Created September 10th 2020 and updated November 24 to match with the new Telia CPS documents.
CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)
Introduction must include:

1) CA's Legal Name
Telia CA (Telia Finland Oyj; part of Telia Company AB)

2) Root CA Info

Distinguished name of the CA	**Issuer**	**SHA2 fingerprint of the CA certificate**

CN = Sonera Class2 CA
O = Sonera, C = FI
	Self-signed	7908B40314C138100B518D0735807FFBFCF8518A0095337105BA386B153DD927□

CN = TeliaSonera Root CA v1□	Self-signed	DD6936FE21F8F077C123A1A521C12224F72255B73E03A7260693E8A24B0FA389
O = TeliaSonera	Sonera Class2 CA	E9563581E712B290F23A749346535EB0D981E3D4A39D56D604684CD0B1698C89
CN = Telia Root CA v2	Self-signed	242B69742FCB1E5B2ABF98898B94572187544E5B4D9911786573621F6A74B82C
O = Telia Finland Oyj, C = FI	TeliaSonera Root CA v1	EF6F29F636F62BDD4753122F41F3419EE7C2877587BE4A9807ADF58946458E7F

CN = TeliaSonera Server CA v2
O = TeliaSonera, C = FI
	TeliaSonera Root CA v1	D721110388CA6F20BBA9FD1A8DBA4EFB8C16392A3DEBAD97C553EEAF0ACACAAC

CN = TeliaSonera Gateway CA v2
O = TeliaSonera, C = FI
	TeliaSonera Root CA v1	46226B7B89E02CA8F5D85D67ED8CB4B19C48382058BB16242199D540CABE9268

CN = Telia Extended Validation CA v3
O = Telia Finland Oyj, C = FI
	Telia Root CA v2	98C2545A2C05A342EDB22A9F6C7CCC1FE98D87595676E3A298ADE97F7B01291D□

CN = Telia Domain Validation CA v2
O = Telia Finland Oyj, C = FI
	TeliaSonera Root CA v1	5B312B7E11B70D07C14E0AB99F08D00748966098C52AA85A06A0822BBE59A02C

CN = Telia Domain Validation CA v3 O = Telia Finland Oyj, C = FI	Telia Root CA v2	A7E83056E9B3D9DDB1816B95518F6A5E5A1DFDFA28F60533B1C850855EAA4263

CN = Telia Server CA v3
O = Telia Finland Oyj, C = FI
	Telia Root CA v2	1281AD8FABE883F209E9636448D1A80C373DAA7686C813A270FAD48F5F5E589A□

CN = TeliaSonera Class 1 CA v2
O = TeliaSonera, C = FI
	TeliaSonera Root CA v1	B95AE54F838E3ABF0B57ACCC1B1266DC68C7A3FA774015FA128D60CDD1AAE280

CN = TeliaSonera Class 2 CA v2
O = TeliaSonera, C = SE
	TeliaSonera Root CA v1	092829433D231949F4A9BC666CBF54B3AA27D7BEBCA048D75E59093E15A72EA5

CN = TeliaSonera Email CA v4
O = TeliaSonera, C = SE
	TeliaSonera Root CA v1	D1F2656AC8382739A3B087C47AB5CAB945A32F162B6149C308783C7E06AF8AE8□

CN = Ericsson NL Individual CA v3
O = Ericsson, C = SE
	TeliaSonera Root CA v1	63ED95B17FFDCB7AE30FEAC6A874653099264E21B268D836D957966F0B04BE43

CN = Telia Document Signing CA v3
O = Telia Finland Oyj, C = FI
	Telia Root CA v2	6924A4DD82948DA53F6FB933E895A0F6581C8DBDEBABB36FC11CAC25E9C0335A□

CN = Telia Class 3 CA v1
C = SE, O = Telia Company AB
	Telia Root CA v2	E7340DC9475E87C4E5A4572C82604C5EFF9BF60B231C5486943173B26A4CAFCC

3) List the specific version(s) of the BRs that you used	BR version 1.7.3. that is self-assessed

4) List of documents for evaluation
Telia Server Certificate CPS (https://cps.trust.telia.com/Telia_Server_Certificate_CPS_v2.9.pdf)
Telia Production CPS (https://cps.trust.telia.com/Telia_Production_CPS_v3.0.pdf)
Telia Root CPS (https://cps.trust.telia.com/Telia_Root_CPS_v2.8.pdf)
Telia Client CPS (https://cps.trust.telia.com/Telia_Client_Certificate_CPS_v1.6.pdf)

NOTE! All items are stated as compliant in this CPS because in its chapter 1.1 it has a statement promising that Telia SSL and EV certificates conform to the current version of related CA Browser Forum specification. Most of the issues are also separately specified in the CPS and those chapters are now listed below.

