Check list for a Traditional X.509 Public Key CAs. IGTF classic profile: IGTF-AP-classic-4-2

CA Website: Name of site being reviewed

Reviewers:

Profile sections	Sections in RFC 3647	Sections in RFC 2527	Item# in Auditing doc.	Does CP/CPS Conform?	
				Y/N	Comments or CP section applicable
1 Introduction					
General description				N/A	RFC 2527 based CP/CPS
2 General Architecture					
There **should** be a Single CA per country, region or International organization.	§ 1.3..1	1, 1.3.1	CA-(2)		
It is **expected** that the organization commit to long term management of the CA. Not a short lived project.				N/A	PMA guidance not a CP/CPS issue
There **should** be a Single EE CA with a network of RAs	§ 1.3.2	1, 1.3.2	CA-(3)		
3 Identity					
The DN **must** be linked to one an only one EE, over the lifetime of the CA.	§ 3.1.5	3.1.4	RA-(8), (9)		
Certificates **must** not be shared among EEs.	§ 4.5.1	2.1.3	CA-(35)		
3.1 Identity Vetting rules					
The CA **must** define an RA role, which is responsible for the Identity vetting of all EEs.	§ 4.1, 4.2, 4.6, 4.7	2.1.2, 4.1	RA-(1)		
People certificates: the subject **should** contact RA in F2F meeting, and present photo-id and/or valid official documents showing that the subject is an acceptable EE as defined by CP/CPS.	§ 4.1, 4.2, 4.6, 4.7	2.1.2, 4.1	RA-(2)		
Host/Service certificates: The RA **should** validate the identity of the person in charge of the entity using a secure method.	§ 4.1, 4.2, 4.6, 4.7	2.1.2, 4.1	RA-(3)		
RA **should** ensure that the requester 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.	§ 4.1, 4.2, 4.6, 4.7	2.1.2, 4.1	RA-(4)		
RA **must** validate the association of the certificate signing request.	§ 4.1, 4.2, 4.6, 4.7	4.3	RA-(5)		
The CA or RA **should** have documented evidence on retaining the same identity over time.	§ 3.2.3	Where?	RA-(6)		
The CA **is responsible for** the maintaining an archival and audit-ability of its records.			RA-(13)		PMA guidance not a cp/cps issue
All communications between the CA and the RA regarding certificate issurance or changes in the status of a certificate **must** be by secure and auditable methods.	§ 4.1, 4.2	4.1, 4.2	RA-(10)		
The CP/CPS **should** describe how the RA or CA is informed of changes that may affect the status of the certificate	§ 4.8, 4.9	4.4	RA-(11)		
The certificate request submitted for certification **must** be bound to the act of identity vetting.	§ 4.1, 4.2, 4.3, 4.4.3, 4.6, 4.7, 4.8.4, 4.8.6, 4.8.7	4.1, 4.2	RA-(7)		
3.2 End-entity certificate expiration, renewal and re-keying					
A certificate whose private key is managed in a **software-based token should** only be re-keyed, not renewed.	§ 3.3.1, 4.6, 4.7, 5.6	3.2, 4.7	CA-(40)		
Certificates associated with a private key (for equivalent RSA key lengths of **2048** bits) restricted solely to a **hardware token may** be renewed for a period of **up to 5 years**.	§ 3.3.1, 4.6, 4.7, 5.6	3.2, 4.7	CA-(41)		
Certificates associated with a private key (for equivalent RSA key lengths of **1024** bits) restricted solely to a **hardware token may** be renewed for a period of **up to 3 years**.	§ 3.3.1, 4.6, 4.7, 5.6	3.2, 4.7	CA-(41)		
Certifications **must not** be renewed or re-keyed for more than 5 years without a form of auditable identity and eligibility verification, and this procedure must be described in the CP/CPS,	§ 3.3.1, 4.6, 4.7, 5.6	3.2, 4.7	CA-(42)		
3.3 Removal of an authority from the authentication profile accreditation.					
An accredited authority **must** be removed from list of accredited authorities under this profile if it fails to comply with this authentication profile document, or with the IGTF Federation Document, via the voting process described in the Charter of the PMA to which this authority is accredited.				N/A	PMA guidance not a CP/CPS issue
4 Operational Requirements					
The CA computer where the signing of the certificates will take place **must be** a dedicated machine, running no other services than those needed by for the CA operations.	§ 6.5.1	6.5.1	CA-(8)		
The CA systems **must** be located in a secure environment where access is controlled, limited to specific trained personnel.	§ 5.1.1, 5.1.2	5.1.1, 5.1.2	CA-(9)		
The CA signing computer **may** be either completely off-line or one-line. On-line Cas **must** use at least FIPS 140-2 level-3 capable HSM or equivalent and the CA system **must** be operated in FIPS 140-2 level 3 mode to protect the CA's private key.	§ 6.1.8, 6.2.1, 6.7	6.1.8, 6.2.1, 6.7	CA-(10)		
If the CA has a FIPS 140-2 HSM it **may** be connected to a highly protected/monitored network, possibly accessible from the internet.				N/A	Not an auditing issue
The secure environment **must** be documented and approved by the PMA, and that document or an approved audit thereof **must** be documented and approved by the PMA.	§ 1.1	1.1	CA-(11)		
CA key **must** have a minimum length of 2048 bits.	§ 6.1.5	6.1.5	CA-(12)		

