TAS^3: Compliance Requirements (Draft 05)

Editor: Sampo Kellomäki (sampo@symlabs.com), EIfEL

January 20, 2010

Abstract

Description of the specific requirements that a deployment must comply with when operating in TAS^3 Trust Network. This is beyond and in addition to the architecture and protocol requirements, as well as governing agreement and trust operator policies described elsewhere.

Contents

1 Introduction

This document describes the TAS^3 Compliance Requirements for Deployments in a normative and prescriptive way. Any deployment claiming "TAS^3" compliance MUST abide by this document as well as [TAS3ARCH], and [TAS3PROTO]. A deployment usually has to satisfy, as well, requirements of the Trust Guarantor's, see [TAS3GLOS], Governance Agreement and certification procedures, some of which concern the software implementation and others the organizational properties. Use of TAS^3 Brand is governed by a separate TAS^3 Brand Agreement.

This document uses the keywords (e.g. MUST, SHOULD) of [RFC2119]. All text is normative unless expressly identified as non-normative. Prose and specification has precedence over examples. In general the examples should not be assumed normative unless no normative specification for the subject matter is available.

For a partner to operate in a TAS^3 Trust Network, it must comply with certain software and protocol requirements described in [TAS3ARCH] and [TAS3PROTO]. However such software can often be configured in a variety of ways. This document incorporates by reference all the requirement described by the above documents, and then adds deployment and configuration specific requirements.

In addition to the present document, the Trust Guarantor of your Trust Network may have published additional policies and requirements. The Governing Agreement of the Trust Network can also specify more requirements.

Many compliance requirements that a Trust Guarantor will likely enforce to its Trust Network are described in the Identity Assurance Framework [IAF].

2 Compliance Requirements

2.1 Other Work

- [SAML2conf]
- [**?**]

2.2 General Compliance Requirements

2.2.1 Legal and Contractual Compliance Requirements

CR21-Lawful All legal requirements MUST be satisfied. Members MUST operate within the law.

CR22-Arch All normative requirements of [TAS3ARCH] MUST be satisfied.

CR23-Proto All normative requirements of [TAS3PROTO] MUST be satisfied.

CR24-File Each member MUST be registered on the file at the Trust Guarantor. The filing MUST include details appropriate for the jurisdiction to identify the entity to the extent needed to raise a law suit and/or coordinate investigation with the tax authorities. Typically this means at least

a. Entity name
b. Address
c. Company registration or VAT number
d. Version of Governance Agreement signed and date signed (Req. *D1.2-6.13-Contract*)

Whenever this information changes, the member MUST prompty inform the Trust Guarantor.

CR25-Policy Each member MUST conspiciously publish a Privacy Policy and Terms of Use for their services on the internet. Member must make available a registry description and offer consultation, rectification, and/or removal of PII.

The Policy and the Terms MUST address at least

a. Entity name and contact for inquiries
b. Data retention policy
c. How is User identified (database keys, properties, such as pseudonymity, of identifier, etc.)
d. With whom data is exchanged and why
e. Whether the policy may change and how existing customers are handled upon the change.

A member MUST adhere to its own Policy and Terms.

2.2.2 General Technical Compliance Requirements

CR26-SSL All transactions that have monetary value or pass authentication credentials MUST run over encrypted (e.g. TLSv1, SSL or VPN) or physically secure network connections. Alternately the payload itself may be encrypted to similar strength, e.g. using [XMLENC].

For a network to be considered secure, it must achieve a security level equivalent to using any of the following cipher suites (assuming safe and sound key management practises):

a. DSA1024-SHA1-AES128-CBC
b. TLS_RSA_WITH_AES_128_CBC_SHA

This compliance requirement satisfies Reqs. *D1.2-2.21-DataProtLaw* and *D1.2-6.11-Confid*.

CR27-Sig All digital signatures MUST achieve at least the security level equivalent to using any of the following cipher suites (assuming safe and sound key management practises):

a. RSA1024-SHA1
b. DSA1024-SHA1

See threat T141-AltSig.

CR28-Vfy When data is signed, the intended recipient (see Audience) MUST verify the signature and MUST reject the operation if the verification fails. Verification of the signature MUST include in addition to the actual crypto operations, establishing that the signature was generated by the claimed trusted source.

For each verification, whether failed or successful, audit trail items MUST be generated, documenting at least

a. Signed data or its message digest (e.g. SHA1)
b. Who signed and how his trustworthiness was established
c. Date of signature and vertification and the credibility of both
d. Outcome of the verification
e. In case of verification failure due to failed message digest, the input to the message digest function

f. In case of verification failure due to failed public key crypto operation, the input to the operation (e.g. the message digest of the signed data).

