ARTICLE 3. DIGITAL SIGNATURES

Rule 1. Definitions

20 IAC 3-1-1 Applicability
Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 1. The definitions in this rule apply throughout this article. *(State Board of Accounts; 20 IAC 3-1-1; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3638; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-1-2 "Approved list of certification authorities" defined
Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 2. "Approved list of certification authorities" means the list of approved certification authorities maintained by the state board of accounts using the criteria in 20 IAC 3-2-4. *(State Board of Accounts; 20 IAC 3-1-2; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3638; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-1-3 "Certificate" defined
Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 3. "Certificate" means a computer-based record that:
(1) identifies the certification authority issuing it;
(2) names or identifies its subscriber;
(3) contains the subscriber's public key;
(4) identifies its operational period;
(5) is digitally signed by the certification authority issuing it; and
(6) at a minimum, conforms to International Telecommunication Union X.509 version 3 standards.
(State Board of Accounts; 20 IAC 3-1-3; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3638; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.

20 IAC 3-1-4 "Certification authority" defined
Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 4. "Certification authority" means a trusted third party who generates and issues digital certificates to a person after investigation of the identity of the person and thereby permits others to have a legally enforceable means of assuring the identity of the person by determining that the private key resulting from that person's certificate was used to digitally sign the message. *(State Board of Accounts; 20 IAC 3-1-4; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3638; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-1-5 "Certification practice statement" defined
Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 5. "Certification practice statement" means the documentation of the practices, procedures, and controls employed by a certification authority. *(State Board of Accounts; 20 IAC 3-1-5; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3638; readopted filed Nov 21,*

2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.

20 IAC 3-1-6 "Digital signature" defined

Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 6. "Digital signature" means an electronic signature that transforms a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether:

(1) the transformation was created using the private key that corresponds to the signer's public key; and

(2) the initial message has not been altered since the transformation was made.

(State Board of Accounts; 20 IAC 3-1-6; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3638; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.

20 IAC 3-1-7 "Intelenet system" defined

Authority: IC 5-24-3-4
Affected: IC 5-21; IC 5-24

Sec. 7. "Intelenet system" means the integrated telecommunication networks and information technology services designed, developed, and managed under IC 5-21. *(State Board of Accounts; 20 IAC 3-1-7; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3638; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-1-8 "Message" defined

Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 8. "Message" means a digital representation of information intended to serve as a written communication with the state. *(State Board of Accounts; 20 IAC 3-1-8; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3638; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-1-9 "Person" defined

Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 9. "Person" means:

(1) an individual;

(2) a corporation;

(3) a partnership;

(4) an association;

(5) a limited liability company; or

(6) other legal entity.

(State Board of Accounts; 20 IAC 3-1-9; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3638; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.

20 IAC 3-1-10 "Private key" defined

Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 10. "Private key" means the key of a key pair used to create a digital signature. *(State Board of Accounts; 20 IAC 3-1-10; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3639; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-1-11 "Public key" defined
Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 11. "Public key" means the key of a key pair used to verify a digital signature. *(State Board of Accounts; 20 IAC 3-1-11; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3639; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-1-12 "Signer" defined
Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 12. "Signer" means the person who digitally signed a message with the use of acceptable digital signature technology to uniquely link the message with the person sending it. *(State Board of Accounts; 20 IAC 3-1-12; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3639; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-1-13 "State" defined
Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 13. "State" means the state of Indiana and includes a state agency. *(State Board of Accounts; 20 IAC 3-1-13; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3639; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-1-14 "State agency" defined
Authority: IC 5-24-3-4
Affected: IC 4-13-1-1; IC 5-24

Sec. 14. "State agency" has the meaning set forth in IC 4-13-1-1. *(State Board of Accounts; 20 IAC 3-1-14; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3639; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-1-15 "Technology" defined
Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 15. "Technology" means the computer hardware and/or software-based method or process used to create digital signatures. *(State Board of Accounts; 20 IAC 3-1-15; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3639; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

Rule 2. General Provisions

20 IAC 3-2-1 Acceptable use of digital signatures
Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 1. (a) A digital signature is valid when:
(1) created by acceptable digital signature technology;
(2) successfully transmitted through the Intelenet system; and
(3) used with the state or a state agency except:
(A) the judicial branch;
(B) the legislative branch;
(C) a state educational institution (as defined in IC 20-12-0.5-1 *[IC 20-12 was repealed by P.L.2-2007, SECTION 390, effective July 1, 2007.]*); and
(D) offices of:
(i) the secretary of state;
(ii) the auditor;
(iii) the treasurer;
(iv) the attorney general;
(v) the superintendent of public instruction; and
(vi) the clerk of the supreme court.

