IMT Standards **IMT Standards Oversight Committee** **Government of Alberta**	**Effective Date: 2010-09-30** **Scheduled Review 2018-02-01** **Last Reviewed: 2017-02-01**
	Type: Technical
Standard number – A000014	
Electronic Signature Metadata	
Category: IM **Keywords: Records Management, Electronic Signature, Secured Electronic Signature, Electronic Signature Specifications, Digital Signature Certificate Requirements, Certification Authority Requirements, Metadata Property Requirements**	

Description of Standard

This standard describes the electronic signature process requirements, the specifications and the metadata requirements that ministries must implement to support the creation of authentic, reliable and trustworthy electronic records that have an electronic signature attachment or association.

Standard Specification

Terms

"Asymmetric Cryptography" [1]means a cryptographic system that relies on key pairs.

"Certification Authority" [1] means a person or entity that issues digital signature certificates and has been approved by the CISO.

"Digital Signature Certificate" [1] in respect of a person, means an electronic record that

(a) identifies the certification authority that issued it and is digitally signed by that certification authority;

[1] Adopted from Secure Electronic Signature Regulations P.C. 2005 – 57 February 1, 2005, Section 1.

(b) identifies, or can be used to identify, the person; and,
(c) contains the person's public key.

"Electronic Signature" or "Basic Electronic Signature" is electronic information that a person creates or adopts in order to sign a record and that is in, attached to, or associated with, the record.

"Hash Function"[1] means an electronic one-way mathematical process that converts data contained in an electronic record into a message digest that is unique to the data in a way that, were that data changed, it would, on conversion, result in a change message digest.

"Key Pair"[1] means a pair of keys held by or for a person that includes a private key and a public key that are mathematically related to, but different from, each other.

"Private Key"[1] means a string of data that

(a) is used in asymmetric cryptography to encrypt data contained in an electronic record; and
(b) is unique to the person who is identified in, or can be identified through, a digital signature certificate and corresponds only to the public key in that certificate.

"Public Key"[1] means a string of data contained in a digital signature certificate that

(a) is used in asymmetric cryptography to decrypt data contained in an electronic record that was encrypted through the application of the private key in the key pair; and
(b) corresponds only to the private key in the key pair.

"Secure Electronic Signature" is an electronic signature for which it can be proved that:

- the electronic signature resulting from the use by a person of the technology or process to create the signature is unique to the person;
- the use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to a digital record is under the sole control of the person;
- the technology or process can be used to identify the person using the technology or process; and

- the electronic signature can be linked with a digital record in such a way that it can be used to determine whether the digital record has been changed since the electronic signature was incorporated in, attached to, or associated with, the digital record.

Signature Requirements

	Type	**Requirements**	**Specifications**
1	Electronic Signature	• Serves as a method to identify and authenticate data.[2] ○ The person that sent the text has practical use (key holder) of the electronic signature; however, may not be the entity (key owner) that has explicit right to use the electronic signature.	(a) Must validate the data. (b) Not a method or technology for entity (key owner) verification.

[2] Report From the Commission To The European Parliament and the Council, Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, Section 2.3.2.

	Type	Requirements[3]	Specifications[4]
2	Secured Electronic Signature	• The electronic signature resulting from the use by a person of the technology or process is unique to the person; • The use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to an electronic record is under the sole control of the person; • The technology or process can be used to identify the person using the technology or process; and, • The electronic signature can be linked with an electronic record in such a way that it can be used to determine whether the electronic record has been changed since the electronic signature was incorporated in,	(a) Application of the hash function to the data to generate a message digest; (b) Application of a private key to encrypt the message digest; (c) Incorporation in, attachment to, or association with the electronic record of the encrypted message digest; (d) Transmission of the electronic record and encrypted message digest together with either (i) a digital signature certificate, or (ii) a means of access to a digital certificate; and (e) After receipt of the electronic record, the encrypted message digest and the digital signature certificate or the means of access to the digital signature certificate, (i) application

[3] Adopted from the *Personal Information Protection and Electronic Documents Act* (2000, c.5) in paragraphs 48(2)(a) to (d).

[4] Adopted from Secure Electronic Signature Regulations P.C. 2005 – 57 February 1, 2005, Section 2.

	Type	Requirements[3]	Specifications[4]
		attached to or associated with the electronic record.	of the public key contained in the digital signature certificate to decrypt the encrypted message digest and produce the message digest referred to in paragraph (a), (ii) application of the hash function to the data contained in the electronic record to generate a new message digest, (iii) verification that, on comparison, the message digests referred to in paragraph (a) and subparagraph (ii) are identical, and (iv) verification that the digital signature certificate is valid in accordance with the Digital Signature Certificate Requirements.

