CHAPTER 10 - ELECTRONIC COMMERCE SECTION

SECTION .0100 - GENERAL ADMINISTRATION

18 NCAC 10 .0101 HOW TO CONTACT THE ELECTRONIC COMMERCE SECTION

(a) The Electronic Commerce Section may be contacted by the following means: Regular mail may be sent to the Electronic Commerce Section at the following address: Electronic Commerce Section, Department of the Secretary of State, PO Box 29622, 2 South Salisbury Street, Raleigh, NC 27626-0622.

(b) Up-to-date contact information regarding the Electronic Commerce Section is contained on the Department of the Secretary of State's Internet site at http://www.state.nc.us/secstate.

History Note: *Authority G.S. 66-58.10;*
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.

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.

SECTION .0300 - PUBLIC KEY TECHNOLOGY

18 NCAC 10 .0301 PUBLIC KEY TECHNOLOGY LICENSING, FEES, RENEWAL

(a) To be considered for licensure under this subsection, a Certification Authority shall utilize certificate-based public key cryptography.

(b) Any applicant seeking licensure must demonstrate compliance with the North Carolina Electronic Commerce Act, G.S. 66, Article 11A, and the rules in this Chapter.

(c) To request licensure, a Certification Authority shall provide the Electronic Commerce Section with a copy of its current Certification Practice Statement and most recent reports of compliance audit(s) as required by 18 NCAC 10 .0303 (k).

(d) A Certification Authority shall adhere to its Certification Practice Statement. If a Certification Authority modifies its Certification Practice Statement, it shall provide an updated copy of the Certification Practice Statement to the Electronic Commerce Section as soon as is practicable, and no later than the date the updated Certification Practice Statement is put into operation. As a condition of continued licensure, the Electronic Commerce Section may require the Certification Authority to undergo an audit to document compliance with its updated Certification Practice Statement and the rules in this Chapter.

(e) An initial licensing fee of two thousand dollars ($2,000 US) shall accompany an initial application.

(f) A renewal fee of two thousand dollars ($2,000 US) shall accompany an application for renewal by a licensed Certification Authority.

(g) A license issued by the Electronic Commerce Section pursuant to this Section shall expire one year after its effective date, unless timely renewed.

(h) Financial Responsibility.

(1) As precondition of licensure a Certification Authority shall obtain a bond issued by a surety company authorized to do business in North Carolina. A copy of the bond shall be filed with the Electronic Commerce Section prior to licensure. The amount of the bond shall not be less than twenty-five thousand dollars ($25,000 US). The bond shall be in favor of the State of North

Carolina. The bond shall be payable for any penalties assessed by the Electronic Commerce Section pursuant to the Rules in this Chapter and for any losses the State encounters resulting from a Certification Authority's conduct of activities subject to the Electronic Commerce Act or arising out of a violation of the Electronic Commerce Act or any Rule promulgated thereunder;

(2) As precondition of licensure a Certification Authority shall obtain indemnity insurance coverage (e.g. "errors and omissions" or "cyber coverage" or similar coverage) to protect subscribers, relying parties and the State for any losses resulting from the Certification Authority's conduct of activities subject to the Electronic Commerce Act or arising out of a violation of the Electronic Commerce Act or any Rule promulgated thereunder. Indemnity coverage shall be obtained and maintained in the amount of not less than one hundred thousand dollars ($100,000 US) per occurrence and not less than one million dollars ($1,000,000 US) for all occurrences;

(3) The failure of a Certification Authority to continuously maintain this surety bond and indemnity insurance coverage may be the basis for revocation or suspension of its license.

History Note: *Authority G.S. 66-58.3; 66-58.10(a)(2);*
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.

18 NCAC 10 .0302 PUBLIC KEY TECHNOLOGY CERTIFICATION AUTHORITY: CERTIFICATE ISSUANCE AND MANAGEMENT - OVERVIEW

(a) Overview. The Rules in this Section specify minimum requirements for issuance and management of certificates that may be used in verifying digital signatures. The digital signatures may be used on categories of electronic communications specified as suitable applications in 18 NCAC 10 .0302(b)(5). Each item in the Rules in this Section must be specifically addressed by the Certification Authority in the Certification Authority's Certification Practice Statement filed with the North Carolina Department of the Secretary of State at the time the Certification Authority submits an application for licensure or renewal.

(b) Community and Applicability.

(1) Certification Authorities. The Rules in this Chapter are binding on each licensed Certification Authority issuing certificates identifying them, and govern Certification Authority performance with respect to all certificates it issues referencing the Rules. Specific Certification Authority Practice Statements and procedures implementing the requirements of the Rules in this Chapter shall be set forth in the Certification Authority Certification Practice Statement;

(2) Certification Authorities Authorized to Issue Certificates Under the Rules in this Chapter. Any Certification Authority may issue certificates identifying the Rules in this Chapter if licensed in the State of North Carolina and the Certification Authority agrees to be bound by and comply with the undertakings and representations of the Rules in this Chapter with respect to such certificates. Issuance of a certificate referencing this Item shall constitute issuing the agreement of the Certification Authority to be bound by terms of the Rules for all certificates referencing them;

(3) Subscribers. A Certification Authority may issue certificates that reference the Rules in this Chapter to the following classes of subscribers:

(A) individuals (unaffiliated);

(B) individuals associated with a sponsor recognized by the Certification Authority ("affiliated individuals"), provided the sponsor is the subscriber of a valid certificate issued by the Certification Authority in accordance with the Rules in this Chapter;

(C) public agencies, as defined in G.S. 66-58.2; and

(D) organizations and businesses qualified as legal entities;

(4) Relying Parties. The Rules in this Chapter benefit the following persons, who may rely on certificates issued to others referencing them ("Qualified Relying Parties"):

(A) individuals intending to engage in a transaction with a public agency;

(B) public agencies, as defined in G.S. 66-58.2;

(C) organizations and businesses, qualified as legal entities, engaged in a transaction with a public agency; and

(D) other parties to a transaction with the entity and a public agency;

(5) Suitable Applications. Certificates referencing this Item are intended to provide a level of identity binding assurance and the protection of document encryption, and are typically suitable for:

(A) System Access / Systems Security

(i) Verifying the identity of electronic mail correspondents for non-critical communications;

(ii) Obtaining access to databases, applications and systems;

(iii) Message / document encryption for protection of contents/identities.

(B) Digital Signature Activity

(i) Commerce involving various goods or services with various values;

(ii) Obtaining personal data relating to the subscriber.

(C) Message / Document Encryption: Documents encrypted to protect contents (e.g. privacy of subscriber);

(6) Some sample applications of the Rules in this Chapter are:

(A) Computing applications providing access to the certificate holder's own personal information;

(B) Request and distribution of text information or other types of copyrighted content for which fees are charged or subscriptions are required;

(C) Verifying the identity of communicating parties;

(D) Verifying signatures on contracts, government benefits statements, and other documentation;

(E) Signing of electronic messages; e.g. official reports, employee leave and travel reporting, tax withholding; and

(F) Secure transport of individual, patient specific medical / other privileged information over public networks.

History Note: *Authority G.S. 66-58.10;*
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.

