GlobalSign Subscriber Agreement - Digital Certificates and Services - Version 2.4

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

This GlobalSign Subscriber Agreement ("Agreement") is effective as of the date of the application for the Digital Certificate (the "Effective Date") between GlobalSign ("GlobalSign"), and the applicant receiving the Digital Certificate ("Subscriber"). "GlobalSign", the contractual party hereto, is either GMO GlobalSign Limited, GMO GlobalSign, Inc., or GMO GlobalSign Pte. Ltd; the GlobalSign entity to which the Subscriber placed an order to purchase the Digital Certificate.

1.0 Definitions and incorporation by reference
The following definitions are used throughout this agreement

- **Applicant:** The private organization, business entity, government entity, international body or individual that applies for (or seeks renewal of) a Digital Certificate naming it as the "Subject".
- **Applicant Representative:** A natural person employed by or an agent of the Applicant acting with the express authority of the Applicant:
- **CA/Browser Forum:** - An industry expert group of CA's and Software Application Providers. Details are available from www.cabfoum.org
- **Certificate Approver:** Applicant's representative who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve Certificate Requests submitted by other Certificate Requesters.
- **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 Managed Service such as MSSL or ePKI.
- **Certificate Revocation List ("CRL"):** A collection of electronic data containing information concerning revoked Digital Certificates
- **Certification Authority ("CA"):** GlobalSign or an entity which is certified by GlobalSign to issue the Digital Certificate to the "Subject". GlobalSign is Applicant's CA hereunder.
- **Contract Signer:** Applicant's representative that may sign and submit a Subscriber Agreement or other service agreement.
- **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 GlobalSign. Certified shall refer to the condition of having been issued a valid Digital Certificate by GlobalSign, which Digital Certificate has not been revoked.
- **Digital Certificate Custodian:** A nominated individual responsible for the lifecycle of the Digital Certificate. This may or may not be the same entity as the Subscriber
- **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.

- **North American Energy Standards Board (NAESB)** Public Key Infrastructure (PKI) Standards – WEQ-012 v3.0 and NAESB Accreditation Requirements for Authorized Certification Authorities. 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 Internet Protocol (IP) used for obtaining the real time revocation status of a digital certificate.
- **OneClickSSL™ Plug-In:** A software application designed and developed to facilitate the request for and installation of SSL/TLS certificates whilst demonstrating the control of a domain.
- **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.
- **Registration Authority ("RA"):** Any entity that is responsible for identification and authentication of the "Subject" in whole or in part to which certificates may subsequently be issued.
- **Subscriber:** The entity responsible for the management of the lifecycle of the digital certificate and any associated public-private keys and the target of this agreement.

The following Certification Practice statements ("CPS") and associated guidelines are included by reference:
- GlobalSign CPS for GlobalSign Products: GlobalSign's CPS is incorporated into this agreement. The latest CPS is located at http://www.globalsign.com/repository
- CA/Browser Forum Base Requirements for the issuance of publically trusted certificates

2.0 Authority to Use Digital Certificates

2.1 Grant of Authority
As from the Effective Date and for the term set forth within the validly period of any issued Digital Certificate ("Valid from" date to "Valid to" date), GlobalSign hereby grants to the Subscriber the authority to use the requested Digital 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 requested Digital Certificate only in connection with properly licensed cryptographic software. Digital Certificate may only be installed on physical servers or systems as prescribed and specified during the enrolment process.

3.0 Services Provided by GlobalSign
After execution of this agreement and payment of all applicable fees, in addition to the "grant of authority", GlobalSign or a third party provider designated by GlobalSign shall provide the following services to the Subscriber from the point of issuance of the Digital 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 Digital Certificate signed and issued by a GlobalSign's CA:
- CRLs for any Digital Certificate containing a CRL Certificate Distribution Point,

- OCSP responders for any certificates containing an OCSP responder URL, and
- Issuing Digital 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 Digital Certificates