See threat T141-AltSig.

CR29-Revoc Whenever long lived or revocable credentials are used (e.g. public key in signature verification), a revocation list or online status service (e.g. OCSP) SHOULD be consulted. If credential is SAML assertion, then long lived means more than 60 seconds. The revocation check SHOULD be done using Assertion Query Profile described in [SAML2prof].

The result MAY be cached for efficiency for duration indicated in relevant protocol and architecture specifications, but lacking clear indication, it should not be cached for longer than risk assessment dictates (if you are confused, do not cache for more than 10 seconds).

CR210-Rnd All signature and crypto operations MUST use a secure source of cryptographically strong random numbers. Acceptable sources include

a. Hardware approaches based on electic noise
b. `/dev/random`
c. `/dev/urandom` on busy machines and when seeded from strong source
d. Pseaudo random number generator with at least 128bit cycle, when seeded from a strong source (such as user input as in PGP).

Unacceptable sources include

i. Any predictable source
ii. Only seeding with current time and/or process identifier
iii. Less than 128bit cycle or search space

The random number pool should be consulted whenever new randomness is needed, but at the same time care should be taken to make sure that the pool is not unduely depleted of entropy. This is especially a risk whe using `/dev/urandom`.

Care should be taken to not to leak the random numbers except as strictly mandated by the protocols.

CR211-Uniq Whenever unique identifiers are called for, uniqueness must either be absolute (within specified namespace) or statistical with at least 128bits of search space.

See threat T61-Replay.

CR212-Trail Audit trail, including logs, MUST be digitally signed or otherwise tamper proof. Tamperproofness MUST achieve at least the security level equivalent to using any of the following cipher suites (assuming safe and sound key management practises):

a. RSA1024-SHA1

b. DSA1024-SHA1

Depending on circumstances, such as hosting of services in a untrusted data center, the logs SHOULD also be encrypted to achieve a security level equivalent to using any of the following cipher suites (assuming safe and sound key management practises):

i. RSA1024-SHA1-AES128-CBC

ii. DSA1024-SHA1-AES128-CBC

See threat T142-Tamper.

This compliance requirement addresses Reqs. *D1.2-2.17-AuditUntamp*, *D1.2-2.15-Resp*, *D1.2-6.10-Redress*, *D1.2-6.17-TechBind*, *D1.2-4.4-CourtProof*.

CR213-Backup All backups or batch data transfers MUST be in encrypted form ensuring security level equivalent to using any of the following cipher suites (assuming safe and sound key management practises):

a. RSA1024-AES128-CBC

b. DSA1024-AES128-CBC

See threat *T101-LeakBackup* and Req. *D1.2-2.21-DataProtLaw*.

CR214-CertSAML If SAML assertions are involved the software implementation MUST have passed the relevant SAML certification administered by the Liberty Alliance certification program.

CR215-CertIDWSF If Liberty ID-WSF is involved the software implementation MUST have passed the relevant certification administered by the Liberty Alliance certification program.

CR216-EntAn When Systems Entities are required to authenticate each other or assymmetrically one party, HTTPS MUST be supported and other X509v3 certificate based methods (PKI) MAY be supported. HTTP Authentication header based methods MAY be supported.

Authentication requirement CAN be satisfied at VPN, SSL, or application layer (e.g. application layer credentials or trusted digital signature over data). In any case, the authentication MUST be part of the audit trail in a cryptographically strong way and SHOULD be referenced by the summary audit events.

This satisfies Req. *D1.2-7.3-An*.

CR217-CertCert Certificates used for entity authentication and digital signatures MUST be obtained from a trustworthy authority. Designation of acceptable authorities MUST be made in the Governance Agreement of the Trust Network.

CR218-PrivKey Private Keys MUST be adequately protected. In the minimum this should mean procedural protections against exposure during generation, certification, install, and backup, as well as operational protection using file system permissions. Disclosure of private keys MUST be on strictly need to know basis.