5) Future work	
For CRL verification we aim to add the reason code for SC31 by September 2020.	

BR Section Number	**List the specific documents and section numbers of those documents which meet the requirements of each BR section**	**Explain how the CA's listed documents meet the requirements of each BR section.**
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.		Compliant with BR 1.2.1

1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*		Compliant with BR 1.2.2
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. *Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs (including non-delegation of domain validation to RAs).*	Telia Server Certificate CPS 1.3.2	Compliant with BR 1.3.2 NOTE: Delegated are not used by Telia CA and all validations are done by Telia CA or its daughter companies.
1.5.2 Contact person BR Section 4.9.3 requires that this section 1.5.2 contain clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates.	Telia Server Certificate CPS 1.5.2	Compliant with BR 1.5.2
2.1. Repositories *Provide the direct URLs to the CA's repositories*	https://cps.trust.telia.com/ http://ocsp.trust.telia.com http://httpcrl.trust.telia.com/soneraclass2ca.crl http://httpcrl.trust.telia.com/teliasonerarootcav1.crl http://httpcrl.trust.telia.com/teliarootcav2.crl http://httpcrl.trust.telia.com/teliasoneraservercav2.crl http://httpcrl.trust.telia.com/teliasoneragatewaycav2.crl http://httpcrl.trust.telia.com/teliaextendedvalidationcav3.crl http://httpcrl.trust.telia.com/teliadomainvalidationcav2.crl http://httpcrl.trust.telia.com/teliadomainvalidationcav3.crl http://httpcrl.trust.telia.com/teliaservercav3.crl http://crl-3.trust.teliasonera.com/teliasoneraclass1cav2.crl http://crl-2.trust.teliasonera.com/teliasoneraclass2cav2.crl http://crl-2.trust.teliasonera.com/teliasoneraemailcav4.crl http://crl.trust.telia.com/ericssonnlindividualcav3.crl http://httpcrl.trust.telia.com/teliadocumentsigningcav3.crl	
2.2 Publication of information - RFC 3647 "The Certificate Policy and/or Certification Practice Statement **MUST be structured in accordance with RFC 3647**."	Telia Server Certificate CPS 1.1	Compliant with BR 2.2
2.2 Publication of information - CAA Section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement SHALL state the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names; that policy shall be consistent with these Requirements. It shall clearly specify the set of Issuer Domain Names that the CA recognizes in CAA "issue" or "issuewild" records as permitting it to issue. The CA SHALL log all actions taken, if any, consistent with its processing practice.	Telia Server Certificate CPS 4.2.4	Compliant with BR 2.2
2.2. Publication of information - BR text "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> ***Copy the specific text that is used into the explanation in this row. (in English)***	Telia Server Certificate CPS 1.1	Compliant with BR 2.2 NOTE: Both OV and DV certificates conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Documents, those Documents take precedence over this document.

2.2. Publication of information - test websites "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> ***List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.***	Pages with CA chain TeliaSonera Root CA v1, Telia Root CA v2 (https://juolukka.cover.telia.fi:10500/) Pages have CA chain Telia Root CA v2 (https://juolukka.cover.telia.fi:10600/)	Compliant with BR 2.2
2.3. Time or frequency of publication "The CA SHALL ... **annually** update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. Section 3.3 of Mozilla's Root Store Policy states: "CPs and CPSes MUST be reviewed and updated as necessary at least once every year, as required by the Baseline Requirements. **CAs MUST indicate that this has happened by incrementing the version number and adding a dated changelog entry**, even if no other changes are made to the document." *Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.*	The process is not yet in the CPS documents and will be added during October 2020.	Compliant with BR 2.3 NOTE: Telia CA CPS is reviewed and updated or modified versions are published at least once per year and in accordance with section 9.12 of this CPS.
2.4. Access controls on repositories *Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.*	Telia Server Certificate CPS 2.4	Compliant with BR 2.4
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	Telia Server Certificate CPS 3.2	Compliant with BR 3.2.2.1 NOTE: Telia CA verifies the identity and address of Applicant using governmental or private database that has been validated to be a reliable data source.
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	Telia Server Certificate CPS 3.2	Compliant with BR 3.2.2.2 NOTE: Telia CA verifies the DBA or tradename of Applicant using governmental or private database that has been validated to be a reliable data source.
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, indicate how your CP/CPS meets the requirements in this section of the BRs.	Telia Server Certificate CPS 3.2	Compliant with BR 3.2.2.3 Telia currently approves only FI, SE, NO, DK, LT, and EE in the country field. Telia use their governmental registers when validating Applicant identity. If any of the customers of the above countries has branches in other non-listed countries we will validate their requests since they have the headquarter office registered in one of the above 6 countries.

