WoSign eCommerce Services Limited
502#, Block A, Technology Building 2, No. 1057, Nanhai Blvd.
Nanshan District, Shenzhen 518067, China
Tel: +86-755-8600 8688 Fax: +86-755-3397 5112

WoSign Certificates Policy & Practice Statement

Version: 1.2

Status: Final Approved

Updated: 2013-04-02

1. INTRODUCTION

1.1 Overview

WoSign is a Certification Authority (CA) that issues high quality and highly trusted digital certificates to entities including private and public companies and individuals in accordance with this CPS. In its role as a CA, WoSign performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing a digital certificate and the maintenance, issuance and publication of Certificate Revocation Lists (CRLs) for users within the WoSign PKI. In delivering its PKI services WoSign complies in all material respects with high-level international standards.

1.2 Document name and identification

This document is the WoSign Certification Practice Statement (CPS) and outlines the legal, commercial and technical principles and practices that WoSign employ in providing certification services that include, but are not

limited to, approving, issuing, using and managing of Digital Certificates and in maintaining a X.509 Certificate based public key infrastructure (PKIX) in accordance with the Certificate Policies determined by WoSign. It also defines the underlying certification processes for Subscribers and describes WoSign's repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the WoSign PKI.

This CPS was approved for publication on Feb. 25, 2013 by the WoSign Policy Authority (WPA). The following revisions were made to the original document:

Date	Changes	Version
Feb. 25, 2013	1. Add "WoSign conforms to the current version of the Baseline Requirements"; 2. Add "WoSign conforms to the current version of the Issuance and Management of Extended Validation Code Signing Certificates"; 3. Add "The certificate applicants can acknowledge the acceptance of CP and CPS electronically on WoSign website" in section 4.1.1.1 4. Add Class 2 SSL certificate and Class 2 Code Signing certificate 5. Add Class 4 EV Code Signing certificate 6. Update the IP address authentication 7. Add 2 IV Intermediate CA and 1 Class 4 EV Intermediate CA 8. Update the EV guideline link to V1.4 9. Add public policy ID 2.23.140.1.2.1 in Class 1 certificates, and policy ID 2.23.140.1.2.2 in Class 3 certificated. 10. Remove Code Signing Certificate "Lifetime Signing" EKU 11. Corrected some spell mistake	V1.2
May 30, 2011	Add IP address support for Class 3 SSL certificate	V1.1

Apr. 17,2011	The original CPS document for public.	V1.0

1.3 PKI participants

1.3.1. Certification authority

1.3.1.1. Principal Statement

WoSign issues EV Certificates to Private Organizations, Government Entities, and Business Entities that satisfy the requirements specified in the Extended Validation Guidelines as published by the CA/Browser Forum.

1.3.1.2. Commitment to comply with applicable standards and the Extended Validation Guidelines

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs. A regular audit is performed by an independent external auditor, to assess WoSign's compliancy with the AICPA/CICA WebTrust program for Certification Authorities.

WoSign conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence

over this document.

For Extended Validation certificates WoSign conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates (“Guidelines”) published at the CA/Browser Forum. In the event of any inconsistency between this document and those guidelines, those guidelines take precedence over this document.

WoSign conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Code Signing Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

1.3.1.3. Implementation of the Extended Validation Guidelines

WoSign implements the Extended Validation Guidelines as published by the CA/Browser Forum and the requirements of the WebTrust Program for CAs and WebTrust EV Program as approved by the CA/Browser Forum. In case multiple or alternative methods or options are possible by the guidelines in order to perform a certain task and/or multiple or alternative methods or options are offered in order to comply to the guidelines, WoSign reserves the right to choose any of the methods or options applicable at any times and may choose to change its procedures at all times and decide to do so on a case to case basis.

1.3.2. Registration authority

Not applicable.

1.3.3. Subscribers

Subscribers of WoSign services are individuals or organizations that use PKI in relation with WoSign supported transactions and communications. Subscribers are parties that are identified in a certificate and hold the private key corresponding to the public key listed in the certificate. Prior to verification of identity and issuance of a certificate, a subscriber is an applicant for the services of WoSign. Each Subscriber must sign the Subscriber Agreement with WoSign, and the Subscriber must sign and seal the agreement and fax or scan and upload to WoSign.

1.3.4. Relying parties

Relying parties use PKI services in relation with WoSign certificates and reasonably rely on such certificates and/or digital signatures verifiable with reference to a public key listed in a subscriber certificate.

To verify the validity of a digital certificate they receive, relying parties must refer to the Certificate Revocation List (CRL) prior to relying on information featured in a certificate to ensure that WoSign has not revoked the certificate. The CRL location is detailed within the certificate.

1.3.5. Other participants

Not applicable.

1.4 Certificate usage

1.4.1. Appropriate certificate uses

By accepting a certificate from WoSign, the subscriber agrees to the rules and regulations outlined in this policy and any accompanied agreement or document. The certificate shall be used lawfully in accordance with the terms of this CP and the relevant CP statements. Certificate usage must be consistent with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate must not be used for signing). Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

Subscribers are notified hereby that electronic signatures can be legally binding. The extent to which they are trusted depends on local legislation. That means that legislation will decide on a case by case base whether or not they are legally binding. Because of these legal implications, subscribers must protect their private keys.

Digital encryption is not meant to be recovered without the private key. If the private key is lost, encrypted data may be lost and cannot be recovered. WoSign does not retain any private keys except its own.

Renewing a certificate follows the same procedures as with a new certificate.

Re-keying or reusing the same private key for any new or renewed certificate shall be avoided by the subscriber.

1.4.2. Prohibited certificate uses

Certificates issued under the provisions of this CPS may not be used for: (i) any application requiring failsafe performance such as: (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) transactions where applicable law prohibits the use of encryption or digital certificates for such transactions or where otherwise prohibited by law.

1.5 Policy administration

1.5.1. Organization administering the document

The WoSign Certificate Policy Authority is responsible for determining the suitability of certificate policies illustrated within the CPS. The Authority is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition. Upon the Certificate Policy Authority accepting such changes deemed by the CA's Policy Authority to have significant impact on the users of this CPS an updated edition of the CPS will be published at the WoSign repository (available at www.wosign.com/policy/), with thirty days notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

Revisions not denoted "significant" are those deemed by the CA's Policy Authority to have minimal or no impact on subscribers and relying parties

using certificates and CRLs issued by CA. Such revisions may be made without notice to users of the CPS and without changing the version number of this CPS.

Controls are in place to reasonably ensure that the WoSign CPS is not amended and published without the prior authorization of the Certificate Policy Authority.

1.6 Definitions and acronyms

1.6.1. Certificate Types

1.6.1.1. Client Certificates are typically used for authentication purpose, signing and encryption of electronic mail and digital documents. They are also referred as S/MIME certificates and may be used for all purposes mentioned above or only for individual usage depending on the key usage limitations found in the certificate.

1.6.1.2. SSL/TLS Server Certificates are typically used by server software for the identification of the server operator and the encrypting of sensitive information during its exposure at the networks.

1.6.1.3. Object Code Signing Certificates are typically used to sign software objects, macros, device drivers, firmware images, virus updates, configuration files or mobile applications.

