery process is required.

6. Laws and regulations: Enforceability and Compliance.

6.1. Legal Enforceability

In a business environment, Identities are used for actions that legally bind the corporation. Therefore, Identities must be legally enforceable across all organisations and locations involved in the interactions.

Together with legal enforceability, regulatory compliance requires technical components that operate based on validated and corroborated electronic policies—not paper policies or legal forms that are asserted to have been in place after the fact.

Identities must be legally enforceable across all organisations and locations involved in interactions.

6.2. Building on Solid Grounds: Legal Basis for an Identity Infrastructure

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.

However, contracts cannot ignore the local legal framework or the international treaties.

Besides, there have been efforts from government and professional institutions to establish reference frameworks or “standards”. This is what TWIST itself is trying to do.

However, for example within the EU, the framework established in the [Electronic Signatures Directive] is useful as a backup or failsafe, should any problem with contract formation occur.

Contracts are the preferred means of establishing the legal basis for an identity infrastructure. It is assumed that at this point a multi-lateral contract is a key ingredient to the establishment of interoperability between different trust environments.

A multi-lateral contractual environment is required for the establishment of interoperability between different trust environments.

6.3. “Closed System”

A main difficulty with a contract-based infrastructure is for it to cover all potential relying parties. When building applications, it is important to determine the extent of the user community and to provide a way of ensuring that only contractually bound members of the user community participate in the system.

An exception may have to be made for governmental entities however. They may only accept statutory compliance as the measure of reliability in digital authentication.

As much as possible, an identity infrastructure must bring all foreseeable relying parties into the participant community that is contractually bound to conform to the infrastructure rules & policies.

An identity infrastructure must bring all foreseeable relying parties into the participant community that is contractually bound to conform to the infrastructure rules & policies…

6.4. Interoperability: Overlapping Communities

Obviously, a user may belong to more than one contractually defined user community. However, one contractual infrastructure may not recognize, or accord validity to the other.

Compatibility between identity infrastructures may arise from a common "scheme', a set of paradigms and requirements, applying to different infrastructures and enabling them to interoperate (e.g. the Liberty alliance).

Furthermore, each relying party should be in a position to accept or reject the identity/certificate of another participant from another identity infrastructure.

This should be based on a common certification or evaluation framework ("referential"). This framework can be spelled out in a multi-lateral contract between the participating "compatible" identity infrastructures.

An Identity infrastructure should be in a position to check the "compatibility" of another identity infrastructure.

Each relying party should be in a position to accept or to reject the identity/certificate of another participant from another community.

6.5. Compliance

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

Identity systems must be sufficiently strong to provide assurance to regulators. Identity systems must be capable of demonstrating compliance to regulation.

6.6. Satisfaction of Legal Requirements for Authentication

Contracts, processes or infrastructures cannot guarantee the validity of a transaction or of a document in court. They may just provide elements of proof. These elements will be considered only if they are produced within specific "schemes" or "frameworks". These schemes or frameworks may be of general interest or restricted to a specific domain. They may refer to best practices in specific areas.

An identity infrastructure should provide elements of proofs with respect to the validity of a transaction or of a document in accordance to the law applicable to the business community or to a specific transaction/contract.

An identity infrastructure should provide elements of proofs with respect to the validity of a transaction or of a document in accordance to the law applicable to the business community or to a specific transaction/contract.

6.7. EU Compliance is Advantageous

Compliance with the [Electronic Signatures Directive] is optional but certain legal and policy outcomes follow if the parties opt to comply. As noted above in relation to authentication requirements, compliance enables an application to satisfy governmentally imposed requirements, which tend to follow statutory lines (albeit those specific to one member state). Compliance also ensures harmony with the overall PKI policy direction of Europe.

An identity infrastructure must be qualified and accredited or recognised as such by an EU member state “certification”.

An identity infrastructure must be qualified and accredited or recognised as such by an EU member state “certification”

6.8. Electronic Digital Signature

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.

An electronic digital signature may provide elements of proof e.g. for authentication, integrity or even non-repudiation. It is advisable to store that “proof” along with the signed message or document. However, a digital signature is not the only item of evidence necessary to establish authenticity.

The current situation: diversity and non-interoperability both at the national and international level.

In Europe the e-invoicing Directive does not mandate electronic signature on e-invoices. It is one of three options.

Each country has established its own rules including accreditation policies and lists that may be discriminatory. This calls for more standards.

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).

6.9. Tracking the Scope of the Risk, Variation in Trust Assurance and Risks

Overall, wide variations in the quality and security of identification used to gain access to information resources and other facilities need to be avoided. That is because of a need to enhance security, increase (Governance) efficiency, reduce fraud and protect personal privacy.

