SECTION .0200 - DEFINITIONS

18 NCAC 10 .0201 APPLICABLE DEFINITIONS

In addition to the definitions in the Electronic Commerce Act, Article 11A of Chapter 66 (G.S. 66-58.1 et seq.), the following apply to the rules in this Chapter:

(1) Affiliated Individual. An "affiliated individual" means the subject of a certificate that is associated with a sponsor approved by the Certification Authority (such as an employee affiliated with an employer). Certificates issued to affiliated individuals are intended to be associated with the sponsor and the responsibility for authentication lies with the sponsor.

(2) Asymmetric Cryptosystem. "Asymmetric cryptosystem" means a computer-based system that employs two different but mathematically related keys. The keys are computer-generated codes having the following characteristics:

(a) either key can be used to electronically sign or encrypt data, such that only the other key in that key pair is capable of verifying the electronic signature or decrypting the signed data; and

(b) the keys have the property that, knowing one key, it is computationally infeasible to discover the other key.

(3) Authorized Certification Authority. "Authorized Certification Authority" means a Certification Authority that has been issued a Certification Authority license by the North Carolina Department of the Secretary of State to issue certificates that reference the rules in this Chapter.

(4) Certification Authority Revocation List. "Certification Authority Revocation List" means a time-stamped list of revoked Certification Authorities digitally signed by a Certification Authority or the Electronic Commerce Section.

(5) Certificate. "Certificate" means a record which:

(a) identifies the certification authority issuing it;

(b) names or identifies its subscriber;

(c) contains a public key that corresponds to a private key under the control of the subscriber;

(d) identifies its operational period or period of validity;

(e) contains a certificate serial number and is digitally signed by the Certification Authority issuing it; and

(f) conforms to the ITU/ISO X.509 Version 3 standards or other standards accepted under the Rules in this Chapter. As used in the rules in this Chapter the term "Certificate" refers to certificates that expressly reference the rules in this Chapter in the "Certificates Policy" filed for an X.509 v.3 certificate.

(6) Certificate Manufacturing Authority. "Certificate Manufacturing Authority" means an entity that is responsible for the manufacturing and delivery of certificates signed by a Certification Authority, but is not responsible for identification and authentication of certificate subjects (i.e., a Certificate Manufacturing Authority is delegated the certificate manufacturing task by a Certification Authority).

(7) Certificate Revocation List. "Certificate Revocation List" means a Certification Authority digitally signed, time-stamped list of revoked certificates.

(8) Certification Authority. "Certification Authority" means an entity authorized by the Secretary of State to facilitate electronic commerce. A Certification Authority is responsible for authorizing and causing certificate issuance. A Certification Authority may perform the functions of a Registration Authority and a Certificate Manufacturing Authority, or it may delegate or outsource either of these functions. A Certification Authority vouches for the connection between an entity and that entity’s electronic signature. A Certification Authority performs two essential functions:

(a) First, it is responsible for identifying and authenticating the intended subscriber named in a certificate, and verifying the subscriber possesses the private key corresponding to the public key listed in the certificate; and

(b) Second, the Certification Authority actually creates (or manufactures) and digitally signs the certificate. The certificate issued by the Certification Authority represents the Certification Authority's statement as to the identity of the person named in the certificate and the binding of that person to a particular public-private key pair.

(9) Certification Practice Statement. "Certification Practice Statement" means documentation of the practices, procedures, and controls employed by a Certification Authority issuing, suspending, or revoking certificates and providing access to same. A Certification Practice Statement shall contain, at a minimum, detailed discussions of the following topics:

(a) technical security controls, including cryptographic modules and management;
(b) physical security controls;
(c) procedural security controls;
(d) personnel security controls;
(e) repository obligations, including registration management, subscriber information protection, and certificate revocation management; and
(f) financial responsibility.

(10) Electronic Commerce Act. The term "Electronic Commerce Act" means The North Carolina Electronic Commerce Act, G.S. 66, Article 11A.

(11) Electronic Commerce Section. "Electronic Commerce Section" means the component of the North Carolina Department of the Secretary of State responsible for reviewing Certification Authority license applications and administering the Electronic Commerce Act in North Carolina.

(12) Electronic signature. "Electronic signature" means any identifier or authentication technique attached to or logically associated with an electronic record intended by the party using it to have the same force and effect as the party's manual signature.

(13) Federal Information Processing Standards. The term "Federal Information Processing Standards" means Federal standards prescribing specific performance requirements, practices, formats, communications protocols for hardware, software, data, and telecommunications operation.

(14) Internet Engineering Task Force. "Internet Engineering Task Force" means a large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

(15) ITS Security Director. "ITS Security Director" means the ITS Security Director of North Carolina State government as designated by the Chief Information Officer for North Carolina State Government.

(16) ITU/ISO X.509 Version 3 standards. "ITU/ISO X.509 Version 3 standards" means Version three of the X.509 standards promulgated by the International Telecommunications Union and the International Organization for Standardization.