3.2.2.4 Validation of Domain Authorization or Control *Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS.* ***Section 2.2 of Mozilla's Root Store Policy states: "For a certificate capable of being used for SSL-enabled servers, the CA must ensure that the applicant has registered all domain(s) referenced in the certificate or has been authorized by the domain registrant to act on their behalf. This must be done using one or more of the methods documented in section 3.2.2.4 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.4 it is complying with. CAs are not permitted to use 3.2.2.5 (4) ("any other method") to fulfill the requirements of method 3.2.2.4.8 (IP Address)."***	Telia Server Certificate CPS 3.2	Compliant with BR 3.2.2.4
3.2.2.4.1 Validating the Applicant as a Domain Contact T**his method SHALL NOT be used.**	Telia Server Certificate CPS 3.2.2.4.1	Compliant with BR 3.2.2.4.1 NOTE: This method is no more used after 2018-08-01 and all domains using this method are revalidated using some other method listed here.
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Telia Server Certificate CPS 3.2.2.4.2	Compliant with BR 3.2.2.4.2 NOTE: Telia CA sends email message to address found at registrant section in Domain register to verify if the applicant has the right to use the domain.
3.2.2.4.3 Phone Contact with Domain Contact **This method has been replaced by 3.2.2.4.15 and SHALL NOT be used. (Validations completed as of 31-May-2019 may be used until 20-August-2021.)**	Telia Server Certificate CPS 3.2.2.4.3	Compliant with BR 3.2.2.4.3 NOTE: Telia CA does not use this method.
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Telia Server Certificate CPS 3.2.2.4.4	Compliant with BR 3.2.2.4.4 NOTE: Telia sends a constructed email message to 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as local part of email recipient address to verify if the applicant has the right to use the domain.
3.2.2.4.5 Domain Authorization Document "T**his method SHALL NOT be used**."	Telia Server Certificate CPS 3.2.2.4.5	Compliant with BR 3.2.2.4.5 NOTE: Telia CA does not use this method.
3.2.2.4.6 Agreed Upon Change to Website Replaced with BR section 3.2.2.4.18 (effective 3/3/2020)	Telia Server Certificate CPS 3.2.2.4.7	Compliant with BR 3.2.2.4.6 NOTE: Telia CA does not use this method.
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Telia Server Certificate CPS 3.2.2.4.7	Compliant with BR 3.2.2.4.7 NOTE: A Random Value is used in DNS system TXT value of domain being validated. The Random Value is generated by Telia CA and is not valid for more than 30 days.
3.2.2.4.8 IP Address If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Telia Server Certificate CPS 3.2.2.4.8	Compliant with BR 3.2.2.4.8 NOTE: Telia CA may confirm the Applicant's control over FQDN by using IP address related to FQDN and IP validation methods.
3.2.2.4.9 Test Certificate **"This method SHALL NOT be used."**	Telia Server Certificate CPS 3.2.2.4.9	Compliant with BR 3.2.2.4.9 NOTE: Telia CA does not use this method.