18 NCAC 10 .0303 PUBLIC KEY TECHNOLOGY: CERTIFICATE POLICY GENERAL PROVISIONS

(a) Certification Authority Obligations. The Certification Authority is responsible for all aspects of certificate issuance and management, including control over:

(1) the application / enrollment process;

(2) the identification and authentication process;

(3) the actual certificate manufacturing process;

(4) certificate publication;

(5) certificate suspension and revocation, publication of the Certificate Revocation List and Certification Authority Revocation Lists, as pertinent;

(6) certificate renewal;

(7) ensuring that all aspects of the Certification Authority services and Certification Authority operations and infrastructure related to certificates issued under the Rules in this Chapter are performed in accordance with the requirements, representations, and warranties of the Rules in this Chapter; and

(8) Delivering certificate updates and revocation transactions to the NC ITS directory, where pertinent.

(b) Representations by Certification Authority. By issuing a certificate referencing the Rules in this Chapter, a Certification Authority certifies to subscriber and all Qualified Relying Parties (who reasonably and in good faith rely on a certificate's information during its operational period in accordance with the Rules in this Chapter) that:

(1) the Certification Authority has verified certificate information unless otherwise noted in its Certification Practice Statement;
(2) the Certification Authority has issued, and will manage, the certificate in accordance with the Rules in this Chapter;
(3) the Certification Authority has complied with the requirements of the rules in this Chapter and its applicable Certification Practice Statement when authenticating the subscriber and issuing the certificate;
(4) there are no misrepresentations of fact in the certificate known to the Certification Authority, and the Certification Authority has verified additional information in the certificate unless otherwise noted in its Certification Practice Statement;
(5) subscriber-provided information in the certificate application has been accurately transcribed to the certificate; and
(6) the certificate meets all material requirements of the rules in this Chapter and the Certification Authority's certification practice statement.

(c) Registration Authority and Certificate Manufacturing Authority Obligations: The Certification Authority shall be responsible for performing all identification and authentication functions and all certificate manufacturing and issuing functions. However, the Certification Authority may delegate performance of these obligations to an identified Registration Authority or Certificate Manufacturing Authority, provided the Certification Authority remains primarily responsible for performance of those services by such third parties in a manner consistent with requirements of the rules in this Chapter.

(d) Repository Obligations: The Certification Authority shall be responsible for providing a repository, performing / providing certificate updates as required and performing all associated functions. However, the Certification Authority may delegate performance of this obligation to an identified Repository Services Provider, provided the Certification Authority remains primarily responsible for performance of those services by such third party in a manner consistent with the requirements of the rules in this Chapter.

(e) Subscriber Obligations. In all cases, the Certification Authority shall require the subscriber to enter an enforceable contractual commitment for the benefit of Qualified Relying Parties obligating the subscriber to:

(1) take precautions to prevent any loss, disclosure, or unauthorized use of the private key;
(2) acknowledge that by accepting the certificate the subscriber is warranting all information and representations made by the subscriber included in the certificate are true;
(3) use the certificate exclusively for authorized and legal purposes, consistent with the rules in this Chapter; and
(4) immediately contact the Certification Authority and instruct the Certification Authority to revoke the certificate promptly upon any actual or suspected loss, disclosure, or other subscriber private key compromise.

(f) Relying Party Obligations. A Qualified Relying Party may rely on a certificate referencing this Item only if the certificate was used and relied upon for lawful purposes and under circumstances where:

(1) the reliance was reasonable and in good faith in light of all circumstances known to the relying party at the time of reliance;
(2) the purpose for which the certificate was used was appropriate under the rules in this Chapter; and
(3) the relying party checked the certificate status certificate prior to reliance, or a check of the certificate's status would have indicated the certificate was valid.

(g) Interpretation & Enforcement.

(1) Governing Law. The laws of the State of North Carolina shall govern the enforceability, construction, interpretation, and validity of the rules in this Chapter.
(2) The holders of North Carolina Certification Authority licenses are not guaranteed any business by public agencies in North Carolina. All other state laws required to engage in business with public agencies in North Carolina must be complied with by the Certification Authority and public agencies.

(h) Fees. A Certification Authority shall not impose any fees for reading the rules in this Chapter or its Certification Practice Statement. A Certification Authority may charge access fees on certificates, certificate status information, or certificate revocation lists, subject to agreement between the Certification Authority and subscriber, and in accordance with a fee schedule published by the Certification Authority in its Certification Practice Statement or otherwise.

(i) Publication and Repositories:

(1) Publication of Certification Authority Information. Each authorized Certification Authority shall operate a secure online repository available to Qualified Relying Parties. The repository shall contain:
  (A) issued certificates that reference the rules in this Chapter;
  (B) a Certificate Revocation List or on-line certificate status database;
  (C) the Certification Authority's certificate for its signing key;
  (D) past and current versions of the Certification Authority's Certification Practice Statement; and
  (E) a copy of the rules in this Chapter.

(2) Frequency of Publication. All information to be published in the repository shall be published promptly after such information is available to the Certification Authority. In no case shall more than 24 hours pass between certification authority awareness of a change and the Certification Authority publishing of the change. Certificates issued by the Certification Authority referencing the rules in this Chapter shall be published promptly upon acceptance of such certificate by the subscriber. Certificate revocations and suspensions shall be published contemporaneously with the act of revocation or suspension. Information relating to revocation or suspension of a certificate shall be published in accordance with 18 NCAC 10 .0305(f)(2) and 18 NCAC 10 .0305(h).

(j) Access Controls. The repository shall be available to Qualified Relying Parties and subscribers 24 hours per day, 7 days per week, subject to published, scheduled maintenance and the Certification Authority's then-current terms of access. A Certification Authority shall not impose any access controls on the rules in this Chapter, the Certification Authority's certificate for its signing key, and past and current versions of the Certification Authority's Certification Practice Statement. A Certification Authority may impose access controls on certificates, certificate status information, or Certificate Revocation Lists at its discretion, subject to agreement between the Certification Authority and subscriber, in accordance with provisions published in its Certification Practice Statement or otherwise.

(k) Required Compliance Audits:

(1) The Certification Authority must submit to audit to determine its stability, prospects for longevity and adequacy of its security practices and conditions. The audits must result in unqualified compliance reports. When a Certification Authority is licensed in North Carolina based on a reciprocity agreement between North Carolina and another state, the Certification Authority may submit certified copies of audit reports required by the other jurisdiction. After review by the Electronic Commerce Section, audit reports may be determined to meet North Carolina Certification Authority audit requirements.

(2) A Certification Authority shall adhere to its Certification Practice Statement. If a Certification Authority modifies its Certification Practice Statement, it shall provide an updated copy of the Certification Practice Statement to the Electronic Commerce Section as soon as practicable and no later than the date the updated Certification Practice Statement is put into operation. At the discretion of the Electronic Commerce Section, the Certification Authority may be required to undergo additional / other audits for license renewal.

