Proposed Top Level Business Requirements for Identity Management in TWIST Standards and Projects

The Market Pressure (Customers, Regulators, Competitors)

Version 1.0

November 25, 2006

Foreword

"The IDWG purpose is to deliver a framework, which 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.

Identity infrastructures are occurrences of architecture, policies, operational and management activities, hardware and software, that cover the lifecycle of identities and their consumption."[1]

This paper proposes the requirements for such a framework from a business point of view. The purpose is to ground the requirements in the business realities of what TWIST is undertaking. It is aimed at understanding what TWIST's business objectives demand of the underlying identity infrastructure in order for it to be serviceable for *e.g.* bank mandates, payments within SEPA, and supply chains.. Its purpose is to channel a discussion.

"Technical" requirements will follow in a separate document.

The Terms of Reference of the IDWG state TWIST's business objectives for IDWG purposes as including "the challenges of responsibility and liability", "dynamic [document] processing", "flexibility in designating…service providers", and "variations in trust assurance and risk". Those topics have prompted the points made in this proposal.

In framing the IDWG's consideration of requirements, this paper divides the subject matter into points that seem likely to require discussion and those that may require little or none (marked R) because they are thought to be rather widely accepted. The resulting compilation is not exhaustive, and more points could be added by the IDWG as the discussion progresses.

History

The first draft of this document V0.1 was prepared by IdenTrust. This version V 0.3 and the preceding V 0.2 were edited by J.Y. Gresser, cochair of the IDWG, which work is supported by InterComputer. This version 1.0 takes into accounts further comments received from IDWG members and correspondents on behalf of corporates, financial services providers and solution providers. Chapter 2 and chapter 3 of version 0.2 are now embedded into a separate document outlining the areas, which will be scrutinized by the IDWG.

Comments are highly welcome!

[1] *Adapted from the IDWG Terms of Reference V5.*

List of content

Introduction

"To small, medium, and large businesses across Europe, the challenges of pan-European business share a significant common factor: the emerging power of, and increased responsibilities for the customer.

Businesses of all sizes are faced with the increasing power of their customers. These customers are increasingly demanding free access to products and services across borders, free access to service providers across borders. In Europe, these requirements are increasingly supported by regulation (e.g., MiFID, SEPA).

Today the growth of traffic and connections on Internet and professional networks substantially multiplies the risk factors. Some risks are known, more are to be discovered. Consumers, merchants, trade, logistics and finance service 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.To start with individual users, acting within their private or professional environment- anonymity is unacceptable , and

2.To depend on actual guarantees given by Web service providers, either state or private controlled.

This means the complex networks, which are taking shape on a global basis must cope with issues such as liability allocation and control, auditability, associability and socialisation of risks (insurability) which are all included in the modern vision of traceability[2].

The key to this traceability is the "identity", actually a digital identifier (a set of data that may apply to individuals, a constituent in a legal entity or an organisation, or an object).

However, 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 Identity Working Group 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.'[3]

What is an "identity" used for?

-To a person (ultimately), it is a pass to a variety of services, internal and external to a company;

-To a "business resource" or a service, it is an "address", a key for access or performance;

-To managers and auditors, it is a tool for administration, traceability in a broad sense and risk containment.

An "identity infrastructure" must provide an adequate response to these very broad and basic requirements. Adequate means proportionate to the set of challenges, which the business have to face.

In the TWIST context:

The goal is to reap the benefits of dematerialization of business transactions administration Financial Value Chain and Straight Through Processing, and… Bank Account Management

(adapted from Scoping of EACT's CAST-Corporate Action on Standards- Projects).

While we examine the various issues. It is important to bear in mind the 2006 state of the art.

In the business environment, corporates are rolling out management infrastructures of their employees identities. This may go with the deployment of a PKI, but not always. Interoperability of these infrastructures with partners, suppliers or customers is on the agenda of a few companies working in the Defence area, pharmaceutical and finance.

