

	Digital Trust Service
	Assessment Checklist – ETSI TS 102 042 v2.1.2 (2010-04)

PKI Appendix n°003A Assessment Checklist ETSI TS 102 042 v2.1.2 (2010-04)

Modifications: full review of the document

34-40, avenue de la Porte Neuve
L-2227 Luxembourg
Boîte Postale 10 : L-2010 Luxembourg
Tél.: (+352) 46 97 46-42
Fax: (+352) 46 97 46-48
jean-philippe.humbert@ilnas.etat.lu

Checked by Jean-Philippe Humbert

Approved by Jean-Marie REIFF

The updated version of this document is available on www.ilnas.lu
The printed versions are not managed.

Assessment details

Assessed entity	
Identification n°	
Location	
Contact person	
Standard	
Type of assessment	
Assessment date(s)	
Lead Assessor	
Technical Assessor (1)	
Technical Assessor (2)	
Expert (1)	
Expert (2)	

Clause number	Requirements	Observations
7	Requirements on CA practice	
	The CA shall implement the controls that meet the following requirements.	
7.1	Certification practice statement	
	The CA shall have a statement of the practices and procedures.	
7.1 a)	The CA's certification practice statement shall address all the requirements identified in the applicable certificate policy.	
7.1 b)	[EVCP] and [EVCP+]: The CA's certification practice statement shall include the item 3 from section 7.1.2 of the EVCG [16].	
7.1 c)	The CA's certification practice statement shall identify the obligations of all external organizations supporting the CA services including the applicable policies and practices.	
7.1 d)	The CA shall make available to subscribers and relying parties its certification practice statement, and other relevant documentation, as necessary to assess conformance to the certificate policy. 1) to subscribers and relying parties; 2) [EVCP] and [EVCP+]: EVCG [16], section 6.2.1 item 1 c).	
7.1 e)	The CA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of the certificate as specified in clause 7.3.4.	
7.1 f)	The CA shall have a high level management body with final authority and responsibility for approving the certification practice statement.	
7.1 g)	The senior management of the CA is responsible for ensuring that the certification practices established to meet the applicable requirements specified in the present document are properly implemented.	
7.1 h)	The CA shall define a review process for certification practices including responsibilities for maintaining the certification practice statement.	
7.1 i)	The CA shall give due notice of changes it intends to make in its certification practice statement and shall, following approval as in e) above, make the revised certification practice statement immediately available as required under c) above.	
7.1 j)	The CA shall document the algorithms and parameters employed.	
7.1 k)	[EVCP] and [EVCP+]: The CA SHALL address the provisions specified in EVCG [16], sections 7.1.3 and 15.2.	
7.2	Public key infrastructure - Key management life cycle	
7.2.1	Certification authority key generation	
	<i>Certificate generation</i>	
	The CA shall ensure that CA keys are generated in controlled circumstances.	

Clause number	Requirements	Observations
7.2.1 a)	Certification authority key generation shall be undertaken in a physically secure environment (see clause 7.4.4) by personnel in trusted roles (see clause 7.4.3) under, at least, dual control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.	
7.2.1 b)	[CHOICE]: [LCP] CA key generation shall be carried out in a product, application or device which ensures that the keys are generated in a trustworthy manner and do not compromise the security of the private key and which: i. meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3] level 2 or higher; or ii. is a trustworthy system which is assured to EAL 3 or higher in accordance to ISO/IEC 15408 [4], or equivalent security criteria. [NCP] CA key generation shall be carried out within a device which either: iii. meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3] level 3 or higher; or iv. meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [6], CWA 14167-3 [7] or CWA 14167-4 [8]; or v. is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [4], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.	
7.2.1 c)	Certification authority key generation shall be performed using an algorithm recognized by industry as being fit for the CA's signing purposes.	
7.2.1 d)	The selected key length and algorithm for CA signing key shall be one which is recognized by industry as being fit for the CA's signing purposes. [EVCP] and [EVCP+]: EVCG [16] appendix A (1) and (2) also apply.	
7.2.1 e)	A suitable time before expiration of its CA signing key (for example as indicated by expiration of CA certificate), the CA shall generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key shall also be generated and distributed in accordance with this policy.	
7.2.1 f)	[EVCP] and [EVCP+]: EVCG [16], section 14.1.5 applies.	
7.2.2	Certification authority key storage, backup and recovery	
	<i>Certificate generation</i>	
	The CA shall ensure that CA private keys remain confidential and maintain their integrity.	

