CA's Self-Assessment of CP/CPS documents to CA/Browse

Introduction :
1) Network Solutions Certificate Authority
2) Audit will evaluate and cover the following root certificates, of
Network Solutions Certificate Authority
(SHA-2) Network Solutions ECC Certificate Authority
(SHA-2) Network Solutions ECC EV Server CA
(SHA-2) Network Solutions RSA Certificate Authority
(SHA-2) Network Solutions RSA EV Server CA
Network Solutions Certificate Authority
Network Solutions DV Server CA 2
Network Solutions EV Server CA 2
Network Solutions OV Server CA 2

3) Used Baseline Requirements v. 1.5.6
4) CPS Statements were updated and evaluated by legal team a
https://legal.web.com/Document/Get/CertificationPracticeStatem
https://legal.web.com/Document/Get/CPSforEVCertification?lang
5) Network Solutions will notate below anything that we are work

BR Section Number
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*
1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. *Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.*
2.1. Repositories *Provide the direct URLs to the CA's repositories*

2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." *--> Copy the specific text that is used into the explanation in this row. (in English)*
2.2. Publication of information "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." *--> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.*
2.3. Time or frequency of publication *Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.*
2.4. Access controls on repositories *Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.*

3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, *indicate how your CP/CPS meets the requirements in this section of the BRs.*
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, *indicate how your CP/CPS meets the requirements in this section of the BRs.*
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, *indicate how your CP/CPS meets the requirements in this section of the BRs.*
3.2.2.4 Validation of Domain Authorization or Control *Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's CP/CPS must clearly describe the acceptable methods of domain validation.* ***It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.***
3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*
3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*

3.2.2.4.8 IP Address If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*
3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, *indicate how your CA meets the requirements in this section of the BRs.*
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then *indicate how your CA meets the requirements in this seciton of the BRs.*
3.2.2.7 Data Source Accuracy *Indicate how your CA meets the requirements in this section of the BRs.*
3.2.2.8 CAs MUST check and process CAA records *Indicate your CA's understanding that this section is a requirement as of September 8, 2017, and how your CA meets the requirements in this section of the BRs.*
3.2.3. Authentication of Individual Identity
3.2.5. Validation of Authority
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.

4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.
4.1.2. Enrollment Process and Responsibilities
4.2. Certificate application processing
4.2.1 Re-use of validation information is limited to 825 days *Indicate your CA's understanding that this is a requirement as of March 1, 2018, and indicate how your CA meets the requirements of this section.*
4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.*
4.2.2. Approval or Rejection of Certificate Applications
4.3.1. CA Actions during Certificate Issuance
4.9.1.1 Reasons for Revoking a Subscriber Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking certificates.*

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking subordinate CA certificates.*
4.9.2. Who Can Request Revocation
4.9.3. Procedure for Revocation Request
4.9.5. Time within which CA Must Process the Revocation Request

4.9.7. CRL Issuance Frequency
Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.

4.9.9. On-line Revocation/Status Checking Availability
4.9.10. On-line Revocation Checking Requirements *Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.*
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.
4.10.1. Operational Characteristics
4.10.2. Service Availability
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS
5.2.2. Number of Individuals Required per Task
5.3.1. Qualifications, Experience, and Clearance Requirements
5.3.3. Training Requirements and Procedures
5.3.4. Retraining Frequency and Requirements
5.3.7. Independent Contractor Controls
5.4.1. Types of Events Recorded *Indicate how your CA meets the requirements of this section.*

5.4.3. Retention Period for Audit Logs
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*
5.5.2. Retention Period for Archive
5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*
6.1.1. Key Pair Generation
6.1.2. Private Key Delivery to Subscriber
6.1.5. Key Sizes
6.1.6. Public Key Parameters Generation and Quality Checking
6.1.7. Key Usage Purposes
6.2. Private Key Protection and Cryptographic Module Engineering Controls
6.2.5. Private Key Archival
6.2.6. Private Key Transfer into or from a Cryptographic Module
6.2.7. Private Key Storage on Cryptographic Module

