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.