Clause number	Requirements	Observations
7.2.2 a)	<p>[CHOICE]:</p> <p>[LCP] The CA private signing key shall be held and used in a product, application or device which does not compromise the security of the private key and which:</p> <ul style="list-style-type: none"> i. meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3], level 2 or higher; or ii. is a trustworthy system which is assured to EAL 3 or higher in accordance to ISO/IEC 15408 [4], or equivalent security criteria. <p>[NCP] The CA private signing key shall be held and used within a secure cryptographic device which:</p> <ul style="list-style-type: none"> iii. meets the requirements identified in FIPS PUB 140-1 [2], or FIPS PUB 140-2 [3] level 3 or higher; or iv. meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [6], CWA 14167-3 [7], CWA 14167-4 [8]; or v. is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [4], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures. 	
7.2.2 b)	<p>[CHOICE]:</p> <p>[LCP] When outside the signature-creation product, application or device, the secrecy of the CA's private key shall be ensured.</p> <p>[NCP] When outside the signature-creation device (see a) above) the CA private signing key shall be protected in a way that ensures the same level of protection as provided by the signature creation device.</p>	
7.2.2 c)	<p>The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. (see clause 7.4.4). The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.</p>	
7.2.2 d)	<p>Backup copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.</p>	
7.2.2 e)	<p>Where the keys are stored in a dedicated key processing hardware module, access controls shall be in place to ensure that the keys are not accessible outside the hardware module.</p>	
7.2.3	Certification authority public key distribution	
	<i>Certificate generation and certificate Distribution</i>	
	<p>The CA shall ensure that the integrity and authenticity of the CA signature verification (public) key and any associated parameters are maintained during its distribution to relying parties.</p>	
7.2.3 a)	<p>CA signature verification (public) keys shall be made available to relying parties in a manner that assures the integrity of the CA public key and authenticates its origin.</p>	

Clause number	Requirements	Observations
7.2.4	Key escrow	
7.2.4 a)	[CONDITIONAL] If the subject's key is to be used for electronic signatures then the CA shall not hold the subject's private signing keys in a way which provides a backup decryption capability (commonly called key escrow).	
7.2.4 b)	[CONDITIONAL] If a copy of the subject's key is kept by the CA then the CA shall ensure that the private key is kept secret and only made available to appropriately authorized persons.	
7.2.5	Certification authority key usage	
	The CA shall ensure that CA private signing keys are not used inappropriately.	
7.2.5 a)	CA signing key(s) used for generating certificates, as defined in clause 7.3.3, and/or issuing revocation status information, shall not be used for any other purpose.	
7.2.5 b)	The certificate signing keys shall only be used within physically secure premises.	
7.2.6	End of CA key life cycle	
	The CA shall ensure that CA private signing keys are not used beyond the end of their life cycle.	
	<i>Certificate generation</i>	
7.2.6 a)	The use of the corresponding CA's private key, shall be limited to that compatible with the hash algorithm, the signature algorithm and signature key length used in the generating certificates, in line with current practice as in clause 7.2.1 d).	
7.2.6 b)	All copies of the CA private signing keys shall be destroyed or put beyond use at the end of their life cycle.	
7.2.7	Life cycle management of cryptographic hardware used to sign certificates	
	[NCP] The CA shall ensure the security of cryptographic device throughout its lifecycle.	
	<i>Certificate generation</i>	
7.2.7 a)	[NCP] Certificate and revocation status information signing cryptographic hardware is not tampered with during shipment;	
7.2.7 b)	[NCP] Certificate and revocation status information signing cryptographic hardware is not tampered with while stored;	
7.2.7 c)	[NCP] The installation, activation, back-up and recovery of the CA's signing keys in cryptographic hardware shall require simultaneous control of at least of two trusted employees;	
7.2.7 d)	[NCP] Certificate and revocation status information signing cryptographic hardware is functioning correctly; and	

Clause number	Requirements	Observations
7.2.7 e)	[NCP] CA private signing keys stored on CA cryptographic hardware are destroyed upon device retirement. This destruction does not affect all copies of the private key. Only the physical instance of the key stored in the cryptographic hardware under consideration will be destroyed.	
7.2.8	CA provided subject key management services	
	The CA shall ensure that any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is assured.	
	<i>Certificate generation</i>	
	[CONDITIONAL] <i>If the CA generates the subject keys:</i>	
7.2.8 a)	CA-generated subject keys shall be generated using an algorithm recognized by industry as being fit for the uses identified in the certificate policy during the validity time of the certificate.	
7.2.8 b)	[CONDITIONAL] CA-generated subject keys shall be of a key length and for use with a public key algorithm which are recognized by industry as being fit for the purposes stated in the certificate policy during the validity time of the certificate. [EVCP] or [EVCP+]: guidance SHALL be taken from the EVCG [16], appendix A but SHALL not override a) and b).	
7.2.8 c)	CA-generated subject keys shall be generated and stored securely before delivery to the subject.	
7.2.8 d)	The subject's private key shall be delivered to the subject in a manner such that the secrecy and integrity of the key is not compromised.	
7.2.8 e)	If a copy of the subject's private key is not required to be kept by the CA, or other authorized entity, (see clause 7.2.4), once delivered to the subject, the private key can be maintained under the subject's sole control. Any copies of the subject's private key held by the CA shall be destroyed.	
7.2.9	Secure user device preparation	
	[NCP+] The CA shall ensure that if it issues to the subject secure user device this is carried out securely.	
	<i>Subject device provision</i>	
	[CONDITIONAL] <i>In particular, if the CA issues a secure user device:</i>	
7.2.9 a)	Secure user device preparation shall be securely controlled by the service provider.	
7.2.9 b)	Secure user device shall be securely stored and distributed.	
7.2.9 c)	Secure user device deactivation and reactivation shall be securely controlled.	
7.2.9 d)	Where the secure user device has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the signature-creation module.	
7.3	Public key infrastructure - Certificate Management life cycle	

