Electronic Signature Technical Standard Common Solutions

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:** Standard

Contents

Statement

The solutions for common government electronic signature use cases provided here support the Electronic Signature Technical Standard. They assist solution designers in mapping existing electronic signature solutions available within the government to business needs, and in designing and implementing standards-compliant electronic signature solutions using preferred technologies.

This document provides business areas and IMT solution designers with a set of common solutions to electronic signature needs within the government for both purely internal scenarios and for scenarios where the signatures must cross organization boundaries, inbound, outbound or both.

Audience

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

Definitions

Definitions from the Electronic Signature Technical Standard apply here.

References and Supporting Resources

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 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

Common Use Cases and Recommended Solutions

Secured Signatures

Certificate-based digital signatures provided by the signatory are preferred for secured signature use cases but may not always be achievable or practical given the business need being addressed.

Use Cases

These use cases represent the most common scenarios where government business areas wish to make use of electronic signatures. They enable signature capture and use across channels and business areas.

Solutions noted may have some weaknesses with regard to common business and technical requirements for IMT solutions to business electronic signature needs; where this is the case, these weaknesses are noted. Analysts and solution designers should discuss the opportunities and risks of these common solutions with business areas to select the optimal solution for a given need.

> **NOTE:** Business risk is present where an electronic signature solution does not meet all of the requirements outlined in this document. This includes COTS and SaaS solutions.
>
> Solution designers are accountable for ensuring that any material risks to their business clients are documented and communicated to their business clients for their action. They are also accountable for ensuring that they communicate their decision and these risks to their current and future solution architecture stakeholders, such as via the risk-related and decision-related sections of a solution architecture document.

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

- 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

NOTE: At the current time:

- 1GX will not make use of MyAlberta Digital ID or MyAlberta Digital ID for business
- It is not known if staff from agencies, boards and commissions or offices of the legislative assembly will be able to use digital signatures provided by the primary domain used by the departments of the GoA
- The 1GX e-Signature solution is being procured but the actual tool is not yet known

This document presumes that the 1GX e-Signature solution being acquired can provide the level of identity verification required to produce secure signatures within 1GX (for members of the public, vendors and all staff in the government). It also does not specify details of the 1GX solution.

This document will be updated once the 1GX solution is available.

Solution designers requiring further information on 1GX e-Signature solution capabilities should consult with subject matter experts in the 1GX team.

Internal Use Cases and Recommended Solutions

The following use cases for electronic signatures are common *within* the departments of the Government of Alberta. Recommended solutions are provided for each, along with additional notes for the solution designer. The solutions noted below **may not** be suitable for capturing signatures originating with or used beyond the departments, such as due to limitations in the ability to validate the signature (e.g. for a digitally signed PDF form that uses certificates issued internally to the departments). Solution designers should use solutions listed in the *External Use Cases and Recommended Solutions* section for those cases.

NOTE: The government prefers that digital information remain digital, and the Electronic Transactions Act enables this for signed documents, with a few exceptions. Manually signed forms (“wet signatures”) and forms that must be printed are actively discouraged for internal use cases. Solution designers should confirm with their business and Information Management colleagues that a physical form or wet signature is a true requirement, such as due to legal or policy needs, before proceeding with such a solution. Designers should record the rationale for the requirement in the solution’s design documentation.

Similarly, the use of fax as a channel within the Departments is actively discouraged and solution designers should record the rationale for the requirement in the solution’s design documentation.

Electronic signature solution designers may wish to review the Electronic Transactions Act in order to have a more complete understanding of the exceptional cases in which a wet signature is a legal requirement for the government.

The focus in the table below is on the capture of the electronic signature, with some information for designers regarding management of the signed record(s). Routine solution design practices (e.g. mechanisms for securing database or enterprise content management system access, logging and auditing system access and changes to records) are not addressed.

