Electronic Signature Technical Standard Solution Requirements

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 set of requirements for electronic signature solutions provided here supports the Electronic Signature Technical Standard. These requirements are to be used when designing a custom electronic signature solution or acquiring a new electronic signature solution for the government.

Audience

This document is directed at solution designers for custom electronic signature solutions and staff involved in acquiring new electronic signature solutions.

Scope

The government wishes to provide Albertans, partners, staff and vendors with a consistent experience in its business services and processes where electronic signatures are required, and to ensure that these signatures meet the government's needs for delivering those services efficiently and effectively, including the government's need to manage its signed electronic records.

This document provides business areas and IMT solution designers with a set of technical requirements for electronic signatures that will produce solutions that conform to the Electronic Signature Technical Standard and address common government business requirements related to electronic signatures.

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 Common Solutions	Common technical solutions to common e-signature use cases within the GoA
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

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.

Electronic Signature Metadata and the Signing Event

GoA has an Electronic Signature Metadata Standard that applies to the signature itself.

Solution designers **must** ensure that the following *additional* metadata is captured to record additional attributes of the signing event. This is particularly critical in cases where the assurance level of the identity providing the signature is low and / or where the signature itself is not a *digital* signature. That is, additional metadata pertaining to the signature is required in cases where the signature itself provides little in terms of the ability to validate the signature and / or avoid repudiation of the signature later.

Note that the "theme" of this metadata is essentially that of a session (in web parlance) i.e. it represents the context under which the electronic signature was captured. The concept of a session is key to designing the business process and the solution for any channel – for non-web channels, the solution designer must ensure that an analogous concept exists for the signature capture portion of the solution.

NOTE: This metadata does not address the validity of the overall signing process, such as clarity in the intent to sign. The solution designer must ensure that the signing process used is valid and meets the associated requirements in the business standards for electronic signatures.

NOTE: The signing process is critical even when the signature is electronic. The business process must be designed to include a valid signing process, as noted in the Requirements List for electronic signatures, and this process must consider how the signing "session" is opened and closed, whether the process is fully or partially automated. Explicit opening of the session surfaces the intent to sign, while explicit closure of the session reduces the signatory's ability to repudiate the signature ("it wasn't me that signed it – I forgot to close the session and someone else signed it").

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.

The metadata noted is considered part of the overall record and must be immutable, such as by being part of the entire record that is itself digitally signed.

An issue with electronic signatures is ease of duplication. In cases where it must be definitively known which copy of a record is the original (particularly if copies vary), capturing the above metadata and making it immutable will allow for this while still enabling copying, rendering to other channels (including physical media) and typical automated system needs such as backup & restoration and disaster recovery.

The table below lists the metadata elements that are required. The *location* and *digital signature of entire record items* will need to vary based on the channel used for signature capture (e.g. physical forms, web application, mobile app, IVR, etc.).

Metadata Element	Mandatory?	Description
Business Activity	Y	An identifier for the business activity for which the signature is required. This should be the same as that used for records management in the associated process.
Channel	Y	On-line / web, mobile, physical, IVR
Identity or Delegate / Agent ID	Y	The identifier associated with the identity providing the electronic signature. If the signature is being recorded by an intermediary in a digital system, which may include conversion from physical-to-digital, the identifier must be that of the person acting on behalf of the signatory and the identify of the signatory should be represented in the data associated with the signature.
Identity Assurance Level	Y	The level of assurance used to validate the identity providing the signature, as per the Digital Identity and Credential Assurance Standard.
Identity Authority	N	The authority of the signatory to provide the signature in this business process. This is particularly critical for business processes involving broker- / agent-style roles – the authority of the agent or broker to provide a signature on behalf of the client at that point in time should be captured.
Capturing System	Y	The identifier of the system or technology that captured the signature.
Capture Timestamp	Y	The time stamp of the moment of signing or conversion of a physical record to a digital format, at the most precise resolution available for the technologies involved. Note that this is required as the Electronic Signature Metadata Standard only captures the date, not the date and time at high resolution. Ideally, this timestamp is itself generated from a secure, central service such as a central signing service.