(3) Stability and Longevity Prospects Audit:
  (A) Before initial approval as a licensed Certification Authority, the Certification Authority (and each Registration Authority, Certificate Manufacturing Authority, and Repository Services Provider, as applicable) shall submit to audit by an independent Certified Public Accounting firm. The audit must address the American Institute of Certified Public Accountants (AICPA) Section 341, "The Auditor's Consideration of an Entity's Ability to Continue as a Going Concern".
  (B) The audit must produce an unqualified report from the CPA firm to the Certification Authority. A certified copy of the audit report must be attached by the Certification Authority to the application for a new Certification Authority license or renewal license, and submitted to the Electronic Commerce Section.
  (C) As a condition of continued licensure, the Electronic Commerce Section may require the Certification Authority to undergo audit to document compliance with expectations for secure operations, an updated Certification Practice Statement, or to document continuing compliance with the ITU/ISO X.509 Version 3 standards and the rules in this Chapter.

(D) A Certification Authority operated by an Agency of the State of North Carolina is exempt from this requirement.

(4) Security Audit. The purpose of a security audit is to verify:

(A) The Certification Authority has in place a secure system assuring quality of Certification Authority Services provided; and

(B) the Certification Authority's system complies with all security requirements of the rules in this Chapter, the Certification Authority's Certification Practice Statement and ITU/ISO X.509 Version 3 standards.

Before initial approval as a licensed Certification Authority, and thereafter at least once every year, the Certification Authority shall submit to a security compliance audit by a security firm. The audit must evidence compliance with Federal Information Processing Standards 140-1 "Security: Cryptographic Modules" Level 2 and TSEC (The Orange Book) C2 criteria or comply with contemporary Certification Authority security criteria as expressed in terms of the "Common Criteria" – ISO 15408-1:1999. In order for an audit firm to be approved by the Electronic Commerce Section, it must engage or employ at least one Certified Information Systems Auditor (CISA) certified by the Information Systems Audit and Control Association (CISACA), 3701 Algonquin Road, Rolling Meadows, Illinois, 60008, www.ISACA.org. A certified copy of the current unqualified security audit report must be attached to an application for a new certification authority license or renewal license, and submitted to the NC Department of Secretary of State, Electronic Commerce Section.

(l) Confidentiality Policy. Subscriber consent must be obtained for each incident of disclosure and for each item of information unless required otherwise by law. The Certification Authority may not sell or exchange information in any circumstance that is not specifically allowed by the Rules in this Chapter or otherwise required by law.

(1) A Certification Authority may not use data gathered in fulfilling its Certification Authority role for any other purpose. A Certification Authority shall not gather information beyond that necessary to authenticate a subscriber nor shall it use information gathered in its Certification Authority role to assemble further information about subscribers; and

(2) Under no circumstance shall a Certification Authority (or any Registration Authority, Repository Services Provider, or Certificate Manufacturing Authority) have access to the signing private key(s) (versus encryption key(s)) of any subscriber to whom it issues a certificate referencing the Rules in this Chapter, except for initial creation of the signing/secret key where the key is not accessed and no enduring record is made of the key.

(m) Information Not Considered Confidential.

(1) Information appearing on certificates is not confidential.

(2) Disclosure of Certificate Revocation / Suspension Information. Information regarding the revocation or suspension status of a certificate is not confidential and is disclosed in the normal course of public key infrastructure activity.

(3) Any information may be disclosed upon owner's request.

History Note: *Authority G.S. 66-58.10;*
Codifier determined on November 23, 1999, agency findings did not meet criteria fo 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.

18 NCAC 10 .0304 PUBLIC KEY TECHNOLOGY; IDENTIFICATION AND AUTHENTICATION

(a) Initial Registration:

(1) Subject to the requirements of this Rule, certificate applications may be communicated from the applicant to Certification Authority or Registration Authority, and authorizations to issue certificates may be communicated from a Registration Authority to the Certification Authority, electronically, via E-mail or a web site, provided all communication is secured by SSL or a similar security protocol, by first class U.S. Mail or similar service.

(2) North Carolina deploys two levels / classes of authentication certificate:

(A) North Carolina Basic Authentication Certificate: A North Carolina Basic Authentication Certificate is a digital certificate manufactured by a licensed Certificate Authority intended to be used to sign routine internal North Carolina government business documents (e.g. personnel leave documents, travel reimbursement requests and similar documents) and to gain access to State systems when deemed appropriate by information technology security policy.

(B) North Carolina Strong Authentication Certificate: A North Carolina Strong Authentication Certificate is a digital certificate manufactured by a North Carolina licensed Certificate Authority intended to be used with a high degree of confidence to sign any document.

(b) Types of Names. The subject name used for certificate applicants shall be the X.509 Distinguished Name. The name shall be unique for each entity certified by a Certification Authority. A Certification Authority may issue more than one certificate with the same subject name for the same subject entity.

(c) Name Meanings. The subject name listed in a certificate must have a reasonable association with the authenticated name of the subscriber. In the case of an individual, this shall be a combination of first name or initials and surname. In the case of an organization, the name shall reflect the legal name of the organization or unit.

(d) Name Uniqueness. The subject name listed in a certificate shall be unambiguous and unique for all certificates issued by the Certification Authority and shall conform to X.500 standards for name uniqueness. If necessary, additional numbers or letters may be appended to the real name to ensure the name's uniqueness within the domain of certificates issued by the Certification Authority and detailed in the Certification Practice Statement.

(e) Verification of Key Pair. The Certification Authority shall establish that the applicant is in possession of the private key corresponding to the public key submitted with the application.

(f) Authentication of an Organization. An organization may be issued a North Carolina Strong Authentication Certificate. An organization shall not be issued a North Carolina Basic Authentication Certificate.

(1) Identification. A Certification Authority shall be presumed to have confirmed that the prospective subscriber organization is the organization to be listed in a certificate where the Certification Authority has assured by investigation:

(A) The organization exists and conducts business at the address listed in the certificate application;

(B) A duly authorized representative of the applicant organization signed the certificate application;

(C) The information contained in the certificate application is correct; and

(D) If required by State law, the organization is authorized to transact business by the Corporations Division of the North Carolina Department of the Secretary of State.

(2) A Certificate Authority or Registration Authority, when authenticating an applicant who is an organization, shall require the following information on a notarized affidavit:

(A) Organization Name;

(B) Street address and mailing address, if different;

(C) City;

(D) State;

(E) Zip;

(F) Tax Payer Identification Number / Employer Identification Number (EIN);

(G) Corporate Identification Number (Issued by Secretary of State);

(H) Date of incorporation or creation;

(I) State or country of incorporation or creation;

(J) Telephone number (optional);

(K) E-mail address (optional);

(L) Post data element (e.g. password) to be a secret shared with the Certification Authority / Registration Authority and used later for authentication in the absence of the digital signature. This element may be used along with additional information to authenticate a request for certificate revocations; and

(M) Name of officially authorized agent, if applicable.

(3) Authentication and Confirmation Procedure. In conducting its review and investigation, the Certification Authority shall review official government records or engage the services of a third party vendor of business information to do so. The Certification Authority or third party review shall provide validation information concerning each organization applying for a certificate,

including legal company name, type of entity, year of formation, names of directors and officers, address, telephone number, and good standing in the jurisdiction where the applicant was incorporated or otherwise organized.

