Category:
Status: Public Consultation
IGTF-PKITechnologyGuidelines-1.0.docx
Editor: David Groep
Last updated: Tue, 10 May 2016
Total number of pages: 6

IGTF PKI Technology Guidelines

Version 1.0-2016

Abstract
The Interoperable Global Trust Federation (IGTF) is a body to establish common policies and guidelines that help establish interoperable, global trust relations between providers of e-Infrastructures and cyber-infrastructures, identity providers, and other qualified relying parties.

The IGTF PKI Technology Guidelines define how X.509 structured credentials are to be issued, managed, distributed, and withdrawn to comply with the IGTF Authentication Profiles. It may be used in conjunction with technology-agnostic identity assurance specifications to define such Authentication Profiles.

Identifications
This document: **urn:oid:1.2.840.113612.5.2.7.1**

Table of Contents

1 About this document

This PKI Technology Guideline applies to X.509 Public Key Certification Authorities (traditional PKI CAs). For subscribers and relying parties they act as trusted third parties within distributed multi-domain ICT infrastructures for the purposes of authentication.

In this document the key words `must', `must not', `required', `shall', `shall not', `recommended', `may', and `optional' are to be interpreted as described in RFC 2119. If a 'should' or 'should not' is not followed, the reasoning for this exception must be explained to relevant accrediting bodies to make an informed decision about accepting the exception, or the applicant must demonstrate to the accrediting bodies that an equivalent or better solution is in place.

2 General Architecture

Certificate Authority trust anchor information comprising certificates and associated meta-data such as revocation distribution information, proposed relying-party defined namespace constraints, and contact details is distributed by the IGTF to relying parties using controlled distribution mechanisms. The IGTF trust anchor distribution, including the content provided by the CAs, must be stable and its integrity protected.

End-user browser trust is not considered in scope for this document.

To achieve sustainability, it is expected that each CA will be operated as a long-term commitment by organisations. *The authorities will use long-term signing keys that are stored in a secure manner.*

3 Identity

3.1 End-entity, subscriber and user identity validation

Each CA must define the role of registration authority (RA) in its Certificate Policy and Certification Practices Statement (CP/CPS) or in an RPS. The RA is responsible for the identity validation of end-entities, organisations, and subscribers.

3.2 Identifier assignment

The credentials issued by the CA are GFD.225[1] X.509 version 3 certificates.
Every issued certificate must have a unique serial number within the context of the issuing CA.

Neither the subject nor the issuer distinguished names (DNs) in the certificate shall be empty.

The issuer DN of the CA must be unique amongst all IGTF distributed CAs, and the accredited organisation should make reasonable efforts to ensure the issuer DN is globally unique.

The subject DN of end-entity certificates shall be a sequence of relative DN (RDN) components, starting the ASN.1 sequence with one or more RDN elements together identifying the accredited organisation and endorsed by the IGTF at the time of accreditation. This initial sequence of RDN components shall be uniquely assigned to this organisation amongst all IGTF distributed CAs. It should consist of a sequence of domainComponent RDNs where the corresponding domain name is controlled by the accredited organisation.

The subject DN (subjectName) in a certificate is the unique non-reassigned identifier assigned to an end-entity. The subject DN shall never be assigned to a different entity. It is however not contrary to this requirement for a single entity to have more than one associated subject DN, e.g., for different key usages, or to have more than one certificate with the same subject DN.

[1] Pending approval of GFD.225, "GFD.125" should be read throughout.

If the assurance specification stipulates that the unique identifier must include a presentation of the actual name of the entity, this actual name must be represented as a *commonName* RDN element as part of the subject DN. Other elements that represent the name of the individual entity that are included in the certificate should be represented in or as a *commonName* as part of the subject DN.

If the credential has elements that allow direct contact to the subject, such as an email address, these elements should be included as subjectAlternativeName.

For certificates issued to end-users, the CP/CPS should state that the associated private key must be protected in accordance with the currently approved version of the "IGTF Guidelines on Private Key Protection" [2]. Otherwise, the private key associated with any certificate must only ever be disclosed to the entity to which the certificate was issued and its subject.

3.3 End-entity certificate expiration, renewal and re-keying

The processes used for the issuing of certificates based on new or previously certified key material must be described in the CP/CPS, and must comply with all corresponding assurance specification requirements.