3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* *This subsection contains major vulnerabilities.* ***If the CA uses this method, then the CA should describe how they are mitigating those vulnerabilities. If not using this method, the CPS should say so.***	Telia Server Certificate CPS 3.2.2.4.10	Compliant with BR 3.2.2.4.10 NOTE: Telia CA does not use this method.
3.2.2.4.11 Any Other Method **"This method SHALL NOT be used."**	Telia Server Certificate CPS 3.2.2.4.11	Compliant with BR 3.2.2.4.11 NOTE: Telia CA does not use this method.
3.2.2.4.12 Validating Applicant as a Domain Contact "This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name." If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs* .	Telia Server Certificate CPS 3.2.2.4.12	Compliant with BR 3.2.2.4.12 NOTE: Used only in special circumstances and such usage must be authorized by supervising Telia Validation Board.
3.2.2.4.13 Email to DNS CAA Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Telia Server Certificate CPS 3.2.2.4.13	Compliant with BR 3.2.2.4.13 NOTE: Used only in special circumstances and such usage must be authorized by supervising Telia Validation Board.
3.2.2.4.14 Email to DNS TXT Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Telia Server Certificate CPS 3.2.2.4.14	Compliant with BR 3.2.2.4.14 NOTE: Used only in special circumstances and such usage must be authorized by supervising Telia Validation Board.
3.2.2.4.15 Phone Contact with Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Telia Server Certificate CPS 3.2.2.4.15	Compliant with BR 3.2.2.4.15 NOTE: Telia CA may use phone number from Registrant section of Domain Name Register to check if the Applicant has the right to use the domain. In the event that someone other than a Domain Contact is reached, the CA will request to be transferred to the Domain Contact.
3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Telia Server Certificate CPS 3.2.2.4.16	Compliant with BR 3.2.2.4.16 NOTE: Used only in special circumstances and such usage must be authorized by supervising Telia Validation Board.
3.2.2.4.17 Phone Contact with DNS CAA Phone Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	Not Applicable	Telia CA does not use this method.
3.2.2.4.18 Agreed-Upon Change to Website v2 If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Telia Server Certificate CPS 3.2.2.4.18	Compliant with BR 3.2.2.4.18 NOTE: A Random Value is used in the content of a file or on a webpage in the form of a meta tag, the file or webpage being accessed via the URL HTTP[S]://<Authorization Domain>/.well-known/pki-validation/file_name over port 80 (HTTP) or 443 (HTTPS).The Random Value is generated by Telia CA and remains valid for use for no more than 30 days from its generation.
3.2.2.4.19 Agreed-Upon Change to Website - ACME If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	Telia Server Certificate CPS 3.2.2.4.19	Compliant with BR 3.2.2.4.19 and according to RFC 8555

3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, ***indicate which methods your CA uses*** *and how your CA meets the requirements in this section of the BRs.* **Section 2.2 of Mozilla's root store policy says: "the CA must ensure that the applicant has control over all IP Address(es) referenced in the certificate. This must be done using one or more of the methods documented in section 3.2.2.5 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.5 it is complying with."**	Page 23 Telia Server Certificate CPS: **Authentication for an IP Address** Method 3.2.2.5.4, Any Other Method, SHALL NOT be used. "After July 31, 2019, CAs SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address."	Compliant with BR 3.2.2.5
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS ID, then *indicate how your CA meets the requirements in this seciton of the BRs.*	Table in Telia Server Certificate CPS 3.1.1	Compliant with BR 3.2.2.6 NOTE: Telia CA performs validation methods 3.2.2.4.2 .4 .7 .8 .15 .18 .19 with wildcard requests.
3.2.2.7 Data Source Accuracy *Indicate how your CA meets the requirements in this section of the BRs.*	Telia Server Certificate CPS 3.2.2	Compliant with BR 3.2.2.7 NOTE: Telia CA ensures the realiability, integrity and authenticity of the data sources.
3.2.2.8 CAs MUST check and process CAA records *Indicate how your CA meets the requirements in this section of the BRs.* *Section 2.2 of the BRs states: "**CA's Certificate Policy and/or Certification Practice Statement ... shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue."***	Telia Server Certificate CPS 4.2.4	Compliant with BR 3.2.2.8
3.2.3. Authentication of Individual Identity	Telia Server Certificate CPS 3.2.3; Telia Organizational User CPS 3.2.3	Compliant with BR 3.2.3 NOTE: Telia CA does not issue SSL certificates for natural persons.
3.2.5. Validation of Authority	Telia Server Certificate CPS 3.2.5	Compliant with BR 3.2.5 NOTE: Authority of Customer is done by calling the contact person via the Customer's PBX number or by making a call to some other verified number in the organization. Phone number or other trusted communication method is verified from a directory maintained by a trusted party. Or If Customer has been previously validated he/she/host can use Telia system credentials which are automatically tied to his/her privileges (authority).
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	Telia Server Certificate CPS 3.2.6	Compliant with BR 3.2.6 NOTE: The only cross-certificate used by Telia is "TeliaSonera Root CA v1" as disclosed in section 2 of this self-assessment (see Root CA info).
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	Telia Server Certificate CPS 4.1.1	Compliant with BR 4.1.1 NOTE: Telia CA will issue server certificates only to organizations that are registered in the European Economic Area. The European Economic Area (EEA) comprises the countries of the European Union (EU), plus Iceland, Liechtenstein and Norway. Telia CA will check EU black listing of persons and companies before authorizing any new persons or companies.