1.6.1.4. Time Stamping Certificates are used to ensure that the code-signing took place at a specific point in time, specifically during the period for which the Code Signing Certificate was valid, thus extending the validity

of the code past its certificate expiration date.

1.6.1.5. Intermediate CA Certificates are used exclusively for the issuing and signing of end user certificates and certificate revocation lists. Each CA certificate is responsible for the signing of a different Class and end purpose.

1.6.1.6. CA Root Certificate is used to exclusively sign and issue the intermediate CA certificates and corresponding certificate revocation list.

1.6.2. Certificate Classes

1.6.2.1. Class 1 Certificates provide modest assurances that the email originated from a sender with the specified email address or that the domain address belongs to the respective server address. These certificates provide no proof of the identity of the subscriber or of the organization. Class 1 certificates are limited to client and server types, whereas the latter is restricted in its usage.

1.6.2.2. Class 2 Certificates provide medium assurances about the subscriber’s identity and subscribers of Class 2 certificates have to prove their identity by various means.

1.6.2.3. Class 3 Certificates provide a high level of assurance about the subscriber’s identity in comparison with Class 1 and 2 certificates and are issued only to organizations to which the WoSign has verified its true identity by phone call and third part authority trusted database.

1.6.2.4. Class 4 Certificates, also Extended Validation (EV) Certificates, implements the validation procedures and requirements of the Extended

Validation Guidelines as published by the CA/Browser Forum.

1.6.3. Acronyms

CA	Certificate Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DV	Domain Control Validation
EPKI	Enterprise Public Key Infrastructure Manager
EV	Extended Validation
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IV	Identity Validation
OV	Organization Validation
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SSL	Secure Sockets Layer
TLS	Transaction Layer Security

URL Uniform Resource Locator

X.509 The ITU-T standard for Certificates and their corresponding authentication framework

1.6.4. Terms:

Applicant: The Applicant is an entity applying for a Certificate.

Subscriber: The Subscriber is an entity that has been issued a certificate.

Relying Party: The Relying Party is an entity that relies upon the information contained within the Certificate.

Subscriber Agreement: The Subscriber Agreement is an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the Digital Certificate product type as presented during the product online order process and is available for reference at www.wosign.com/policy/ .

Relying Party Agreement: The Relying Party Agreement is an agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference at www.wosign.com/policy/ .

Certificate Policy: The Certificate Policy is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context.

All other definitions and acronyms are according to the Extended Validation

Guidelines.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

WoSign publishes a repository of legal notices regarding its PKI services, including this CPS, agreements and notices, references within this CPS as well as any other information it considers essential to its services. The WoSign legal repository may be accessed at www.wosign.com/policy/ .

2.2 Publication of certification information

WoSign manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by WoSign are X.509v2 CRLs, in particular as profiled in RFC3280. Users and relying parties are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate. The CRL distribution points are included in the certificates.

2.3 Time or frequency of publication

WoSign updates and publishes a new CRL every 24 hours or whenever a CA Certificate is revoked. The CRL of root and intermediate CA certificates may be valid for one year and shall be updated accordingly.

The last CRL of issuer certificates which reach end-of-life (expired) shall remain

published available for a period of 365 days. Such last CRL shall be archived with other related records of the expired issuer certificate.

2.4 Access controls on repositories

Access to the CRL and CPS repositories is not limited.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1. Types of names

WoSign uses the standard X.509, version 3 to construct digital certificates for use within the WoSign PKI. X.509 allows a CA to add certain certificate extensions to the basic certificate structure. The Wosign CA uses a number of certificate extensions for the purposes intended by X.509 version 3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

3.1.1.1. Class 1

3.1.1.1.1. Client Authentication and S/MIME certificates

E = Validated email address

Certificate shall be valid for 365 days.

3.1.1.1.2. SSL/TLS server certificates

CN = Validated domain name (www.domain.com)

Subject Alt Name extension is not critical and contains the CN field value and the base domain.

Certificate shall be valid for up to 2 years.

3.1.1.2. Class 2

3.1.1.2.1. Client Authentication and S/MIME certificates

CN = First and last name

L = Locality

ST = State, administrative or geographical region

C = Country

E = Validated email address

Certificate shall be valid for up to 2 years.

3.1.1.2.2. SSL/TLS server certificates

CN = Validated domain name (domain.com)

O = Validated individual name

L = Locality

ST = State, administrative or geographical region

C = Country

Subject Alt Name extension is not critical and may contain multiple validated domain name field values.

Certificate may be valid for up to 2 years.

3.1.1.2.3. Object Code Signing certificates

CN = Validated individual name

O = Validated individual name

L = Locality

ST = State, administrative or geographical region

C = Country

Certificate may be valid for up to 2 years.

3.1.1.3. Class 3

3.1.1.3.1. Client Authentication and S/MIME certificates

CN = First and last name

O = Validated organization name

L = Locality

ST = State, administrative or geographical region

C = Country

E = Validated email address

Certificate may be valid for up to 3 years.

3.1.1.3.2. SSL/TLS server certificates

CN = Validated domain name or Ipv4 address (domain.com / 1.2.3.4)

O = Validated organization name

L = Locality

ST = State, administrative or geographical region

C = Country

Subject Alt Name extension is not critical and may contain multiple validated domain name field values.

Certificate may be valid for up to 3 years.

3.1.1.3.3. Object Code Signing certificates

CN = Validated organization name

O = Validated organization name

L = Locality

ST = State, administrative or geographical region

C = Country

Certificate may be valid for up to 3 years.

3.1.1.4. Class 4 (Extended Validation)

3.1.1.4.1. SSL/TLS server certificates

CN = Validated domain name (www.domain.com)

O = Validated organization name

L = Locality

ST = State, administrative or geographical region

C = Country

OID 2.5.4.5 = Serial or registration number

OID 2.5.4.15 = Business Category (This field MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of Section 7.2.2, 7.2.3, 7.2.4 or 7.2.5 of the EV Guidelines, respectively.)

OID 2.5.4.9 = Street address (optional)

OID 2.5.4.17 = Postal or zip code (optional)

OID 1.3.6.1.4.1.311.60.2.1.1 = Locality of incorporation (optional)

OID 1.3.6.1.4.1.311.60.2.1.2 = State or province of incorporation (optional)

OID 1.3.6.1.4.1.311.60.2.1.3 = Country of incorporation

Subject Alt Name extension is not critical and may contain multiple validated domain name field values.

Certificate may be valid 2 years.

The special EV OIDs are 1.3.6.1.4.1.36305.2

3.1.1.4.2. Object Code Signing certificates

CN = Validated organization name

O = Validated organization name

L = Locality

ST = State, administrative or geographical region

C = Country

OID 2.5.4.5 = Serial or registration number

OID 2.5.4.15 = Business Category (This field MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of Section 7.2.2, 7.2.3, 7.2.4 or 7.2.5 of the EV Guidelines, respectively.)

OID 2.5.4.9 = Street address (optional)

OID 2.5.4.17 = Postal or zip code (optional)

OID 1.3.6.1.4.1.311.60.2.1.1 = Locality of incorporation (optional)

OID 1.3.6.1.4.1.311.60.2.1.2 = State or province of incorporation (optional)

OID 1.3.6.1.4.1.311.60.2.1.3 = Country of incorporation

Certificate may be valid 3 years.