[2] Not to forget that this traceability may be in contradiction with privacy.

[3] *Adapted from the IDWG Terms of Reference V5.*

At the same time governments, state administrations and healthcare institutions are defining and will deliver identity cards or credentials/token etc. which might apply to specific domains or might extend, at will, to applications beyond state or local administration services.

Banks have already deployed local, regional or global infrastructures. But these infrastructures are mainly for inter-bank transactions and very few are actually open to corporates. When they do so, they are restricted to bilateral transactions between a treasurer and one bank.

While we look at risk, we should recall that “identity theft” is, by far. the most published (thanks to State laws) security breach in the US. There is unfortunately little information of what is actually going on in other parts of the world. Banks already took measures against e.g. spoofing or phishing.

We can learn from theses measures that the quality of an “identity infrastructure” derives from:

-its build-in processes, as well as

-the processes that can be build around it.

These will be addressed in chapter II.

Section 1 of chapter I will take the (corporate) “user” point of view. Section 2 will address issues for the financial service providers. While section 3 will deal with responsibility and liability of all parties.

1. Identities: Content & Reach

In the paper world, the access to bank services is made possible by presenting, to bank personnel or to the representative of any other party, personal or company financial credentials (born on a plastic card or a paper-form), often supplemented by a personal ID, one hand-written signature (at least) and/or a second form of financial credentials.

Financial credentials bear security tokens. Nowadays with cards, whether there are ordinary plastic or smart cards, there is an off-line or on-line dialog with a machine that will ask you beyond “what you possess” or “have”, “what you know” (typically a pin code or password) and sometimes “who you are” (e.g. via a biometric device).

In the e-business world, the situation bears a lot of similarities, with the use of Identifiers and passwords. Biometrics is not quite there. There are big differences though. “Presence” is an issue. In real time presence may be acertain, while it cannot in batch mode.

In any case it is important to remember that in the e-world we are dealing with “digital representations” (you certainly remember the famous caricature “nobody knows I am a dog”) whether we want them to stay in real life or “play” in virtual worlds. This gives rise to specific risks we have to deal with.

Let us not forget that our aim is to fully exploit the broad opportunities of transacting across sectors and across borders.

1.1 You said "bank ID"?

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[4].

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[5] (or identifiers[6]):

-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.

[4] 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".

[5] (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)

[6] (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.)

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

There is however 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[7]. 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.

The current ambiguities between a person’s identities, bank IDs and bank account numbers should be resolved.

In the following, we will deal with “identities”, attached to a person, a group (often referred to as “generic identities”) or a company.

Identification/discovery of resource or services is the purpose of section 2.

1.2 Identity: Personal or “Generic”? Meaningful identities or pseudos? Multiple or single identities? ID based or Role Based?

These issues are not specific to our context. The current trend in the corporate context is two-folds:

-to separate personal from professional “attributes”,

-to issue personal identities (or certificates embedding such identities).

This trend bears a strong relationship with…

> *Privacy & Data Protection Laws & Regulations: Personally Identifiable Information* [8]

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 online means.

---

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

[8] *“Generic names” may be used as pseudos. This is a recommendation of the French equivalent to the DoD, applicable for example to general accounting practices.*

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

At the same time, there is a strong demand for …

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

Corporates would like to use the same standards, processes and infrastructure with all of their banks while even small corporates often have multiple bank relationships with multiple accounts.

With respect to the ability to use the same infrastructure, a significant requirement is the ability to use an established identity with multiple banks. Concretely speaking…

If a corporate has established an electronic identity with a particular bank, it should be possible to use that same identity with other banks.

This is already the case in a few European countries… This obviously would cut out enormous costs for both corporates and banks.

(Electronic Bank Account Management[9]-also applies to the Financial Supply Chain)

Simplicity means efficiency. Let's take two examples in the Financial Supply Chain:

-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.