4.1.2. Enrollment Process and Responsibilities	Telia Server Certificate CPS 4.1.2	Compliant with BR 4.1.2 NOTE: There are two different processes: a) any person can fill an application on Telia's public web page b) Pre-verified Customers may use Telia's self-service tool to create their own certificates. Telia CA verifies each application or tool delivery manually using BR rules. In both process Customer must accept Telia CA Customer responsibilities (https://support.partnergate.sonera.com/download/CA/CA_Customers_Responsibilities_en.pdf)
4.2. Certificate application processing BR section 2.2 says that section 4.2 of the CP/CPS SHALL state the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names.	Telia Server Certificate CPS 4.2	Compliant with BR 4.2
4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.* **Re-use of validation information is limited to 825 days**	Telia Server Certificate CPS 4.2.1	Compliant with BR 4.2.1
4.2.2. Approval or Rejection of Certificate Applications "CAs SHALL NOT issue certificates containing Internal Names."	Telia Server Certificate CPS 4.2.2	Compliant with BR 4.2.2 NOTE: Telia CA does not issue certificates containing internal names because domain validation as described in CPS 4.2 prevents such certificates.
4.3.1. CA Actions during Certificate Issuance	Telia Server Certificate CPS 4.3.1	Compliant with BR 4.3.1 NOTE: The certificate is created by the CA according to the information contained in the certificate request and configured for the Customer. However, the CA may overwrite or delete some certificate information using pre-defined certificate profile specific standard values.
4.9.1.1 Reasons for Revoking a Subscriber Certificate *Indicate how your CA's CP/CPS lists the reasons for revoking end entity certificates and is consistent with the timeframes required by this section of the BRs.*	Telia Server Certificate CPS 4.9.1; Telia Organizational User CPS 4.9.1	Compliant with BR 4.9.1.1
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate *Indicate how your CA's CP/CPS lists the reasons for revoking subordinate CA certificates and is consistent with the timeframes required by this section of the BRs.*	Telia Root CPS 4.9.1	Compliant with BR 4.9.1.2
4.9.2. Who Can Request Revocation	Telia Server Certificate CPS 4.9.2; Telia Organizational User CPS 4.9.2	Compliant with BR 4.9.2
4.9.3. Procedure for Revocation Request **The CA SHALL publicly disclose the instructions through a readily accessible online means and in section 1.5.2 of their CPS.**	Telia Server Certificate CPS 4.9.3	Compliant with BR 4.9.3 NOTE: Subscriber or Applicant may contact Telia Revocation Service by telephone or use a URL (details in Telia Server Certificate CPS 1.5.2). Self-service may be used by Subscribers if they have been pre-validated. Revocation of certifcates using ACME is also available.
4.9.5. Time within which CA Must Process the Revocation Request	Telia Server Certificate CPS 4.9.5	Compliant with BR 4.9.5 NOTE: Telia will handle revocation requests within 24 hours.
4.9.7. CRL Issuance Frequency *Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.*	Telia Server Certificate CPS 4.9.7	Compliant with BR 4.9.7 NOTE: Telia CA will issue normal CRLs at least with frequency of 48 hours. Offline-CRLs are issued at least with frequency of 12 months.
4.9.9. On-line Revocation/Status Checking Availability	Telia Server Certificate CPS 4.9.9	Compliant with BR 4.9.9 NOTE: Telia CA provides on-line revocation status checking via the OCSP protocol.

