GlobalSign Subscriber Agreement - Version 3.8

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, CANCEL YOUR ORDER WITHIN SEVEN (7) DAYS OF THE AVAILABILITY OF THE CERTIFICATE FOR A FULL REFUND. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT legal@globalsign.com

This GlobalSign Subscriber Agreement (the "Agreement") between GlobalSign and the Applicant or Subscriber is effective as of the date of the application for the Certificate (the "Effective Date").

1.0 Definitions and Incorporation by Reference

The following definitions are used in this Agreement:

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

Application Software Supplier: A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.

Authority Information Access: A Certificate extension that indicates how to access information and services for the issuer of the Certificate in which the extension appears.

CA/Browser Forum: An industry expert group of CA's and Application Software Suppliers. Details are available from www.cabforum.org.

Certificate: An electronic document that uses a Digital Signature to bind a Public Key and an identity.

Certificate Beneficiaries: The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom GlobalSign has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier, and all Relying Parties who reasonably rely on a Valid Certificate.

Certificate Custodian: A nominated individual responsible for the lifecycle of the Certificate. This may or may not be the same entity as the Subscriber.

Certificate Request: Communications described in Section 10.2 of the CA/Browser Forum Baseline Requirements for the Issuance of Publicly-Trusted Certificates (the "Baseline Requirements") requesting the issuance of a Certificate.

Certificate Requester: Applicant's representative who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits Certificate Requests on behalf of the Applicant. Certificate Requesters can be pre-approved via the functionality of a GlobalSign managed service such as MSSL or EPKI.

Certificate Revocation List ("CRL"): A regularly updated timestamped list of revoked Certificates that is created and Digitally Signed by the CA that issued the Certificates.

Certification Authority ("CA"): An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs. GlobalSign or an entity which is certified by GlobalSign to issue the Certificate to the "Subject". GlobalSign is Applicant's CA hereunder.

Digital Signature: To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made. Digitally Signed shall refer to electronic data to which a Digital Signature has been appended.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Name System: An Internet service that translates Domain Names into IP addresses.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

GlobalSign: The GlobalSign entity with which the Subscriber placed an order to purchase the Certificate, either GMO GlobalSign Limited, GMO GlobalSign, Inc., GMO GlobalSign Pte. Ltd, GMO GlobalSign Certificate Services Pvt. Ltd or GMO GlobalSign Russia LLC.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

North American Energy Standards Board ("NAESB") Accreditation Requirements for Authorized Certification Authorities ("NAESB Accreditation Specification"): The technical and

management details which a Certification Authority is required to meet in order to be accredited as an Authorized Certification Authority ("ACA") by NAESB.

Online Certificate Status Protocol ("OCSP"): An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate.

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.

Registration Authority ("RA"): Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such supplier merely displays information relating to a Certificate.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

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 or detection, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes. **Terms of Use:** Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

The following policies and associated guidelines are incorporated by reference into this Agreement:

- the GlobalSign Certification Practice Statement ("CPS"). The current version of the CPS is located at http://www.globalsign.com/repository; and
- the Baseline Requirements.

2.0 Authority to Use Certificates

2.1 Grant of Authority: From the Effective Date and for the term set forth within the validity period of any issued Certificate ("Valid from" date to "Valid to" date), GlobalSign hereby grants to the Subscriber the authority to use the Certificate in conjunction with Private Key and/or Public Key operations. The obligations of the Subscriber in section 4.0 with respect to Private Key protection are applicable from the Effective Date.

2.2 Limitations on Authority: The Subscriber shall use the Certificate only in connection with properly licensed cryptographic software.

3.0 Services Provided by GlobalSign

After acceptance of this Agreement and payment of applicable fees, in addition to the "Grant of Authority", GlobalSign or a third party provider designated by GlobalSign shall provide the following services from the point of issuance of the Certificate.

3.1 Provision of Certificate Revocation Lists (CRL), Online Certificate Status Protocol (OCSP) Services and Certificate Issuing Authority Details: GlobalSign shall use reasonable efforts to compile, aggregate and make electronically available for all Certificates signed and issued by GlobalSign's CA:

- CRLs for any Certificate containing a CRL Certificate distribution point;
- OCSP responders for any Certificates containing an OCSP responder URL, and
- Issuing Certificate information from the Authority Information Access locations; provided, however that GlobalSign 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 GlobalSign.

