Network Solutions Certification Practice Statement

Version 2.8

Table of Contents

Terms and Acronyms Used in the CPS Acronyms:

CA Certificate Authority
CPS Certification Practice Statement
CRL Certificate Revocation List
CSR Certificate Signing Request
EPKI Enterprise Public Key Infrastructure Manager
FTP File Transfer Protocol

HTTP Hypertext Transfer Protocol
ITU International Telecommunication Union
ITU-T ITU Telecommunication Standardization Sector
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

Terms:

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

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.

Digital Certificate or Certificate shall mean a digitally signed message that contains a Subscriber's public key and associates it with information authenticated by Network Solutions or a Network Solutions-authorized entity.

Network Solutions Site Seal shall mean a hyperlinked graphic provided by Network Solutions to a Subscriber for display on the Subscriber's web site that identifies the Subscriber as the holder of a Network Solutions Digital Certificate and/or having been properly vetted as a valid entity as defined in this CPS. A Network Solutions Site Seal can be a Network Solutions Secure Site Seals or a Network Solutions Assured Site Seal.

Network Solutions Secure Site Seal shall mean a hyperlinked graphic provided by Network Solutions to a Subscriber for display on the Subscriber's web site that identifies the subscriber as the holder of a Network Solutions SSL Certificate and that the Subscriber has been validated in accordance with the standards set forth in the Network Solutions CPS related to SSL Certificates. When the Secure Site Seal is selected by a user, the user's browser is directed to open a SSL-encrypted link to a Network Solutions site to verify that the Secure Site Seal holder has been issued a Network Solutions SSL Certificate and has been validated in accordance with the standards set forth in the Network Solutions CPS. The Network Solutions site sends to the user's browser over the SSL-encrypted link a message indicating the results of the verification along with other information. The response from the Network Solutions site can be displayed on the user's browser as a graphic or web page (that can include client-executable code) containing information about the organization or person to whom the Secure Site Seal pertains and the result of the requested verification. The Secure Site Seal accompanies any issued Network Solutions SSL Certificate and shares the guarantee level associated with the SSL Certificate it accompanies.

Network Solutions Assured Site Seal shall mean a hyperlinked graphic provided by Network Solutions to a Subscriber for display on the Subscriber's web site to indicate that the Subscriber has been validated in accordance with the standards set forth in the Network Solutions CPS related to Digital Certificates. When the Assured Site Seal is selected by a user, the user's browser is directed to open a SSL-encrypted link to a Network Solutions site to verify that the Network Solutions Assured Site Seal holder has been validated in accordance with the standards set forth in the Network Solutions CPS. The Network Solutions site sends to the user's browser over the SSL-encrypted link a message indicating the results of the verification along with other information. The response from the Network Solutions site can be displayed on the user's browser as a graphic or web page (that can include client-executable code) containing information about the organization or person to whom the Assured Site Seal pertains and the result of the requested verification.

Relying Party: The Relying Party is an entity that relies upon the information contained within the Certificate and/or Network Solutions Site Seal.

Relying Party Agreement: The Relying Party Agreement is an agreement which must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate, relying on a Network Solutions Site Seal, or accessing or using Network Solutions' Repository, and is available for reference at http://www.networksolutions.com/legal/SSL-legal-repository-rpa.jsp.

Subscriber: The Subscriber is an entity that has been issued a Certificate and/or Network Solutions Site Seal.

Subscriber Agreement: The Subscriber Agreement is an agreement which must be read and accepted by an Applicant before applying for a Certificate or a Network Solutions Site Seal. The Subscriber Agreement is available for reference at http://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp.

1. GENERAL
This document is the Network Solutions Certification Practice Statement: Basic, Advanced, Wildcard (CPS) and outlines the legal, commercial and technical principles and practices that Network Solutions employs 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 Network Solutions. It also defines the underlying certification processes for Subscribers and describes Network Solutions' repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate-based practices within the Network Solutions PKI. Some of the services and/or the practices described in this CPS may be performed on Network Solutions' behalf by third-party vendors selected by Network Solutions. Consequently, references in this CPS to activities, practices, etc., of "Network Solutions" shall mean Network Solutions and/or its selected third-party vendors.

1.1) Network Solutions

Network Solutions 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 Network Solutions 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 Network Solutions PKI. Network Solutions extends, under agreement, membership of its PKI to approved third parties known as Registration Authorities. The international network of Network Solutions RA's share Network Solutions' policies and practices and CA infrastructure to issue Network Solutions Digital Certificates, or if appropriate, private labeled Digital Certificates.

1.2) Network Solutions CPS

The Network Solutions CPS is a public statement of the practices of Network Solutions and the conditions of issuance, revocation and renewal of a Certificate issued under Network Solutions' own hierarchy. Pursuant to the division of the tasks of a CA, this CPS is divided in the following sections: Technical, Organizational, Practices and Legal.

This CPS, related agreements and Certificate policies referenced within this document are maintained by the Network Solutions Certificate Policy Authority. The Certificate Policy Authority may be contacted at the below address:

Attention: Digital Certificates Support
Certificate Policy Authority
2325 Dulles Corner Blvd. Suite 700
Telephone: 703-668-4600
Email: sslcpa@networksolutions.com
This CPS, related agreements and Certificate policies referenced within this document are available online at http://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp.

Back to Top

1.2.1) Network Solutions CPS Suitability, Amendments and Publication

The Network Solutions 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 Network Solutions repository (available at http://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp), with seven days notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

Revisions not denoted "significant" shall be 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 Network Solutions CPS is not amended and published without the prior authorization of the Certificate Policy Authority.

1.3) Other Practice Statements & Agreements

The CPS is only one of a set of documents relevant to the provision of certification services by Network Solutions and that the list of documents contained in this clause are other documents which this CPS will from time to time mention, although this is not an exhaustive list. The document name, location of and status, whether public or private, are detailed below:

Document	Status	Location
Network Solutions Certification Practice Statement	Public	Network Solutions Repository:http://www.networksolutions.com/legal/SSL-legal-repository-cps.jsp
Relying Party Guarantee	Public	Network Solutions Repository:http://www.networksolutions.com/legal/SSL-legal-repository-rpg.jsp
Relying Party Agreement	Public	Network Solutions Repository:http://www.networksolutions.com/legal/SSL-legal-repository-rpa.jsp
Network Solutions Certificate and Site Seal Subscriber Agreement (including Schedules for each Certificate and Site Seal type)	Public	Network Solutions Repository:http://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp
Network Solutions Wholesale Agreement	Confidential	Presented to partners accordingly.
SRSPlus Agreement	Confidential	Presented to partners accordingly.

Back to Top

1.4) Liability of Network Solutions

For legal liability of Network Solutions under the provisions made in this CPS, please refer to section 5; legal conditions of issuance.

1.5) Compliance with applicable standards

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. An annual audit is or will be performed by an independent external auditor to assess Network Solutions' compliancy with the AICPA/CICA WebTrust program for Certification Authorities. Topics covered by the annual audit include but are not limited to the following:

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

Back to Top

1.6) Digital Certificate Policy Overview

A digital certificate is formatted data that cryptographically binds an identified subscriber with a public key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card. As detailed in this CPS, Network Solutions offers a range of distinct certificate types. The different certificate types have differing intended usages and differing policies.

Applicant	Certificate Type	Channels	Available Validation Levels1	Suggested Usage
Individual or Company	nsProtect™ Secure Xpress	- Network Solutions Website	Confirmation of right to use the domain name used in the application evidenced by an e-mail from someone who has control of the domain name.	Establishes SSL / TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session.
Individual or Company	Secure Server Certificate: nsProtect™ Secure Basic	- Network Solutions Website - Wholesale - SRSPlus	Confirmation of right to use the business name used in the application through the use of internal and third party databases and / or business documentation plus right to use the domain name used in the application. Validation is a four step process, requiring both automatic and manual validation including direct contact with the client.	Establishes SSL / TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session.
Individual or Company	Secure Server Certificate: nsProtect™ Secure Advanced SSL	- Network Solutions Website - Wholesale - SRSPlus	Confirmation of right to use the business name used in the application through the use of internal and third party databases and / or business documentation plus right to use the domain name used in the application. Validation is a four step process, requiring both automatic and manual validation including direct contact with the client.	Establishes SSL / TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session.
Individual or Company	Secure Server Certificate: Network Solutions nsProtect™ Secure Wildcard SSL	- Network Solutions Website - Wholesale - SRSPlus	Confirmation of right to use the business name used in the application through the use of internal and third party databases and / or business documentation plus right to use the domain name used in the application. Validation is a four step process, requiring both automatic and manual validation including direct contact with the client.	Establishes SSL / TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session.

As the suggested usage for a Digital Certificate differs on a per application basis, Subscribers are urged to appropriately study their requirements for their specific application before applying for a specific Network Solutions Certificate.

Back to Top

1.7) Network Solutions PKI Hierarchy

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. The following high-level representation of the Network Solutions PKI is used to illustrate the hierarchy utilized.