Clause number	Requirements	Observations
7.3.1	Subject registration	
	The CA shall ensure that evidence of subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorized sources, and that certificate requests are accurate, authorized and complete according to the collected evidence or attestation.	
	<i>Registration</i>	
7.3.1 a)	Before entering into a contractual relationship with a subscriber, the CA shall inform the subscriber of the terms and conditions regarding use of the certificate as given in clause 7.3.4.	
7.3.1 b)	[CONDITIONAL]: If the subject is a person and not the same as the subscriber, the subject shall be informed of his/her obligations.	
7.3.1 c)	The CA shall communicate this information through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.	
7.3.1 d)	The service provider shall collect either direct evidence, or an attestation from an appropriate and authorized source, of the identity (e.g. name) and, if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation. Verification of the subject's identity shall be at time of registration by appropriate means and in accordance with national law. [EVCP] and [EVCP+]: Guidance on Information Verification requirements SHALL be taken from the EVCG [16], section 10.	
7.3.1 e)	[CHOICE]: - [LCP] No requirement. - [NCP] If the subject is a physical person evidence of the subject's identity (e.g. name) shall be checked against a physical person either directly or shall have been checked indirectly using means which provides equivalent assurance to physical presence (see note 2). Evidence for verifying other entities shall involve procedures which provide the same degree of assurance.	
7.3.1 f)	[CONDITIONAL] If the subject is a physical person, evidence shall be provided of: i. full name (including surname and given names consistent with the applicable law and national identification practices); ii. date and place of birth, reference to a nationally recognized identity document, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name.	

Clause number	Requirements	Observations
7.3.1 g)	<p>[CONDITIONAL] If the subject is a physical person who is identified in association with a legal person, or organizational entity (e.g. the subscriber), evidence shall be provided of:</p> <ul style="list-style-type: none"> i. full name (including surname and given names, consistently with the applicable law and national identification practices) of the subject; ii. date and place of birth, reference to a nationally recognized identity document, or other attributes of the subscriber which may be used to, as far as possible, distinguish the person from others with the same name; iii. full name and legal status of the associated legal person or other organizational entity (e.g. the subscriber); iv. any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity; v. evidence that the subject is associated with the legal person or other organizational entity. 	
7.3.1 h)	<p>[CONDITIONAL] If the subject is an organizational entity, evidence shall be provided of:</p> <ul style="list-style-type: none"> i. full name of the organizational entity (private organization, government entity or non-commercial entity); [EVCP] and [EVCP+]: Guidance on Information Verification requirements SHALL be taken from the EVCG [16], sections 10.2 to 10.6; ii. of reference to a nationally recognized registration, or other attributes which may be used to, as far as possible, distinguish the organizational entity from others with the same name. iii. [EVCP] and [EVCP+]: EVCG [16]. Section 6.2.1 item 1) and 2) apply. 	
7.3.1 i)	<p>[CONDITIONAL] If the subject is a device or system operated by or on behalf of an organizational entity, evidence shall be provided of:</p> <ul style="list-style-type: none"> i. identifier of the device by which it may be referenced (e.g. Internet domain name); [EVCP] and [EVCP+]: Domain verification requirements SHALL be taken from the EVCG [16], section 10.6; ii. full name of the organizational entity; iii. a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the organizational entity from others with the same name. 	
7.3.1 j)	<p>The CA shall record all the information necessary to verify the subject's identity and, if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.</p>	

Clause number	Requirements	Observations
7.3.1 k)	<p>If an entity other than the subject is subscribing to the CA services (i.e. the subscriber and subject are separate entities - see clause 4.4) then evidence shall be provided that the subscriber is authorized to act for the subject as identified (e.g. is authorized for all members of the identified organization). [EVCP] and [EVCP+]: Guidance on roles SHALL be taken from the EVCG [16], section 10.7.</p>	
7.3.1 l)	<p>The subscriber shall provide a physical address, or other attributes, which describe how the subscriber may be contacted. [EVCP] and [EVCP+]: Guidance on Verification of the applicant's location should be taken from the EVCG [16], section 10.4.</p>	
7.3.1 m)	<p>The CA shall record the signed agreement with the subscriber including:</p> <ul style="list-style-type: none"> i. agreement to the subscriber's obligations (see clause 6.2); ii. if required by the CA, agreement by the subscriber to user secure user device; iii. consent to the keeping of a record by the CA of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation (see clause 7.4.11), the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the CA terminating its services; iv. whether, and under what conditions, the subscriber requires and the subject consents to the publication of the certificate; v. confirmation that the information held in the certificate is correct. vi. [EVCP] and [EVCP+]: Guidance on Verification of the signatures and of the approval of EV request SHALL be taken from the EVCG [16], sections 10.8 and 10.9. 	
7.3.1 n)	<p>The records identified above shall be retained for the period of time as indicated to the subscriber (see c) above) and as necessary for the purposes for providing evidence of certification in legal proceedings. [EVCP] and [EVCP+]: at least seven years after any EV Certificate based on that documentation ceases to be valid as stated in EVCG [16], section 13.2.2.</p> <ul style="list-style-type: none"> i. the law of the country where the CA is established should always be considered; ii. where subjects are registered through a registration authority in another country to where the CA is established then that RA should also apply its own country's regulations; iii. where some subscribers are also in another country then contractual and other legal requirements applicable to those subscribers should also be taken into account. 	