3.2 Revocation Services for Certificates: Revocation of a Subscriber Certificate shall be performed by GlobalSign within twenty-four (24) hours under the following circumstances:

- The Subscriber requests in writing to the GlobalSign entity which provided the Certificate that the Subscriber wishes to revoke the Certificate;
- The Subscriber notifies GlobalSign that the original Certificate Request was not authorized and does not retroactively grant authorization;
- GlobalSign obtains reasonable evidence that there has been a Key Compromise of the Subscriber's Private Key , no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, or that the Certificate has otherwise been misused;
- GlobalSign receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under this Subscriber Agreement or Terms of Use;
- GlobalSign is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- GlobalSign is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- GlobalSign receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
- GlobalSign is made aware that the Certificate was not issued in accordance with the Baseline Requirements or GlobalSign's CP or this CPS;

- If GlobalSign determines that any of the information appearing in the Certificate is not accurate or is misleading;
- GlobalSign ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
- GlobalSign's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless GlobalSign has made arrangements to continue maintaining the CRL/OCSP Repository;
- GlobalSign is made aware of a possible Key Compromise of the Subordinate CA used for issuing the Certificate;
- Revocation is required by GlobalSign's CP and/or CPS;
- The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time); or
- GlobalSign is made aware that the Certificate was used to sign malicious software or "malware".

Revocation of a Subscriber Certificate may also be performed by GlobalSign within a commercially reasonable period of time under the following circumstances:

- The Subscriber or organization administrator requests revocation of the Certificate through a GCC account which controls the lifecycle of the Certificate;
- The Subscriber requests revocation through an authenticated request to GlobalSign's support team or GlobalSign's Registration Authority;
- GlobalSign receives notice or otherwise become aware that the Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of GlobalSign's jurisdiction of operation;
- GlobalSign determines, in its sole discretion, that the use of the Certificate may compromise the security, reputation or trust status of the GlobalSign CA or GlobalSign;
- Following a request for cancellation of a Certificate;
- If a Certificate has been reissued, GlobalSign may revoke the previously issued Certificate;
- Under certain licensing arrangements, GlobalSign may revoke Certificates following expiration or termination of the applicable license agreement;
- GlobalSign determines the continued use of the Certificate is otherwise harmful to the business of GlobalSign or third parties When considering whether Certificate usage is harmful to GlobalSign's or a third party's business or reputation, GlobalSign will consider, among other things, the nature and number of complaints received; the identity of the complainant(s); relevant legislation in force; response to the alleged harmful use by the Subscriber;
- If Microsoft, in its sole discretion, identifies a Code Signing or EV Code Signing Certificate as either containing a deceptive name or as being used to promote malware or unwanted software, Microsoft will contact GlobalSign and request that it revoke the Certificate. GlobalSign will either revoke the Certificate within a commercially-reasonable timeframe, or request an exception from Microsoft within two (2) business days of receiving Microsoft's request. Microsoft may either grant or deny the exception at its sole discretion. In the event that Microsoft does not grant the exception, GlobalSign will revoke the Certificate within a commercially-reasonable timeframe not to exceed two (2) business days; or
- If Microsoft, it its sole discretion, identifies an SSL or Code Signing Certificate is being used to promote malware or unwanted software, Microsoft will contact GlobalSign and request that it revoke the Certificate. GlobalSign will either revoke the Certificate within a commercially-reasonable timeframe, or request an exception from Microsoft within two (2) business days of receiving Microsoft's request. Microsoft may either grant or deny the exception at its sole discretion. In the event that Microsoft does not grant the exception, GlobalSign will revoke the Certificate within a commercially-reasonable timeframe not to exceed two (2) business days.

3.3 Key Generation: If Key Pairs are generated by GlobalSign on behalf of the Subscriber offered as Token, PKCS#12 or AutoCSR options, GlobalSign will endeavor to use trustworthy systems in order to generate such Key Pairs, in which case, the following terms also apply. GlobalSign does not generate Key Pairs for publicly trusted SSL certificates:

- GlobalSign will generate Key Pairs using a platform recognized as being fit for such purpose and will ensure that Private Keys are encrypted if transported to the Subscriber,
- GlobalSign will use a key length and algorithm which is recognized as being fit for the purpose of Digital Signature, and
- In the case of both Code Signing and EV Code Signing Certificates, Subscriber acknowledges that GlobalSign will not sign Key Pairs that are smaller than 2048 bits and, in the case of EV Code Signing, will offer SHA2 as the only option for the signature algorithm.