This calls for secure and reliable forms of identification that:

- **ARE ISSUED BASED ON SOUND CRITERIA FOR VERIFYING AN INDIVIDUAL EMPLOYEE’S IDENTITY**

- **ARE STRONGLY RESISTANT TO FRAUD, TAMPERING, COUNTERFEITING AND TERRORIST EXPLOITATION**

- **CAN BE RAPIDLY AUTHENTICATED ELECTRONICALLY**

- **ARE ISSUED ONLY BY PROVIDERS WHOSE RELIABILITY HAS BEEN ESTABLISHED BY AN OFFICIAL ACCREDITATION PROCESS.**

A thoroughly thought through “Scheme” is required that would then be implemented as a multi-lateral contract between participating parties. Such a Scheme needs to ensure flexibility in selecting the appropriate level of security for each application” and needs to be able to be adjusted dynamically (e.g., the EC project Serenity).

7. Technology

7.1 A Note on Digital Certificates

Digital certificates are often referred to as *"digital identities.*This may be misleading. In a business environment, certificates are data objects issued by or on behalf of a company to its employees or other entities for accessing to information or services. Both information and services may be internal or external to the company (e.g., web services).

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 person or the other 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 (like supply chain, treasury services).

7.2 Capturing and Managing the Identity Life Cycle

The identity life cycle consists of a number of underlying processes to do with the management of the identity (?). Several attempts are currently carried out to model these processes. For example, ISO/IEC J1SC has identified the following elements as composing the identity life cycle:

- Identity choice, provisioning and enrolment
- Identity authentication
- Binding identities with attributes
- Identity certification
- Identity change
- Unbinding of attributes from identities
- Identity revocation
- controls

The quality of an identity infrastructure will derive from:

The processes that form the life cycle of the identity (e.g., creation, maintenance etc.)

The processes that can be built around it and that are to do with the consumption of the identity (e.g., authorisation, authentication etc.)

The consumption of identities assumes that valid identities are "at hand" - i.e., that underlying identity management processes covering the identity life cycle were put in place.

7.3 Identity Management and Application Service Providers

The following are examples of processes that take place once a customer has located (discovered) an application service provider:

- Along with the electronic transaction, the customer passes the identity that was provided by the service provider.

- The service provider authenticates the customer: he verifies whether the identity is valid for this customer).
- The service provider gathers information from the identity to perform authorization and process the electronic transaction.

The same processes with the involvement of an identity provider may look as follows:

- The customer uses his existing PKI Identity to “log-on” to the service provider’s application,
- The service provider authenticates the customer with the identity provider.
- The service provider receives identity information (attributes) from the identity provider that the customer has authorised the service provider to see.
- Based on this information, the service provider authorises and processes the electronic transaction.

7.4. Public Key Infrastructures

7.4.1. Capitalise on existing investments

The current technology consists of established and deployed public key infrastructure (PKI) schemes and technologies. Usually, these schemes are either internal to an organization (e.g., VPN system) or external under uniform rules and procedures (e.g., Bolero, IdenTrust).

Building on current identity management platforms is an essential need and requires a consistent approach with a valid basis, if costs and benefits are acceptable to business.

Current technology infrastructures are to be used as a basis for further development if costs and benefits are acceptable to business.

7.4.2. Public Key Infrastructure (PKI) components

PKI infrastructures contain the following components:

Certificates

X509v3

Trusted Third Parties

Registration Authorities

Trusted Time Stamps

Certificate Status Services

7.4 Extensible Identity Management (NB There is a whole universe around identity centric architectures)

The ultimate goal of identity systems is to have a ubiquitous set of easily understood mechanisms that would provide a transparent means of transacting business.

Identity systems must provide a means, plan or technology to move toward an extensible identity management systems.

Identity systems should be deployed in such a way as to be re-useable within the context of an extensible identity management system.

7.5. Distributed Validation

Distributed validation reflects the need to validate at the end-points i.e. by each participant. Distributed validation must be able to be carried out without additional connectivity.

7.6. Interoperability

7.6.1. The need for interoperability

Interoperability refers to the ability of companies and customers to uniformly resolve integrity and trust requirements at the end-points, not as a function of connectivity to a single or multiple external sources.

Interoperability often constrained by proprietary commercial interests is more than a single subscription to X.509 digital certificates. Standardised representation bodes well and leveraging existing technology components for that representation within digital certificates where a common and consistent representation that has verifiably reliable content, would allow the almost anonymous entity to participate in processes like RFP (the wording is still very technical!).

7.6.2. Pervasive Secure Interoperability PSI

While many IT and business sectors have surfaced many requirements over the years, businesses unlike technology has a basic set of needs, some of which depend upon the integrity of representation (truth in advertising) and the reliability of exchange (fail-secure).

IT then needs to assure businesses that the platforms, IDs and processes can be trusted, with clearly specified limits within which trust is warranted.