Clause number	Requirements	Observations
7.3.1 o)	[CONDITIONAL] If the subject's key pair is not generated by the CA, the certificate request process shall ensure that the subject has possession of the private key associated with the public key presented for certification.	
7.3.1 p)	The CA shall ensure that the requirements of the applicable national data protection legislation are adhered to (including the use of pseudonyms if applicable) within their registration process.	
7.3.1 q)	The CA's verification policy shall only require the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.	
7.3.1 r)	[EVCP] and [EVCP+]: the CA MUST abide by EVCG [16] requirements in section 10.11.1. The Acceptable methods of verifications are specified in EVCG [16] requirements in section 10.11.2.	
7.3.1 s)	[EVCP] and [EVCP+] : For a dual control procedure follow EVCG [16], section 12.1.3.	
7.3.2	Certificate renewal, rekey and update	
	The CA shall ensure that requests for certificates issued to a subject who has previously registered with the same CA are complete, accurate and duly authorized. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes.	
	<i>Registration</i>	
7.3.2 a)	The CA shall check the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the subject are still valid; [EVCP] and [EVCP+]: Guidance on Pre-existing information or documentation SHALL be taken from the EVCG [16], section 13.3.2.	
7.3.2 b)	If any of the CA terms and conditions have changed, these shall be communicated to the subscriber and agreed to in accordance with clause 7.3.1 a), b), c) and m).	
7.3.2 c)	If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information is verified, recorded, agreed to by the subscriber in accordance with clause 7.3.1 d) to l);	
7.3.2 d)	The CA shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised.	
7.3.3	Certificate generation	
	The CA shall ensure that it issues certificates securely to maintain their authenticity.	
	<i>Certificate generation</i>	

Clause number	Requirements	Observations
7.3.3 a)	<p>The certificates shall include in accordance with X.509 [9] and RFC 5280 [17]:</p> <ul style="list-style-type: none"> i. identification of the CA (certification-service-provider) and the country in which it is established; ii. the name of the subject, or a pseudonym which shall be identified as such; iii. provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended; iv. the public key which corresponds to the private key under the control of the subject; v. an indication of the beginning and end of the period of validity of the certificate; vi. the serial number of the certificate; vii. the electronic signature of the certification authority issuing it; viii. limitations on the scope of use of the certificate, if applicable; and ix. limits on the value of transactions for which the certificate can be used, if applicable. x. [EVCP] and [EVCP+]: Requirements in clauses 8.1 and 8.2 on certification content and on policy identification shall be applied. Guidance on Validity period SHALL be taken from the EVCG [16], section 8.3. In the case of EV certificate for SSL/TSL EVCG [16], annex B applies. 	
7.3.3 b)	<p>The CA shall take measures against forgery of certificates, and, in cases where the CA generates the subjects' private key, guarantee confidentiality during the process of generating such data.</p>	
7.3.3 c)	<p>The procedure of issuing the certificate is securely linked to the associated registration, certificate renewal or rekey, including the provision of any subject generated public key;</p>	
7.3.3 d)	<p>[CONDITIONAL] If the CA generated the subjects key:</p> <ul style="list-style-type: none"> i. the procedure of issuing the certificate is securely linked to the generation of the key pair by the CA; ii. [LCP], [NCP] the private key is securely passed to the registered subject. iii. [NCP+] the secure user device containing the subject's private key is securely passed to the registered subject. 	
7.3.3 e)	<p>The CA shall ensure that over the life time of the CA a distinguished name which has been used in a certificate by it is never re-assigned to another entity.</p>	
7.3.3 f)	<p>The confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber/subject or between distributed CA system components;</p>	
7.3.3 g)	<p>The CA shall verify that registration data is exchanged with recognized registration service providers, whose identity is authenticated, in the event that external registration service providers are used.</p>	
7.3.4	<p>Dissemination of terms and conditions</p>	

