# Summary of changes

# Highlighted additions and deletions in yellow that haven’t been changed by Ben Wilson have been suggested by Doug Beattie of GlobalSign

# Added a new 3rd column “As of 1/2017” which specifies the Cryptographic Algorithm and Key Requirements for SSL Certificates and the CA certificates in the chain required for SSL Certificates to be properly validated on, or after 1/1/2017.

# Ben Wilson edited this heading for Root CAs to specify that a Root CA issued on 1/1/2016 can’t be a SHA1 and note \*\* was edited to add “[a Root CA Certificate] issued with SHA-1 prior to January 1, 2016, MAY still serve as a trust anchor for Subscriber Certificates .

# When the requirements do not change from one milestone (column) to the next, said “No Change” instead of repeating the parameters, for clarity.

# Added “Cross Certificates” to the heading for Subordinate CAs. I believe they should be treated the same and we need a specification for cross certificates.

# Deleted the following footnote and references to it because we now have a date for this transition:

# \* SHA-1 MAY be used with RSA keys until SHA-256 is supported widely by browsers used by a substantial portion of relying-parties worldwide.

# Just to make this more clear, I rejected a few deletions of the “\*” footnote and rephrased this to read, “SHA-1 has been deprecated, although it MAY be used with RSA keys to sign Subordinate CA Certificates, Cross Certificates, and Subscriber Certificates until January 1, 2016. SHA-256 is CAs SHOULD advise their Customers that Subscriber Certificates signed with SHA1 will stop working in major browsers on January 1, 2017supported widely by browsers used by a substantial portion of relying-parties worldwide.”

* Split the rows for “Minimum DSA modulus and divisor size (bits)” into two rows (one for modulus and one for divisor) – the repeated info was not clear in the table.
* I have put the rows back together and tried to explain the significance of L N p and q. Then, hidden in the same footnote “\*\*”, I noticed that we said these things, so I just deleted it in the footnote.

# Appendix A ‐ Cryptographic Algorithm and Key Requirements (Normative)

Certificates MUST meet the following requirements for algorithm type and key size.

#### Root CA Certificates

|  |  |  |  |
| --- | --- | --- | --- |
|  | Validity period beginning on or before 31 Dec 2010 | Validity period beginning after 31 Dec 2010 | Validity period beginning after 1 January 2016\*\* |
| Digest algorithm | MD5 (NOT RECOMMENDED)  SHA-1, SHA-256, SHA-384 or SHA- 512 | SHA-1~~\*~~, SHA-256, SHA-384 or SHA-512 | SHA-256, SHA-384 or SHA-512 |
| Minimum RSA modulus size (bits) | 2048\*\* | 2048 | No Change |
| ECC curve | NIST P-256, P-384, or P-521 | No change | No Change |
| Minimum  DSA modulus (*p*) size “L” (in bits) and “N“ is length of divisor *q* of *p*-1 | FIPS186-allowed tuples (L,N):  L= 2048, N= 224,  L= 2048, N= 256, and  L= 3072, N=256 | No change | No Change |

#### Subordinate CA Certificates and Cross Certificates

|  |  |  |  |
| --- | --- | --- | --- |
|  | Validity period beginning  on or before 31 Dec 2010 and ending on or before 31 Dec 2013 | Validity period beginning after 31 Dec 2013 and ending before 31 Dec 2015 | As of 1 January 2017 |
| Digest algorithm | SHA-1, SHA-256, SHA-384 or SHA- 512 | No change | SHA-256, SHA-384 or SHA-512 |
| Minimum RSA modulus size (bits) | 1024 | 2048 | 2048 |
| ECC curve | NIST P-256, P-384, or P-521 | No change | No change |
| Minimum  DSA modulus size (bits) | L= 2048, N= 224 or  L= 2048, N= 256, | No change | No Change |
| Minimum  DSA divisor (*p*)  size “L” (in bits) and “N” is length of divisor *q* of *p*-1 | FIPS186-allowed tuples (L,N):  L= 2048, N= 224 or  L= 2048, N= 256, | No change | No Change |

#### Subscriber Certificates

|  |  |  |  |
| --- | --- | --- | --- |
|  | Validity period ending on or before 31 Dec 2013 | Validity period ending after 31 Dec 2013 or before 31 Dec 2016 | As of 1 January 2017 |
| Digest algorithm | SHA1~~\*~~, SHA-256, SHA-384 or SHA- 512 | SHA-1\*, SHA-256, SHA-384 or SHA-512 | SHA-256, SHA-384 or SHA-512 |
| Minimum RSA modulus size (bits) | 1024 | 2048 | 2048 |
| ECC curve | NIST P-256, P-384, or P-521 | No change | No change |
| Minimum  DSA modulus size (bits) | L= 2048, N= 224 or  L= 2048, N= 256, | No change | No Change |
| Minimum  DSA divisor (*p*)  size “L” (in bits) and “N” is length of divisor *q* of *p*-1 | FIPS186-allowed tuples (L,N):  L= 2048, N= 224 or  L= 2048, N= 256, | No change | No Change |

\* SHA-1 has been deprecated, although it MAY be used with RSA keys to sign Subordinate CA Certificates, Cross Certificates, and Subscriber Certificates until January 1, 2016. CAs SHOULD advise their Customers that Subscriber Certificates signed with SHA1 will stop working in major browsers on January 1, 2017.

\*\* A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits or one issued with SHA-1 prior to January 1, 2016, MAY still serve as a trust anchor for Subscriber Certificates issued in accordance with these Requirements.

#### General requirements for public keys

RSA: The CA SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 216+1 and 2256-1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89].

DSA: Although FIPS 800-57 says that domain parameters may be made available at some accessible site, compliant DSA certificates MUST include all domain parameters. This is to insure maximum interoperability among relying party software. The CA MUST confirm that the value of the public key has the unique correct representation and range in the field, and that the key has the correct order in the subgroup. [Source: Section 5.3.1, NIST SP 800-89].

ECC: The CA SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.5 and 5.6.2.6, respectively, NIST SP 800- 56A].