-E-invoicing *(adapted fromCAST)*

A standard invoice, used internationally by all industries would give a big push to "dematerialization". It may be seen as a document with multiple interlinked segments to serve specific purposes (compliance with order, match with DDT, check prices, book and pay transaction, basis for financing etc.).

To correctly exploit these multiple links identities must be passed along these different segments. A feature some call "interoperability" and which actually covers

"Multi-Recognition" and "Multi-Acceptance" by multiple parties, globally.

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.

The identities must be able to be used throughout the globe without respect to borders.

Identities need to be recognised by parties around the globe (i.e. across borders) and be accepted for a number of key business processes, either "horizontal" (invoicing, accounting…) or "vertical" shared by business communities.

(Adapted from Electronic Bank Account Management)

[9] *This relates to the electronic handling of bank account opening, closing and maintenance processes and audit and mandate letters. The TWIST Bank Mandate Working Group has set itself the objective to produce standards to enable electronic collaboration between banks and their corporate customers in this process. The goal is clearly to replace the current paper-based process.*

Bank account management obviously applies to all accounts a corporate has with all of its banks. It implies are notification processes across banks.

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.

Identity systems must operate 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.

Identity systems must be able to operate on open networks.

2. Services: Access & Discovery.

2.1 Flexibility in Designating Service Providers

(to be developed. Current Recommendation is to have a "portable IBAN")

2.2 Broader Access to Capital Market : An Example of Opportunities in the Financial Supply Chain:

There is a significant market of "smaller suppliers" who are interested in financing their working capital at rates that are more attractive than what they are getting from their "smaller local banks".

This is mirrored by the fact that larger financial institutions can leverage the balance sheets of their larger importer customers to the benefit of these smaller suppliers *(Financial Supply Chain)*.

3. The Challenges of Responsibility and Liability- Administration, Due Diligence, Control, Compliance & Traceability.

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 good 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 one's 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.

3.1 Control of operations and practices

Assigning and controlling roles/responsibilities in Corporations

The business entity of particular interest to TWIST is the corporation. Leaving the legal definition to lawyers, 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.

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

Identity systems must provide and protect corporate identities.

Employees

A person who is in the employ of a corporation also needs some identification for operation within a business context. People, human beings, by their 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 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.

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[10].

Business continuity

Reliability

Business need to have reliable processes running within the IT space—processes with *verifiably correct operations*. This is not true today. In the abstraction between pen and paper business process and electronically mediated business process 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.

(BM and FSC cases to be developed from the following checklists)

Confidentiality

Disclosure of information to unauthorized persons (inside, outside)

Unauthorized access to data, applications, systems

Interception of communications (transactions)

Etc.

Integrity

Input, operator errors

Program errors, hardware malfunctions

Manipulation or suppression of input documents

Consider controls over preparation and approval of input documents; reasonableness checks; validation of cash and stock records; exception reporting; audit checking; exception reporting; and confirmation with third party records.

Unauthorised Use of Transaction Facilities

Consider controls over logical access to data entry facilities; use of unique user Ids amongst staff; secrecy of passwords; procedures for reporting and investigation of attempted security violations; security administration procedures; access to system by third parties; controls over checking of input transactions; reconciliation of file control totals; checking of cash and stock levels.

Unauthorised Modification to Programs

[10] Identification and authorization are linked.

Unauthorised Modification to File

Manipulation of Job Streams

Etc.

Improvement of Due Diligence Processes in the Financial Supply Chain:

"Know your customer" regulation and requirements put significant demands on the establishment and electronic exchange of identities *(Financial Supply Chain)*.

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

(to be developed – includes BFG sources)

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.

Accountability

Accountability is needed by Business, and so is Liability Allocation, especially between businesses in B2B. Process Identity is as valuable as individual identities, where audit is needed. And, there are technical components below the horizon of Business, that need to be enabled to produce verifiable ID and Liability Allocation—not integrity via marketing claims of protection *(unclear to be reformulated)*.

