

TuringSign Terms & Conditions

These TuringSign Terms and Conditions ("Terms and Conditions") apply to the products and services, including but not limited to digital certificate ("Certificate") and its related products and services, provided by TuringSign Global SA, a company incorporated in Singapore under the laws of Singapore or any of its affiliates ("TuringSign or "we") to any entity or person ("Customer or "Customers"), as identified by the TuringSign management portal or related API made available to Customer ("Portal") or individually issued digital certificates ("Certificate" or "Certificates") or subscriber and user on TuringSign E-commerce platform or its related websites. These Terms and Conditions apply throughout the entire life cycle of certificate, from the initial activities related to Customer's issuance of Certificate(s) until its expiration and/or revocation date.

Any and all agreements that incorporate these Terms and Conditions (Agreement) accepted or signed shall be considered as having all relevant parties read and understood these Terms and Conditions. If Customers' agent or representative are to access any TuringSign related sites, including but not limited to TuringSign's Website, E-commerce platform, Portal, and CertifyID account, as defined below, on behalf of the Customer, such person or entity is (i) acting as the authorized representative of the Customer to the Agreement in discussion, (ii) has the authority to obtain the company's official stamp, seal or signatures, (iii) can verify the authenticity of the Customer's website, (iv) control all uses of the Certificate, and (iv) is expressly authorized by Customer to approve Certificate requests on Customer's behalf. In the event of any discrepancy between these Terms and Conditions and any other agreements or proposals accepted by Customer in relation to other products or services offered by TuringSign or its affiliates and partners, these Terms and Conditions shall apply unless explicitly stated that it is the intention of the parties to modify these Terms and Conditions.

Changes to the Terms and Conditions

1. TuringSign Website Account Users ("Website Users")

TuringSign reserves the rights to disable or restrict access, withdraw or amend any parts of the Site at any time, including services or materials provided, without prior notice. We will not be liable for any part of the Site becoming unavailable at any time period. Website Users may be asked to provide certain registration details or information when accessing the Site, in such case, Website Users are required to provide correct, updated and complete information and take responsibilities for any wrongful information. Website Users must treat authentication credentials, including but not limited to usernames, passwords, as confidential and not disclose to any other person or entity. Website Users are required to notify TuringSign immediately of any unauthorized access or use of such credentials for any security breach.



TuringSign reserves the rights to disable usernames, passwords, accounts if any defects from provision of Terms and User are identified at any time.

2. Intellectual Property Rights

Customer's capacity as, including but not limited to, owner, account holder, user or subscriber, acknowledge that TuringSign, its vendors and licensors retain all property rights to its contents, features (including but not limited to information, software, design, images, videos); Any reproduction, distribution, modification without prior confirmation from TuringSign are considered violation of this Terms and Conditions. For more information about Intellectual Property Rights, refer to Subscriber Agreement at <https://turingsign.com/wp-content/uploads/2023/05/Subscriber-Agreement-WiseKeyxTuringSign-May2023.pdf>

3. CertifyID Account Users

Users who have been granted access to the TuringSign Certificate Management Portal CertifyID ("CertifyID") are not allowed to appoint other users as administrators for their account. At all times, Customer must be acting as a Certificate Requester and shall be in charge of communicating with TuringSign about the issuance and management of Certificates. TuringSign reserves the rights to validate and approve Certificates. Customer is responsible for periodically reviewing and reconfirming which individuals have authority to request Certificates, and TuringSign is not liable of incorrect issuance and management of Certificate by Customers or their administrators or employees. If Customer wishes to remove any Portal Account user(s), Customer shall take the necessary measures to prevent such user's access to the Portal, including but not limited to (i) contacting TuringSign for removing such user's account, or (ii) changing its password and authentication mechanisms. Customers are required to notify TuringSign immediately if any unauthorized use of the Portal Account is detected.

4. Certificate Requests:

Customer is permitted to request Certificates solely for domain names that are either registered to Customer, an affiliate of Customer, or any other entity that has been explicitly authorized by TuringSign to allow Customer to obtain and manage Certificates for the corresponding domain name.

