1. OVERVIEW

This document describes an agreement between Telia Finland Oyj, a Helsinki based company (“Telia Certification Authority (CA)”), and the Applicant/Subscriber (“Subscriber”), and it specifies the rights and responsibilities of the parties (“Subscriber Agreement”). It also describes provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the Telia or is the CA (Terms of Use).

Telia Group Security Policy and Telia´s general delivery terms[1] apply to this document.

Certificates issued by Telia CA are utilized in connection with several security services offered by Telia or other parties. This Agreement includes the obligations and responsibilities for the users trusting, using or registration Telia certificates.

2. DEFINITIONS

Affiliate	A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
Certification Authority (CA)	CA is an entity such as Telia that is authorized to create, sign, distribute, and revoke certificates. CA is also responsible for distributing certificate status information and providing a repository where certificates and certificate status information is stored.
CA/Browser Forum	A group of representatives from certificate authorities and browser vendors to discuss issues surrounding the existing market for server certificates, e.g., certificates used in authenticating TLS-enabled web sites and other servers (e.g., mail servers) to users.
Certificate	An electronic document issued by Telia to a person or entity mainly for verifying the identity of the sender/receiver of an electronic message, and/or for providing the means to encrypt/decrypt messages between sender and receiver (e.g., binding an entity to their public key).
Certificate Request	A process where a natural person (the Subscriber or someone employed by the Subscriber) or an authorized agent with the authority of representing the Subscriber that completes and submits a certificate requestion.
Client Certificate	A digital certificate in which information about the organization and email of holding the certificate has been validated by Telia.
Certificate Practice Statement (CPS)	CPS is a document that defines the legal, commercial and technical practices for approving, issuing, using and managing Telia Server and Client certificates. It also outlines the roles and responsibilities of the parties involved in maintaining the Telia public key infrastructure.
Digital Signature	A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.
Domain name	The label assigned to a node in the Domain Name System.

[1] Delivery terms for business customers: https://www.telia.fi/dam/jcr:5f8ae50b-f587-4829-8499-c07028580d8b/Telias%20General%20Delivery%20Terms%20for%20Business%20Customers%20Concerning%20Services.pdf

Domain Validated (DV) TLS Server Certificate	A digital certificate for a web site or other server in which the information about the domain name has been validated by Telia.
Registration Authority (RA)	An employee or agent of an organization unaffiliated with Telia who authorizes issuance of certificates to that organization.
Fully Qualified Domain Name (FQDN)	A domain name that specifies its exact location in the tree hierarchy of the Domain Name System.
OV TLS Server Certificate	A digital certificate in which information about the business entity holding the certificate has been validated by Telia.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Relying Party	Anybody who relies on the certificates issued by Telia (including all end users and operating system vendors who trust Telia certificates).
Repository	An online database containing publicly-disclosed Telia PKI governance documents, and certificate status information, either in the form of a Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) response. https://cps.trust.telia.com.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Service Element	The CA internal systems, processes or services such as certificate enrolment, PKI support, backup and system monitoring.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subscriber	A person or entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement and Terms of Use.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the CABF requirements when the Applicant/Subscriber is an Affiliate of the Telia CA or is the CA.

3. SERVICES

3.1 Certificate Types. The following certificate types ("Services") are offered by Telia: (i) **Telia TLS DV certificate:** to authenticate servers and establishing secure Transport Layer Security (TLS) sessions with end clients. In this type the server domain name is validated by Telia, (ii) **Telia TLS OV certificate:** to authenticate servers and establishing secure TLS sessions with end clients. In this type domain name of the server, existence of the organisation and other attributes including name, type, status, and physical address is validated by Telia, (iii) **Telia client certificate**: for identifying individual users, securing email communications and document signing, or (iv) **Telia**

document signing (Seal) certificate: for authenticating documents from Adobe PDF, OpenOffice, Microsoft Office and LibreOffice.

3.2 Certificate Request. In order for Subscriber to obtain a Certificate, the Subscriber shall submit a certificate request in a form specified by Telia for each ordered Certificate ("Certificate Request"). Forms for a Certificate Request are available on Telia CA's website and may be completed electronically.