6.3.2 Certificates issued after March 1, 2018, MUST have a Validity Period no greater than 825 days *Indicate how your CA meets the requirements of this section.*
6.5.1. Specific Computer Security Technical Requirements The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance. *Indicate how your CA meets the requirements of this section.*
7.1. Certificate profile CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG. *Indicate how your CA meets the requirements of this section.*
7.1.1. Version Number(s)
7.1.2. Certificate Content and Extensions; Application of RFC 5280
7.1.2.1 Root CA Certificate
7.1.2.2 Subordinate CA Certificate
7.1.2.3 Subscriber Certificate
7.1.2.4 All Certificates
7.1.2.5 Application of RFC 5280
7.1.3. Algorithm Object Identifiers
7.1.4. Name Forms
7.1.4.1 Issuer Information
7.1.4.2 Subject Information - Subscriber Certificates

7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates
7.1.5. Name Constraints *Indicate your CA's understanding of Mozilla's requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section.*
7.1.6. Certificate Policy Object Identifier
7.1.6.1 Reserved Certificate Policy Identifiers
7.1.6.2 Root CA Certificates
7.1.6.3 Subordinate CA Certificates
7.1.6.4 Subscriber Certificates
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS
8.1. Frequency or circumstances of assessment The period during which the CA issues Certificates SHALL be dividied into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration. For new CA Certificates: The point-in-time readiness assessment SHAL be completed no earlier than twelve months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate. *Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.*
8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*
8.4. Topics covered by assessment
8.6. Communication of results

Also indicate your understanding and compliance with Mozilla's Root Store Policy, which says:
"Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps).
....
The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information:
- name of the company being audited;
- name and address of the organization performing the audit;
- Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope;
- audit criteria (with version number) that were used to audit each of the certificates;
- a list of the CA policy documents (with version numbers) referenced during the audit;
- whether the audit is for a period of time or a point in time;
- the start date and end date of the period, for those that cover a period of time;
- the point-in-time date, for those that are for a point in time;
- the date the report was issued (which will necessarily be after the end date or point-in-time date); and
- For ETSI, a statement to indicate if the audit was a full audit, and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements for trust service providers).
"

8.7. Self-Audits

9.6.1. CA Representations and Warranties

9.6.3. Subscriber Representations and Warranties

9.8. Limitations of liability

9.9.1. Indemnification by CAs
9.16.3. Severability

r Forum Baseline Requirements (BRs)

which all passed the 2016-2017 audit.

t Network Solutions and Web.com.
ent?language=English
guage=English
ing to update this year.

List the specific documents and section numbers of those documents which meet the requirements of each BR section
Network Solutions Certification Practice Statement
Network Solutions Certification Practice Statement
Network Solutions does delegate tasks to third parties. CPS section 1.11
https://legal.web.com/TermsAndConditions/SslRepository

Network Solutions Certification Practice Statement section 3.12

SSL Repository contains:
Certification Practice Statement
CPSforEVCertifiation
Extended Validation (EV) Certificate Subscriber Agreement
Relying Party Agreement Party Agreement
Relying Party Guarantee
SSL Certificate and Assured Site Seal Subscriber Agreement

We disclose this information on CPS section 2.12.4. Also, subject identification is listed in cooresponding tab attached to this file.
We disclose this information on CPS section 2.12.4. Also, subject identification is listed in cooresponding tab attached to this file.
We disclose this information on CPS section 2.12.4. Also, subject identification is listed in cooresponding tab attached to this file.
CPS Section 4.2.1 Secure Server Certificate Application Validation Process
CPS Section 4.2.1 Secure Server Certificate Application Validation Process
CPS Section 4.2.1 Secure Server Certificate Application Validation Process
CPS Section 4.2.1 Secure Server Certificate Application Validation Process
CPS Section 4.2.1 Secure Server Certificate Application Validation Process
CPS Section 4.2.1 Secure Server Certificate Application Validation Process

CPS Section 4.2.1 Secure Server Certificate Application Validation Process
CPS Section 4.2.4 Certificate Authority Authorization
CPS 4.2.4
CPS Sections 1.2.1 and 4.3.3
CPS Section 2.1.1 and lifecycle management 3.5.1

CPS Sections 5.29 and 5.30
CPS Section 4.1
CPS Section 4.1
CPS Section 1.6
Not applicable to Network Solutions
Not applicable to Network Solutions
CPS 4.13, 4.13.1 and 4.13.2

CPS 4.13, 4.13.1 and 4.13.2
CPS section 4.13 of Network Solutions Certification Practice Statement
CPS section 4.13 of Network Solutions Certification Practice Statement
CPS section 4.13 of Network Solutions Certification Practice Statement
CPS 4.13.2
CPS section 4.13 of Network Solutions Certification Practice Statement
Not listed in CPS, as handled by Comodo per contractual agreement.
Not applicable to Network Solutions
CPS 1.5
CPS 1.5
CPS 2.1.6 and 2.2
CPS 1.2
Not listed in CPS
CPS 5.17
CPS 5.17
CPS 5.17
CPS 6.4