(g) Authentication of Individual -- No Affiliation: An unaffiliated individual may be issued a North Carolina Strong Authentication Certificate, North Carolina Basic Authentication Certificate, or both. In determining the type of certificate required, agencies shall evaluate the application's risk of loss involved and nature of business with which the certificate holder shall be associated. Based on the evaluation, a NC Basic Authentication Certificate may be appropriate. In other cases, it may be appropriate to require a North Carolina Strong Authentication Certificate may be appropriate. In other cases, it may be appropriate to require a North Carolina Strong Authentication Certificate.

(1) Identification:

(A) North Carolina Strong Authentication Certificate. A Certification Authority shall be presumed to have confirmed that the prospective subscriber is the person to be listed in a certificate where the Certification Authority has been presented with at least two identification documents. At least one piece of identification shall be a current federal or state government-issued picture-type identification such as a military or government identification card, driver's license, or similar identification document issued under authority of another country, or passport. The Certification Authority or Registration Authority shall initial, date and archive copies of identification used to establish the subscriber's identity.

(2) Authentication for a North Carolina Strong Authentication Certificate. Authenticating an unaffiliated individual applicant, the Certification Authority or Registration Authority shall require the following elements of information from the applicant on a notarized affidavit:

(A) Last name (family name);
(B) First name (given name);
(C) Middle Name(s);
(D) Street address and mailing address, if different;
(E) City;
(F) State;
(G) Zip;
(H) Social Security Number (SSN), national identification number or passport number;
(I) Driver's license number, or state identification card number;
(J) Date of birth;
(K) Place of birth;
(L) Telephone number (optional);
(M) E-mail address (optional);
(N) Post data element (e.g. mother's maiden name, password) to be used later for authenticating an individual in the absence of their digital signature. This element may be used along with additional information to authenticate a request for certificate revocations; and
(O) Name of officially authorized agent, if applicable.

(3) Authentication for a North Carolina Basic Authentication Certificate. Certification Authorities or Registration Authorities shall require a notarized affidavit from the applicant's personnel officer, signed by the applicant including:

(A) Last name (family name);
(B) First name (given name);
(C) Middle name(s);
(D) Street address and mailing address, if different;
(E) City;
(F) State;
(G) Zip;
(H) Social Security Number (SSN), national identification number or passport number;
(I) Driver's license number, or state identification card number;
(J) Date of birth;
(K) Place of birth;
(L) Business Telephone number (optional);

(M) Business E-mail address (optional) as assigned by agency;
(N) Post data element (e.g. mother's maiden name, password) to be used later for authenticating an individual in the absence of their digital signature. This element may be used along with additional information to authenticate a request for certificate revocations;
(O) Name of officially authorized agent, if applicable;
(P) Beginning date of employment; and
(Q) Ending date of employment (if known).

(4) Investigation and Confirmation. Verification of the name and SSN and the Name and Driver's License (or ID Number) data elements may be accomplished via checks with the Social Security Administration and the appropriate state motor vehicle administration. Verification of the name and address data elements may be accomplished through access to either a commercial or governmental data source (e.g. Department of Motor Vehicles, personnel office, etc.). The address confirmation data sources may consist of either online databases or local business records (e.g., a bank's customer records, the U.S. Postal Service, state motor vehicle department records, state personnel office).

(5) Personal Presence. Authentication of an unaffiliated individual requires the applicant must either:
(A) personally present himself or herself to a Registration Authority to be authenticated prior to certificate issuance. An individual may meet expectations for personal presence by an attorney-in-fact, trustee or other court appointed fiduciary; or
(B) securely deliver signed and notarized copies of the requisite identification to the Certification Authority [in which case, once notarized copies are delivered parties may communicate electronically]. Where the applicant delivers notarized copies of identification to the Certification Authority, authentication of such identification shall be confirmed through the use of a shared secret [such as a personal identification number]. The shared secret is separately communicated to the applicant in a manner that assures its confidentiality and included with the documents delivered as part of the certificate application process.

(h) Authentication of Individual – Affiliated Certificate.

(1) Identification.
(A) The Certification Authority may establish a trustworthy procedure whereby a sponsoring organization that has been authenticated by the Certification Authority and issued a certificate may designate one or more Responsible Individuals, and authorize them to represent the sponsoring organization concerning the issuance and revocation of certificates for affiliated individuals. The Certification Authority may rely on a designated Responsible Individual appointed by the sponsor to properly authenticate the individual applicant, if the Certification Authority has previously authenticated the sponsor as an organization and the Responsible Individual as an unaffiliated individual, in accordance with the rules in this Chapter. A Certification Authority shall be presumed to have confirmed a prospective subscriber is the person to be listed in a certificate where the Certification Authority relies on a designated Responsible Individual appointed by the sponsor to properly authenticate the individual applicant, if the Certification Authority has previously authenticated the sponsor as an organization and the Responsible Individual as an unaffiliated individual, in accordance with the rules in this Chapter.
(B) In the absence of a trustworthy procedure, If the requirements of 18 NCAC 10 .0304(h)(1)(A) cannot be met, then affiliated individuals shall be authenticated in the same manner as unaffiliated individuals.

(2) Authentication Confirmation Procedure. Authentication of the individual shall be confirmed through the use of a shared secret [such as a Personal Identification Number]. The shared secret is distributed by an out of band communication to the applicant (either directly or via the sponsor) and included in the application process as part of the certificate enrollment process.

(3) Personal Presence.
(A) Applicants affiliated with an approved sponsor may be authenticated through an electronically submitted application, based on an agreement with the sponsor, the approval of a designated Responsible Individual, and the distribution of Personal Identification Numbers or a similar security device.

(B) If a Certification Authority elected to use an online commercial database, the application may be filled out and submitted via the Internet from a home or business computer. In the case where a Certification Authority elects to use a local record check, the application process may take place over the Internet, or alternatively, the Certification Authority may require the applicant personally appear at a designated business site in order to enter required information at a local terminal.

(4) Duties of Responsible Individual. The Responsible Individual represents the sponsoring organization with respect to the issuance and management of certificates. In that capacity he or she is responsible for properly indicating which subscribers are to receive certificates.

(i) Renewal Applications (Routine Re-key). A subscriber may request issuance of a new certificate for a new key pair from the Certification Authority issuing the original certificate. The request may be made electronically by a digitally signed message based on the old key pair in the original certificate under these conditions:

(1) The request must occur during the period two months prior to normal scheduled certificate expiration;

(2) The subscriber must be authenticated following the principles of the rules in this Chapter; and

(3) The original certificate has not been suspended or revoked.

(j) Re-key after Revocation. Revoked or expired certificates shall not be renewed under any conditions. Applicants without a valid certificate from the Certification Authority that references the rules in this Chapter shall be re-authenticated by the Certification or Registration Authority on certificate application, just as with a first-time application.

(k) Revocation Request.

(1) Electronic Revocation Request.

(A) A revocation request submitted electronically may be authenticated by digital signature using the "old" key pair.

(B) Electronic revocation requests authenticated on the basis of the old (compromised) key pair shall always be accepted as valid. Other revocation request authentication mechanisms are acceptable. These authentication mechanisms balance the need to prevent unauthorized revocation requests against the need to quickly revoke certificates.

(2) Non-Electronic Revocation Request.

(A) Organization initiated revocation of affiliated certificate(s) shall be authenticated by communication from a known person or official authorized to initiate revocations on behalf of an organization.

