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.