

EV Subscriber Agreement



Cybertrust Sureserver EV Subscriber Agreement

Cybertrust Sureserver EV Subscriber Agreement

CYBERTRUST SURESERVER EV SUBSCRIBER AGREEMENT

This Subscriber Agreement ("Agreement") between Cybertrust ("Cybertrust") and the Applicant ("Subscriber") identified below and signatories hereto consists of this signature page and is made effective as of the effective date specified below ("Effective Date").

This Certificate Request ("Request") between Cybertrust and the Requestor identified below and signatories hereto consists of the detailed certificate request data and this signature page and is made effective as of the effective date specified below ("Effective Date").

The Subscriber and Requestor may be the same entity or different entities. The person performing the technical process of handling the certificate request must sign as the Requestor, and the person employed by the Applicant with contract binding authority that can be proven consistent with the EV Guidelines of the CA/Browser Forum must sign as the Subscriber. When the Subscriber and Requestor are different entities, full legal name and address of the requestor must be included on this signature page.

Intending to be legally bound and having reviewed this Agreement in its entirety, Cybertrust and Applicant have caused this Agreement to be executed by their authorized representatives. Applicant and Requestor shall complete the following sections of this Agreement as their execution, Cybertrust shall accept and execute the agreement by its delivery of an EV SSL certificate on completion of Cybertrust's validation processes and therefore does not countersign this Agreement.

("Subscriber")

AND ("Requestor")

Address: _____

Address: _____

Reg. No/Tax ID: _____

Reg. No/Tax ID: _____

Agreed for and on behalf of Cybertrust:

Agreed for and on behalf of Subscriber:

Name : _____
Title : _____
Date : _____
Signature : _____

Name : _____
Title : Contract Signer
Date : _____
Signature : _____

AGREEMENT DETAILS:

Effective Date: ___/___/___ (eg: 01-JAN-2006)

IT IS AGREED AS FOLLOWS:

The parties acknowledge that the present subscriber agreement applies to the SureServer EV digital certificate to be issued pursuant to the provisions set forth in Cybertrust Certification Practice Statement (CPS) which incorporates by reference the CA/Browser Forum Guidelines for Extended Validation Certificates.

The parties therefore acknowledge that the CA/Browser Forum Guidelines for Extended Validation Certificates set forth mandatory requirements as to issuance and management of SureServer EV certificates.

Cybertrust Sureserver EV Subscriber Agreement

Cybertrust CPS is incorporated by reference hereto and is available at cybertrust.omniroot.com/repository. The CA/Browser Forum Guidelines for Extended Validation Certificates are available at www.cabforum.org.

The parties shall ensure that the present subscriber agreement is properly signed before requesting the issuance of the Cybertrust SureServer EV digital certificate.

The parties shall ensure that the present certificate request is properly signed before requesting the issuance of the Cybertrust Sureserver EV digital certificate.

1. Authority to Use Digital Certificates

Grant of Authority

As to the Effective Date, Cybertrust hereby grants to the subscriber the authority for the term set forth in Sections 6 and 7 to use the requested SureServer EV Certificate to create Digital Signatures or to use the SureServer EV Certificate in conjunction with private key or public key operations.

Limitations on Authority

The subscriber shall use the requested SureServer EV Certificate only in connection with properly licensed cryptographic software.

2. Services Provided by Cybertrust

After execution of this agreement and payment of all applicable fees, in addition to the grant of authority pursuant of Section 2, Cybertrust or a third party provider designated by Cybertrust shall provide the following services to the subscriber:

CRL Availability

Cybertrust shall use best efforts to compile, aggregate and make electronically available to all CAs and certified users in the Secure Server Hierarchy (i) Cybertrust current CRL and (ii) the CRLs provided by CAs to Cybertrust; provided, however that Cybertrust 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 Cybertrust.

Revoke Digital Certificates

Cybertrust, upon the request of the subscriber, shall promptly revoke the digital certificate of the subscriber. Cybertrust agrees that it shall, promptly after revoking the subscriber's certificate at the subscriber's request, issue a new SureServer EV certificate upon data verification and validation and payment by the subscriber of the then-current applicable fee.

3. Subscriber's Obligations

Data accuracy

The subscriber undertakes to provide accurate and complete information at all times to Cybertrust, both in the SureServer EV Certificate Request and as otherwise requested by Cybertrust CA in connection with the issuance of the SureServer EV Digital Certificate(s) to be supplied by Cybertrust.