The special EV OIDs are 1.3.6.1.4.1.36305.2

3.1.1.5. Intermediate CA Certificates

E = Validated email address (optional)

CN = WoSign Class [1-4] [DV | IV | OV | EV] [Server | Client | Object] CA

O = Organization

C = Country

Certificate shall be valid up to 15 years.

Subscriber certificates are issued during the 1st to 12th year, whereas during the last two years of the validity of the intermediate CA certificate no subscriber certificates are issued. The intermediate certificate continues to issue the corresponding CRL during the last two years.

3.1.2. Need for names to be meaningful

Any content of the subject Distinguished Name (DN) must have been validated. Validations depend on the verification level per class.

3.1.3. Anonymity or pseudonymity of subscribers

Not applicable.

3.1.4. Rules for interpreting various name forms

Distinguished Names in Certificates shall be interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5. Uniqueness of names

Name uniqueness is ensured through the use of either the Common Name attribute of the Subject Field for server certificates, the emailAddress attribute of the Subject Field for S/MIME certificates and the Common Name and Organization attribute of the Subject Field for code signing certificates.

3.1.6. Recognition, authentication, and role of trademarks

WoSign performs sanity and fraud prevention checks in order to limit accidental issuing of certificates whose domain or organization names might be misleading and/or might be used to perform an act of fraud, identity theft or infringement of trademarks.

3.2 Initial identity validation

3.2.1. Method to prove possession of private key

WoSign offers the creation of key pairs and certificate signing requests (CSR) for server certificates through the CA system. The private key is delivered encrypted and protected by a pass phrase via SSL secured connection to the subscriber. The private key generation utility employs a Real Hardware Random Number Generator for the seeding of the entropy. The use of the private key generation utility at the WoSign web site is at the sole risk of the subscriber. WoSign doesn't keep any private keys and pass phrases / passwords and any such information is deleted and/or overwritten if necessary.

Subscribers may produce and prepare their own private keys and certificate signing requests (CSR) for server certificates and submit them via SSL secured connection to CA system. In this case, private key delivery to the subscriber is unnecessary.

Client S/MIME and Object Code Signing keys are always generated at the client side via appropriate browser functions. In this case, private key delivery to the subscriber is unnecessary.

3.2.2. Authentication

3.2.2.1. Class 1

3.2.2.1.1. Email Addresses

Email accounts are validated by sending an electronic mail message with a verification code to the requested email account. The subscriber has to return and submit the verification code as prove of ownership of the email account within a limited period sufficient enough to receive an electronic mail message.

The validation may be valid for 30 days for the generation of digital certificates.

3.2.2.1.2. Domain Names

Fully qualified domain names, typically “www.domain.com” or “domain.com” are validated by sending an electronic mail message with a verification code to one of the following administrative electronic mail accounts:

- webmaster@domain.com
- hostmaster@domain.com
- postmaster@domain.com

The subscriber has to return and submit the verification code as prove of ownership of the domain name within a limited period sufficient enough to receive an electronic mail message. Additionally the existence of the domain name is verified by checking the WHOIS records provided by the domain name registrar. If the WHOIS data contain additional email addresses, they may be offered as additional choices to the above mentioned electronic mail accounts.

WoSign performs additional sanity and fraud prevention checks as outlined in section 3.1.6. Wild card domain names like “*.domain.com” are not issued in the Class 1 level.

The validation may be valid for 30 days for the generation of certificates.

3.2.2.1.3. IPv4 Addresses

Ipv4 addresses must bind to a FQDN and must not be reserved by IANA (according to http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml).

The subscriber must provide attestation about the right to use the relevant IP addresses, for example a contract with a hosting provider or dedicated leased line agreement.

The validation may be valid for 30 days for the generation of certificates.

3.2.2.2. Class 2

3.2.2.2.1. Personal Identity

The verification process of personal identities of subscribers are performed manually. The WoSign CA validates without any reasonable doubt that the following details are correct:

- First and last name

- Residence, Address
- State or Region
- Country

The subscriber has to provide in a secure and reliable fashion one scanned or photographed identification papers in high quality and resolution. The documents must be valid in every respect and not be expired.

If the accuracy of the documents is in doubt as to the correctness of the details provided, WoSign may request the original documents and/or a copy of the original document confirmed, signed and stamped by the issuing authority or Latin notary via postal mail. Any document obtained physically may be scanned or photographed for archiving purpose at the premise of WoSign and shall be returned to the sender via registered postal mail.

WoSign may verify the correctness of the identity through payment transactions to its banking accounts by the subscriber. The transaction details must state the correct personal details of the subscriber. Alternatively WoSign may use third party records to establish that a phone number is owned by the subscriber and by performing a verification call.

Email control validation is performed as in Class 1. The validation may be valid for 350 days for the generation of digital certificates.

3.2.2.3. Class 3

3.2.2.3.1. Organization

The verification process of organizations implies same level identity validation of the subscriber (responsible person) and are performed manually. WoSign validates without any reasonable doubt that the following details are correct:

- Registered organization name
- Address
- State or Region
- Country

The subscriber has to provide in a secure and reliable fashion supporting documentation. The documents must be valid in every respect and not be expired.

If the accuracy of the documents is in doubt as to the correctness of the details provided, WoSign may request the original documents and/or a copy of the original document confirmed, signed and stamped by the issuing authority via postal mail. Any document obtained physically may be scanned or photographed for archiving purpose at the premise of WoSign and shall be returned to the sender via registered postal mail.

WoSign may verify the correctness of the organization details through payment transactions to its banking accounts by the subscriber. The

transaction details must state the correct organization details of the subscriber. Additionally WoSign obtains through third party records a phone number that is owned by the organization and by performing a verification call. During the verification call WoSign establishes the authority of the subscriber.

Domain and email control validation is performed as in Class 1. Domain control may be also established through verification of the WHOIS records and matching subscriber information.

The validation may be valid for 350 days for the generation of digital certificates.

3.2.2.4. Class 4 (Extended Validation)

Extended Validation for organizations are performed according to the validation procedures and requirements of the Extended Validation Guidelines as published by the CA/Browser Forum. Applicants for EV must be at least Class 2 Identity validated prior to engagement for Extended validation.

3.2.3. Non-verified subscriber information

Not applicable.

3.2.4. Validation of authority

WoSign confirms and verifies that the subscriber is duly authorized to represent the organization and obtain the certificates on their behalf by obtaining an authorization statement and by contacting the authorizer. The obtained and confirmed organization documents should state the authorizer and position, but WoSign may rely on other means and sources to obtain the necessary authority if necessary. WoSign may assume proper authorization in case the validated subscriber is either the appointed CEO, Director, President or owner and sole proprietor.

3.2.5. Criteria for inter-operation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

Subscribers should not reuse private keys for successive certificates after expiration thereof and it's highly recommended to create a new key for every certificate.

3.3.2. Identification and authentication for re-key after revocation

Private keys of certificates which were revoked should not be reused.