Use Case	**Signature Type**	**Description**	**Recommended Solution**	**Additional Notes**
Digitally Signed PDF Form	Secure	Use of fillable PDF forms with a true digital signature in a signature field. Such forms are typically e-mailed (possibly by logic embedded in the form) or stored in a repository, which may be capable of content management. Common examples in GoA are HR-related forms.	Adobe technologies for form design (Pro or LiveCycle). Adobe technologies for form review and signature validation. Acrobat Reader with Windows Digital ID issued for GoA domain login for completion of form.	The business process around the form should be structured to validate, via manual or automated means, that the signature is from a GoA-issued certificate and **not** based on a self-signed certificate, as users can create self-signed certificates on GoA machines. Only the GoA-issued certificate provides a reasonable level of identity assurance. Some metadata will be captured in the signature on the form. Other elements of the metadata are implicit. Non-repudiation relies on the domain login. Use of an enterprise content management system (ECM) is recommended to manage the signed record. The form and any

Use Case	**Signature Type**	**Description**	**Recommended Solution**	**Additional Notes**
				supporting documents should be treated as the holistic record. Ideally, the form allows for adding digital attachments so there is only one signed file to manage. Designers preferring non-ECM solutions must document this decision, its drivers and its rationale, such as in the solution architecture document.
Electronically Signed PDF Form (checkbox or equivalent)	Basic	Use of fillable PDF forms with a checkbox (or similar field) for acknowledgement / signing. Such forms are typically e-mailed (possibly by logic embedded in the form) or stored in a repository, which may be capable of content management. An example is the Leadership Program Application.	Adobe technologies for form design (Pro or LiveCycle). MS Office tools may also be acceptable depending on the business need. Adobe technologies for form review. MS Office and native web browser capabilities are also acceptable. Acrobat Reader for completion of form.	The business process around the form should be structured to validate the identity, form and signature to the level required. The form itself may be used to capture some of the recommended metadata. Identity assurance and non-repudiation are only implicitly provided. Use of this style of form for high-assurance situations is not recommended. Use of an ECM is recommended to manage the signed record. The form and any supporting documents should be treated as the holistic record. Ideally, the form allows for adding digital attachments so there is only one signed file to manage.
1GX Forms	Basic or Secure	Forms used within the government's 1GX (ERP) solution. This includes all elements of 1GX: AESG itself (S4/HANA, Ariba, SuccessFactors, Concur and Kyriba, plus AESG OpenText) and systems integrating with 1GX where the signature must be usable within 1GX. Examples here include HR- and expense-related forms. It is expected that many HR-related forms will be converted to 1GX forms over time.	The 1GX e-Signature solution, for signatures that originate in a component of AESG The 1GX e-Signature solution is also the recommended solution where signatures originate in systems within the 1GX ecosystem (i.e. systems integrated to AESG) if an	Forms and forms management are built into 1GX and solution designers should work with this existing functionality when implementing electronic signatures in 1GX. Solution designers should understand the life cycle of the form and record within 1GX, particularly in cases where form and signature data may cross between the component parts of 1GX and / or enter or leave 1GX to be represented in another system integrated with 1GX before finalizing their designs. The government's Active Directory remains the authentication system for staff within departments, even within 1GX.