3.2.1 GlobalSign will revoke the Digital Certificate it has issued upon the occurrence of any of the following events:

- The Subscriber requests revocation of the Digital Certificate through a GlobalSign Certificate Centre (GCC) account which controls the lifecycle of the Digital Certificate,
- The Subscriber requests revocation of the Digital Certificate via a OneClickSSL revocation workflow process,
- The Subscriber requests revocation through an authenticated request to GlobalSign's Support team or GlobalSign Registration Authority,
- GlobalSign obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has been compromised, created using a weak algorithm, or that the Digital Certificate has otherwise been misused,
- GlobalSign receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement,
- GlobalSign receives notice or otherwise becomes aware that a Subscriber uses the certificate for criminal activities such as phishing attacks, fraud, certifying or signing malware etc.,
- GlobalSign receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use any of the elements within the "Subject" or "Subject Alternative Name" of the Digital Certificate, or that the Subscriber has failed to renew or maintain control of any of those elements,
- GlobalSign receives notice or otherwise becomes aware of a material change in the information contained in the Digital Certificate,
- A determination, in GlobalSign's sole discretion, that the Digital Certificate was not issued according to best practice or any of GlobalSign own published policies,
- If GlobalSign determines that any of the information appearing in the Digital Certificate is not accurate,
- GlobalSign ceases operations for any reason and has not arranged for another CA to provide revocation support for the Digital Certificate,
- GlobalSign's right to issue Digital Certificate expires or is revoked or terminated,
- GlobalSign's Private Key for the relevant issuing CA Certificate is compromised,
- GlobalSign receives notice or otherwise become aware that a 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,
- The continued use of the certificate is harmful to the business of GlobalSign and relying parties.

3.2.2 When considering whether certificate usage is harmful to GlobalSign, GlobalSign considers, among other things, the following:

- The nature and number of complaints received,
- The identity of the complainant(s),
- Relevant legislation in force, and
- Responses to the alleged harmful use from the Subscriber.

3.3 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 500,000 [five-hundred-thousand] impressions per day. GlobalSign maintains 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 500,000 [five-hundred-thousand] validations per certificate per day is set. GlobalSign maintains the right to enforce OCSP stapling if this limit is exceeded.

3.4 Time-stamping Services for CodeSigning Digital Certificate

GlobalSign offers the ability to timestamp code signed with its CodeSigning Digital Certificate as a non chargeable service when used reasonably. A reasonable limit of 50 timestamp operations per month for the duration of the certificate is set. GlobalSign withholds the right to withdraw the service or charge for the service where the volume of time stamping operations performed is in excess of this limit.

3.5 Time-stamping Services for PDF Signing for Adobe CDS Digital 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 agreed during the application process. GlobalSign withholds the right to withdraw the service or charge additional fees for the service where the volume of time stamping operations performed is in excess of the agreed limit.

4.0 Subscriber's Obligations

This Subscriber Agreement specifically names Microsoft as an express third-party beneficiary for Code Signing and Extended Validation Code Signing certificates.
The Subscriber warrants and covenants the following to GlobalSign and 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 Suppliers and all beneficiaries of the Digital Certificate who reasonably rely on a valid certificate including:

4.1 Exclusive Domain Control for SSL/TLS Digital Certificate

The Subscriber acknowledges and asserts that they have exclusive control of the domain(s) or IP Address listed in the SubjectAltName(s) for which they are applying for the SSL/TLS Digital Certificate. Should exclusive control cease for any domain(s), the subscriber acknowledges that they will promptly inform GlobalSign in accordance with the obligations of the 'Reporting and Revocation' section below.

4.2 Exclusive e-mail Control for PersonalSign Digital Certificate

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

4.3 Data Accuracy

The Subscriber undertakes to provide accurate and complete information at all times to GlobalSign or any GlobalSign RA. The Subscriber shall refrain from submitting to GlobalSign or any GlobalSign RA any material that contains statements that violate any law or the rights of any party. This includes no misleading information within the Subject:organizationalUnitName attribute.