3.3 Validation. Upon Telia's acceptance of Subscriber's Certificate Request, Telia validate the information provided in accordance with the applicable CPS. If Telia validate the Subscriber successfully, Telia issue the Certificate(s) to Subscriber. Telia may reject a Certificate Request and refuse to issue any ordered Certificate in its sole discretion.

3.4 Revocation. Telia may revoke a Certificate if Telia believes or has reason to believe that:

a) Subscriber requests a certificate revocation;
b) Telia CA obtains evidence that the certificate was misused;
c) Telia CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
d) Telia CA is made aware of any circumstance indicating that use of a FQDN or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
e) Telia CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
f) Telia CA is made aware of a material change in the information contained in the certificate;
g) Telia CA is made aware that the certificate was not issued in accordance with the Baseline Requirements or the applicable CSP;
h) Telia CA determines or is made aware that any of the information appearing in the certificate is inaccurate;
i) Telia CA's right to issue certificates under the Baseline Requirements expires or is revoked or terminated, unless Telia CA has made arrangements to continue maintaining the CRL/OCSP Repository;
j) Revocation is required by Telia CA' applicable CPS; or
k) Telia CA is made aware of a demonstrated or proven method that exposes the Subscriber's private key to compromise, methods have been developed that can easily calculate it based on the public key, or if there is clear evidence that the specific method used to generate the private key was flawed.

After revoking a Certificate, Telia may, in its sole discretion, reissue the Certificate to Subscriber and/or terminate this Agreement.

4. SUBSCRIBER OBLIGATIONS

This chapter describes shortly the obligations and warranties for all the CA certificate subscribers and holders. This Agreement shall remain in effect until the Certificate has expired or is earlier revoked.

4.1 Acceptance of Certificate. The Subscriber is considered to have accepted the certificate when: (a) subscriber use of the certificate's key pair, or (b) one calendar month is passed from the certificate issuance date.

4.2 Retention. The information provided by the subscriber for certificate validation, and copies of certificates regardless of their status will be retained no less than 8 years. The retention date shall start from the rejection, revocation or expiration date of the certificates.

4.3 Accuracy of Information. The subscriber is obliged to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s).

4.4 Protection of Private Key. The subscriber is obliged to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token).

If a cryptographic device is used the Subscriber shall only use the Subject's Private Key(s) for cryptographic functions within the secure cryptographic device. If the Subject's keys are generated under control of the Subscriber or Subject: an obligation to generate the Subject's keys within the secure cryptographic device.

4.5 Use of Certificate. The subscriber is obliged to install the Certificate only on servers, domains, or devices that are controlled or owned by at the subjectAltName(s) listed in the Certificate or are otherwise applicable, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with these Subscriber Agreement requirements

4.6 Reporting and Revocation. The subscriber is obliged to promptly cease using a Certificate and its associated Private Key, and promptly request Customer’s Registration Officer or the CA to revoke the Certificate, in the event that: (a) any essential information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber’s Private Key associated with the public Key included in the Certificate.

Subscriber is hereby informed, and acknowledges understanding, of the reasons for revoking a Certificate, including those stated in section 4.9 of the Telia CA Server Certificate CPS, which is incorporated herein by reference and made a part of this Agreement.

4.7 Termination of Use of Certificate. The subscriber is obliged to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

4.8 Responsiveness. The subscriber is obliged to respond to the CA’s instructions concerning Key Compromise or Certificate misuse within reasonable time.

4.9 Acknowledgment and Acceptance. The subscriber is obliged to acknowledge and accept that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of this document.

5. FEES

Subscriber pays Telia for a service and its use pursuant to a price-list or agreement according to invoicing periods defined by Telia. If Subscriber revokes Certificate(s) or requests a revocation to be done by Telia, then the purchase fee will be cancelled and Subscriber is not required to pay the Certificate invoice.

6. INTELLECTUAL PROPERTY RIGHTS

Telia retains, and Subscriber will not obtain or claim, any title, interest, or ownership rights in any services, including all software associated with the Services, or techniques and ideas embedded therein; all copies or derivative works of such products or services or software provided by Telia, regardless of who produced, requested, or suggested the copy or derivative work; all documentation and marketing material provided by Telia to Subscriber; and all of Telia's copyrights, patent rights, trade secret rights and other proprietary rights.

7. CONFIDENTIALITY

All Subscriber's information that is collected, generated, transmitted or maintained by the issuer is classified in accordance with the Telia's Group Security Policy.