For DV (Domain Validated) Certificates (nsProtect™ Secure Xpress):

- AddTrust External CA Root (serial number = 01, expiry = 30 May 2020 10:48:38)
- Network Solutions DV Server CA (serial number = 48 fc 4b 0a 37 06 ff 46 fe d3 de 5d 4c 1e ca 62, expiry 30 May 2020 10:48:38)
- End Entity certificate (serial number = x, expiry = 1 month or up to 10 year(s) from

  issuance) For UTN/AddTrust Certificates:

  Visible on IE compatible browsers as follows:

- UTN-USERFirst-Hardware (serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2a fe 65 0a fd, expiry = 09 July 2019 19:19:22)
- Network Solutions Certificate Authority (serial number = 10 e7 76 e8 a6 5a 6e 37 7e 05 03 06 d4 3c 25 ea, expiry = 30 May 2020 11:48:38)
- End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

Cross signed and therefore visible on Netscape compatible browsers as follows:

- AddTrust External CA Root (serial number = 01, expiry = 30 May 2020 10:48:38)
- UTN-USERFirst-Hardware (serial number = 48 4b ac f1 aa c7 d7 13 43 d1 a2 74 35 49 97 25, expiry = 30 May 2020 11:48:38)
- Network Solutions Certificate Authority (serial number = 10 e7 76 e8 a6 5a 6e 37 7e 05 03 06 d4 3c 25 ea, expiry = 30 May 2020 11:48:38)
- End Entity SSL/End Entity Secure Email (serial number = x, expiry = 1 month or up to 10 year(s) from issuance)

1.8) Network Solutions Certification Authority

In its role as a Certification Authority (CA) Network Solutions provides certificate services within the Network Solutions PKI. The Network Solutions CA will:

- Conform its operations to the CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the Network Solutions repository (http://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp).
- Issue and publish certificates in a timely manner in accordance with the issuance times set out in this CPS.
- Upon receipt of a valid request to revoke the certificate from a person authorized to request revocation using the revocation methods detailed in this CPS, revoke a certificate issued for use within the Network Solutions PKI.
- Publish CRLs on a regular basis, in accordance with the applicable Certificate Policy and with provisions described in this CPS
- Distribute issued certificates in accordance with the methods detailed in this CPS
- Update CRLs in a timely manner as detailed in this CPS
- Notify subscribers via email of the imminent expiry of their Network Solutions issued certificate (for a period disclosed in this CPS)

Back to Top

1.9) Network Solutions Registration Authorities

Network Solutions, directly and/or through its third-party providers, has established the necessary secure infrastructure to fully manage the lifecycle of Digital Certificates within its PKI. Through a network of Registration Authorities (RA), Network Solutions also makes its certification authority services available to its subscribers. Network Solutions RAs:

- Accept, evaluate, approve or reject the registration of certificate applications.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of application as specified in the Network Solutions validation guidelines documentation.
- Use official, notarized or otherwise indicated document to evaluate a subscriber application.

- Verify the accuracy and authenticity of the information provided by the subscriber at the time of reissue or renewal as specified in the Network Solutions validation guidelines documentation.

  A Network Solutions RA acts locally within their own context of geographical or business partnerships on approval and authorization by Network Solutions in accordance with Network Solutions practices and procedures.

  RAs are restricted to operating within the set validation guidelines published by Network Solutions to the RA upon joining the programs. Certificates issued through an RA contain an amended Certificate Profile within an issued certificate to represent the involvement of the RA in the issuance process to the Relying Party.

Back to Top

1.10) Subscribers

Subscribers of Network Solutions services are individuals or companies that use PKI in relation to Network Solutions supported transactions and communications. Subscribers are parties that are identified in a certificate and hold the private key corresponding to the public key that is listed in a subscriber certificate. Prior to verification of identity and issuance of a certificate a subscriber is an applicant for the services of Network Solutions.

1.11) Relying Parties

Relying parties use PKI services in relation with Network Solutions 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 Network Solutions has not revoked the certificate. The CRL location is detailed within the certificate.

1.12) Issuance and Management of Publicly-Trusted Certificates

This Certificate Practice is committed to conform with the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.4.1 located at: https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.4.1.pdf

Back to Top

2. Technology

This section addresses certain technological aspects of the Network Solutions infrastructure and PKI services.

2.1) Network Solutions CA Infrastructure

The Network Solutions CA Infrastructure uses trustworthy systems to provide certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation and enforce a security policy.

2.1.1) Network Solutions Root CA Signing Key Protection & Recovery

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.

CA Number	Description	Usage	Lifetime	Size
61	AddTrust/UTN signed Network Solutions Certificate authority	Intermediate CA for SSL certificates	To 30 May 2020	2048
32	AddTrust signed UTN Hardware Certificate Authority	Intermediate CA for SSL certificates	To 30 May 2020	2048
38	AddTrust External CA Root	Root CA for SSL certificates	To 30 May 2020	2048
488	Network Solutions RSA DV Server CA	SHA-2 Intermediate CA for SSL certificates	To 14 Dec 2031	2048
489	Network Solutions RSA OV Server CA	SHA-2 Intermediate CA for SSL certificates	To 14 Dec 2031	2048
992	Network Solutions ECC DV Server CA	SHA-2 Intermediate CA for SSL certificates	To 14 Dec 2031	256
991	Network Solutions ECC OV Server CA	SHA-2 Intermediate CA for SSL certificates	To 14 Dec 2031	256

463	Network Solutions RSA Certificate Authority	SHA-2 Root CA for RSA certificates	To 18 Jan 2038	4096
998	Network Solutions ECC Certificate Authority	SHA-2 Root CA for ECDSA certificates	To 18 Jan 2038	384

Back to Top

For CA Root key recovery purposes, the Root CA signing keys are encrypted and stored within a secure environment. The decryption key is split across m removable media and requires n of m to reconstruct the decryption key. Custodians in the form of 2 or more authorized Network Solutions representatives are required to physically retrieve the removable media from the distributed physically secure locations.

Where CA Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

The UTN and AddTrust CA Root key pairs are protected in accordance with an AICPA/CICA WebTrust program compliant infrastructure and CPS. Details are available at the following website: www.comodogroup.com/repository/

2.1.2) Network Solutions CA Root Signing Key Generation Process

Network Solutions securely generates and protects its own private key(s), using a trustworthy system comprising a Hardware Signing Module (HSM) accredited to FIPS PUB 140-2 level 3 or higher, and takes necessary precautions to prevent the compromise or unauthorized usage of it. The Network Solutions CA Root key was generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference. The activities undergone and the Network Solutions personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

2.1.3) Network Solutions CA Root Signing Key Archival

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.

2.1.4) Procedures employed for CA Root Signing Key Changeover

Towards the end of the private key's lifetime, a new CA signing key pair is commissioned and all subsequently issued certificates and CRLs are signed with the new private signing key. Both keys may be concurrently active. The corresponding new CA public certificate is provided to subscribers and relying parties through the delivery methods detailed in section 2.1.5 of this CPS.

Back to Top

2.1.5) Network Solutions CA Root Public Key Delivery to Subscribers

Network Solutions makes all its CA Root Certificate available at its online repository at http://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp. The UTN USERFirst Hardware certificate is present in Explorer 5.01 and above and is made available to relying parties through this browser. The AddTrust External CA Root certificate is present in Netscape 4.77 and above and Opera 5.0 and above and is made available to relying parties through these browsers. Network Solutions provides the full certificate chain (see section 1.7 of this CPS) to the Subscriber upon issuance and delivery of the Subscriber certificate.

2.1.6) Physical CA Operations

Access to the secure part of Network Solutions (or its selected third-party vendors') facilities is limited through the use of physical access control and is only accessible to appropriately authorized individuals (referred to herein as Trusted Personnel). Card access systems are in place to control, monitor and log access to all areas of the facility. Access to the physical machinery within the secure facility is protected with locked cabinets and logical access control. Network Solutions has made reasonable efforts to ensure all secure facilities are protected from:

- Fire and smoke damage (fire protection is made in compliance with local fire regulations)
- Flood and water damage

All secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating / air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

Network Solutions asserts that it makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets and interruption to business activities.

Back to Top

2.2) Digital Certificate Management

Network Solutions certificate management refers to functions that include but are not limited to the following:

- Verification of the identity of an applicant of a certificate.
- Authorizing the issuance of certificates.
- Issuance of certificates.
- Revocation of certificates.
- De-commissioning of the corresponding private keys through a process involving the revocation of certificates.
- Listing of certificates.
- Distributing certificates.
- Publishing certificates.
- Storing certificates.
- Retrieving certificates in accordance with their particular intended use.

Network Solutions conducts the overall certification management within the Network Solutions PKI, either directly or through a Network Solutions approved RA. Network Solutions is not involved in functions associated with the generation, issuance, decommissioning or destruction of a Subscriber key pair.

2.3) Network Solutions Directories, Repository and Certificate Revocation List

Network Solutions manages and makes publicly available directories of revoked certificates through the use of Certificate Revocation Lists (CRLs). Users and relying parties are strongly urged to consult the directories of issued and revoked certificates at all times prior to relying on information featured on a certificate. Network Solutions updates and publishes a new CRL every 24 hours or more frequently under special circumstances.

Network Solutions also 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 Network Solutions legal repository may be accessed at http://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp.

Back to Top

2.4) Types of Network Solutions Certificates

Network Solutions currently offers a portfolio of Digital Certificates and related products that can be used in a way that addresses the needs of users for secure personal and business communications, protection of online transactions and identification of persons, whether legal or physical, or devices on a network or within a community.

Network Solutions may update or extend its list of products, including the types of certificates it issues, as it sees fit. The publication or updating of the list of Network Solutions products creates no claims by any third party. Upon the inclusion of a new certificate product in the Network Solutions hierarchy, an amended version of this CPS will be made public within two days, or as soon thereafter as is commercially practicable, on the official Network Solutions websites.

Issued certificates are published in Network Solutions directories. Suspended or revoked certificates are appropriately referenced in CRLs and published in Network Solutions directories. Network Solutions does not perform escrow of subscriber private keys.

2.4.1) Network Solutions Certificates

Network Solutions makes available Certificates that in combination with a Secure Socket Layer (SSL) web server attest the public server's identity providing full authentication and enable secure communication with corporate customers and corporate business partners. Network Solutions Certificates are offered in four variants: nsProtect™ Secure Xpress, nsProtect™ Secure Basic SSL, nsProtect™ Secure Advanced SSL, and nsProtect™ Secure Wildcard SSL. Pricing for the certificates are made available on the relevant official Network Solutions websites. All variants of the Secure Server Certificates are sold with a Secure Site Seal as specified in section 2.4.3.1 of this CPS.

a) nsProtect™ Secure Xpress

nsProtect™ Secure Xpress Certificates are low assurance level Secure Server Certificates from Network Solutions. These certificates are ideal for mail servers and server to server communications. They are not intended to be used for websites conducting e-commerce or transferring data of value.

