Electronic Signature Technical Standard

Office of the Corporate Chief Information Officer, Modernization & EIE Branch

Version: 1.0

Approved by: Stephen Bull, Corporate Chief Information Officer and Sr. ADM, Office of the Corporate CIO and Telecommunications	**Owner:** Dale Huhtala, Executive Director, Modernization & EIE Branch
Approval date: May 15, 2020	**Review date:** September 30, 2020
Contact: Dwayne Budzak, Director, Enterprise Architecture (dwayne.budzak@gov.ab.ca)	**Policy Instrument type:** Standard

Contents

Standard Statement

This document establishes the Government of Alberta's (GoA's) technical standards for its information management and technology (IMT) solutions to its electronic signature business needs.

Authority

- *Electronic Transactions Act*
- *Government Organization Act*
- Records Management Regulation

Scope

This standard applies to:

- all departments defined under schedule 11 section 14(1) of the *Government Organization Act*; and
- agencies, boards and commissions as defined in schedule 1 of the Freedom of Information and Protection of Privacy Regulation.

Departments requiring an exception must follow the Chief Information Security Office exception process. Please contact your Sector Information Security Officer (SISO) to discuss the exception process; if your department is not part of a sector, please contact your department ISO.

Agencies, board and commissions that are not contained within schedule 1 of the Freedom of Information and Protection of Privacy Regulation are encouraged to align with this standard.

Standard Description

This standard describes the technical requirements that enable the use of electronic signatures in the government. E- Signatures in the government must be:

- Reliable i.e. verifiable to the signatory's identity and the integrity of the signature and record;
- Non-repudiable i.e. auditable to prove the signatory's intent to sign and the validity of the signature, and;
- Binding to the required agreement to provide confidence in government records.

References

This standard is supported with an implementation guide and other material that address both currently available tooling and interoperability, and the government's IMT landscape of custom, commercial and cloud solutions.

E-signature technical solutions must align with the following standards and guides. E-signature technical solutions must also align with GoA's IMT strategies, principles and information and records management practices.

Related Standards and Guidelines	Description
Electronic Signature Technical Standard Implementation Guide	GoA Guide for implementing e-signatures that conform to this standard
Electronic Signature Technical Common Solutions	Common technical solutions to common e-signature use cases within the GoA
Electronic Signature Technical Solution Requirements	GoA technical solution requirements to support tool acquisitions and custom solutions, where these are required. Includes requirements for metadata capture and signing events.
Digital Identity and Credential Assurance Standard	GoA standard with respect to digital identity and credential assurance.
Electronic Signature Types Standard	Types of electronic signatures used in the government – Basic and Secured
Electronic Signatures Solution Guideline	GoA business area considerations for implementing e-Signatures
Electronic Signature Metadata Standard	GoA Electronic Signature process requirements, specification and metadata requirements
Enterprise Architecture Principles	GoA Enterprise Architecture Principles for IMT

The Government of Canada (GoC) publishes guidance for the use of electronic signatures. The Government of Alberta's approach aligns to this standard. Electronic signature solution designers should also familiarize themselves with GoC guidance.[1]

Standard Specification

Both electronic and digital signatures must be interoperable across signature issuers and consumable by all signature stakeholders across digital and physical channels.

Electronic signatures within the government must**:**

- Be authoritatively verifiable to be considered secure;
- Prevent repudiation of the signature and signing event;
- Use encryption to prevent tampering with the signature and record;

[1] See https://www.canada.ca/en/government/system/digital-government/online-security-privacy/government-canada-guidance-using-electronic-signatures.html and https://wiki.gccollab.ca/E-signature_Options_2020-04

- Use approved identity sources:
    - Staff identities must use domain authentication;
    - Identities for the public must use MyAlberta Digital ID, with verified MyAlberta Digital ID's for Secured Electronic Signatures;
    - Identities for external organizations must use MyAlberta Digital ID for Business.
- Adhere to the retention and disposition of the associated record;
- Be renderable to digital and physical channels;
- Conform to government data exchange standards;
- Ensure interoperability across systems, signature providers and media / channels; and
- Capture any additional metadata to record attributes of the signing event, this is further explained in the Electronic Signature Technical Standard Solution Requirements document.