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 some government agency. There are proscribed bounds under which the bank operates.

In the current political climate, banks are one of the controls on the misuse and inappropriate movement of money. Criminal use of money has become a major focus of legislatures and government regulators. Banks represent a significant control on money movement; consequently, 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.

In modern economies, all significant money movement is done through banks. Corporations of any size will have accounts with banks. 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.

Identity systems must be able to track vetting and proofing of corporations, their agents, and their contractors.

Identity systems must be able to assist in the tracking and movement of money. Reliability and privacy are major concerns.

Auditability

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

Identity systems must be auditable. Identity systems must provide mechanisms for the auditing of transactions.

Identity systems must provide means to examine a transaction at any stage in its progress.

Loss/ Damage Recovery

is an immediate need of business and a business interruption needs to be evaluated viz its impact to 1st, 2nd and 3rd parties.

The recovery process must itself must be independently, verifiable by parties who can represent liability coverage.

3.3 Laws and regulations: Enforceability and Compliance.

Business requirements are legal in nature. Identities will be used in a business context for transactions, document signing, and other functions that commit the business to certain actions. The identities used must be legally enforceable across all organizations and locations involved in the interactions.

Identities actions must be legally enforceable.

Identities must respect the legal codes of the jurisdictions in which they operate.

Regulatory Compliance is no less an issue, with "legal enforceability" it requires 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 (see the "technical Requirements" document) .

Building on Solid Grounds: Legal Basis for a Identity Infrastructure[11]

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.

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

However contracts cannot ignore the local legal framework nor the international treaties.

Besides, there have been efforts from government or professional institutions to establish reference framework or "standards". This is what the TWIST itself is trying to do.

However, see 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[12].[13]

Contracts are the preferred means of establishing the legal basis for an identity infrastructure.

"System" Closure

A principal difficulty with a contract-based infrastructure is extending it to cover all potential relying parties. In developing applications, it is important to determine the extent of the user community and provide a way of ensuring that only contractually bound members of the user[14] community participate in the system.

An exception may have to be made for governmental entities, who may perhaps accept only 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.[15]

[12]

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

[14] *Participants in a community are not only users. The section seems to call for a single infrastructure while one of the key issue seems to be interoperability between several infrastructures.*

[15] *Original proposal included: "In cases where that is not possible (as with governmental organizations), the system must provide for authentication in the legally required form."*

Interoperability: Overlapping Communities

Sometimes a user may belong to more than one contractually defined user community. For example, an IdenTrust user may also be a SWIFTnet user. Each community will have its own contractual specifications.

One of the contractual infrastructures may not recognize, or accord validity to the other. [The reason for that "incompatibility" may not be technically or legally insurmountable.

An identity infrastructure must not depend on an incompatible contract-based infrastructure from another system to prescribe the basic operating rules of a TWIST compliant identity infrastructure][16].

An Identity infrastructure should be in a position to check easily[17] the "compatibility" of another identity infrastructure.

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

Furthermore…

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

This should be based on a common certification or evaluation framework ("referentiel") (see e.g. in France PRIS v1 and v2)

Compliance

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

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

Satisfaction of Legal Requirements for Authentication etc.[18][19]

NB Contracts, processes or infrastructures cannot guarantee the validity of a transaction or of a document in a court. They may just provide elements of proof[20]. These elements will be considered only if they are produced within specific "schemes" or "frameworks". These schemes or frameworks may be public of general interest or restricted to a specific domain. They may refer to best practices in specific areas.

---

[16] *This part [] needs to be explained and rephrased. It is obscure to me (JYG).*

[17] How? This is a key issue to be considered in the "technical" document.