Metadata Element	Mandatory?	Description
Location	Y	Recommended metadata to capture varies by channel: • Physical: Use guidance for channel into which the electronic signature and associated record are stored (typically uses web or mobile application). • Web & mobile: IP address of client & server • Fax, SMS & IVR: Originating telephone number • E-mail: Sending and receiving e-mail addresses
Authentication Session ID	Y	Authentication session ID for the channel in use. Typically, a session ID or token for a web application. May be any other identifier used by the business activity to distinguish one transaction from another if no explicit session ID is available from the underlying technology.
Digital Signature of Entire Record	Y	This item is channel-dependent. Digital signature applied to entire record i.e. electronic signature, associated record (including any attachments) and all other metadata not generated from the signing service.

Requirements List

The following set of requirements must be used for solution acquisition and solution design in cases where the government's existing electronic signature solutions do **not** fit the business need.

As these requirements are intended to fit a diverse set of electronic signature needs, analysts and solution designers may customize the requirements set below to suit their specific business need. As noted previously, analysts and solution designers are expected to record a rationale for the omission of common requirements. Custom requirements lists **must** be approved by the owner of the Electronic Signatures Technical Standard before the new solution is transitioned into production. Earlier review and approval is recommended to avoid re-work.

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

Note that some non-functional requirements are embedded into the major functional topics to facilitate readability and to allow the solution designer to ensure requirements coverage for their solution.

Table of Functional Requirements

ID	Category	Name	Requirement (Req't) Description	Business or Technical Req't?	Requirement Type
DIG1.0	Digital Gov't	Digital Govt	Enable delivery of GoA services on digital channels to enable citizen convenience, meet service volumes at reasonable cost, etc.	Business	Business Objective
DIG1.1	Digital Gov't	Omni-channel Signature	Enable cross-channel delivery of GoA services, including from non-digital to digital and vice versa	Business	Business Objective
DIG1.1.1	Digital Gov't	Physical-to-Digital	Enable conversion of signatures from non-digital to digital form as electronic signatures	Business	User - Functional
DIG1.1.1.1	Digital Gov't	Physical-to-Digital Quality Assurance	Enable validation of the quality of the converted signature and its suitability for subsequent use	Business	Non-functional
DIG1.1.2	Digital Gov't	Digital-to-physical	Enable conversion of signatures from digital to non-digital form	Business	User - Functional
DIG1.2	Digital Gov't	Whole-of-Government / Full Business Process	e-Signatures must be accepted by all parts of GoA that must use the associated records	Business	Business Objective

ID	Category	Name	Requirement (Req't) Description	Business or Technical Req't?	Requirement Type
DIG1.2.1	Digital Gov't	All Departments Using Record	e-Signatures must be accepted by all departments of GoA that must use the associated records regardless of which body in the GoA obtained the signature	Business	Business Objective
DIG1.2.2	Digital Gov't	All ABCs Using Record	e-Signatures must be accepted by all ABCs that must use the associated records regardless of which body in the GoA obtained the signature	Business	Business Objective
DIG1.2.3	Digital Gov't	All Partners Using Record	e-Signatures must be accepted by all partners that must use the associated records regardless of which body in the GoA obtained the signature	Business	Business Objective
DIG1.2.4	Digital Gov't	Signature Exchange Standard	e-Signatures should have a GoA-wide data exchange standard	Technical / Solution	Non-functional
DIG1.3	Digital Gov't	Citizen Expectations	e-Signatures must meet citizen expectations for digital service	Business	Business Objective
DIG1.3.1	Digital Gov't	Citizen Signatures	Citizens (and organizations) must be able to provide e-	Business	Business Objective

