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.