

VikingCloud Subscriber Agreement for Digital Certificates
Ver. 24MAY23

IMPORTANT: PLEASE READ THIS AGREEMENT AND THE VIKINGCLOUD CERTIFICATE POLICY AND CERTIFICATION PRACTICES STATEMENTS LOCATED AT [HTTPS://CERTS.SECURETRUST.COM/CA/](https://certs.securetrust.com/ca/) ("CPS") CAREFULLY BEFORE USING THE CERTIFICATE ISSUED TO YOUR ORGANIZATION. BY USING THE CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT AND THE CPS. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, E-MAIL US AT ca@vikingcloud.com . IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT APPLY FOR A CERTIFICATE AND DO NOT CLICK ON "I ACCEPT" OR "I AGREE" BELOW, DO NOT CLICK "CONTINUE" AND PROMPTLY EXIT THE BROWSER.

THIS VIKINGCLOUD SUBSCRIBER AGREEMENT FOR DIGITAL CERTIFICATES ("Agreement") is effective as of the date of the accompanying Certificate (the "Effective Date") and is entered into by Viking Cloud, Inc. ("VikingCloud", Provider", "We", "Our", or "Us") and the applicant set forth in the Order Form and that is receiving the Certificate ("Client").

The legal name of the Client is as stated in the Order Form. _____

The name of the Contract Signer (as hereinafter defined) duly authorized by the Client to bind the Client to this Agreement is as stated in the Order Form. _____

Each Certificate that VikingCloud issues to Client shall be governed by this Agreement, any Order Form, and the CPS. Further, the parties hereby agree that Relying Parties and Application Software Vendors (as such terms are defined below) are intended third party beneficiaries of this Agreement.

1. DEFINITIONS

Application Software Vendors

A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as, but not limited to, KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.

Certificate

Any certificate that contains information specified in the CPS and/or the Guidelines, as applicable, and that has been validated in accordance with the CPS and/or the Guidelines, as applicable.

Certificate Revocation List ("CRL")

A regularly updated time-stamped list of revoked or invalid Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority ("CA")

VikingCloud or an entity which is certified by VikingCloud to issue Certificates to Users. VikingCloud is Client's CA hereunder.

Contract Signer

The natural person who is employed by the Client, or an authorized agent who has express authority to represent the Client who has signed this Agreement on behalf of the Client and who has authority on behalf of the Client to sign this Agreement on behalf of the Client.

Digital Signature

Information encrypted with a Private Key which is appended to electronic data to identify the owner of the Private Key and verify the integrity of the electronic data. Digitally Signed shall refer to electronic data to which a Digital Signature has been appended.

Guidelines

Guidelines for Extended Validation Certificates, and other Certificates as adopted by the CA/Browser Forum and as amended, revised and updated from time to time.

Key Pair

The Private Key and Public Key that correspond to each other.

Order Form

The statement of work, order form (online or otherwise), or other ordering document, that references this Agreement, is accepted by VikingCloud and identifies the Services, price, term length and other transactional information.

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 Parties

Any person (individual or entity) that relies on a Valid Certificate. An Application Software Vendor is not considered a Relying Party when software distributed by such Vendor merely displays information regarding a Certificate.

Secure Server Hierarchy

A collection of CAs and their certified Users.

Subscriber

A natural person or legal entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement.

Suspect Code

Code that contains malicious functionality or serious vulnerabilities, including spyware, malware, and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

User

An individual or an organization that has requested a CA to issue him, her or it a Certificate.

Valid Certificate

A Certificate that has not expired and has not been revoked.

2. AUTHORITY TO USE CERTIFICATE

Grant of Authority

As of the Effective Date, VikingCloud hereby grants to Client the authority for the term set forth in Section 7 to use the Certificate to create Digital Signatures or to use the Certificate in conjunction with Private Key or Public Key operations.

Limitations on Authority

Client shall use its Certificate only in connection with properly licensed cryptographic software.

