قائمة التدقيق المرجعية : Reference Auditing List

(الملحق رقم ٣)

Technical requirement reference	Short description	Comply / Not Comply	Reason of not Comply	Action Required	Comments
[ETSI 319 411-1] Clause 5	**General provisions on CPS and CP**				
[ETSI 319 411-1] Clause 5.1	**General requirements**				
[ETSI 319 411-1] Clause 5.2	**CPS requirements**				
[ETSI 319 401] Clause 6.1 a	Addresses all requirements				
[ETSI 319 401] Clause 6.1 b	Obligations on supporting CA services				
[ETSI 319 401] Clause 6.1 c	make available as necessary				
[ETSI 319 401] Clause 6.1 d	High level management authority				
[ETSI 319 401] Clause 6.1 e	Ensure properly implemented				
[ETSI 319 401] Clause 6.1 f	Review process				
[ETSI 319 401] Clause 6.1 g	Notice of changes				
[ETSI 319 401] Clause 6.1 h	Indicate how to terminate the service				
[ETSI 319 411-1] Clause 5.2 b	identify root and sub CAs				
[ETSI 319 411-1] Clause 5.2 c	document algorithms and parameters employed				
[ETSI 319 411-1] Clause 5.2 d	publicly disclose the CSP on a 24x7 basis				
[ETSI 319 411-1] Clause 5.2 e	publicly adhere to CABF docs latest versions				
[ETSI 319 411-1] Clause 5.2 f	update CPS adequately				
[ETSI 319 411-1] Clause 5.2	specify CA signing keys, CRLs and OCSP				

h					
[ETSI 319 411-1] Clause 5.3	**Certificate policy name and identification**				
[ETSI 319 411-1] Clause 5.3	CP identifier				
[ETSI 319 411-1] Clause 5.4	**PKI participants**				
[ETSI 319 411-1] Clause 5.4.1	**Certification Authority**				
[ETSI 319 411-1] Clause 5.4.1	Use other parties for providing certification services				
[ETSI 319 411-1] Clause 5.4.1	Include a hierarchy of CAs				
[ETSI 319 411-1] Clause 5.4.2	**Subscriber and subject**				
[ETSI 319 411-1] Clause 5.4.3	Other participants to be identified				
[ETSI 319 411-1] Clause 5.5	**Certificate usage**				
[ETSI 319 411-1] Clause 5.5	For Extended Validation Certificates **G**uidelines				
[ETSI 319 411-1] Clause 5.5	For PTC (Publicly-Trusted Certificates)				
[ETSI 319 411-1] Clause 6	**SP practice**				
[ETSI 319 411-1] Clause 6.1	**Publication and Repository Responsibilities**				
[ETSI 319 411-1] Clause 6.1 a	certificate available to subscriber				
[ETSI 319 411-1] Clause 6.1 b	subject's consent for certificate availability				
[ETSI 319 411-1] Clause 6.1 c	Terms and conditions available to Relying Parties. Check also clause 6.9.4				
[ETSI 319 411-1] Clause 6.1 d	terms and conditions identifiable for a given certificate				
[ETSI 319 411-1] Clause 6.1 e i)	LCP (Lightweight Certificate Policy) : information in b) and c) availability				
[ETSI 319 411-1] Clause 6.1 e ii)	NCP(Normalized Certificate Policy): information in b) and c) availability 24x7				

[ETSI 319 411-1] Clause 6.1 f	information on terms and conditions publicly and internationally available				
[ETSI 319 411-1] Clause 6.1 g	certificate publicly and internationally available				
[ETSI 319 411-1] Clause 6.2	**Identification and Authentication**				
[ETSI 319 411-1] Clause 6.2.1	**Naming**				
[ETSI 319 411-1] Clause 6.2.1 Naming	Requirements for naming in certificates are as specified in Recommendation ITU-T X.509 or IETF RFC 5280 and the appropriate part of ETSI EN 319 412.				
[ETSI 319 411-1] Clause 6.2.2	**Initial Identity Validation**				
[ETSI 319 411-1] Clause 6.2.2 a	Verification on subject´s identity				
[ETSI 319 411-1] Clause 6.2.2 b	Evidence of subject´s identity when a natural person				
[ETSI 319 411-1] Clause 6.2.2 c	evidences to be checked for a natural person				
[ETSI 319 411-1] Clause 6.2.2 d	Evidence of subject´s identity when a natural person associated to a legal person				
[ETSI 319 411-1] Clause 6.2.2 e	evidences to be checked for a natural person when in association with a legal person				
[ETSI 319 411-1] Clause 6.2.2 e 1)	full name				
[ETSI 319 411-1] Clause 6.2.2 e 2)	date and place of birth				
[ETSI 319 411-1] Clause 6.2.2 e 3)	full name and legal status of the legal person				
[ETSI 319 411-1] Clause 6.2.2 e 4)	existing registration evidence of the legal person				
[ETSI 319 411-1] Clause	affiliation of the natural person to the legal				