4.4 Key Generation and Usage

4.4.1 Where keys are generated by the Subscriber or the Certificate Requester, trustworthy systems must be used in order to generate public-private key pairs, in which case, the following terms also apply:

- Keys must be generated using a platform recognized as being fit for purpose. In the case of PDF Signing for Adobe CDS 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 purpose for Digital Signature,
- The Subscriber shall ensure that the Public Key submitted to the GlobalSign CA correctly corresponds to the Private Key used,
- The Subscriber shall exercise appropriate and reasonable care to avoid unauthorized use of its Private Key.

4.4.2 Where keys are generated by GlobalSign on behalf of the Subscriber offered as PKCS#12 or AutoCSR options, or OneClickSSL Plug-In is installed and executed by the Subscriber, then GlobalSign will endeavor to use trustworthy systems in order to generate public-private key pairs, in which case, the following terms also apply:

- GlobalSign will generate keys using a platform recognized as being fit for purpose and will ensure that keys are encrypted if transported to the Subscriber,
- GlobalSign will use a key length and algorithm which is recognized as being fit for purpose for Digital Signature.

4.4.3 Where keys are generated in hardware as required by the applicable CPS:

- The Subscriber maintains processes, including, without limitation, changing of activation data, that assure that each Private Key within a HSM or token can be used only with the knowledge and explicit action of only one human being within the organization (the "Digital Certificate Custodian"),
- The Subscriber ensures that the Digital Certificate Custodian has received security training appropriate for the purposes for which the Digital Certificate is issued,
- All parties 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 Digital Certificate as well as any associated authentication mechanism to access the key - e.g., password to a token or Hardware Security Module.

4.5 Use of GlobalSign Digital Certificate

The Subscriber shall install the Digital Certificate only on the platform, which corresponds to the agreed certificate as highlighted in the appropriate Certificate Policy and to use the GlobalSign certificate solely in compliance with all applicable laws, solely up to contracted platform licenses, solely for authorized company business, and solely in accordance with this subscriber agreement. In the event of a Digital Certificate that is used to sign a PDF, the Subscriber shall maintain information that permits a determination of who approved the signature of a particular document.

In the case of EV Code Signing certificates, Subscriber accepts additional obligations and warranties to not knowingly sign software that contains Suspect Code and use the EV code Signing Certificate as follows:

a) Only to sign code that complies with the requirements set forth in the CA/Browser Forum : Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates V1.1.
b) Solely in compliance with all applicable laws
c) Solely for authorized company business; and
d) Solely in accordance with this Subscriber Agreement

4.6 Acceptance of a Digital Certificate

The Subscriber shall not use the Digital Certificate until it has reviewed and verified the accuracy of the data incorporated into the Digital Certificate.

4.7 Reporting and Revocation

4.7.1 The Subscriber undertakes to promptly cease using the Digital Certificate and its associated Private Key, and promptly request GlobalSign to revoke the Digital Certificate, in the event that:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key of the certificate's "Subject",
- The Subscriber indicates that the original Certificate Signing Request (CSR) was not authorized and does not retroactively grant authorization,
- The Subscriber has breached a material obligation of the CPS,
- The Subscriber requests in writing that the CA revoke the certificate (or uses an agreed mechanism to authenticate the request to the CA to revoke such as a GCC account)
- The performance of a person's obligations under the CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised,
- There has been a modification of the information regarding the "Subject" of the Digital Certificate,
- This Subscriber Agreement has been terminated,
- The affiliation between the "Subject" of the Digital Certificate with the Subscriber is terminated or has otherwise ended,
- The information within the Digital Certificate, other than non - verified "Subscriber Information" contained in the OU field, is incorrect or has changed,
- Termination of use of the Digital Certificate.
- In the case of EV Code Signing, there is evidence that the certificate was used to sign suspect code.

4.7.2 The Subscriber shall promptly cease all use of the Private Key corresponding to the Public Key listed in the Digital Certificate upon:

- Revocation of the Digital Certificate due to a Private Key compromise or a suspected key compromise,
- Revocation of the Digital Certificate by GlobalSign due to a material breach of its Subscriber Agreement,
- Upon expiry of the Digital Certificate where the CPS specifically forbids a renewal of the Digital Certificate using the same key material.
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser 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).

4.8 NAESB – Specific Obligations

NAESB Subscribers acknowledge their understanding of the following obligations to the WEQ PKI standards through GlobalSign.