3. SERVICES PROVIDED BY VIKINGCLOUD

After execution of this Agreement and payment of all applicable fees, in addition to the grant of authority pursuant to Section 2, VikingCloud or a third party provider designated by VikingCloud shall:

CRL Availability

use reasonable efforts to compile, aggregate and make electronically available to all CAs and certified Users in the Secure Server Hierarchy: (i) VikingCloud's current CRL; and (ii) the CRLs provided by CAs to VikingCloud; provided, however, that VikingCloud shall not be in breach of its obligations hereunder as a result of any delay in or failure of performance on its part which arises out of any equipment failure or telecommunications breakdown beyond the reasonable control of VikingCloud;

Revocation Status Services

use reasonable efforts to provide to CAs, certified Users and users of those Certificates in the Secure Server Hierarchy information concerning the status of particular Certificates; provided, however, that VikingCloud shall not be in breach of its obligations hereunder as a result of any delay in or failure of performance on its part which arises out of any equipment failure or telecommunications breakdown beyond the reasonable control of VikingCloud; and

Revoke Certificates

promptly upon the request of Client, revoke the Certificate of Client. VikingCloud agrees that it, promptly after revoking Client's Certificate at Client's request, shall issue Client a new Certificate upon verification and approval by the appropriate CA and payment by Client of the then-current applicable fee.

4. CLIENT OBLIGATIONS

User Identification Information

All information provided by Client to VikingCloud for the purpose of obtaining its Certificate shall be truthful, accurate, and not misleading. If at any time, the name of Client contained in the Certificate request provided by Client has changed, Client shall immediately cease using such Certificate, request that VikingCloud revoke such Certificate, and provide VikingCloud with such changed information. If at any time, any other significant information, in particular Client's organization name, city, state, or country changes from that contained in the Certificate request, Client shall request that VikingCloud revoke the Certificate in accordance with Section 3 above.

Compromised Certificate

If Client has any reason to believe that the security of Client's Private Key may have been compromised, Client shall immediately request that VikingCloud revoke Client's Certificate and VikingCloud shall revoke said Certificate immediately upon Client's request.

Accuracy of Information

Client hereby agrees and warrants that it will provide accurate and complete information at all times to VikingCloud, both in the Certificate request and as otherwise requested by VikingCloud in connection with the issuance of the Certificate(s) to be supplied by VikingCloud.

Protection of Private Key

Client hereby agrees and warrants that it (and its authorized subcontractors) will take all reasonable measures necessary 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 access information or device – e.g., password or token). Client hereby assumes a duty to retain control of Client's Private Key, to use a trustworthy system, and to take reasonable precautions to prevent its loss, disclosure or unauthorized use.

Client further agrees to generate and protect code signing Private Keys using one of the following:

1. A Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+;
2. A cloud-base key generation and protection solution with the following requirements:
 - a. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+;
 - b. Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.

Verification of Private Key

Client further agrees to provide VikingCloud proof that their code signing Private Keys were generated and protected using one of the above methods. That proof would take the form of one of the following items:

1. The Client counter-signs certificate requests that can be verified by using a manufacturer's certificate, commonly known as key attestation, indicating that the Private Key was generated in a non-exportable way using a suitable Hardware Crypto Module;
2. The Client provides an internal or external IT audit indicating that it is only using a suitable Hardware Crypto Module to generate Key Pairs to be associated with Code Signing Certificates; or
3. The Client provides a suitable report from the cloud-based key protection solution subscription and resources configuration protecting the Private Key in a suitable Hardware Crypto Module.

Private Key Reuse

Client hereby agrees and warrants that it will not apply for a code signing Certificate if the Public Key in the Certificate is or will be used with a non-code signing Certificate.

Acceptance of Certificate

Client hereby agrees and warrants that it will not install and use the Certificate(s) until it has reviewed and verified the accuracy of the data in each Certificate. Client is required to notify VikingCloud immediately if there is an error in its Certificate.