6.2.2 e 5)	person				
[ETSI 319 411-1] Clause 6.2.2 e 6)	what and how to include in this association				
[ETSI 319 411-1] Clause 6.2.2 e 7)	Approval by the natural and legal person				
[ETSI 319 411-1] Clause 6.2.2 f	When the subject is a legal person				
[ETSI 319 411-1] Clause 6.2.2 g	Evidences to be checked when the subject is a legal person				
[ETSI 319 411-1] Clause 6.2.2 g 1)	Full name of the organization				
[ETSI 319 411-1] Clause 6.2.2 g 2)	what and how to include in this association				
[ETSI 319 411-1] Clause 6.2.2 h	When the subject is a device operated by a legal person				
[ETSI 319 411-1] Clause 6.2.2 i	Evidences to be checked when the subject is a device operated by a legal person				
[ETSI 319 411-1] Clause 6.2.2 i 1)	identify the device				
[ETSI 319 411-1] Clause 6.2.2 i 2)	Full name of the organization				
[ETSI 319 411-1] Clause 6.2.2 i 3)	existing registration evidence of the legal person				
[ETSI 319 411-1] Clause 6.2.2 i 4)	nationally recognized identity number				
[ETSI 319 411-1] Clause 6.2.2 i 5)	what and how to include in this association				
[ETSI 319 411-1] Clause 6.2.2 j	When the subject is a device operated by a natural person				
[ETSI 319 411-1] Clause 6.2.2 k	Evidences to be checked when the subject is a device operated by a natural person				
[ETSI 319 411-1] Clause	identifier of the device				

6.2.2 k 1)					
[ETSI 319 411-1] Clause 6.2.2 k 2)	nationally recognized identity number				
[ETSI 319 411-1] Clause 6.2.2 l	recording all the information necessary				
[ETSI 319 411-1] Clause 6.2.2 m	Evidence of acting on behalf of. Check also clause 5.4.2				
[ETSI 319 411-1] Clause 6.2.2 m 1)	full name of the subscriber				
[ETSI 319 411-1] Clause 6.2.2 m 2)	evidences when the subscriber is a natural person				
[ETSI 319 411-1] Clause 6.2.2 m 3)	evidences when the subscriber represents a legal person				
[ETSI 319 411-1] Clause 6.2.2 n	provide physical address				
[ETSI 319 411-1] Clause 6.2.2 o	adhere to national data protection Legislations				
[ETSI 319 411-1] Clause 6.2.2 p	verification policy only for the intended used of the certificate				
[ETSI 319 411-1] Clause 6.2.2 q	Subscriber and SP to be separate entities				
[ETSI 319 411-1] Clause 6.2.3	**Identification and authentication for Re-key requests**				
[ETSI 319 411-1] Clause 6.2.3	Request for certificates issued previously				
[ETSI 319 411-1] Clause 6.2.3 a	check certificate				
[ETSI 319 411-1] Clause 6.2.3 a i)	check the existence and validity of the certificate				
[ETSI 319 411-1] Clause 6.2.3 a ii)	**EVCP** (Extended Validation Certificate Policy) and **EVCG** (Extended Validation Certificate Guidelines)				

[ETSI 319 411-1] Clause 6.2.3 a iii)	**OVCP** (Organization Validation Certificate Policy) and **BRG** (Baseline Requirements Guidelines)				
[ETSI 319 411-1] Clause 6.2.3 b	check SP terms & conditions				
[ETSI 319 411-1] Clause 6.2.3 c	Follow requirements of clause 6.2.2				
[ETSI 319 411-1] Clause 6.2.4	**Identification and authentication for revocation requests**				
[ETSI 319 411-1] Clause 6.2.4 § 1	certificates are revoked in a timely manner				
[ETSI 319 411-1] Clause 6.2.4 a	procedures for revocation are documented as required				
[ETSI 319 411-1] Clause 6.2.4 a i)	Who can submit				
[ETSI 319 411-1] Clause 6.2.4 a ii)	How can be submitted				
[ETSI 319 411-1] Clause 6.2.4 a iii)	Additional requirements for confirmation				
[ETSI 319 411-1] Clause 6.2.4 a iv)	revocation status "suspended"				
[ETSI 319 411-1] Clause 6.2.4 a v)	the mechanism to distribute the revocation information				
[ETSI 319 411-1] Clause 6.2.4 a vi)	Max delay between request and revocation status change				
[ETSI 319 411-1] Clause 6.2.4 a vii)	Max delay between confirmation of revocation/suspension and its updating to be available for relying parties				
[ETSI 319 411-1] Clause 6.2.4 a viii)	Synchronization with UTC (Coordinated Universal Time)				
[ETSI 319 411-1] Clause 6.2.4 b	requests processed on receipt				
[ETSI 319 411-1] Clause 6.2.4 c	requests and reports authenticated				

[ETSI 319 411-1] Clause 6.3	**Certificate Life-Cycle Operational Requirements**				
[ETSI 319 411-1] Clause 6.3.1	**Certificate Application**				
[ETSI 319 411-1] Clause 6.3.1 a	Subject´s possession of the private key				
[ETSI 319 411-1] Clause 6.3.1 b	dual control for validation process				
[ETSI 319 411-1] Clause 6.3.2	**Certificate application processing**				
[ETSI 319 411-1] Clause 6.3.2	Application from trusted registration service				
[ETSI 319 411-1] Clause 6.3.2 a	registration data control				
[ETSI 319 411-1] Clause 6.3.3	**Certificate issuance**				
[ETSI 319 411-1] Clause 6.3.3	Issue certificates securely				
[ETSI 319 411-1] Clause 6.3.3 a	Certificate profiles.				
[ETSI 319 411-1] Clause 6.3.3 b	measures against forgery				
[ETSI 319 411-1] Clause 6.3.3 c	Certificate generation procedure linked to registration/renewal procedures				
[ETSI 319 411-1] Clause 6.3.3 d i)	procedure of issuing certificates linked to the generation of the key pairs				
[ETSI 319 411-1] Clause 6.3.3 d ii)	private key securely passed				
[ETSI 319 411-1] Clause 6.3.3 d iii)	secure crypto device secure delivered				
[ETSI 319 411-1] Clause 6.3.3 e	uniqueness of name				
[ETSI 319 411-1] Clause	representing the subscriber				