(17) Key pair. The term "key pair" means two mathematically related keys, having the properties that one key can be used to encrypt a message that can only be decrypted using the other key, and even knowing one key, it is computationally infeasible to discover the other key.

(18) Object Identifier. An "object identifier" means an unambiguous identifying specially formatted number assigned in the United States by the American National Standards Institute (ANSI).

(19) Operational Period of a Certificate. The "operational period of a certificate" means the period of its validity. It begins on the date the certificate is issued (or such later date as specified in the certificate), and ends on the date and time it expires as noted in the certificate or as earlier revoked or suspended.

(20) PKIX. The term "PKIX" means an Internet Engineering Task Force Working Group developing technical specifications for a public key infrastructure components based on X.509 Version 3 certificates.

(21) Private Key. "Private key" means the key of a key pair used to create a digital signature. This key must be kept a secret. It is also known as the confidential key or secret key.

(22) Public Key. "Public key" means the key of a key pair used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided in a Certification Authority issued certificate and is often obtained by accessing a repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key. It is also known as the published key.

(23) Public Key Cryptography. "Public Key Cryptography" means a type of cryptographic technology employing an asymmetric cryptosystem.

(24) Registration Authority. The term "Registration Authority" means an entity responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of a Certification Authority).

(25) Relying Party. "Relying party" means a recipient of a digitally signed message who relies on a certificate to verify the digital signature on the message.

(26) Repository. "Repository" means a trustworthy system for storing and retrieving certificates and other information relating to those certificates.

(27) Repository Services Provider. "Repository Services Provider" means an entity that maintains a repository accessible to the public, or at least to relying parties, for purposes of obtaining copies of certificates or verifying the status of such certificates.

(28) Responsible Individual. "Responsible Individual" means a person designated by a sponsor to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

(29) Revoke A Certificate. "Revoke a certificate" means to prematurely end the operational period of a certificate from a specified time forward.

(30) Secretary. "Secretary" means the North Carolina Secretary of State.

(31) Sponsor. "Sponsor" means an organization with which a subscriber is affiliated (e.g., as an employee, user of a service, business partner, or customer).

(32) Subscriber. A "subscriber" means the person to whom a certificate is issued. A subscriber means a person who:

(a) is the subject named or identified in a certificate issued to such person;

(b) holds a private key that corresponds to a public key listed in that certificate; and

(c) to whom digitally signed messages verified by reference to such certificate are to be attributed.

(33) Suspend a certificate. "Suspend a certificate" means to temporarily suspend the operational period of a certificate for a specified time period or from a specified time forward.

(34) Transaction. "Transaction" means an electronic transmission of data between an entity and a public agency, or between two public agencies, including, but not limited to contracts, filings, and other legally operative documents not specifically prohibited in the Electronic Commerce Act.

(35) Trustworthy System. "Trustworthy system" means computer hardware, software, and procedures that:

(a) are secure from intrusion and misuse;

(b) provide a level of availability, reliability, and correct operation;

(c) are suited to performing their intended functions; and

(d) adhere to Federal Information Processing Standards.

(36) Valid Certificate. A "valid certificate" means one that:

(a) a Certification Authority has issued;

(b) the subscriber listed in it has accepted;

(c) has not expired; and

(d) has not been suspended or revoked.

A certificate is not valid until it is both issued by a Certification Authority and accepted by the subscriber.

(37) X.500. "X.500" means a directory standard / protocol for connecting local directory services to form one distributed global directory. X.500 is an OSI (Open System Interconnection) protocol, named after the number of the ITU (International Telecommunications Union - a United Nations Specialized Agency) CCITT (International Telegraph and Telephone Consultative Committee) Recommendation document containing its specification. This document is known as "Recommendation X.500 (03/00) - Information technology - Open systems interconnection - The Directory: public-key and attribute frameworks," and is available from International Telecommunication Union on the World Wide Web, www.itu.int, 183 Swiss Francs, price subject to change.

(38) X.509. "X.509" means a standard / protocol adopted by the International Telecommunication Union (formerly known as the International Telegraphy and Telephone Consultation Committee). For purposes of the Rules in this Chapter, all references to X.509 shall be construed as referring to version 3. Compliance with X.509 versions 1 or 2 shall not be construed as compliance with X.509. This document is known as "Recommendation X.509 (03/00) - Information technology - Open systems interconnection - The Directory: public-key and attribute frameworks," and is available from International Telecommunication Union on the World Wide Web, www.itu.int, 183 Swiss Francs, price subject to change.

History Note: *Authority G.S. 66-58.10(a)(1);*
Temporary Adoption Eff. February 23, 1999;
Codifier determined on November 23, 1999, agency findings did not meet criteria for temporary rule;
Temporary Adoption Eff. December 3, 1999;
Eff. March 26, 2001;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. December 6, 2016.