Use Case	**Signature Type**	**Description**	**Recommended Solution**	**Additional Notes**
			element of AESG must rely on the signature.	The 1GX e-Signature solution will provide a range of electronic signature capabilities, from "clickwrap" through certificates based on digital signatures.
Custom Application Screen(s)	Basic	Form(s) implemented within a custom GoA application used within the departments of the GoA. As this is a basic signature use case, login by the signatory (or an agent representing the signatory) to the application itself or to the GoA domain is not a requirement or such login has a low level of identity assurance, such as for an anonymous poll. The signature is likely a checkbox acknowledgement or the simple act of submitting the form. The application may have been constructed with any GoA software development platform, from 3GL to low-code.	Metadata capture and digital signing of the associated record.	If the use case is to support anonymous use but requires the prevention of tampering with captured data such as in a poll, any information that is potentially personally identifiable, including IP addresses, should be scrubbed prior to the application of the digital signature. Full anonymity may not be achievable in such scenarios, such as if the timestamp of the record may be used to identify the user. Process design may need to consider this, as must the design of any digital signature service. Any attachments provided with the form should be considered part of the overall recorded and their data must be used in the generation of the digital signature to allow for tamper-proofing. Use of a database for the management of the form data and metadata is presumed. Use of an ECM is recommended to manage any attachments; storage of attachments as BLOBs in the database or as scanned images in a file system is actively discouraged as this inhibits search and content management. BLOB storage may be acceptable if the attachments are scanned, run through an optical character recognition tool (OCR'ed) and indexed for search and retrieval. Note that the OCR'ed text should also be considered in the digital signature to ensure that its integrity is also maintained.
Custom Application Screen(s)	Secured	Form(s) implemented within a custom GoA application used within the departments of the GoA. As this is a secure signature use case, login by the signatory (or an agent representing the signatory) to the application itself or to	GoA domain or application login to provide identity assurance. Use of multi-factor authentication is recommended where	Most such applications should be used directly by the signatory. Where an agent role is required, business process design for the signing event must ensure the intent to sign and authorization of the agent, which may also be captured on the form. In agent scenarios, the form must capture the signatory's identify information while the agent's identify information is captured as metadata.

Use Case	Signature Type	Description	Recommended Solution	Additional Notes
		the GoA domain is a requirement or the business process used must both require the agent to login and confirm the authorization of the signatory to submit the form. The signature may range from a checkbox acknowledgement to the application of a certificate-based digital signature. The application may have been constructed with any GoA software development platform, from 3GL to low-code.	higher levels of assurance are required. Metadata capture and digital signing of the associated record. If a digital signature is a requirement, use of the Windows Digital ID issued for GoA domain login by the signatory or their agent is recommended.	The login to the GoA domain or application provides the required level of identity assurance, while the metadata captured around the signing event and its linkage to the login and application provides non-repudiation for the signature. Digital signing of the record(s) and associated signature(s) provides for overall tamper-proofing. Use of a database for the management of the form data and metadata is presumed. Use of an ECM is recommended to manage any attachments; storage of attachments as BLOBs in the database or as scanned images in a file system is actively discouraged. BLOB storage may be acceptable if the attachments are scanned, OCR'ed and indexed for search and retrieval. Note that the OCR'ed text should also be considered in the digital signature to ensure that its integrity is also maintained.
COTS Application Screen(s), Including SaaS	Basic	Form(s) implemented within a COTS application used within the departments of the GoA. As this is a basic signature use case, login by the signatory (or an agent representing the signatory) to the application itself or to the GoA domain is not a requirement or such login has a low level of identity assurance, such as for an anonymous poll. The signature is likely a checkbox acknowledgement or the simple act of submitting the form. The application may have been constructed with any software development platform.	No specific solution is recommended	The actual solution is provided by the vendor. Evaluation of solution capabilities against the provided requirements list in the context of the business need should take place during solution selection or evaluation. Solution designers should prefer COTS or SaaS solutions that use approaches similar to those required of custom GoA solutions, including guidance with regard to use of GoA ECM services and storage of attachments.