3.4 Identification and authentication for revocation request

See Sections 4.9.1 through 4.9.3 for information about Certificate revocation procedures.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1. Who can submit a certificate application

Any individual who is the subject of the certificate

Any authorized representative of an Organization or entity

4.1.1.1. Subscriber Agreement Requirements

By accepting a certificate from WoSign, the subscriber agrees to the rules and regulations outlined in this policy and any accompanied agreement or document. The certificate shall be used lawfully in accordance with the terms of this CP and the relevant CP statements. The certificate applicants can acknowledge the acceptance of CP and CPS electronically on WoSign website. Certificate usage must be consistent with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate must not be used for signing). Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

For EV certificates the subscriber has to enter into a legally valid and enforceable subscriber agreement with WoSign that satisfies the requirements of the CA/Browser Forum Guidelines. WoSign requires that the subscriber makes the commitments and warranties set forth in the “Subscriber Agreement Requirements” section of the CA/Browser Forum Guidelines.

4.1.1.2. Certificate Request Requirements for DV/IV/OV Certificates

Accept the Subscriber Agreement Requirements and demonstration of possession and/or exclusive control of the private key corresponding to the public key.

4.1.1.3. Certificate Request Requirements for EV Certificates

Applicants for EV certificates must validate their identity prior to engagements for extended validation. The applicant shall serve as the "Contract Signer", "Certificate Approver", and "Certificate Requester" as defined by the Extended Validation Guidelines. The applicants must make the request by the designated utility at the WoSign operated web site and sign the "WoSign Extended Validation Subscriber Agreement".

4.1.2. Enrollment process and responsibilities for DV/IV/OV Certificates

The certificates and listed details therein are validated by WoSign according to the requirements under section 3.2.2 Authentication.

4.1.3. Enrollment process and responsibilities for EV Certificates

WoSign verifies the applicants authorization for signing the "WoSign Extended Validation Subscriber Agreement" and authorization for approving and requesting EV certificates on behalf of the subscriber according to the requirements of the Extended Validation Guidelines.

4.2 Certificate application processing

4.2.1. Performing identification and authentication functions

See section 3.2.2

WoSign verifies the applicant's legal existence and identity according to the “Verification Requirements” and “Methods of Verification” specified in the Extended Validation Guidelines as published by the CA/Browser Forum.

4.2.2. Approval or rejection of certificate applications

Following successful completion of all required validations of a certificate application, WoSign approves an application for a digital certificate.

If the validation of a certificate application fails, WoSign rejects the certificate application. WoSign reserves the right to reject applications to issue a certificate to applicants if, on its own assessment and may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal. Applicants whose applications have been rejected may subsequently re-apply.

4.2.3. Time to process certificate applications

Notification of issuance of a certificate to others than the subscriber and subject of the certificate are generally not performed. Issuance and delivery of a certificate is part of the procedures for obtaining a certificate by the subscriber.

WoSign makes reasonable efforts to confirm certificate application

information and issue EV Certificates within a reasonable time frame. This greatly dependents on the Applicant providing the necessary details and documentation in a timely manner. Upon the receipt of the necessary details and documentation, WoSign aims to confirm submitted application data and to complete the validation process and issue or reject a certificate application.

4.3 Certificate issuance

4.3.1. CA actions during certificate issuance

WoSign offers different certificate types to make use of SSL, Code Signing and S/MIME technology for secure online transactions, secure electronic file and secure email respectively. Prior to the issuance of a certificate, WoSign will validate an application in accordance with this CPS which may involve the request by WoSign to the applicant for relevant official documentation supporting the application or according to the Extended Validation guidelines.

4.3.2. Notification to subscriber by the CA of issuance of certificate

An issued certificate is either delivered through an on-line collection method or retrieved from the provided on-line interfaces. A subscriber is deemed to have accepted a certificate when delivered and installed into client or server software or when retrieved from the on-line interfaces.

4.4 Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

By accepting a certificate from WoSign, the subscriber agrees to the rules and regulations outlined in this policy and any accompanied agreement or document. The certificate shall be used lawfully in accordance with the terms of this CP and the relevant CP statements. Certificate usage must be consistent with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate must not be used for signing).

The Certificate Requester is responsible for installing the issued certificate on the Subscriber’s computer or hardware security module according to the Subscriber's system specifications.

4.4.2. Publication of the certificate by the CA

WoSign publishes the certificate by delivering it to the Subscriber. No other publication or notification to others occurs.

4.5 Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

Subscribers are notified hereby that electronic signatures can be legally binding. The extent to which they are trusted depends on local legislation.

That means that legislation will decide on a case by case base whether or not they are legally binding. Because of these legal implications, subscribers must protect their private keys.

Digital encryption is not meant to be recovered without the private key. If the private key is lost, encrypted data may be lost and cannot be recovered. WoSign does not keep any private keys except its own.

4.5.2. Relying party public key and certificate usage

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the relying party must obtain such assurances for such reliance to be deemed reasonable. Before any act of reliance, relying parties shall independently assess:

- That the certificate is being used in accordance with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
- The status of the end entity certificate and all the CA certificates in the chain that issued the certificate. If any of the certificates in the certificate chain have been revoked, the relying party shall not rely on the end user certificate or other revoked certificates in the certificate chain.

4.6 Certificate renewal

Renewing a certificate follows the same procedures as with a new certificate.

4.7 Certificate re-key

Re-keying or reusing the same private key for any new or renewed certificate shall be avoided by the subscriber.

4.8 Certificate modification

Not applicable.

4.9 Certificate revocation and suspension

4.9.1. Circumstances for revocation

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. A certificate will be revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

- The subscriber’s private key is lost or suspected to be compromised
- The information in the subscriber’s certificate is suspected to be inaccurate
- The information supplied may be misleading (e.g., paypa1.com, micr0soft.com)
- The subject has failed to comply with the rules in this policy

- The system to which the certificate has been issued has been retired
- The subscriber makes a request for revocation
- The Subscriber indicates that the original Certificate Request was not authorized and does not retroactively grant authorization
- The subscriber violated his/her obligations

4.9.2. Who can request revocation

Certificate revocation can be requested by the subscriber of the certificate or by any other entity presenting proof of knowledge of circumstances for revocation.

4.9.3. Procedure for revocation request

Subscribers may request revocation of a certificate by using the on-line utility provided at the CA web site.

Certificate revocation may also be requested by sending an electronic mail message to certmaster@wosign.com with clear identification and information details, according to the above mentioned circumstances for revocation. WoSign makes every reasonable effort to verify the claims, reason and identity of the requester.

The subscriber will be notified of the revocation via electronic mail message. Upon the revocation of a subscriber's certificate, the newly revoked certificate is recorded and an updated CRL shall be issued. Notification of

revocation of a certificate to others than the subscriber and subject of the certificate, beyond the published CRL, are generally not performed.

4.9.4. Revocation request grace period

Not applicable.

4.9.5. Time within which CA must process the revocation request

WoSign revokes the certificate and issues a CRL as soon as it has determined that a properly supported revocation request has been made.

4.9.6. Revocation checking requirement for relying parties

Relying parties must verify the certificate against the revocation list (CRL) and/or OCSP responder, check against expiry time, certificate chain, the validity check of the certificates in the chain and the identification of the domain and email.

