

CS1/07-0271 Proposed US NB Contribution to the SC 27/ WG 5 Liaison Statement to the ITU-T Focus Group on their Identity Management Reports from Sheila Brand/Cygnacom, Neville Pattinson/Gemalto and Dick Brackney/NSA

We have reviewed the six documents comprising the output of the ITU-T Focus Group on Identity Management. In general we are extremely impressed by the thoroughness of the work and the focus group's grasp of the complexity of the issues involved in trying to develop global interoperability of identity-based transactions. This is a tremendous undertaking and we wish the ITU-T success in helping to make the interoperable, global identity layer that you envision a reality.

The reports were reviewed with the objective of (1) using information in them to fuel future initiative within SC27 /WG5; (2); using information from your reports as a resource for current SC27 standards under development and (3) when appropriate, suggesting additions to the findings of your report.

1. FUEL FOR FUTURE INITIATIVES WITH SC27/WG5

There are two areas that have broad applicability within the study: federated IdM, and the Identity Plane model.

Federated Identity Management: The study has done an excellent job at describing the concept, security problems, issues, gaps, and recommendations in this area. If nothing else is achieved, ITU-T is to be congratulated on bringing these issues into clear focus. We agree that at the point where federated systems are being established the requirements listed in Report No 5 should be enforced on all effected parties.

The Identity Plane: The entire ITU-T FG report is built on the "Identity Plane" query-response architecture model of a three-party system, where all analysis relies on the interaction of an Asserting Party, a Relying Party and an Identity Provider. Given the network-centric perspective of ITU-T this model is extremely useful. We will adopt this model for all WG5 initiative where it is applicable. As a first use of the model, we will be incorporating it into our IdM Framework document, IS 24760. (See below for specific examples of this)

The reports have provided us with a wealth of information for future initiatives in IdM. Here is a list of some of the future standards efforts that WG5 plans to start based on information from your work.

Proposal: to develop joint ITU-T/SC27 standards dealing with the security gaps delineated in Report 4, clause 5 and clause 13 as well as requirements in Report 5 (N6245)

- IdM Security Reference Architecture
- Inter-federation and bridge IdM security policies
- Categorization of IdM transaction types as a starting point for identifying levels of sensitivity and therefore levels of protection for each type of data/transaction.
- Negotiation mechanisms and procedures for establishing security between federations that have to communicate
- Mutual authentication procedures and mechanisms to be used by all three entities (i.e., Asserting Party, a Relying Party and an Identity Provider) to authenticate themselves to each other
- Minimum levels of protection (i.e., authentication, access control, confidentiality, integrity, non-repudiation, availability and audit) to be afforded by all federations involved in inter-federation data sharing
- Types of security (e.g., encryption, digital signing, etc) to be used and their levels of assurance for different categories of IdM transactions.
- Minimum risk assessment, parameters, metrics, and procedures
- Uniform procedures/mechanisms to be used by Identity Providers to support Single Sign On/Log Out
- Standardized revocation procedures and mechanisms for Identity Providers to use to alert all affected parties whether within the same federation or not.
- Specification of minimal levels of protection/security to be afforded personally identifiable information. This guidance to be used by all Identity Providers and relying parties
- Standards for logging by Identity Providers information of use by auditors (e.g. assignment of identities and validation of identities and association of attributes with a particular identity).
- A compendium of services to be supported by all Identity Providers – both within one federation and among all federations

2. USE OF ITU-T REPORTS AS A RESOURCE FOR CURRENT SC27/WG5 INITIATIVES

The following provides examples of where SC27/WG5 can use the material from your reports. It represents a mapping of information from FG IdM Reports to clauses in several WG5 documents. This is not an exhaustive analysis, but rather serves to indicate that there is much material in these reports that is directly related to WG5's work and will be appropriately leveraged.

As you have stated, the intent of the IdM Reports is to make IdM concepts used in the development of ITU-T Recommendations available to those who want to use it. By incorporating material from the six ITU-T IdM reports into our work we will be helping to begin global inter-working of the diverse IdM platforms that will surely exist.

