Classic X.509 secured profile version 4.2 Proposed Changes

David Groep, Nov 7nd, 2008

Updates

- Propose to change the Classic AP
  - Improved wording
  - RobotReady™
  - Accommodate GFD.125
  - Better CRL handling
  - Realistic re-keying

- See also http://www.eugridpma.org/guidelines/IGTF-AP-classis-difference-4-1-to-4-2.pdf

Identity vetting rules

- Updates to better reflect existence of robot certificates

In order for an RA to validate the identity of a person, the subject should contact the RA face-to-face and present photo-id and/or valid official documents showing that the subject is an acceptable end entity as defined in the CP/CPS document of the CA.
In case of non-personal certificate requests, the RA should validate the identity and eligibility of the person in charge of the specific entities using a secure method.
For host and service certificate requests, the RA should ensure that the requestor is appropriately authorized by the owner of the associated FQDN or the responsible administrator of the machine to use the FQDN identifiers asserted in the certificate.
The RA must validate the association of the certificate signing request.
The CA or RA should have documented evidence on retaining the same identity over time.
The CA is responsible for maintaining an archive of these records in an auditable form.

Wording improvements on CA/RA

- New wording to accommodate CP/CPS-es with a secure but novel method for securing CA-RA communications

All communications between the CA and the RA regarding certificate issuance or changes in the status of a certificate must be by secure and auditable methods. The CP/CPS should describe how the RA or CA is informed of changes that may affect the status of the certificate.

- Updates on the rekeying and renewal section
  - Better wording and expression of intent

The CA issuing system

- Improved wording on issuing system

4 Operational Requirements

The CA systems must be located in a secure environment where access is controlled, limited to specific trained personnel.
The CA computer where the signing of the certificates will take place must be a dedicated machine, running no other services than those needed for the CA signing operations. The CA signing computer may be either

- on-line: the certificate issuing machine is directly or indirectly connected (by wire, wireless

Certificate Profile – GFD.125 cleanup

4.3 Certificate and CRL profile

The accredited authority must provide and allow distribution of a (sufficient collection of) X.509 certification authority certificates to enable validation of end-entity certificates. All certificates , including all end-entity certificates subject to this Authentication Profile, must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

The authority shall issue X.509 certificates to end-entities based on cryptographic data generated by the applicant, or based on cryptographic data that can be held only by the applicant on a secure hardware token.

The end-entity keys must be at least 1024 bits long. The end-entity certificates must have a maximum lifetime of 1 year plus 1 month.

In the end-entity certificate extensions:

- a *policyIdentifier* must be included and must contain an OID identifying the CP document under which the certificate was issued, and should contain only OIDs
- the *policyIdentifier* must include the OID for this profile: 1.2.840.113612.5.2.2.1
- *CRLDistributionPoints* must be included and contain at least one http URL
- an OCSP URI may be included in the *AuthorityInfoAccess* extension only if the OCSP responder is operated as a production service by or on behalf of the issuing CA

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.

The authority must publish CRLs, and these CRLs should be compliant with RFC5280

Certificate Profile - OIDs

- New text makes it explicit that the OID of the profile MUST be included in the certificates issued under this profile

- Also, add relevant 1SCP OID

This will enable relying parties to make judgements based on the OIDs

… and will get us out of the chicken-and-egg mess

Revocation

- Accommodate on-line CAs that can auto-reissue a CRL frequently, **and** make up for too-short CRLs

4.4 Revocation

The CA must publish a CRL. The CA must react as soon as possible, but within one working day, to any revocation request received. After determining its validity, a CRL must be issued immediately. For CAs issuing certificates to end-entities, the maximum CRL lifetime[3] must be at most 30 days. The CA 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

[3] The CRL life time is defined as the difference between the times stated in *nextUpdate* and *thisUpdate*.

automatically issued CRLs by on-line CAs, and immediately after a revocation. The CRLs must be published in a repository at least accessible via the World Wide Web, as soon as issued.

Subscriber due diligence

- Improved wording

9.1 Due diligence for subscribers

The CA should make a reasonable effort to make sure that subscribers realize the importance of properly protecting their private data. 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.

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 certificate is no longer valid.

Implementation

- EUGridPMA has standing guidelines to implement changes in the profile within 6 mo
- Please have a look at these proposed changes


eu
gridpma