4.9.7. CRL issuance frequency

The corresponding Certificate Revocation Lists (CRL) of subscriber certificates are updated at least every 24 hours or every time a certificate is revoked, whichever comes first. The CRL is published via Internet download. Each intermediate CA issues its own corresponding CRL for the certificates issued. The CRL distribution points are included in the certificates.

The CRL of root and intermediate CA certificates may be valid for one year

and shall be updated accordingly.

The last CRL of issuer certificates which reach end-of-life (expired) shall remain published available for a period of 365 days. Such last CRL shall be archived with other related records of the expired issuer certificate.

4.9.8. Maximum latency for CRLs

Certificate Revocation Lists is published at the on-line repository within a commercially reasonable time after generation. This is generally done automatically and within one hour after generation of a new CRL.

4.9.9. On-line revocation/status checking availability

An OCSP responder service is provided and the respective URL location of the service is included in the certificates. The OCSP responder provides results about the status of a certificate instantly. The current CRLs are reloaded at least every 60 minutes. Error responses by the OCSP responder may be unsigned and include regular HTTP status errors.

4.9.10. On-line revocation checking requirements

Relying parties must verify the certificate against the revocation list (CRL) and/or OCSP responder, check against expiry time, certificate chain, the validity check of the certificates in the chain and the identification of the domain and email.

4.9.11. Other forms of revocation advertisements available

Not applicable.

4.9.12. Special requirements re-key compromise

Not applicable.

4.9.13. Circumstances for suspension

Certificates issued to subscriber may be either valid, expired or revoked. WoSign does not perform certificate suspension and subscribers are advised to request a new certificate in case of expiration or revocation of previously valid certificates.

4.9.14. Who can request suspension

Not applicable.

4.9.15. Limits on suspension period

Not applicable.

4.10 Certificate status services

Not applicable.

4.11 End of subscription

A Subscriber may terminate its subscription to certificate services by allowing the term of a Certificate or applicable agreement to expire without renewal. A Subscriber may also voluntarily revoke a Certificate as explained in Section 4.9.

4.12 Key escrow and recovery

WoSign does not perform escrow or recovery of subscriber private keys.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1. Site Location and Construction

WoSign operates a tightly controlled and restricted, underground infrastructure which is comprised of physical boundaries, computer hardware, software and procedures that provide an acceptable resilience against security risks and provide a reasonable level of availability, reliability and correct operation and the enforcing of a security policy. The hardware and software is protected and constantly monitored by authorized service personnel for intrusion and compromise. Various programs and tools are installed to assist in this task. Hardware equipment and operating systems are maintained at the highest possible level of security.

5.1.2. Physical Access

The hardware is located in a dedicated, resistant server room. Access to the facility by individuals (personnel and others) is strictly controlled and restricted to authorized and trusted personnel only. Maintenance and other services applied to the cryptographic devices and server systems must be authorized by the CEO or COO of WoSign or equally authorized caretaker of the WoSign PKI. Physical access to the server infrastructure and facilities shall be logged and signed by at least one other witness on the four eyes principal. Otherwise physical access to the systems shall be avoided.

5.1.3. Network Security

The CA root key(s) are kept off-line and brought online only when necessary to sign intermediate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

5.1.4. Power and Air Condition

The locality is fully air conditioned to prevent overheating and to maintain a suitable humidity level. Primary and secondary power supplies ensure continuous, uninterrupted access to electric power. Electricity power backup (UPS) is supported by an external, independent electricity power source for cases of prolonged power outages.

5.1.5. Water Exposures

All server equipment and devices are elevated above the ground. No water lines exist above equipment.

5.1.6. Fire Prevention and Protection

Fire alarm and intrusion prevention equipment are installed, maintained and available at the premise.

5.1.7. Media Storage

The server room is monitored by a closed-circuit camera and television monitoring system with recording capabilities and records shall be archived in a rolling and increasing mode.

Daily backup of its CA related data that are rotated and stored according to either on-site or off-site according to an established backup rotation schedule.

5.1.8. Waste Disposal

WoSign implemented procedures for the disposal of waste (paper, media, or any other waste) in order to prevent the unauthorized use of, or access to, or disclosure of waste containing confidential information.

5.1.9. Off-site Backup

Backup copies of CA Private Keys and activation data are stored on-site in separate safety vaults accessible only by trusted personnel.

Other data is backed up in a rolling fashion and secure manner at a off-site facility beyond 150 miles of WoSign's infrastructure.

5.2 Procedural controls

5.2.1. Trusted roles

WoSign follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.

5.2.2. Number of persons required per task

Handling of CA Private Keys (throughout the entire CA key lifecycle) requires the involvement of at least two trusted persons. Physical and logical access controls exist for the key activation material in order to maintain multi-party control over the Hardware Security Modules containing CA Private Keys.

The signing of Intermediate Certificates and Certificate Revocation Lists covering the Intermediate CAs shall be performed exclusively by an executive officer and in attendance of at least one witness.

5.2.3. Identification and authentication for each role

Personnel in trusted roles must authenticate themselves to the certificate management system before they are allowed access to the components of the system necessary to perform their trusted roles.

5.2.4. Roles requiring separation of duties

The signing of CA Root Certificates, Intermediate Certificates and Certificate Revocation Lists covering the Intermediate CAs shall be performed exclusively by an executive officer of WoSign and attendance by at least one witness.

5.3 Personnel controls

WoSign implements various access codes, smart cards, electronic tokens and physical locks in multiple combinations thereof for facility access, work stations, CA administration programs, server administration programs and monitoring devices to restrict and control access according to the defined roles and permissions.

5.4 Audit logging procedures

5.4.1. Types of events recorded

Events and audit logs are generally produced automatically on an ongoing basis and reviewed constantly. Those events include any access to the WoSign CA systems and designed user interfaces, being it for personnel or subscribers. System reports are produced on a daily basis and reviewed daily by WoSign's management.

Special reports are issued for any CA key life cycle management event. Records are produced on hardware and software introduction and/or modifications and/or maintenance.

5.4.2. Frequency of processing log

See above.

5.4.3. Retention period for audit log

WoSign retains the records of the issued certificates and the associated documentation for no less than seven (7) years. The retention term begins on the date of expiration or revocation. Copies of certificates are held, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that WoSign may see fit.

5.4.4. Protection of audit log

Such records are archived and maintained in a form that prevents unauthorized modification, substitution or destruction.

5.4.5. Audit log backup procedures

Data is backed up daily in a rolling and increasing mode, including critical system data or any other sensitive information, like personal data and event log files. Archives and other materials of critical system data important for recovery in case of a disaster are stored in a secure manner at a off-site facility beyond 150 miles of WoSign's infrastructure.

5.4.6. Audit collection system (internal vs. external)

No stipulation.

5.4.7. Notification to event-causing subject

No stipulation.

5.4.8. Vulnerability assessments

WoSign's Security Program includes regular risk assessments that:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any data or processes.
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal data and certificate issuance processes.
- Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that WoSign has in place to control such risks.

Based on the Risk Assessment, WoSign implements and maintains a Security Plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the data and processes, as well as the complexity and scope of the activities of WoSign.

The Security Plan includes administrative, organizational, technical and physical safeguards appropriate to the size, complexity, nature, and scope of the WoSign's business.