Clause number	Requirements	Observations
	The CA shall ensure that the terms and conditions are made available to subscribers and relying parties.	
7.3.4 a)	<p>The CA shall make available to subscribers and relying parties the terms and conditions regarding the use of the certificate:</p> <ul style="list-style-type: none"> i. the certificate policy being applied, including a clear statement as to whether the policy is for certificates issued to the public and whether the policy requires the use of any particular product, application or device for the purposes of applying the key-pair associated with the certificate being issued; ii. any limitations on its use; iii. the subscriber's obligations as defined in clause 6.2, including whether the policy requires the use of any particular product, application or device for the purposes of applying the key-pair associated with the certificate being issued; iv. information on how to validate the certificate, including requirements to check the revocation status of the certificate, such that the relying party is considered to "reasonably rely" on the certificate (see clause 6.3); v. any limitations of liability, including the purposes/uses for which the CA accepts (or excludes) liability; vi. the period of time which registration information (see clause 7.3.1) is retained; vii. the period of time which CA event logs (see clause 7.4.11) are retained; viii. procedures for complaints and dispute settlement; ix. the applicable legal system; and x. if the CA has been assessed to be conformant with the identified certificate policy, and if so through which scheme. 	
7.3.4 b)	The information identified in a) above shall be available through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.	
7.3.5	Certificate dissemination	
	The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties.	
	<i>Dissemination</i>	
7.3.5 a)	Upon generation, the complete and accurate certificate shall be available to subscriber or subject for whom the certificate is being issued;	
7.3.5 b)	Certificates are available for retrieval in only those cases for which the subject's consent has been obtained;	
7.3.5 c)	The CA shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 7.3.4);	
7.3.5 d)	The applicable terms and conditions shall be readily identifiable for a given certificate;	

Clause number	Requirements	Observations
7.3.5 e)	<p>[CHOICE]:</p> <p>i. [LCP] the information identified in b) and c) above shall be available as specified in the CA's Certification Practice Statement;</p> <p>ii. [NCP] the information identified in b) and c) above shall be available 24 hours per day, 7 days per week.</p> <p>Upon system failure, service or other factors which are not under the control of the CA, the CA shall apply best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement.</p>	
7.3.5 f)	<p>[CONDITIONAL] If the CA is issuing certificate to the public the information identified in b) and c) above shall be publicly and internationally available.</p>	
7.3.6	<p>Certificate revocation and suspension</p>	
	<p>The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests.</p>	
	<p><i>Revocation management</i></p>	
7.3.6 a)	<p>The CA shall document as part of its certification practice statement (see 7.1) the procedures for revocation of certificates including:</p> <p>i. who may submit revocation reports and requests;</p> <p>ii. how they may be submitted;</p> <p>iii. any requirements for subsequent confirmation of revocation reports and requests;</p> <p>iv. whether and for what reasons certificates may be suspended;</p> <p>v. the mechanism used for distributing revocation status information;</p> <p>vi. the maximum delay between receipt of a revocation request or report and the change to revocation status information being available to all relying parties. This shall be at most :</p> <p>[CHOICE] [LCP] 72 hours [NCP] 24 hours</p>	
7.3.6 b)	<p>Requests and reports relating to revocation (e.g. due to compromise of subject's private key, death of the subject, unexpected termination of a subscriber's or subject's agreement or business functions, violation of contractual obligations) shall be processed on receipt.</p>	
7.3.6 c)	<p>[EVCP] and [EVCP+]: Requirement from EVCG [16], section 11.3.3.</p>	
7.3.6 d)	<p>Requests and reports relating to revocation shall be authenticated, checked to be from an authorized source. Such reports and requests will be confirmed as required under the CA's practices.</p>	

Clause number	Requirements	Observations
7.3.6 e)	A certificate's revocation status may be set to "suspended" whilst the revocation is being confirmed. The CA shall ensure that a certificate is not kept suspended for longer than is necessary to confirm its status.	
7.3.6 f)	The subject, and where applicable the subscriber, of a revoked or suspended certificate, shall be informed of the change of status of its certificate.	
7.3.6 g)	Once a certificate is definitively revoked (i.e. not suspended) it shall not be reinstated.	
7.3.6 h)	[CHOICE] : i. [LCP] Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used, these shall be published at least every 72 hours; ii. [NCP] Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used, these shall be published at least every 24 hours; iii. [EVCP] and [EVCP+]: Requirement from EVCG [16], section 11.1.1, item 1) and item 2).	
7.3.6 i)	Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used as the sole means of providing revocation status information: i. every CRL shall state a time for next scheduled CRL issue; and ii. a new CRL may be published before the stated time of the next CRL issue; iii. the CRL shall be signed by the certification authority or an authority designated by the CA.	
	<i>Revocation status</i>	
7.3.6 j)	[CHOICE]: i. [LCP] Revocation status information shall be available as specified in the CA's Certification Practice Statement. ii. [NCP] Revocation status information, shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the CA, the CA shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement. iii. [EVCP] and [EVCP+]: Requirement from EVCG [16], section 11.1.1.	
7.3.6 k)	[EVCP] and [EVCP+]: Requirement from EVCG [16], section 11.1.1.	
7.3.6 l)	[EVCP] and [EVCP+]: Requirement from EVCG [16], section 11.1.2.	
7.3.6 m)	[EVCP] and [EVCP+]: Requirement from EVCG [16], section 11.1.3.	
7.3.6 n)	The integrity and authenticity of the status information shall be protected.	
7.3.6 o)	[CONDITIONAL] If the CA is issuing certificate to the public, Revocation status information shall be publicly and internationally available.	

