Category: guidelines document
Status: Approved
Document: IOTA-Secured-Infra-AP-1.0.doc
Editor: davidg
Last updated: Fri, 13 December 2013
Total number of pages: 8

Identifier-Only Trust Assurance with Secured Infrastructure

Abstract

This is an Authentication Profile of the IGTF describing the minimum requirements on X.509 PKI authorities where the identity vetting is adequate to ensure unique, non-re-assigned identities, and generated by authorities using secured and trusted infrastructure. Such authorities are not required to collect more data than are necessary for fulfilling the uniqueness requirements, and credentials issued by authorities under this profile may not provide sufficient information to independently trace individual subscribers, and should be used in conjunction with complementary identification and vetting processes.

This document is an EUGridPMA Guidelines Document, to be referred to as the "Guidelines on Identifier-Only Trust Assurance with Secured Infrastructure Authentication Profile", with OID 1.2.840.113612.5.2.2.6.1.

Table of Contents

1 Abstract

This is an Authentication Profile of the IGTF describing the minimum requirements on X.509 PKI authorities where the identity vetting is adequate to ensure unique, non-re-assigned identities, and generated by authorities using secured and trusted infrastructure. Such authorities are not required to collect more data than are necessary for fulfilling the uniqueness requirements, and credentials issued by authorities under this profile may not provide sufficient information to independently trace individual subscribers, and should be used in conjunction with complementary identification and vetting processes.

This Authentication Profile is managed by the EUGridPMA.

2 General Architecture

The authorities accredited under this authentication profile are long-term issuing entities serving a constituency of significant size, typically employing a distributed identity vetting model with a single credential issuance instance. Issued credentials are typically based on federated identity management services, where the subscriber identity is maintained by the credential issuing authority or by third parties trusted by the authority for the purposes of identifier assignment. Any such third parties must have a documented and verifiable relationship with the issuing authority, and through this relationship the issuing authority must have documented, verifiable and auditable means to ensure the requirements of this authentication profile are met. Credential issuance can be based on any primary authentication service, as long as this primary authentication service meets the requirements of this Profile.

Traceability of the credential is provided only in a cooperative way jointly with other parties that provide other elements of identity-related data. Credentials issued by authorities operating under this Authentication Profile should be used primarily in conjunction with vetting and authentication data collected by the relying parties, such that there is less need for collecting data that would otherwise duplicate efforts already performed by such relying parties.

Authorities are not required to collect more data than are necessary for fulfilling the uniqueness requirements. Credentials issued by authorities under this profile may not provide sufficient information to independently trace individual subscribers, and should be used in conjunction with complementary identification and vetting processes.

The authorities issue long-term credentials to end-entities, who will themselves possess and control their key pair and their activation data. These authorities act as organisationally-independent trusted third parties for both subscribers and relying parties within the infrastructure. These authorities will use long-term signing keys, which are stored in a secure manner as defined in the Profile.

To achieve sustainability, it is expected that each authority will be operated as a long-term commitment by institutions or organisations.

3 Identification

3.1 Persistency of name binding

Any single subject name in a credential must be linked with one and only one entity for the whole lifetime of the service. This subject name may be assigned to a person or automated actor. *In case the subject name is assigned to a non-human entity, the owner, being a human person or organisational group, should initiate the identification process.*

Validation of the credential request establishes the permanent binding between the end-entity, the owner, and the subject name.

3.2 Naming

The name elements contained in the issued credential must be sufficient to uniquely identify an individual.

If a commonName element is included in the credential, it must contain either an opaque unique identifier or a name chosen by the requestor and obtained from (a list proposed by) the IdP on which the issuer will enforce uniqueness.

The set of subject name elements included must:

- identify the identity management system via which the identity of this person was vetted, unless the vetting is done directly and solely by the issuing authority;
- contain sufficient information such that an enquiry via the issuer to the identity management system or issuing authority providing only this data allows unique identification of the vetted entity in this identity management system;
- be used only in conjunction with a verified element in the credential that allows direct contact to the subject (e.g. an email address[1]), which is known to be correct at time of issuance;
- be used only in conjunction with a subjectAlternativeName that contains an emailAddress attribute

No anonymous credentials may be issued under this profile.

3.3 Renewal and re-keying

Renewal or re-keying of a credential with a given subject name may only and exclusively proceed if there is conclusive evidence that the entity requesting this renewal or re-keying is the same entity as the one to whom the original credential was issued, and that the information contained in the new credential is correct.