CAs that issue EE certificates: CA signing cert lifetime must be no less then 2 times the maximum lifetime of an EE certificate.	§ 5.6	4.7	CA-(21)		
CA signing cert lifetime **should** not be more then 20 years.	§ 5.6	4.7	CA-(20)		
The CA private key **must** be protected with a pass phrase of as least 15 elements and known to specify CA personnel.	§ 6.2.8	6.2.7	CA-(13)		
HSM equipped CAs **must** have an equivalent level of security to protect access to the HSM.	§ 6.2.8	6.2.7	CA-(13)		
Copies of the encrypted private key **must** be kept on offline media in secure location, with access control.	§ 6.2.4	6.2.4	CA-(14)		
4.1 On-line CAs					
Approved On-line CA architecture setup:					
An authentication/request server, suitably protected and connected to the public network, and a separate signing system, connected to the front-end via a private link, that only processes approved signing requests and logs all certificate issuances (model A)				**N/A**	PMA guidance not a cp/cps issue
An authentication/request server containing also the HSM hardware, connected to a dedicated network that only carries traffic destined for the CA and is actively monitored for intrusions and is protected via a packet-inspecting stateful firewall (model B)				**N/A**	PMA guidance not a cp/cps issue
The on-line CA architecture **must** provide for a log of issued certificates and revocations. The log **should** be tamper-protected.	§ 5.5.1, 5.5.3	4.6.1, 4.6.3	CA-(16)		
4.2 Certificate Policy and Practice Statement Identification.					
Every CA **must** have a Certification Policy and Certificate Practice Statement (CP/CPS Document) and assign it a globally unique object identifier (OID)	§ 1.2	1.2	CA-(1), (4)		
CP/CPS documents should be structured as defined in RFC 3647.	§ 1.1	1.1	CA-(7)	**N/A**	Established RFC 2527 CAs can operate without upgrading to RFC 3647 format
Whenever there is a change in the CP/CPS the OID of the document **must** change.	§ 9.12	8.1	CA-(5)		
Major changes to the CP/CPS **must** be announced to the accrediting PMA and approved before signing any certificates under the new CP/CPS.	§ 9.12	8.1	CA-(5)		
All versions of the CP/CPS under which valid Certificates are issued **must** be available on the web.	§ 2.2, 4.4.2, 4.4.3, 4.6.6, 4.6.7, 6.7.6, 4.7.7, 4.8.6, 4.8.7	2.6.1	CA-(6)		
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.	§ 2.2	2.6.1, 8.2	CA-(19)		
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* .	§ 7.1	7.1	CA-(22)		
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.	§ 4.1, 4.2	4.1, 6.1.1	CA-(36)		
The EE keys **must** be as least 1024 bits long.	§ 6.1.5	6.1.5	CA-(33)		
The EE certificate **must** have a maximum lifetime of 1 year plus 1 month.	§ 5.6	4.7	CA-(34)		
The authority must publish CRLs, and these CRLs should be compliant with RFC5280.	§ 4.9.7, 7.2.1	2.1.1, 7.2.1	CA-(27), (32)		
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	§ 7.1	7.1	CA-(38)		
The *policyIdentifier* **must** include the OID for this profile: 1.2.840.113612.5.2.2.1	§ 7.1	7.1	CA-(38)		
CRLDistributionPoints **must** be included and contain at least one http URL	§ 7.1	7.1	CA-(38)		
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	§ 7.1	7.1	CA-(38)		
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.	§ 3.1.2	3.1.2	CA-(39)		
4.4 Revocation					
The CA **must** publish a CRL.	§ 4.9.7	2.1.1	CA-(27)		
The CA **must** react as soon as possible, but within one working day, to any revocation request received.	§ 4.9.5	4.4.3	CA-(24)		
After revocation the CRL **must** be issued immediately.	§ 4.9.9	4.4.9	CA-(30)		
For CAs issuing certificates to end-entities, the maximum CRL lifetime **must** be at most 30 days.	§ 4.9.9	4.4.9	CA-(28)		
The CA **must** issue a new CRL at least 7 days before the time stated in the *nextUpdate* field if the CA is an **off-line CA**.	§ 4.9.9	4.4.9	CA-(29)		
The CA **must** issue a new CRL at least 3 days before the time stated in the *nextUpdate* field if the CA is an **on-line CA** and the CRL is issued automatically.	§ 4.9.9	4.4.9	CA-(29)		
The CRLs **must** be published in a repository **at least** accessible via the World Wide Web, as soon as issued.	§ 4.9.9	4.4.9	CA-(31)		
Revocation requests **can be** made by end-entities, Registration Authorities and the CA.	§ 4.8.2, 4.9.2	4.4.2	CA-(23)		
Revocation requests **must** be properly authenticated.	§ 4.9.3	4.4.3	CA-(26)		
Others **can** request revocation if they can sufficiently prove compromise or exposure of the associated private key.	§ 4.8.2, 4.9.2	4.4.2	CA-(23)		
4.5 CA Key change over					
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.	§ 3.3.1, 4.6, 4.7, 5.6	3.2, 4.7	CA-(17)		PMA guidance not a CP/CPS issue