5. Scope of Verification:

TuringSign shall review the Certificate request from Customer and verify the information as per the TuringSign Certification Practices Statement (hereby referred to as "CPS") and relevant Industry Standards (hereby referred to as "Industry Standards"). This includes compliance with applicable laws

and regulations. TuringSign has sole discretion in verifying such requests and reserves the right to refuse Certificate issuance without reason. Although TuringSign will inform the Customer of a refusal, it is not obligated to provide an explanation. "CPS" refers to TuringSign's written statements outlining policies and practices for operating its public key infrastructure. For further details on TuringSign's published CPS, please visit our website at <https://turingsign.com/wp-content/uploads/2022/08/turingsign-cps.pdf>.

6. Life Cycle of Certificate & Modification

An issued Certificate's lifecycle is determined by the Certificate type, any customizations made during order placement, CPS requirements, and the intended use of the Certificate. TuringSign reserves the right to modify the lifecycle of unissued Certificates to satisfy the Agreement, Industry Standards, or third-party regulations, such as those from auditors, software vendors, or government entities. Upon the expiration date of the Certificate or its revocation by TuringSign, CUSTOMER must discontinue using the Certificate and its related Private Key (as defined in the Agreement).

7. Certificate Issuance and Delivery

Upon successful validation of the Certificate request, TuringSign shall issue and deliver the Certificate to the Customer by utilizing any reasonable means of delivery. Such means may include but are not limited to delivering the Certificate via email to an address specified by the Customer, as an electronic download in the Portal, or in response to an API call made by the Customer via the Portal. The Customer shall be responsible for complying with all applicable laws, regulations, and Industry Standards while ordering and using the Certificates. Furthermore, we reserve the right to limit distribution of our SSL Certificates to certain regions to comply with international export control, sanctions, regulations and TuringSign internal policies.

8. Customer's Rights and Responsibilities

The issuance of each Certificate and related services regardless of when it was performed, before or after issuance of the certificate, and corresponding key set is solely for the benefit of the certificate's subject and is subject to the terms outlined herein, all applicable laws, regulations, and industry standards. Customer may use the Certificate immediately upon receiving it until it expires or is revoked, subject to the purposes described in the CPS. Certificates must adhere to all applicable industry standards requirements, including those found in applicable application software vendor root store policies and the CPS, regardless of usage. Any use that is not allowed by applicable industry standards or the CPS is prohibited.

TuringSign advises against using certificates in a way that could make it challenging for the customer to comply with the revocation timelines or other CPS requirements, such as certificate or key pinning, or

using certificates trusted for the web with non-web PKI. Any such use will not be considered a sufficient reason to delay revocation.

The key set refers to a set of two or more mathematically related keys, including private keys or key shares, along with a public key. The public key can encrypt a message that only the private key(s) can decrypt, and even knowing the public key, it is computationally infeasible to discover the private key(s). The customer must promptly inform TuringSign if they become aware of any misuse of a certificate, private key, or the portal. The customer is responsible for obtaining and maintaining any authorization or license necessary to order, use, and distribute a certificate to end-users and systems, including any license required under the Swiss Confederation Export Law. SSL certificates may be used on one or more physical servers or devices at a time. But, TuringSign shall have the right to charge a fee for the use of certificates on additional servers or devices.

9. Key Sets and Related Responsibilities

We understand the importance of confidentiality when it comes to your Private Key, a key used by the Customer to create digital signatures and decrypt electronic records or files that have been encrypted with the corresponding Public Key. The Public Key, on the other hand, is a publicly disclosed key contained in the Certificate and corresponds to the secret Private Key used.

To ensure the utmost security, we require our customers to take the following steps: (i) generate Key Sets using reliable systems, (ii) ensure that they are at least equivalent to RSA 2048 bit keys, and (iii) maintain the confidentiality of all Private Keys. Please note that the Customer bears sole responsibility for any failure to protect their Private Keys. For all other Certificate types, secure software or hardware systems may be used for storage.