See section 3.5.4 Log Retention Period in Certification Practice Statement
Provided to EY during audit assessment period. Not publically displayed.
See sections 2.13 and 3.5.4 Log Retention Period in Certification Practice Statement
CPS 2.1.6 and 2.2
CPS 2.1.1
CPS 2.1.1
CPS 2.1.1
CPS 2.1.2
CPS 2.1.2
CPS 2.8
CPS 2.1.3
Not applicable to Network Solutions, as reflected in CPS 2.7
CPS 2.8

CPS 4.8
CPS 1.7
CPS 4.42
CPS 1.2.1
CPS 4.2.4
2.12.1
CPS 5.15
CPS 2.10
CPS 2.12.1 also, roots are exact as listed on cooresponding tab and on WebTrust audit reports
CPS 2.6.1
CPS 4.1.1
CPS 4.3.1
CPS 2.10.1

CPS 2.10.1
CPS 2.6.2
CPS 4.1.1
CPS 4.1.1
https://cert.webtrust.org/ViewSeal?id=2290
https://cert.webtrust.org/ViewSeal?id=2292
CPS 2.10, 2.10.1
CPS 1.5 - Annual audits by Ernst & Young for SSL products
CPS 1.5 - Annual audits by Ernst & Young for SSL products
CPS 1.5 - Annual audits by Ernst & Young for SSL products
CPS 1.5 - Annual audits by Ernst & Young for SSL products

Self audit is provided to EY during audit assessment period. Not publically displayed.
CPS 5.27 and 5.28
CPS 5.16 and 5.17
CPS 5.3

CPS 5.3.6
CPS 5.42

(SHA-2)

Version 2.8

Version 1.6

Explain how the CA's listed documents meet the requirements of each BR section.
Network Solutions has reviewed each item in section 1.2.1 and do acknowledge this CA is in compliance with all the forum ballot items. We completed 1.4.4 in February 2018. We have plans to integrate CNAME validation method in preparation for new root certs to be included in Q4 of 2018. We do not use the not permitted validation methods as stated in ballot 218.
Network Solutions intends to include the most current link to the official version 1.5.6 in the upcoming quarterly revision, on or before June 30, to the CPS statement, adding the suggested clause as mentioned in section 2.2 Publication of Information.
We do allow for deligated third parties, specifically, Comodo, to represent and assist our CA to validate organizational subject details in OV and EV to maintain and fullfill best business practices and validation standards.
SSL Legal Repository is available from Network Solutions 'legal' link in website footer.

Network Solutions conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published by the Certificate Authority/Browser Forum at http://www.cabforum.org. In the event of any inconsistency between this CPS and the Baseline Requirements, the Baseline Requirements take precedence over this document. CPS Statements were updated and evaluated by legal team at Network Solutions and Web.com on March 31, 2018. As stated in section 1.2.2, Network Solutions intends to include the most current link to the official BR version 1.5.6 in the upcoming quarterly revision, on or before June 30, to the CPS statement, adding the suggested clause as mentioned in section 2.2 Publication of Information.
CN=Network Solutions https://www.networksolutions.com/ https://www.current-expired-ns-cert.com/ https://www.current-revoked-ns-cert.com/ CN= Network Solutions Certificate Authority https://www.networksolutions.com/ https://www.current-expired-ns-cert.com https://www.current-revoked-ns-cert.com CN= Network Solutions ECC Certificate Authority https://netsolencryption.com https://ecc-expired-ns-cert.com/ https://ecc-revoked-ns-cert.com/ CN= Network Solutions RSA Certificate Authority https://www.rsa-valid-ns-cert.com/ https://www.rsa-expired-ns-cert.com/ https://www.rsa-revoked-ns-cert.com/
We review the CPS statements on a quarterly basis and update the document as necessary and required based on CAB guidelines and ballot issues. The latest update was completed on March 31, 2018.
All CPS and SSL Repositories will continue to remain publicly available at this location: https://legal.web.com/

Yes, we are in compliance and make the Subject Identity information publically available in both CPS statements.
We only insert the subject:countryName field for OV and EV SSL certificates, and do not insert it for DV certificates, so the countryName always relates to the subject identity as verified in our CPS section 2.12.4
We do not use this validating method.
We do not use this validating method.
This method is rarely utilized and is under consideration for removal on our upcoming CPS revision at the end of Q2.

