Electronic Signature Technical Standard Implementation Guide

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

Version: 1.0

Approved by: Dale Huhtala, Executive Director, Modernization & EIE Branch	**Owner:** Enterprise Architecture, 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:** Guideline

Contents

Guide Statement

This guide extends the core standard by providing electronic signature solution design guidance that complies with the government's standards, context and business needs that is not available elsewhere.

Audience

This document is directed at solution designers for electronic signature solutions.

Background

This guide is intended to support the Electronic Signature Technical Standard. It is to be utilized to assist designers or staff in implementation or design of E-Signature solutions.

E-signature Limitations

Currently, there are no international standards for e-signatures that enable interoperability within and across commercial and custom solutions, or across jurisdictions.

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

The Government of Alberta also does not support and validate digital identities attested to by credentials issued by external certifying authorities at this time.

Definitions

As this is a guide in support of the Electronic Signature Technical Standard, definitions from Appendix B in that document apply here.

References and Supporting Resources

This guide assumes that readers are familiar with the relevant business-oriented electronic signature standards and the other documents supporting the Electronic Signature Technical Standard, particularly:

- Electronic Signature Technical Standard Solution Requirements
- Electronic Signature Technical Standard Common Solutions

Information available in those documents is not replicated here.

Additional references:

[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

Related Standards and Guidelines	Description
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

Prerequisites for Designing an Electronic Signature Solution

Electronic signature solution designers must always start with the business need, including in terms of understanding the business process requiring the signature and the desired outcome(s) from acquiring a signature.

Solution designers should ensure that they are familiar with Electronic Signatures Types Standard and the Electronic Signatures Solution Guideline and that the processes described there have been completed before proceeding with technical solution design.

Design Principles

The following design principles must by followed by electronic signature solution designers and align with the government's overall enterprise architecture (EA) principles:

1. Start with the business need.
2. Design the business process before or concurrent to designing the electronic signature solution.
    - The business process design is critical to assuring identity and capturing required metadata.
    - Identity assurance and metadata capture distinguish basic and secured electronic signatures in many cases, not the solution technology.
3. Prefer standard GoA solutions.
4. Prefer centralized digital signing in your solution.
5. Prefer certificate-based digital signatures for secure electronic signature use cases.
6. Evaluate commercial-off-the-shelf (COTS) and software-as-a-service (SaaS) solutions against the requirements in the accompanying Solution Requirements document in the context of the business need.

Interoperability, Identity, and International Standards

A current limitation is the lack of an international standard for e-signatures to enable interoperability within and across commercial and custom solutions.

Solution designers must strongly consider interoperability and data exchange needs for electronic signatures to ensure that signatures captured in one solution, channel, or business process can be used by all users of the signature across all required channels and in all business processes. This includes consideration of the longevity of the signature – the signature must have the same longevity as its associated record. Solution designers must understand the mandated retention periods for the associated records.

Digital signatures used as all or portions of electronic signatures have greater interoperability and standardization, particularly with regard to certificates. However, GoA does not currently have the capability to validate the identities attested to by credentials issued by certifying authorities outside the GoA. Solution designers must consider this when designing solutions using digital signatures.

Checklist for an Electronic Signature Solution Design Process

The typical steps for an electronic signature solution design process are listed below and are recommended to the solution designer.

These form a checklist for the solution designer to use to increase the likelihood of the solution designer producing a standards-compliant solution that meets business needs with acceptable costs, benefits, and risks. The steps noted include the consultations and collaborations that are usually required to produce a compliant solution that meets business needs.

- ☐ The process within the Electronic Signatures Solution Guideline has been completed
- ☐ The requirements for the signature solution are known
    - The experience of the signatory has been considered
    - The business processes that will create or use the signature are defined
    - The highest level of identity assurance for the signatory required by the business processes that will create or use the signature is known
    - The signature type required (basic or secured) to meet the business need is known, and is incorporated into the business process design
    - A valid signing process that will generate the required type of signature has been designed
    - Legal, FOIP / Information Management, information security, and enterprise architecture consultations have been carried out to confirm the requirements
    - Information collected with the signature is traceable (appropriate meta-data collected) and auditable, and is appropriate for all users of the signature
- ☐ The business need has been reviewed against common use cases and solutions noted in the Electronic Signature Technical Standard Common Solutions
- ☐ Alternative options have been considered and weighed before making a selection

- The costs, benefits and risks associated with the options, and particularly those of the selected option, have been discussed with business stakeholders and accepted by them

- The Electronic Signature Technical Standard has been followed
    - Any non-standard solution or requirements set has been approved for implementation

Signature Types and Electronic Signature Technical Solutions

Electronic Signature Requirements

Signature types requiring technical solutions are the basic and secured electronic signature. The requirements noted in the Electronic Signature Technical Standard Solution Requirements document are sufficient to allow solution designers to provide solutions that cover either type of signature, as the business need requires. As this is a relatively generic requirements set and recognizing that some business needs may have differing requirements, solution designers may choose not to fulfill all requirements noted in this document depending on the actual business need that they are meeting. Solution designers should confirm omissions with their business stakeholders and document their rationales for these omissions to assist the maintenance and evolution of their solutions.

