**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.*