In accordance with section 4.3 (Validation Practices) of this CPS, nsProtect™ Secure Xpress Certificates receive limited validation by Network Solutions. Network Solutions, at its discretion may establish domain control by utilizing third party domain name registrars and directories, by verifying control of the domain by practical and reasonable demonstration of the control of the domain, by implementing further validation processes including out of bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement.

Due to the increased validation speed, the lack of robust validation, and the nature of how Network Solutions intends nsProtect™ Secure Xpress Certificates to be used, the maximum aggregate guarantee limit for all claims associated with nsProtect™ Secure Xpress Certificates pursuant to the Relying Party Guarantee is $10,000, and $1,000 per incident. The terms of the Relying Party Guarantee can be found in Network Solutions' Repository.

nsProtect™ Secure Xpress Certificates are available from the following channel(s): Network Solutions' Website.

b) nsProtect™ Secure Basic SSL

nsProtect™ Secure Basic SSL Certificates are the professional level Secure Server Certificates from Network Solutions. Their intended usage is for websites conducting high value ecommerce and transferring data and also within internal networks.

In accordance with section 4.3 (Validation Practices) of this CPS, nsProtect™ Secure Basic SSL Certificates may also utilize private databases to assist as part of the certificate application. All nsProtect™ Secure Basic SSL Certificate applications include a validation of the applicant's submitted information.

The maximum aggregate guarantee limit for all claims associated with a nsProtect™ Secure Basic SSL Certificate pursuant to the Relying Party Guarantee is $50,000, and $1,000 per incident. The terms of the Relying Party Guarantee can be found in the Repository.

Subscriber fees for an nsProtect™ Secure Basic SSL Certificate are available from the official Network Solutions website.

c) nsProtect™ Secure Advanced SSL

nsProtect™ Secure Advanced SSL Certificates are the professional level Secure Server Certificates from Network Solutions. Their intended usage is for websites conducting high value ecommerce and transferring data and also within internal networks.

In accordance with section 4.3 (Validation Practices) of this CPS, nsProtect™ Secure Advanced SSL Certificates may also utilize private databases to assist as part of the certificate application. All nsProtect™ Secure Advanced SSL Certificate applications include a validation of the applicant's submitted information.

The maximum aggregate guarantee limit for all claims associated with a nsProtect™ Secure Advanced SSL Certificate is $1,000,000, and $1,000 per incident. The terms of the Relying Party Guarantee can be found in the Repository.

Subscriber fees for an nsProtect™ Secure Advanced SSL Certificate are available from the official Network Solutions website.

d) nsProtect™ Secure Wildcard SSL

nsProtect™ Secure Wildcard SSL Certificates are professional level Secure Server Certificates used securing multiple sub -domains with a single Network Solutions SSL #2 Certificate. Their intended use is for websites conducting high value ecommerce and transferring data and also within internal networks.

In accordance with section 4.3 (Validation Practices) of this CPS, nsProtect™ Secure Wildcard SSL Certificates may also utilize private databases to assist as part of the certificate application. All nsProtect™ Secure Wildcard SSL Certificate applications include a validation of the applicant's submitted information.

The maximum aggregate guarantee limit for all claims associated with a nsProtect™ Secure Wildcard SSL Certificate is $1,000,000, and $1,000 per person per incident. The terms of the Relying Party Guarantee can be found in the Repository.

Subscriber fees for an nsProtect™ Secure Wildcard SSL Certificate are available from the official Network Solutions website.

2.4.2) Reserved

Back to Top

2.4.3) Site Seal

"Network Solutions Site Seal" shall mean a hyperlinked graphic provided by Network Solutions to a Subscriber for display on the Subscriber's web site that identifies the Subscriber as the holder of a Network Solutions Digital Certificate and/or having been properly vetted as a valid entity as defined in this CPS. A Network Solutions Site Seal can be a Network Solutions Secure Site Seals or a Network Solutions Assured Site Seal.

2.4.3.1) Secure Site Seal

"Network Solutions Secure Site Seal" shall mean a hyperlinked graphic provided by Network Solutions to a Subscriber for display on the Subscriber's web site that identifies the subscriber as the holder of a Network Solutions SSL Certificate and that the Subscriber has been validated in accordance with the standards set forth in the Network Solutions CPS related to SSL Certificates. When the Secure Site Seal is selected by a user, the user's browser is directed to open a SSL-encrypted link to a Network Solutions site to verify that the Secure Site Seal holder has been issued a Network Solutions SSL Certificate and has been validated in accordance with the standards set forth in the Network Solutions CPS. The Network Solutions site sends to the user's browser over the SSL-encrypted link a message indicating the results of the verification along with other information. The response from the Network Solutions site can be displayed on the user's browser as a graphic or web page (that can include client-executable code) containing information about the organization or person to whom the Secure Site Seal pertains and the result of the requested verification. The Secure Site Seal accompanies any issued Network Solutions SSL Certificate and shares the guarantee level associated with the SSL Certificate it accompanies.

2.4.3.2) Assured Site Seal

"Network Solutions nsProtect™ Assured Site Seal" shall mean a hyperlinked graphic provided by Network Solutions to a Subscriber for display on the Subscriber's web site to indicate that the Subscriber has been validated in accordance with the standards set forth in the Network Solutions CPS related to Digital Certificates. When the Assured Site Seal is selected by a user, the user's browser is directed to open a SSL-encrypted link to a Network Solutions site to verify that the Network Solutions nsProtect™ Assured Site Seal holder has been validated in accordance with the standards set forth in the Network Solutions CPS. The Network Solutions site sends to the user's browser over the SSL-encrypted link a message indicating the results of the verification along with other information. The response from the Network Solutions site can be displayed on the user's browser as a graphic or web page (that can include client-executable code) containing information about the organization or person to whom the Assured Site Seal pertains and the result of the requested verification.

2.5) Reserved

Back to Top

2.6) Extensions and Naming

2.6.1) Digital Certificate Extensions

Network Solutions uses the standard X.509, version 3 to construct Digital Certificates for use within the Network Solutions PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. Network Solutions use a number of certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. X.509v3 is the standard of the International Telecommunications Union for digital certificates.

2.6.2) Incorporation by Reference for Extensions and Enhanced Naming

Enhanced naming is the usage of an extended organization field in an X.509v3 certificate. Information contained in the organizational unit field is also included in the Certificate Policy extension that Network Solutions may use.

2.7) Subscriber Private Key Generation Process

The Subscriber is solely responsible for the generation of the private key used in the certificate request. Network Solutions does not provide key generation, escrow, recovery or backup facilities as part of the Certificate services.

Upon making a certificate application the Subscriber is solely responsible for the generation of an RSA key pair appropriate to the certificate type being applied for. During application the Subscriber will be required to submit a public key and other personal / corporate details in the form of a Certificate Signing Request (CSR).

Typically, secure server Certificate requests are generated using the key generation facilities available in the Subscriber's webserver software.

2.8) Subscriber Private Key Protection and Backup

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.

Network Solutions strongly urges Subscribers to use a password or equivalent authentication method to prevent unauthorized access and usage of the Subscriber private key.

2.9) Subscriber Public Key Delivery to Network Solutions

Secure server Certificate requests are generated using the Subscriber's webserver software and the request is submitted to Network Solutions in the form of a PKCS #10 Certificate Signing Request (CSR). Submission is made electronically via the Network Solutions website or through a Network Solutions approved RA.

Back to Top

2.10) Delivery of Issued Subscriber Certificate to Subscriber

Delivery of Subscriber certificates to the associated Subscriber is dependent on the certificate product type:

2.10.1) Secure Server Certificate: nsProtect™ Secure Xpress, nsProtect™ Secure Basic SSL, nsProtect™ Secure Advanced SSL, nsProtect™ Secure Wildcard SSL

nsProtect™ Secure Xpress, nsProtect™ Secure Basic SSL, nsProtect™ Secure Advanced SSL, nsProtect™ Secure Wildcard SSL certificates are made available to the Subscriber upon successful completion of the application process via download through the Subscriber's account manager.

2.11) Delivery of Issued Subscriber Certificate to Wholesale Partners

Issued Subscriber secure server Certificates applied for through a Wholesale Partner on behalf of the Subscriber are emailed to the administrator contact of the Wholesale Partner account.

2.12) Network Solutions Certificates Profile

A Certificate Profile contains fields as specified below:

2.12.1) Key Usage extension field

Network Solutions certificates are general purpose and may be used without restriction on geographical area or industry. In order to use and rely on a Network Solutions certificate the relying party must use X.509v3 compliant software. Network Solutions certificates include key usage extension fields to specify the purposes for which the 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 Network Solutions.

The possible key purposes identified by the X.509v3 standard are the following:

a) Digital signature, for verifying digital signatures that have purposes other than those identified in b), f) or g), that is, for entity authentication and data origin authentication with integrity

b) Non-repudiation, for verifying digital signatures used in providing a non-repudiation service which protects against the signing entity falsely denying some action (excluding certificate or CRL signing, as in f) or g) below)

c) Key encipherment, for enciphering keys or other security information, e.g. for key transport

d) Data encipherment, for enciphering user data, but not keys or other security information as in c) above

e) Key agreement, for use as a public key agreement key

f) Key certificate signing, for verifying a CA's signature on certificates, used in CA certificates only

g) CRL signing, for verifying a CA's signature on CRLs

h) Encipher only, public key agreement key for use only in enciphering data when used with key agreement

i) Decipher only, public key agreement key for use only in deciphering data when used with key agreement

Back to Top

2.12.2) Extension Criticality Field

The Extension Criticality field denotes two separate uses for the Key Usage field. If the extension is noted as critical, then the key in the certificate is only to be applied to the stated uses. To use the key for another purpose in this case would break the issuer's policy. If the extension is not noted as critical, the Key Usage field is simply there as an aid to help applications find the proper key for a particular use.

2.12.3) Basic Constraints Extension

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or only as an end-entity certificate. Reliance on basic constraints extension field is dependent on correct software implementations of the X.509v3 standard and is outside of the control of Network Solutions.

2.12.4) Certificate Profile

Certificate Policy (CP) is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context. A policy identifier is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a certificate profile.