Clause number	Requirements	Observations
7.3.6 p)	Revocation status information shall include information on the status of certificates at least until the certificate expires.	
7.4	CA management and operation	
7.4.1	Security management	
	The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards.	
	<i>CA General</i>	
7.4.1 a)	The CA shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk analysis shall be regularly reviewed and revised if necessary;	
7.4.1 b)	The CA shall retain responsibility for all aspects of the provision of certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the CA and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the CA. The CA shall retain responsibility for the disclosure of relevant practices of all parties.	
7.4.1 c)	The CA management shall provide direction on information security through a suitable high level steering forum that is responsible for defining the CA's information security policy and ensuring publication and communication of the policy to all employees who are impacted by the policy.	
7.4.1 d)	The CA shall have a system or systems for quality and information security management appropriate for the certification services it is providing;	
7.4.1 e)	The information security infrastructure necessary to manage the security within the CA shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the CA management forum;	
7.4.1 f)	The security controls and operating procedures for CA facilities, systems and information assets providing the certification services shall be documented, implemented and maintained;	
7.4.1 g)	The CA shall ensure that the security of information shall be maintained when the responsibility for CA functions has been outsourced to another organization or entity.	
7.4.2	Asset classification and management	
	The CA shall ensure that its assets and information receive an appropriate level of protection.	
	<i>CA General</i>	

Clause number	Requirements	Observations
7.4.2 a)	The CA shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.	
7.4.3	Personnel security	
	The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations.	
	CA General	
7.4.3 a)	The CA shall employ a sufficient number of personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function;	
7.4.3 b)	Appropriate disciplinary sanctions shall be applied to personnel violating CA policies or procedure;	
7.4.3 c)	Security roles and responsibilities, as specified in the CA's security policy, shall be documented in job descriptions. Trusted roles, on which the security of the CA's operation is dependent, shall be clearly identified;	
7.4.3 d)	CA personnel (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Where appropriate, these shall differentiate between general functions and CA specific functions;	
7.4.3 e)	Personnel shall exercise administrative and management procedures and processes that are in line with the CA's information security management procedures (see clause 7.4.1);	
	Registration, certificate generation, subject device provision, revocation management	
7.4.3 f)	Managerial personnel shall be employed who possess experience or training in the electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions;	
7.4.3 g)	All CA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations;	

Clause number	Requirements	Observations
7.4.3 h)	<p>Trusted roles include roles that involve the following responsibilities:</p> <ul style="list-style-type: none"> i. Security Officers: Overall responsibility for administering the implementation of the security practices. Additionally approve the generation/revocation/suspension of certificates. ii. System Administrators: Authorized to install, configure and maintain the CA trustworthy systems for registration, certificate generation, subject device provision and revocation management. iii. System Operators: Responsible for operating the CA trustworthy systems on a day-to-day basis. Authorized to perform system backup and recovery. iv. System Auditors: Authorized to view archives and audit logs of the CA trustworthy systems. 	
7.4.3 i)	CA personnel shall be formally appointed to trusted roles by senior management responsible for security;	
7.4.3 j)	The CA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed. [EVCP] and [EVCP+]: this applies to EVCG [16], section 12.1.1.	
7.4.4	Physical and environmental security	
	The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized.	
	CA General	
7.4.4 a)	Physical access to facilities concerned with certificate generation, subject device preparation, and revocation management services shall be limited to properly authorized individuals;	
7.4.4 b)	Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities; and	
7.4.4 c)	Controls shall be implemented to avoid compromise or theft of information and information processing facilities.	
	Certificate generation, subject device provision (in particular preparation) and revocation management	
7.4.4 d)	The facilities concerned with certificate generation, subject device preparation (see clause 7.2.9) and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.	
7.4.4 e)	Any persons entering this physically secure area shall not be left for any significant period without oversight by an authorized person.	