Use Case	Signature Type	Description	Recommended Solution	Additional Notes
COTS Application Screen(s), Including SaaS	Secured	As this is a secure signature use case, login by the signatory (or an agent representing the signatory) to the application itself or to the GoA domain is a requirement or the business process used must both require the agent to login and confirm the authorization of the signatory to submit the form. The signature may be range from a checkbox acknowledgement to the application of a certificate-based digital signature. The application may have been constructed with any software development platform.	GoA domain or application login to provide identity assurance. Use of multi-factor authentication is recommended where higher levels of assurance are required. If a digital signature is a requirement, use of the Windows Digital ID issued for GoA domain login by the signatory or their agent is recommended.	The actual solution is provided by the vendor. Evaluation of solution capabilities against the provided requirements list in the context of the business need should take place during solution selection or evaluation. Solution designers should prefer COTS or SaaS solutions that use approaches similar to those required of custom GoA solutions, including guidance with regard to use of GoA ECM services and storage of attachments. Most such applications should be used directly by the signatory. Where an agent role is required, business process design for the signing event must ensure the intent to sign and authorization of the agent, which may also be captured on the form. In agent scenarios, the form must capture the signatory's identify information while the agent's identify information is captured as metadata. The login to the GoA domain or application provides the required level of identity assurance, while the metadata captured around the signing event and its linkage to the login and application provides non-repudiation for the signature. Digital signing of the record(s) and associated signature(s) provides for overall tamper-proofing. Use of a database for the management of the form data and metadata is presumed. Use of an ECM is recommended to manage any attachments; storage of attachments as BLOBs in the database or as scanned images in a file system is actively discouraged. BLOB storage may be acceptable if the attachments are scanned, OCR'ed and indexed for search and retrieval. Note that the OCR'ed text should also be considered in

Use Case	Signature Type	Description	Recommended Solution	Additional Notes
				the digital signature to ensure that its integrity is also maintained.
Physical-To-Electronic Signature Conversion	Basic or Secure	This is a "wet" signature scenario. Other types of physical signatures (e.g. biometric information) are typically immediately converted into digital format by the mechanism used to capture the physical signature or are treated the same as a traditional ink signature (e.g. a fingerprint). Use of (PDF, MS Office or other) printed forms. The form may be completed either fully manually (i.e. printing and manually filling out and signing) or partially manually (i.e. typing in data in any available fields and manually completing the rest and signing). The manually completed form is typically scanned and converted to digital format. The user of the automated system, which may or may not be the signatory, then retrieves the scan. The user of the automated system used to capture and manage the digitized form in this case is often **not** the person signing the form. Identity proofing is also performed manually, such embedding a requirement in the business process to validate a presented physical form of identification (e.g. driver's license, Alberta identity card, GoA ID card).	Scanner for scanning signed form Also recommended: Optical Character Recognition (OCR) to convert data on the scanned form into usable / searchable digital text. This is not required by the electronic signature as such, but is a "good practice". The process used for scanning should include quality assurance for the scan, to ensure that it is suitable for subsequent use.	Business process design must account for both the physical paper form and the digital form, as both are records requiring management. The business process around the form should be structured to validate the identity, form and signature to the level required. The form itself may be used to capture some of the recommended metadata. The mechanism used to perform identity proofing may also be captured digitally and submitted in support of the signed record (e.g. a scan of a driver's license), if this is appropriate to the business process and level of assurance required. The signature metadata in this case may be captured in part on the form and in part in the system that receives the scanned document. In essence, some aspects of the *signing* event are captured as signature metadata while aspects of the *submission* or *capture* event of the digital record in the automated system are considered to be metadata associated with the signature to assist later validation, avoid repudiation, etc. The digital identity that submits the form may not be that of the signatory. Regardless, the identity should be captured as part of the metadata associated with the signed form. Where optical character recognition (OCR) is used to convert the form into usable digital data, the scanned form should be retained as the authoritative record. Alternatively, the signature portion of the scanned form may be retained and the rest discarded, as long as a digital signature is applied to the entire record (the OCR'ed fields and the scanned signature) to ensure its immutability.