3.4 Site Seal Services for SSL/TLS Certificates and OCSP/CRL Responses: GlobalSign permits the Applicant to make use of GlobalSign's site seal on the Applicant's web site with a maximum daily rate of five hundred thousand (500,000) impressions per day. GlobalSign reserves the right to limit or stop the availability of the seal if this limit is exceeded.

GlobalSign provides a 24x7 service to check the validity of an issued Certificate either through an OCSP responder or CRL. A maximum daily rate of five hundred thousand (500,000) validations per Certificate per day is set. GlobalSign reserves the right to enforce OCSP stapling if this limit is exceeded.

3.5 Timestamping Services for Code Signing Certificate: GlobalSign offers the ability to timestamp code signed with a Code Signing Certificate as a non-chargeable service provided the service is used reasonably. As a best practice, GlobalSign requests that Subscriber timestamp the digital signature after signing his/her code. GlobalSign establishes a limit of a reasonable number of timestamps for the validity period of the Code Signing Certificate and reserves the right to withdraw the service or charge additional fees for the service where the volume of timestamps is deemed excessive by GlobalSign.

3.6 Time stamping Services for PDF Signing for Adobe CDS Certificate: GlobalSign offers the ability to timestamp Portable Document Format (PDF) documents as a paid GlobalSign service. The number of signatures per year allowed by this service is established during the application process. GlobalSign reserves the right to withdraw the service or charge additional fees for the service where the volume of time stamps is in excess of the agreed limit.

3.7 Time stamping Services for Adobe Authorized Trust List (AATL) Certificate: GlobalSign may offer the ability to timestamp Portable Document Format (PDF) and Microsoft Office documents as a paid GlobalSign service. The number of signatures per year allowed by this service is established during the application process. GlobalSign reserves the right to withdraw the service or charge additional fees for the service where the volume of time stamps is in excess of the agreed limit.

4.0 Subscriber's Obligations and Warranties

Subscriber and/or Applicant warrants for the benefit of GlobalSign and the Certificate Beneficiaries that:

4.1 Accuracy of Information: Subscriber will provide accurate, complete and truthful information at all times to GlobalSign, both in the Certificate Request and as otherwise requested by GlobalSign in connection with issuance of a Certificate, including but not limited to, the application name, information URL and application description in relation to EV Code Signing Certificates.

4.2 Protection of Private Key: Applicant shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key to be included in the requested Certificate(s) and any associated activation data or device, e.g. password or token. For Code Signing Certificates, the Subscriber will provide adequate network and other security controls to protect against misuse of the Private Key and that GlobalSign will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys. .

4.3 Private Key Reuse: For Code Signing Certificates, the Applicant/Subscriber shall 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.

4.4 Prevention of Misuse: For Code Signing Certificates, the Subscriber will provide adequate network and other security controls to protect against misuse of the Private Key and that GlobalSign will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys.4.3

4.5 Acceptance of Certificate: Subscriber shall not use the Certificates until after Applicant, or an agent of Applicant, has reviewed and verified the Certificate contents for accuracy.

4.6 Use; Restrictions: Subscriber shall install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.

In the event a Certificate is used to sign a PDF, the Subscriber shall maintain information that permits a determination of who approved the signature of a particular document.

Under no circumstances must the Certificate be used for criminal activities such as phishing attacks, fraud, certifying or signing malware. Subscriber should not use a Certificate to knowingly sign software that contains Suspect Code or otherwise distribute content that has the effect of misleading, inconveniencing or annoying the recipient such as software that includes unwelcome features or programs not disclosed appropriately to the user prior to installation, or is recognized as unwelcome or suspicious by commercial anti-virus scanning applications.

Subscriber also accepts these additional obligations and warrants to use the EV Code Signing Certificate:

- Only to sign code that complies with the requirements set forth in the latest version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates;
- Solely in compliance with all applicable laws;
- Solely for authorized company business; and
- Solely in accordance with this Agreement.

If Subscriber becomes aware (by whatever means) that it has signed code that contains malicious software or a serious vulnerability, the Subscriber must immediately inform GlobalSign.

Subscriber acknowledges that Microsoft may independently determine that a Certificate is malicious or there has been a Key Compromise, and Microsoft services and applications may have the ability to modify Microsoft customer experiences to reflect Microsoft's determination without notice and without regard to the revocation status of the Certificate.

4.7 Reporting and Revocation: Subscriber shall promptly cease using a Certificate and its associated Private Key and promptly request that the CA revoke the Certificate if the Subscriber believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused or compromised, or (c) in the case of a Code Signing Certificate, if there is evidence that the Certificate was used to sign Suspect Code.