Clause number	Requirements	Observations
7.4.4 f)	Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation, subject device preparation (see clause 7.2.9) and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter.	
7.4.4 g)	Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The CA's physical and environmental security policy concerned with certificate generation, subject device preparation (see clause 7.2.9) and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc.	
7.4.4 h)	Controls shall be implemented to protect against equipment, information, media and software relating to the CA services being taken off-site without authorization.	
7.4.5	Operations management	
	The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure.	
	CA General	
7.4.5 a)	The integrity of CA systems and information shall be protected against viruses, malicious and unauthorized software.	
7.4.5 b)	Damage from security incidents and malfunctions shall be minimized through the use of incident reporting and response procedures.	
7.4.5 c)	Media used within the CA shall be securely handled to protect media from damage, theft and unauthorized access.	
7.4.5 d)	Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.	
7.4.5 e)	Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of certification services.	
	Media handling and security	
7.4.5 f)	All media shall be handled securely in accordance with requirements of the information classification scheme (see clause 7.4.2). Media containing sensitive data shall be securely disposed of when no longer required.	
	System Planning	

Clause number	Requirements	Observations
7.4.5 g)	[CHOICE]: i. [LCP] no requirement; ii. [NCP] capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.	
	Incident reporting and response	
7.4.5 h)	The CA shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident.	
7.4.5 i)	Audit processes, meeting requirements specified in clause 7.4.11, shall be invoked at system startup, and cease only at system shutdown.	
7.4.5 j)	Audit logs shall be monitored or reviewed regularly to identify evidence of malicious activity.	
	Certificate generation, revocation management	
	Operations procedures and responsibilities	
7.4.5 k)	CA security operations shall be separated from normal operations.	
7.4.6	System Access Management	
	The CA shall ensure that CA system access is limited to properly authorized individuals.	
	CA General	
7.4.6 a)	Controls (e.g. firewalls) shall be implemented to protect the CA's internal network domains from external network domains accessible by third parties.	
7.4.6 b)	Sensitive data shall be protected against unauthorized access or modification. Sensitive data shall be protected (e.g. using encryption and an integrity mechanism) when exchanged over networks which are not secure.	
7.4.6 c)	The CA shall ensure effective administration of user (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access.	
7.4.6 d)	The CA shall ensure access to information and application system functions are restricted in accordance with the access control policy and that the CA system provides sufficient computer security controls for the separation of trusted roles identified in CA's practices, including the separation of security administrator and operation functions. Particularly, use of system utility programs is restricted and tightly controlled. Access shall be restricted only allowing access to resources as necessary for carrying out the role(s) allocated to a user.	

Clause number	Requirements	Observations
7.4.6 e)	CA personnel shall be successfully identified and authenticated before using critical applications related to certificate management.	
7.4.6 f)	CA personnel shall be accountable for their activities, for example by retaining event logs (see clause 7.4.11).	
7.4.6 g)	Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.	
Certificate generation		
7.4.6 h)	The CA shall ensure that local network components (e.g. routers) are kept in a physically secure environment and their configurations periodically audited for compliance with the requirements specified by the CA.	
7.4.6 i)	Continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.	
Dissemination		
7.4.6 j)	Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.	
Revocation management		
7.4.6 k)	Continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.	
Revocation status		
7.4.6 l)	Revocation status application shall enforce access control on attempts to modify revocation status information.	
7.4.7	Trustworthy Systems Deployment and Maintenance	
	The CA shall use trustworthy systems and products that are protected against modification.	
CA General		
7.4.7 a)	An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the CA or on behalf of the CA to ensure that security is built into IT systems.	
7.4.7 b)	Change control procedures exist for releases, modifications and emergency software fixes for any operational software.	
7.4.8	Business continuity management and incident handling	
	The CA shall ensure in the event of a disaster, including compromise of the CA's private signing key, operations are restored as soon as possible.	
CA General		

Clause number	Requirements	Observations
7.4.8 a)	The CA must define and maintain a continuity plan to enact in case of a disaster.	
7.4.8 b)	CA systems data necessary to resume CA operations shall be backed up and stored in safe places suitable to allow the CA to timely go back to operations in case of Incident/disasters;	
7.4.8 c)	Back-up and restore functions shall be performed by the relevant trusted roles specified in clause 7.4.3.	
CA key compromise		
7.4.8 d)	The CA's business continuity plan (or disaster recovery plan) shall address the compromise or suspected compromise of a CA's private signing key as a disaster and the planned processes shall be in place.	
7.4.8 e)	Following a disaster the CA shall, where practical, take steps to avoid repetition of a disaster.	
Revocation status		
7.4.8 f)	In the case of compromise the CA shall as a minimum provide the following undertakings: i. Inform the following of the compromise: all subscribers and other entities with which the CA has agreements or other form of established relations, among which relying parties and CAs. In addition, this information shall be made available to other relying parties. ii. Indicate that certificates and revocation status information issued using this CA key may no longer be valid.	
7.4.8 g)	Should any of the algorithms, or associated parameters, used by the CA or its subscribers become insufficient for its remaining intended usage then the CA shall: i. Inform all subscribers and relying parties with whom the CA has agreement or other form of established relations. In addition, this information shall be made available to other relying parties. ii. Revoke any affected certificate.	
7.4.9	CA termination	
	The CA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.	
CA General		
7.4.9 a)	Before the CA terminates its services the following procedures shall be executed as a minimum: i. the CA shall inform the following of the termination: all subscribers and other entities with which the CA has agreements or other form of established relations, among which relying parties and CA. In addition, this information shall be made available to other relying parties;	