Reporting and Revocation Upon Compromise

Client hereby agrees and warrants that it will promptly cease using a Certificate and its associated Private Key, and promptly request VikingCloud to revoke the Certificate, in the event that: (a) any information in the Certificate is or becomes incorrect or inaccurate, (b) there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key listed in the Certificate, or (c) there is evidence that the Certificate was used to sign Suspect Code.

Revocation Reason Codes

Client is hereby informed and acknowledges the reasons for revoking a Certificate, including those stated in Section 7.2.2 of the CPS, which as previously stated above, is incorporated herein by reference and made a part of this Agreement.

Termination of Use of Certificate

Client hereby agrees and warrants that it will promptly cease all use of the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of that Certificate.

Use of Certificate

Client hereby agrees and warrants that it will install the Certificate only on the server accessible at the domain name listed on the Certificate, and to use the Certificate solely in compliance with all applicable laws, for authorized company business, and in accordance with this Agreement, the CPS, and the Guidelines.

Furthermore, with respect to code signing Certificate(s) and in addition to the other obligations herein, Client hereby agrees and warrants that it: (i) shall not intentionally include Suspect Code in its code signed software; (ii) shall not knowingly sign software that contains Suspect Code; and (iii) shall inform VikingCloud of the following circumstances:

- (a) it is discovered, by whatever means, that the signed code is suspect; or
- (b) it discovers or suspects that a copy of its Private Key or key activation data is no longer under its sole control.

Prevention of Misuse

Client hereby agrees and warrants that it will provide adequate network and other security controls to protect against misuse of a code signing Private Key. VikingCloud will revoke code signing Certificates without requiring prior notification if there is unauthorized access to the Private Keys.

Sharing of Information

Client hereby acknowledges and accepts that if: (a) the Certificate or the Client is identified as a source of Suspect Code; (b) the authority to request the Certificate cannot be verified; or (c) the Certificate is revoked for reasons other than Subscriber request (e.g. as a result of private key compromise, discovery of malware, etc.), then VikingCloud is authorized to share information about the Client, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.

Acknowledgement and Acceptance:

Client acknowledges and agrees that VikingCloud shall have the right to modify the Subscriber Agreement when necessary to comply with any changes in the Requirements or the Baseline Requirements.

Client further acknowledges and agrees that VikingCloud is entitled to revoke the certificate immediately if Client violates the Subscriber Agreement.

5. PERMISSION TO PUBLISH INFORMATION & RECEIVE COMMUNICATIONS

Client agrees that VikingCloud may publish the serial number of Client's Certificate in connection with VikingCloud's dissemination of CRLs and Certificate status information within and outside of the VikingCloud Secure Server Hierarchy. Client agrees to receive communications from VikingCloud via email.

6. DISCLAIMER OF WARRANTY AND LIMITATION OF LIABILITY

VIKINGCLOUD'S AGGREGATE LIABILITY TO CLIENT, REGARDLESS OF THEORY OF LIABILITY, FOR ALL CLAIMS, DAMAGES, COSTS, LOSSES, EXPENSES AND OTHER AMOUNTS ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE SERVICES PROVIDED HEREUNDER SHALL NOT EXCEED THE FEES PAID TO VIKINGCLOUD BY CLIENT IN THE TWELVE MONTHS PRECEDING THE DATE OF THE EVENT GIVING RISE TO SUCH CLAIM. NOTWITHSTANDING THE FORGOING, ANY LIABILITY IN RESPECT OF FRAUD, FRAUDULENT MISREPRESENTATION, PERSONAL INJURY OR DEATH CAUSED BY VIKINGCLOUD'S GROSS NEGLIGENCE, RECKLESSNESS OR WILLFUL MISCONDUCT SHALL NOT BE LIMITED OR EXCLUDED. NO ACTION ARISING OUT OF THIS AGREEMENT, REGARDLESS OF FORM, MAY BE BROUGHT BY EITHER PARTY MORE THAN ONE (1) YEAR AFTER THE CAUSE OF ACTION HAS ACCRUED.

