V10 Networks Certificate Practice Statement

1.0 Introduction

This document describes the Certificate Practice as administered by V10 Networks. This document outlines how we issue certificates, how we practice our security, how we determine eligibility and how we determine the length of our issued certificates.

2.0 Definition

“We” – As in V10 Networks

“CA” and/or “Certificate Authority” – Carries the same meaning as “We”

“Subordinate CA” and/or “Subordinate Certificate Authority (-ies)” – The certificate that has been issued for the purposes of further issuing certificates within our X.509 certification chain

“Root Certificate” – The Certificate used to authenticate issued certificates for Subordinate Certificate Authorities.

“Subordinate Certificate” – The Certificate issued by the Certificate Authority.

“PKI” – The Public Key Infrastructure as based on the X.509 Standard

“RSA” – Rivest, Shamir, Adleman algorithm for generating private keys

“ECDSA” – Elliptical Curve Digital Signature Algorithm

3.0 Scope of Document

This document only cover certificates issued with our X.509 based Public Key Infrastructure’s Private Keys and/or certificates.

4.0 Definition of Document with Object Identifier

This Certificate Practice Statement is defined with the Object Identifier 1.3.6.1.4.1.41734.10.0. This Object Identifier shall be static, regardless if the Certificate Authority renews the certificate due to the expiry of the root certificate.

Commented [JL1]: Should this typeface be Courier New?

For subordinate certificate authorities, their certificate practice statement’s object identifier shall have a prefix 1.3.6.1.4.1.41734.10.1. The unique object ID shall be assigned accordingly by the certificate authority.

5.0 Technical Details

5.1 Certificate Thumbprint and Serial Number

This CA’s certificate thumbprint is defined with the hexadecimal number
cb:a4:22:83:c9:09:d9:fb:26:6f:b6:f1:1a:1b:db:69:83:f6:70:40

The serial number for this CA is defined with the hexadecimal number
00:a2:27:2f:55:1d:d8:47:6b:84:c2:37:79:94:29:32:34:a6:1b:2e:84:ca
:07:0c:30:e9:38:1e:e8:ee:f4:13:d9

5.2 Certificate Revocation Lists

This CA’s Certificate Revocation List is available on the HTTP URI http://pki.v10networks.ca/root_crl.crl. The location to the Certificate Revocation List shall be embedded in Authority Information Access extension of the certificate. This requirement shall also extend to the Subordinate CA’s.

5.3 Minimum Private Key Length

The minimum Private Key length for the Root and Subordinate Certificate Authorities shall be at least 4096-bits, in RSA.

- Certificates issued by the subordinate CA shall have a minimum key length of 2048-bits; however the subordinate CA may raise the length as needed.

If the ECDSA algorithm is used for the subordinate certificate authorities in place of the RSA algorithm, a key length that is at least equivalent or better than the RSA 4096-bit private key shall be used.

5.4 Certificate hashing requirements

The Root CA shall at a minimum, use the SHA2 256 algorithm to hash certificates. Using older methods such as SHA-1 or MD5 is strictly forbidden under this statement and/or agreement.

6.0 Key Personnel

The following contacts below are the key personnel essential to the operation of the PKI system of V10 Network's Certification Authority

Technical Contact:

Jeff Leung
4-8220 Bennett Rd
Richmond BC V6Y 1N5
Canada

Phone: +1 (778) 803-5949
E-Mail: jleung@v10networks.ca

Administrative Contact:

Jeff Leung
4-8220 Bennett Rd
Richmond BC V6Y 1N5
Canada

Phone: +1 (778) 803-5949
E-Mail: jleung@v10networks.ca

7.0 Usage of Certificate

7.1 Root Certificate

The usage of the Root Certificate shall be restricted to issuing certificates to Subordinate Certificate Authorities. An example of such restriction, but not limited to is using the root certificate for a web server that is either meant to authenticate or encrypt traffic between the end-user and the web server.

7.2 Subordinate Certificate(s)

The usage of the Subordinate Certificate(s) shall be restricted to issuing certificates to end-users unless authorized. An example of such restriction, but not limited to is using the root certificate for a web server that is either meant to authenticate or encrypt traffic between the end-user and the web server.

8.0 Certificate Authority's Security Obligations

8.1 Root Certificate Authority

The Certificate Authority shall maintain the private key used to sign certificates for Subordinate CA's in an environment that is not connected to the public internet. The Certificate Authority is also obliged to store the Private Key in a physically secure environment. When feasible, the Certificate Authority may encrypt the Private Key with a strong passphrase.

8.2 Subordinate Certificate Authorities

The Certificate Authority shall maintain the private key used to sign certificates for Subordinate CA's in a reasonably secure environment. The Subordinate Certificate Authority is also obliged to archive the Private Key in a physically secure environment. When feasible, the Subordinate Certificate Authorities may encrypt the Private Key with a strong passphrase.

