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.