It is also crucial that the Customer ensures their acquisition, use, or acceptance of Key Sets generated by TuringSign complies with the Agreement, applicable local laws, rules, and regulations, including those pertaining to export and import, rules and regulations in the jurisdiction where the Customer acquires, uses, accepts, or receives such Key Sets. Please be aware that when Private Keys (including copies) are imported or exported in connection with the use of specific TuringSign services, we cannot be held liable for the usage or storage of Private Keys (including copies) that are not created in the applicable Portal or service or that are used outside such Portal or service, even after they are exported from the said Portal or service.

10. Consent To Public Disclosure

TuringSign may make public disclosure about Customer from time to time or as it deems necessary

without separately informing Customer. As such, Customer consents to: (i) TuringSign's public disclosure of information (such as Customer's official organization name, domain name, jurisdiction of incorporation), embedded in an issued Certificate; and (ii) Customer's Certificates and information embedded therein being logged by or on behalf of TuringSign in publicly-accessible Certificate transparency databases for purposes of detecting and preventing phishing attacks and other forms of fraud. Such publication of Certification information will be in accordance with the applicable CPS.

11. Required Notice Period

In accordance with any requests or reports submitted by Customer complying with the below notice periods, TuringSign shall issue, manage, renew, and revoke a Certificate:

Change of Customer's Info: Customer shall provide accurate and complete information when communicating with TuringSign and will notify TuringSign within 5 Business Days if any information relating to its account on the Portal changes.

Inquiries from TuringSign: Customer shall respond to any inquiries from TuringSign regarding the validity of information provided by Customer within 5 Business Days after Customer receives notice of the inquiry.

Certificates are considered accepted by Customer thirty (30) days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Customer used the Certificate. Although TuringSign will automatically send a reminder about activating Certificates or alert email about expiring Certificates, TuringSign is under no obligation to do so and Customer is solely responsible for ensuring Certificates are properly activated and renewed prior to expiration.

12. Remedy for Defective Certificates

It is Customer's responsibility to notify any defect in a Certificate ("Defect") to TuringSign. TuringSign is not obligated to correct a Defect if (i) Customer misused, damaged, or modified the Certificate, (ii) Customer did not promptly report the Defect to TuringSign, or (iii) Customer has breached any provision of the Agreement. Customer's sole and maximum remedy for a Defect in a Certificate is to require TuringSign to use commercially reasonable efforts to cure the defect after receiving notice of such Defect from Customer.

13. Warranty

Customer recognizes that the Relying Party Warranty is solely for the benefit of Relying Parties. The term "Relying Party Warranty" refers to a warranty that is offered to a Relying Party, subject to certain conditions as specified in the Relying Party Agreement and Limited Warranty available on the TuringSign website. The Relying Party Warranty for Certificates issued by a QTSP or a TuringSign affiliate is posted at <https://www.quovadisglobal.com/repository>. Customer has no rights under the Relying Party Warranty,

including the right to enforce its terms or make a claim under it. The term "Relying Party" has the same meaning as set forth in the Relying Party Warranty. An Application Software Vendor is not considered a Relying Party when the software they distribute only displays information about a Certificate or assists in its use.

14. Customer's Representations

For each requested Certificate, Customer represents and warrants that: a. Customer has the right to use or is the lawful owner of (i) any domain name(s) specified in the Certificate, and (ii) any common name or organization name specified in the Certificate; b. Customer will use the Certificate only for authorized and legal purposes; c. Customer has read, understands, and agrees to the CPS; d. Customer will immediately report in writing to TuringSign any non-compliance with the CPS or Baseline Requirements; and e. the organization included in the Certificate and the registered domain name holder is aware of and approves of each Certificate request.