Specific Network Solutions certificate profiles are as per the tables below:

Network Solutions Secure Server Certificate – nsProtect™ Secure Xpress		
Signature Algorithm	Sha1	
Issuer	CN	Network Solutions DV Server CA
	O	Network Solutions L.L.C.
	C	US
Validity	1 Year / 2 Year / 3 Year	
Subject	CN	Domain Name
	OU	nsProtect™ Secure Xpress
Authority Key Identifier	KeyID= 58 d8 25 92 a4 55 5a 6e d9 a3 d1 a3 7c 0c aa 04 21 71 2e 60	

Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)
Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication(c0)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.782.1.2.1.9.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.networksolutions.com/legal/SSL-legal-repository-cps.jsp
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.netsolssl.com/NetworkSolutionsDVServerCA.crl
Thumbprint	*Generated Per Certificate*

Network Solutions Secure Server Certificate – nsProtect™ Secure Basic SSL, nsProtect™ Secure Advanced SSL, nsProtect™ Secure Wildcard SSL		
Signature Algorithm	Sha1	
Issuer	CN	Network Solutions Certificate Authority
	O	Network Solutions LLC
	C	US
Validity	1 Year / 2 Year / 3 Year	
Subject	CN	Domain Name
	OU	/*One of:*/ { nsProtect™ Secure Basic SSL | nsProtect™ Secure Advanced SSL | nsProtect™ Secure Wildcard SSL }
	O	Organization
	OU	Organization Unit
	STREET	Street Address
	L	Locality
	S	Street
	PostalCode	Zip / Postal Code
	C	Country
Authority Key Identifier	KeyID= 3c 41 e2 8f 08 08 a9 4c 25 89 8d 6d c5 38 d0 fc 85 8c 62 17	
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)	
Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication(c0)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.782.1.2.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.networksolutions.com/legal/SSL-legal-repository-rpa.jsp	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.netsolssl.com/NetworkSolutions_CA.crl	

Back to Top

2.13) Network Solutions Certificate Revocation List Profile

The profile of the Network Solutions Certificate Revocation List is as per the table below:

Version	[Version 2]	
Issuer Name	commonName=[Root Certificate Common Name] CN = Network Solutions Certificate Authority O = Network Solutions L.L.C. C = US	
Effective Date	[Date of Issuance]	
Next Update	[Date of Issuance + 24 hours]	
Revoked Certificates	CRL Entries	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

Back to Top

3. Organization

Network Solutions operates within the United States. All sites relevant to the provision of the services described herein operate under a security policy designed to, within reason, detect, deter and prevent unauthorized logical or physical access to CA related facilities. This section of the CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

3.1) Conformance to this CPS

Network Solutions conforms to this CPS and other obligations it undertakes through adjacent contracts when it provides its services.

3.2) Termination of CA Operations

In case of termination of CA operations for any reason whatsoever, Network Solutions will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, Network Solutions will where possible take the following steps:

- Providing subscribers of valid certificates with ninety (90) days notice of its intention to cease acting as a CA. Revoking all certificates that are still unrevoked or unexpired at the end of the ninety (90) day notice period without seeking subscriber's consent.
- Giving timely notice of revocation to each affected subscriber.
- Making reasonable arrangements to preserve its records according to this CPS.
- Reserving its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as Network Solutions'.
- The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

Back to Top

3.3) Form of Records

Network Solutions retains records in electronic or in paper-based format for a period detailed in section 3.4 of this CPS. Network Solutions may require subscribers to submit appropriate documentation in support of a certificate application.

Network Solutions Registration Authorities are required to submit appropriate documentation as detailed in the RA agreements, prior to being validated and successfully accepted as an approved Network Solutions Registration Authority.

In their role as a Network Solutions Registration Authority, RAs may require documentation from subscribers to support certificate applications. In such circumstances, RAs are obliged to retain such records in line with the practices of record retention and protection as used by Network Solutions and as stated in this CPS.

3.4) Records Retention Period

Network Solutions retains the records of Network Solutions Digital Certificates and the associated documentation for a term of no less than 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 Network Solutions may see fit.

Such records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction.

Back to Top

3.5) Logs for Core Functions

For audit purposes Network Solutions maintains electronic or manual logs of the following events for core functions. All logs are backed up on removable media and the media held at a secure off-site location on a daily basis. These media are only removed by Network Solutions staff or other authorized personnel on a visit to the data center, and when not in the data center are held either in a safe in a locked office within the development site, or offsite in a secure storage facility.

An audit log is maintained of each movement of the removable media. Logs are archived by the system administrator on a weekly basis and event journals reviewed on a weekly basis by CA management. Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction. When the removable media reaches the end of its life it is wiped by a third party secure data destruction facility and the certificates of destruction are archived.

All logs include the following elements:

- Date and time of entry
- Serial or sequence number of entry
- Method of entry
- Source of entry
- Identity of entity making log entry

3.5.1) CA & Certificate Lifecycle Management

CA Root signing key functions, including key generation, backup, recovery and destruction

- Subscriber certificate life cycle management, including successful and unsuccessful certificate applications, certificate issuances, certificate re-issuances, certificate renewals
- Subscriber certificate revocation requests, including revocation reason
- Subscriber changes of affiliation that would invalidate the validity of an existing certificate
- Certificate Revocation List updates, generations and issuances
- Custody of keys and of devices and media holding keys
- Compromise of a private key

3.5.2) Security Related Events

System downtime, software crashes and hardware failures

- CA system actions performed by Network Solutions or other authorized personnel, including software updates, hardware replacements and upgrades
- Cryptographic hardware security module events, such as usage, de-installation, service or repair and retirement Successful and unsuccessful Network Solutions PKI access attempts
- Secure CA facility visitor entry and exit

Back to Top

3.5.3) Certificate Application Information

The documentation and other related information presented by the applicant as part of the application validation process

Storage locations, whether physical or electronic of presented documents

3.5.4) Log Retention Period

Network Solutions maintain logs for a period of 7 years, or as necessary to comply with applicable laws.

Back to Top

3.6) Business Continuity Plans and Disaster Recovery

To maintain the integrity of its services Network Solutions implements, documents and periodically tests appropriate contingency and disaster recovery plans and procedures. Such plans are revised and updated as may be required at least once a year.

- Network Solutions operates a fully redundant CA system. The backup CA is readily available in the event that the primary CA should cease operation. All of our critical computer equipment is housed in a co -location facility run by a commercial data -center, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. The duplicate equipment is ready to take over the role of providing the implementation of the CA, and allows us to specify a maximum system outage time (in case of critical systems failure) within 1 hour.
- Backup of critical CA software is performed weekly and is stored offsite.
- Backup of critical business information is performed daily and is stored offsite.
- Network Solutions operations (directly and through its selected third-party vendors) are distributed across several sites worldwide. All sites offer facilities to manage the lifecycle of a certificate, including but not limited to the application, issuance, revocation and renewal of such certificates.

  As well as a fully redundant CA system, Network Solutions maintains provisions for the activation of a backup CA and a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that Network Solutions (and/or its selected third-party vendor(s)) will endeavor to minimize interruptions to its CA operations.

3.7) Availability of Revocation

Network Solutions publishes Certificate Revocation Lists (CRLs) to allow relying parties to verify a digital signature made using a Network Solutions issued SSL Certificate. Each CRL contains entries for all revoked unexpired certificates issued and is valid for 24 hours. Network Solutions issues a new CRL every 24 hours and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances Network Solutions may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in section 3.4 of this CPS) for a period of 7 years, or longer if applicable. Network Solutions does not support OCSP (Online Certificate Status Protocol).

Back to Top

3.8) Publication of Critical Information

Network Solutions publishes any revocation data on issued Digital Certificates, this CPS, certificate terms and conditions, the relying party agreement and copies of all subscriber agreements in the official Network Solutions repository at http://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp. The Network Solutions repository

is maintained by the Network Solutions Certificate Policy Authority and all updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in this CPS.

3.9) Confidential Information

Network Solutions observes applicable rules on the protection of personal data deemed by law or the Network Solutions privacy policy (see section 3.11 of this CPS) to be confidential.

3.9.1) Types of Information deemed as Confidential

Network Solutions keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- Subscriber agreements.
- Certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
- Transaction records and financial audit records.
- External or internal audit trail records and reports, except for WebTrust audit reports which may be published at the discretion of Network Solutions.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of Network Solutions infrastructure, certificate management and enrolment services and data.

3.9.2) Types of Information not deemed as Confidential

Subscribers acknowledge that revocation data of all certificates issued by the Network Solutions CA is public information is periodically published every 24 hours at the Network Solutions repository. Subscriber application data marked as "Public" in the relevant subscriber agreement and submitted as part of a certificate application is published within an issued Digital Certificate in accordance with section 2.12.4 of this CPS.

3.9.3) Access to Confidential Information

All personnel in trusted positions handle all information in strict confidence. Personnel of RA/LRAs especially must comply with the requirements of the U.S. and/or English law on the protection of personal data.

3.9.4) Release of Confidential Information

Network Solutions is not required to release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- The party to whom Network Solutions owes a duty to keep information confidential.
- The party requesting such information.
- A court order, if any.

Back to Top

3.10) Personnel Management and Practices

Consistent with this CPS Network Solutions 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. Trusted roles

Trusted roles relate to access to the Network Solutions account management system, with functional permissions applied on an individual basis.

Trusted personnel must identify and authenticate themselves to the system before access is granted. Identification is via a username, with authentication requiring both a password and SSL Certificate.

Personnel controls

All trusted personnel of Network Solutions or its selected third-party vendors, as applicable, have background checks before access is granted to Network Solutions' systems. These checks include, but are not limited to, credit history, employment history for references and a Companies House cross -reference to disqualified directors. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.

3.11) Privacy Policy

Network Solutions has implemented a privacy policy, which is in compliance with this CPS. The Network Solutions privacy policy is published at the Network Solutions LLC website at http://customersupport.networksolutions.com/article.php?id=306.