4.8 Termination of Use of Certificate: Subscriber shall promptly cease use of the Private Key associated with the Public Key in the Certificate upon expiration or revocation of the Certificate.

4.9 Responsiveness: Subscriber shall respond to GlobalSign's instructions concerning Key Compromise or Certificate misuse within forty-eight (48) hours.

4.10 Acknowledgement and Acceptance: Subscriber acknowledges and accepts that GlobalSign is entitled to revoke the Certificate immediately if the Applicant violates the terms of the Subscriber Agreement or if GlobalSign discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

With respect to EV Code Signing Certificates used in connection with Microsoft services and applications, Subscriber further acknowledges that even though an EV Code Signing Certificate may not be revoked by GlobalSign Microsoft may independently determine that the Certificate is malicious or compromised and modify the Microsoft customer experience in the applicable Microsoft services and applications to reflect Microsoft's determination without notice and without regard to the revocation status of the Certificate.

4.11 Sharing of Information: With respect to Code Signing Certificates, Subscriber 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 Key Compromise, discovery of malware, etc.), then the CA 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.

4.12 Compliance with Industry Standards: Subscriber acknowledges and accepts that the GlobalSign may modify the Subscriber Agreement when necessary to comply with any changes in the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, published at https://aka.ms/csbr or the Baseline Requirements.

4.13 Domain Control for SSL/TLS Digital Certificate: The Subscriber acknowledges and asserts that s/he has control of the domain(s) or IP Address listed in the SubjectAltName(s) for which s/he is applying for the SSL/TLS Certificate. Should control cease for any domain(s), the Subscriber acknowledges that s/he must promptly inform GlobalSign in accordance with the obligations of the 'Reporting and Revocation' section below.

4.14 E-mail Control for PersonalSign Digital Certificate: The Subscriber acknowledges and asserts that s/he have control of the e-mail address for which they are applying for a PersonalSign Certificate. Should control cease for any e-mail address(s), the Subscriber acknowledges that s/he must promptly inform GlobalSign in accordance with the obligations of the 'Reporting and Revocation' section below.

4.15 Key Generation and Usage

Where Key Pairs are generated by the Subscriber or the Certificate Requester, trustworthy systems must be used in order to generate Key Pairs, in which case, the following terms also apply:

- Key Pairs must be generated using a platform recognized as being fit for such purpose. In the case of PDF Signing for Adobe CDS, AATL secure email and document signing, and EV Code Signing, this must be FIPS 140-2 Level 2 compliant,
- A key length and algorithm must be used which is recognized as being fit for the purpose of Digital Signature, and
- The Subscriber shall ensure that the Public Key submitted to the GlobalSign correctly corresponds to the Private Key used.

Where Key Pairs are generated in hardware (as required by the CPS):

- The Subscriber must maintain processes, including, without limitation, changing of activation data, that assure that each Private Key within a hardware security module (HSM) or token can be used only with the knowledge and explicit action of the "Certificate Custodian",
- The Subscriber must ensure that the Certificate Custodian has received security training appropriate for e purposes for which the Certificate is issued, and
- Certificate Custodians undertake 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 Certificate as well as any associated authentication mechanism to access the key - e.g., password to a token or HSM.
- For Code Signing Certificates, Subscriber must use one of the following methods to generate and protect their Code Signing Certificate Private Keys. GlobalSign recommends Subscriber use method 1 or 2 over method 3:

  1. A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Subscriber'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+).

  The Subscriber also warrants that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

- For Qualified Certificates, Subscriber keys must be generated and stored within a certified Qualified Signature Creation Device (QSCD) that meets the requirements laid down in Annex II of Regulation (EU) No 910/2014. The Subscriber agrees to use the Certificate only within a QSCD which has either been supplied or approved in writing by GlobalSign and the QSCD certification status must be monitored by the Subscriber and appropriate measures must be taken if the certification status of the QSCD changes.

4.16 NAESB Certificates

Subscribers for NAESB Certificates acknowledge their understanding of the following obligations of the NAESB Wholesale Electric Quadrant Business Practice Standards WEQ-012 (the "WEQ PKI Standards"):

Subscribers participating in the WEQ PKI Standards shall be required to be registered in the NAESB EIR and furnish proof that they are an entity authorized to engage in the wholesale electricity industry. Entities or organizations that may require access to applications using authentication specified under the

WEQ PKI Standards, but do not qualify as a wholesale electricity market participant (e.g., regulatory agencies, universities, consulting firms, etc.) must register.