ID	Category	Name	Requirement (Req't) Description	Business or Technical Req't?	Requirement Type
			Signatures usable by GoA for service delivery		
DIG1.3.2	Digital Gov't	Citizen Channel Support	Citizens (and organizations) must be able to provide e-Signatures on the digital channels that they most commonly use	Business	Business Objective
DIG1.3.3	Digital Gov't	Citizen Self-Service	e-Signatures must support citizen self-service	Business	Business Objective
DIG1.3.3	Digital Gov't	Citizen Devices	e-Signatures must support citizen devices / endpoints (and IMT capabilities)	Business	Business Objective
SIGTYPE1.0	Signature Type	Basic Signature	e-Signatures must support a basic electronic signature that allows electronic signing by any party representing themselves as the identity performing the signing i.e. the owner of the signature	Business	User - Functional
SIGTYPE2.0	Signature Type	Verified Signature	e-Signatures must support a secured / verified level of signature where the identity of the signatory is assured / validated as is their authority to sign	Business	User - Functional
LEGAL1.0	Legal	Legal Sufficiency	Electronic signatures must be of equal force as "wet" signatures i.e. be of the necessary legal sufficiency for the business purpose for which they are obtained	Business	Business Objective

ID	Category	Name	Requirement (Req't) Description	Business or Technical Req't?	Requirement Type
LEGAL1.1	Legal	Signing Process	The signature must be attached via a valid signing process is the overall set of means, processes, and procedures whereby: 1. A person applies an electronic form of signature to an electronic record, 2. The person's intent to sign the record is made manifest, 3. The electronic form of signature is attached to or logically associated with the record being signed, 4. The signatory is identified and authenticated, and 5. The integrity of the signed record is assured (from UESFOT).	Business	User
LEGAL1.1.1	Legal	e-Signature only on e-Record	Electronic signatures must only be associated with electronic records.	Technical / Solution	Non-functional
LEGAL1.1.1.1	Legal	e-Signature optional on e-Record	Electronic records governed by the Electronic Transactions Act may have electronic signatures.	Business	User - Functional
LEGAL1.1.2	Legal	Intent to Sign	The signatory must only be able to sign the document intentionally.	Business	User - Functional
LEGAL1.1.3	Legal	e-Signature associated to e-Record	The signature must be attached to / logically associated with the record during the signing process.	Technical / Solution	Non-functional

ID	Category	Name	Requirement (Req't) Description	Business or Technical Req't?	Requirement Type
LEGAL1.1.4	Legal	Identified / Authenticated Signatory	The signatory must be identified and authenticated during signing	Technical / Solution	Non-functional
LEGAL1.1.5	Legal	Integrity of Signature & Record	Electronic signatures must assure the integrity of the signature itself and associated record, and the combination of the two i.e. the association between them	Technical / Solution	Non-functional
LEGAL1.1.5.1	Legal	Tamper-resistant	The signature and all signed content must be tamper-resistant	Technical / Solution	Non-functional
LEGAL1.1.5.2	Legal	Integral to Record	An e-Signature must be implemented as an integral part of the record with which it is associated	Technical / Solution	Non-functional
LEGAL1.1.5.2.1	Legal	Non-repudiation	Electronic signatures must ensure that the signatory cannot repudiate signing	Business	Non-functional
LEGAL1.1.5.2.2	Legal	Integrity	Electronic signatures must be removed and re-created when the associated record is updated	Technical / Solution	Non-functional
LEGAL1.1.5.3	Legal	Immutable	e-Signatures must be immutable -- they may be replaced but not changed	Technical / Solution	Non-functional
LEGAL1.1.5.4	Legal	Authoritative Signature	There must be an authoritative signature associated to the authoritative record	Technical / Solution	Non-functional

ID	Category	Name	Requirement (Req't) Description	Business or Technical Req't?	Requirement Type
LEGAL1.1.5.4.1	Legal	Non-duplication	Copies of authoritative records and their associated signatures must clearly indicate that the digital copy is a copy and not the original, authoritative record	Technical / Solution	User - Functional
LEGAL1.1.5.5	Legal	Authority of Signatory	The authority of the signatory at the time of signing must be captured along with the electronic signature	Technical / Solution	User - Functional
LEGAL1.2	Legal	Consent	The signatory must consent to signing digitally, either explicitly or implicitly	Business	User
CONTENT1.0	Content Type	Content Type	Electronic signatures must be able to be associated with a record regardless of the content type (structured information, unstructured information, semi-structured information) of that record	Technical / Solution	Non-functional
COMPLIANCE1.0	Compliance	Compliance	Conformance to Legislation, Regulation and Policy	Business	Business Objective
COMPLIANCE1.1	Compliance	Business Goal	Electronic signatures must conform to the Electronic Transactions Act	Business	Business Objective
COMPLIANCE1.2	Compliance	Business Goal	Electronic signatures must conform to the Records Management Regulation	Business	Business Objective