4.9.10. On-line Revocation Checking Requirements *Indicate how your CA meets all of the requirements listed in this section,* ***including support of GET, update frequency, preventing errounious return of "good" status.***	Telia Server Certificate CPS 4.9.10	Compliant with BR 4.9.10 NOTE: The OCSP responder may use the previous status value for a certificate if it is fresher than two hours old (refresh time). In rare circumstances where the connection between OCSP and CA is broken the status information may be up to 48 hours old (grace period). OCSP responder will respond with an "unknown" status for certificates that do not exist in the CA database. The Telia OCSP responder supports requests sent using HTTP GET or POST. Data in subordinate CA OCSP service is updated at least every twelve months or within 24 hours if subordidate CA is revoked.
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	Not Applicable	Compliant with BR 4.9.11 NOTE: Telia CA does not use this method.
4.10.1. Operational Characteristics	Telia Server Certificate CPS 4.10.1	Compliant with BR 4.10.1 NOTE: Telia CA keeps the CRL information until the certificate is valid.
4.10.2. Service Availability	Telia Server Certificate CPS 4.10.2	Compliant with BR 4.10.2
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS	Telia Production CPS 5	Compliant with BR 5
5.2.2. Number of Individuals Required per Task	Telia Production CPS 5.2.2	Compliant with BR 5.2.2 NOTE: CA private key related operations are done only in physically secured place and when at least two trusted persons from Telia CA are on site.
5.3.1. Qualifications, Experience, and Clearance Requirements	Telia Production CPS 5.3.1	Compliant with BR 5.3.1
5.3.3. Training Requirements and Procedures	Telia Production CPS 5.3.3	Compliant with BR 5.3.3
5.3.4. Retraining Frequency and Requirements	Telia Production CPS 5.3.4	Compliant with BR 5.3.4
5.3.7. Independent Contractor Controls	Telia Production CPS 5.3.7	Compliant with BR 5.3.7 Delegated third parties are not currently utilized except in product development.
5.4.1. Types of Events Recorded *Indicate how your CA meets the requirements of this section*	Telia Production CPS 5.4.1	Compliant with BR 5.4.1
5.4.3. Retention Period for Audit Logs	Telia Production CPS 5.4.3	Compliant with BR 5.4.3 NOTE: PKI audit logs are currently archived for at least ten years
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*	Telia Production CPS 5.4.8	Compliant with BR 5.4.8 NOTE: Telia CA has qualified third party assessments performed at least annually or when a major revision of software has been done and Telia CA has a continuing automated
5.5.2. Retention Period for Archive	Telia Production CPS 5.5.2	Compliant with BR 5.5.2 NOTE: Archive data related to enrollment, verification and revocation is currently stored for at least 10 years.
5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*	Telia Production CPS 5.7.1	Compliant with BR 5.7.1 NOTE: Telia has incident and disaster recovery plans. CA test, review and update these annually.
6.1.1. Key Pair Generation	Telia Production CPS 6.1.1	Compliant with BR 6.1.1 NOTE: CA key pair generation related to publicly trusted CAs is done only in a physically protected "CA Vault" and at least two trusted persons are required to be pesent. All BR requirements are followed. Subscriber keys are generated by Subscriber but Telia CA will verify that key quality follow BR requirements.
6.1.2. Private Key Delivery to Subscriber	Not Applicable	Compliant with BR 6.1.2 NOTE: Private keys are generated by the Subscriber.
6.1.5. Key Sizes	Telia Production CPS 6.1.5	Compliant with BR 6.1.5 NOTE: The CA requires that the Subscribers generate at least 2048 bit RSA keys or ECC curve NIST P256 and P384 keys. CA RSA keys must be 4096 bits.
6.1.6. Public Key Parameters Generation and Quality Checking	Telia Production CPS 6.1.6	Compliant with BR 6.1.6 CA verifies that the value of the RSA public exponent is an odd number equal to 3 or more. A warning is given if it's not in the range between 2^16+1 and 2^256 1.
6.1.7. Key Usage Purposes	Telia Production CPS 6.1.7	Compliant with BR 6.1.7 NOTE: Telia CA keys may be used to sign SubCA certificates, CRL lists or OCSP responder certificates. Subscriber keys may use other key purposes except keyCertSign and crlSign.