3.12) Publication of Information

The Network Solutions certificate services and the Network Solutions repository are accessible through several means of communication:

- On the web: www.networksolutions.com
- By email from sslcpa@networksolutions.com
- And by mail from:
  Network Solutions, LLC
  Attention: Digital Certificates Support,
  2325 Dulles Corner Blvd. Suite 700
  Herndon, VA 20171, USA.
  Tel: 703-668-4600

Back to Top

4. Practices and Procedures

This section describes the certificate application process, including the information required to make and support a successful application.

4.1) Certificate Application Requirements

Other than applicants for nsProtect™ Secure Xpress, Certificate applicants must complete the enrollment process which includes:

- Generate a RSA key pair and demonstrate to Network Solutions ownership of the private key half of the key pair through the submission of a valid PKCS#10 Certificate Signing Request (CSR)
- Make all reasonable efforts to protect the integrity the private key half of the key pair
- Submit to Network Solutions a certificate application, including application information as detailed in this CPS, a public key half of a key pair, and agree to the terms of the relevant subscriber agreement
- Provide proof of identity through the submission of official documentation as requested by Network Solutions during the enrolment process Certificate applications are submitted to either Network Solutions or a Network Solutions approved Registration Authority (RA). The following table details the entity(s) involved in the processing of certificate applications. Network Solutions issues all certificates regardless of the processing entity.

Certificate Type	**Enrollment Entity**	**Processing Entity**	**Issuing Authority**
Secure Server Certificate - *all types as per section 2.4.1 and 2.4.2 of this CPS.*	End Entity Subscriber	Network Solutions	**Network Solutions**
Secure Server Certificate - *all types as per section 2.4.1 and 2.4.2 of this CPS.*	**SRSPlus or Wholesale Partner on behalf of End Entity Subscriber**	**SRSPlus or Wholesale Partner**	**Network Solutions**

Back to Top

4.1.1) Methods of application

Generally, applicants will complete the online forms made available by Network Solutions or by approved RAs at the respective official websites. Under special circumstances the applicant may submit an application via e-mail, however this process is available at the discretion of Network Solutions or its RAs.

4.2) Application Validation

Prior to issuing a Certificate (which includes a Network Solutions Secure Site Seal) or issuing a Network Solutions nsProtect™ Assured Site Seal, Network Solutions employs controls to validate the identity of the subscriber information featured in the certificate application. Such controls are indicative of the product type:

4.2.1) Secure Server Certificate Application Validation Process

Network Solutions utilizes an organizational entity validation process prior to the issuance of a secure server Certificate.

This process involves Network Solutions, automatically and manually, reviewing the application information provided by the applicant (as per section 4.3 of this CPS) in order to check the following:

1. If the applicant is a consumer, verifying the applicant is listed as the registrant for the domain name used in the application and is an accountable legal entity.

For each domain name to be included in the SSL certificate Subject, Network Solutions verifies the Applicants control of the domain name in accordance with the CA/B Forum *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 1.4.1, section 3.2.2.4,* as follows;

1. Communicating directly with the Domain Name Registrant using a postal address, email address, or telephone number provided by the Domain Name Registrar;
    i. Email, Fax, SMS, or Postal Mail to Domain Contact
    (as defined in section 3.2.2.4.2 of v1.4.1 of the Baseline Requirements)
    Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail to a recipient identified as a Domain Contact and then receiving a confirming response utilizing the Random Value.
    The Random Value is generated by Network Solutions and remains valid for use in a confirming response for no more than 30 days from its generation;
    ii. Phone Contact with Domain Contact
    (as defined in section 3.2.2.4.3 of v1.4.1 of the Baseline Requirements)
    Confirming the Applicant's control over the requested FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN;
2. Communicating directly with the Domain Contact confirming the Applicant's control over the requested FQDN using a constructed email address (as defined in section 3.2.2.4.4 of v1.4.1 of the Baseline Requirements) by:
    (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name,
    (ii) including a Random Value in the email, and
    (iii) having the applicant submit (by clicking or otherwise) the Random Value to Network Solution’s servers to confirm receipt and authorization.
    The Random Value is generated by Network Solutions and remains valid for use in a confirming response for no more than 30 days from its generation;
3. Confirming the Applicant's control over the requested FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document (as defined in section 3.2.2.4.5 of v1.4.1 of the Baseline Requirements).
    The Domain Authorization Document must substantiate that the communication came from the Domain Contact. We will verify that either:
    (i) the Domain Authorization Document is dated on or after the date of the domain validation request or
    (ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space;
4. Confirming the Applicant's control over the requested FQDN by having them make an agreed-upon change to the website (as defined in section 3.2.2.4.6 of v1.4.1 of the Baseline Requirements).
    Confirming that the Request Token or Random Value appear in the content of a file or on a webpage in the form of a meta tag, the file or webpage being accessed via the URL HTTP[S]://<Authorization Domain>/.well-known/pki-validation/FileName over port 80 (HTTP) or 443 (HTTPS).
    The Random Value is generated by Network Solutions and remains valid for use for no more than 30 days from its generation;
5. Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME or CAA record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character (as defined in section 3.2.2.4.7 of v1.4.1 of the Baseline Requirements).

The Random Value is generated by Network Solutions and remains valid for no more than 30 days from its generation;

Confirming the Applicant's control over the requested FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN (as defined in section 3.2.2.4.8 of the Baseline Requirements).

- Validation is supplemented by directly contacting the applicant to submit by fax additional forms of verification of identity such as utility bills and photo IDs and checking those bills and IDs against the application.

  If the applicant submits incorrect information, then services may be denied, or the applicant will be contacted regarding the incorrect information. If the application is rejected, the customer specified will be contacted.

Back to Top

2. If the applicant is an organization, verifying the applicant is listed as the registrant for the domain name used in the application and the contact listed represents an accountable legal entity.

- Validated by reviewing domain name registration records available publicly through WHOIS queries and private registration records if available. Then if incorporated, checking company's articles of incorporation online if available or requesting them to be faxed.
- Validation is supplemented through additional identity verification. If company is listed in Dunn & Bradstreet database, comparing Dunn & Bradstreet entry with application. If the company is not listed in Dunn & Bradstreet, directly contacting applicant to submit additional forms of verification, namely a utility bill.

  If the applicant submits incorrect information, then the applicant will be contacted regarding the incorrect information. If the application is rejected, the customer specified will be contacted.

4.2.2) nsProtect™ Secure Xpress, nsProtect™ Secure Basic SSL, nsProtect™ Secure Advanced SSL, nsProtect™ Secure Wildcard SSL

Certificates are processed by Network Solutions in accordance with the validation process outlined in section 4.2.1 of this CPS.

Network Solutions may employ the data held in private databases to increase the integrity of the validation process. In any case, the application is processed manually by Network Solutions in accordance with the validation process outlined in section 4.2.1 of this CPS.

4.2.3) Time to Process Certificate Applications

Network Solutions makes reasonable efforts to confirm Certificate application information and issue a digital Certificate within a reasonable time frame. The time frame is greatly dependent on the Subscriber providing the necessary details and / or documentation in a timely manner.

Upon the receipt of the necessary details and / or documentation, Network Solutions aims to confirm submitted application data and to complete the validation process and issue / reject a Certificate application within 2 working days.

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.

4.2.4) Certificate Authority Authorization

Where an application is for a Certificate which includes a domain-name and is to be used for server authentication, Network Solutions examines the Certification Authority Authorization (CAA) DNS Resource Records as specified in RFC 6844 as amended by Errata 5065 (Appendix A) and, if such CAA Records are present and do not grant Network Solutions the authority to issue the Certificate, the application is rejected. Where the ‘issue’ and ‘issuewild’ tags are present within a CAA record, Network Solutions recognizes the following domain names within those tags as granting authorization for issuance by Network Solutions:

NetworkSolutions.com
Web.com.

Back to Top

4.3) Validation Information for Certificate Applications

Applications for Network Solutions Certificates are supported by appropriate documentation to establish the identity of an applicant. From time to time, Network Solutions may modify the requirements related to application

information for individuals to respond to Network Solutions' requirements, the business context of the usage of a SSL Certificate, or as it may be prescribed by law.

4.3.1) Application Information for Organizational Applicants

The following elements are critical information elements for a Network Solutions certificate issued to an Organization. Those elements marked with PUBLIC are present within an issued certificate and are therefore within the public domain. Those elements not marked with PUBLIC remain confidential in line with the privacy and protection of data provisions outlined in this CPS.

- Legal Name of the Organization (PUBLIC)
- Organizational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- Company / DUNS number (if available)
- 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

Back to Top

4.3.2) Supporting Documentation for Organizational Applicants

Documentation requirements for Organizational applicants include any / all of the following:

- Articles of Association / Incorporation
- Business License
- Certificate of Compliance
- Certificate of Incorporation
- Certificate of Authority to Transact Business
- Tax Certification
- Corporate Charter
- Official letter from an authorized representative of a government organization
- Official letter from office of Dean or Principal (for Educational Institutions)
- Primary Utility Bills
- Banking Statement

Network Solutions may accept at its discretion other official organizational documentation supporting an application.

4.3.3) Application Information for Individual Applicants

The following elements are critical information elements for a Network Solutions certificate issued to an individual:

- 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

Back to Top

4.3.4) Supporting Documentation for Individual Applicants

Documentation requirements for Individual applicants shall include identification elements such as:

- Passport
- Driving License
- Bank statement
- Primary Utility Bills

Network Solutions may accept at its discretion other official documentation supporting an application.

4.4) Validation Requirements for Certificate Applications

Upon receipt of an application for a Digital Certificate and based on the submitted information, Network Solutions confirms the following information:

- The certificate applicant is the same person as the person identified in the certificate request.
- The certificate applicant holds the private key corresponding to the public key to be included in the certificate.
- The information to be published in the certificate is accurate, except for non-verified subscriber information.
- Any agents who apply for a certificate listing the certificate applicant's public key are duly authorized to do so.

In all types of Network Solutions Certificates the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Network Solutions of any changes that would affect the validity of the Certificate. Failure to comply with the obligations as set out in the subscriber agreement will result in the revocation of the Subscriber's Digital Certificate without further notice to the Subscriber and the Subscriber shall pay any charges payable but not yet paid under the Agreement.