IN NO EVENT WILL VIKINGCLOUD BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, WHETHER FORSEEABLE OR UNFORSEEABLE, OF ANY KIND WHATSOEVER, ARISING OUT OF OR IN CONNECTION WITH FURNISHING, PERFORMANCE OR USE OF THE SERVICES PROVIDED HEREUNDER OR THE USE, DELIVERY, LICENSE, PERFORMANCE OR NONPERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS AGREEMENT OR THE CPS, INCLUDING BUT NOT LIMITED TO, LOST PROFITS, LOSS OF REVENUE, LOSS OF BUSINESS OPPORTUNITIES, LOSS OR DAMAGE TO GOODWILL, LOSS OF DATA, LOSS OF USE OF SYSTEM(S) OR NETWORK OR THE RECOVERY OF SUCH, BUSINESS INTERRUPTION OR DOWNTIME, EVEN IF VIKINGCLOUD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES, WHETHER BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE. FURTHER, VIKINGCLOUD SHALL NOT BE LIABLE FOR ANY DAMAGES DUE TO THE DELAY IN PERFORMING THE SERVICES PROVIDED HEREUNDER OR IN ANY CIRCUMSTANCE RELATING TO THE CLIENT BREACHING ITS REPRESENTATIONS OR OBLIGATIONS UNDER SECTION 4 OF THIS AGREEMENT.

7. TERM AND TERMINATION

- i. This Agreement shall commence on the Effective Date and shall, subject to the other provisions of this Agreement, terminate on the expiration date of the Certificate issued.
- ii. VikingCloud may terminate this Agreement if Client materially breaches this Agreement and does not cure such breach within fifteen (15) days after receipt of written notice from VikingCloud of such breach.
- iii. VikingCloud may terminate this Agreement for cause if: (a) Client fails to pay VikingCloud when fees are due within thirty (30) days of VikingCloud providing Client notice of nonpayment; (b) the services provided hereunder require third party products or services which either: (i) substantially change in scope and/or price or (ii) VikingCloud no longer has access to such third party product or services; (c) Client (i) becomes insolvent, makes an assignment for the benefit of creditors, becomes subject to direct control of a trustee, receiver or similar authority (ii) becomes subject to any bankruptcy or insolvency proceeding, or (iii) terminates or suspends its business.
- iv. Termination of this Agreement shall not affect Client's obligation to pay for the Certificate(s).

8. EFFECT OF TERMINATION

Upon termination of this Agreement for any reason, Client's Certificate shall be revoked by VikingCloud in accordance with VikingCloud's procedures then in effect. Upon revocation of Client's Certificate for any reason, all authority granted to Client pursuant to Section 2 shall terminate. Such termination or revocation shall not affect Sections 5, 6, 7, 9 and 10 of this Agreement which shall continue in full force and effect to the extent necessary to permit the complete fulfillment thereof.

9. MISCELLANEOUS PROVISIONS

GOVERNING LAW

THE PARTIES ACKNOWLEDGE THAT THE TRANSACTION THAT IS THE SUBJECT MATTER HEREIN BEARS A REASONABLE RELATION TO THE STATE OF DELAWARE IN THE UNITED STATES OF AMERICA AND THAT THIS AGREEMENT SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF DELAWARE (WITHOUT REFERENCE TO CONFLICT OF LAWS) AND SHALL BE SUBJECT TO THE EXCLUSIVE JURISDICTION OF THE STATE AND FEDERAL COURTS LOCATED IN CHICAGO, IL. THE PARTIES EXPRESSLY AGREE TO EXCLUDE FROM THIS AGREEMENT ANY APPLICATION OF THE UNITED NATIONS CONVENTIONS ON CONTRACTS FOR THE INTERNATIONAL SALE OF GOODS, 1980, AND ANY SUCCESSOR THERETO.