6.3.3 f					
[ETSI 319 411-1] Clause 6.3.3 g	Use the policy identifier				
[ETSI 319 411-1] Clause 6.3.4	**Certificate acceptance**				
[ETSI 319 411-1] Clause 6.3.4 § 1	Terms and conditions available				
[ETSI 319 411-1] Clause 6.3.4 a	CA inform subscriber on the use of the certificate				
[ETSI 319 411-1] Clause 6.3.4 b	Subject informed of obligations if different from subscriber				
[ETSI 319 411-1] Clause 6.3.4 c i)	Terms and conditions communicated through a durable means of communication				
[ETSI 319 411-1] Clause 6.3.4 c ii)	Terms and conditions transmitted electronically and in understandable language				
[ETSI 319 411-1] Clause 6.3.4 c iii)	Terms and conditions use the PDS (PKI Disclosure Statement) described in Annex A				
[ETSI 319 411-1] Clause 6.3.4 d	Recording signed agreement with subscriber.				
[ETSI 319 411-1] Clause 6.3.4 e	when the subject and subscriber are different				
[ETSI 319 411-1] Clause 6.3.4 e part 1	Sign by the subscriber				
[ETSI 319 411-1] Clause 6.3.4 e part 1 i)	Agreement to the subscriber obligations				
[ETSI 319 411-1] Clause 6.3.4 e part 1 ii)	The use of a cryptographic device				
[ETSI 319 411-1] Clause 6.3.4 e part 1 iii)	Keeping of record				
[ETSI 319 411-1] Clause 6.3.4 e part 1 iv)	conditions to consent the publication of the certificate				

[ETSI 319 411-1] Clause 6.3.4 e part 1 v)	confirmation of the certification information correctness				
[ETSI 319 411-1] Clause 6.3.4 e part 1 vi)	obligations applicable to subjects				
[ETSI 319 411-1] Clause 6.3.4 e part 1 vii)	**PTC** (Publicly- Trusted Certificate) and **BRG** (Baseline Requirements Guidelines)				
[ETSI 319 411-1] Clause 6.3.4 e part 1 viii)	**EVCG** (Extended Validation Certificate Guidelines)				
[ETSI 319 411-1] Clause 6.3.4 e part 2	Sign by the subject				
[ETSI 319 411-1] Clause 6.3.4 e part 2 i)	Agreement by the subject				
[ETSI 319 411-1] Clause 6.3.4 e part 2 ii)	obligations applicable to subjects				
[ETSI 319 411-1] Clause 6.3.4 e part 2 iii)	The use of a cryptographic device				
[ETSI 319 411-1] Clause 6.3.4 e part 2 iv)	Keeping of record				
[ETSI 319 411-1] Clause 6.3.4 f	when the subject and subscriber are the same				
[ETSI 319 411-1] Clause 6.3.4 g	agreement in electronic form				
[ETSI 319 411-1] Clause 6.3.4 h	records retained for a period of time				
[ETSI 319 411-1] Clause 6.3.5	**Key Pair and Certificate Usage**				
[ETSI 319 411-1] Clause 6.3.5 § 1	Subscriber´s obligations as per clause 6.3.4 items a) to j)				
[ETSI 319 411-1] Clause 6.3.5 § 2	Subject´s obligations to include items b) c) e) f) h) i) and j)				
[ETSI 319 411-1] Clause 6.3.5 a	accurate and complete information to SP				

[ETSI 319 411-1] Clause 6.3.5 b	limitation on the use of the key pairs				
[ETSI 319 411-1] Clause 6.3.5 c	unauthorized use of private key				
[ETSI 319 411-1] Clause 6.3.5 d i)	when subject/subscriber generate keys, use an algorithm fit to the industry				
[ETSI 319 411-1] Clause 6.3.5 d ii)	when subject/subscriber generate keys, use a key length fit to the industry				
[ETSI 319 411-1] Clause 6.3.5 e	when private key is for signatures or seals				
[ETSI 319 411-1] Clause 6.3.5 f	use the private key when in a secure device				
[ETSI 319 411-1] Clause 6.3.5 g	when generating keys in the secure device				
[ETSI 319 411-1] Clause 6.3.5 h	notify SP of any issue				
[ETSI 319 411-1] Clause 6.3.5 i	discontinue private key after compromise				
[ETSI 319 411-1] Clause 6.3.5 j	Ensure the private key is not used after compromise or revocation				
[ETSI 319 411-1] Clause 6.3.5 k	Verify validity of revocation status. Check applicable requirements in clauses 6.2.4, 6.3.9 and 6.3.10				
[ETSI 319 411-1] Clause 6.3.5 l	Limits on the use of the certificate.				
[ETSI 319 411-1] Clause 6.3.5 m	taking some other measures				
[ETSI 319 411-1] Clause 6.3.5 m i) 1)	Problem reporting				
[ETSI 319 411-1] Clause 6.3.5 m i) 2)	Problem reporting				
[ETSI 319 411-1] Clause	**Certificate Renewal**				