4.4.1) Third-Party Confirmation of Business Entity Information

Network Solutions may use the services of a third party to confirm information on a business entity that applies for a SSL Certificate. Network Solutions accepts confirmation from third party organizations, other third party databases and government entities.

Network Solutions controls include Trade Registry transcripts that confirm the registration of the applicant company and state the members of the board, the management and Directors representing the company.

Network Solutions may use any means of communication at its disposal to ascertain the identity of an organizational or individual applicant. Network Solutions reserves right of refusal in its absolute discretion.

4.4.2) Serial Number Assignment

Network Solutions assigns certificate serial numbers that appear in Network Solutions certificates. Assigned serial numbers are unique.

Back to Top

4.5) Time to Confirm Submitted Data

Network Solutions makes reasonable efforts to confirm certificate application information and issue a SSL Certificate within reasonable time frames.

Network Solutions assures that all certificates will be issued within 2 working days after the receipt of all required validation information as per this CPS.

4.6) Approval and Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application Network Solutions approves an application for a SSL Certificate.

If the validation of a certificate application fails, Network Solutions rejects the certificate application. Network Solutions reserves its right to reject applications to issue a certificate to applicants if, on its own assessment, by issuing a certificate to such parties the good and trusted name of Network Solutions might get tarnished, diminished or have its value reduced and under such circumstances 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.

4.7) Certificate Issuance and Subscriber Consent

Network Solutions issues a Certificate upon approval of a certificate application. A SSL Certificate is deemed to be valid at the moment a subscriber accepts it (refer to section 4.9 of this CPS). Issuing a Digital Certificate means that Network Solutions accepts a certificate application.

4.8) Certificate Validity

Certificates are valid upon issuance by Network Solutions. Network Solutions verifies all information that is included in SSL Certificates at time intervals of thirty-nine months or less. Network Solutions reserves the right, however, to offer validity periods outside of this standard validity period.

4.9) Certificate Acceptance by Subscribers

A subscriber is deemed to have accepted a certificate when the certificate is either delivered to the Subscriber via email or installed on a subscriber's computer / hardware security module through an online collection method.

Back to Top

4.10) Verification of Digital Signatures

Verification of a digital signature is used to determine that:

- The digital signature was created by the private key corresponding to the public key listed in the signer's certificate.
- The signed data associated with this digital signature has not been altered since the digital signature was created.

4.11) Reliance on Digital Signatures

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party. Reliance on a digital signature should only occur if:

- The digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate.
- The relying party has checked the revocation status of the certificate by referring to the relevant Certificate Revocation Lists and the certificate has not been revoked.
- The relying party understands that a SSL Certificate is issued to a subscriber for a specific purpose and that the private key associated with the SSL Certificate may only be used in accordance with the usages suggested in the CPS and named as Object Identifiers in the certificate profile.

Reliance is accepted as reasonable under the provisions made for the relying party under this CPS and within the relying party agreement. If the circumstances of reliance exceed the assurances delivered by Network Solutions under the provisions made in this CPS, the relying party must obtain additional assurances.

4.12) Certificate Suspension

Network Solutions does not utilize certificate suspension.

4.13) Certificate 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. Network Solutions will revoke a Digital Certificate if:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key associated with the certificate.
- The Subscriber or Network Solutions has breached a material obligation under this CPS or the Certificate and Site Seal Subscriber Agreement.
- Either the Subscriber's or Network Solutions' obligations under this CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised.
- There has been a modification of the information pertaining to the Subscriber that is contained within the certificate.

Back to Top

4.13.1) Request for Revocation

The subscriber or other appropriately authorized parties such as RAs can request revocation of a certificate. Prior to the revocation of a certificate Network Solutions will verify that the revocation request has been:

- Made by the organization or individual entity that has made the certificate application.
- Made by the RA on behalf of the organization or individual entity that used the RA to make the certificate application

Network Solutions employs the following procedure for authenticating a revocation request:

- The revocation request must be received by the administrator contact associated with the certificate application. Network Solutions may if necessary also request that the revocation request be made by either / or the organizational contact and billing contact.
- Upon receipt of the revocation request Network Solutions will request confirmation from the known administrator contact details, either by telephone or fax.
- Validation personnel will then command the revocation of the certificate and logging of the identity of validation personnel and reason for revocation will be maintained in accordance with the logging procedures covered in this CPS.

Back to Top

4.13.2) Effect of Revocation

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate will be placed within the Certificate Revocation List (CRL) and remains on the CRL until some time after the end of the certificate's validity period. An updated CRL is published on the Network Solutions website every 24 hours, however under special circumstances the CRL may be published more frequently.

4.14) Renewal

Depending on the option selected during application, and the actual certificate issuance date, and subject to Section 4.8 above, the validity period of Network Solutions certificates is generally one year, two years, three years or four years from the date of issuance and is detailed in the relevant field within the certificate. Renewal fees are detailed on the official Network Solutions website and within communications sent to subscribers approaching the certificate expiration date.

Renewal application requirements and procedures are the same as those employed for the application validation and issuance requirements detailed for new customers unless the subscriber had provided offline supporting documentation during the initial validation process. In such instances, the renewal process will include Network Solutions sending the subscriber a copy of all supporting documentation including the initial offline supporting documentation that the subscriber provided in order to secure a certificate. A subscriber must review and confirm in writing to Network Solutions that such documentation is still valid and no changes have been made to the documentation.

4.15) Notice Prior to Expiration

Network Solutions shall make reasonable efforts to notify subscribers via e -mail, of the imminent expiration of a SSL Certificate. Notice shall ordinarily be provided within a 60 day period prior to the expiry of the certificate.

Back to Top

5. Legal Conditions of Issuance

This part describes the legal representations, warranties and limitations associated with Network Solutions SSL Certificates. This CPS also incorporates the Network Solutions Relying Party Guarantee available at http://www.networksolutions.com/legal/SSL-legal-repository-rpg.jsp.

5.1) Network Solutions Representations

Network Solutions makes to all subscribers and relying parties certain representations regarding its public service, as described below. Network Solutions reserves its right to modify such representations as it sees fit or required by law.

5.2) Information Incorporated by Reference into a SSL Certificate.

Network Solutions incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the digital certificate.
- Any other applicable certificate policy as may be stated on an issued Network Solutions certificate, including the location of this CPS.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customized elements of the standard X.509v3.
- Content of extensions and enhanced naming that are not fully expressed within a certificate.
- Any other information that is indicated to be so in a field of a certificate.

Back to Top

5.3) Displaying Liability Limitations, and Warranty Disclaimers

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. To communicate information Network Solutions may use:

- An organizational unit attribute.
- A Network Solutions standard resource qualifier to a certificate policy.
- Proprietary or other vendors' registered extensions.

5.4) Publication of Certificate Revocation Data

Network Solutions reserves its right to publish a CRL (Certificate Revocation List) as may be indicated.

5.5) Duty to Monitor the Accuracy of Submitted Information

In all cases and for all types of Network Solutions certificates the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Network Solutions of any such changes.

5.6) Publication of Information

Published critical information may be updated from time to time as prescribed in this CPS. Such updates shall be indicated through appropriate version numbering and publication date on any new version.

Back to Top

5.7) Interference with Network Solutions Implementation

Subscribers, relying parties and any other parties shall not interfere with, or reverse engineer the technical implementation of Network Solutions PKI services including the key generation process, the public web site and the Network Solutions repositories except as explicitly permitted by this CPS or upon prior written approval of Network Solutions. Failure to comply with this as a subscriber will result in the revocation of the Subscriber's SSL Certificate without further notice to the Subscriber and the Subscriber shall pay any charges payable but not yet paid under the SSL Certificate and Site Seal Subscriber Agreement. Failure to comply with this as a relying party will result in the termination of the agreement with the relying party, the removal of permission to use or access the Network Solutions repository and any SSL Certificate or service provided by Network Solutions.

5.8) Standards

Network Solutions assumes that user software that is claimed to be compliant with X.509v3 and other applicable standards enforces the requirements set out in this CPS. Network Solutions cannot warrant that such user software will support and enforce controls required by Network Solutions, and the user should seek appropriate advice.

5.9) Network Solutions Partnerships Limitations

Partners of the Network Solutions network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the Network Solutions products and services. Network Solutions partners shall specifically refrain from seeking partnerships with other root authorities or apply procedures originating from such authorities. Failure to comply with this will result in the termination of the agreement with the relying party, the removal of permission to use or access the Network Solutions repository and any SSL Certificate or service provided by Network Solutions.

5.10) Network Solutions Limitation of Liability for a Network Solutions Partner

As the Network Solutions network may include RAs that operate under Network Solutions practices and procedures, Network Solutions guarantees to all Relying Parties, pursuant and subject to the terms of the Relying Party Guarantee, the integrity of any certificate issued under its own root.

Back to Top

5.11) Choice of Cryptographic Methods

Parties are solely responsible for and have exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

5.12) Reliance on Unverified Digital Signatures

Parties relying on a SSL Certificate must verify a digital signature at all times by checking the validity of a SSL Certificate against the relevant CRL published by Network Solutions. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the subscriber.

Relying on an unverifiable digital signature may result to risks that the relying party, and not Network Solutions, assume in whole.

By means of this CPS, Network Solutions has adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository available at http://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp or by contacting via the contact address as specified in the Document Control section of this CPS.

Back to Top

5.13) Rejected SSL Certificate Applications

The private key associated with a public key which has been submitted as part of a rejected SSL Certificate application may not under any circumstances be used to create a digital signature if the effect of the signature is to create conditions of reliance upon the rejected certificate. The private key may also not be resubmitted as part of any other certificate application

5.14) Refusal to Issue an SSL Certificate

Network Solutions reserves its right to refuse to issue a SSL Certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Network Solutions reserves the right not to disclose reasons for such a refusal.