3.4 Retention of records

If the authority supports renewal or re-keying of credentials where the subject name is re-asserted, the authority must retain sufficient information, or have sufficient information retained on its behalf, such that the persistency of name binding can be guaranteed. This is to ensure that the subject name, if subsequently reissued, refers to the same end-entity. Unless recorded documentary evidence is available to the authority at time of issuance, the subject name must not be bound in any renewed or re-keyed credential. The authority may rely in good faith on identity management systems by third parties, provided such third parties retain the necessary records.

3.5 Traceability requirements

At credential issuing time, the authority must reasonably demonstrate how it can verify identity information and trace this information back to a physical person (or for non-human credentials to a named group). At the time of issuance, the authority may rely in good faith on any identity management system by a third party with which it has entered into an agreement and that meets the requirements on third parties set forth in the General Architecture.

[1] e.g. one obtained from the identity management system, or one verified by the authority, or an obfuscated forward provided by the authority which redirects to a so-verified address

Ability to demonstrate persistent long-term authentication is required if the authority supports renewal or re-keying, in keeping with audit retention requirements. In the event that documented authentication persistency is lost, the subject name must never be re-asserted in any credential.

4 Operational requirements

The credential issuing system, where the signing of the end-entity credentials will take place, must be a dedicated system running no other services than those needed for credential issuing operations. The system must be located in a secure environment where access is controlled and limited to specific trained personnel. Due to the nature of the credential issuance, the issuing system will usually be connected to a network. To protect the private key material used to generate credentials, this system should be equipped with either

- a FIPS 140-2 level 3 capable Hardware Security Module (HSM) or equivalent where the CA system is operated in FIPS 140 level 3 mode to protect the CA's private key, or
- a FIPS 140-2 level 2 capable module with compensatory auditing mechanisms and physical security controls to attain a similar protection level for compromise or exposure of the private key.

An issuing authority that does not employ a FIPS 140-2 level 3 Hardware Security Module should describe the security precautions taken to protect the key material contained on the issuing system(s). The issuing systems architecture should provide for a tamper-protected log of issued credentials. The issuing computer must only be connected to a highly protected/monitored network, which may be accessible from the Internet.

The secure environment must be documented and approved by the accrediting body, and that document or an approved audit thereof must be available to the accrediting body.

The authority signing key must use the RSA method and have a minimum length of 2048 bits. Copies of the encrypted private key must be kept on off-line media in secure places where access is controlled. The signing certificate lifetime should not be more than 20 years.

4.1 Policy and practice statement

Every authority must have a Certification Policy and Certificate Practice Statement (CP/CPS document) and assign it a globally unique object identifier (OID). CP/CPS documents should be structured as defined in RFC3647. Whenever there is a change in the CP/CPS the OID of the document must change and the major changes must be announced to the accrediting body and approved before signing any certificates under the new CP/CPS. All the CP/CPS documents under which valid certificates are issued must be available on the web.

4.2 Certificate and CRL profile

The accredited authority must publish a X.509 certificate as a root of trust. This root of trust, as well as any higher-level certificates used to validate this root of trust up to a self-signed credential, must comply with the certificate profile as defined in GFD.125.

The authority must issue and publish RFC5820 version 2 certificate revocation lists (CRLs), and have the capability to list revoked certificates. The maximum 'validity' period of CRLs must be at most 30 days, i.e. the next update date must be no longer than 30 days beyond the time of issuance. The authority must issue a new CRL at least 7 days before the time stated in the nextUpdate field for off-line CAs, at least 3 days before the time stated in the nextUpdate field for automatically issued CRLs by on-line CAs, and immediately after a revocation.

The authority shall issue X.509 certificates to end entities based on cryptographic data generated and stored according to the Private Key Protection guidelines. Cryptographic data pertaining to the issued credential should be under sole effective control of the applicant.

The end-entity certificates keys must use the RSA method and be at least 2048 bits long. Issuing credentials must have a maximum validity period not extending beyond 400 days of issuance, and it may be as short as the authority will support.

The end-entity certificates must be in X.509v3 format and compliant with GFD.125. It must contain a OID policy identifier for this authentication profile. If the issuing authority operates a production service OCSP responder, the AuthorityInfoAccess extension must be included and must contain at least one URI.

If a commonName component is used as part of the subject DN, it must comply with the requirements on naming in section 3.

The message digests of the certificates and revocation lists must be generated by a trustworthy and cryptographically sound mechanism.