ID	Category	Name	Requirement (Req't) Description	Business or Technical Req't?	Requirement Type
COMPLIANCE1.3	Compliance	Compliance	Biometric information may not be included in an electronic signature without specific authority	Business	Business Objective
COMPLIANCE1.4	Compliance	Testability / Verifiability	Electronic signatures must be able to be tested for validity by any party making use of them.	Technical / Solution	User - Functional
COMPLIANCE1.4.1	Compliance	Automated Verification	Automated processes making use of e-signatures should be able to test them for validity, including determining the level of identity assurance associated with the signature	Technical / Solution	User - Functional
CHANNELS1.0	Digital Channels	Digital Channels	Electronic signatures must be obtainable and renderable on all channels on which the associated service is offered / the associated record may be created or updated.	Business	Business Objective
CHANNELS1.1	Web Channel	Web Channel	Electronic signatures must be obtainable and renderable on the web channel when the associated record is created, updated or displayed there	Technical / Solution	User - Functional
CHANNELS1.2	Mobile App Channel	Mobile App Channel	Electronic signatures must be obtainable and renderable on mobile apps when the associated record is created, updated or displayed there	Technical / Solution	User - Functional
CHANNELS1.3	IVR Channel	IVR Channel	Electronic signatures must be obtainable and renderable on IVR when the associated record is created, updated or displayed there	Technical / Solution	User - Functional

ID	Category	Name	Requirement (Req't) Description	Business or Technical Req't?	Requirement Type
CHANNELS1.4	FAX Channel	FAX Channel[1]	Electronic signatures must be obtainable and renderable on faxes when the associated record is created, updated or displayed there	Technical / Solution	User - Functional
CHANNELS1.4	E-mail Channel	E-mail Channel	Electronic signatures must be obtainable and renderable via e-mail when the associated record is created, updated or displayed there	Technical / Solution	User - Functional
CHANNELS1.5	Social Media Channel	Social Media Channel	Electronic signatures must be obtainable and renderable via social media when the associated record is created, updated or displayed there	Technical / Solution	User - Functional
CAPTURE1.0	e-forms	e-forms	Electronic signatures must be able to be captured via and displayed in electronic forms	Technical / Solution	User - Functional
CAPTURE1.1	PDF Capture	PDF Capture	Electronic signatures must be able to be captured via and displayed in PDF forms	Technical / Solution	User - Functional
CAPTURE1.2	Web Forms	Web Forms	Electronic signatures must be able to be captured via and displayed in forms in web applications	Technical / Solution	User - Functional

[1] Note that the government is reducing its use of the fax channel where this is possible

ID	Category	Name	Requirement (Req't) Description	Business or Technical Req't?	Requirement Type
CAPTURE2.0	Digital Documents	Digital Documents	Electronic signatures must be able to be captured via digital documents	Technical / Solution	User - Functional
STAKEHOLDER1.0	Staff Support	Staff Support	GoA staff must be able to apply their own e-Signatures to digital records	Business	Business Objective
STAKEHOLDER2.0	Citizen Support	Citizen Support	Citizens must be able to apply e-Signatures to digital records	Business	Business Objective
STAKEHOLDER3.0	Partner Support	Partner Support	Partners must be able to apply e-Signatures to digital records	Business	Business Objective
STAKEHOLDER4.0	Vendor Support	Vendor Support	Vendors must be able to apply e-Signatures to digital records	Business	Business Objective
MULTI-SIG1.0	Multiple Signatures	Multiple Signatures	Records must be able to be associated with multiple e-Signatures where business needs require	Business	User - Functional
REPORTING1.0	Reports Include Signatures	Reports Include Signatures	Reports that include records with e-Signatures must be able to include the e-Signature and / or its metadata where this is justified	Technical / Solution	User - Functional
VALIDATION1.0	Signature Validation	Signature Validation	e-Signatures must be able to be validated as having come from the signatory	Business	User - Functional