Information published in the Repository such as public certificates or certificate revocation information are not considered as confidential.

8. WARRANTIES

8.1 Mutual warranties. Each party warrants that it has full power and authority to enter into and perform its obligations under the Agreement which, when agreed, will constitute binding obligations on the warranting party.

8.2 Usage. Telia CA makes no representation concerning the quality of the Services and does not promise that the Services will: (a) meet the Subscriber's requirements or be suitable for a particular purpose, including that the use of the Services will fulfil or meet any statutory role or responsibility of the Subscriber; or (b) The provided Services will be error free.

9. LIABILITIES AND INDEMNITIES

9.1 Liabilities. Telia CA accepts no liability for damages incurred by a relying party accepting one of its certificates, or by a Subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party. It also accepts no liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with the applicable CPS.

9.2 Indemnities. Telia CA will not pay indemnities for damages arising from the use or rejection of certificates it issues. Subscribers shall indemnify and hold harmless the Telia CA and all appropriate RAs operating under the applicable CPS against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate which violates the provisions of the applicable CPS.

10. TERMS AND TERMINATION

10.1 Term. Unless otherwise terminated as allowed herein, this Agreement is effective upon Subscriber's acceptance and lasts for as long as a Certificate issued under this Agreement is valid.

10.2 Termination. Services can be terminated individually according to the Subscriber's needs, during the agreement period, if the termination does not essentially affect the quality and scope of Services according to the Agreement. Individual Service Elements should be terminated in writing. The Subscriber receives a written confirmation of the termination and, if needed, the appendix documents of the amended service agreement which refer to the termination. The invoicing will continue until the end of the month when the termination was notified.

11. PRIVACY CONSIDERATIONS

Telia does not collect any sensitive or confidential data from Subscriber. Except in scenarios where the CA or RA archive copies of identification documents to validate the identity of a Subscriber. The collected personal information will not be used for any other purpose and Telia's privacy policy[2] governs the CA operations. Telia's Privacy Notice applies to all processing of personal data[3].

12. DISPUTES

12.1 Good faith negotiations. Before taking any Court action, a party must use best efforts to resolve any dispute under through good faith negotiations.

12.2 Legal actions. Any disputes arising from or relating to this Agreement shall be finally settled by arbitration in accordance with the Arbitration Rules of the Finland Chamber of Commerce. The number of arbitrators shall be one, unless the other party requires that the arbitral tribunal be composed of three members. The place of arbitration is Helsinki, Finland, and the language of the arbitration is Finnish. Without prejudice to the above, the parties have the right to bring a legal action at the Helsinki District Court when the value of the dispute does not exceed one hundred thousand (100,000) Euros.

12.3 Obligations continue. Each party must, to the extent possible, continue to perform

[2] Telia Group Policy - Privacy and Data Protection: https://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/public-policy/group-policy---privacy-and-data-protection.pdf

[3] Telia Privacy Notice: https://www.telia.fi/tietosuoja-ja-tietoturva/privacy-notice

its obligations under the Agreement even if there is a dispute.

12.4 Right to seek relief. This clause 12 does not affect either party's right to seek urgent interlocutory and/or injunctive relief.

13. MISCELLANEOUS

13.1 Amendments. Subscribers will not be notified if the applicable CPS document is changed. When changes are made, they will be published in the Repository for public review and after 15 days will be in effect. Changes to the Telia Group Security Policy will be communicated to third parties, where applicable. Changes to this Agreement that affects each parties' obligations will be communicated to the Subscribers.

13.2 Law. The Agreement is governed by, and must be interpreted in accordance with, the laws of Finland without regard to the conflict of law provisions.

13.3 Security. Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the CA will also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

14. CONSENT

Acknowledgement to the terms and conditions set forth in this Agreement by the Subscriber shall be witnessed in either of the following means:

14.1 By embedding this Agreement by reference in mutual agreement with Telia Company or Telia Company's subsidiaries and the Subscriber governing Telia Certificate Services.

14.2 By selecting the checkbox "I agree" you acknowledge that you have read and understand this agreement and that you will comply with all the items stated in the Terms and Conditions. This includes your consent to the CA to make the Certificate available for the Relying Parties when necessary. If you do not agree to the terms of this Agreement do not press the "I agree" button and do not request, accept, or use Telia Certificates.