Difference: LiveAPSecuredInfra (6 vs. 7)

Revision 7 2013-05-07 - DavidGroep

Line: 1 to 1

META TOPICPARENT	name="PolicyDrafts"

Light-weight Identity Vetting Environment with Secured Infrastructure Authentication Profile

Line: 8 to 8

This is an Authentication Profile of the International Grid Trust Federation describing the minimum requirements on X.509 PKI CAs where the identity vetting is adequate to ensure unique, non-re-assigned identities, and generated by authorities using secured and trusted infrastructure. Tracability is provided for the life time of the credential 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.

Changed:

< Authorities may collect only so much data as is 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.

> 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 CAs 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 is stored in a secure manner as defined in the Profile.

Line: 16 to 16

General Architecture

Changed:

< 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 identity vetting and verification. 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.

> 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.

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

Changed:

< ## Identity
<

> ## Identification
>

Persistency of name binding

Changed:

< 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, to a service, or to a networked system. In case the subject name is assigned to a non-human entity, a human person or organsational group is registered as the name owner, and the authority asserts that the person or organisational group has valid rights to exclusive use of that subject name.

> 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, a human person or organsational group should initiate the identification process.*

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

Changed:

< Any private key materials associated with the issued credential must not be disclosed to or shared with end-entities other than the one to which the
< credential was issued. For certificates issued to persons, the private key must be protected in accordance with the currently approved version of the "Guidelines on Private Key Protection" (1).

Notes

1 : OID 1.2.840.113612.5.4.1.1.1.5 at http://www.eugridpma.org/guidelines/pkp

> Any private key materials associated with the issued credential 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).

Naming

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

Changed:

< If a commonName element is included in the credential, is must contain an appropriate representation of the real name of the entity. This name
<
- in case of network entities, must include the fully qualified domain name or which the subdomain part registered in a public domain registry must be explicitly validated by the authority;
- in case of service or other non-human entities, must include either the fully qualified domain name from which the credential is used, validated as for regular network entities, or a name uniquely identifying the responsible person, or an identifier of a group in such a way that this group can be contacted based on the registered information;
- in case of human entities, must be an appripriate representation of the persons real name.

> If a commonName element is included in the credential, it must contain either a opaque unique identifier or a name chosen by the requestor on which
> the issuer will enforce uniqueness.

Changed:

< If pseudonymous naming is used, such a name element must
< - only be used for human entities;

>
> The set of 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;

Changed:

< - contain sufficient information such that an enquiry 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 subject name element that allows direct contact to the subject (e.g. an email address), which is known to be correct at time of issuance;
- be used only in conjunction with a subject name element that explicitly indicates, in human-understandable form, that this credential is pseudonymous;
- be used only in conjunction with a subjectAlternativeName that contains an emailAddress attribute.

> - 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), 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.

Re-issuance, renewal and re-keying

Changed:

< Re-issuance, 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 re-issuance, renewal or re-keying is the same entity as the one to whom the original credential was issued. For non-homan entities, the person or organisational group requesting this re-issuance, renewal or re-keying of the credential must at time of re-issuance still hold the exclusive use of the subject name listed in the credential.

> Re-issuance, 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 re-issuance, renewal or re-keying is the same entity as the one to whom the original credential was issued.

Retention of records

If the authority supports re-issuance, 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.

Changed:

< This is to ensure that the subject name, if subsequently reissued, refers to the same end-entity. Unless recoded documentary evidence if available to
< the authority at time of issuance, the subject name must not be bind in any re-issued, renewed or re-keyed credential. The autority may rely in good faith on identity management systems by third parties, provided such third parties retain the necessary records and these records are subject or may be made subject to external auditing.

> This is to ensure that the subject name, if subsequently reissued, refers to the same end-entity. Unless recorded documentary evidence if available to
> the authority at time of issuance, the subject name must not be bound in any re-issued, renewed or re-keyed credential. The autority may rely in good faith on identity management systems by third parties, provided such third parties retain the necessary records.

Tracability Requirements

Changed:

< When issuing credentials to end-entities, the authority must provide subject name accountability. At credential issuing time, the authority must
< demonstrate how it can verify identity information and trace this information back to a physical person (or for non-human credentials to named group) at the time of issueance. 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 section 2.

> 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 named group) at the time of issuance. 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 General Architecture.

Changed:

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

> Ability to demonstrate persistent long-term authentication is required if the authority supports re-issuance, 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.

Operational Requirements

Changed:

< 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 issuign system will usually be connected to a network. To protect the private key material used to generate credentials, this system must be equipped with at least a FIPS 140 level 3 capable Hardware Security Module (HSM) or equivalent, and the CA system must be operated in FIPS 140 level 3 mode to protect the CA's private key. The issuing system may employ a FIPS 140-2 level 2 capable module and have compensatory auditing mechanisms and physical security controls to attain a similar protection level. 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 certificates. The CA computer must only be connected to a highly protected/monitored network, which may be accessible from the Internet.