(B) Subscriber initiated requests for revocation of certificate(s) shall be authenticated by presentation of a signed and notarized request for revocation.

(C) Subscriber initiated requests for revocation of certificates via an attorney-in-fact shall be authenticated by presentation of

(i) a notarized request for revocation by the attorney-in-fact; and

(ii) a certified copy of the power of attorney.

(D) Revocation by a court of competent jurisdiction may be made by presentation of a certified court order.

History Note: *Authority G.S. 66-58.10;*
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.

18 NCAC 10 .0305 PUBLIC KEY TECHNOLOGY: OPERATIONAL REQUIREMENTS

(a) Certificate Application. A certificate applicant shall complete a certificate application in a form prescribed by the Certification Authority Certificate Policy and enter into a subscriber agreement with the Certification Authority. All applications are subject to Certification Authority review, approval, and acceptance. A Certificate Policy shall define the minimum content to be used for a certificate application. The Certificate Policy shall also specify that all applications are subject to review, approval, and acceptance by the Policy Authority in addition to the Issuer.

(b) Certificate Issuance. Upon successful completion of the subscriber identification and authentication process in accordance with the rules in this Chapter and complete and final approval of the certificate application, the Certification Authority shall:

(1) issue the requested certificate;

(2) notify the applicant thereof; and

(3) make the certificate available to the applicant using a procedure that:

(A) assures the certificate is only delivered to or available for subscriber pickup; and

(B) provides adequate proof of subscriber identification in accordance with the Rules in this Chapter.

A Certification Authority shall not issue a certificate without the consent of the applicant and, if applicable, the applicant's sponsor.

(c) Certificate Acceptance. Following certificate issuance, the Certification Authority shall continually require the subscriber to expressly indicate certificate acceptance or rejection to the Certification Authority, in accordance with established Certification Authority Certification Practice Statement procedures.

(d) Circumstances for Revocation of Certificate.

(1) Permissive Revocation. A subscriber may request revocation of his, her, or its certificate at any time for any reason. A sponsoring organization, where applicable, may request certificate revocation of any affiliated individual at any time for any reason. The issuing Certification Authority may also revoke a certificate upon failure of the subscriber, or where applicable, sponsoring organization failure to meet its obligations under the rules in this Chapter, the applicable Certification Practice Statement, or any other agreement, regulation, or law applicable to the certificate that may be in force.

(2) Required Revocation. A subscriber or sponsoring organization, where applicable, shall promptly request revocation of a certificate when:

(A) any information on the certificate changes or becomes obsolete;

(B) the private key, or the media holding the private key associated with the certificate is, or is suspected of having been compromised; or

(C) an affiliated individual is no longer affiliated with the sponsor.

(3) The issuing Certificate Authority shall revoke a certificate:

(A) upon request of the subscriber or sponsoring organization;

(B) upon failure of the subscriber (or the sponsoring organization, where applicable) to meet its material obligations under the Rules in this Chapter, any applicable Certification Practice Statement, or any other agreement, regulation, or law applicable to the certificate that may be in force;

(C) if knowledge or reasonable suspicion of compromise is obtained; or

(D) if the Certification Authority determines that the certificate was not properly issued in accordance with the rules in this Chapter and any applicable Certification Practice Statement.

(4) Notice of the Certification Authority ceasing operation shall be posted to the Certification Authority Revocation List maintained by the Electronic Commerce Section of the Department of the Secretary of State.

(e) Who Can Request Revocation. The only persons permitted to request revocation of a certificate issued pursuant to the Rules in this Chapter are:

(1) the subscriber;

(2) the sponsoring organization (where applicable); and

(3) the issuing Certification Authority.

(f) Procedure for Revocation Request.

(1) A certificate revocation request shall be promptly communicated to the issuing Certification Authority, either directly or through a Registration Authority. A certificate revocation request may be communicated electronically if it is digitally signed with the private key of the subscriber, or where applicable, the sponsoring organization. Requests digitally signed by the subscriber, or by the sponsoring organization, are considered authenticated when received by the Certification Authority or Registration Authority. Alternatively, the subscriber, or where applicable, the sponsoring organization, may request revocation by contacting the Certification Authority or an authorized Registration Authority in person and providing adequate proof of identification to authenticate the request in accordance with 18 NCAC 10 .0304(f)(1) or (g)(1). Copies of the

digitally signed request must be archived by the Certification Authority or Registration Authority. Other identification used to establish the subscriber's identity shall be photocopied and initialed by an authorized representative of the Certification Authority or Registration Authority and archived.

(2) Repository/Certificate Revocation List Update. Promptly, within less than 2 hours of revocation, the Certificate Revocation List, or certificate status database in the repository, as applicable, shall be updated. All revocation requests and the resulting actions taken by the Certification Authority shall be archived.

(g) Revocation Request Grace Period. Certificate revocation requests shall be authenticated and processed within 2 hours of receipt by the Certification Authority.

(h) Certificate Suspension. The procedures and requirements stated for certificate revocation must also be followed for certificate suspension, where implemented.

(i) Certificate Revocation List Issuance Frequency. When Certificate Revocation Lists are used, an up-to-date Certificate Revocation List shall be issued to the repository at least every 2 hours. If no change has been made to the Certificate Revocation List, an update to the Certificate Revocation List in the repository is not necessary.

(j) Online Revocation / Status Checking Availability. Whenever an online certificate status database is used as an alternative to a Certificate Revocation List, such database shall be updated no later than 2 hours after certificate revocation.

(k) Computer Security Audit Procedures. All security events, including but not limited to:

(1) corruption of computing resources, software or data;

(2) revocation of the entity public key;

(3) compromise of the entity key; or

(4) the invocation of a disaster recovery plan, on the Certification Authority system shall be automatically recorded in audit trail files. The audit log shall be processed and archived at least once a week.

Such files shall be retained for at least 6 months onsite, and thereafter shall be securely archived.

(l) Records, Archival.

(1) Types of Records Archived. The following data and files must be archived by (or on behalf of) the Certification Authority:

(A) All computer security audit data;

(B) All certificate application data;

(C) All certificates, and all Certificate Revocation Lists or certificate status records generated;

(D) Key histories; and

(E) All correspondence between the Certification Authority and Registration Authority, Certificate Manufacturing Authority, Repository Services Provider, and subscriber.

(2) Retention Period for Archive. Key and certificate information and archives of audit trail files must be retained for at least 30 years.

(3) Protection of Archive. The archive media must be protected either by physical security alone, or a combination of physical security and cryptographic protection. The archive must be protected from environmental threats such as temperature, humidity, and magnetism. The Certification Practice Statement must address the procedure for transferring and preserving the archive media in the case of the Certification Authority ceasing operation in this State.

(4) Archive Backup Procedures. Adequate backup procedures must be in place. In event of loss or destruction of primary archives, a complete set of backup copies shall be readily available within no more than 24 hours. Back up procedures must be tested regularly.

(m) Procedures to Obtain and Verify Archive Information. During the compliance audit required by the rules in this Chapter, the auditor shall verify integrity of the archives. Either copy of the archive media determined corrupted or damaged in any way, shall be replaced with the backup copy held in the separate location and noted in the compliance audit report.