6.3.6					
[ETSI 319 411-1] Clause 6.3.6	Certificate requests are complete				
[ETSI 319 411-1] Clause 6.3.6 a i)	Certificate to renew exists				
[ETSI 319 411-1] Clause 6.3.6 a ii)					
[ETSI 319 411-1] Clause 6.3.6 a iii)					
[ETSI 319 411-1] Clause 6.3.6 b	Terms and condition changes. Check also clause 6.3.4 a, b, c and d				
[ETSI 319 411-1] Clause 6.3.6 c	Revalidation of registration information. Check also clause 6.2.2 h to l				
[ETSI 319 411-1] Clause 6.3.6 d	Issue a new certificate if meet conditions				
[ETSI 319 411-1] Clause 6.3.7	**Certificate Re-key**				
[ETSI 319 411-1] Clause 6.3.7	check with 6.2.3				
[ETSI 319 411-1] Clause 6.3.8	**Certificate Modification**				
[ETSI 319 411-1] Clause 6.3.8	Certificate requests are complete				
[ETSI 319 411-1] Clause 6.3.8 a	Requirements of 6.2.2 apply				
[ETSI 319 411-1] Clause 6.3.9	**Certificate Revocation and Suspension**				
[ETSI 319 411-1] Clause 6.3.9 §1	Revoke certificates in a timely manner				
[ETSI 319 411-1] Clause 6.3.9 a	subject informed of the change in the status of the certificate				
[ETSI 319 411-1] Clause	not reinstating a revoked certificate				

6.3.9 b					
[ETSI 319 411-1] Clause 6.3.9 c	daily publication of CRLs				
[ETSI 319 411-1] Clause 6.3.9 c i)	Stating a time for next scheduled CRL issue				
[ETSI 319 411-1] Clause 6.3.9 c ii)	new CRL published before the stated time				
[ETSI 319 411-1] Clause 6.3.9 c iii)	CRL signed by the CA or any entity designed by the SP				
[ETSI 319 411-1] Clause 6.3.9 d	Operate and maintain certificates status information				
[ETSI 319 411-1] Clause 6.3.9 e	Operate and maintain certificates status information				
[ETSI 319 411-1] Clause 6.3.9 f	generation of CARLs (Certificate Authority Revocation List)				
[ETSI 319 411-1] Clause 6.3.9 g	CARLs every month for cross-certificates				
[ETSI 319 411-1] Clause 6.3.10	**Certificate Status Services**				
[ETSI 319 411-1] Clause 6.3.10 §1	SP to provide services for checking the status of the certificates				
[ETSI 319 411-1] Clause 6.3.10 a	revocation management services 24/7				
[ETSI 319 411-1] Clause 6.3.10 b	Protect the integrity of the status information				
[ETSI 319 411-1] Clause 6.3.10 c	include status information until the certificate expires				
[ETSI 319 411-1] Clause 6.3.10 d	Support OCSP (Online Certificate Status Protocol)				
[ETSI 319 411-1] Clause 6.3.10 e	Support CRL (Certificate Revocation List)				

[ETSI 319 411-1] Clause 6.3.10 f	All revocation status information shall be consistent				
[ETSI 319 411-1] Clause 6.3.10 g	revocation information shall be publicly and internationally available				
[ETSI 319 411-1] Clause 6.3.11	**End of Subscription**				
[ETSI 319 411-1] Clause 6.3.12	**Key Escrow and Recovery**				
[ETSI 319 411-1] Clause 6.3.12 a	Same security level for duplicated subject´s private keys				
[ETSI 319 411-1] Clause 6.3.12 b	number of duplicated subject´s private keys				
[ETSI 319 411-1] Clause 6.3.12 c	subject´s private key to be used for digital signatures				
[ETSI 319 411-1] Clause 6.3.12 d	subject´s private key to be used for authentication				
[ETSI 319 411-1] Clause 6.3.12 e	subject´s private key to be used for decryption				
[ETSI 319 411-1] Clause 6.3.12 f	CA requires the subject´s private key used for decryption				
[ETSI 319 411-1] Clause 6.3.12 g	Copy of the subject's private key				
[ETSI 319 411-1] Clause 6.4	**Facility, Management, and Operational Controls**				
[ETSI 319 411-1] Clause 6.4.1	**General**				
[ETSI 319 401] Clause 5	having a risk assessment				
[ETSI 319 401] Clause 6.3 a	SP security policy				
[ETSI 319 401] Clause 6.3 b	Overall responsibility for the procedures described in the security policy				
[ETSI 319 401] Clause 6.3 c	Inventory of assets				

[ETSI 319 401] Clause 7.3.1	general requirements on asset management				
[ETSI 319 401] Clause 7.3.2	media handling on asset management				
[ETSI 319 411-1] Clause 6.4.2	**Physical Security Controls**				
[ETSI 319 401] Clause 7.6 a	Physical access to authorized individuals				
[ETSI 319 401] Clause 7.6 b	controls on assets and business				
[ETSI 319 401] Clause 7.6 c	control on information processing facilities				
[ETSI 319 401] Clause 7.6 d	critical components secure protected				
[ETSI 319 411-1] Clause 6.4.2 a	controlled access				
[ETSI 319 411-1] Clause 6.4.2 b	oversight by authorized persons				
[ETSI 319 411-1] Clause 6.4.2 c	security perimeters				
[ETSI 319 411-1] Clause 6.4.2 d	physical and environmental security controls				
[ETSI 319 411-1] Clause 6.4.2 e	controls against CA assets taken off without authorization				
[ETSI 319 411-1] Clause 6.4.2 f	Additional functions for limiting access to authorized personnel				
[ETSI 319 411-1] Clause 6.4.2 g	Root CA private keys physically isolated				
[ETSI 319 411-1] Clause 6.4.3	**Procedural Controls**				
[ETSI 319 401] Clause 7.4 b	effective administration of user				
[ETSI 319 401] Clause 7.4 c	access to information and application system functions restricted in accordance with access control policy				
[ETSI 319 401] Clause 7.4 d	personnel properly identified and authenticated before using critical applications				
[ETSI 319 401] Clause 7.4 e	personnel accountable for their activities				