We do not use this validating method.
We do not use this validating method.
We do not use this validating method.
This method is rarely utilized and is under consideration for removal on our upcoming CPS revision at the end of Q2.
We coordinate with Comodo when necessary to use an automated process to fetch the Public Suffix List. We use the data in the PSL to determine if a domain to which a wildcard is to be prepended is a public suffix.
We securely collect data from customers when they request certs to be issued. The list of Reliable Data Sources that we use verify Subject Identity information is a fixed list from which our validators (and systems) may not vary. When
We understand and comply with the requirements of 3.2.2.8, using the method stated in our CPS.
• Legal Name of the Individual (PUBLIC) • Organizational unit (PUBLIC) • Street, city, postal/zip code, country (PUBLIC) • Server Software Identification • Payment Information • Administrator contact full name, email address and telephone • Billing contact persons and organizational representative • Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC) • Public Key (PUBLIC) • Proof of registration of domain name • Proof of existence and organizational status of the Organization • Subscriber agreement, signed or agreed to online
Disclosed in the CCADB

Following best practices of CCADB, Network Solutions checks credentials against accounts. When previous attempts have been made to obtain a certificate and either issuance was blocked or a certificate revoked because of suspected fraud or other violation of terms of the subscriber agreement, we can suspend and blacklist IP addresses from which such applications have been made. We also have the ability to blacklist domain names where we become aware that the domain has been used for faudulent use or otherwise has been the subject of activity counter to the terms of the subscriber agreement.
Network Solutions has implemented this requirement to limit the re-use of validation information to 825 days.
We have a process which examines subject details and domain names, for matches or near matches to some known high profile or pre-notified names that may indicate that a certificate is at a higher than normal risk of fraudulent applications being made and in those cases we flag a certificate application for a manual review.
There is an automated feed of new gTLDs from ICANN and our system incorporates checks on the validity of the domain name taking the list of gTLDs into account. This section actually has very little effect as we have not been able to issue trusted certificates for Internal Names for some time.
The only certificates we issue from our root CAs are intermediate CA certificates. Our CA has no facility for the automated signature of such certificates, so this activity necessarily involves manual intervention by privileged users to sign such certificates.
The reasons for revoking certs: 1) Requests from customers 2) Insufficient payment or fraud detected 3) AUP suspension occurs to customer. 4) Revoke based on abuse report. While we comply in fact with the requirements of BR 4.9.1.1, our CPS does not delineate all of the options offered by BR 4.9.1.1. We will add to the CPS the delta needed to make explicit all of the options available under BR 4.9.1.1 in the next CPS revision, scheduled for end of June.

We have a contractual relationship with Comodo that would explain the nature of a revocation incident.
Customers, Web.com, Comodo
Outlined in the CPS and CPS for EV. Authorized agent level employees, with the permission of the customer, may request to revoke their certificate. This is done through the Network Solutions Secure SSL Control Panel within the Account Manager.
We will abide by the requirements that mandate review within 24 hours.
An updated CRL is published on the Network Solutions website every 24 hours, however under special circumstances the CRL may be published more frequently. Example of a revoked certificate : https://www.current-revoked-ns-cert.com/
The SSL Control Panel available to customers in the Account Manager will confirm the status.
We rely on the contractual agreement with Comodo that has OCSP responders which support both GET and POST requests. Their OCSP responses are valid for 96 hours (4 days). As stated in 7.3, our OCSP responders are capable of providing a 'good' or 'revoked' status for all certificates issued under the terms of this CPS.
We support stapling but do not enforce its use and do not amend our CPS where stapling is to be used.
Network Solutions CA operates an ISO27001 compliant ISMS which, as well as the WebTrust audits, is subject to SOC2 and SOC3 audits.
Over 45 in various capacities: Technical, Organizational, Practices and Legal.
We do not to list this information publically.
From time to time, events outside of the control of Network Solutions may delay the issuance process however Network Solutions will make every reasonable effort to meet issuance times and to make applicants aware of any factors that may affect issuance times in a timely manner.