Table of Non-Functional Requirements

ID	Category	Name	Requirement Description	Business or Technical Reqt?	Requirement Type
COST1.0	Cost	Reduce Service Cost	e-Signatures should reduce overall cost of service delivery	Business	Business Objective
COST1.1	Cost	Stay Digital	e-Signatures should enable records to stay digital throughout their lifecycles to reduce overall service delivery cost across the GoA	Technical / Solution	User
COST1.2	Cost	Support Business Process Automation	e-Signatures must support business process automation / reduce manual effort required in business processes (including records mgmt)	Technical / Solution	User
ACCESSIBILITY1.0	Access	Access to Record	Electronic signatures must be accessible to parties with access to the associated record	Technical / Solution	Non-functional
ACCESSIBILITY2.0	Access	Accessibility to Those with Disabilities	Electronic signatures must be able to be captured from, retrieved by and used (including for signature verification) by persons with disabilties	Technical / Solution	User
ACCESSIBILITY2.1	Access	Web Channel Accessibility	Electronic signature mechanisms used on the web channel must conform to GoA standards for web accessibility	Technical / Solution	Non-functional
DISTRIBUTABILITY1.0	Distributability	Distributability	Electronic signatures must be distributable to parties that receive the associated record	Technical / Solution	Non-functional
DISTRIBUTABILITY2.0	Distributability	Redaction	Electronic signatures must be able to be redacted from electronic records when they are	Technical / Solution	User - Functional

			distributed where redaction is required		
DISTRIBUTABILITY3.0	Distributability	Non-Electronic	Electronic signatures must be able to be rendered into non-electronic form alongside their associated record when that record is distributed in non-electronic form	Technical / Solution	User - Functional
AUTHENTICATION1.0	Authentication	Identity Assurance	Electronic signatures must be able to capture the level of identity assurance used when identifying and authenticating the signatory	Business	User - Functional
AUTHENTICATION1.1	Authentication	Assurance Level Capture	The level of assurance used to capture the signature must be captured as part of the signature, associated record or signature metadata	Technical / Solution	User - Functional
AUTHENTICATION1.1	Authentication	Appropriate Assurance	The level of assurance used to capture the signature should be appropriate for all currently known uses of the record across the Government of Alberta as a whole	Business	User - Functional
AUTHENTICATION2.0	Authentication	Standard Authentication Technologies	e-Signatures should rely on identities from standard GoA technologies	Technical / Solution	Non-functional
AUTHENTICATION2.1	Authentication	Public Authentication	e-Signatures should rely on identities from MADI and MADI-B for authenticating the public.	Technical / Solution	Non-functional
AUTHENTICATION2.2	Authentication	Staff Authentication	e-Signatures should rely on identities from Active Directory for authenticating staff	Technical / Solution	Non-functional

AUTHENTICATION2.3	Authentication	Partner Authentication	e-Signatures should rely on identities from MADI-B for authenticating partners	Technical / Solution	Non-functional
AUTHORIZATION1.0	Authorization	Authorized Signatory	Only authorized identities should be able to sign records	Business	User - Functional
AUTHORIZATION2.0	Authorization	Authorized Reader / Confidentiality	Only authorized identities should be able to read signatures	Business	User - Functional
AUTHORIZATION3.0	Authorization	No Copying	Signatures cannot be copied from one record to another	Business	User - Functional
METADATA1.0	Signature Metadata	Signature Metadata	e-Signatures must have the ability to associate metadata with the signature	Business	Non-functional
METADATA1.1	Timestamp	Timestamp	e-Signatures must be timestamped, including the date	Business	Non-functional
METADATA1.2	Assurance Level	Assurance Level	e-Signatures must include metadata specifying the level of identify assurance under which signing occurred	Technical / Solution	Non-functional
METADATA1.3	Authority of Signatory	Authority of Signatory	The authority of the signatory at the time of signing must be captured along with the electronic signature	Technical / Solution	Non-functional
SECURITY1.0	Information Security Classification	Information Security Classification	Electronic signatures associated with a record must have the same information security classification as the record	Business	Non-functional
STORAGE1.0	Digital Storage	Digital Storage	Electronic signatures must be able to be stored as part of or logically connected to the associated record	Technical / Solution	Non-functional
STORAGE2.0	Digital Storage	Digital Storage	Electronic signatures must be capable of being stored in the government's standard digital storage mechanisms	Technical / Solution	Non-functional