[ETSI 319 411-1] Clause 6.4.3 a	multi factor authentication for certificate issuance				
[ETSI 319 411-1] Clause 6.4.4	**Personnel Controls**				
[ETSI 319 401] Clause 7.2 a	Personnel is qualified				
[ETSI 319 401] Clause 7.2 b	Personnel is trained				
[ETSI 319 401] Clause 7.2 c	disciplinary sanctions				
[ETSI 319 401] Clause 7.2 d	roles and responsibility in job description				
[ETSI 319 401] Clause 7.2 e	separation of duties				
[ETSI 319 401] Clause 7.2 f	personnel exercises in line with SP procedures				
[ETSI 319 401] Clause 7.2 g	managerial personnel experience in eSignature and information security				
[ETSI 319 401] Clause 7.2 h	no conflict of interest				
[ETSI 319 401] Clause 7.2 i	trusted roles				
[ETSI 319 401] Clause 7.2 j	formal appointment in trusted roles				
[ETSI 319 401] Clause 7.2 k	no access before applicable checks				
[ETSI 319 411-1] Clause 6.4.4 a	additional trusted roles as per CEN TS 419 261				
[ETSI 319 411-1] Clause 6.4.4 b	additional trusted role as per CABF docs				
[ETSI 319 411-1] Clause 6.4.5	**Audit Logging Procedures**				
[ETSI 319 401] Clause 7.10 a	confidentiality and integrity of current and archived records				
[ETSI 319 401] Clause 7.10 b	records archived in accordance with disclosed business practices				
[ETSI 319 401] Clause 7.10 c	records made available for providing evidences of operation correctness				
[ETSI 319 401] Clause 7.10 d	record of significant event				
[ETSI 319 401] Clause 7.10 e	appropriate retention period				

[ETSI 319 401] Clause 7.10 f	Log events				
[ETSI 319 411-1] Clause 6.4.5 a	log all events relating to security				
[ETSI 319 411-1] Clause 6.4.5 b	events relating to registration are logged				
[ETSI 319 411-1] Clause 6.4.5 c	Registration information to record.				
[ETSI 319 411-1] Clause 6.4.5 d	privacy of subject information				
[ETSI 319 411-1] Clause 6.4.5 e	log all events relating to the life-cycle of CA keys				
[ETSI 319 411-1] Clause 6.4.5 f	log all events relating to the life-cycle of certificates				
[ETSI 319 411-1] Clause 6.4.5 g	log all events relating to the life cycle of keys managed by the CA				
[ETSI 319 411-1] Clause 6.4.5 h	log all events relating to revocation				
[ETSI 319 411-1] Clause 6.4.6	**Records Archival**				
[ETSI 319 411-1] Clause 6.4.6 a	Retain logs				
[ETSI 319 411-1] Clause 6.4.6 a i)	logs all events related to life cycle of keys				
[ETSI 319 411-1] Clause 6.4.6 a ii)	Documentation				
[ETSI 319 411-1] Clause 6.4.7	**Key Changeover**				
[ETSI 319 411-1] Clause 6.4.8	**Compromise and Disaster Recovery**				
[ETSI 319 401] Clause 7.9	Monitoring system activities				
[ETSI 319 401] Clause 7.9 a	Sensitive of information monitored				
[ETSI 319 401] Clause 7.9 b	Report abnormal system activities				

[ETSI 319 401] Clause 7.9 c	startup and shutdown monitor				
[ETSI 319 401] Clause 7.9 d	Respond quickly to incidents				
[ETSI 319 401] Clause 7.9 e	Establish procedure for notifying				
[ETSI 319 401] Clause 7.9 f	Notifying security breaches				
[ETSI 319 401] Clause 7.9 g	Monitor audit logs				
[ETSI 319 401] Clause 7.9 h	Mitigate critical vulnerabilities				
[ETSI 319 401] Clause 7.9 i	Procedures for incident reporting and responses				
[ETSI 319 401] Clause 7.11	Business continuity management				
[ETSI 319 411-1] Clause 6.4.8 a	CA systems data backup and recovery in safe place				
[ETSI 319 411-1] Clause 6.4.8 b	Backup copies				
[ETSI 319 411-1] Clause 6.4.8 c	Back-up by trusted roles. Check also clause 6.4.4				
[ETSI 319 411-1] Clause 6.4.8 d	Risk analysis identifying dual control				
[ETSI 319 411-1] Clause 6.4.8 e	business continuity address CA key compromise				
[ETSI 319 411-1] Clause 6.4.8 f	taking measures to avoid a disaster				
[ETSI 319 411-1] Clause 6.4.8 g i)	information to provide in case of compromise				
[ETSI 319 411-1] Clause 6.4.8 g ii)	indicate the status information in case of compromise				
[ETSI 319 411-1] Clause 6.4.8 g iii)	revoke certificates in case of compromise				
[ETSI 319 411-1] Clause 6.4.8 h i)	inform subscribers in case of algorithm compromise				
[ETSI 319 411-1] Clause 6.4.8 h ii)	revoke certificates in case of algorithm compromise				
[ETSI 319 411-1] Clause 6.4.9	**CA or RA Termination**				

