Trustwave Subscriber Agreement for Digital Certificates
Ver. 15FEB17

IMPORTANT: PLEASE READ THIS AGREEMENT AND THE TRUSTWAVE CERTIFICATION PRACTICES STATEMENTS ("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@trustwave.com OR CALL US AT 312-873-7500.

THIS TRUSTWAVE SUBSCRIBER AGREEMENT FOR DIGITAL CERTIFICATES ("Agreement") is effective as of the date of the accompanying Certificate (the "Effective Date") between Trustwave Holdings, Inc. ("Trustwave") and the organization receiving the Certificate ("Applicant").

The legal name of the Applicant is _____.

The name of the Contract Signer (as hereinafter defined) duly authorized by the Applicant to bind the Applicant to this Agreement is _____.

Unless agreed otherwise by the parties, each Certificate that Trustwave issues to Applicant shall be governed by this Agreement 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 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")

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

Contract Signer

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

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.

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.

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.

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.

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, Trustwave hereby grants to Applicant 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

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

3. **SERVICES PROVIDED BY TRUSTWAVE**

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

CRL Availability

Use its reasonable efforts to compile, aggregate and make electronically available to all CAs and certified Users in the Secure Server Hierarchy (i) Trustwave's current CRL, and (ii) the CRLs provided by CAs to Trustwave; provided, however, that Trustwave 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 Trustwave.

Revocation Status Services

Use its 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 Trustwave 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 Trustwave.

Revoke Certificates

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

4. **APPLICANT OBLIGATIONS**

User Identification Information

All information provided by Applicant to Trustwave for the purpose of obtaining their Certificate shall be truthful, accurate, and not misleading. If at any time, the name of Applicant contained in the Certificate request provided by Applicant has changed, Applicant shall immediately cease using such Certificate, request that Trustwave revoke such Certificate, and provide Trustwave with such changed information. If at any time, any other significant information, in particular Applicant's organization name, city, state, or country changes from that contained in the Certificate request, Applicant shall request that Trustwave revoke the Certificate. Trustwave agrees that it shall, promptly after revoking Applicant's Certificate at Applicant's request, issue Applicant a new Certificate upon acceptable completion of verification process and payment by Applicant of the then-current applicable fee.

Compromised Certificate

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

Accuracy of Information

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

Protection of Private Key

Applicant hereby agrees and warrants that it (and it 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). Applicant hereby assumes a duty to retain control of Applicant's Private Key, to use a trustworthy system, and to take reasonable precautions to prevent its loss, disclosure or unauthorized use.

Applicant further agrees to generate and protect code signing private keys using one of the following:

1. A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Applicant's private key protection through a TPM key attestation.
2. A hardware crypto module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.
3. Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). Applicant warrants that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

Trustwave shall have the right to audit Applicant's compliance with this requirement provided Trustwave gives Applicant at least 5 days advance written notice. Applicant shall cooperate and comply with Trustwave's requests with respect to said audit.

Applicant further agrees to use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys used for code signing.

Private Key Reuse

Applicant 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

Applicant 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. Applicant is required to notify Trustwave immediately if there is an error in its Certificate.

Reporting and Revocation Upon Compromise

Applicant hereby agrees and warrants that it will promptly cease using a Certificate and its associated Private Key, and promptly request Trustwave 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.

Termination of Use of Certificate

Applicant 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

Applicant 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, Applicant 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 Trustwave 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

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

Sharing of Information

Applicant hereby acknowledges and accepts that if: (a) the Certificate or the Applicant 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 Trustwave is authorized to share information about the Applicant, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.

Acknowledgement and Acceptance:

Applicant acknowledges and agrees that Trustwave shall have the right to modify the Terms of Use or Subscriber Agreement when necessary to comply with any changes in these Requirements or the Baseline Requirements.

Applicant further acknowledges and agrees that Trustwave is entitled to revoke the certificate immediately if Applicant violates the Terms of Use or the Subscriber Agreement.

5. **PERMISSION TO PUBLISH INFORMATION & RECEIVE COMMUNICATIONS**

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

6. **DISCLAIMER OF WARRANTY AND LIMITATION OF LIABILITY**

NO WARRANTIES OF ANY KIND INCLUDING ANY WARRANTY REGARDING MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSED OR ARE TO BE IMPLIED IN THE TRANSACTION EVIDENCED BY THIS AGREEMENT.

IN NO EVENT SHALL TRUSTWAVE BE LIABLE TO THE APPLICANT, SUBSCRIBER, OR ANY OTHER THIRD PARTIES FOR ANY DAMAGES, LOSSES, OR CLAIMS IN EXCESS OF $2,000.

IN NO EVENT SHALL TRUSTWAVE BE LIABLE FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA, OR OTHER INDIRECT, CONSEQUENTIAL OR PUNITIVE DAMAGES ARISING FROM OR IN CONNECTION WITH 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. TRUSTWAVE WILL NOT BE HELD LIABLE IN ANY CIRCUMSTANCE RELATING TO THE APPLICANT BREACHING ITS REPRESENTATIONS OR OBLIGATIONS UNDER SECTION 4 OF THIS AGREEMENT.

7. **TERM AND TERMINATION**

i. This Agreement shall terminate on the earliest of:

a. The expiration date of the Certificate issued; or

b. Failure by Applicant to perform any of its material obligations under this Agreement if such breach is not cured within fifteen (15) days after receipt of notice thereof from Trustwave.

ii. Termination of this Agreement shall not affect your obligation to pay for the Certificate(s).

8. **EFFECT OF TERMINATION**

Upon termination of this Agreement for any reason, Applicant's Certificate shall be revoked by Trustwave in accordance with Trustwave's procedures then in effect. Upon revocation of Applicant's Certificate for any reason, all authority granted to Applicant 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 Applicant's Certificate shall be assignable by Applicant. Any such purported assignment or delegation shall be void and of no effect and shall permit Trustwave to terminate this Agreement. Trustwave may assign this Agreement to its parent company, wholly-owned subsidiary or as a result of a merger, acquisition, sale, transfer or other disposition of all or substantially all of its assets.

Issuance Disclaimer

Notwithstanding anything herein to the contrary, if Applicant 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, Trustwave shall have no obligation to issue such Certificate(s). Furthermore, the terms under this section shall not affect the Applicant’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 Applicant desires or is required to give any notice, demand, or request to Trustwave 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 Trustwave, Attn. Legal Department, 70 W. Madison St., Suite 1050, Chicago, IL 60602. Such communications shall be effective when they are received.

Trade Names, Logos

By reason of this Agreement or the performance hereof, Applicant and Trustwave 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, Trustwave's Websites, or any Certificate issued by Trustwave 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 Trustwave 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 Trustwave wishes to have the Trustwave 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, Applicant 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 Applicant 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.

Signature _____

Name _____

Title _____

Date _____