6.2. Private Key Protection and Cryptographic Module Engineering Controls	Telia Production CPS 6.2	Compliant with BR 6.2 NOTE: CA private keys are always protected by HSM and its mechanisms. A combination of physical, logical and procedural controls protect them.
6.2.5. Private Key Archival	Telia Production CPS 6.2.5	Compliant with BR 6.2.5 NOTE: CA private keys are archived in encrypted format offline devices stored in physically protected places so that only Telia Trusted persons have access to them. Details of private key archival are classified information.
6.2.6. Private Key Transfer into or from a Cryptographic Module	Not Applicable	Compliant with BR 6.2.6 MOTE: Private keys are generated by the subordinate CA.
6.2.7. Private Key Storage on Cryptographic Module	Telia Production CPS 6.2.7	Compliant with BR 6.2.7 NOTE: CA private keys are protected according to FIPS 140-2 level3 on HSM device.
6.3.2 Certificates issued after March 1, 2018, MUST have a Validity Period no greater than 825 days *Indicate how your CA meets the requirements of this section.*	Telia Production CPS 6.3.2	Compliant with BR 6.3.2 NOTE: Maximum validity period currently SSL certificates is 397 days.
6.5.1. Specific Computer Security Technical Requirements **The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.** *Indicate how your CA meets the requirements of this section.*	Telia Production CPS 6.5.1	Compliant with BR 6.5.1 NOTE: Telia requires SSL admins to use client certificate or SMS one-time-password combined to password/PIN . When Security Zone boundary is crossed, a multi-factor authentication is required. All Trusted Roles accounts use multi-factor SMS OTP or SecurID authentication.
7.1. Certificate profile **CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG.** *Indicate how your CA meets the requirements of this section.*	Telia Server Certificate CPS 7.1	Compliant with BR 7.1
7.1.1. Version Number(s)	Telia Server Certificate CPS 7.1.1	Compliant with BR 7.1.1
7.1.2. Certificate Content and Extensions; Application of RFC 5280	Telia Server Certificate CPS 7.1.2	Compliant with BR 7.1.2
7.1.2.1 Root CA Certificate	Telia Root CPS 7.1	Compliant with BR 7.1.2.1
7.1.2.2 Subordinate CA Certificate	Telia Root CPS 7.1	Compliant with BR 7.1.2.2
7.1.2.3 Subscriber Certificate	Telia Server Certificate CPS 7.1; Telia Organizational User CPS 7.1	Compliant with BR 7.1.2.3
7.1.2.4 All Certificates	Telia Server Certificate CPS 7.1.2	Compliant with BR 7.1.2.4
7.1.2.5 Application of RFC 5280	Telia Server Certificate CPS 7.1.2	Compliant with BR 7.1.2.5
7.1.3. Algorithm Object Identifiers	Telia Server Certificate CPS 7.1.3	Compliant with BR 7.1.3
7.1.4. Name Forms	Telia Server Certificate CPS 7.1.4	Compliant with BR 7.1.4
7.1.4.1 Issuer Information	Telia Server Certificate CPS 7.1, table row "Issuer"	Compliant with BR 7.1.4.1 NOTE: Every DN will be in the form of an X.501 DirectoryString and Issuer DN is same than Subject DN of the Issuing CA in certificates.
7.1.4.2 Subject Information - Subscriber Certificates	Telia Server Certificate CPS 3.1.1	Compliant with BR 7.1.4.2

7.1.4.2.1 Subject Alternative Name Extension **This extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. Wildcard FQDNs are permitted.** **CAs SHALL NOT issue certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.** **Entries in the dNSName MUST be in the "preferred name syntax", as specified in RFC 5280, and thus MUST NOT contain underscore characters ("_").**	Telia Server Certificate CPS 3.1.1, 3.2.2.4.8 and 7.1.2	Compliant with BR 7.1.4.2.1 NOTE: Telia CA will not issue certificates with underscore in the DNS field and following the BR. If there is underscore in the request we will reject the CSR.
7.1.4.2.2 Subject Distinguished Name Fields If present, this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.4.2.1).	Telia Server Certificate CPS 3.1.1	Compliant with BR 7.1.4.2.2
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates	Telia Root CPS 7.1, table row "Subject"	Compliant with BR 7.1.4.3
7.1.5. Name Constraints ***Indicate your CA's understanding of section 5.3 of Mozilla's root store policy, and requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section of the BRs.*** ***"All certificates that are capable of being used to issue new certificates, that are not technically constrained, and that directly or transitively chain to a certificate included in Mozilla's root program:*** ***MUST be audited in accordance with Mozilla's Root Store Policy. ...*** ***MUST be publicly disclosed in the CCADB by the CA that has their certificate included in Mozilla's root program. The CA with a certificate included in Mozilla's root program MUST disclose this information within a week of certificate creation, and before any such subordinate CA is allowed to issue certificates. ..."***	Telia Server Certificate CPS 7.1.5	Compliant with BR 7.1.5 and Mozilla's root store policy 5.3
7.1.6. Certificate Policy Object Identifier	Telia Server Certificate CPS 7.1.6	Compliant with BR 7.1.6
7.1.6.1 Reserved Certificate Policy Identifiers	Telia Server Certificate CPS 1.1	Compliant with BR 7.1.6.1 NOTE: Telia CA is using reserved BR OID values for SSL certifictes. For client certificates, internal Telia CA OIDs are used.
7.1.6.2 Root CA Certificates	Telia Root CPS 1.2	Compliant with BR 7.1.6.2
7.1.6.3 Subordinate CA Certificates	Telia Root CPS 1.2	Compliant with BR 7.1.6.3
7.1.6.4 Subscriber Certificates	Telia Server Certificate CPS 1.2; Telia Organizational User CPS 1.2	Compliant with BR 7.1.6.4 NOTE: Telia subscriber SSL certificates use reserved BR OID values. Telia subscriber client certificates use Telia OID values
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	Telia Server Certificate CPS 1.1 and 8	Compliant with BR 8 NOTE: Telia CA is compliant with relevant laws, BR and audit requirements