The Security Plan also takes into account the available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.5 Records archival

5.5.1. Types of records archived

All accesses to the on-line and off-line systems and actions are logged as events including but not limited to remote IP addresses, identity, role, user agent, type of event, type of action, description, date and time. Security related events are additionally recorded with an issues tracking tool. Critical events are logged in a special report and signed by the CEO or COO of WoSign.

5.5.2. Retention period for archive

Same as 5.4.3

5.5.3. Protection of archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution or destruction.

5.5.4. Archive backup procedures

Same as 5.4.5

5.5.5. Requirements for time-stamping of records

System times are updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every day. All recorded events are time-stamped in the events and audit logs.

5.5.6. Archive collection system (internal or external)

Archive information is collected internally.

5.5.7. Procedures to obtain and verify archive information

Records are archived and maintained in a form that prevents unauthorized modification, substitution or destruction. Such records may be retained in electronic, in paper-based format or any other format that WoSign may see fit.

5.6 Key changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, WoSign ceases using its expiring CA Private Key to sign Certificates

(well in advance of expiration) and uses the old Private Key only to sign CRLs. A new CA signing key pair is commissioned and all subsequently issued certificates and CRL's are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed below.

5.7 Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

In the event that a CA private key is suspected to have been compromised, WoSign's CEO or COO will immediately convene an emergency Incident Response Team to assess the situation to determine the degree and scope of the incident and take appropriate actions. Those include collection of information related to the incident, investigation, informing law enforcement and other interested parties, further prevention and short term corrections, compiling and issuing of a critical events report. In case it was determined that a CA private key was compromised, the affected key shall be revoked (where possible) and a replacement issued after appropriate solutions are implemented to prevent recurrence.

5.7.2. Computing resources, software, and/or data are corrupted

WoSign performs system back-ups on a daily basis. Back-up copies are made of CA Private Keys and are stored off-site in a secure location. In the event of

a disaster whereby the CA operations become inoperative, WoSign will re-initiate its operations on replacement hardware using backup copies of its software, data and CA private keys at a comparable, secured facility.

5.7.3. Entity private key compromise procedures

See 5.7.1

5.7.4. Business continuity capabilities after a disaster

See 5.7.1

5.8 CA termination

The WoSign CA policy is subject to changes and it is the responsibility of the subscribers and relaying party's to review the policy from time to time. All changes, if at all, including the CA policy itself are published at the designated web site for the CA operations. Subscribers and relaying parties will not be notified of impending changes of the policy. The policy is legally binding from the moment of its publication.

WoSign shall continue its CA operations for one year (365 days) in case of the termination of the WoSign CA, excluding issuance of new subscriber certificates. All remaining certificates still valid after the one year extension period shall be revoked on the last day and included in the corresponding certificate revocation list.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1. Key pair generation

6.1.1.1. CA Keys

Key pair generation shall be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys.

The WoSign CA root is an off-line CA and shall be used only for the signing of Intermediate CA certificates and the relevant Certificate Revocation Lists. For key generation and other signing procedures by the CA root, a strictly off-line system must be used. The computer system utilizes a real hardware random number generator for entropy seeding. The resulting private and public keys and certificate revocation lists must be then stored in removable devices and/or security modules according to the defined procedures.

The private CA root key must be stored in encrypted form in safety vaults, divided into two external media devices and stored at two different locations and protected by a pass phrase. Only both external devices may recreate the private CA root key, which is needed for signing actions such as issuance of Intermediate CA certificates and Certificate Revocation Lists. Strict dual control is implemented for the handling of the CA root key and

controls are in place to prevent compromise of the CA root key.

The signing of Intermediate Certificates and Certificate Revocation Lists covering the Intermediate CAs shall be performed exclusively by an executive officer of WoSign and attendance of at least one witness.

The signing of subscriber certificates is strictly and only performed by the Intermediate CA keys which are operating at the on-line equipment. CA private keys shall be archived after expiration of the public key according to the same procedure as the CA root key.

6.1.1.2. Subscriber Keys

See section 3.2.1

6.1.2. Private key delivery to subscriber

See section 3.2.1

6.1.3. Public key delivery to certificate issuer

See section 4.3.2

6.1.4. CA public key delivery to relying parties

The public root CA keys are published from the following repository:

- http://aia.wosign.com/ca1.cer (DER encoded)
- http://aia.wosign.com/ca1.pem (PEM encoded)
- http://aia.wosign.com/ca2.cer (DER encoded)
- http://aia.wosign.com/ca2.pem (PEM encoded)

The public root CA keys shall be embedded within popular software applications, making special root distribution mechanisms unnecessary.

Intermediate CA public keys are published and distributed via Internet from the following repository:

- http://aia.wosign.com/

All public CA keys of WoSign may be downloaded via secured and encrypted protocols (SSL).

Distribution of Intermediate CA public keys to relaying parties is generally unnecessary, provided that the public CA root key is installed in the software used by the relying party.

6.1.5. Key sizes

All keys must be 2048-bit or bigger RSA Key with Secure Hash Algorithm version 1 or 2 (SHA-1 or SHA-256).

6.1.6. Public key parameters generation and quality checking

WoSign checks the submitted keys for known vulnerabilities and eventual

weak randomness. Private keys generated by WoSign or by the subscriber must have adequate key sizes and signature algorithms deemed secure at the time of creation in order to provide sufficient protection according to section 6.1.5.

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

CA certificates include key usage extension fields to specify the purposes for which the CA Certificate may be used and also to technically limit the functionality of the certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of WoSign. Key usages are specified in the Certificate Profile set forth in Section 7.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The private keys of the Intermediate CA certificates are stored in Hardware Security Modules (HSM) FIPS 140-2 Level 3 certified devices, suitable for the signing of Subscriber Certificates and the on-line Certificate Revocation Lists. For recovery and archival purpose the private keys of the Intermediate CA certificates are also stored off-line according to the same procedure as the CA root key.

6.3 Other aspects of key pair management

6.3.1. Public key archival

Copies of all Public Keys for archival in accordance with Section 5.5.

6.3.2. Certificate operational periods and key pair usage periods

All certificates and corresponding keys shall have maximum validity periods (not exceeding):

- Root CA 30 years
- Sub CA 15 years
- Subscriber 1 - 3 years

Pursuant to Section 5.6 CA Private Keys are retired from signing subordinate certificates before the periods listed above to accommodate the key changeover process (i.e., the retiring CA Private Key is still used to sign CRLs to provide validation services for certificates issued with that retiring CA Private Key.)

6.4 Activation data

No stipulation.

6.5 Computer security controls

See section 5.4.8

6.5.1. Specific computer security technical requirements

WoSign implements various access codes, smart cards, electronic tokens and physical locks in multiple combinations thereof for facility access, work stations, CA administration programs, server administration programs and monitoring devices to restrict and control access according to the defined roles and permissions.

6.5.2. Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1. System development controls

Development of the CA related infrastructures, hardware, libraries, programs, protective programs are performed by personnel with the appropriate knowledge and training. Changes to configuration files and settings, sources, binaries and hardware components must be reviewed and approved by the management. Modifications to the processes and certificates are tested for eventual flaws. Maintenance and other activities on hardware the CA require prior approval by the management and are logged accordingly, monitored and recorded.

