

TURINGSIGN (OISTE/WISEKEY) CERTIFICATE SUBSCRIBER AGREEMENT

Upon acknowledgement of this certificate request, you (“certificate subscriber”) agree to the terms and conditions of this agreement and are thereby bound to comply with its provisions from the date of such submission.

1. Scope: This agreement regulates the provision of certification services by WISEKey to Certificate Subscribers and their use of such certification services.

2. Object: The certification services provided by WISEKey shall be undertaken in accordance with the OISTE Foundation and WISEKey Certificate Practices and Policies available at www.wisekey.com/repository/

3. WISEKey Warranty: In providing its Certification Services, WISEKey shall comply with its obligations in accordance with its Certification Practices and Policies. Upon acceptance of a certificate by you, WISEKey warrants to you compliance with such obligations.

4. Outsourced Certification Services: provide part of the certification services, such as:

- The processing of requests for the issuance and revocation of certificates;
- The verification of the identity of certificate applicants;
- The archival of personal data corresponding to the applicants whose certificates have been processed by them in compliance with local Data Protection or Privacy regulations; and cryptographic key pair generation.

TuringSign shall warrant compliance with the WISEKey practices and the policies referred to in clause 2 of this agreement.

5. Certificate Subscriber Acknowledgement: Upon accepting this agreement, you acknowledge that:

- You are aware of WISEKey’s Policies and Practices;
- You have on the use, security precautions, and functionalities of certificates, cryptographic keys, and certification services provided by WISEKey and TuringSign;
- You understand the nature of the services provided by WISEKey and TuringSign;
- You understand the warranties and that limitations on liability and damages apply as is indicated in the WISEKey Policies and Practices, and in this subscriber agreement;
- WISEKey and/or TuringSign may, in their sole and absolute discretion, decide not to process or issue a certificate to you;

- That your certificate may be treated as public information and made available to other parties;
- WISEKey or TuringSign may revoke your certificate if the you so request it or if WISEKey or TuringSign receives information that:
 - o The private key corresponding to the public key in the certificate has been potentially or effectively lost, disclosed without authorization, stolen or compromised in any way.
 - o Inaccuracy or changes to the certificate content, as notified to you;
 - o You do not meet material obligations of your agreements with WISEKey or TuringSign;
 - o A material prerequisite to the issuance of the certificate not being satisfied;
 - o A material fact in the certificate is known, or reasonably believed, to be false.
 - o Any other circumstance that may reasonably be expected to affect the reliability, security or integrity of the certificate or the cryptographic key pair associated with it;
 - o Any other reason for revocation stipulated in WISEKey's CPS or mandated by any applicable regulation such as Root Programs.

In the event that you want to become a “Relying Party”, by accepting this Subscriber Agreement you are implicitly giving consent to the Relying Party Agreement. (Available at <https://www.oiste.org/repository>).

6. Your Obligations and Warranties: Upon applying for the issuance of a certificate, you agree to:

- Provide accurate and complete information in order to process the certificate issuance application;
- Generate or have generated its cryptographic keys in a way that complies with the requirements of the applicable policy;
- Review the certificate issued to it to determine the accuracy of the data contained in it and either accept the certificate or notify WISEKey or TuringSign of any modifications required.
- Upon accepting the certificate issued to you, you warrant that:
 - o The data contained in the certificate is accurate;
 - o You shall only use the cryptographic key pair and certificates in accordance with the applicable Certificate Policy;

- o The private cryptographic key associated with the public key contained in the certificate has not been compromised;
 - o You shall exercise reasonable care to maintain the security of the private cryptographic key associated with the public key contained in the certificate as well as avoid its unauthorized use;
 - o You shall promptly notify WISeKey to revoke the certificate if you suspects or knows that your private key, the device it is stored in, or the PIN/Passphrase has been compromised, lost or its security is in any other way materially affected.
 - o You shall pay the fees for the certification services provided in accordance with the applicable price list.
- You shall accept the potential need to revoke your certificate due to compliance requirements, within the mandated deadlines imposed by the CA/Browser Forum and/or Root Programs. In such case you shall follow the necessary procedures for the revocation of certificates in accordance with applicable practices and policies, and you accept that the CA will not be liable of having to respect those revocation deadlines due to compliance requirements.
- If you request to revoke your certificate, you need to specify the appropriate reason among these options:
 - “Key Compromise”: The certificate subscriber must choose the “key compromise” revocation reason code when they have reason to believe that the private key of their certificate has been compromised, e.g., an unauthorized person has had access to the private key of their certificate.
 - “Affiliation Changed”: The certificate subscriber should choose the “affiliation changed” revocation reason code when their organization’s name or other organizational information in the certificate has changed.
 - “Superseded”: The certificate subscriber should choose the “superseded” revocation reason code when they request a new certificate to replace their existing certificate.
 - “Cessation Of Operation”: The certificate subscriber should choose the “cessation of operation” revocation reason code when they no

longer own all of the domain names in the certificate or when they will no longer be using the certificate because they are discontinuing their website.

- “Privilege Withdrawn”: The CA will specify the “privilege withdrawn” revocation reason code when they obtain evidence that the certificate was misused or the certificate subscriber has violated one or more material obligations under the subscriber agreement or terms of use.