4.3 Revocation

Revocation requests can be made by certificate holders, identity management system managers and the issuing authority. Such requests must be properly authenticated before being acted upon. Any other entity can request revocation if they can sufficiently demonstrate compromise or exposure of the associated private key material, or if they can demonstrate that any data contained in the credential is incorrect. Managers of identity management systems involved in issuing credentials may request revocation of credentials if their stored identity data changes or when traceability to the person is lost. Individual holders of a credential must request revocation if the private key pertaining to the credential is lost or has been compromised, or if the data in the credential are no longer valid.

The authority must react as soon as possible, but within one working day, to any revocation request received. After determining its validity, the published revocation information must be updated immediately. Credential revocation information must be published in a repository at least accessible via the http protocol in CRL format.

5 Security requirements

The credential issuing system, supportive directory system(s), and in general systems involved in the identification of entities either part of the authority or at third parties with which the authority has entered into an agreement for identity management should be highly secure and trustworthy systems, managed according to current IT industry best practices for security sensitive systems, for example ISO27000 series, SP800-63, DIN, etc.

Any private key materials associated with issued credentials must not be disclosed to or shared with end-entities other than the one to which the credential was issued and the private key must be protected in accordance with the currently approved version of the “Guidelines on Private Key Protection”[2].

5.1 Third parties involved in identity management

The authority must not knowingly continue to rely on data from third parties that provide inaccurate or fraudulent information. It is strongly recommended that any third party on which the issuing authoritity relies has an incident response capability and is willing to participate in resolving such incidents.

[2] OID 1.2.840.113612.5.4.1.1.1.5. See http://www.eugridpma.org/guidelines/pkp

The identity management system(s) of the organizations or federations must be well protected, and all communications between the identity management systems and the credential issuance setup must be protected against exposure and tampering and be authenticated.

6 Publication and repository responsibilities

Each authority must publish for their subscribers, relying parties and for the benefit of distribution by the accreding body and the federation:

- a http or https URL of the web page of the authority containing general information;
- a X.509v3 formatted root certificate or set of certificates up to a self-signed root;
- a http or https URL pointing to a copy of these certificates on the authority web site, in PEM or DER format;
- a http URL of a PEM or DER formatted certificate revocation list;
- the CP and CPS documents, and a http link thereto on the authority web site;
- an official contact email address for inquiries and fault reporting;
- a physical or postal contact address.

The authority should provide a means to validate the integrity of their root of trust. Furthermore, the authority must provide their trust anchor to a trust anchor repository, specified by the accrediting body, via the method specified in the policy of the designated trust anchor repository.

The repository operated by the authority must be run at least on a best-effort basis, with an intended continuous availability.

The authority must grant to the accrediting body and any federations in which it participates – by virtue of its accreditation – the right of unlimited re-distribution of the above-listed published information.

7 Audits

The authority must record and archive all requests for certificates, along with all the issued certificates, all the requests for revocation and the login, logout, and reboot actions affecting the issuing machine. The authority must keep these records for at least three years, and these records must be made available to external auditors in the course of their work as auditor.

Each authority must accept being audited by another accredited authority to verify its compliance with the rules and procedures specified in its CP/CPS document.

The authority should perform internal operational audits of its staff and of interfaces between components and systems. These audits should be performanced at least once per year to verify its compliance with the rules and procedures specified in its CP/CPS document. Audit results shall be made available to the accrediting body upon request. A list of authority and site identity management personnel should be maintained and verified at least once per year.

The auditing does not necessarily extend to identity vetting systems operated by third parties and used for credential issuance.

8 Privacy and confidentiality

Accredited authorities must define and follow a privacy and data release policy compliant with the relevant national legislation. The authority is not required to release private information information unless provided by a valid request according to national laws applicable to that authority.

9 Compromise and disaster recovery

The authority should have a business continuity and disaster recovery plan and be willing to discuss this procedure with the accrediting body. The procedure need not be disclosed in the CP/CPS.

9.1 Due diligence for subscribers

The authority should make a reasonable effort to ensure that subscribers are informed of the importance of properly protecting their private data, as described in the Private Key Protection guidelines. When using software tokens, the private key must be protected with a strong pass phrase, i.e. at least 12 characters long and following current best practice in choosing high-quality passwords.

Subscribers must request revocation as soon as possible, but within at least one working day, after detection of loss or compromise of the private key pertaining to the certificate, or if the data in the credential is no longer valid. A subscriber should request revocation if the credential is no longer in active use.