6.6.2. Security management controls

WoSign has mechanisms in place to control and monitor the security-related configurations of its CA systems. Change control processes consist of change control data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. In this manner, WoSign can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

6.6.3. Life cycle security controls

No stipulation.

6.7 Network security controls

The CA root key(s) are kept off-line and brought online only when necessary to sign intermediate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

6.8 Time-stamping

See section 5.5.5

7. CERTIFICATE, CRL, AND OCSP PROFILES

Information for interpreting the following Certificate and CRL Profiles may be found in IETF's RFC 2459 (http://www.ietf.org/rfc/rfc2459.txt). WoSign uses the ITU X.509, version 3 standard to construct digital certificates for use within the WoSign PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure.

7.1 Certificate profile

All certificates are X.509 version 3 certificates.

7.2 Certificate extensions

Subscriber S/MIME Client Certificates:

- Basic Constraint: CA:FALSE
- Key Usage: Digital Signature, Key Encipherment, Data Encipherment
- Extended Key Usage:
  - Client Authentication (1.3.6.1.5.5.7.3.2)
  - Secure Email (1.3.6.1.5.5.7.3.4)
- Subject Key Identifier: Hash
- Subject Alternative Name: email:email@address
- CRL Distribution Points: URL

- Authority Info Access: Access Method (1.3.6.1.5.5.7.48.2), OCSP URL
- Authority Key Identifier: Key ID
- Issuer Alternative Name: URI:http://url
- Certificate Policies: Policy Identifier (1.3.6.1.4.1.36305.<policy>.<class-level>.<cert-type>.<major-version>.<minor-version>)

Subscriber SSL/TLS Server Certificates:

- Basic Constraint: CA:FALSE
- Key Usage: Digital Signature, Key Encipherment, Key Agreement
- Extended Key Usage:
  - Server Authentication (1.3.6.1.5.5.7.3.1)
- Subject Key Identifier: Hash
- Subject Alternative Name: DNS: fqdn.com, IP:1.2.3.4
- CRL Distribution Points: URL
- Authority Info Access: Access Method (1.3.6.1.5.5.7.48.2), OCSP URL
- Authority Key Identifier: Key ID, Certificate Issuer
- Issuer Alternative Name: URI:http://url
- Certificate Policies: Policy Identifier (1.3.6.1.4.1.36305.<policy>.<class-level>.<cert-type>.<major-version>.<minor-version>)

EV Policy OID: 1.3.6.1.4.1.36305.2

Code Signing Certificates:

- Basic Constraint: CA:FALSE
- Key Usage (Critical): Digital Signature
- Extended Key Usage (Critical):
  - Code Signing (1.3.6.1.5.5.7.3.3)
  - MS Code Commercial (1.3.6.1.4.1.311.2.1.22)
- Subject Key Identifier: Hash
- CRL Distribution Points: URL
- Authority Info Access: Access Method (1.3.6.1.5.5.7.48.2), OCSP URL
- Authority Key Identifier: Key ID, Certificate Issuer
- Issuer Alternative Name: URI:http://url
- Certificate Policies: Policy Identifier (1.3.6.1.4.1.36305.<policy>.<class-level>.<cert-type>.<major-version>.<minor-version>)

Intermediate Certificates:

- Basic Constraint (Critical): CA:TRUE
- Key Usage:
  - Digital Signature
  - Key Encipherment

- Certificate Signing
- CRL Signing

- Subject Key Identifier: Hash
- Authority Key Identifier: Key ID, Certificate Issuer
- Issuer Alternative Name: URI:http://url
- Certificate Policies: Policy Identifier (1.3.6.1.4.1.36305.<policy>.<class-level>.<cert-type>.<major-version>.<minor-version>)
- Any Policy (2.5.29.32.0)

Online Certificate Status Protocol (OCSP) Responder:

- Online Certificate Status Protocol responders conform to RFC 2560.
- Basic Constraint: critical, CA:FALSE
- Key Usage:
  - Digital Signature
  - Key Encipherment
  - Key Agreement
- Extended Key Usage:
  - OCSP Signing
  - OCSP No Check

Time Stamping Authority (TSA) Certificate:

- Basic Constraint: CA:FALSE

- Key Usage (Critical):
  - Digital Signature
  - Non Repudiation
- Extended Key Usage (Critical):
  - Time Stamping

7.3 Algorithm object identifiers

7.3.1. Key Attributes

RSA Algorithm
2048 bit or higher

7.3.2. Hash Algorithm

SHA-1, SHA-256

7.4 Name forms

See 3.1

7.5 Name constraints

No stipulation.

7.6 Certificate policy object identifier

An object identifier (OID) is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a Certificate Policy and/or Certification Practice Statement, such as this CPS.

The unique IANA assigned OID of WoSign is 1.3.6.1.4.1.36305 and the Policy Identifier included in certificates is 1.3.6.1.4.1.36305.<policy>.<class-level>.<cert-type>.<major-version>.<minor-version>, whereas <policy> is always the number ONE (1) and <major-version>.<minor-version> represents the CPS version number.

The special EV OID for Extended Validation certificates is 1.3.6.1.4.1.36305.2.

The policy identifier of 2.23.140.1.2.1 should be included in Class 1 certificates, and the policy identifier of 2.23.140.1.2.2 should be included in Class 3 certificate.

7.7 Policy qualifiers syntax and semantics

WoSign certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and disclaimers of warranty that may apply.

7.8 CRL profile

- Version: v1
- Signature Algorithm: SHA-1 or SHA-256 with RSA encryption
- Issuer: Identification of the CA issuing the CRL
- Last Update: Time of CRL issue
- Next Update: Time of next CRL issue (48 hours)
- Revoked certificates: Listing of information for revoked certificates

CRLs are updated at least every 12 hours or upon adding of a new entry, e.g. every time a certificate is revoked. However the next update entry in the CRL is set to 48 hours.

7.9 OCSP profile

Online Certificate Status Protocol responders conform to RFC 2560.

- Basic Constraint: critical, CA:FALSE
- Key Usage:
  - Digital Signature
  - Key Encipherment
  - Key Agreement
- Extended Key Usage:
  - OCSP Signing
  - OCSP No Check

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The practices specified in this CA policy & practice statements have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs. An annual audit is or will be performed by an independent external auditor to assess WoSign's compliance with the AICPA/CICA WebTrust program for Certification Authorities and WebTrust Extended Validation Audit. Topics covered by the annual audit include but are not limited to the following:

- CA business practices disclosure
- Service integrity
- CA environmental controls

8.2 Compliance Improvement

Upon detection of deficiencies and possible weaknesses of the CA infrastructure and/or established procedures as a result of internal or external auditing or in case of non-compliance thereof, WoSign shall take corrective measures and actions in order to correct deficiencies and ensure future compliance within a reasonable time-frame. WoSign shall record, approve and report any corrective

action steps taken and/or action steps that are anticipated to correct the non-compliant areas. The annual audit shall confirm the improvements and corrective measures taken.