2.3 Compliance Requirements for Governing Agreements

CR30-GA Governing Agreement should at least address

a. Governance structure, such as advisory and audit boards
b. Criteria to join and stay on the network, including certification and audits (Req. *D1.2-6.14-Compat*)
c. Process for removal from the network
d. Process for complaints, arbitration, and disciplinary action (Req. *D1.2-6.9-Complaint*)
e. Commercial liability and its fair appropriation
f. Liability due to negligence in criminal cases and its fair appropriation
g. Privacy protection
h. Redress for users that have suffered unwarranted disclosure (Req. *D1.2-6.10-Redress*)
i. Minimal mandatory security practises and policies (Reqs. *D1.2-6.11-Confid* and *D1.2-6.15-MinPolicy*)
j. Acceptable use for Service Providers
k. Acceptable use for Users

l. Requirement to be legally bound (Reqs. *D1.2-6.16-Bound* and *D1.2-6.17-TechBind*)

CR31-CheckList Any prospective Trust Network member should document the answer to the following questions:

a. Are you collecting or using PII as part of the service?
b. Do you have a Privacy Policy that you are bound to follow?
c. Do you use PII for any purpose other than providing the service?
d. Do you get User's consent or let him opt out before his information is used for other purposes than providing the specific service?
e. Do you share PII beyond your company or family of companies?
f. Do you get user's consent or let him opt out before your share his information with any other company not needed to provide the specific service?
g. Do you allow user to manage these preferences over time and change my options?

2.4 Compliance Requirements for Trust Guarantors

CR41-CoI Trusted Guarantor MUST NOT have a conflict of interest with any of the parties that are designed to trust it.

CR42-Records Trust Guarantor MUST maintain credible business records, including:

a. Members of the Trust Network (see CR24-File).

2.5 Compliance Requirements for Service Providers

CR51-DNSpub Service Provider MUST use DNS to publish its network addresses in a symbolic form. This requirement facilitates reconfigurations of the network. It is a well accepted "best practise".

CR52-BPM Service Provider's business processes MUST be modelled.

CR53-DontLogTok Service Requester SHOULD NOT log, even in encrypted form, the the tokens destined to the Service Responder or other parties if threat T107-LogTokLeak is a concern. If audit trail requires logging tokens, then the tokens must be blinded so that the correlatable part is not visible or

the token MUST be encrypted such that legitimate viewers of audit trail can decrypt it, but SP itself can not.

Compliance with this requirement is established with audits.

CR54-CorrConsent Service Provider MUST have user's consent before leaking a correlation handle of any kind.

CR55-MDExp Service Provider MUST implement Well-Known Location (WKL) method of metadata export, see [SAML2meta] section 4.1 "Publication and Resolution via Well-Known Location", p.29, for normative description of this method.

CR56-MDImp Service Provider MUST implement Well-Known Location (WKL) method of metadata import, see [SAML2meta] section 4.1 "Publication and Resolution via Well-Known Location", p.29, for normative description of this method. The Import MUST NOT unintentionally lead to a trust relationship.

CR57-VfyAn Service Provider MUST authenticate the Service Requester according to CR216-EntAn.

CR58-An Service Provider MUST authenticate itself to the Service Requester according to CR216-EntAn.

2.6 Compliance Requirements for Service Requesters

CR61-DNS Service Requester MUST use DNS to resolve names. This requirement facilitates configuration and provides a load balancing method (round robin DNS) for the SPs. DNS query results MUST NOT be cached beyond their TTL.

CR65-MDExp Service Requester MUST implement Well-Known Location (WKL) method of metadata export, see [SAML2meta] section 4.1 "Publication and Resolution via Well-Known Location", p.29, for normative description of this method.

CR66-MDImp Service Requester MUST implement Well-Known Location (WKL) method of metadata import, see [SAML2meta] section 4.1 "Publication and Resolution via Well-Known Location", p.29, for normative description of this method. The Import MUST NOT unintentionally lead to a trust relationship.

CR67-VfyAn Service Requester MUST authenticate the Service Provider according to CR216-EntAn.

CR68-An Service Requester MUST authenticate itself to the Service Provider according to CR216-EntAn.

2.7 Compliance Requirements for Databases Storing PII

Since Databases Storing Personally Identifiable Information (PII) usually are SPs, the requirements for SP also apply.

A future version of this document will specify in detail

- Special encryption concerns
- Special privacy protection
- Record keeping and audit

2.8 General Compliance Requirements for Trusted Third Parties

CR81-CoI Trusted Third Party MUST NOT have a conflict of interest with any of the parties that are designed to trust it.

2.9 Compliance Requirements for Identity Provider

CR91-CoI Identity Provider MUST NOT have a conflict of interest with any of the Service Providers or Users. In general, IdP functions can not be performed by a SP.