> 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 must be equipped with at least a FIPS 140 level 3 capable Hardware Security Module (HSM) or equivalent, and the CA system must be operated in FIPS 140 level 3 mode to protect the CA's private key. The issuing system may employ a FIPS 140-2 level 2 capable module and have compensatory auditing mechanisms and physical security controls to attain a similar protection level. 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.

Line: 80 to 75

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.

Changed:

< The authority must issue and publish certificate revocation lists (CRLs), and have the capability to list revoked certificates unless none of the issued end
< entity certificates have a validity beyond 1 million seconds (~ 11 days) of date of issuance. The maximum 'validity' period of CRLs must be at most 30 days, i.e. the next update date should 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 must issue and publish 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.

Changed:

< 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 by the applicant.

> 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.

Changed:

< 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 1 year and one month from date of issuance, and it may be as short as the authority will support.

> 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.

Changed:

<
< If a commonName component is used as part of the subject DN, it should contain an appropriate presentation of the actual name of the end-entity.
<

>
> 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 must be generated by a trustworthy and cryptographically sound mechanism.

Revocation

Changed:

< 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 of they can demonstrate that any data contained in the credential is incorrect. Managers of identity management systems involved in issuing credentials should request revocation of credentials if their stored identity data changes or when traceability to the person is lost.

> 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 should request revocation of credentials if their stored identity data changes or when traceability to the person is lost.

Changed:

< 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.

> 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.

Security Requirements

Line: 105 to 99

The secure environment must be documented, and this documentation must be approved by the accrediting body. If technical details are not included in the that document an approved audit thereof must be available to the accrediting body.

Deleted:

< This secure environment minimally includes the following:

<

- The credential issuing computer should be equipped with at least a FIPS 140-2 level 2 rated Hardware Security Module or equivalent, and the system operated substantially in FIPS 140-2 level 2 mode [FIPS140], to protect the signing key material. Additionally, the private key should not be exportable from this system in plaintext form. Alternative configurations must demonstrate how the security precautions taken to protect the signing key meet the functional security objectives of FIPS 140-2 and substantially meet the security requirements of security level 2, to the satisfaction of the accrediting body.
- The credential issuing computer must only be connected to a highly protected/monitored network, which may be accessible from the Internet.
- The credential issuing computer, i.e. the system where the signing of the credentials will take place, must be a dedicated machine, and must run no other services than those needed for the credential issuing operations.
- The credential issuing computer must be located in a secure environment where access is limited to specific trained personnel.
- The issuer signing key must use the RSA algorithm and must have a minimum length of 4096 bits.
- Copies of the encrypted signing key must be kept on off-line media only in secure places where access is controlled.
- The issuer signing certificate lifetime should not be more than 20 years.

Third parties involved in identity management

Changed:

< Any third parties with which the authority has entered into an agreement to provide identity information must participate in security incident response.

< This includes but is not limited to serving as a conduit for messages to the subscriber in case the authority does not itself retain such information, or in cases where the recoded information is no longer accurate or is deemed to be false or fraudulent. In cases of sufficient gravity, involved third parties shall actively participate in joint investigations with the issuing authority and take all necessary action to prevent the incident from spreading or re-occuring, and support investigative enquiries and legal action if and when appropriate.

> The authority must not knowingly continue to rely on data from third parties that provide inaccurate or fraudulent information. It is 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.

Changed:

< 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 well secured and authenticated.

> 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.

Publication and Repository responsibilities

Line: 136 to 121

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

Changed:

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

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

Audits

Line: 144 to 129

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

Changed:

< The authority should perform internal operational audits of its staff and of systems interfaces between components and systems. These audit 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 authority should perform internal operational audits of its staff and of interfaces between components and systems. These audit 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.

Changed:

< Any identity vetting systems used for credential issuance, including those operated by third parties with which the authority has entered into an
< agreement, must allow auditing by the authority of the third party systems' policies, procedures and practices. The results of such audits must be made availble to the accrediting body upon request. Audits of third parties must demonstrate that sufficient information is retained to ensure that any name bindings made by the system are unique, persistent and non-reusable, i.e. that name binding uniqueness is ensured.

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

Privacy and confidentiality

Changed:

< Accredited authorities must define and follow a privacy and data release policy compliant with the relevant national legislation. The authority is
< responsible for recording or having recorded, at the time of validation, sufficient information to identify the person getting the certificate. The CA is not required to release such information unless provided by a valid legal request according to national laws applicable to that authority. Unless prohibited by such national law, the any and all parties involved in the vetting process shall cooperate fully with security incident response processes.

> 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 such information unless provided by a valid request according to national laws applicable to that authority.

Compromise and disaster recovery

Line: 158 to 143

Due diligence for subscribers

Changed:

< The authority should make a reasonable effort to make sure that subscribers realize 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. Private keys pertaining to host and service certificate may be stored without a passphrase, but must be adequately protected by system methods.

> The authority should make a reasonable effort to make sure that subscribers realize 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.

Changed:

< Subscribers must request revocation as soon as possible, but within 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.

> 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.

-- DavidGroep - 2013-01-15 \ No newline at end of file