Registered end entities and the user community they represent shall be required to meet to all end entity obligations in the WEQ PKI Standards.

Subscriber organization certifies to GlobalSign that it has reviewed and acknowledges the following WEQ PKI Standards:

4.16.1. Subscriber acknowledges the electric industry's need for secure private electronic communications that facilitate the following purposes:

- Privacy: The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended;
- Authentication: The assurance to one entity that another entity is who he/she/it claims to be;
- Integrity: The assurance to an entity that data has not been altered (intentionally or unintentionally) between "there" and "here," or between "then" and "now"; and
- Non-Repudiation: A party cannot deny having engaged in the transaction or having sent the electronic message.

4.16.2. Subscriber acknowledges the industry's endorsement of Public Key cryptography which utilizes Certificates to bind a person's or computer system's Public Key to its entity and to support symmetric encryption key exchange.

4.16.3 Subscriber has reviewed the WEQ PKI Standards with respect to industry guidelines for establishing a trusted PKI.

4.16.4. Subscriber has evaluated GlobalSign's CPS in light of those industry standards.

If applicable, Subscribers shall be obligated to register their legal business identification and secure an "Entity Code" that will be published in the NAESB EIR and used in all Subscriber applications submitted by, and Certificates issued to, that end entity. In complying with the WEQ-012 requirements, when issuing Certificates for use within the energy industry for other than WEQ-012 applications, ACAs must comply with the provisions of the WEQ PKI Standards, except provisions in WEQ-012.12.1.9, WEQ-012-1.3.3, and WEQ-012.1.4.3, which require end entity registration within the NAESB EIR.

Subscribers shall also be required to comply with the following requirements:

- Protect their Private Keys from access by other parties.
- If applicable, identify, through the NAESB EIR, that they have selected GlobalSign to use as their ACA.
- Execute all agreements and contracts with GlobalSign necessary for GlobalSign to issue Certificates to the end entity for use in securing electronic communications.
- Comply with all obligations required and stipulated by GlobalSign in its CPS, e.g., Certificate application procedures, Applicant identity proofing/verification, and Certificate management practices.
- Confirm that it has a Certificate management program, has trained all affected employees in that program, and has established controls to ensure compliance with that program. This program shall include, but is not limited to:
- Certificate Private Key security and handling policy(ies)
- Certificate revocation policy(ies)

- Identify the type of Subscriber (I.e., individual, role, device or application) and provide complete and accurate information for each Certificate Request.

5.0 Consent to Publish Information

By providing personal information when applying for a Certificate, Subscriber consents to GlobalSign's disclosure of this information publicly by (i) embedding the information in issued the Certificate and (ii) publishing the Certificate in Certificate Transparency (CT) logs.

6.0 GlobalSign Limited Warranty

EXCEPT TO THE EXTENT PROHIBITED BY LAW OR AS OTHERWISE PROVIDED HEREIN, GLOBALSIGN DISCLAIMS ALL WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

TO THE EXTENT GLOBALSIGN HAS ISSUED AND MANAGED THE CERTIFICATE IN ACCORDANCE WITH THE BASELINE REQUIREMENTS AND THE CPS, GLOBALSIGN SHALL NOT BE LIABLE TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY LOSSES SUFFERED AS A RESULT OF USE OR RELIANCE ON SUCH CERTIFICATE. OTHERWISE, GLOBALSIGN'S LIABILITY TO THE SUBSCRIBER, RELYING PARTY OR ANY THIRD PARTIES FOR ANY SUCH LOSSES SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS ($1,000) PER CERTIFICATE; PROVIDED HOWEVER THAT THE LIMITATION SHALL BE TWO THOUSAND DOLLARS ($2,000) PER CERTIFICATE FOR AN EV CERTIFICATE OR AN EV CODE SIGNING CERTIFICATE.

THIS LIABILITY CAP LIMITS DAMAGES RECOVERABLE OUTSIDE OF THE CONTEXT OF THE GLOBALSIGN WARRANTY POLICY. AMOUNTS PAID UNDER THE WARRANTY POLICY ARE SUBJECT TO THEIR OWN LIABILITY CAPS.

IN NO EVENT SHALL GLOBALSIGN SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, 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, RELIANCE UPON, LICENSE, PERFORMANCE OR NON PERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS CPS.

THIS LIABILITY LIMITATION SHALL BE THE SAME REGARDLESS OF THE NUMBER OF DIGITAL SIGNATURES, TRANSACTIONS, OR CLAIMS RELATED TO SUCH CERTIFICATE.