Note that both basic and secured signatures have similar key requirements, including for tamper-proofing. A key differentiator between the two types of signature is the level of identity and credential assurance required.[2]

Secured Signature

Where a secured signature is required, solution designers should select solutions that use digital signatures.

[2] The government endorses the Government of Canada's Standard on Identity and Credential Assurance. Solution designers are referred to the government's Digital Identity and Credential Assurance Standard for further information.

NOTE: Where a secured signature is required but digital signatures cannot be used, solution designers must prefer solutions that:

1. Provide the required level of assurance of the identity that is providing the signature
2. Capture sufficient metadata associated with that identity, the electronic signature and the signing event such that the electronic signature is sufficiently reliable for the business use case.
    - This must consider *both* business process and technical needs & changes
    - Metadata may be embodied in the signature itself, such as when the electronic signature is a certificate-based digital signature issued by a certificate authority
3. Digitally sign the core data being gathered (including any forms and attachments regardless of their format or channel or origin), the signature and the metadata as a holistic digitally signed record, to tamper-proof the record

Digital Signatures without Acceptable Credentials are not Secured Signatures

Note that only digital signatures where GoA is able to fully validate the identity of the signer will provide for a secured signature. Digital signatures that GoA cannot validate with an acceptable authority (e.g. a signature making use of a self-signed certificate) are equivalent to a basic signature as GoA cannot validate that the signatory is the indicated entity, and the digital signature itself only provides a minimum level of tamper-proofing.

Digital Signature Service

A GoA digital signature is required to protect the signature and associated record from tampering regardless of whether the signature type is basic or secured and regardless of whether the electronic signature is also based on a digital signature. As GoA's electronic signature standard requires that GoA augment the metadata typically captured by a digital signature, solution designers may have to apply an additional GoA digital signature to the entire record (the record plus the augmented metadata) even if a digital signature was originally provided by the signatory.

Given this, solution designers should prefer solutions that feature a *single* digital signature service that provides GoA digital signatures for a set of data and also provides authoritative timestamps. This is both to facilitate change to the digital signing approach within the solution and to enable migration to a GoA-wide signing solution when such is available.

Designing the Solution

The government prefers the reuse of existing IMT solutions to meet business needs. Electronic signature solution designers must use the recommended solutions below. Where this is not possible, solution designers must seek approval from the standard owner for the use of a custom solution.

Recommended Common Solutions

The following common use cases for electronic signatures, with both internal and external scenarios, are addressed in this standard:

- Signed PDF forms (not associated with 1GX)
- 1GX forms
- Forms presented as web application screens (custom or COTS / SaaS)
- Physical-to-electronic signature conversion
- Electronic-to-physical signature conversion

The noted solutions must be used in these use cases, or an exception to this standard must be sought.

Details of the use cases and solutions are provided in the accompanying Electronic Signature Technical Standard Common Solutions document.

Procuring Solutions Requiring Electronic Signature

When procuring electronic signature solutions, solution designers must ensure that the procurement approach used informs vendors of the GoA's recommended electronic signature solutions and its requirements for electronic signature solutions as documented in the Electronic Signature Technical Standard Solution Requirements document.

Solution designers must prefer acquiring solutions that reuse GoA's Electronic Signature Common Solutions. Where this is not feasible, designers must prefer acquiring solutions that meet the requirements specified in the Solution Requirements document to the greatest extent.

Custom Electronic Signature Solutions

The development of custom solutions is actively discouraged.

Where a custom solution is required, solution designers must use the requirements documented in the Electronic Signature Technical Standard Solution Requirements document as their base electronic signature requirements. Where one or more of these requirements does not apply to the business need, the rationale must be documented in the solution's requirements.

The owner of the Electronic Signature Technical Standard must approve all custom electronic signature solution designs prior to the design being implemented, and the custom design must be treated as an exception to the standard and follow the CISO exception process previously noted.

Earlier review and approval of custom electronic signature solution requirements and designs is recommended to avoid re-work.

Electronic Signature Metadata

GoA has an Electronic Signature Metadata Standard that applies to the signature itself. Solution designers must ensure that additional metadata is captured to record additional attributes of the signing event. This metadata may be captured explicitly, whether as part of the signature itself or as additional metadata captured alongside the signature, or implicitly, given the business

process being undertaken even if the metadata is mandatory (e.g. for internal GoA PDF forms, the capturing system is usually Adobe Acrobat Reader). It is left to the solution designer to determine how best to meet business needs with regard to metadata capture.

Further information on this metadata is provided in the Electronic Signature Technical Standard Solution Requirements document.