Binding Effect

Except as otherwise provided herein, this Agreement shall be binding upon, and inure to the benefit of, the successors, executors, heirs, representatives, administrators and assigns of the parties hereto. Neither this Agreement nor Client's Certificate shall be assignable by Client. Any such purported assignment or delegation shall be void and of no effect and shall permit VikingCloud to terminate this Agreement. VikingCloud may assign this Agreement to its parent company, wholly-owned subsidiary, or any affiliate, or as a result of a merger, acquisition, sale, transfer or other disposition of all or substantially all of its assets to which the services hereunder relate.

Issuance Disclaimer

Notwithstanding anything herein to the contrary, if Client does not complete the application process for the issuance of any or all Certificate(s) purchased hereunder within 12 months from acceptance of this Agreement, VikingCloud shall have no obligation to issue such Certificate(s). Furthermore, the terms under this section shall not affect the Client's obligation to pay for the Certificate(s).

Severability

If any provision of this Agreement, or the application thereof, shall for any reason and to any extent, be invalid or unenforceable, the remainder of this Agreement and application of such provision to other persons or circumstances shall be interpreted so as best to reasonably effect the intent of the parties hereto.

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EACH AND EVERY PROVISION OF THIS AGREEMENT WHICH PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES OR EXCLUSION OF DAMAGES IS INTENDED BY THE PARTIES TO BE SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND TO BE ENFORCED AS SUCH.

Entire Agreement

This Agreement constitutes the entire understanding and agreement of the parties hereto with respect to the subject matter hereof and supersedes all prior and contemporaneous agreements or understandings between the parties.

Notices

Whenever Client desires or is required to give any notice, demand, or request to VikingCloud with respect to this Agreement, each such communication shall be in writing and shall be effective only if it is delivered by a courier service that confirms delivery in writing or mailed, certified or registered mail, postage prepaid, return receipt requested, addressed to VikingCloud, Attn. Legal Department, 5775 Glenridge Drive, Building D, Suite #450, Atlanta, Georgia, 30328, United States of America. Such communications shall be effective when they are received.

Trade Names, Logos

By reason of this Agreement or the performance hereof, Client and VikingCloud shall acquire no rights of any kind in any trademark, brand name, logo or product designation of the other party and shall not make any use of the same for any reason except as otherwise authorized in writing by the party which owns all rights to such trademarks, trade names, logos or product designation.

Dispute Settlement

Any dispute, controversy or claim arising under, in connection with or relating to this Agreement, the CPS, VikingCloud's Websites, or any Certificate issued by VikingCloud shall be subject to and settled finally by binding arbitration in accordance with the Arbitration Rules of the American Arbitration Association (AAA). All arbitration proceedings shall be held in Chicago, IL. There shall be one arbitrator appointed by the AAA who shall exhibit a reasonable familiarity with the issues involved or presented in such dispute, controversy or claim. The award of the arbitrator shall be binding and final upon all parties, and judgment on the award may be entered by any court having proper jurisdiction thereof. This Agreement, the CPS and the rights and obligations of the parties hereunder and under any Certificate issued by VikingCloud shall remain in full force and effect pending the outcome and award in any arbitration proceeding hereunder. In any arbitration arising hereunder, each party to the preceding shall be responsible for its own costs incurred in connection with the arbitration proceedings, unless the arbitrator determines that the prevailing party is entitled to an award of all or a portion of such costs, including reasonable attorneys' fees actually incurred.

Intended Third Party Beneficiaries

The parties understand and agree that Microsoft and any other third party that VikingCloud wishes to have the VikingCloud roots included in the third party's certificate store, browsers, devices, software, and other products is an intended third party beneficiary of this Agreement.

10. ACCEPTANCE

By agreeing to use the Certificate, Client agrees to be bound by this Agreement and the CPS. Further, in accordance with the Uniform Electronic Transactions Act and, to the extent applicable, the Federal U.S. law governing Electronic Signatures in Global and National Commerce, the Client agrees to be bound by this Agreement and the CPS by providing an electronic signature logically associated with this Agreement. In accordance with Section 9 above, this Agreement (including the manner of acceptance) is governed by and construed in accordance with the laws of the State of Delaware.