Report on IdM Use Cases and Gap Analysis (N6244)

1. Clause 5.2 "IdM Architectural Model" and Figure 3 of this FG IdM Report contain a high level description of an IdM common query – response model that includes an example of how the query-response model is used in mutual authentication. The model and figure will be introduced and appropriately described in SC27's Framework for IdM, 3rd WD 24760.
2. Clause 8, "InterFederation/Inter-CoT Interoperability" is directly related to Clause 9.8, "Federation and Interoperability" in WD 24760 and will be appropriately summarized to include a brief explanation of Figure 18.
3. Clause 10, "Identity Assurance" includes material useful in Clause 6.4.3 "Mutual authentication" in WD 24760 and will be appropriately summarized to include a brief explanation of Figure 18.
4. Clause 10 "Identity Assurance" is also directly related to SC27 Project N29115, "Entity Authentication Assurance". This FG IdM material will be appropriately addressed by the Editors of N29115. In particular, the gaps that are identified in Section 10.4 and summarized in Clause 17.1, page 132 will be an extremely useful resource.
5. Clause 11, "Transparency, Notice, Access and Privacy" is directly related to SC27 Projects on Privacy and contains use cases (Clauses 11.2 and 11.6), requirements (Clause 11.3) and gaps in standards (Clause 11.5) that will be appropriately considered in SC27's Privacy Framework and Privacy Architecture projects. This material may be summarized and included in Clause 7.5.2 of SC27's Framework for IdM, 3rd WD 24760.

6. Clause 12 “Integration of IdM with Object management” is directly related to Clause 9.6.2, “Device Identifiers” and 9.6.3, “Information object identification”, especially the classification of non-human objects on page 91 and 92.
7. Clause 7, “Discovery of Identity Resources” is an important component of an IdM framework and will be briefly introduced in SC27’s Framework for IdM, 3rd WD 24760.

Report on Requirements for Global Interoperable Identity Management (N6245)

This is a comprehensive set of requirements however in practice a significant challenge is to establish equivalence of assurance levels by all parties operating in a global infrastructure. Equivalence is the notion of ensuring that during the process of establishing/authenticating an identity, it is done with similar or same practices/procedures and uses similar quality of reference documents/material across different identity providers. Without equivalence for assurance levels an imbalance may result in relative levels of trust across transactional relationships in a global environment.

1. Clause 5.2.6, “Provision of identity assurance levels” is directly related to SC27 Project N29115, “Entity Authentication Assurance” and will be made use of. As R38 to 40 deal with assurance levels, we will pay particular attention to these recommendations where appropriate.
2. Clause 5.5.2, “Protection and use of Personally Identifiable Information” is directly related to SC27/WG 5 privacy framework and Clause 7.5.2, “Privacy protection” of SC27’s Framework for IdM, 3rd WD 24760. Requirements R64-R66 will be appropriately addressed.
3. Clause 5.3, “Discovery of authoritative Identity Provider resources, services and federations” is an important component of an IdM framework and will be briefly introduced in SC27’s Framework for IdM, 3rd WD 24760.
4. This includes 73 requirements that were derived from a standards gap analysis of many different uses cases. The requirements were divided amongst seven different basic capabilities as shown in Figure 1, page 2 of the Report. These requirements, especially those in Clause 5.5 “Security and other measures ...” (e.g. R51-R65) will be considered material for Clause 7.4 “IdM Requirements” in our Framework for IdM, 3rd WD 24760. In addition many of them are the basis of proposed standards delineated earlier in our liaison statement to you.
5. Clause 5.5.2 “Protection and use of Personally Identifiable Information” contain information useful to our Privacy Framework WD 29100 and will be used appropriately in that document.

6. Clause 5.6 “Auditing and compliance, including policy enforcement and protection of personally identifiable information” is a topic that will be included in SC27’s Framework for IdM, 3rd WD 24760. Auditing and compliance are capabilities that are key drivers of IdM deployments. In addition Clause 5.6 is the basis of a proposed standard delineated earlier in our liaison statement to you.

Report on Identity Management Framework for Global Interoperability (N6246)

When considering an IDM framework for global interoperability, privacy must be considered and embedded at the outset. There appears little emphasis on privacy and how to achieve privacy considerations in this model as it stands today. Recommend this model undergoes a full review for privacy considerations.

There is a need to consider identity theft in this report and how/what mechanisms there will be for redress to set the situation right. Identity revocation is not the only mechanism needed as the identity may be rooted on a real life identity and revocation is not appropriate in a complete context. (I.e. they are not going to change their name as a result of digital ID theft).