Use Case	**Signature Type**	**Description**	**Recommended Solution**	**Additional Notes**
				Use of an ECM is recommended to manage the signed record. The form and any supporting documents should be treated as the holistic record. Ideally, the form allows for adding digital attachments so there is only one signed file to manage.
Electronic-To-Physical Signature Conversion	Basic or Secure	Rendering of an electronic signature into a physical format on a channel that can represent such (e.g. paper, audio). Printing of the signature with some or all contextual metadata will be the most common scenario. Fax is treated as printing. Basic and secure signatures are only differentiated by the rendering of the signature and its metadata, particularly the assurance level of the identity providing the signature.	Varies by interaction channel.	The actual signature itself should be rendered to the channel in a format suitable to the interaction channel (e.g. printed on paper, “spoken” by a chatbot) along with a sufficient amount of the captured metadata to provide evidence of the signing event and attest to the reliability / validity of the electronic signature. Access to the metadata may require an additional action on behalf of the user, akin to requesting the message envelope information in a voicemail system. The public key of the digital signature service may also require rendering to the channel depending on the use case. Use of an ECM technology is beneficial here, as the technology allows for rendering of the record and its content to different media / formats.

External Use Cases and Recommended Solutions

The following use cases for electronic signatures are common where signatures must cross the boundaries of the departments of the GoA, such as in cases where a member of the public, a vendor or a partner signs the document or uses the signature as an authorization to render a service. Recommended solutions are provided for each, along with additional notes for the solution designer.

The focus in the table below is on the capture of the electronic signature, with some information for designers regarding management of the signed record(s). Routine solution design practices (e.g. mechanisms for securing database or ECM access, logging and auditing system access and changes to records) are not addressed.

NOTE: MyAlberta Digital ID (MADI) Verified can only be used by Alberta residents as it requires validation with Alberta government identification. Solution designers should validate the target groups for their use cases when considering using MADI Verified for secure signatures.

Use Case	**Signature Type**	**Description**	**Recommended Solution**	**Additional Notes**
Digitally Signed PDF Form	Secure	Use of fillable PDF forms with a true digital signature in a signature field. The form containing the digital signature will be submitted to the GoA on a digital channel. As this is an *external* scenario, GoA provides the technology to *create* the form but does not provide the technology actually used to *capture* the digital signature, so this may vary. This also means that the certifying authority used to create the certificate upon which the digital signature is based is not in The government's control.	Adobe technologies for form design (Pro or LiveCycle). Adobe technologies for form review and signature validation.	The business process around the form should be structured to validate the signature and check the integrity of the document as appropriate. Automated validation is preferred for higher-volume forms, while manual validation may be acceptable for lower-volume forms. Signature validation with Adobe technologies requires that the certificate of the signatory (or a parent certificate under whose authority the signatory's certificate was issued) is trusted by GoA. This implies that this type of validation is only useful for scenarios where potential signers or the certificate authorities that they will use can be known in advance of validation by GoA, which somewhat limits the value of the digital signature (although it remains useful for integrity checking). The overall business need and process will determine whether this is acceptable. For 1GX, the 1GX e-Signature solution should be used to ensure that the signature meets the criteria of a secure signature. If the PDF is to be signed outside of this solution and then incorporated into 1GX business processes, solution designers should consult with the 1GX team for alternative

Use Case	Signature Type	Description	Recommended Solution	Additional Notes
				approaches and may need to consider business process change, as 1GX does not provide logins with identity verification. If a secure signature is required and the GoA cannot validate the digital signature, such forms should be submitted via a channel that provides an appropriate level of identity assurance (e.g. a web application with a MyAlberta Digital ID Verified, or MADI Verified, login) rather than channels that provide low levels of identity assurance (e.g. e-mail). Some metadata will be captured in the signature on the form. Other elements of the metadata are implicit. Non-repudiation relies on the domain login. Use of an ECM is recommended to manage the signed record. The form and any supporting documents should be treated as the holistic record. Ideally, the form allows for adding digital attachments so there is only one signed file to manage.
Electronically Signed PDF Form (checkbox or equivalent)	Basic	Use of fillable PDF forms with a checkbox (or similar field) for acknowledgement / signing. The form containing the electronic signature will be submitted to the GoA on a digital channel. As this is an *external* scenario, GoA provides the technology to *create* the form but does not provide the technology actually used to *capture* the electronic signature, so this may vary.	Adobe technologies for form design (Pro or LiveCycle). MS Office tools may also be acceptable depending on the business need. Adobe technologies for form review. MS Office and native web browser capabilities are also acceptable.	The business process around the form should be structured to validate the identity, form and signature to the level required. The form itself may be used to capture some of the recommended metadata. Identity assurance and non-repudiation are only implicitly provided. Use of this style of form for high-assurance situations is not recommended unless used in combination with a channel that provides the higher level of assurance (e.g. an upload of such a form into a web application that uses MADI Verified for logins or the use of the 1GX e-Signature solution for 1GX). Use of an ECM is recommended to manage the signed record. The form and any supporting documents should be treated as the holistic record. Ideally, the form allows for adding digital attachments so there is only one signed file to manage.

