TAS^3: Glossary (Draft 02)

Editor: TBD Quentin? (this version by Sampo)

January 20, 2010

Abstract

Look here for acronym expansion and explanation of TAS^3 terms.

1 Glossary

AAPML A markup language for declaring data availability and acceptable use policies a Provider. Part of [IGF].

Audition Aiming at providing only high quality service to the users, the provider of a directory service can be interested in testing that the services asking for registration are of "good" quality. For this purpose, the directory could submit the service under registration to a verification step before granting the registration. The implementation of such process with respect to the technical assessment is called Audition (Automatic Model-Based Interface Testing In Open Networks).

Behavioural Factors Aspects of feedback used in define a reputation. For example for a helpdesk one could consider politeness, responsiveness, usefulness of supplied information, etc. These factors may be combined into the reputation differently depending on the needs of the user.

BPM Business Process Modelling

Business Process Modelling Using a formal methodology to describe a business process. Such formal model will usually allow some of the configuration details for implementing the business model to be automatically derived.

BPEL Business Process Execution Language

CARML A markup language for declaring data needs of a Client. Part of [IGF].

Client While general meaning as in "customer" is acknowledged, in protocol contexts "Client" is taken to mean requestor of a service. Thus Client is the counter part of a Service Provider. Client is a business entity and quite different from a User. A Service Provider can be a Client towards other entities that it calls.

CoT Circle of Trust. Synonymous with Trust Network.

Circle of Trust Synonymous with Trust Network.

DNS Domain Name System. The scheme for attributing alphanumeric, human readable "web addresses". DNS will map the human readable string to an IP address. Sometimes a `/etc/hosts` file replaces the function of the DNS, but this solution, while allowing more local control, is generally very burdensome to maintain.

GA Governing Agreement.

Governing Agreement Legal document that every member of Trust Network MUST agree to. This can be seen as the charter of the Trust Network.

IAF Identity Assurance Framework

IGF Identity Governance Framework

IdM General acronym meaning Identity Management

IdP Identity Provider.

Identity Provider An entity that specializes in identifying (collecting identity information or PII), and authenticating users. IdP is usually, and in SAML case especially, charged with the role of facilitating Single Sign On (SSO). IdP often also conveys PII when authenticating the User. IdP has prime visibility to the usage patterms of a User and is therfore especially vulnarable or in need of special business or administrative protections. IdP function is often associated with ID Service Discover and Token Mapping functions. Core of an IdP is a federation database where mappings between several pseudonymous identities and relationships with the service providers are evident. This database constitutes a fat target when an identity system is attached.

KPIs or Key Performance Indicators are combinations of different Business Performance factors such as Time to deliver, or number of patent application, etc.

MS Message Signer. Digitally signs request.

MV Message Verifier. Verifies digital signature and other constraints of a request.

PEP Policy Enforcement Point

ADPEP Application Dependent PEP. Apply specific rules that relate to the application roles. Typically comminicates with ADPDP.

AIPEP Application Independent PEP, typically communicates with AIPDP (cf. Architecture: Anatomy of PEP)

PEP-P Service Provider Policy Enforcement Point

PEP-R Requester Policy Enforcement Point

PDP Policy Decision Point

ADPDP Application Dependent PDP. Apply specific rules that relate to the application roles. Typically comminicates with ADPEP, but may also proxy requests in relevant special cases to outside PDPs or gather Information for its decisions from outside, including from Reputation Providers.

AIPDP Application Independent PDP, more properly TAS3 Network PDP or External PDP Aggregator (cf. Architecture: Anatomy of PEP)

PDP-P Service Provider Policy Decision Point

PDP-R Requester Policy Decision Point

T-PDP Trust Policy Decision Point. Returns a trust decision. (I think what is meant here is "reputation" decision.)

PMS Policy Management Service.

Policy Management Service Handles the management of user policies and 'organization wide' policies. Moreover it will have a functionality to attach policies to a request respectively a response. This is an ongoing task in WP8 under the name of 'Aggregating Policies'.