1. Clause 5, “Identity” is directly related to Clause 6.2, Identity Life Cycle” in SC27’s Framework for IdM, 3rd WD 24760 and will be utilized appropriately.
2. Clause 5.2.2 “Identity authentication” is directly related to Clause 6.4, Identity authentication” in SC27’s Framework for IdM, 3rd WD 24760 will be utilized appropriately.
3. Clause 5.3, “Binding identities with attributes”, Clause 5.4 “identity certification, Clause 5.5 “Identity Change” Clause 5.6 “Unbinding of attributes from identities” and Clause 5.7 “Identity revocation” are directly related to Clause 6.6, Binding and unbinding attributes with identities, certification, identity changes” in SC27’s Framework for IdM, 3rd WD 24760. Consequently, this material will be utilized where appropriate.
4. The definitions provided in Clause 5.8, pages 9 and 10 will be considered as definitions for the corresponding terms in Clause 3.0 of SC27’s Framework for IdM, 3rd WD 24760.
5. Clause 8.0. “Framework Components” describes various IdM services and how they relate to the three party query response model. We will consider this as another way to describe the information contain in Clause 8.1 of SC27’s Framework for IdM, 3rd WD 24760.

6. Appendix A1.1. “Lifecycle Management Interactions” of this FG IdM Report contains useful material for the SC27’s N29115, “Entity Authentication Assurance and for Clause 6.2 of SC27’s Framework for IdM, 3rd WD 2460 and will be used appropriately.

3. SUGGESTED ADDITIONS TO THE ITU-T IdM REPORTS

Report on Identity Management Ecosystem and Lexicon (N6243)

SC 27/WG5 and ITU-T SG 17 agreed to work closely together in the development of Identity management standards. In particular, Project N29115 was approved as a common ITU-T and ISO/IEC/JTC 1/SC27/WG5 text standard. For this joint work, it is important that both organizations use common IdM terminology. The Editors of WG5 documents have reviewed the ITU-T Focus Group IdM Lexicon and are providing a few new definitions to be added to the Lexicon. They are included below. We will continue to provide modifications and/or updates as appropriate. The goal will be to achieve a common set of IdM terms for work in SC27 and ITU-T.

A.2. Need to add **Center for Ethical Identity Assurance (CEIA)** as a research organization. (www.ceiaglobal.org)

Recommended additions to Report No. 3 – Ecosystem and Lexicon Annexe B- Identity Management Terms and Definitions¹

Access control: a procedure used to determine if a party should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

Attribute: A subject is an entity represented or existing in the digital realm which is being described or dealt with. Every subject has a finite number of identity attributes. A subject can be human or non-human. Non-human examples include: devices and computers, digital resources, policies and relationships between other subjects.

Identity attributes exist within the context of ontologies. A simple example of an ontology is “A cat is a kind of animal” An entity represented in this ontology as a “cat” is therefore invariably also considered to be an “animal.” In establishing the contextual relationship of identity attributes to one another, ontologies are able to represent identity

¹ These definitions are from the Financial Services Technology Consortium (FSTC) Project on Better Mutual Authentication Terminology.

http://www.fstc.org/projects/completed/bma-ph-1/BMA_terminology.pdf

in terms of pre-defined structures. This in turn allows computer applications to process identity attributes in a reliable and useful manner.

For humans, some examples of identity attributes are name, address, phone number, color hair, social security number, height, weight, and so on.

Authentication assurance level: the level of confidence that the authentication process is correct. NIST has described four authentication assurance levels: Level 1 – Little or None, is sometimes associated with requiring no authentication, not even ID and password. Level 2 – Some is sometimes associated with a single factor authentication, such as ID and password. Level 3 – High, is sometimes associated with 2 factor authentication, such as ID and Password and a hardware token (something you possess). Level 4 - Very High, is sometimes associated with 3 factor authentication, such as something you know, something you possess, something you are.

Authenticator:² An information object or condition that can be evaluated in order to confirm the veracity of an authentication *claim*. Some examples of common *authenticifiers* include:

- Shared secrets, including passwords and keys used to generate one-time passwords
- Asymmetric cryptographic keys
- Physical metrics, including biometrics
- Access to a common resource, including use of alternative channels such as telephone circuits
- Shared knowledge—*e.g.*, challenge question to claimant with associated response
- Contextual clues—*e.g.*, characteristics of the computer or network connection used by a claimant, including dynamic conditions
- Behavioral patterns

In general, an *authenticator* must be associated with a specific claim. However, there are a variety of schemes for making such associations and maintaining the association of claim to authenticifier throughout a life cycle.