Use Case	Signature Type	Description	Recommended Solution	Additional Notes
1GX Forms	Basic or Secure	Forms used within the government's 1GX (ERP) solution. This includes all elements of 1GX: AESG itself (S4/HANA, Ariba, SuccessFactors, Concur and Kyriba) and systems integrating with 1GX where the signature must be usable within 1GX. Examples here include vendor-related forms.	Native 1GX forms or the 1GX e-Signature solution may be used for all situations requiring basic signature. The 1GX e-Signature solution should be used for all secure signature requirements where the signature originates in a component of AESG, The 1GX e-Signature solution is also the recommended solution where signatures originate in systems within the 1GX ecosystem (i.e. systems integrated to AESG) if an element of AESG must rely on the signature.	Forms and forms management are built into 1GX and solution designers should work with this functionality when implementing electronic signatures in 1GX. Solution designers should understand the life cycle of the form and record within 1GX, particularly in cases where form and signature data may cross between the component parts of 1GX and / or enter or leave 1GX to be represented in another system integrated with 1GX before finalizing their designs. 1GX's form capabilities will provide for basic signatures in all cases. Secure signatures can be provided natively in 1GX for use cases where the signatory is authenticated to 1GX via a method that supports the required level of identity assurance – currently, this exists only for staff in the departments of the GoA. For all other cases, use of the 1GX e-Signature solution is recommended. The 1GX e-Signature solution will provide a range of electronic signature capabilities, from "clickwrap" through certificates based on digital signatures. If digital signatures are used, GoA should be able to trust the certificates issued where these are issued via the 1GX e-Signature solution regardless of the signatory being external to GoA i.e. GoA will be relying on certificates that it has issued and can do so confidently and securely. This allows for both basic and secure signatures.
Custom Application Screen(s)	Basic	Form(s) implemented within a custom GoA application used by stakeholders *external* to the GoA. As this is a basic signature use case, login by the signatory (or an agent representing the signatory) to the application itself is not a requirement or such login has a low level	Metadata capture and digital signing of the associated record.	If the use case is to support anonymous use but requires the prevention of tampering with captured data such as in a poll, any information that is potentially personally identifiable, including IP addresses, should be scrubbed prior to the application of the digital signature. Full anonymity may not be achievable in such scenarios, such as if the timestamp of the record may be used to identify the user. Process design may need to consider this, as must the design of any digital signature service.