PII Personally Identifiable Information.

Personally Identifiable Information Information that may allow identifying a User, or impersonation of the User.

PCP Personal Competency Profile.

Principal Liberty and SAML terminology meaning User.

PUPPET Pick UP Performance Evaluation Test-bed. It is an approach for the automatic generation of test-beds to empirically evaluate the QoS characteristics of a Web Service under development. Specifically, the generation exploits the information about the coordinating scenario, the service description (WSDL) and the specification of the agreed QoS properties.

QoS Quality Of Service

IDL Interface Description Language. For example within the standards of the family WS*, WSDL is an IDL.

RS Response Signer. Digitally signs request.

RV Response Verifier. Verifies digital signature and other constraints of a response.

Security Officer A job function or role at Trust Guarantor. Similar function, with the same name, may also exist at Trusted Third Parties, and Service Providers. Security Officer's job is to on continuing basis verify and validate that the members of a Trust Network adhere to the rules. To do this Security Officer usually operates and monitors automated auditing and systems monitorin tools. If discrepancies are found, or complaints are reported, the Security Officer will investigate manually in more detail. Security Officer also participates in approving new members to the network and in taking disciplinary action, such as removal from the network, against the offenders.

SOA Service Oriented Architecture.

Service Oriented Architecture A conglomeration of web services, or in a briader sense any kind of services. SOA paradigm attempts to abstract the services so that they are reusable components that can be composed in different arrangements at will. Parallel to the orchestration, there is identity propagation infrastructure and authorization infrstructure, which in its turn relies on trust infrastructure. Real life SOAs are mucl less generic and recomposing the components in any reliable way remains a dream.

SP Service Provider.

Service Provider An entity that provides a service. In TAS^3 context the service is foreseen to be provided over a network, usually the Internet.

SPPE Service Provider Process Engine. Controlling logic of the Service Provider.

SRPE Service Requester Process Engine. Controlling logic of the Client.

SSO Single Sign-On

SLO Single Logout (the logical complement of SSO)

Structural trust rules can be simple trust statements as Provider X is trusted to supply Job Vacancies and the combinations trust relations for example when the party trusted to issue credentials is itself determined by trust rules; Provider X is trusted to supply Job Vacancies if a trusted Accreditation agency certifies them. An Accreditation agency is trusted to certify Providers if it is registered at a national registry and has a good reputation, etc.

TAXI Testing by Automatically generated XML Instances. A tool by CNR that generates XML instances from an XML Schema automatically. The methodology is largely inspired by the Category Partition testing technique.

Trust Information Collector a point which gathers feedback information needed to calculate reputations (see also WP02 D2.1 deliverable).

TAS3 See TAS^3. This is just an alternate spelling.

TAS^3 EU FP7 Project.

TAS^3 Trust Network A trust network that adheres to the TAS^3 rules, as specified in [TAS3ARCH], [TAS3PROTO], and [TAS3COMPLIANCE]. N.B. that such network need not be operated or governed by TAS^3 consortium. Any TO can set up a TAS^3 Trust Network by simply satisfying the requirements.

Trust Ecosystem The users, members, suppliers, and stake holders of a Trust Network.

TN Trust Network.

Trust Network An online business environment where parties can interact with each other securely. While the network does not warrant hones behaviour of the members in the network, it does ensure that everybody adheres to some basic principles especially in nonrepudiation, data security, communucations security, and IT security. Thus a Trust Network promotes trust between its members.

TPN Trust and Privacy Negotiator.

TO Trust Operator, now renamed as Trust Guarantor (TG).

Trust Operator See TG.

TLG Top Level Guarantor. Formerly Trust Operator, TO, now TG.

TG Trust Guarantor (formerly Trust Operator, TO, or Top Level Guarantor, TLG).

Trust Guarantor Governing entity of a Trust Network. The top level Trusted Third Party that administers the Trust Network.

TTP Trusted Third Party.