8.3 Self-Audits

As part of its Security Program, WoSign controls its service quality by performing ongoing self audits against a randomly selected sample of at least three percent (3%) of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

9. **OTHER BUSINESS AND LEGAL MATTERS**

9.1 Fees

WoSign charges Subscriber fees for some of the certificate services it offers, including issuance, renewal and reissuance. Such fees are detailed on the official WoSign websites (www.wosign.com, www.wosign.cn).
WoSign does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a WoSign issued certificate using Certificate Revocation Lists. WoSign retains its right to affect changes to such fees.

9.2 Financial responsibility

9.2.1. Insurance coverage

WoSign's operations related to the issuing of digital certificates are covered by a Commercial General Liability insurance (occurrence form) with policy limits of at least US$ 2 million in coverage, and Professional Liability/Errors & Omissions insurance with policy limits of at least US$ 5 million in coverage and include coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining digital certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

Certificates issued in accordance to the Extended Validation Guidelines shall be treated according to those guidelines as published by the CA/Browser Forum in respect to liability and insurance policy requirements. WoSign shall adhere to those requirements only for certificates explicitly marked as EV certificates and which were issued according to the EV guidelines.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance or warranty coverage for end-entities

In case of erroneous issuance of a digital certificate that resulted in a loss to a relying party, relying parties may be eligible under the certificate warranty to receive up to US$ 10,000 per incident. Except to the extent of willful misconduct, the liability of WoSign is limited to the negligent issuance of

certificates. The cumulative maximum liability of WoSign to all applicants, subscribers and relying parties for each certificate cumulative is set to US$ 10,000.

Beyond the coverage of the certificate insured warranty above, WoSign denies any responsibility for damages or impairments resulting from its operation and assumes no financial responsibility with respect of the use of any issued certificate or provided service.

9.3 Confidentiality of business information

See section 9.4

9.4 Privacy of personal information

WoSign respects the privacy of individuals and entities and shall not disclose personal details of certificate applicants or other identifying information it retains from and about them to third parties.

Any information about subscribers that is not publicly available through the content of the issued certificate, certificate directory and certificate revocation lists, shall be treated as private and regarded as protected information. Obtained private details and information shall not be used without the consent of the party to whom that information applies beyond the tasks WoSign has to perform for successful validation and verification purpose. WoSign shall save and secure subscriber information it retains from compromise and disclosure to

third parties and shall comply with applicable local privacy laws for the protection of such information. If disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents, WoSign shall be entitled to disclose private information to law officials without penalty.

9.5 Intellectual property rights

Digital certificates which are the result of the operations of WoSign, are at any given time and remain during their whole life-time the property of WoSign. Ownership of digital certificates issued by and through the operations of WoSign can't be claimed by subscribers, relying parties, software vendors or any other party. Issuance of a certificate to the end user gives the subscriber the right to use the issued certificate(s), subjected to the requirements and obligations set forth in this policy, acceptance of the terms and conditions of WoSign as published on the related web site(s) and to the extent of the key usage and extended key usage fields of the certificate, until expiration or revocation of the certificate, whichever comes first. WoSign exclusively retains the copyright of all certificates produced, created, published and issued by WoSign at all times and all rights are reserved.

9.6 Representations and warranties

See *EV Certificate Warranties and Representations* of the Extended Validation Guidelines.

9.7 Disclaimers of warranties

See section 9.8

9.8 Limitations of liability

WoSign gives no guaranties whatsoever about the security or suitability of the services provided that are identified by a certificate issued by WoSign or the use of thereof, including but not limited to the use of its websites and programs or any other service offered currently or in the future. The certification services are operated according to the highest possible levels of security and to the highest industry standards, but without any warranty.

Relying parties have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a certificate, and as such are solely responsible for deciding whether or not to rely on such information, and therefore shall bear the legal consequences of their failure to perform the Relying Party Obligations outlined in this policy.

Under no circumstances, including negligence, shall WoSign or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this or

other services, even if advised of the possibility of such damage.

9.9 Indemnities

By accepting or using a certificate, each Subscriber and Relying Party agrees to indemnify and hold WoSign, as well as any of its respective parent companies, subsidiaries, directors, officers, employees, agents, and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that WoSign, and/or the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from that party's: (i) misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional; (ii) violation of the Subscriber Agreement, Relying Party Agreement, this CPS, or any applicable law; (iii) compromise or unauthorized use of a Certificate or Private Key caused by the negligence of that party and not by WoSign (unless prior to such unauthorized use WoSign has received an authenticated request to revoke the Certificate); or (iv) misuse of the Certificate or Private Key.

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, WoSign understands and acknowledges that the Application Software Vendors who have a root certificate distribution agreement in place with WoSign do not assume any obligation or potential liability of WoSign under the EV Guidelines or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. WoSign shall defend, indemnify, and hold harmless each Application Software Vendor for any

and all claims, damages, and losses suffered by such Application Software Vendor related to a Certificate issued by WoSign, regardless of the cause of action or legal theory involved. This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to a Certificate issued by WoSign where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the online repository, and the software either failed to check such status or ignored an indication of revoked status).

9.10 Term and termination

See section 5.8

9.11 Individual notices and communications with participants

9.12 Amendments

WoSign is responsible for determining the suitability of certificate policies illustrated within this document. WoSign is also responsible for determining the suitability of proposed changes to the policy and practice statements prior to the publication of an amended version.

Subscribers and relaying parties will not be notified of impending changes of

the policy. The policy is legally binding from the moment of its publication.

Subscriber certificates for the Classes 1 through 4 include an policy identifier whose root OID is 1.3.6.1.4.1.36305.<policy>.<class-level>.<cert-type>.<major-version>.<minor-version>, where <major-version>.<minor-version> represents the policy version the identifier is referring to. Changes to the policy requires increasing of the policy version number by one. Extended Validation certificates may include additional policy identifiers for the recognition by software vendors.

Controls are in place to reasonably ensure that the policy and practice statements are not amended and published without the prior authorization by the management of WoSign.

9.13 Dispute resolution provisions

Disputes arising in relation to certificates issued according to the Extended Validation Guidelines as published by the CA/Browser Forum shall be treated according those guidelines and only to the extend and scope set forth by those guidelines. This may include different interpretation of applicable laws and the locality of jurisdiction. The parties may however agree to solve disputes under different applicable laws and jurisdiction.

9.14 Governing law

Any party involved shall try to resolve all disputes that might arise in a spirit of

cooperation without formal procedures. Any legal dispute which cannot be resolved without formal procedures shall take place in Hong Kong, China or at a different location if the parties agree or are ordered to do so by law.

9.15 Compliance with applicable law

This CPS shall be subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting or importing software, hardware or technical information.

9.16 Miscellaneous provisions

9.16.1. Entire agreement

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended usage of the product or service described herein. Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

9.16.2. Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent by WoSign.

9.16.3. Severability

Interpretation of legal disputes arising from the operation of WoSign shall be treated according to the Israeli legal system and laws.

If any term of this policy should be invalid under applicable laws, the affected term shall be replaced by the closest match according to applicable laws and the validity of the other terms should not be affected.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

9.16.5. Force Majeure

WOSIGN INCURS NO LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT ITS FAULT OR NEGLIGENCE.

9.16.6. Other provisions

Not applicable.