PKI credentials can be extended or renewed as permitted by the assurance specification, but once the maximum validity period has passed, the key pair on which the credential was based must not be re-used.

The identity and eligibility re-verification procedure must be described in the CP/CPS.

3.4 Revocation

Revocation requests can be made by the authenticated end-entity to which a certificate belongs, by RAs, or by the CA. Others can request revocation if they can sufficiently prove compromise or exposure of the associated private key, or violation of the policy requirements. Neither an RA nor the CA can charge for revocation of a certificate.

The CA must react as soon as possible, but within one working day, to any valid revocation request received.

4 Operational Requirements

4.1 Systems requirements for off-line and on-line CAs

The CA system 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

1. entirely and continuously off-line, i.e. kept disconnected from any kind of network at all times, or
2. must comply with the "Guidelines for On-line PKI Certification Authorities"[3].

Any CA where the certificate issuing machine is directly or indirectly connected (by wire, wireless or any other means) to any other computer device (including peripherals that themselves could be simultaneously connected to devices not an integral part of the certificate issuing machine) is considered to be an on-line CA.

[2] OID 1.2.840.113612.5.4.1.1.1.5 at http://www.eugridpma.org/guidelines/pkp
[3] https://www.eugridpma.org/guidelines/online-cas

4.2 CA Certificate and Private Key Requirements

The length of the CA key for RSA based cryptography must be at least 2048 bits and should be at least 4096 bits[4]. For CAs that issue end-entity certificates the lifetime of the CA certificate must be no less than two times of the maximum lifetime of an end entity certificate and should not be more than 20 years.

Software-based private keys of the CA must be protected with a pass phrase of at least 15 characters and that is known only by designated personnel of the Certification Authority.
CAs using an HSM must adopt an equivalent or better level of security.
Copies of the encrypted private key must be kept on off-line media and only in secure places where access is controlled.

4.3 Certificate Policy and Certification Practices Statement Identification

Every CA must have CP and CPS documents. These documents may be combined, and should be structured as defined in RFC 3647. All relevant sections of RFC3647 should be completed and provide sufficient information to assess compliance of the CA with the applicable assurance specification and with these PKI Technology Guidelines by Relying Parties and accrediting PMAs.

The CA must assign a globally unique object identifier (OID) to the CP and CPS documents.

Whenever there is a material change in the CP/CPS the OID of the document must change and the major changes must be announced to the accrediting PMA and approved before signing any certificates under the new CP/CPS. The applicable CP/CPS under which valid certificates are issued must be available to qualified Relying Parties and accrediting PMAs.

4.4 Certificate and CRL profile

The accredited authority must provide and allow distribution of a (sufficient collection of) X.509 certification authority certificates. Similarly, validation data for an applicable chain to enable verification of end-entity certificates must be provided.

All certificates, including all end-entity certificates subject to the relevant Authentication Profile, must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.225 or its latest successor document.

The authority shall issue X.509 certificates to end-entities based on cryptographic data generated according to the IGTF PKP Guidelines.

RSA-based end-entity keys must be at least 2048 bits long, and other key types of at least equivalent cryptographic strength.

The end-entity certificates must have a defined lifetime, and the end of its validity should not exceed its ability to be validated.

The subject and issuer DN shall be constructed as defined by the identifier assignment, exclusively as a sequence of size-one-sets of attribute-value pairs.

In the end-entity certificate extensions:

- a *policyIdentifier* must be included, and it must contain only OIDs.
  It must include at least the OID for the appropriate Authentication Profile compliant to which the certificate was issued.
  It may contain the OIDs for the assurance specification indicated in the Authentication Profile.
  It should also contain an OID identifying the CP document under which the certificate was issued and other applicable OIDs;

[4] Or of equivalent strength, as described in e.g. NIST SP800-57.

- the *CRLDistributionPoints* extension must be included and must contain at least one http URL;
- an OCSP URI should be included in the *AuthorityInfoAccess* extension, but must not be included unless the OCSP responder is operated as a secure production service by or on behalf of the issuing CA with sufficient availability for its intended use.

Issued CRLs should be substantially[5] compliant with RFC5280 and its update RFC6818.