[18] *What happens if the signatory is "revoked" in the mean time?*

[19]

[20] *This makes the following proposal inapplicable in Europe, at least.*

The contract infrastructure must require the parties to treat a digital signature as sufficient authentication of a digital document, provided that the digital signature satisfies certain specifications that ensure its quality. The obligation to treat a signature as legally valid must remain consistent over time and across jurisdictions in order to ensure that all participants in the system follow the same rules.

The participants in a TWIST system must not reject a document for lack of authentication where the document bears a digital signature that conforms to the specifications agreed as of the time when the digital signature was made.

An identity infrastructure should provide elements of proofs re. 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.

EU Compliance is Advantageous

Compliance with the [Electronic Signatures Directive] is optional[21]rather than mandatory, but certain legal and policy outcomes follow if the parties opt to comply. As noted in 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 recognized as such by an EU member state "certification".

Digital Signature [22]

A digital signature may provide a 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…

3.4 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"[23] while there is "a need to enhance security, increase (Governance) efficiency, reduce fraud and protect personal privacy".

This calls for "Secure and reliable forms of identification… identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to fraud, tampering, counterfeiting and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is 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. In such a scheme, a reasonable balance needs to be found, "to ensure flexibility in selecting the appropriate level of security for each application", and to be adjusted *dynamically* (see e.g. the EC project Serenity)

Such a scheme will be proposed in the" technical requirements" document.

Conclusion

This document proposes for discussion some basic, general requirements for the identity aspects of TWIST projects. It does not exhaust the possibilities for requirements, and the varying perspectives among IDWG participants will no doubt bring forward further suggestions.

Perhaps the eventual result of this requirements exercise will be a compilation of basic "must" and "must not" statements that establish a baseline for authentication and confidentiality services in TWIST-compliant endeavours. The compilation probably will not be comprehensive, but it will mark out benchmarks for determining whether an available identity infrastructure is suitable for use in TWIST enabled services. The list can be expected to grow and evolve with experience, developments in the state of the art, and the needs of projects undertaken by TWIST.

[21] *It is literally but Europeans cannot avoid abiding to European law? In any case customers and service providers will scrutinize the "legal value" of the signature they can generate from any system.*

[22]

[23] *The citations in this section are adapted from Hspd-12.*

Summary Table of the "Business Requirements"

The current ambiguities between a person's identities, bank IDs and bank account numbers should be resolved.
Multiple identities/certificates per individual are necessary in order to realize the required degree of personal and business control.
If a corporate has established an electronic identity with a particular bank, it should be possible to use that same identity with other banks.
Identities need to be recognised by parties around the globe (i.e. across borders) and be accepted for a number of key business processes, either "horizontal" (invoicing, accounting…) or "vertical" shared by business communities.
Identity systems must operate globally, if so required. 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.
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.
Identity systems must be able to operate on open networks.
"Open" commercial exchanges, especially those of value, need to be given effective and measurable protections.
A relying party across the Internet needs to know or to be able to evaluate its own processing commitments, risks and liabilities.
Identity systems must be able to track vetting and proofing of corporations, their agents, and their contractors.
Identity systems must be able to assist in the tracking and movement of money. Reliability and privacy are major concerns.
Identity systems must be auditable. Identity systems must provide mechanisms for the auditing of transactions.
Identity systems must provide means to examine a transaction at any stage in its progress.
Contracts are the preferred means of establishing the legal basis for an identity infrastructure.
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.[24]
An Identity infrastructure should be in a position to check easily 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.
Identity systems must be sufficiently strong to provide assurance to regulators. Identity systems must be capable of demonstrating compliance to regulation.
An identity infrastructure should provide elements of proofs re. 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 authority".
Where a service requires a participant to accept a high risk of identification error, it must provide reasonable means of tracking the extent of that risk. However, the tracking mechanism must not expose confidential information to the tracker without the consent of the parties to whom the information is confidential.

[24] *Original proposal included: "In cases where that is not possible (as with governmental organizations), the system must provide for authentication in the legally required form."*

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