9.0 Validity

9.1 Root Certificate

The Root Certificate has a maximum validity period of 30 years.

9.2 Subordinate Certificates

The Subordinate CA Certificates shall have a maximum validity period of 15 years, but not exceeding the expiry date of the root certificate.

Certificates issued from the Subordinate CA shall not exceed the validity period of the Subordinate CA certificate itself.

10.0 Eligibility

10.1 Subordinate Certificate Authorities

- The only eligible entity for receiving Subordinate CA certificates from the CA is only limited to V10 Network's own internal systems and/or departments. However the Subordinate CA's may issue certificate to external entities if permitted under an agreement and/or is designated to do so.

11.0 Requirement of Certificate Revocation Lists

11.1 Requirement to Publish:

- The CA shall publish a Certificate Revocation List. The revocation list shall be published at least every 30 calendar days.
- The Subordinate CA shall publish a Certificate Revocation List. The revocation list shall be published at least every 30 calendar days.

11.2 Requirement for providing a OCSP(Online Certificate Status Protocol) Server

- The CA may optionally provide an OCSP responder if technically feasible under the network infrastructure.
- The Subordinate CA may provide an OSCP responder if technically feasible under their current network infrastructure.

11.3 Requirement to revoke certificates

The CA shall revoke the certificates when the following condition occurs:

- The Subordinate CA's private key becomes compromised.
- The Subordinate CA has been obtained via fraudulent and/or misleading means.
- The Subordinate CA has violated conditions set out in their Certificate Practice Statement.

The Subordinate CA shall follow the requirement to revoke as laid out above; however they may impose additional conditions if they see fit during the course of operation.

Once a certificate has been revoked the CA and/or subordinate CA shall deny requests from the subordinate CA and/or end-user if they generate a certificate request using the same private/public key pair.

12.0 Observation of External Policies

At this time, the Root Certificate Authority shall observe the following policies as set out by CA/Browser Forum

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- Guidelines For The Issuance And Management Of Extended Validation Certificates

Should there be any discrepancies between this Certificate Practice Statement and the two guidelines mentioned above, the guidelines above take precedence in lieu of this Certificate Practice Statement.

13.0 Certificate Practice Statement Acting as Legal Agreement Between CA and Subordinate CA's

In most cases, the Certificate Practice Statements drafted by V10 Networks for subordinate certificate authorities shall also act as an agreement between the CA and the Subordinate CA; however the CA may impose a legal contract and/or agreement if the Certificate Practice Statement has been drafted by the subordinate CA and/or under the discretion of the CA.

14.0 Legal

14.1 Ownership of Certificate

All Certificates issued by V10 Networks remain the property of V10 Networks, including certificates issued by Subordinate CA's. End-Users and/or subordinate CA's shall never claim ownership of certificate even if it was issued to them. The identified subject has the right to operate the certificate subject to an agreement, unless otherwise revoked by the Certificate Authority.

14.2 Limitation of Liabilities

The root CA gives no guaranties whatsoever about the integrity and/or security of the goods or services provided by the subjects as identified in the certificates issued by the root CA. Nor does the CA endorse and/or approve any services provided by the parties identified in the certificate.

It is the sole responsibility of the end-user to determine if the subject certified by V10 Networks and/or any of their subordinate CA’s is suitable to provide such goods and or services.

Although the root CA has demonstrated the amount of due diligence to ensure the security and integrity of issued certificates, but without any guarantees or warranty.

In no event shall V10 Networks be liable or responsible for any direct, indirect, incidental, special, exemplary or consequential damages

14.3 Compliance of Applicable Law

The Certificate Authority and the subordinate Certificate Authorities shall meet compliance with applicable Canadian laws while retaining the interest of its subordinate Certificate Authorities.

14.4 Term and Termination

This Certificate Practice Statement shall remain in full force until a new amendment supersedes the CPS.

14.5 Amendments

Amendments will be published in an online repository as defined in the CPS extension of the Certificate. The Certificate Authority shall have measures to reasonably unauthorized amendments from being in that said online repository.

14.6 Force Majeure

V10 NETWORKS CERTIFICATION AUTHORITY INCURS NO LIBABILITIES IF IT IS PREVENTED OR FORBIDDEN OR DEPLAYED FROM PERFOMRING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: ANY PROVISON OF ANY APPLICABLE CANADIAN LAW OR MILITARY AUTHORITY; FAILURE OF ANY COMMUNICATION SYSTEMS OR ELECTRICAL SYSTEMS OR ANY OTHER SYSTEMS OPERATED BY ANY PARTIES OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD OR NATURAL DISASTERS; ACTS OF TERRORISM OR WAR; ACTS OF GOD; OR SIMILAR CAUSES BEYOND REASONABLE CONTROL AND WITHOUT ITS FAULT OR NEGLIENCE.

14.7 Other Stipulations

None at this time.