4.5 Revocation

The CA must publish a Certificate Revocation List (CRL).

The CA must react as soon as possible, but within one working day, to any valid revocation request received. After determining its validity, a CRL must be issued forthwith.

For CAs issuing certificates to end-entities, the maximum CRL lifetime[6] must be at most 30 days.

A CA that is off-line must issue a new CRL at least 7 days before the time stated in the *nextUpdate* field or promptly after processing a revocation.
A CA that is on-line and issues CRLs automatically, must issue a new CRL at least 3 days before the time stated in the *nextUpdate* field or promptly after processing a revocation.

CRLs must be published in a repository accessible via HTTP as soon as issued.

Revocation data may also be published in other formats.

4.6 CA key changeover

When the CA's cryptographic data needs to be changed, such a transition shall be managed; from the time of distribution of the new cryptographic data, only the new key will be used for certificate signing purposes. The accrediting PMAs shall be informed of the new CA data.

The overlap of the validity periods of the certificates relating to the old and new keys must be at least the longest time an end-entity certificate is valid and also until at least the *nextUpdate* time of the last CRL after all previously valid certificates have been revoked or have expired.

The older but still valid certificate must be available to verify old signatures – and the secret key to sign CRLs and other revocation data – until all the certificates signed using the associated private key have also expired or been revoked, and the CA has been withdrawn from the IGTF Distribution.

5 Site security

The CA systems must be located in a secure environment where access is controlled, limited to specific, authorized, and trained personnel.

The pass phrase of the encrypted private key of the CA must be kept also on an offline medium, separated from the encrypted keys and guarded in a safe place where only the authorized personnel of the Certification Authority have access. Alternatively, another documented procedure that is equally secure may be used.

[5] As further specified at http://wiki.eugridpma.org/Main/IGTFCRLProfile
[6] The CRL lifetime is defined as the difference between the times stated in *nextUpdate* and *thisUpdate.*

6 Publication and Repository responsibilities

Each authority must publish, on the world-wide web and gratis, for their subscribers, relying parties and for the benefit of distribution by the IGTF:

- the CA root certificate and the set of CA certificates up to a self-signed root;
- at least one http or https URL of the PEM or DER formatted CA certificate(s);
- at least one http URL of the PEM or DER formatted CRL(s);
- an http or https URL of a web page of the CA for general information;
- the relevant CP and/or CPS documents or a corresponding URL;
- an official contact email address for inquiries and fault reporting, and valid messages sent to this address must be responded to within one working day;
- a physical or postal contact address of the CA organisation.

The authority must grant to the PMA and the IGTF Federation – by virtue of its accreditation – the right of unlimited and gratis re-distribution of this information.

The repository is expected to be continuously available, maintained on at least a best-effort basis. The CA must respond within a reasonable time period to all valid communications sent ot the CA.

The CA should provide a means to validate the integrity of its root of trust. Furthermore, the CA shall provide their trust anchor to a trust anchor repository, specified by the accrediting PMA, via the method specified in the policy of the trust anchor repository.

7 Audits

The CA must record and archive all requests for certificates, along with all the issued certificates, all the requests for revocation, all the issued CRLs and the login, logout, start-up, and shutdown of the issuing system.

All certificates issued by an end-entity issuing CA are subject to the auditing requirements. Intermediate CAs and Root CAs are subject to the auditing requirements insofar as their certificates, and the certificates they issued, pertain to an accredited subordinate issuing CA. The accrediting PMA must be able to assess that auditing requirements are being met on an ongoing basis.

8 Privacy and confidentiality

The content of issued certificates may be considered public and not subject to privacy and confidentiality controls. The CA must describe its privacy and confidentiality plan in the CP and/or CPS.

9 Compromise and disaster recovery

A compromise and disaster recovery plan must be described in the CP and/or CPS.

10 Other obligations

10.1 Due diligence for subscribers and users

Private keys used with certificates issued to end-users must be generated and stored in accordance with the currently approved version of the “Guidelines on Private Key Protection”[7].

Private keys pertaining to host and service certificates may be stored without a passphrase, but must be adequately protected by system methods against disclosure and unauthorized access.

[7] OID 1.2.840.113612.5.4.1.1.1.5 at http://www.eugridpma.org/guidelines/pkp