(n) Compromise and Disaster Recovery.

(1) Disaster Recovery Plan:

(A) The Certification Authority must have a disaster recovery/business resumption plan in place. The Certification Authority must set up and render operational a facility located in a geographic area not affected or disrupted by the disaster. The facility must provide Certification Authority Services in accordance with the Rules in this Chapter. The alternate facility must be operational within 24 hours of an unanticipated emergency.

Disaster recovery planning shall include a complete and periodic test of facility readiness. Such plan shall be identified and referenced within the Certification Practice Statement available to Qualified Relying Parties.

(B) The disaster recovery plan shall have been reviewed during Certification Authority initial and subsequent third party audits.

(2) Key Compromise Plan. The Certification Authority must have a key compromise plan in place. The plan must address procedures to be followed in the event the Certification Authority's private signing key used to issue certificates is compromised or in the event the private signing key of any Certification Authority higher in the chain of trust is compromised. Such plan shall include procedures for revoking all affected certificates and promptly notifying all subscribers and all Qualified Relying Parties.

(o) Certification Authority Termination. In the event that the Certification Authority ceases operation, the North Carolina Department of the Secretary of State Electronic Commerce Section, North Carolina Information Technology Services, all subscribers, sponsoring organizations, Registration Authorities, Certificate Manufacturing Authorities, Repository Service Providers, and Qualified Relying Parties shall be promptly notified of the termination. In addition, all Certification Authorities with which cross-certification authority agreements are current at the time of cessation must be promptly informed of the termination. All certificates issued by the Certification Authority referencing the rules in this Chapter shall be revoked no later than the time of termination.

History Note: *Authority G.S. 66-58.10;*
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;
Recodified to Rule .0701 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.

18 NCAC 10 .0306 PUBLIC KEY TECHNOLOGY: PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

(a) Physical Security -- Access Controls.

(1) The Certification Authorities, and all Registration Authorities, Certificate Manufacturing Authorities and Repository Services Providers, shall implement physical security controls to restrict access to hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing Certification Authority Services. Access to such hardware and software shall be limited to personnel performing in a Trusted Role as described in this Rule. Access shall be controlled through the use of electronic access controls, mechanical combination lock sets, or deadbolts. Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

(2) Breach of physical security or access control expectations may result in revocation of the Certification Authority's license.

(b) Procedural Controls.

(1) Trusted Roles. All employees, contractors, and consultants of a Certification Authority (collectively "personnel") having access to or control over cryptographic operations that may materially affect the Certification Authority's issuance, use, suspension, or revocation of certificates shall, for purposes of the rules in this Chapter, be considered as serving in a trusted role. This includes access to restricted operations of the Certificate Authority's repository. Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the Certification Authority's operations.

(2) Multiple Roles (Number of Persons Required Per Task). To ensure that one person acting alone cannot circumvent safeguards, multiple roles and individuals shall share Certification Authority server responsibilities. Each account on the Certification Authority server shall have limited capabilities commensurate with the role of the account holder.

(c) Personnel Security Controls.

(1) Background and Qualifications. Certification Authorities, Registration Authorities, Certificate Manufacturing Authorities and Repository Service Providers shall formulate and follow personnel and management policies sufficient to provide assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with the rules in this Chapter.

(2) Background Investigation.

(A) Certification Authorities shall conduct a background investigation of all personnel who serve in trusted roles (prior to their employment and at least every five years thereafter) to verify their trustworthiness and competence in accordance with the requirements of the rules in this Chapter and the Certification Authority's personnel Practice Statements or their equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.

(B) Operative personnel shall not ever have been convicted of a felony or a crime involving fraud, false statement or deception.

(C) Any civil or administrative findings involving fraud, false statement or deception involving operative personnel must be disclosed.

(3) Training Requirements. All Certification Authority, Registration Authority, Certificate Manufacturing Authority and Repository Services Provider personnel must receive training in order to perform their duties, and update briefings thereafter as necessary to remain current.

(4) Documentation Supplied to Personnel. All Certification Authority, Registration Authority, Certificate Manufacturing Authority, and Repository Services Provider personnel must receive comprehensive user manuals detailing the procedures for certificate creation, update, renewal, suspension, revocation, and software functionality.

History Note: *Authority G.S. 66-58.10;*
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.

18 NCAC 10 .0307 PUBLIC KEY TECHNOLOGY: TECHNICAL SECURITY CONTROLS

(a) Key Pair Generation and Installation.

(1) Key Pair Generation. Key pairs for Certification Authorities, Registration Authorities, Certificate Manufacturing Authorities, Repository Services Providers, and subscribers must be generated in such a way that the private key is not known by other than the authorized user of the key pair. Acceptable methods include:

(A) Having all users (Certification Authorities, Certificate Manufacturing Authorities, Registration Authorities, Repository Services Providers and subscribers) generate their own keys on a trustworthy system, and not reveal the private keys to anyone else; or

(B) Having keys generated in hardware tokens from which the private key cannot be extracted.

(2) Certification Authority, Registration Authority, and Certificate Manufacturing Authority keys must be generated in hardware tokens. Key pairs for Repository Services Providers, and end-entities may be generated in either hardware or software as detailed in the Certification Practice Statement.

(b) Private Key Delivery to Entity. The private (secret) key shall be delivered to the subscriber in an "out of band" transaction. The secret key may delivered to the subscriber in a tamper-proof hardware or software container. The secret key may be delivered to the subscriber embedded in a hardware token protected by encryption and password protected.

(c) Subscriber Public Key Delivery to Certification Authority. The subscriber's public key must be transferred to the Registration Authority or Certification Authority in a way that ensures:

(1) it has not been changed during transit;

(2) the sender possesses the private key that corresponds to the transferred public key; and

(3) the sender of the public key is the legitimate user claimed in the certificate application.

(d) Certification Authority Public Key Delivery to Users. The public key of the Certification Authority signing key pair may be delivered to subscribers in an on-line transaction in accordance with Internet Engineering Task Force Public Key Infrastructure Part 3, or by another mechanism which assures the Certification Authority public key is delivered in a manner that assures the key originates with the Certification Authority and that assures the Certification Authority public key has not been altered in transit.

(e) Key Sizes – Asymmetric Cryptographic Applications.

(1) Minimum key length for other than elliptic curve based algorithms is 1024 bits;

(2) Minimum key length for elliptic curve group algorithms is 170 bits.

(f) Acceptable algorithms for public key cryptography applications include, but are not limited to:

(1) RSA (Rivest, Shamir, Adelman) -- digital signature and information security;

(2) ElGamal -- digital signature and information security;

(3) Diffie – Hellman -- digital signature and information security; and

(4) DSA /DSS (Digital Signature Algorithm) -- digital signature applications.

(g) Certification Authority Private Key Protection. The Certification Authority (and the Registration Authority, Certificate Manufacturing Authority and Repository Services Provider) shall each protect its private key(s) in accordance with the provisions of the rules in this Chapter.

(1) Standards for Cryptographic Module. Certification Authority signing key generation, storage and signing operations shall be on a hardware crypto module rated at Federal Information Processing Standards 140-1 Level 2 (or higher). Subscribers shall use Federal Information Processing Standards 140-1 Level 1 approved cryptographic modules (or higher) and related pertinent cryptographic module security requirements of the Common Criteria – ISO 15408-1 "Evaluation Criteria".