15. Limitations and Restrictions

Customer shall only use a TLS/SSL Certificate on the servers accessible at the domain names listed in the issued Certificate. Furthermore, Customer shall not: a. modify, sublicense, or create a derivative work of any TLS/SSL Certificate (except as required to use the Certificate for its intended purpose) or Private Key; b. upload or distribute any files or software that may damage the operation of another's computer; c. impersonate or misrepresent Customer's affiliation with any entity; d. use a Certificate or any related software or service (such as the Portal) in a manner that could reasonably result in a civil or criminal action being taken against Customer or TuringSign; e. use a Certificate or any related software to breach the confidence of a third party or to send or receive unsolicited bulk correspondence; f. interfere with the proper functioning of the TuringSign website or with any transactions conducted through the TuringSign website; g. attempt to use a Certificate to issue other Certificates or use any end-entity Certificate to sign any Certificate; h. submit Certificate information to TuringSign that infringes the intellectual property rights of any third party; or i. intentionally create a Private Key that is substantially similar to a TuringSign or third-party Private Key.

16. TuringSign's Right to Revoke Certificate

TuringSign may revoke a Certificate without notice for the reasons stated in the CPS, including if TuringSign reasonably believes that:

- a. Customer requested revocation of the Certificate or did not authorize the issuance of the Certificate;
- b. Customer is using TuringSign's products or services to post or make accessible any materials that infringes our or any third party's rights;
- c. Customer has breached the Agreement or an obligation it has under the CPS;

- d. any provision of an agreement with Customer containing a representation or obligation related to the issuance, use, management, or revocation of the Certificate terminates or is held invalid;
- e. Customer is added to a government prohibited person or entity list or is operating from a prohibited destination under the laws of Singapore, Switzerland, EU and/or the United States;
- f. the Certificate contains inaccurate or misleading information or used outside of its intended purpose;
- g. the Private Key associated with the Certificate was disclosed or compromised;
- h. the Certificate was (i) misused, (ii) used or issued contrary to law, the CPS, or Industry Standards, or (iii) used, directly or indirectly, for illegal or fraudulent purposes, such as phishing attacks, fraud, or the distribution of malware, other illegal or fraudulent purposes, or any other violations as outlined in the TuringSign Acceptable Use Policy;
- i. revocation is necessary to protect the rights, confidential information, operations, or reputation of TuringSign or a third party.

17. Communication with Customers

Email is the main form of communication between TuringSign and Customers. Customers agree that (1) the content of communication shall be strictly limited to communication or notice about TuringSign products or services and (2) Customers shall follow applicable laws (including all applicable electronic communication laws and data privacy/data protection laws).

18. Indemnity Clause

Customer agrees to defend, indemnify, and hold harmless TuringSign, TuringSign Affiliates, and each of their respective directors, officers, employees, and agents from and against any and all third-party claims, demands, and liabilities, including reasonable attorneys fees, resulting from or arising out of: (i) any breach of Customer's representations in relation to Terms and Conditions and/or Agreement; or (ii) Customer's failure to comply with Customer's obligations under any and all laws, rules or regulations applicable to Customer under Terms and Conditions and/or Agreement, except to the extent such violation arises out of TuringSign's failure to comply with its obligations.

19. Authorization of Information Sharing

Customer understands and accepts that if (i) the authority to request the Certificate cannot be verified, or (ii) the Certificate is revoked for reasons other than Customer request, including but not limited to, as a result of private key compromise, discovery of malware, TuringSign is authorized to share information about Customer, any application or object signed with the Certificate, the Certificate, and the surrounding circumstances with other certification authorities or industry groups, including the CAB Forum. More about sharing of information can be found in our Privacy Policy.

20. Mutual Compliance

It is hereby agreed that both parties shall be obligated to comply with all pertinent laws and Industry Standards that apply to the Certificates. In the event that an applicable law or Industry Standard undergoes a change that affects the Certificates or other services provided under this Agreement, the Company reserves the right to modify the services or to amend or terminate the Agreement to the extent required for compliance with such change.

21. Continuation of Certificate Terms and Conditions

In the event of termination of the Agreement, the Certificate Terms and Conditions shall continue to remain in full force and effect until such time as all issued Certificates have either been revoked or have expired.