Electronic Signatures Solutions Guideline

Data, Privacy and Innovation Division

Version: 2.0

Approved by: Hilary Faulkner Executive Director Privacy, Policy and Governance Branch	**Owner:** Hilary Faulkner Executive Director Privacy, Policy and Governance Branch	
Approval date: November 28, 2022	**Last reviewed:** November 28, 2022	**Review date:** November 28, 2024
Contact: Sa.InformationManagement@gov.ab.ca	**Policy Instrument type:** Guideline	

Contents

Introduction

Purpose

This guideline describes the process that business areas must follow in order to use an approved electronic signature solution. This guideline is intended to help:

- identify risks and/or prohibitions associated with meeting legal and evidentiary requirements;
- mitigate potential risks; and
- ensure the appropriate implementation and use of an approved electronic signature solution.

Adherence to this guideline and the use of approved electronic signature solutions supports the integrity, validity and security of records containing electronic signatures created in, and/or retained by, the Government of Alberta.

The process detailed in this guideline supports implementation of the Electronic Signature Types Standard, and aligns with the Canadian General Standards Board (CGSB) 72.34-2017, Electronic records as documentary evidence standard established by the Government of Canada.

NOTE: Government use of electronic signature solutions that have not been approved by the Government of Alberta is neither endorsed nor recommended.

Background

"Electronic signature" is a broad term that encompasses any electronic information that a person creates or adopts in order to sign/endorse a record, and that is in, attached to, or associated with the record (e.g., signing a contract electronically, using check box verification on a website, providing verification/sign-in credentials, etc.). In the same way that a "wet" signature becomes part of a paper record, an electronic signature is attached to, or is associated with, an electronic record throughout the record's lifecycle.

Under Alberta's *Electronic Transactions Act*, the legal requirement for a signature can be satisfied by an electronic signature in many instances. A record to which the *Electronic Transactions Act* applies cannot be denied legal effect or enforceability solely on the basis that it is in electronic form.

Even where legally permissible, an electronic signature must meet certain requirements established by legislation and Government of Alberta information management technology (IMT) standards to be considered "valid"—these requirements may vary depending on the type and nature of the record.

Process

Business areas will identify and collaborate with relevant subject matter experts (SMEs) throughout this process to:

- evaluate the need for a signature;
- establish the value of an electronic signature;
- review legislative requirements;
- determine identity and credential assurance;
- evaluate findings; and
- implement an approved electronic signature solution.

SMEs may include (but are not limited to) information technology (IT) support, Information Management Portfolio Directors, and legal counsel. Topics on which SMEs can provide expertise include (but are not limited to):

- legal opinions (e.g., department legal contact);
- information management (e.g., IM program contacts);
- Cybersecurity; and
- privacy (e.g., FOIP Coordinators).

Step 1: Evaluate the need for a signature

First, determine if a signature is required. A signature's primary function is to provide evidence of the signatory's:

- identity;
- intent to sign the record and/or complete the transaction; and
- agreement to be bound by the contents of the record and/or transaction.

If there is no need to confirm one or more of these, then a signature may be unnecessary.

Step 2: Establish the value of an electronic signature

If a business area has determined that a signature is required, the business area must then determine if implementing an electronic signature provides stakeholder and/or process value. Some questions to ask throughout this evaluation include (but are not limited to):

- Will implementing an electronic signature solution enhance service?
- What are the benefits for businesses or the public in finalizing their records or transactions electronically?
- How much time do government staff spend processing paper signatures?
- Does the business area frequently require reengaging with the public due to errors resulting from missing, illegible, or otherwise incorrect "wet" signatures?
- What is the risk of someone disputing a signature?
- Is the risk of a dispute significant from a business or legal perspective?
- What are the potential consequences of a dispute over a signature?
- If multiple signatures are required by the business process, are there any special considerations (e.g., the order in which signatures are collected)?
- Do you need to have documentation regarding the signatory's consent to sign electronically?
- If a situation occurs in which a record is copied, is there a need to validate the signature on each copy?

Step 3: Review legislative requirements

Once a business area has established the need for a signature and the preference for an electronic signature, a review of relevant policy instruments must occur to determine if implementing an electronic signature is possible. This review must include (but is not limited to):

- examination of applicable legislation and/or regulations;
- examination of IMT policy instruments (e.g., IMT standards); and
- consultation with department legal counsel.

Some questions to ask during this review include (but are not limited to):

- Is there a legislative requirement for a signature?
  - If a signature is required by legislation, does the legislation include specific details

regarding the method, technology, or process involved in obtaining or attaching a signature to a record?

- Does the *Electronic Transactions Act* limit the ability to leverage an electronic signature?
  - Is there other legislation which limits or otherwise prohibits the ability to leverage electronic signatures?
- Have the legal risks been identified?
  - If risks have been identified, what kind of mitigation strategies are available? What level of risk still exists if mitigation strategies are implemented?
  - If mitigation strategies cannot be implemented, or if the mitigation strategies insufficiently reduce risk, does the business area accept the risk?
    - If yes, how will the business area document that the risk has been identified and accepted?

Once the business area has completed this review, it may be necessary to obtain a legal opinion; business should consult with appropriate department legal counsel.

NOTE: If it is determined that there is no need for a signature, but one is required in legislation (i.e., by an act or regulation), the department may want to consider if there is interest in, and/or cause for, amending the relevant legislation.

Step 4: Determine identity and credential assurance

When assessing options for implementing an electronic signature solution there are several foundational aspects that must be considered, including (but not limited to):

- the level of confidence that someone is who they claim to be;
- the level of confidence that a record has not been manipulated by either parties; and
- how, and to what degree, the integrity of a record can be evaluated.

Drawing upon the results of the evaluation conducted in the previous steps, and in alignment with the Digital Identity and Credential Assurance Standard, business areas can determine the appropriate identity and credential assurance level required for the electronic signature solution.

Step 5: Evaluate findings

After establishing business requirements and reviewing applicable policy instruments, business areas should evaluate the findings to ensure that an approved electronic signature solution satisfies the criteria developed through research and consultation.

If an approved electronic signature solution does not satisfy the criteria established by the business area, it is recommended that the business area consult SMEs and stakeholders to identify alternate options.

Step 6: Implement an approved electronic signature solution

Once the previous steps have been completed, and in consultation with IT subject matter experts, implementation of an approved electronic signature solution can be requested through the BERNIE portal.

Supporting Documents

- Digital Identity and Credential Assurance Standard
- Electronic Signature Types Standard