(2) Private Key Escrow:

(A) Certification Authority signing private keys shall not be escrowed;

(B) Keys used solely for encryption purposes within and by employees of the State of North Carolina shall be escrowed, unless otherwise provided by law.

(3) Private Key Backup. An entity may back up its own private key.

(4) Private Key Archival. An entity may archive its own private key.

(5) Other Aspects of Key Pair Management. Key Replacement. Certification Authority key pairs must be replaced at least every three years. Registration Authority and subscriber key pairs must be replaced not less than every two years and a new certificate issued.

(6) Restrictions on Certification Authority's Private Key Use.

(A) The Certification Authority's signing key used for issuing certificates conforming to the Rules in this Chapter shall be used only for signing certificates and, optionally, Certificate Revocation Lists.

(B) A private key used by a Registration Authority or Repository Services Provider for purposes associated with its Registration or Repository Services Provider function shall not be used for any other purpose without the express written permission of the Certification Authority.

(C) A private key held by a Certificate Manufacturing Authority and used for purposes of manufacturing certificates for the Certification Authority:

(i) is considered the Certification Authority's signing key;

(ii) is held by the Certificate Manufacturing Authority as a fiduciary for the Certification Authority; and

(iii) shall not be used for any reason without the express written permission of the Certification Authority.

(D) Any other private key used by a Certificate Manufacturing Authority for purposes associated with its Certificate Manufacturing Authority function shall not be used for any other purpose without the express written permission of the Certification Authority.

(h) Computer Security Controls. All Certification Authority servers must include the functionality satisfying Federal Information Processing Standards 140-1 Level 2 (or higher) and pertinent cryptographic module security requirements of the Common Criteria – ISO 15408-1 "Evaluation Criteria" for IT Security either through the operating system, or combination of operating system, public key infrastructure application, and physical safeguards.

(i) Life Cycle Technical Controls - System Development Controls. System design and development shall be conducted using an industrial standard methodology, e.g. systems development life cycle approach (SDLC).

History Note: *Authority G.S. 66-58.10;*
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.

18 NCAC 10 .0308 PUBLIC KEY TECHNOLOGY: CERTIFICATE AND CERTIFICATE REVOCATION LIST PROFILES

(a) Certificate Profile:

(1) Certificates referencing the Rules in this Chapter shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages, i.e. public keys used for digital signature verification;

(2) All certificates referencing the Rules in this Chapter shall be issued in the X.509 version 3 format and shall include a reference to the Object Identifier for the rules in this Chapter, when assigned, within the appropriate field. The Certification Practice Statement shall identify the certificate extensions supported, and the level of support for those extensions.

(b) Certificate Revocation List Profile. If utilized, Certificate Revocation Lists shall be issued in the X.509 version 2 format. The Certificate Practice Statement shall identify the Certificate Revocation List extensions supported and the level of support for these extensions.

History Note: *Authority G.S. 66-58.10;*
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.

18 NCAC 10 .0309 PUBLIC KEY TECHNOLOGY: RULE ADMINISTRATION

(a) List of Items. Notice of all proposed changes to the Rules in this Chapter under consideration by the Department of the Secretary of State, that may affect users of the Rules (other than editorial or typographical corrections, or changes to the contact details) shall be provided to licensed Certification Authorities. Notice shall be posted on the World Wide Web site of the North Carolina Department of the Secretary of State. Authorized Certification Authorities shall post notice of such proposed changes in their repositories and shall advise their subscribers, in writing or by e-mail, of such proposed changes.

(b) Publication and Notification Procedures:

(1) A copy of the rules in this Chapter is available in electronic form on the Internet at www.secretary.state.nc.us/ecomm/;

(2) Authorized Certification Authorities shall post copies of the rules in this Chapter in their repositories.

History Note: *Authority G.S. 66-58.10;*
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.

SECTION .0400 - BIOMETRICS (RESERVED)

Editor's Note: Temporary Rules .0401 and .0402 effective February 23, 1999 were recodified as Rules .0801 and .0802.

SECTION .0500 - SIGNATURE DYNAMICS (RESERVED)

Editor's Note: Temporary Rule .0501 effective February 13, 1999 was recodified as Rule .0901.

SECTION .0600 - RESERVED FOR FUTURE CODIFICATION

SECTION .0700 – ALTERNATE TECHNOLOGIES

18 NCAC 10 .0701 ALTERNATE TECHNOLOGIES AND PROVISIONAL LICENSING

Alternate Technologies: Any person may petition the Electronic Commerce Section to initiate rulemaking to recognize a technology not currently recognized under the rles in this Chapter. The petition shall be made pursuant to G.S. 150B-20. G.S. 150B-20 and other statutes may be viewed at the North Carolina General Assembly's Internet site at http://www.ncga.state.nc.us/. In addition to the requirements of G.S. 150B-20, in order to enable the Electronic Commerce Section to best consider the petition, the petitioner shall also provide a detailed explanation of the proposed technology, and a discussion of how the technology complies with the substantive intent of the Electronic Commerce Act.

History Note: *Authority G.S. 66-58.10;*
Temporary Adoption Eff. February 23, 1999;
Codifier determined on November 23, 1999, agency findings did not meet criteria for temporary rule;
Recodified from 18 NCAC 10 .0305 Eff. December 3, 1999;
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.

SECTION .0800 – SANCTIONS AND ENFORCEMENT

18 NCAC 10 .0801 CIVIL SANCTIONS

(a) If, upon investigation, the Electronic Commerce Section finds that a Certification Authority has violated any provision of the Electronic Commerce Act or the rules in this Chapter, or finds that the Certification Authority has had a license revoked or suspended in any other jurisdiction, the Electronic Commerce Section may revoke or suspend any license issued under the Electronic Commerce Act and the rules in this Chapter. The revocation or suspension may be in addition to any civil monetary penalty issued against the Certification Authority. As a condition of license reinstatement following a period of suspension, the Electronic Commerce Section may require that the Certification Authority submit updated or additional documentation or assurances regarding its operations.
(b) If, upon investigation, the Electronic Commerce Section finds that a Certification Authority has violated any provision of the Electronic Commerce Act or the rules in this Chapter, the Electronic Commerce Section may assess a civil monetary penalty of not more than five thousand dollars ($5,000 US) for each violation. The civil monetary penalty may be in addition to any revocation or suspension of the Certification Authority's license. As a condition of continued licensure following assessment of a civil monetary penalty, the Electronic Commerce Section may require that the Certification Authority submit updated or additional documentation or assurances regarding its operations.
(c) Adjustment factors. In determining the length of any suspension or amount of any civil monetary penalty, the Electronic Commerce Section shall consider:

(1) The organizational size of the Certification Authority cited for violating the provisions of the Electronic Commerce Act;
(2) The good faith of the Certification Authority cited, including but not limited to any procedures or processes implemented by the violator to prevent the violation from recurring;
(3) The gravity of the violation;

(4) The prior record of the violator in complying or failing to comply with the Electronic Commerce Act or the rules in this Chapter; and

(5) The risk of harm cause by the violation.