CR95-MDExp Identity Provider MUST implement Well-Known Location (WKL) method of metadata export, see [SAML2meta] section 4.1 "Publication and Resolution via Well-Known Location", p.29, for normative description of this method.

CR96-MDImp Identity Provider MUST implement Well-Known Location (WKL) method of metadata import, see [SAML2meta] section 4.1 "Publication and Resolution via Well-Known Location", p.29, for normative description of this method. The Import MUST NOT unintentionally lead to a trust relationship.

2.10 Compliance Requirements for Discovery Providers

CR101-CoI Discovery Providers MUST NOT have a conflict of interest with any of the Service Providers or Users. In general, the discovery and token mapping functions can not be performed by a SP.

CR105-MDExp Discovery Service MUST implement Well-Known Location (WKL) method of metadata export, see [SAML2meta] section 4.1 "Publication and Resolution via Well-Known Location", p.29, for normative description of this method.

CR106-MDImp Discovery Service MUST implement Well-Known Location (WKL) method of metadata import, see [SAML2meta] section 4.1 "Publication and Resolution via Well-Known Location", p.29, for normative description of this method. The Import MUST NOT unintentionally lead to a trust relationship.

2.11 Compliance Requirements for Trust and Reputation Provider

CR111-CoI Trust and Reputation Provider MUST NOT have a conflict of interest with any of the Service Providers or Users to which it provides trust scorings.

2.12 Compliance Requirements for Audit Provider

CR121-CoI Audit Provider, Audit Event Bus operator, or shared Event Bus Operator MUST NOT have a conflict of interest with any of the Service Providers or Users. In general, apart from SP internal audit, the audit functions can not be performed by a SP.

2.13 TAS^3-Lite Compliance Profile

The compliance requirements have been drafted to ensure true security and accountability. However we recognize that some of the compliance requirements are quite onerous and could be a hindrance to TAS^3 adoption in some low value situations. Therefore we define in this section a TAS^3-Lite profile that can be used in low value situations as long as the risks are recongnized and the deployment is not misrepresented as fully TAS^3 compliant. The TAS^3-Lite relaxations are as follows:

1. CR24-File and CR25-Policy are dropped. Informal means should be used to achieve the same end result. Dropping these requirements seriously compromises the ability of the Trust Network and the Users to hold parties accountable.

2. CR214-CertSAML and CR215-CertIDWSF are dropped due to financial cost of the certification. Attending cheaper informal interop events is still highly recommended.

3. CR217-CertCert is dropped. Self-certification is allowed.

4. CR30-GA is dropped. Informal governance structure is allowed. The consequence of this is most likely that parties can not be held responsible in case of serious violations.

5. CR52-BPM is dropped. Informal modelling is still recommended.

3 Future Work

- Elaborate more compliance categories

References

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

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

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

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

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

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

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

[IAF] Russ Cutler, ed.: "Identity Assurance Framework", Liberty Alliance, 2007. File: liberty-identity-assurance-framework-v1.0.pdf (from http://projectliberty.org/liberty/resource_center/papers)

[IGF] "An Overview of the Identity Governance Framework", Liberty Alliance, 2007. File: overview-id-governance-framework-v1.0.pdf (from http://projectliberty.org/liberty/resource_center/papers)

[LibertyLegal] Victoria Sheckler, ed.: "Contractual Framework Outline for Circles of Trust", Liberty Alliance, 2007. File: Liberty Legal Frameworks.pdf (from http://projectliberty.org/liberty/resource_center/papers)

[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

[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

Revision History

05 31.5.2009 Sampo

- Removed references to MD5

04 22.5.2009 Sampo

- Created TAS3-Lite profile
- Merged common entity reauirements to entity req section
- Diluted CR53-DontLogTok to apply only to situations where T107-LogTokLeak is imminent

03 30.3.2009 Sampo

- Added statement about applicability of [IAF]

02 24.3.2009 Sampo

- Added requirements re metadata
- Added requirements for peer entity authentication

01 14.3.2009 Sampo (sampo@symlabs.com)

- First draft out of blue, very incomplete and early status

Document ID `draft-tas3-compliance-v05.pdf`

Repository path `repo.tas3.eu:/var/lib/tas3repo/arch/tas3-compliance.pd` (1.20)

```
export CVSROOT=:ext:repo.tas3.eu:/var/lib/tas3repo
cvs co arch
cd arch
# modify tas3-*.pd
cvs ci -m 'What changed...'
```

URL path `https://portal.tas3.eu/arch/review/tas3-compliance-v05.pdf`

Commenting

- Please comment on the `TAS3WP02@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.