5.15) Subscriber Obligations

Unless otherwise stated in this CPS, subscribers shall exclusively be responsible:

- To minimize internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- To generate their own private / public key pair to be used in association with the certificate request submitted to Network Solutions or a Network Solutions RA.
- Ensure that the public key submitted to Network Solutions or a Network Solutions RA corresponds with the private key used.
- Ensure that the public key submitted to Network Solutions or a Network Solutions RA is the correct one.
- Provide correct and accurate information in its communications with Network Solutions or a Network Solutions RA.
- Alert Network Solutions or a Network Solutions RA if at any stage whilst the certificate is valid, any information originallysubmitted has changed since it had been submitted to Network Solutions.
- Generate a new, secure key pair to be used in association with a certificate that it requests from Network Solutions or a Network Solutions RA.
- Read, understand and agree with all terms and conditions in this Network Solutions CPS and associated policies published in the Network Solutions Repository athttp://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp.
- Refrain from tampering with a Network Solutions certificate.
- Use Network Solutions SSL Certificates for legal and authorized purposes in accordance with this suggested usages and practices CPS.
- Cease using a Network Solutions SSL Certificate if any information in it becomes misleading obsolete or invalid.

- Cease using a Network Solutions certificate if such certificate is expired and remove it from any applications and/or devices it has been installed on.
- Refrain 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.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in a Network Solutions certificate.
- Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a Network Solutions certificate.
- For acts and omissions of partners and agents they use to generate, retain, escrow, or destroy their private keys.

Back to Top

5.16) Representations by Subscriber upon Acceptance

Upon submitting an application for a certificate the subscriber represents to Network Solutions and to relying parties that at such time and until further notice:

- Digital signatures created using the private key corresponding to the public key included in the certificate is the digital signature of the subscriber and the certificate has been accepted and is properly operational at the time the digital signature is created.
- No unauthorized person has ever had access to the subscriber's private key.
- All representations made by the subscriber to Network Solutions regarding the information contained in the certificate are accurate and true.
- All information contained in the certificate is accurate and true to the best of the subscriber's knowledge or to the extent that the subscriber had notice of such information whilst the subscriber shall act promptly to notify Network Solutions of any material inaccuracies in such information.
- The certificate is used exclusively for authorized and legal purposes, consistent with this CPS.
- It will use a Network Solutions certificate only in conjunction with the entity named in the organization field of a SSL Certificate (if applicable).
- The subscriber retains control of her private key, use a trustworthy system, and take reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The subscriber is an end-user subscriber and not a CA, and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as a CA or otherwise, unless expressly agreed in writing between subscriber and Network Solutions.
- The subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of Network Solutions.
- The subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems, etc.
- The subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

Back to Top

5.17) Indemnity by Subscriber

By accepting a certificate, the subscriber agrees to indemnify and hold Network Solutions, as well as its agent(s) 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 Network Solutions, and the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from:

- Any false or misrepresented data supplied by the subscriber or agent(s).
- Any failure of the subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, Network Solutions, or any person receiving or relying on the certificate.
- Failure to protect the subscriber's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

5.18) Obligations of Network Solutions Registration Authorities

A Network Solutions RA operates under the policies and practices detailed in this CPS. The RA is bound under contract to:

- Receive applications for Network Solutions certificates in accordance with this CPS.
- Perform all verification actions prescribed by the Network Solutions validation procedures and this CPS.
- Receive, verify and relay to Network Solutions all requests for revocation of a Network Solutions certificate in accordance with the Network Solutions revocation procedures and the CPS.
- Act according to relevant Law and regulations.

Back to Top

5.19) Obligations of a Relying Party

A party relying on a Network Solutions certificate accepts that in order to reasonably rely on a Network Solutions certificate they must:

- Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate, the relying party must have reasonably made the effort to acquire sufficient knowledge on using SSL Certificates and PKI.
- Study the limitations to the usage of SSL Certificates and be aware through the Relying Party Agreement the maximum value of the transactions that can be made using a Network Solutions Digital Certificate.
- Read and agree with the terms of the Network Solutions CPS and Relying Party Agreement.
- Verify a Network Solutions certificate by referring to the relevant CRL and also the CRLs of intermediate CA and root CA as available in the Network Solutions repository.
- Trust a Network Solutions certificate only if it is valid and has not been revoked or has expired.
- Rely on a Network Solutions certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

5.20) Legality of Information

Subscribers shall solely be responsible for the legality of the information they present for use in certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed.

5.21) Subscriber Liability to Relying Parties

Without limiting other subscriber obligations stated in this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the certificate.

5.22) Duty to Monitor Agents

The subscriber shall control and be responsible for the data that an agent supplies to Network Solutions. The subscriber must promptly notify the issuer of any misrepresentations and omissions made by an agent. The duty of this article is continuous.

Back to Top

5.23) Use of Agents

For certificates issued at the request of a subscriber's agent, both the agent and the subscriber shall be bound by the Certificate and Site Seal Subscriber Agreement and shall jointly and severally indemnify Network Solutions, and its agents and contractors.

5.24) Conditions of usage of the Network Solutions Repository and web site

Parties (including subscribers and relying parties) accessing the Network Solutions Repository (http://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp) and official web site(s) agree with the provisions of this CPS and any other conditions of usage that Network Solutions may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by using a Network Solutions issued certificate.

Failure to comply with the conditions of usage of the Network Solutions Repositories and web site may result in terminating the relationship between Network Solutions and the party.

5.25) Accuracy of Information

Network Solutions recognizing its trusted position makes all reasonable efforts to ensure that parties accessing its Repositories receive accurate, updated and correct information. Network Solutions, however, cannot accept any liability beyond the limits set in this CPS and the Network Solutions insurance policy.

Failure to comply with the conditions of usage of the Network Solutions Repositories and web site may result in terminating the relationship between Network Solutions and the party.

Back to Top

5.26) Obligations of Network Solutions

To the extent specified in the relevant sections of the CPS, Network Solutions promises to:

- Comply with this CPS and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide (directly or through its selected third-party vendors) infrastructure and certification services, including but not limited to the establishment and operation of the Network Solutions Repository and web site for the operation of PKI services.
- Provide trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its private key(s).
- Provide and validate application procedures for the various types of certificates that it may make publicly available.
- Issue digital certificates in accordance with this CPS and fulfill its obligations presented herein.
- Upon receipt of a request from an RA operating within the Network Solutions network act promptly to issue a Network Solutions certificate in accordance with this Network Solutions CPS.
- Upon receipt of a request for revocation from an RA operating within the Network Solutions network act promptly to revoke a Network Solutions certificate in accordance with this Network Solutions CPS.
- Publish accepted certificates in accordance with this CPS.
- Provide support to subscribers and relying parties as described in this CPS

- Revoke certificates according to this CPS.
- Provide for the expiration and renewal of certificates according to this CPS.
- Make available a copy of this CPS and applicable policies to requesting parties.

The subscriber also acknowledges that Network Solutions has no further obligations under this CPS.

5.27) Fitness for a Particular Purpose

Network Solutions disclaims all warranties and obligations of any type, including but not limited to any warranty of fitness for a particular purpose, warranty of merchantability, warranty of non-infringement, and any warranty of the accuracy of unverified information provided, except as expressly provided otherwise herein or as cannot be excluded at law.

5.28) Other Warranties

Network Solutions does not warrant:

- The accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of Network Solutions except as it may be stated in the relevant product description below in this CPS and in the Network Solutions insurance policy.
- The accuracy, authenticity, completeness or fitness of any information contained in any Network Solutions Personal certificates, class 1, free, trial or demo certificates.
- And shall not incur liability for representations of information contained in a certificate except as otherwise expressly provided for herein.
- The quality, functions or performance of any software or hardware device.
- Although Network Solutions is responsible for the revocation of a certificate it cannot be held liable except as expressly provided for herein.
- The validity, completeness or availability of directories of certificates issued by a third party (including an agent) unless that is specifically stated by Network Solutions.

Back to Top

5.29) Non Verified Subscriber Information

Without limiting in any way the limitations of warranties and liabilities under this CPS, Network Solutions shall not be responsible for non-verified subscriber information submitted to Network Solutions, or the Network Solutions directory or otherwise submitted with the intention to be included in a certificate.

5.30) Exclusion of Certain Elements of Damages

In no event shall Network Solutions be liable to any person or entity for:

- Any indirect, incidental or consequential damages.
- Any loss of profits.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non performance of certificates or digital signatures.
- Any other transactions or services offered within the framework of this CPS.
- Any other damages except for those of a Relying Party due to the Relying Party's reasonable reliance on a Certificate or Site Seal, and then only as provided in the Relying Party Guarantee.
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the applicant. Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this CPS.

- Any liability that arises from the usage of a certificate that is not valid.
- Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or on the CPS.
- Any liability that arises from security, usability, integrity of products, including hardware and software a subscriber uses.
- Any liability that arises from compromise of a subscriber's private key.

Network Solutions does not limit or exclude liability for death or personal injury.

5.31) Site Safe SLL Certificate and Assured Site Seal Relying Party Guarantee

The cumulative maximum liability accepted by Network Solutions under the Relying Party Guarantee (which can be found in the Repository) is set forth below.

5.31.1) nsProtect™ Secure Xpress

The cumulative liability of Network Solutions to all Relying Parties in respect of each nsProtect™ Secure Basic SSL Certificate pursuant to the Relying Party Guarantee shall not exceed $10,000 (ten thousand US dollars) in the aggregate or $1,000 per person per incident.

5.31.2) nsProtect™ Secure Basic SSL Certificate

The cumulative liability of Network Solutions to all Relying Parties in respect of each nsProtect™ Secure Basic SSL Certificate pursuant to the Relying Party Guarantee shall not exceed $50,000.00 (fifty thousand US dollars) in the aggregate or $1,000 per person per incident.

5.31.3) nsProtect™ Secure Advanced SSL Certificate

The cumulative liability of Network Solutions to all Relying Parties in respect of each nsProtect™ Secure Advanced SSL Certificate pursuant to the Relying Party Guarantee shall not exceed $1,000,000.00 (one million US dollars) in the aggregate or $1,000 per person per incident.