(d) Continuing Violations. After the receipt of notice of a violation, if any Certification Authority willfully continues to violate by action or inaction the Electronic Commerce Act or the rules in this Chapter, each day or transaction the violation continues or is repeated may be considered a separate violation.

(e) Civil Sanction Notification. When the Electronic Commerce Section determines that a civil sanction shall be assessed, the Electronic Commerce Section shall notify the Certification Authority of the following information by electronic mail, if possible, and by any means permitted under Rule 4 of the North Carolina Rules of Civil Procedure:

(1) The nature of the violation;

(2) The proposed civil sanction;

(3) That the proposed civil sanction will become final unless within 60 days after receiving notice of the proposed sanction the Certification Authority either:

(A) takes exception to the proposed sanction by filing a contested case petition with the Office of Administrative Hearings; or

(B) submits a written request for the reduction of the proposed sanction; and

(4) The procedure for taking exception to the violation or seeking the reduction of the proposed sanction.

(f) Civil Sanction Finality. The Certification Authority must file a contested case petition pursuant to G.S. 150B-23 or submit a written request for the reduction of the proposed sanction within 60 days of receipt of the notice of the proposed civil sanction or the proposed sanction shall become the sanction imposed. Notice shall be deemed received at the time of service by any method permitted under Rule 4 of the North Carolina Rules of Civil Procedure.

(g) Request for Reduction of Proposed Civil Sanction. A Certification Authority that admits a cited violation but wishes to seek reduction of the length of a proposed suspension or the amount of a proposed civil monetary penalty may request reduction of the proposed civil sanction.

(1) Any request for reduction of a proposed civil sanction shall be submitted to the Electronic Commerce Section in writing and must include a written statement supporting the reduction request. Requests for reduction of a proposed sanction are solely for the purpose of allowing the Certification Authority to contest the reasonableness of the proposed civil sanction arising under this Rule. The Certification Authority shall not attempt to contest the existence of a violation or raise questions of law in the request for reduction of the proposed sanction.

(2) The Electronic Commerce Section shall determine if the proposed sanction is to be reduced pursuant to a reduction request and shall notify the Certification Authority of its decision in writing.

(3) If the Electronic Commerce Section determines that the reduction request raises issues of fact or questions of law, the Electronic Commerce Section may decline to consider the reduction request, and shall notify the Certification Authority by certified or registered mail that it must file a contested case petition with the Office of Administrative Hearings in order to preserve its claim and legal rights. The Certification Authority must file a contested case petition with the Office of Administrative Hearings within 60 days of receipt of notice or the sanction assessed shall be final.

(4) If the reduction request does not raise issues of fact or questions of law, the Electronic Commerce Section shall determine if the proposed sanction is to be reduced, and shall notify the Certification Authority of its decision in writing by electronic mail, if possible, and by any other means permitted under Rule 4 of the North Carolina Rules of Civil Procedure. In the event the Electronic Commerce Section denies the reduction request, or grants the reduction request in an amount unacceptable to the Certification Authority, the Certification Authority must file a contested case petition with the Office of Administrative Hearings within 60 days of receipt of notice of the Electronic Commerce Section's decision, or the decision shall become the final decision. Notice shall be deemed received at the time of service by any method permitted under Rule 4 of the North Carolina Rules of Civil Procedure.

(h) Payment. Any civil monetary penalty shall be due within 60 days of the date of the initial assessment of the penalty, except that if the Certification Authority files a contested case petition pursuant to G.S. 150B-23 or submits a written request for reduction of the penalty, the penalty shall be due within 60 days of the date of the final decision. The penalty shall be paid with cash or certified funds by personal delivery or certified mail to the

Electronic Commerce Section. In the event the Certification Authority fails to pay the penalty assessed within the time periods set forth in this Rule, the Electronic Commerce Section may collect the amount of the penalty from the bond required by the rules in this Chapter.

History Note: *Authority G.S. 66-58.6; 66-58.10;*
Temporary Adoption Eff. February 23, 1999;
Codifier determined on November 23, 1999, agency findings did not meet criteria for temporary rule;
Recodified from 18 NCAC 10 .0401 Eff December 3, 1999;
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.

18 NCAC 10 .0802 CRIMINAL PENALTIES AND INJUNCTIVE RELIEF

History Note: *Authority G.S. 66-58.6; 66-58.8; 66-58.10;*
Temporary Adoption Eff. February 23, 1999;
Recodified from Rule .0402;
Codifier determined on November 23, 1999 that agency findings did not meet criteria for temporary rule;
Temporary Adoption Eff. December 3, 1999;
RRC Objection May 18, 2000 due to lack of necessity;
RRC returned rule to agency on July 20, 2000;
Temporary Adoption Expired on July 20, 2000.

SECTION .0900 - RECIPROCITY

18 NCAC 10 .0901 RECIPROCAL AGREEMENTS AND LICENSURE BY RECIPROCITY

(a) Certification Authorities licensed by other jurisdictions may request North Carolina licensure by the North Carolina Electronic Commerce Section. The applicant must be currently licensed in good standing with another jurisdiction.

(b) To seek reciprocal licensure in North Carolina, Certification Authorities licensed by other jurisdictions shall do the following:

(1) Pay the licensing fee as described in the Rules in this Chapter and comply with 18 NCAC 10 .0301(a), (c), (d), (e), (f), (g) and (h);

(2) Provide the Electronic Commerce Section with evidence of licensure in good standing from the other licensing jurisdiction;

(3) Provide the Electronic Commerce Section with a complete copy of the licensing application that led to the Certification Authority becoming licensed in the other jurisdiction, including any amendments thereto;

(4) Provide full disclosure of any former, current or proposed disciplinary action or criminal proceeding arising from or related to the Certification Authority's license or activities as a Certification Authority;

(5) Provide a complete history of licensure in all other jurisdictions, whether continuous or disrupted, and if disrupted the length of the disruption and basis therefore; and

(6) Provide any additional information necessary to substantiate compliance with the audit requirements identified in 18 NCAC 10 .0303(k), as may be required by the Electronic Commerce Section.

(c) The Electronic Commerce Section may impose civil sanctions against a reciprocal licensee on the same basis that the Electronic Commerce Section can impose civil sanction against a Certification Authority license otherwise issued, or upon finding that the Certification Authority has had a license revoked or suspended in another jurisdiction.

(d) Any Certification Authority that obtains a reciprocal license under the Rules in this Chapter shall inform the Electronic Commerce Section in writing of any civil or criminal proceeding that arises from or relates to the

Certification Authority's license or any disciplinary action commenced against the Certification Authority in any other jurisdiction within ten days of notice of the proceeding or action.

History Note: *Authority G.S. 66-58.3; 66-58.6; 66-58.7; 66-58.8; 66-58.10; 66-58.11;*
Temporary Adoption Eff. February 23, 1999;
Codifier determined on November 23, 1999, agency findings did not meet criteria for temporary rule;
Recodified from 18 NCAC 10 .0501 Eff. December 3, 1999;
Temporary Adoption Eff. December 3, 1999;
Eff. March 26, 2001;
Amended Eff. April 1, 2001;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. December 6, 2016.