Use Case	**Signature Type**	**Description**	**Recommended Solution**	**Additional Notes**
		of identity assurance, such as for an anonymous poll. The signature is likely a checkbox acknowledgement or the simple act of submitting the form. The application may have been constructed with any GoA software development platform, from 3GL to low-code.		Any attachments provided with the form should be considered part of the overall recorded and their data must be used in the generation of the digital signature to allow for tamper-proofing. Use of a database for the management of the form data and metadata is presumed. Use of an ECM is recommended to manage any attachments; storage of attachments as BLOBs in the database or as scanned images in a file system is actively discouraged. BLOB storage may be acceptable if the attachments are scanned, OCRed and indexed for search and retrieval. Note that the OCRed text should also be considered in the digital signature to ensure that its integrity is also maintained.
Custom Application Screen(s)	Secured	Form(s) implemented within a custom GoA application used within the departments of the GoA. As this is an external secure signature use case, login by the signatory (or an agent representing the signatory) to the application itself is a requirement or the business process used must both require the agent to login and confirm the authorization of the signatory to submit the form. The signature may range from a checkbox acknowledgement to the application of a certificate-based digital signature. The application may have been constructed with any GoA software development platform, from 3GL to low-code.	Application login to provide identity assurance. Use of MADI Verified is recommended where higher levels of assurance are required and the signatory or an external agent logs in to the application. Metadata capture and digital signing of the associated record.	Most such applications should be used directly by the signatory. Where an agent role is required, business process design for the signing event must ensure the intent to sign and authorization of the agent, which may also be captured on the form. In agent scenarios, the form must capture the signatory's identify information while the agent's identify information is captured as metadata. If this is an agent scenario and the agent is also external to the GoA, use of MADI Verified by the agent is recommended. The login to the GoA domain or application provides the required level of identity assurance, while the metadata captured around the signing event and its linkage to the login and application provides non-repudiation for the signature. Digital signing of the record(s) and associated signature(s) provides for overall tamper-proofing. Use of a database for the management of the form data and metadata is presumed. Use of an ECM is recommended to

Use Case	**Signature Type**	**Description**	**Recommended Solution**	**Additional Notes**
				manage any attachments; storage of attachments as BLOBs in the database or as scanned images in a file system is actively discouraged. BLOB storage may be acceptable if the attachments are scanned, OCRed and indexed for search and retrieval. Note that the OCRed text should also be considered in the digital signature to ensure that its integrity is also maintained.
COTS Application Screen(s), Including SaaS	Basic	Form(s) implemented within a COTS application used within the departments of the GoA. As this is an *external* basic signature use case, login by the signatory (or an agent representing the signatory) to the application itself or to the GoA domain is not a requirement or such login has a low level of identity assurance, such as for an anonymous poll. The signature is likely a checkbox acknowledgement or the simple act of submitting the form. The application may have been constructed with any software development platform.	No specific solution is recommended	The actual solution is provided by the vendor. Evaluation of solution capabilities against the provided requirements list in the context of the business need should take place during solution selection or evaluation. Solution designers should prefer COTS or SaaS solutions that use approaches similar to those required of custom GoA solutions, including guidance with regard to use of GoA ECM services and storage of attachments.
COTS Application Screen(s), Including SaaS	Secured	As this is an *external* secure signature use case, login by the signatory (or an agent representing the signatory) to the application itself or to the GoA domain is a requirement or the business process used must both require the agent to login and confirm the authorization of the signatory to submit the form.	Application login to provide identity assurance. Use of MADI Verified is recommended where higher levels of assurance are required and the signatory or an external agent logs in to the application.	The actual solution is provided by the vendor. Evaluation of solution capabilities against the provided requirements list in the context of the business need should take place during solution selection or evaluation. Solution designers should prefer COTS or SaaS solutions that use approaches similar to those required of custom GoA