5.31.4) nsProtect™ Secure Wildcard SSL Certificate

The cumulative liability of Network Solutions to all Relying Parties in respect of each nsProtect™ Secure Wildcard SSL Certificate pursuant to the Relying Party Guarantee shall not exceed $1,000,000.00 (one million US dollars) in the aggregate or $1,000 per person per incident.

Back to Top

5.31.5) Network Solutions Secure Site Seal

The Network Solutions Secure Site Seal shares the cumulative liability of the SSL Certificate to which it corresponds, and therefore, the cumulative liability of Network Solutions to all Relying Parties in respect of each Network Solutions Secure Site Seal pursuant to the Relying Party Guarantee shall not exceed the cumulative liability of (nor shall the per person per incident limit exceed the per person per incident limit of) the SSL Certificate to which it corresponds.

5.31.6) nsProtect™ Assured Site Seal

The cumulative liability of Network Solutions to all Relying Parties in respect of each nsProtect™ Assured Site Seal pursuant to the Relying Party Guarantee shall not exceed $50,000.00 (fifty thousand US dollars) in the aggregate or $1,000 per person per incident.

5.32) Financial Limitations on Certificate Usage

Network Solutions certificates may only be used in connection with data transfer and transactions having a US dollar (US$) value no greater than $10,000 (ten thousand dollars).

5.33) Reserved

5.34) Conflict of Rules

When this CPS conflicts with other rules, guidelines, or contracts, this CPS, Version 2.8, shall prevail and bind the subscriber and other parties except as to:

- Contracts predating the first public release of the present version of this CPS;
- Contracts expressly superseding this CPS which such contract shall govern as to the parties thereto, and to the extent permitted by law; or
- Relying Party Agreements, Certificate and Site Seal Subscriber Agreements, and the terms of the Relying Party Guarantee.

5.35) Intellectual Property Rights

Except as otherwise set forth herein, all right, title and interest in and to all, (i) registered and unregistered trademarks, service marks and logos; (ii) patents, patent applications, and patentable ideas, inventions, and/or improvements; (iii) know-how; (iv) all divisions, continuations, reissues, renewals, and extensions thereof now existing or hereafter filed, issued, or acquired; (v) registered and unregistered copyrights including, without limitation, any forms, images, audiovisual displays, text, software ("Network Solutions Intellectual Property Rights") are owned by Network Solutions or its licensors, and you agree to make no claim of interest in or ownership of any such Network Solutions Intellectual Property Rights. You acknowledge that no title to the Network Solutions Intellectual Property Rights is transferred to you, and that you do not obtain any rights, express or implied, in the Network Solutions or its licensors' service, other than the rights expressly granted in this Agreement. To the extent that you create any derivative work (any work that is based upon one or more preexisting versions of a work provided to you, such as an enhancement or modification, revision, translation, abridgement, condensation, expansion, collection, compilation or any other form in which such preexisting works may be recast, transformed or adapted) such derivative work shall be owned by Network Solutions and all right, title and interest in and to each such derivative work shall automatically vest in Network Solutions. Network Solutions shall have no obligation to grant you any right in any such derivative work.

Back to Top

5.36) Infringement and Other Damaging Material

Network Solutions subscribers represent and warrant that when submitting to Network Solutions and using a domain and distinguished name (and all other certificate application information) they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortuous interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

Although Network Solutions will provide all reasonable assistance, certificate subscribers shall defend, indemnify, and hold Network Solutions harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of Network Solutions.

5.37) Ownership

Certificates are the property of Network Solutions. Network Solutions gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. Network Solutions reserves the right to revoke the certificate at any time.

5.38) Governing Law

This CPS shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of Network Solutions SSL Certificates or other products and services. Virginia law applies in all Network Solutions commercial or contractual relationships in which this CPS may apply or be quoted implicitly or explicitly in relation to Network Solutions products and services where Network Solutions acts as a provider, supplier, beneficiary receiver or otherwise.

5.39) Jurisdiction

Each party, including Network Solutions partners, subscribers and relying parties, irrevocably agrees to submit to the exclusive jurisdiction and venue of the state and federal courts in Fairfax County, Virginia and the Eastern District of Virginia, respectively, for the resolution of any dispute arising out of or in connection with this CPS or the provision of Network Solutions PKI services.

Back to Top

5.40) Dispute Resolution

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) all parties other than Network Solutions agree to notify Network Solutions of the dispute with a view to seek dispute resolution.

5.41) Successors and Assigns

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are freely assignable by Network Solutions, but not by any other party.

5.42) Severability

If any provision of this CPS, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted in such manner as to affect the original intention of the parties. Each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

5.43) Interpretation

The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices, if any, and definitions to this CPS, are for all purposes an integral and binding part of the CPS.

5.44) No Waiver

This CPS shall be enforced as a whole, whilst failure by any person to enforce any provision of this CPS shall not be deemed a waiver of future enforcement of that or any other provision.

5.45) Notice

Network Solutions accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from Network Solutions the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

2325 Dulles Corner Blvd.
Suite 700
Herndon, VA 20171
Attention: Legal Practices
Email: sslcpa@networksolutions.com

Back to Top

This CPS, related agreements and Certificate policies referenced within this document are available online at http://www.networksolutions.com/legal/SSL-legal-repository-sa.jsp.

5.46) Fees

Network Solutions charges Subscriber fees for some of the certificate services it offers, including issuance, renewal and reissues (in accordance with the Network Solutions Reissue Policy stated in 5.47 of this CPS). Such fees are detailed on the official Network Solutions websites (www.networksolutions.com).

Network Solutions does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a Network Solutions issued certificate through the use of Certificate Revocation Lists.

Network Solutions retains its right to affect changes to such fees. Network Solutions partners, including Wholesale Partners and SRSPlus Partners, will be suitably advised of price amendments as detailed in the relevant partner agreements.

5.47) Reissue Policy

Network Solutions offers a 30 day reissue policy. During a 30 day period (beginning when a certificate is first issued) the Subscriber may request a reissue of their SSL Certificate and incur no further fees for the reissue. If details other than just the public key require amendment, Network Solutions reserves the right to revalidate the application in accordance with the validation processes detailed within this CPS. If the reissue request does not pass the validation process, Network Solutions reserves the right to refuse the reissue application. Under such circumstances, the original SSL Certificate may be revoked and a refund provided to the applicant. Network Solutions is not obliged to reissue a certificate after the 30 day reissue policy period has expired.

5.48) Refund Policy

Except as otherwise expressly provided for herein, all payments made to Network Solutions are non-refundable.

Back to Top

6. General Issuance Procedure

6.1) General

Network Solutions offers different certificate types to make use of SSL and S/MIME technology for secure online transactions and secure email respectively. Prior to the issuance of a certificate Network Solutions will validate an application in accordance with this CPS which may involve the request by Network Solutions to the applicant for relevant official documentation supporting the application.

Network Solutions certificates are issued to organizations or individuals.

The validity period of Network Solutions certificates varies dependent on the certificate type, but typically a certificate will be valid for either 1 year, 2 years, 3 years or 4 years. Network Solutions reserves the right to, at its discretion, issues certificates that may fall outside of these set periods.

6.2) Certificates issued to Individuals and Organizations

A SSL Certificate request can be done according to the following means:
On-line: Via the Web (https). The certificate applicant submits an application via a secure online link according to a procedure provided by Network Solutions. Additional documentation in support of the application may be required so that Network Solutions verifies the identity of the applicant. The applicant submits to Network Solutions such additional documentation. Upon verification of identity, Network Solutions issues the certificate and sends a notice to the applicant. The applicant downloads and installs the SSL Certificate to its device. The applicant must notify Network Solutions of any inaccuracy or defect in a SSL Certificate promptly after receipt of the SSL Certificate or earlier notice of informational content to be included in the certificate.

Network Solutions may at its discretion accept applications via email.

6.3) Content

Typical content of information published on a nsProtect™ Secure ™ SSL Certificate may include but is not limited to the following elements of information:

6.3.1) Secure Server Certificates

- Applicant's fully qualified domain name.
- Applicant's organizational name.
- Code of applicant's country.
- Organizational unit name, street address, city, state.
- Issuing certification authority (Network Solutions).
- Applicant's public key.
- Network Solutions digital signature.
- Type of algorithm.

- Validity period of the digital certificate.
- Serial number of the digital certificate.

6.3.2) Reserved

Back to Top

6.4) Time to Confirm Submitted Data

Network Solutions makes reasonable efforts to confirm certificate application information and issue a SSL Certificate within reasonable time frame. The time frame is greatly dependent on the Subscriber providing the necessary details and / or documentation in a timely manner. Upon the receipt of the necessary details and / or documentation, Network Solutions aims to confirm submitted application data and to complete the validation process and issue / reject a certificate application within 2 working days.

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.

6.5) Issuing Procedure

The following steps describe the milestones to issue a Secure Server Certificate:

a) The applicant fills out the online request on Network Solutions' web site and the applicant submits the required information: Certificate Signing Request (CSR), e -mail address, common name, organizational information, country code, verification method and billing information.

b) The applicant accepts the on line subscriber agreement.

c) The applicant submits the required information to Network Solutions.

d) The applicant pays the certificate fees.

e) Network Solutions verifies the submitted information using third party databases and Government records

f) Upon successful validation of the application information, Network Solutions may issue the certificate to the applicant or should the application be rejected, Network Solutions will alert the applicant that the application has been unsuccessful.

g) Renewal is conducted as per the procedures outlined in this CPS and the official Network Solutions websites.

h) Revocation is conducted as per the procedures outlined in this CPS.

Back to Top

Document Control

This document is Network Solutions' Certification Practice Statement **Version 2.8**, created on September 4, 2018, for all SSL Certificates that it offers and is approved by the Network Solutions Certificate Policy Authority.

Please visit the Repository or contact Network Solutions for the publication date of this version.

Network Solutions, LLC
Digital Certificates Support
2325 Dulles Corner Blvd. Suite 700
Herndon, VA 20171, USA.
URL: http://www.networksolutions.com
E-mail: sslcpa@networksolutions.com
Tel: 703-668-4600