7.0 Term and Termination

This Agreement shall terminate upon the earliest of:

- The expiration date of the Certificate issued to the Subscriber either directly, indirectly or through a MSSL or ePKI service that has not yet expired; or
- Failure by the Subscriber to perform any of its material obligations under this Agreement if such breach is not cured within five (5) days after receipt of notice thereof from GlobalSign.

8.0 Effect of Termination

Upon termination of this Agreement for any reason, GlobalSign may revoke the Subscriber's Certificate in accordance with GlobalSign procedures. Upon revocation of the Subscriber's Certificate, 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.

9.0 Miscellaneous Provisions

9.1 Governing

If you placed your order with GMO GlobalSign Limited, this Agreement shall be governed by, construed under and interpreted in accordance with the laws of England and Wales without regard to its conflict of law provisions. Venue shall be in the courts of England.

If you placed your order with GMO GlobalSign, Inc., this Agreement shall be governed by, construed under and interpreted in accordance with the laws of the State of New Hampshire U.S.A. without regard to its conflict of law provisions. Venue shall be in the courts of the New Hampshire State.

If you placed your order with GMO GlobalSign Pte. Ltd., this Agreement shall be governed by, construed under and interpreted in accordance with the laws of Singapore without regard to its conflict of law provisions. Venue shall be in the courts of Singapore.

If you placed your order with GMO GlobalSign Certificate Services Pvt. Ltd, this Agreement shall be governed by, construed under and interpreted in accordance with the laws of India and the related State laws without regard to its conflict of law provisions. Venue shall be in the courts of India.

If you placed your order with GMO GlobalSign Russia LLC, this Agreement shall be governed by, construed under and interpreted in accordance with the law of Russian Federation without regard to its conflict of law provisions. Venue shall be in the courts of Russian Federation.

9.2 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 not the Subscriber's rights in the Certificate shall be assignable by the Subscriber. Any such purported assignment or delegation shall be void and of no effect and shall permit GlobalSign to terminate this Agreement.

9.3 Entire Agreement

This Agreement, along with all documents referenced herein, any product or service agreement, and the reseller agreement (if you are a reseller) constitute the entire agreement between the parties and supersedes any prior oral or written agreements, commitments, understandings, or communications with respect to the subject matter of this Agreement.

9.4 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.

9.5 Notices

Whenever Subscriber desires or is required to give any notice, demand, or request to GlobalSign 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 GlobalSign at one of our International offices as listed at http://www.globalsign.com/company/contact.htm, Attention: Legal Department. Such communications shall be effective when they are received.

9.6 Privacy; Use of third party databases

GlobalSign shall follow the privacy policy posted on its website when receiving and using information from Subscriber. GlobalSign may amend the privacy policy at any time by posting the amended privacy policy on its website.

By providing personal information when applying for a Certificate, Subscriber consents to GlobalSign's processing, disclosure and transfer of this information on a global basis to its affiliates, agents and subcontractors as necessary to validate and issue a Certificate, including processing, disclosure and transfer to countries that may have data protection laws that are less protective than those in the country where Subscriber is located.

For natural persons, GlobalSign may validate items such as name, address and other personal information supplied during the application process against appropriate third party databases. By entering into this Agreement, the Subscriber consents to such checks being made. In performing these checks, personal information provided by the Subscriber may be disclosed to registered credit reference agencies, which may keep a record of that information. Such check is done only to confirm identity, and as such, a credit check is not performed. The Subscriber's credit rating will not be affected by this process.

If you placed your order with GMO GlobalSign Russia LLC, GlobalSign may, for natural persons, validate items such as name, address and other personal information supplied during the application. By entering into this Agreement, the Subscriber consents to their personal data being processed by GlobalSign in the following ways: collecting, classifying, processing, storing, editing, using, depersonalizing, blocking and deleting, as stated by Russian Federal Law FZ-No.152 at 27.07.2006, as well as transferring to third parties in cases established by regulations of the higher authorities and the law.

9.7 Trade Names, Logos

By reason of this Agreement or the performance hereof, Subscriber and GlobalSign 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.

10.0 Customer Support

The Subscriber must notify GlobalSign through any of our international offices listed on http://www.globalsign.com/company/contact.htm immediately if there is an error in the Certificate. If Subscriber fails to do so within seven (7) days from receipt, the Certificate shall be deemed accepted.

GlobalSign shall provide refunds pursuant to the "GlobalSign Refund Policy" published at http://www.globalsign.com/repository/

[V 3.8 6-15-18]