[ETSI 319 401] Clause 7.12 a	Up to date termination plan				
[ETSI 319 401] Clause 7.12 b	Procedures to execute as minimum				
[ETSI 319 401] Clause 7.12 b i)	Inform to subscribers				
[ETSI 319 401] Clause 7.12 b ii)	terminate authorization of all subcontractors				
[ETSI 319 401] Clause 7.12 b iii)	Transfer to a reliable party its obligations				
[ETSI 319 401] Clause 7.12 b iv)	Private keys to be destroyed				
[ETSI 319 401] Clause 7.12 b v)	make arrangements to transfer possible customer services				
[ETSI 319 401] Clause 7.12 c	Cover costs in case of bankruptcy				
[ETSI 319 401] Clause 7.12 d	Minimum provisions when terminate in its CPS				
[ETSI 319 401] Clause 7.12 d i)	notification of affected entities				
[ETSI 319 401] Clause 7.12 d ii)	transfer SP obligations to other parties				
[ETSI 319 401] Clause 7.12 e	Transfer to a reliable party its obligations				
[ETSI 319 411-1] Clause 6.4.9 a	SP obligations after CA termination. Check also clauses 6.2.2, 6.3.1, 6.3.4, 6.3.10, 6.4.5, 6.4.6 and 6.8.10				
[ETSI 319 411-1] Clause 6.4.9 b	handling of the revocation status for unexpired certificates				
[ETSI 319 411-1] Clause 6.4.9 c	Another cross certified SP ceases its operations				
[ETSI 319 411-1] Clause 6.5	**Technical Security Controls**				
[ETSI 319 411-1] Clause 6.5.1	**Key Pair Generation and Installation**				
[ETSI 319 401] Clause 7.5	Cryptographic controls				
[ETSI 319 411-1] Clause 6.5.1 a	Physically secure. Check also clauses 6.4.2 and 6.4.4				

[ETSI 319 411-1] Clause 6.5.1 b	Key generation algorithm fit for purpose				
[ETSI 319 411-1] Clause 6.5.1 c	CA signing algorithm and key length fit for purpose				
[ETSI 319 411-1] Clause 6.5.1 d	CA certificate expiration				
[ETSI 319 411-1] Clause 6.5.1 e	Operations performed in between expiry date and last certificate signed				
[ETSI 319 411-1] Clause 6.5.1 f	Key generation ceremony procedure				
[ETSI 319 411-1] Clause 6.5.1 g	Key generation ceremony for root and sub CAs carried out as indicated in the procedure				
[ETSI 319 411-1] Clause 6.5.1 h	Certification authority public key distribution				
[ETSI 319 411-1] Clause 6.5.1 i	Key generation algorithm fit for purpose				
[ETSI 319 411-1] Clause 6.5.1 j	Subject keys fit for purpose				
[ETSI 319 411-1] Clause 6.5.1 k	Secure generation before delivery				
[ETSI 319 411-1] Clause 6.5.1 l	Secure delivery				
[ETSI 319 411-1] Clause 6.5.1 m	Copy of a private key				
[ETSI 319 411-1] Clause 6.5.1 n	secure the issuance of a secure cryptographic device to a subject				
[ETSI 319 411-1] Clause 6.5.1 n i)	Secure cryptographic device preparation securely				
[ETSI 319 411-1] Clause 6.5.1 n ii)	Secure cryptographic device securely stored and distributed				
[ETSI 319 411-1] Clause 6.5.2	**Private Key Protection and Cryptographic Module Engineering Controls**				

[ETSI 319 411-1] Clause 6.5.2 a	CA key generation carried out in a secure cryptographic device				
[ETSI 319 411-1] Clause 6.5.2 a i)	Requirements as per ISO 15408				
[ETSI 319 411-1] Clause 6.5.2 a ii)	Requirements as per ISO 19790 or FIPS 140-2 level 3				
[ETSI 319 411-1] Clause 6.5.2 b	CA private key held and used in a secure cryptographic device				
[ETSI 319 411-1] Clause 6.5.2 c	protection outside device				
[ETSI 319 411-1] Clause 6.5.2 d	Backup process				
[ETSI 319 411-1] Clause 6.5.2 e	Copies of private keys with the same security level				
[ETSI 319 411-1] Clause 6.5.2 f	Access control				
[ETSI 319 411-1] Clause 6.5.2 g	not tampered during shipment				
[ETSI 319 411-1] Clause 6.5.2 h	not tampered while storage				
[ETSI 319 411-1] Clause 6.5.2 i	Secure cryptographic device correctly functioning				
[ETSI 319 411-1] Clause 6.5.2 j	Destruction of secure cryptographic device at end of life				
[ETSI 319 411-1] Clause 6.5.3	**Other Aspects of Key Pair Management**				
[ETSI 319 411-1] Clause 6.5.3	Use appropriately the CA signing key				
[ETSI 319 411-1] Clause 6.5.3 a	Other usage				
[ETSI 319 411-1] Clause 6.5.3 b	Secure premises				