Digital Signature Certificate Requirements[5]

The digital signature certificate is valid if, at the time when the data contained in an electronic record is digitally signed in accordance with the Secured Electronic Signature specification and the certificate is:

[5] Adopted from Secure Electronic Signature Regulations, P.C. 2005 – 57 February 1, 2005. Section 3(1) (a) to (b) and 3(2).

a) readable or perceivable by any person or entity who is entitled to have access to the digital signature certificate;
(b) has not expired or been revoked; and
(c) when the digital signature certificate is supported by other digital signature certificates, in order for the digital signature certificate to be valid, the supporting certificates must also be valid.

Certification Authority Requirements

To recognize a person or entity as a certification authority, the CISO must verify that the person or entity has the capacity to issue digital signature certificate in a secure and reliable manner within the context of Requirements for Secured Electronic Signatures.

Metadata Requirements

Metadata describes business objects or resources and are stored within the trusted digital repository for at least as long as the records to which they relate are retained.

	Signature Type	**Metadata Elements**
1	Electronic Signature	• signature • signer • date signed
2	Secured Electronic Signature	• signature • signer • date signed • algorithm identifier • algorithm parameters • date signature verified • validated by • validated token • certificate issuer • certification service provider • counter signature • electronic certificate • electronic certificate serial number • encryption algorithm

		• encryption level

Where to Apply This Standard

This standard applies to all Government of Alberta departments, boards, agencies and commissions.

Authority and Exceptions

- Verify individual Ministry Acts to determine any specific exclusion.
- This standard does not apply to[6]:
  - records that are prescribed, or that belong to a class that is prescribed, as records or a class of records to which this standard does not apply;
  - wills, codicils and trusts created by wills or codicils;
  - enduring power of attorney under the Powers of Attorney Act;
  - personal directives under the Personal Directives Act;
  - records that create or transfer interest in land, including interest in mines and minerals;
  - documents of title;
  - guarantees under the Guarantees Acknowledgment Act; and,
  - negotiable instruments.

Supporting Documentation

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures
- *Electronic Transactions Act,* S.A. 2001, c. E-5.5
- MoReq2 Model Requirements For The Management of Electronic Records, Update and Extension, 2008, Appendix 9 To The MoReq2 Specification: Metadata Model
- *Personal Information Protection and Electronic Documents Act* S.C., 2000, c.5

[6] Adopted from *Electronic Transactions Act*, S.A. 2001, c. E-5.5, Section 7(1) and (2).

- Report From the Commission To The European Parliament and The Council, Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures.
- Secure Electronic Signature Regulations P.C. 2005 – 57 February 1, 2005

Owner

Service Alberta, Information Management Branch
SA.InformationManagement@gov.ab.ca

Contact

GoA IMT Standards at imt.standards@gov.ab.ca

Additional Information

Audience	GOA
Source	Service Alberta, Information Management and Logistics
Sensitivity	Unrestricted
Proposed Date	2009-12-23
Proposed By	Service Alberta, Information Management and Logistics – Barbara Seeley, Manager ECM Program Development and Innovation 780-427-3947

Appendix A

Metadata

Legend

- **Name of Term:** a name for the metadata property.
- **Definition:** a short description of the metadata property.
- **Purpose:** the reason for which something exists or is done.
- **Applies To:** to which series, folder, folder part, or record the property applies to.
- **Obligation:** whether value for property is mandatory or optional for compliance.
- **Repeatable:** whether more than one value is allowed for the property**.**
- **Populated:** how the values for this element are produced.
- **Guidance:** conditions and rules that govern the use and value(s) of the property.

signature	
Metadata Property	
Name of Term:	signature
Definition:	The electronic signature itself
Purpose:	Contains the electronic signature used to determine authenticity.
Applies To:	Record
Obligation:	Mandatory
Repeatable:	No
Populated:	System generated
Guidance:	• Electronic Signature • Secured Electronic Signature • Can not be modified
signer	

Metadata Property	
Name of Term:	signer
Definition:	This is a textual description identifying the entity that signed the object.
Purpose:	To describe the signer for display purposes when showing the record.
Applies To:	Record
Obligation:	Optional
Repeatable:	No
Populated:	System generated
Guidance:	• Electronic Signature • Secured Electronic Signature • Element is not protected from modification by an electronic signature and its value cannot be trusted to remain unchanged.

date signed	
Metadata Property	
Name of Term:	date signed
Definition:	Date and time the signature was applied.
Purpose:	To provide indication of when the record was signed.
Applies To:	Record
Obligation:	Optional
Repeatable:	No
Populated:	System generated
Guidance:	• Electronic Signature • Secured Electronic Signature