Network Solutions follows a protocol to retain the audit logs for a period of seven years.
We conduct an annual risk assessment on our certificate authority as part of our ISMS operation. This is subject to audit under WebTrust.
Network Solutions maintains logs for a period of seven years to comply with applicable laws.
We have a business continuity plan. We have multiple locations from which our CA could operate.
The UTN and AddTrust CA Root key pairs are protected in accordance with an AICPA/CICA WebTrust program compliant infrastructure and CPS.Network Solutions ensures the protection of its CA Root signing key pairs with the use of Hardware Signing Module (HSM) devices, which are certified to FIPS 140-2 Level 3 or higher, for key generation, storage and use.
We don't openly provide a private key to users as we install the certs for them on our hosting platform. However, If we have a request from customer to attain their private key we provide an encrypted file, which the end user must be able to decrypt.
2048
We verify RSA and ECDSA keys, including subscriber keys per BR 6.1.6.
Installation
Network Solutions strongly urges Subscribers to use a password or equivalent authentication method to prevent unauthorized access and usage of the Subscriber private key. The Subscriber is solely responsible for protection of the Subscriber's private keys. Network Solutions maintains no involvement in the generation, protection or distribution of such keys as part of the Certificate services.
When the Network Solutions CA Root Signing Key pair expire they will be archived for at least 7 years. The keys will be archived in a secure cryptographic hardware module as per their secure storage prior to expiration, as detailed in section 2.1.1 of this CPS.
We do not provide this to users.
We do not priovide storage on this platform.

Network Solutions has removed the ability on storefront and in all backend billing and processing systems to sell or renew any 3 year term certificates as of March 1, 2018.
Network Solutions relies on UTN-USERFIRST-Hardware, AddTrust External CA Root for its Root CA Certificates for Digital Certificates issued after July 20, 2006. These relationships allow Network Solutions to issue highly trusted Digital Certificates by inheriting the trust level associated with the UTN root certificate named UTN-USERFIRST-Hardware and the AddTrust root certificate named AddTrust External CA Root.
Network Solutions CA generates 128 bit serial numbers as provided from a secure API call to Comodo. The numbers are the output of a CSPRNG. We have a separate uniqueness check that verifies that serial numbers are never re-used.
All Network Solutions certificate are x.509 v3
Network Solutions complies with all of the requirements of BR 7.1.2 and its sub-sections. We will consider the need to add this to the upcoming CPS statement update within the audit period.
In compliance and in progress with audit of all certificates from June 30, 2017 to March 31, 2018
Network Solutions refrains from using the subscriber's private key corresponding to the public key in a Network Solutions issued certificate to issue end-entity SSL Certificate or subordinate CAs
Network solutions follows recommended extensions id-qt 1 (RFC 5280]
In compliance and in progress with audit of all certificates from June 30, 2017 to March 31, 2018
Network Solutions does not consider a precertificate to qualify or be considered a certificate.
Network Solutions does not issue SHA-1 certificates under these guidelines. Additionally, we do not issue SHA-2 end entity certificates from SHA-1 subordinate CAs.
Acceptable names are listed in the CPS section 4.3.1.
Network Solutions CA certificates, the content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support Name chaining.
In compliance

In compliance
Network Solutions understands the requirement to disclose all subordinate CA certificates that are not technically contrained by name.
Network Solutions understands and complies with the BRs 7.1.6 concerning the use of Policy Object Identifiers. We will clarify in CPS in the next revision within the upcoming audit period July 2018.
We understand and comply with annual audits that do not have any gaps or unbroken sequence of audits. The upcoming audit will cover July 1, 2017 to March 31, 2018.
Network Solutions CA engages EY LLC to perform WebTrust audits. EY are independannt from us, are skilled in performing WebTrust for CAs audits, employ properly trained and skilled individuals to perform the audits, are bound by a professional code of ethics, and maintains professional LE&O insurance of > $1m.
Every year, Network Solutions provides EY with evidence that we maintain the integrity of keys and certificates, along with protection for the lifecycle of the SSLs. Information of the subscriber is properly collected and authenticated.
See audit WebTrust reports and management assertions.

We comply with Mozilla's root store policy to follow best practices related to audit compliance, in that we maintain a strict adherance to the annual schedule as set forth by the EY organization and CAB forum policy.
The Legal department and Product Manager at Network Solutions complete regular self audits of all SSL products under management and provide necessary evidence every audit period.
Network Solutions certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, intended purpose of the certificate and disclaimers of warranty that may apply. Subscribers must agree to Network Solutions Certificate and Site Seal Subscriber Agreement before signing-up for a certificate, as well as agreeing to bind their relying parties to the Network Solutions Relying Party Agreement.
In compliance
In compliance

In compliance
In compliance