Trusted Third Party An entity that is technically trusted by the infrastructure to assure correctness of some transaction or relationship. TTP is generally subordinate to Trust Operator, the latter being responsible for the overall oversight..

TLG Top Level Guarantor. Synonymous with TO. See [TAS3BIZ].

TTL Time-To-Live. Parameter that indicates how long a cache entry is valid. Generally a cache entry will not be refetched until TTL expires. This concept is especially used by the DNS.

T&S Trust and Security.

User Human that uses the Trust Network. In Liberty and SAML contexts User is synonymous with Principal.

CoT Circle of Trust

Disco Service discovery, sometimes specifically identity enabled service discovery such as Liberty ID-WSF Discovery Service. Discovery service corresponds to one of the bulletin boards in Danny's "snake" diagram.

DB Dashboard, a web GUI for viewing audit records, work flow status, and/or viewing and manipulating privacy settings and permissions.

FE Frontend, here means web site, i.e. SP

WS Web Service, SOAP based machine to machine communication. Sometimes specifically Identity enabled web service, e.g. Liberty ID-WSF based WS.

WSC Web Service Client, aka Service Requester

WSP Web Services Provider

2 Future Work

- Ontology harmonization
- Maintain this glossary on some formal notation, to facilitate ontology work

References

[TAS3DESIGNREQ] Gilles Montagnon (SAP), ed.: "Design Requirements", TAS3 Consortium, 20081221. Document: TAS3_D1p4_Design_Requirements_1_V2p0.pdf

[TAS3DESIGNRAR] David Chadwick (Kent), ed.: "Requirements Assesment Report", TAS3 Consortium, 20090102. Document: TAS3_D1p2_Requirements_Assesment_Report_1_V1p0.pdf

[TAS3BIZ] Sampo Kellomäki (EIfEL), ed.: "TAS3 Business Model", TAS3 Consortium, 2009. Document: draft-sampo-tas3-biz-model-2009-v03.pdf

[TAS3THREAT] Sampo Kellomäki (EIfEL), ed.: "TAS3 Threat Analysis", TAS3 Consortium, 2009. Document: tas3-threats-vXX.pdf

[TAS3ARCH] Sampo Kellomäki (EIfEL), ed.: "TAS3 Architecture", TAS3 Consortium, 2009. Document: tas3-arch-vXX.pdf

[TAS3PROTO] Sampo Kellomäki (EIfEL), ed.: "TAS3 Protocols and Concrete Architecture", TAS3 Consortium, 2009. Document: tas3-proto-vXX.pdf

[TAS3COMPLIANCE] Sampo Kellomäki (EIfEL), ed.: "TAS3 Compliance Requirements", TAS3 Consortium, 2009. Document: tas3-compliance-vXX.pdf

[TAS3GLOS] Sampo Kellomäki (EIfEL), ed.: "TAS3 Gloassary", TAS3 Consortium, 2009. Document: tas3-glossary-vXX.pdf

[TAS3CONSOAGMT] "TAS3 Consortium Agreement", TAS3 Consortium, 2008. (Not publicly available.)

[IAF] Liberty Alliance: "Identity Assurance Framework"

[IGF] Liberty Alliance: "Identity Governance Framework"

[SAML11core] SAML 1.1 Core, OASIS, 2003

[SAML11bind] "Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1", Oasis Standard, 2.9.2003, oasis-sstc-saml-bindings-1.1

[IDFF12] http://www.projectliberty.org/resources/specifications.php

[IDFF12meta] Peted Davis, Ed., "Liberty Metadata Description and Discovery Specification", version 1.1, Liberty Alliance Project, 2004. (liberty-metadata-v1.1.pdf)

[SAML2core] "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-core-2.0-os

[SAML2prof] "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-profiles-2.0-os

[SAML2bind] "Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-bindings-2.0-os

[SAML2context] "Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-authn-context-2.0-os

[SAML2meta] Cantor, Moreh, Phipott, Maler, eds., "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-metadata-2.0-os

[SAML2security] "Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-sec-consider-2.0-os