	• The time should be specified at least to the minute. • This value is not protected from modification by the electronic signature and its value consequently can not be trusted to remain unchanged.

algorithm identifier	
Metadata Property	
Name of Term:	algorithm identifier
Definition:	Identifies the cryptographic algorithm used to generate the signature.
Purpose:	Necessary to verify the electronic signature
Applies To:	Record
Obligation:	Mandatory
Repeatable:	No
Populated:	System generated
Guidance:	• Secured Electronic Signature • System generated • The value of this element indicates the combination of electronic signature algorithm and hashing algorithm used to generate the electronic signature.

algorithm parameters
Metadata Property

Name of Term:	algorithm parameters
Definition:	This element contains any parameters required by the electronic signature algorithm.
Purpose:	Additional information to verify the electronic signature.
Applies To:	Record
Obligation:	Optional
Repeatable:	No
Populated:	System generated
Guidance:	• Secured Electronic Signature

date signature verified	
Metadata Property	
Name of Term:	date signature verified
Definition:	The date and time the electronic signature was verified.
Purpose:	To determine when the electronic signature was verified.
Applies To:	Record
Obligation:	Mandatory
Repeatable:	Yes
Populated:	System generated
Guidance:	• Secured Electronic Signature • Can not be modified

validated by

Metadata Property	
Name of Term:	validated by
Definition:	System identifier of an agent who has initiated the validation of an electronic signature or certificate.
Purpose:	To determine which agent validated the electronic signature or certificate.
Applies To:	Record
Obligation:	Mandatory
Repeatable:	No
Populated:	System generated or manual entry
Guidance:	• Secured Electronic Signature • Mandatory if checking a certificate • Not mandatory if checking an electronic signature. • Null if the check is initiated automatically by the system. • Can not be modified.

validated token	
Metadata Property	
Name of Term:	validated token
Definition:	A validation ticket or token issued by a certification service provider.
Purpose:	To identify the electronic signature
Applies To:	Record
Obligation:	Optional
Repeatable:	No
Populated:	System generated or manual entry

Guidance:	• Secured Electronic Signature • Can not be modified

certificate issuer	
Metadata Property	
Name of Term:	certificate issuer
Definition:	The issuer of an electronic certificate
Purpose:	To determine the issuer of an electronic certificate
Applies To:	Record
Obligation:	Mandatory
Repeatable:	No
Populated:	System generated
Guidance:	• Secured Electronic Signature • Can not be modified

certificate service provider	
Metadata Property	
Name of Term:	certification service provider
Definition:	The certification service provider issuing the electronic certificate.
Purpose:	To identify who issued the electronic certificate.
Applies To:	Record
Obligation:	Mandatory
Repeatable:	No
Populated:	System generated
Guidance:	• Secured Electronic Signature

	• Can not be modified

counter signature	
Metadata Property	
Name of Term:	counter signature
Definition:	A certification service provider's counter-signature.
Purpose:	A counter-signature is required by some electronic signature applications.
Applies To:	Record
Obligation:	Optional
Repeatable:	Yes
Populated:	System generated
Use Condition:	• Secured Electronic Signature • Can not be modified

electronic signature	
Metadata Property	
Name of Term:	electronic certificate
Definition:	The electronic certificate of a record.
Purpose:	To capture the electronic certificate.
Applies To:	Record
Obligation:	Mandatory
Repeatable:	Yes
Populated:	System generated
Use Condition:	• Secured Electronic Signature • Can not be modified

electronic certificate serial number	
Metadata Property	
Name of Term:	electronic certificate serial number
Definition:	The serial number of the electronic certificate.
Purpose:	To capture the serial number of the electronic certificate.
Applies To:	Record
Obligation:	Mandatory
Repeatable:	No
Populated:	System generated
Use Condition:	• Secured Electronic Signature • Can not be modified

encryption algorithm	
Metadata Property	
Name of Term:	encryption algorithm
Definition:	The encryption algorithm used to encrypt the record.
Purpose:	Used to encrypt the record.
Applies To:	Record
Obligation:	Mandatory
Repeatable:	No
Populated:	System generated or manual entry
Use Condition:	• Secured Electronic Signature • Can not be modified • Updated automatically when a different algorithm is used.

encryption level	
Metadata Property	
Name of Term:	encryption level
Definition:	The encryption level of the encryption code used on the record.
Purpose:	To determine the encryption level.
Applies To:	Record
Obligation:	Mandatory
Repeatable:	No
Populated:	System generated
Use Condition:	• Secured Electronic Signature • Updated automatically when a different level is used.