The requestor represents that the data submitted on behalf of the subscriber is accurate to the best extent of their ability.

The subscriber shall also refrain from submitting to Cybertrust or any Cybertrust CA directory any material that contains statements that violate any law or the rights of any party.

Cybertrust Sureserver EV Subscriber Agreement

Key Generation

Under the Cybertrust model the subscriber uses a trustworthy system in order to generate, its own private-public keys, in which case the following terms also apply:

- (a) The subscriber generates subscriber keys using an algorithm recognized as being fit for the purposes of electronic signatures;
- (b) The subscriber uses a key length and algorithm, which is recognized as being fit for the purposes of electronic signatures.

Protection of Private Key

The subscriber or a subcontractor (e.g. hosting provider) undertakes to 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 SureServer EV certificate(s) (and any associated access information or device - e.g., password or token).

The subscriber shall ensure that the public key submitted to the Cybertrust CA correctly corresponds to the private key used.

The subscriber shall exercise appropriate and reasonable care to avoid unauthorized use of its private key.

Establishment of Certificate Approver Authority

The subscriber shall participate in a verification process which establishes the authority of a Certificate Approver as either an employee or appointed agent of the subscriber. Once confirmed, such authority shall be considered to be perpetual and surviving beyond the termination of this agreement until explicitly revoked by the subscriber. Certificate Approver shall be defined consistent with the current version of the EV Guidelines in force at the time of this agreement.

Acceptance of SureServer EV Certificate

The subscriber shall not install and use the SureServer EV certificate(s) until it has reviewed and verified the accuracy of the data in each SureServer EV Certificate.

Use of SureServer EV Certificate

The subscriber shall install the SureServer EV certificate only on the server accessible at the domain name listed on the SureServer EV certificate, and to use the SureServer EV certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the subscriber agreement.

Reporting and Revocation Upon Compromise

The Subscriber undertakes to promptly cease using a SureServer EV certificate and its associated private key, and promptly request the CA to revoke the SureServer EV certificate, in the event that:

- (a) any information in the SureServer EV 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 listed in the SureServer EV certificate;

Termination of Use of SureServer Certificate

The subscriber shall promptly cease all use of the Private Key corresponding to the Public Key listed in a SureServer EV certificate upon expiration or revocation of that SureServer EV certificate.

4. Permission to Publish Information

Cybertrust Sureserver EV Subscriber Agreement

The subscriber agrees that Cybertrust may publish the serial number of the subscriber's SureServer EV certificate in connection with Cybertrust dissemination of CRLs and OCSP within and outside the Cybertrust Secure Server Hierarchy.

5. Disclaimer of Warranty

IN NO EVENT (EXCEPT FOR FRAUD OR WILFULL MISCONDUCT) SHALL CYBERTRUST BE LIABLE FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA OR OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE OR NON PERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THE CPS, EXCEPT FOR DAMAGE DUE TO RELIANCE (IN ACCORDANCE WITH THE CPS) ON THE VERIFIED INFORMATION ON THE MOMENT OF ISSUANCE OF THE CERTIFICATE IN A SECURE SERVER CERTIFICATE TILL AN AMOUNT OF 2,000 \$ PER SUBSCRIBER OR RELYING PARTY PER SURESERVER CERTIFICATE. CYBERTRUST WILL NOT BE LIABLE IN THIS CASE IF THE FAULT IN THIS VERIFIED INFORMATION IS DUE TO FRAUD OR WILFULL MISCONDUCT OF THE APPLICANT. CYBERTRUST WILL NOT BE LIABLE IN THIS CASE IF THE USER HAS NOT RESPECTED HIS OBLIGATIONS MENTIONED IN THE CPS AND IN THIS AGREEMENT

6. Term and Termination

This agreement shall terminate at the earliest of

6.1. one year after the expiration date of any Sureserver EV certificate issued pursuant to this agreement.

6.2. failure by the subscriber to perform any of its material obligations under this agreement if such breach is not cured within thirty (30) days after receipt of notice thereof from Cybertrust.

This agreement shall be considered as reasonable future proof of contract signing authority by the Contract Signer to the extent permitted by the EV Guidelines of the CA/Browser Forum.