End Entities participating in the Business Practice Standard WEQ-012 v3.0 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 NAESB Business Practice Standard

WEQ-012, 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 these Business Practice Standards.
Each subscriber organization acknowledges their understanding of the following obligations to the WEQ 012 v3.0 PKI standard through GlobalSign CA as follows:-

Each End Entity organization shall certify to their certification entity that they have reviewed and acknowledge the following Business Practice Standard WEQ-012.

A.   End Entity acknowledges the electric industry's need for secure private electronic communications that facilitate the following purposes:

   o   Privacy: The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended;
   o   Authentication: The assurance to one entity that another entity is who he/she/it claims to be;
   o   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
   o   Non-Repudiation: A party cannot deny having engaged in the transaction or having sent the electronic message.

B.   End Entity acknowledges the industry's endorsement of public key cryptography which utilizes public key Certificates to bind a person's or computer system's public key to its entity and to support symmetric encryption key exchange.

C.   End Entity has evaluated each of its selected certificate authority's Certification Practices Statement in light of those industry standards as identified by the certificate authority.

End Entities 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.

End Entities shall also be required to comply with the following requirements:

•   Protect their private keys from access by other parties.

•   Identify, through the NAESB EIR, the specific entity they have selected GlobalSign to use as their Authorized Certification Authority
•   Execute all agreements and contracts with the GlobalSign as required by GlobalSign's Certification Practices Statement necessary for the GlobalSign to issue Certificates to the End Entity for use in securing electronic communications.
•   Comply with all obligations required and stipulated by the by GlobalSign in this certification practices agreement, e.g., certificate application procedures, Applicant identity proofing/verification, and certificate management practices.

- Confirm that it has a PKI 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 Permission to Publish Information

The Subscriber agrees that GlobalSign may publish the serial number of the Subscriber's Digital Certificate in connection with GlobalSign dissemination of CRL's and possible OCSP within and outside the GlobalSign CA Hierarchy.

6.0 Disclaimer of Warranty

IN NO EVENT, EXCEPT FOR FRAUD OR WILLFUL MISCONDUCT, SHALL GLOBALSIGN 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 TILL AN AMOUNT AS INDICATED BY THE WARRANTY COMMUNICATION DOCUMENT IN THE APPROPRIATE LEGAL REPOSITORY OF GLOBALSIGN'S WEB SITE. GLOBALSIGN WILL NOT BE LIABLE IN THIS CASE IF THE FAULT IN THIS VERIFIED INFORMATION IS DUE TO FRAUD OR WILLFUL MISCONDUCT OF THE APPLICANT. GLOBALSIGN WILL NOT BE LIABLE IN THIS CASE IF THE USER HAS NOT RESPECTED HIS OBLIGATIONS MENTIONED IN THE CPS AND IN THIS AGREEMENT

7.0 Term and Termination

This agreement shall terminate at the earliest of:
- The expiry date of any Digital Certificate issued to the Subscriber from GlobalSign either directly, indirectly or through a MSSL or ePKI service that has not yet expired,
- Failure by the Subscriber to perform any of its material obligations under this Subscriber Agreement if such breach is not cured within thirty (30) days after receipt of notice thereof from GlobalSign.

8.0 Effect of termination

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

If the contract party is 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 the contract party is 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 the contract party is 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.

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

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 on http://www.globalsign.com/company/contact.htm , Attention: Legal department. Such communications shall be effective when they are received.

9.6 Permission to utilize third party databases.

For natural persons, GlobalSign may validate items such as name, address and other personal information supplied during the application 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.

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 other wise authorized in writing by the party which owns all rights to such trademarks, trade names, logos or product designation.

10.0 NOTICE

The Subscriber must notify GlobalSign through any of our International offices as listed on http://www.globalsign.com/company/contact.htm immediately if there is an error in the Digital Certificate. Without reaction from the Subscriber within 7 days from receipt, the Digital Certificate is deemed accepted.
GlobalSign shall provide refunds pursuant to its "GlobalSign Refund Policy" published at http://www.globalsign.com/repository/