[SAML2conf] "Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-conformance-2.0-os

[SAML2glossary] "Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0", Oasis Standard, 15.3.2005, saml-glossary-2.0-os

[XML-C14N] XML Canonicalization (non-exclusive), http://www.w3.org/TR/2001/REC-xml-c14n-20010315; J. Boyer: "Canonical XML Version 1.0", W3C Recommendation, 15.3.2001, http://www.w3.org/TR/xml-c14n, RFC3076

[XML-EXC-C14N] Exclusive XML Canonicalization, http://www.w3.org/TR/xml-exc-c14n/

[Shibboleth] http://shibboleth.internet2.edu/shibboleth-documents.html

[XMLENC] "XML Encryption Syntax and Processing", W3C Recommendation, 10.12.2002, http://www.w3.org/TR/xmlenc-core

[XMLDSIG] "XML-Signature Syntax and Processing", W3C Recommendation, 12.2.2002, http://www.w3.org/TR/xmldsig-core, RFC3275

[Disco2] Liberty ID-WSF Discovery service 2.0

[Disco12] Liberty ID-WSF Discovery service 1.1 (liberty-idwsf-disco-svc-v1.2.pdf)

[SecMech2] Liberty ID-WSF 2.0 Security Mechanisms

[SOAPAuthn2] Liberty ID-WSF 2.0 Authentication Service

[SOAPBinding2] Liberty ID-WSF 2.0 framework document that pulls together all aspects

[DST21] Liberty Data Services Template 2.1

[DST20] Liberty DST v2.0

[DST11] Liberty DST v1.1

[IDDAP] Liberty Identity based Directory Access Protocol

[IDPP] Liberty Personal Profile specification.

[Interact11] Liberty ID-WSF Interaction Service protocol 1.1

[FF12] Liberty ID Federation Framework 1.2, Protocols and Schemas

[SUBS2] Liberty Subscriptions and Notifications specification

[CardSpace] InfoCard protocol (aka CardSpace) from Microsoft

[Schema1-2] Henry S. Thompson et al. (eds): XML Schema Part 1: Structures, 2nd Ed., WSC Recommendation, 28. Oct. 2004, http://www.w3.org/2002/XMLSchema

[XML] http://www.w3.org/TR/REC-xml

[RFC1950] P. Deutcsh, J-L. Gailly: "ZLIB Compressed Data Format Specification version 3.3", Aladdin Enterprises, Info-ZIP, May 1996

[RFC1951] P. Deutcsh: "DEFLATE Compressed Data Format Specification version 1.3", Aladdin Enterprises, May 1996

[RFC1952] P. Deutcsh: "GZIP file format specification version 4.3", Aladdin Enterprises, May 1996

[RFC2246] TLSv1

[RFC2251] LDAP

[RFC3548] S. Josefsson, ed.: "The Base16, Base32, and Base64 Data Encodings", July 2003. (Section 4 describes Safebase64)

[RFC2119] S. Bradner, ed.: "Key words for use in RFCs to Indicate Requirement Levels", Harvard University, 1997.

[MS-MWBF] Microsoft Web Browser Federated Sign-On Protocol Specification, 20080207, http://msdn2.microsoft.com/en-us/library/cc236471.aspx

[RM-ODP] http://en.wikipedia.org/wiki/RM-ODP

Revision History

02 24.3.2009 Sampo

- Handoever to Quentin

01 14.3.2009 Sampo (sampo@symlabs.com)

- First draft out of blue

Document ID `draft-tas3-glossary-v02.pdf`

Repository path `repo.tas3.eu:/var/lib/tas3repo/arch/tas3-glossary.pd` (1.2)

```
CVSROOT=:ext:repo.tas3.eu:/var/lib/tas3repo cvs co arch
```

Commenting

- Please comment on the TAS3ALL@LISTSERV.CC.KULEUVEN.AC.BE mailing list, or that failing, send your comments to the editor.
- Any footnotes in this document will not appear in final version. They are editorial comments that may help reviewers to put material in context.