[ETSI 319 411-1] Clause 6.5.3 c	Limited use of CA´s private key. Also check 6.5.1 c				
[ETSI 319 411-1] Clause 6.5.3 d	copies of the CA private signing keys				
[ETSI 319 411-1] Clause 6.5.3 e	Use of self-signed certificates				
[ETSI 319 411-1] Clause 6.5.4	**Activation Data**				
[ETSI 319 411-1] Clause 6.5.4 a	Dual control for key recovery				
[ETSI 319 411-1] Clause 6.5.4 b	secure activation and deactivation				
[ETSI 319 411-1] Clause 6.5.4 c	separation				
[ETSI 319 411-1] Clause 6.5.5	**Computer Security Controls**				
[ETSI 319 401] Clause 7.4 a	controls on SP internal network				
[ETSI 319 401] Clause 7.4 f	Sensitive data in re-used storage objects protected				
[ETSI 319 411-1] Clause 6.5.5 a	certificate generation network secure				
[ETSI 319 411-1] Clause 6.5.5 b	multi-factor authentication				
[ETSI 319 411-1] Clause 6.5.5 c	Access control to add or delete certificates				
[ETSI 319 411-1] Clause 6.5.5 d	monitoring on revocation facilities				
[ETSI 319 411-1] Clause 6.5.5 e	certificate generation monitored and alarm for detection unauthorized access				
[ETSI 319 411-1] Clause 6.5.6	**Life Cycle Security Controls**				
[ETSI 319 401] Clause 7.7 a	Analysis of security requirements				

[ETSI 319 401] Clause 7.7 b	Change control procedures				
[ETSI 319 401] Clause 7.7 c	virus protection				
[ETSI 319 401] Clause 7.7 d	protection of SP media				
[ETSI 319 401] Clause 7.7 e	protection of SP media against obsolescence				
[ETSI 319 401] Clause 7.7 f	procedures for trusted and administrative roles				
[ETSI 319 401] Clause 7.7 g	Secure patching				
[ETSI 319 411-1] Clause 6.5.6 a	capacity demands on NCP				
[ETSI 319 411-1] Clause 6.5.6 b	capacity demands on CABF				
[ETSI 319 411-1] Clause 6.5.6 c	See 6.5.5 e)				
[ETSI 319 411-1] Clause 6.5.7	**Network Security Controls**				
[ETSI 319 401] Clause 7.8 a	segmentation into networks or zones				
[ETSI 319 401] Clause 7.8 b	restrict access and communications between zones				
[ETSI 319 401] Clause 7.8 c	maintain systems critical elements in high security zones				
[ETSI 319 401] Clause 7.8 d	Test platform separated from production				
[ETSI 319 401] Clause 7.8 e	Trusted channels for communications				
[ETSI 319 401] Clause 7.8 f	Redundancy in networking connections				
[ETSI 319 401] Clause 7.8 g	Vulnerability scan				
[ETSI 319 401] Clause 7.8 h	penetration test				
[ETSI 319 411-1] Clause 6.5.7 a	To maintain and protect the CA systems				
[ETSI 319 411-1] Clause 6.5.7 b	Secure configuration of the CA systems				
[ETSI 319 411-1] Clause 6.5.7 c	Trusted roles for CA systems				
[ETSI 319 411-1] Clause	Root CA in a high security zone				

6.5.7 d					
[ETSI 319 411-1] Clause 6.5.8	**Time stamping**				
[ETSI 319 411-1] Clause 6.6	**Certificate, CRL, and OCSP Profiles**				
[ETSI 319 411-1] Clause 6.6.1	**Certificate Profile**				
[ETSI 319 411-1] Clause 6.6.1	requirements on certificates profiles				
[ETSI 319 411-1] Clause 6.6.1	certificates to natural persons				
[ETSI 319 411-1] Clause 6.6.1	certificates to legal persons				
[ETSI 319 411-1] Clause 6.6.1	certificates to web sites				
[ETSI 319 411-1] Clause 6.6.2	**CRL Profile**				
[ETSI 319 411-1] Clause 6.6.2	Profile definition				
[ETSI 319 411-1] Clause 6.6.3	**OCSP Profile**				
[ETSI 319 411-1] Clause 6.6.3	Profile definition				
[ETSI 319 411-1] Clause 6.7	**Compliance Audit and Other Assessment**				
[ETSI 319 411-1] Clause 6.8	**Other Business and Legal Matters**				
[ETSI 319 411-1] Clause 6.8.1	**Fees**				
[ETSI 319 411-1] Clause 6.8.2	**Financial Responsibility**				
[ETSI 319 401] Clause 7.1.1 c	maintain sufficient financial resources				
[ETSI 319 411-1] Clause 6.8.3	**Confidentiality of Business Information**				