Digital signatures within the government must**:**

- Use certificates issued by a trusted source
    - Staff digital signatures must use certificates issued by IMT and assigned to domain users
    - Members of the public and external organizations must use digital signatures issued by a GoA-trusted source
- Follow the Digital Signature Certificate Requirements as outlined in the Electronic Signature Metadata standard.

Roles and Responsibilities

IMT Professionals (including, but not limited to, contractors) will:

- follow the standard when analyzing, designing and acquiring IMT solutions to GoA electronic signature needs;
- formally request exceptions to the standard when the standard does not meet business needs in terms of the presented electronic signature technical requirements or solutions; and
- abide by the decision of the governing body or role responsible for reviewing exception requests.

Compliance

All new solutions to business electronic signature needs within government must comply with this standard.

Compliance is determined by either:

- use of solution(s) for a common use case(s) referenced in the Electronic Signature Technical Standard Common Solutions; or
- the approval of a custom approach by the owner of this standard and the subsequent approval of an exception request

Existing solutions to business electronic signature needs that do not comply with this standard are risks for the government. Stewards or owners for such applications must follow the exception process noted in this standard.

Non-compliance with this standard could result in damage to the Government of Alberta's reputation, expose Albertans to harm and / or incur unnecessary costs.

- Depending on the severity of non-compliance, either informal or formal requests and / or follow-ups may be made by Enterprise Information Management, Corporate Internal Audit Services, Corporate Information Security Office, Office of the Information Privacy Commissioner, Office of the Auditor General, and / or Public Service Commission.
- Legislated disciplinary action (i.e., Public Service Act) may be taken depending on the severity of non-compliance by GoA staff.
- Non-compliance by GoA contract staff may result in a requirement to remediate at the contracted entity's cost, in addition to any other remedies available under the applicable contract.

References and Supporting Resources

- Electronic Signature Types Standard
- Electronic Signature Solutions Guideline

- Electronic Signature Metadata
- Electronic Signature Technical Standard Implementation Guide
- Electronic Signature Technical Standard Solution Requirements
- Electronic Signature Technical Standard Common Solutions
- Digitization Process
- Digitization Technical Requirements

Appendix A – Solution Requirements Areas

Electronic signature solutions must fit a diverse set of electronic signature needs. This standard provides solution designers with a set of common electronic signature solution requirements in the Electronic Signature Technical Solution Requirements document.

The solution requirements provided cover the following major topics:

Functional

Digital government	Signature Types	Legal
Compliance	Channels	Capture
Multi-signature	Reporting	Validation

Non-functional

Cost	Accessibility	Distributability
Authentication	Authorization	Metadata
Security	Storage	Scalability
Concurrency	Usability	Configurability
Availability	Disaster Recovery	Auditing
Logging	Curation	Portability
Standards Conformance	Supportability	Compatibility

Appendix B - Definitions

All definitions for terms used in this standard and its supporting materials are provided below.

For convenience, definitions for such terms that are provided in other electronic signature standards are available here. Where this is done, the original source document is hyperlinked within the definition. The original source remains authoritative for the definition.

1GX: A shortened form of the name for the government's enterprise resource planning system, One Government Experience.

AESG: The Accenture Enterprise Services for Government solution that forms the core of 1GX.

Basic Electronic Signature: (from the Electronic Signature Types Standard) 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.

COTS: An acronym for commercial-off-the-shelf solutions.

Custom Electronic Signature Solution: A solution to a business electronic signature need that differs materially from the recommended solutions in this standard. Such solutions require approval prior to their implementation.

Digital Signature: A mathematical process applied to an electronic record using public key cryptography in a way that allows a recipient of the signed record to verify the integrity of the record and information about the signer.[2]

Digitized Signature: A digital image of a handwritten signature, commonly a scanned image of an ink-based signature handwritten on paper or a signature captured from a computer input device, such as a touchscreen or digital pen and pad.

SaaS: An acronym for software-as-a-service.

Secured Electronic Signature: (from the Electronic Signature Types Standard) 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.

[2] Definitions have been adapted from other sources, including the US Nuclear Regulatory Commission – see https://www.nrc.gov/docs/ML1728/ML17283A173.pdf

Solution Designer: The role performed by anyone designing an IMT solution to a business need. Solution designers may be formally titled architects. Solution designers are also commonly business or systems analysts. Regardless of title, any designer of a solution incorporating electronic signatures must fulfill the mandates of the Electronic Signatures Technical Standard.