Use Case	Signature Type	Description	Recommended Solution	Additional Notes
		The signature may be range from a checkbox acknowledgement to the application of a certificate-based digital signature. The application may have been constructed with any software development platform.	Metadata capture and digital signing of the associated record.	solutions, including guidance with regard to use of GoA ECM services and storage of attachments. Most such applications should be used directly by the signatory. Where an agent role is required, business process design for the signing event must ensure the intent to sign and authorization of the agent, which may also be captured on the form. In agent scenarios, the form must capture the signatory's identify information while the agent's identify information is captured as metadata. The login to the application provides the required level of identity assurance, while the metadata captured around the signing event and its linkage to the login and application provides non-repudiation for the signature. Digital signing of the record(s) and associated signature(s) provides for overall tamper-proofing. Use of a database for the management of the form data and metadata is presumed. Use of an ECM is recommended to manage any attachments; storage of attachments as BLOBs in the database or as scanned images in a file system is actively discouraged. BLOB storage may be acceptable if the attachments are scanned, OCRed and indexed for search and retrieval. Note that the OCRed text should also be considered in the digital signature to ensure that its integrity is also maintained.
Physical-To-Electronic Signature Conversion	Basic or Secure	This is a "wet" signature scenario where the signatory is an individual *external* to GoA. This scenario assumes that the physical form is what GoA receives, not an image scanned by the signatory. Other types of physical signatures (e.g. biometric information) are typically	Scanner for scanning signed form Also recommended: Optical Character Recognition (OCR) to convert data on the scanned form into usable	Business process design must account for both the physical paper form and the digital form, as both are records requiring management. The business process around the form should be structured to validate the identity, form and signature to the level required. The form itself may be used to capture some of the recommended metadata. The mechanism used to perform

Use Case	Signature Type	Description	Recommended Solution	Additional Notes
		immediately converted into digital format by the mechanism used to capture the physical signature or are treated the same as a traditional ink signature (e.g. a fingerprint). Use of (PDF, MS Office or other) printed forms. The form may be completed either fully manually (i.e. printing and manually filling out and signing) or partially manually (i.e. typing in data in any available fields and manually completing the rest and signing). The manually completed form is typically scanned and converted to digital format. The user of the automated system, which may or may not be the signatory, then retrieves the scan. The user of the automated system used to capture and manage the digitized form in this case is often **not** the person signing the form. Identity proofing is also performed manually, such embedding a requirement in the business process to validate a presented physical form of identification (e.g. driver's license, Alberta identity card, GoA ID card).	/ searchable digital text. This is not required by the electronic signature as such, but is a "good practice". The process used for scanning should include quality assurance for the scan, to ensure that it is suitable for subsequent use.	identity proofing may also be captured digitally and submitted in support of the signed record (e.g. a scan of a driver's license), if this is appropriate to the business process and level of assurance required. The signature metadata in this case may be captured in part on the form and in part in the system that receives the scanned document. In essence, some aspects of the *signing* event are captured as signature metadata while aspects of the *submission* or *capture* event of the digital record in the automated system are considered to be metadata associated with the signature to assist later validation, avoid repudiation, etc. The digital identity that submits the form may not be that of the signatory. Regardless, the identity should be captured as part of the metadata associated with the signed form. Where OCR is used to convert the form into usable digital data, the scanned form should be retained as the authoritative record. Alternatively, the signature portion of the scanned form may be retained and the rest discarded, as long as a digital signature is applied to the entire record (the OCR'ed fields and the scanned signature) to ensure its immutability. Use of an ECM is recommended to manage the signed record. The form and any supporting documents should be treated as the holistic record. Ideally, the form allows for adding digital attachments so there is only one signed file to manage.
Electronic-To-Physical Signature Conversion	Basic or Secure	Rendering of an electronic signature into a physical format on a channel that can represent such (e.g. paper, audio).	Varies by interaction channel.	The actual signature itself should be rendered to the channel in a format suitable to the interaction channel (e.g. printed on paper, "spoken" by a chatbot) along with a sufficient amount of the captured metadata to provide evidence of the signing event and attest to the reliability / validity of the electronic signature. Access to the metadata may require an additional action on

Use Case	Signature Type	Description	Recommended Solution	Additional Notes
		Printing of the signature with some or all contextual metadata will be the most common scenario. Fax is treated as printing. Basic and secure signatures are only differentiated by the rendering of the signature and its metadata, particularly the assurance level of the identity providing the signature.		behalf of the user, akin to requesting the message envelope information in a voicemail system. The public key of the digital signature service may also require rendering to the channel depending on the use case. Use of an ECM technology is beneficial here, as the technology allows for rendering of the record and its content to different media / formats.