The overlap of the old and new key **must** be at least the longest time an end-entity certificate can be valid. The older but still valid certificate **must** be available to verify old signatures – and the secret key to sign CRLs – until all the certificates signed using the associated private key have also expired.	§ 3.3.1, 4.6, 4.7, 5.6	3.2, 4.7	CA-(18)		PMA guidance not a CP/CPS issue
5 Site Security					
The pass phrase of the encrypted private key (CA) **must** be kept 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.	§ 6.2.4, 6.2.5	6.2.4, 6.2.5	CA-(15)		
6 Publication and Repository Responsibilities.					
The originating authority **must** grant to the PMA and the Federation – by virtue of its accreditation – the right of unlimited re-distribution of its information.			CA-(51)	**N/A**	PMA guidance not a CP/CPS issue
The repository **must** be run at least on a best-effort basis, with an intended continuous availability.	§ 2.1	2.6.4	CA-(49)		
The CA **should** provide a means to validate the integrity of their root of trust.			CA-(52)	**N/A**	PMA guidance not a CP/CPS issue
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.			CA-(53)	**N/A**	PMA guidance not a CP/CPS issue
Each authority **must** publish the following information:	§ 2.2, 4.4.2, 4.6.6, 4.7.6, 4.8.6	2.6.1	CA-(50)		
A CA root certificate or set of CA root certificates up to a self-signed root.	§ 2.2, 4.4.2, 4.6.6, 4.7.6, 4.8.6	2.6.1	CA-(50)		
A http or https URL of the PEM-formatted CA certificate.	§ 2.2, 4.4.2, 4.6.6, 4.7.6, 4.8.6	2.6.1	CA-(50)		
A http URL of the PEM or DER formatted CRL.	§ 2.2, 4.4.2, 4.6.6, 4.7.6, 4.8.6	2.6.1	CA-(50)		
A http or https URL of the web page of the CA for general information.	§ 2.2, 4.4.2, 4.6.6, 4.7.6, 4.8.6	2.6.1	CA-(50)		
The CP and/or CPS documents	§ 2.2, 4.4.2, 4.6.6, 4.7.6, 4.8.6	2.6.1	CA-(50)		
An official contact email address for inquiries and fault reporting.	§ 2.2, 4.4.2, 4.6.6, 4.7.6, 4.8.6	2.6.1	CA-(50)		
A physical or postal contact address.	§ 2.2, 4.4.2, 4.6.6, 4.7.6, 4.8.6	2.6.1	CA-(50)		
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/reboot of the issuing machine.	§ 5.5.1	4.6.1	CA-(43)		
The CA **must** keep these records for at least three years.	§ 5.5.2	4.6.2	CA-(45)		
Identity validation records **must** be kept at least as long as there are valid certificates based on such a validation.	§ 5.5.2	4.6.2	CA-(45)		
The records **must** be made available to external auditors in the course of their work as auditor.	§ 8	2.7	CA-(44)		
The CA **must** accept being audited by other accredited CAs to verify its compliance with the rules and procedures specified in its CP/CPS document.	§ 8	2.7	CA-(46)		
The CA **should** perform operational audits of the CA/RA staff at least once per year.	§ 5.4	4.5	CA-(47)		
A list of CA and RA personnel **should** be maintained and verified at least once per year.			CA-(48)	**N/A**	PMA guidance not a CP/CPS issue
8 Privacy and confidentiality					
Accredited CAs **must** define a privacy and data release policy compliant with the relevant national legislation.	§ 9.3, 9.4	2.8	CA-(54)		
The CA **is responsible for** recording, at the time of validation, sufficient information regarding the subscribers to identify the subscriber.	§ 9.3, 9.4	2.8	CA-(54)		
The CA **is not required** to release such information unless provided by a valid legal request according to national laws applicable to that CA.			CA-(54)	**N/A**	PMA guidance not a CP/CPS issue
9 Compromise and disaster recovery					
The CA **must** have an adequate compromise and disaster recovery procedure.	§ 5.7, 5.7.1	4.8	CA-(55)		
The CA **must** be willing to discuss this procedure in the PMA. The procedure **need not** be disclosed in the policy and practice statements.			CA-(55)	**N/A**	PMA guidance not a cp/cps issue
9.1 Due deligence for subscribers					
The CA **should** make a reasonable effort to make sure that subscribers realize the importance of properly protecting their private data.	§ 6.2.8	6.2.7	CA-(37)		
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.	§ 6.2.8	6.2.7	CA-(37)		
Private keys pertaining to host and service certificate **may** be stored without a passphrase, but **must** be adequately protected by system methods if stored without passphrase.	§ 6.2.8	6.2.7	CA-(37)		
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.	§ 4.9.1	2.1.3, 4.4.1	CA-(25)		
Comments:					