Clause number	Requirements	Observations
	<ul style="list-style-type: none"> ii. the CA shall terminate all authorization of subcontractors to act on behalf of the CA in the performance of any functions related to the process of issuing certificates; iii. the CA shall perform necessary undertakings to transfer obligations for maintaining registration information (see clause 7.3.1), revocation status information (see clause 7.3.6) and event log archives (see clause 7.4.11) for their respective period of time as indicated to the subscriber and relying party (see clause 7.3.4); iv. the CA shall destroy, or withdraw from use, its private keys, as defined in clause 7.2.6. 	
7.4.9 b)	The CA shall have an arrangement to cover the costs to fulfill these minimum requirements in case the CA becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.	
7.4.9 c)	<p>The CA shall state in its practices the provisions made for termination of service. This shall include:</p> <ul style="list-style-type: none"> i. the notification of affected entities; ii. the transfer of its obligations to other parties; iii. the handling of the revocation status for unexpired certificates that have been issued. 	
7.4.10	Compliance with Legal Requirements	
	The CA shall ensure compliance with legal requirements.	
	<i>CA General</i>	
7.4.10 a)	CA shall ensure it meets all applicable statutory requirements (including requirements of the Data Protection Directive [1] - see next item) for protecting records from loss, destruction and falsification. Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clause 7.4.11).	
7.4.10 b)	The CA shall ensure that the requirements of the European data protection Directive, as implemented through national legislation, are met.	
7.4.10 c)	Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	
7.4.10 d)	The information that users contribute to the CA shall be completely protected from disclosure without the user's agreement, a court order or other legal authorization.	
7.4.11	Recording of information concerning certificates	
	The CA shall ensure that all relevant information concerning a certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.	

Clause number	Requirements	Observations
	<i>General</i>	
7.4.11 a)	The confidentiality and integrity of current and archived records concerning certificates shall be maintained.	
7.4.11 b)	Records concerning certificates shall be completely and confidentially archived in accordance with disclosed business practices.	
7.4.11 c)	Records concerning certificates shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings. The subject, and within the constraints of data protection requirements (see clause 7.4.10) the subscriber, shall have access to registration and other information relating to the subject.	
7.4.11 d)	The precise time of significant CA environmental, key management and certificate management events shall be recorded.	
7.4.11 e)	Records concerning certificates shall be held for a period of time as indicated in the CA's terms and conditions (see clause 7.3.4) in accordance with applicable legislation.	
7.4.11 f)	The events shall be logged in a way that they cannot be easily deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held.	
7.4.11 g)	The specific events and data to be logged shall be documented by the CA.	
	<i>Registration</i>	
7.4.11 h)	The CA shall ensure all events relating to registration including requests for certificate re-key or renewal, are logged.	
7.4.11 i)	The CA shall ensure that all registration information including the following is recorded: i. type of document(s) presented by the applicant to support registration; ii. record of unique identification data, numbers, or a combination thereof (e.g. applicant's drivers license number) of identification documents, if applicable; iii. storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 7.3.1 m); iv. any specific choices in the subscriber agreement (e.g. consent to publication of certificate) see clause 7.3.1 m); v. identity of entity accepting the application; vi. method used to validate identification documents, if any; vii. name of receiving CA and/or submitting Registration Authority, if applicable.	
7.4.11 j)	The CA shall ensure that privacy of subject information is maintained.	
	<i>Certificate generation</i>	
7.4.11 k)	The CA shall log all events relating to the life-cycle of CA keys.	

Clause number	Requirements	Observations
7.4.11 l)	The CA shall log all events relating to the life-cycle of certificates.	
	<i>Subject device provision</i>	
7.4.11 m)	The CA shall log all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA.	
7.4.11 n)	If applicable, the CA shall log all events relating to the preparation of secure user devices.	
	<i>Revocation management</i>	
7.4.11 o)	The CA shall ensure that all requests and reports relating to revocation, as well as the resulting action, are logged.	
7.5	Organizational	
	The CA shall ensure that its organization is reliable.	
	<i>CA general</i>	
7.5 a)	Policies and procedures under which the CA operates shall be non-discriminatory.	
7.5 b)	The CA shall make its services accessible to all applicants whose activities fall within its declared field of operation.	
7.5 c)	The CA is a legal entity according to national law.	
7.5 d)	The CA has adequate arrangements to cover liabilities arising from its operations and/or activities.	
7.5 e)	The CA has the financial stability and resources required to operate in conformity with this policy.	
7.5 f)	The CA has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of electronic trust services or any other related matters.	
7.5 g)	The CA has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.	
	<i>Certificate generation, revocation management</i>	
7.5 h)	The parts of the CA concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services; in particular its senior executive, senior staff and staff in trusted roles, must be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.	
7.5 i)	The parts of the CA concerned with certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.	