Technologies for
Identity Infrastructures

Version 0.1D

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 to regroup the consideration on technologies.

History

This version is a sketch, with extracts from previous IDWG papers.

List of content

Technologies for 1
Identity Infrastructures.....1
Foreword.....1
History1
List of content.....2
Introduction:.....3
Identities, identifiers, certificates, identity infrastructures.....3
(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.)3
Managing the Identity Life-Cycle.....5
Managing the Identity Based Applications 6
Current Technology: Migration from current platforms.....6
Public Key Infrastructure (PKI) include.....6
NB some underlying confusions about public and private key technologies.....6
Extensible Identity Management.....7
Distributed Validation 7
Interoperability.....7
Pervasive Secure Interoperability PSI.....7
NB A usual misconception, is that cryptographic identifications can be resolved in and via applications, which is shown to be false.....7
Reliance-Side Assurances Besides Validation.....7
Preference for Centrally Administered Encryption.....8
Technical Compliance: Encryption Regulation 8
*Prevailing PKI standards *.....8*
References.....9
Glossaries.....9
French and English.....9
English.....10
French10

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".

---

[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.)

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 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.

[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.

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)

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.

Capturing the Identity Life-Cycle

There are currently several attempts[6] [7] [8] 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.

---

[6] *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.

[7] *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.*

[8] *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.*

Managing the Identity Based Applications

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.

Outline Identity "Consuming" Processes[9]

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.

Current Technology: Migration from current platforms.

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 under uniform rules and procedures (e.g. IdenTrust).

Migration from current platforms is an essential need and requires a consistent approach with a valid basis, again 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.

Public Key Infrastructure (PKI) include

Certificates

X509v3

Trusted Third Parties

Registration Authorities

Trusted Time Stamps

Certificate Status Services

NB some underlying confusions about public and private key technologies

may have persisted, along with fundamental cryptologic concepts which may not have been clarified.

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

Despite various national efforts, which may tend to confuse the word Certificate with a physical pen-and-paper analogue of a credential, and with the physical ID card which might be renamed, even as a private key secret metamorphosed in a publicly usable individual certificate, these are not the same as a cryptographic public key certificates. And should not be confused with them.

Extensible Identity Management

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.

Distributed Validation

is the need to evaluate at the end-points; this must be without additional connectivity.

Interoperability

as a need touches on 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. Standardized 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.

Pervasive Secure Interoperability PSI

While many IT and business sectors have surfaced many requirements over the years, Business 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 business that the platforms, IDs and processes enabled can be trusted, and the limits within which trust is warranted. Internally verifiable, electronically processed metrics are a must.

Considerations for 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?

NB A usual misconception, is that cryptographic identifications can be resolved in and via applications, which is shown to be false.

Service providers have had difficulties allowing interoperability of identity across services and applications [only because they do not use a common and consistent approach to ID], even though the exact same technology is being used in most implementations (X.509 v3 certificates).

Reliance-Side Assurances Besides Validation[10]

SAML technology[11] provides a robust means for accommodating different relying-party requirements for assurance provided by a certification service provider. Instead of establishing a common, bridge-able set of requirements on the front end, SAML works from the reliance side of the four-corner model explained in [CARAT Guidelines] section C2. SAML standards are a basic building block that can be designed to provide each relying party

[10] *In business terms this relates to the preceding issue. Could an example be given?*

[11] *Again that's jumping to rapidly into the TR while there are business issues at stake. Again they should be clearly separated.*

with the authentication assurance that they require without having to agree on a common level throughout the user community.

If TWIST participants cannot agree on a single level of trust assurance for relying parties, a TWIST 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). An implementation of SAML can be such a means.

Preference for Centrally Administered Encryption[12]

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.

TWIST 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

Technical Compliance: Encryption Regulation[13] [14]

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

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

Prevailing PKI standards *

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.

[12] *Within a companies perimeter? This is unclear to me.*

[13] *Two comments, which apply to this point as well as the next ones (appearance… referencing… archive): a) they are not BR requirements per se, they may fall either under a broader compliance point or in the TR categories, b) some of the considerations apply to any subject, the risk is to be distracted from key and specific issues on ID's. I agree not to delete the item (I is always better to be redundant than to forget about an item) but it might be more appropriate to put them in a more proper category.*

[14] *This does not solve the problem which may arise in cross-boarder transactions from contradictions between national regulations.*

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

The 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)