Internally verifiable and electronically processed metrics are a must.

Effective and secure processing from the end-points are more a reality than a capability.

Pervasive Secure Interoperability is a fundamental business need both in functionality and integrity. What are electronically mediated processes and identities if they do not exhibit integrity?..

7.6.3. A misconception about cryptographic identifications

A common misconception about cryptographic identifications is that they can be resolved in and via applications. Service providers have had difficulties allowing interoperability of identity across services and applications, even though the exact same technology is being used in most implementations (X.509 v3 certificates). It is believed that this is because service providers do not use a common approach (?) to identity management.

7.6.4. Reliance-Side Assurances Besides Validation

If participants in a particular system cannot agree on a single level of trust assurance for relying parties, the system must provide a means for a relying party to specify its requirements and obtain the level of trust assurance that it requires (assuming that the

market can provide that level of trust assurance). There are techniques that can provide each relying party with the authentication and authorization assurance that they require without having to agree on a common level throughout the user community.

7.6.5. Preference for Centrally Administered Encryption

Although it is technically feasible for each individual in a company to have an individual encryption capability, administering a large number of such capabilities is difficult, in part because safely keeping a copy of each individual's decryption key is the only way to prevent unwanted destruction of data. Individual encryption capabilities are necessary only where highly granular intra-company confidentiality is necessary. Often it is not, and centrally administered encryption, such as SSL/TLS encryption, provides adequate assurance of confidentiality while being much easier to administer.

Systems should avoid designs requiring individual encryption capabilities for each employee. Instead, SSL/TLS or other centrally administered encryption capabilities are preferable.

The level of centralization needs to be defined per company, per business environment

7.6.6. Technical Compliance: Encryption Regulation

The export, import, sale, and/or use of encryption technology is regulated in most countries. It is best to rely on technology providers to comply with these regulations, which are often complex and somewhat discretionary.

Systems must rely on commercially distributed encryption technology rather than on bespoke development of encryption solutions.

7.6.7. Prevailing PKI standards *(too technical?)*

There seems little need to re-invent the standards generally used for public key certificates, such as ITU X.509 and IETF RFC 3280 (certificate content) and IETF RFC 2560.

All certificates used in a TWIST system should be as required in ITU X.509 and IETF RFC 3280. All OCSP requests and responses should be as required in IETF RFC 2560.

Summary Table of the Business Requirements

Multiple identities/certificates per individual are necessary in order to realize the required degree of personal and business control.

Multiple Identities / Certificates are necessary in order to realize the required degree of personal & business control.

Identity and authority need to be interoperable across geographical, functional or community boundaries.

Identity systems must recognize the central role of a corporation in managing its identity resources.

Identity systems must provide and protect corporate identities.*

Identity systems must provide identities appropriate to employee function and roles within the corporation.

Identity systems must acknowledge the personal privacy of individuals in their operation.

Identity systems must prove the identity of an individual in the context of the corporation and his role in the corporation.

“Open” commercial exchanges, especially those of value, need to be given effective and measurable protections.

Procedures and mechanisms must be in place to guarantee confidentiality of information internally as well as externally.*

Procedures and mechanisms must be in place to guarantee integrity of information.*

A relying party across the Internet needs to know or to be able to evaluate its own processing commitments, risks and liabilities as well as those of the other participants in a business transaction.

Procedures and mechanisms must be in place to produce verifiable liability allocation.*

There is a role for banks in the establishment, verification, proofing and vetting of the identity of corporations, including their agents and contractors.

Identity systems must be auditable. Identity systems must provide mechanisms for the auditing of transactions at every stage of their life-cycle.

An independently verifiable recovery process is required.*

Identities must be legally enforceable across all organizations and locations involved in interactions.*

A multilateral contractual environment is required for the establishment of interoperabilitybetween trust environment.*

An identity infrastructure must bring all foreseeable relying parties into the participant community that is contractually bound to conform to the infrastructure rules & policies.

An Identity infrastructure should be in a position to check the “compatibility” of another identity infrastructure.

Each relying party should be in a position to accept or to reject the identity/certificate of another participant from another community.

An identity infrastructure should provide elements of proofs with respect to. the validity of a transaction or of a document in accordance to the law applicable to the business community or to a specific transaction/contract.

An identity infrastructure must be qualified and accredited or recognized as such by an EU member state “certification”.

Current technology infrastructures are to be used as a basis for further development if costs and benefits are acceptable to business.

Identity systems must provide a means, plan or technology to move toward an extensible identity management systems.

Identity systems should be deployed in such a way as to be re-useable within the context of an extensible identity management system.

References

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

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 to TWIST IDW 2

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

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 Interoperable Identity Infrastructure for Finance and Services in the EU, Draft, Release 10 Dec 2005, TWIST, 2006 Jan 19

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