² “Authenticator” is not a word in the English language (though it is a French word). It is being introduced here as a more convenient term than some of the compound phrases, such as “authentication information,” that are sometimes used in security literature. The NAS/NRC “Who Goes There” report suggests “authenticator” as an equivalent term, but this can also mean “one who authenticates.” Another reason for introducing “authenticator” is to explicitly avoid misuse of terms, such as “token,” or “credential” that have taken on confusing semantic baggage.

One way that claims are bound to authenticifiers is through use of a *credential*. However, it is important to avoid confusing authenticifiers with credentials. In particular, while every credential refers to at least one authenticifier, an authenticifier need not be associated with a credential.

For example, an asymmetric key pair can be used as an authenticifier, where the claimant holds the private key and an authenticating party has access to the corresponding public key. A credential, in the form of a digital certificate, might serve to bind the public key to the claimant (or the claim). During authentication, the claimant can be presented with a challenge that is cryptographically processed with the claimant's private key to produce a response that can subsequently be tested using the public key contained in the digital certificate. Note that, in this example, the authenticating party need *not* depend on a digital certificate, but could use some other means to associate the appropriate public key with the claim.

Claim: Within the context of *authentication*, a party (or entity) presents a *claim* that will be tested for authenticity as part of an authentication procedure ... Typically, a claim is presented in the form of a *name* ... that indirectly references whatever rights or entitlements are associated with the claim—*i.e.*, the *name* is a shorthand means of referencing a *claim* that may involve many parameters or attributes. However, in some cases, claims to privileges or entitlements are stated directly within an authentication process. For example, when enrolling for authenticifiers ... or credentials ... to be used in subsequent authentication procedures, the claim may need to state what privileges or entitlements are to be associated with the credential.

Claimant: Within the context of *authentication*, the party (or entity) that presents a *claim* to be authenticated is referred to as a *claimant*. A claimant may be a true person, or an insentient system or service. It doesn't really matter who, or what, a claimant is, only that it is the presenter of the claim.

In retail financial services, a customer seeking access to a financial service for a specific account is a claimant, but so is the financial service itself. The customer is claiming the rights, privileges or entitlements associated with their account, while the financial service is claiming to be the legitimate provider of services associated with the customer's account.

Entitlement (privileges, rights): Entitlement refers to being granted rights to access and modify information and resources, such as financial data, confidential records, web services and programs.

Interoperability: The ability of software and hardware on different machines from different vendors to share data; to exchange or use information.

Mutual Authentication : the process whereby an FI's (i.e., Financial institution) customer and a financial services application exchanging [message traffic | information]

each obtains sufficient assurance that the other party is authentic, and that the [message stream | information exchange] has integrity, and that no other parties are able to participate in the information exchange. The level of assurance shall be appropriate to the risk associated with the interaction.

Name: Within the context of electronic *authentication systems*, the *names* associated with various parties, entities, and resources are of critical importance. *Claims* are often expressed indirectly via a *name* that maps to the claim being made. For example, a financial institution may claim to its customer that it is the legitimate provider of financial services in an online context by presenting a domain name or URL (both names) during a web-based interaction. Similarly, a customer may provide their account number (a name) as a shorthand expression of the claim that they are the party authorized to access account information or conduct transactions involving the account.

... there are many types of names that can be used to refer to an entity or as a shorthand reference to a claim, often with substantial overlap. For example, a consumer may be known by their common name, taxpayer number, drivers' license number, employee number, mailing address, email address, telephone number, financial account number, or some userid assigned to them for the purpose of authentication or access control. Similarly, the plethora of names consumers must use to reference their financial institutions is a source of potential confusion, especially as financial institution names change on a frequent basis due to system updates or mergers/acquisitions.

Role: In a role-based authentication software system, users are assigned one or more predefined roles. These roles then determine the user's privileges; the information they can see areas they can access, and items they are able to change.

Single sign-on: a specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems

Validate: To establish the soundness or correctness of a construct. Example: certificate validation. ... It includes any process that aims to establish that data relationships are properly maintained, or that data structural rules have not been violated. Since *validation* merely determines that a construct is correct, it is a weaker statement than *verifying* some claim. However, validation is often a necessary process in authentication, and may be associated with "controls" used to audit compliance with stated practices.

Verify: To test or prove the truth or accuracy of a fact or value. *claims* are *verified* during an authentication procedure—*i.e.*, verification is an assessment of the authenticity of a claim.