8.1. Frequency or circumstances of assessment **The period during which the CA issues Certificates SHALL be dividied into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.** For new CA Certificates: The point-in-time readiness assessment SHAL be completed no earlier than twelve months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate. *Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.*	Telia Server Certificate CPS 8.1	Compliant with BR 8.1 NOTE: An annual Compliance Audit will be performed by an independent, qualified third party covering all Telia's publicly trusted certificates
8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*	Telia Server Certificate CPS 8.2	Compliant with BR 8.2
8.4. Topics covered by assessment	Telia Server Certificate CPS 8.4	Compliant with BR 8.4 NOTE: WebTrust 2.2 and Network Security v2.4 are used for the assessment.
8.6. Communication of results	Telia Server Certificate CPS 8.6	Compliant with BR 8.6
Also indicate your understanding and compliance with section 3 of Mozilla's Root Store Policy, which says: "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps). **....** **The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information:** **- name of the company being audited;** **- name and address of the organization performing the audit;** **- Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope;** **- audit criteria (with version number) that were used to audit each of the certificates;** **- a list of the CA policy documents (with version numbers) referenced during the audit;** **- whether the audit is for a period of time or a point in time;** **- the start date and end date of the period, for those that cover a period of time;**	Telia Server Certificate CPS 8.6	Compliant with BR 8.6
8.7. Self-Audits	Telia Server CPS 8.7	Compliant with BR 8.7
9.6.1. CA Representations and Warranties	Telia Production CPS 9.6.1	Compliant with BR 9.6.1 NOTE: Telia CA will operate in accordance with this CPS and each CPS referring to Production CPS, when issuing and managing certificates.
9.6.3. Subscriber Representations and Warranties	Telia Production CPS 9.6.3	Compliant with BR 9.6.3 NOTE: Telia CA will require that Subscribers comply with all the relevant provisions of this CPS and applicable CPS referring to Production CPS. Subscriber Agreement or Terms of Use accepted by all subscribers is this: https://support.partnergate.sonera.com/download/CA/CA_Customers_Responsibilities_en.pdf. Certificate portal users also must accept Telia CA terms before using the portal.

9.8. Limitations of liability	Telia Production CPS 9.8	Compliant with BR 9.8 NOTE: Telia CA assumes no liability except as stated in the relevant Customer contracts pertaining to certificate issuance and management. Telia is not using Delegated third parties.
9.9.1. Indemnification by CAs	Telia Production CPS 9.9	Compliant with BR 9.9.1 NOTE: Telia SSL certificates conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at https://cabforum.org
9.16.3. Severability	Telia Server Certificate CPS 1.1	Compliant with BR 9.16.3 NOTE: Telia SSL certificates conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at https://cabforum.org
APPENDIX A - RFC 6844 ERRATA 5065 To prevent resource exhaustion attacks, CAs SHOULD limit the length of CNAME chains that are accepted. However CAs MUST process CNAME chains that contain 8 or fewer CNAME records.	Telia Server Certificate CPS 4.2.4	Compliant with Appendix A NOTE: CNAME of 8 levels in the chain are supported.
APPENDIX B – DNS CONTACT PROPERTIES These methods allow domain owners to publish contact information in DNS for	Not Applicable	These methods are not used currently at Telia CA.