(b) Each entity excluded by subsection (a)(3) may elect to be subject to this article if the supervising body records its written consent with the state board of accounts. *(State Board of Accounts; 20 IAC 3-2-1; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3639; errata filed Sep 23, 1998, 10:31 a.m.: 22 IR 462; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-2-2 Criteria for acceptable digital signature technology

Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 2. A digital signature on a message received by or filed with the state shall be effective if the digital signature technology used to create the digital signature enables it to meet the following criteria:
(1) It is unique to the person using it, including the following:
(A) The private key used to create the signature on the message is only required to be known by the signer.
(B) The digital signature is created when the signer runs a message through a one-way function, creating a message digest, then encrypting the resulting message digest using an asymmetrical cryptosystem and the signer's private key.
(C) The signer has been issued a certificate by a certification authority on the approved list of certification authorities to certify that he or she controls the private key used to create the signature.
(D) It is computationally infeasible to derive the private key from knowledge of the public key.
(2) It is capable of verification. The acceptor of the digitally signed message can verify:
(A) by using the signer's public key, that the message was digitally signed by using the signer's private key;
(B) that the certificate was valid at the time of the transaction; and
(C) either through a certification practice statement or through the content of the certificate itself, the proof of identification the certification authority required of the signer prior to issuing the certificate.
(3) It is under the sole control of the person using it. The person who holds the private key, as identified in the certificate, assumes a duty to retain control of the private key and prevent its disclosure to any person not authorized to create the subscriber's digital signature.
(4) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.

(State Board of Accounts; 20 IAC 3-2-2; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3639; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.

20 IAC 3-2-3 Acceptable digital signature technology

Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 3. The technology known as public key cryptography is the acceptable digital signature technology for use by persons

dealing with the state through the Intelenet system provided that the digital signature is created consistent with the provisions in section 2 of this rule. *(State Board of Accounts; 20 IAC 3-2-3; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3640; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-2-4 Digital signature certification authorities

Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 4. (a) The state board of accounts shall maintain an approved list of certification authorities authorized to issue certificates for digitally signed communication with the state and shall make the list available to persons wishing to deal electronically with the state.

(b) The Intelenet system shall only accept certificates from certification authorities that appear on the approved list of certification authorities.

(c) The state board of accounts shall place a certification authority on the approved list of certification authorities after the certification authority provides the state board of accounts with either of the following:

(1) A copy of an unqualified performance audit performed in accordance with standards set in the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards No. 70 (SAS 70) to ensure that the certification authority's practices and policies are consistent with the requirements of the certification authority's certification practice statement and section 2 of this rule. A certification authority that has been in operation for:

(A) one (1) year or less shall undergo an SAS 70 Type One audit, A Report of Policies and Procedures Placed in Operation, receiving an unqualified opinion; or

(B) longer than one (1) year shall undergo an SAS 70 Type Two audit, A Report of Policies and Procedures Placed in Operation and Test of Operating Effectiveness, receiving an unqualified opinion.

(2) Proof of accreditation by an accreditation body, acceptable to the state board of accounts whose requirements for accreditation are consistent with section 2 of this rule.

(d) To remain on the approved list of certification authorities, a certification authority shall annually provide to the state board of accounts proof of compliance with the following:

(1) A new audit of the type described in subsection (c)(1)(A) or a new or renewed accreditation of the type described in subsection (c)(1)(B).

(2) The bond requirements described in subsection (f).

(e) A certification authority may be removed from the approved list of certification authorities if:

(1) the certification authority fails to provide current proof of accreditation to the state board of accounts annually;

(2) the certification authority fails to receive an annual unqualified SAS 70 performance audit;

(3) the state board of accounts is informed that a certification authority has had its accreditation revoked by an accreditation body that meets the criteria of subsection (c)(2); or

(4) the certification authority fails to meet the requirements in subsection (f).

(f) The certification authority shall furnish the state board of accounts annually with proof of a fidelity and surety bond underwritten by an insurer approved by the state, maintained currently in force, in an amount not less than fifty thousand dollars ($50,000) per year.

(g) The certification authority shall be registered to do business in the state. *(State Board of Accounts; 20 IAC 3-2-4; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3640; errata filed Sep 23, 1998, 10:31 a.m.: 22 IR 462; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-2-5 Retention of certificates

Authority: IC 5-24-3-4
Affected: IC 5-24

Sec. 5. All digitally signed messages received by the state in accordance with this rule, as well as any information resources necessary to permit access to the message and to verify the digital signature, shall be retained by the state as necessary to comply

with applicable law pertaining to records retention requirements for that message as established by the commission on public records. *(State Board of Accounts; 20 IAC 3-2-5; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3640; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-2-6 Digital signature repudiation

Authority: IC 5-24 3-4
Affected: IC 5-24

Sec. 6. It is the responsibility of the rightful holder of the private key to maintain the private key's security. Repudiation of a digitally signed and transmitted message may only occur by the determination of a court of competent jurisdiction that the private key of the rightful holder was compromised through no fault of the rightful holder and without knowledge on the part of the rightful holder. It is the legal prerequisite for a claim of repudiation that the repudiator have filed a notice of revocation with the certification authority prior to making the claim of repudiation. *(State Board of Accounts; 20 IAC 3-2-6; filed Jun 1, 1998, 3:33 p.m.: 21 IR 3641; readopted filed Nov 21, 2005, 9:15 a.m.: 29 IR 1381; readopted filed Nov 22, 2011, 2:19 p.m.: 20111221-IR-020110584RFA) NOTE: Expiration postponed by Executive Order #04-31, December 29, 2004.*

20 IAC 3-2-7 Electronic submission of information

Authority: IC 5-24-3-4
Affected: IC 5-24; IC 13-14-13-2

Sec. 7. Electronic submission of information that meets the requirements of 40 CFR 3 shall be deemed to satisfy the standards referred to in IC 13-14-13-2(1). *(State Board of Accounts; 20 IAC 3-2-7; filed Mar 27, 2009, 9:56 a.m.: 20090422-IR-020080898FRA)*

*