[ETSI 319 411-1] Clause 6.8.4	**Privacy of Personal Information**				
[ETSI 319 401] Clause 7.13 c	measures to protect personal data				
[ETSI 319 411-1] Clause 6.8.4 a	registration data protection				
[ETSI 319 411-1] Clause 6.8.4 b	Records securely retained to meet statutory requirements. Check also clauses 6.4.5 and 6.4.6				
[ETSI 319 411-1] Clause 6.8.5	**Intellectual Property Rights**				
[ETSI 319 411-1] Clause 6.8.6	**Representations and Warranties**				
[ETSI 319 401] Clause 6.3 b	Overall responsibility of conformance with the procedures				
[ETSI 319 411-1] Clause 6.8.6 a	Certification services consistent with the CPS				
[ETSI 319 411-1] Clause 6.8.6 b					
[ETSI 319 411-1] Clause 6.8.7	**Disclaimers of Warranties**				
[ETSI 319 411-1] Clause 6.8.8	**Limitations of Liability**				
[ETSI 319 411-1] Clause 6.8.8	Limitations covered by the terms and conditions				
[ETSI 319 411-1] Clause 6.8.9	**Indemnities**				
[ETSI 319 411-1] Clause 6.8.10	**Term and Termination**				
[ETSI 319 411-1] Clause 6.8.11	**Individual notices and communications with participants**				
[ETSI 319 411-1] Clause 6.8.12	**Amendments**				

[ETSI 319 411-1] Clause 6.8.13	**Dispute Resolution Procedures**				
[ETSI 319 401] Clause 6.2 i	Procedures for complaints and dispute settlement				
[ETSI 319 401] Clause 7.1.1 e	Procedures for resolution of complaints regarding provisioning of services				
[ETSI 319 411-1] Clause 6.8.14	**Governing Law**				
[ETSI 319 411-1] Clause 6.8.15	**Compliance with Applicable Law**				
[ETSI 319 401] Clause 7.13 a	evidence on meeting the legal requirements				
[ETSI 319 411-1] Clause 6.8.16	**Miscellaneous Provisions**				
[ETSI 319 411-1] Clause 6.9	**Other Provisions**				
[ETSI 319 411-1] Clause 6.9.1	**Organizational**				
[ETSI 319 401] Clause 7.1.1 a	policies & procedures non discriminatory				
[ETSI 319 401] Clause 7.1.1 b	services available to applicant that agree to abide obligations				
[ETSI 319 401] Clause 7.1.1 c	adequate arrangements to cover liabilities				
[ETSI 319 401] Clause 7.1.1 d	financial stability and resources				
[ETSI 319 401] Clause 7.1.1 e	policies and procedures for the resolution of complaints				
[ETSI 319 401] Clause 7.1.1 f	properly documented agreement and contractual relationship				
[ETSI 319 401] Clause 7.1.2	Segregation of duties				
[ETSI 319 411-1] Clause 6.9.1 a	certificate generation and revocation management independence				

[ETSI 319 411-1] Clause 6.9.1 b	certificate generation and revocation management documented structure which safeguards impartiality of operations				
[ETSI 319 411-1] Clause 6.9.2	**Additional testing**				
[ETSI 319 411-1] Clause 6.9.2 a	Additional testing				
[ETSI 319 411-1] Clause 6.9.2 b	Certificates are for testing clearly indicated				
[ETSI 319 411-1] Clause 6.9.3 c					
[ETSI 319 411-1] Clause 6.9.4 d	Cross certificates				
[ETSI 319 411-1] Clause 6.9.3	**Disabilities**				
[ETSI 319 401] Clause 7.13 b	services accessible for persons with disabilities				
[ETSI 319 411-1] Clause 6.9.4	**Terms and conditions**				
[ETSI 319 401] Clause 6.2	Terms and Conditions availability				
[ETSI 319 401] Clause 6.2 a	trust service policy applicable				
[ETSI 319 401] Clause 6.2 b	limitations on the use of the service				
[ETSI 319 401] Clause 6.2 c	subscriber´s obligations				
[ETSI 319 401] Clause 6.2 d	information for relying parties				
[ETSI 319 401] Clause 6.2 e	period of time logs retained				
[ETSI 319 401] Clause 6.2 f	limitations on liability				
[ETSI 319 401] Clause 6.2 g	limitations on the use of the service including damages				
[ETSI 319 401] Clause 6.2 h	applicable legal system				
[ETSI 319 401] Clause 6.2 i	procedures for complains and disputes				
[ETSI 319 401] Clause 6.2 j	SP assessed and which scheme				
[ETSI 319 401] Clause 6.2 k	SP contact information				

[ETSI 319 401] Clause 6.2 l	Availability				
[ETSI 319 411-1] Clause 6.9.4 a	Include a notice				
[ETSI 319 411-1] Clause 6.9.4 b					
[ETSI 319 411-1] Clause 7	**Framework for the definition of other certificate policies**				
[ETSI 319 411-1] Clause 7.1	**Certificate policy management**				
[ETSI 319 411-1] Clause 7.1 a	Identify basis of certificate policy				
[ETSI 319 411-1] Clause 7.1 b	Certificate policy management authority				
[ETSI 319 411-1] Clause 7.1 c	Risk analysis				
[ETSI 319 411-1] Clause 7.1 d	Review process				
[ETSI 319 411-1] Clause 7.1 e	CPS supports certificate policies				
[ETSI 319 411-1] Clause 7.1 f	Make available the CPs				
[ETSI 319 411-1] Clause 7.1 g	Make available revision of CPs				
[ETSI 319 411-1] Clause 7.1 h	incorporates requirements of clauses 5 and 6				
[ETSI 319 411-1] Clause 7.1 i	Certificate profile requirements specified by the CPs				
[ETSI 319 411-1] Clause 7.1 j	Profiles according to ETSI				
[ETSI 319 411-1] Clause 7.1 k	Unique identifier				
[ETSI 319 411-1] Clause 7.2	**Additional requirements**				
[ETSI 319 411-1] Clause 7.2	Inform subscribers and relying parties of policies applied. Check applicable additional				

	requirements in clause 6.9.4				