7. Certificate Acceptance: Certificate acceptance by you will occur when any of the following events takes place:

- Acknowledging the certificate request that informs of this agreement in electronic form;
- Upon signing a certificate acceptance form and submitting it to the entity that processed the certificate application;
- Upon payment of the certificate issuance services; or
- Upon your first use of the certificate for purposes other than verifying the content of the certificate and testing its functionality.

(As part of the assessment done by the Certificate Subscriber in order to decide whether to accept it or not).

8. Certificate Subscription Validity Period and Fees: You may engage for a certificate service subscription valid for up to five (5) years, subject to payment of fees in accordance with the schedule provided in the applicable price list. The initial validity period of the certificate issued to you shall be limited to the maximum allowed by the relevant regulations or Root Program. You will be entitled to obtain successive certificates until completion of the subscription period.

9. Liability: The disclaimers and liability clauses contained in the Practices and Policies referred to in Clause 2 of this agreement operate with regards to all claims arising in relation to certificates and certification services provided by WISEKey and TuringSign. If TuringSign and/or WISEKey breaches the warranty, and if you meet the requirements specified in this agreement and are in compliance with this agreement, then the reimbursement cap according to the class of the certificate and the product line is specified in the table below in Swiss Francs:

Class	Product Line	Liability Cap (in CHF)	
		Maximum Aggregate Liability per Certificate	Total Aggregate Liability per Certificate
Personal Certificate	Free / Basic	No liability accepted	No liability accepted
Personal Certificate	Advanced	1,000	10,000
Personal Certificate	Qualified	5,000	50,000
DV SSL	Basic DV	10,000	500,000
DV SSL	DV Wildcard	50,000	1,000,000
OV SSL	Basic OV	100,000	1,250,000
OV SSL	OV Wildcard	250,000	1,750,000
EV SSL	Standard EV	300,000	2,000,000

10. Whereas:

- **“Maximum Liability per Certificate”** is the maximum aggregate per year liability on a single certificate, applicable to a single relying party.
- **“Total Aggregate Liability per Certificate”**. Is the maximum aggregate per year liability on a single certificate, applicable to all End users, Relying Parties and any other entities party that could be affected for that certificate.

- **“Global Liability”**: is the Global aggregate liability limit towards all End users, Relying Parties and any other entities that are not Subordinate PKI Entities for the whole of the validity period of certificates issued by the Root CA (unless revoked or suspended prior to its expiry) towards all persons regarding such certificates. The Global Liability for all damages sustained by all Relying Parties is CHF 5,000,000 in the aggregate as specified in the WISEKey CertifyID Certification Practices Statement (“WISEKey CPS”). WISEKey administers all claims on a first-come, first-serve basis. You may only make one warranty claim related to a transaction regardless of whether you relied on multiple products and services on the same website. If the applicable aggregate limit in the table in this section is met, then you waive WISEKey of any liability for all remaining unreimbursed unauthorized charges.

The foregoing limitations shall apply to any liability whether based in contract, tort (including negligence) or any other theory of liability, including any direct, indirect, special, punitive, exemplary, consequential, reliance, or incidental damages, with the exception of liability due to the possible effects of the revocation of the certificate within the deadlines imposed by the CA/Browser Forum and Root Programs.

11. Data Protection and Privacy: You hereby consent to the WISEKey Privacy Policy and therefore authorize the publication of data you have indicated for inclusion in the certificate you request as well as the relevant certificate status information. Such publication shall take place on the Internet and by any other means WISEKey considers necessary for the purposes of its provision of certification services. You further authorize WISEKey or TuringSign to disclose any relevant information required for any judicial evidence or discovery purposes regarding the reliability and/or legal validity of the certificate or any digital signatures backed by the certificate issued, regardless of whether such certificate is valid, expired, revoked or suspended.

12. Indemnification: You will indemnify and hold the WISEKey, TuringSign, as well as their respective directors, officers, employees, agents and affiliates harmless from any and all liability arising out of the your use of WISEKey Certificates for other than its intended use or in any way that materially breaches its obligations under this Agreement.

13. Electronic Contracting: Upon consenting to this agreement, you agree to the formation and conclusion of contracts, delivery of notifications and communications in general by electronic means (including the signing of this contract and termination notices) with WISEKey for the purposes of the digital certification services. You acknowledge that you are prepared and have the capability and equipment to do so.

14. Termination: This Agreement may be terminated by either party at any time. In the event of termination without cause by you, no refund shall be made for any fees paid. In the event of termination without cause by WISEKey, it will refund you in accordance with its adopted refund policy. Where termination is done by WISEKey with cause (due to breach or other material reasons) no refund shall be paid to you. In all cases, the current contract shall be terminated upon expiration or revocation of the certificate issued to you.

15. Severability: If any section, sentence, clause or phrase of this agreement should be held to be invalid or unconstitutional by a court of competent jurisdiction, such invalidity or unconstitutionality shall not affect the validity or constitutionality of any other section, sentence, clause or phrase of this agreement.

16. Applicable Law: This agreement shall be governed and interpreted in accordance with the laws of Switzerland and the parties consent to the exclusive jurisdiction of the courts of Geneva.

This document has been issued by:

Policy Approval Authority

WISEKey SA (operator of the OISTE Foundation Root CA)

Avenue Louis-Casaï 58

1216 Cointrin – Geneva

Switzerland

Phone: +41 22 594 3000

Email: cps@wisekey.com

Service provided by:

TuringSign Global SA

Unlimitrust Campus

Route des Flumeaux 42-48 1008 PRILLY

Switzerland

Email: sslsupport@turingsign.com