The Certificate Approver granted approval authority during the verification of this certificate request shall be considered to have a perpetual right to approve certificate requests for the Subscriber until such authority is explicitly revoked by the Subscriber.

7. Effect of termination

Upon termination of this agreement for any reason, the subscriber's SureServer EV Certificate shall be revoked by Cybertrust in accordance with Cybertrust procedures then in effect. Upon revocation of the subscriber's SureServer EV Certificate for any reason, all authority granted to the subscriber pursuant to section 2 shall terminate. Such termination shall not affect sections 4, 5, 6, 8 and 9 of this agreement which shall continue in full force and effect to the extent necessary to permit the complete fulfillment thereof.

8. Miscellaneous Provisions

Applicable Law

This Agreement shall be governed by and construed in accordance with the laws of Belgium in all cases except those where the Subscriber's verified jurisdiction of incorporation country is the United States. In such case, this Agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia.

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

Cybertrust Sureserver EV Subscriber Agreement

agreement not the subscriber's digital certificate shall be assignable by the subscriber. Any such purported assignment or delegation shall be void and of no effect and shall permit Cybertrust to terminate this agreement.

Entire Agreement

This Agreement constitutes the entire agreement between the parties and supersedes all prior understandings, oral or written, between the parties.

Notices

When the subscriber desires or is required to give any notice, demand, or request to Cybertrust 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 mailed, postage prepaid, return receipt requested, addressed to Cybertrust, Philipssite 5, 3001 Leuven, Belgium, Attention: Secure Server Center.

Such communications shall be effective when they are received.

Severability

Invalidity or unenforceability of one or more provisions of this Agreement shall not affect any other provision of this Agreement.

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.

Trade names, Logos

By reason of this agreement or the performance hereof, the subscriber and Cybertrust 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.

9. Notice

You have to notify Cybertrust immediately if there is an error in your certificate. Without reaction from the subscriber with 15 days after receipt, the certificate is deemed accepted.

By accepting the certificate, the customer assumes a duty to retain control of the customer's private key, to use a trustworthy system, and to take reasonable precautions to prevent its loss, disclosure or unauthorized use.

Definitions

Digital Certificate

A collection of electronic data consisting of a Public Key, identifying information about the owner of the Public Key, and validity information, which has been Digitally Signed by Cybertrust. Certified shall refer to the condition of having been issued a valid Digital Certificate by Cybertrust, which Digital Certificate has not been revoked.

Certificate Approver

A specific role defined in the scope of the EV Guidelines of the CA/Browser forum as either an employee or designated agent of the Subscriber who is alleged to be granted the authority to verify that the Certificate Requestor is acting on behalf of the Subscriber and the Subscriber is aware of the Certificate Requestor's

Cybertrust Sureserver EV Subscriber Agreement

actions. Such authority of the Certificate Approver is validated by Cybertrust through direct contact with the Contract Signer during the validation process in a manner consistent with the EV Guidelines in effect at the execution of this agreement.

Certificate Requestor

A specific role defined in the scope of the EV Guidelines of the CA/Browser forum as either an employee or designated agent of the Subscriber who has delivered the EV certificate signing request and completed the corresponding certificate enrollment forms for an EV certificate allegedly acting on behalf of the Applicant and with the Applicant's awareness of the Requestor's actions. Such alleged awareness shall be validated during the validation process in a manner consistent with the EV Guidelines in effect at the execution of this agreement.

Certificate Revocation List ("CRL")

A collection of electronic data containing information concerning revoked Digital Certificates

Certification Authority ("CA")

Cybertrust or an entity which is certified by Cybertrust to issue Digital Certificates to Users in a Digital Certificate Hierarchy Cybertrust is Customer's CA hereunder.

Contract Signer

A specific role defined in the scope of the EV Guidelines of the CA/Browser forum as an employee of the Applicant who has been granted verifiable authority to bind the Applicant into contracts. Such authority will be validated by Cybertrust during the validation process in a manner consistent with the EV Guidelines in effect at the execution of this agreement.

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.

Private Key

A mathematical key which is kept private to the owner and which is used to create Digital Signatures or to decrypt electronic data

Public Key

A mathematical key which is available publicly and which is used to verify Digital Signatures created with the matched Private Key and to encrypt electronic data which can only be decrypted using the matched Private Key.

Secure Server Hierarchy

A collection of CAs and their Certified Users

User

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