STORAGE2.0	Signature Size	Signature Size	e-Signature sizes must be allowed to vary based on business need	Technical / Solution	Non-functional
SCALE1.0	Record Size	Record Size	E-signatures must be able to be associated with digital records regardless of the record's own digital size	Technical / Solution	Non-functional
SCALE2.0	User volumes	User volumes	E-Signature solutions must scale to the maximum projected volumes of GoA e-services, with millions of users and hundreds or thousands of concurrent users	Technical / Solution	Non-functional
SCALE2.1	Real-time	Real-time	e-Signature capture, publishing / rendering and validation must be executable in real-time on the channel in use given projected concurrent user volumes and data sizes	Technical / Solution	Non-functional
CONCURRENCY1.0	Concurrent Reads	Concurrent Reads	E-signatures must be concurrently readable by authorized readers	Technical / Solution	Non-functional
USABILITY1.0	User Experience	User Experience	E-signatures must support the overall user experience desired for the target service	Technical / Solution	Non-functional
CONFIGURABILITY1.0	Configurability	Optionality	System and information designers must be able to specify which electronic records require electronic signatures	Technical / Solution	User - Functional
CONFIGURABILITY2.0	Configurability	Configurable Channels	System and information designers should be able to specify which channels should be supported for signing / rendering electronic signatures	Technical / Solution	User - Functional
CONFIGURABILITY3.0	Configurability	Configurable Level	System and information designers should be able to	Technical / Solution	User - Functional

			specify the level of electronic signature required		
CONFIGURABILITY4.0	Configurability	Configurable Data	System and information designers should be able to specify what digital information is required to constitute a valid digital signature on a channel	Technical / Solution	User - Functional
CONFIGURABILITY4.0	Configurability	Configurable Metadata	System and information designers should be able to specify what metadata should be captured with a digital signature on a channel	Technical / Solution	User - Functional
ARCH4.0	Architecture	Availability	e-Signature solutions must support the availability requirements of the business process	Technical / Solution	Non-functional
ARCH4.1	Architecture	Disaster Recovery / Business Continuity	e-Signature solutions must support the business continuity plans of the supported business process and its associated IMT solutions and their disaster recovery plans	Technical / Solution	Non-functional
ARCH7.0	Architecture	Auditing	Auditing	Technical / Solution	Non-functional
ARCH7.1	Architecture	Logging	Logging	Technical / Solution	Non-functional
ARCH8.0	Architecture	Recoverability	System Recoverability	Technical / Solution	Non-functional
ARCH9.0	Architecture	Curation	e-Signatures must remain accessible despite changes in underlying storage or display technologies	Technical / Solution	Non-functional

ARCH10.0	Architecture	Portability	e-Signatures must be portable across technologies used by participants in a business process, within or across organizations	Technical / Solution	Non-functional
ARCH10.1	Architecture	Platform Portability	e-Signatures should be portable across versions of the same technology	Technical / Solution	Non-functional
ARCH10.2	Architecture	Channel Portability	e-Signatures should be portable across digital channels	Technical / Solution	Non-functional
ARCH11.0	Architecture	IMT Policy Instrument Conformance	e-Signatures should conform to applicable GoA IMT policy instruments, such as its ISMDs	Technical / Solution	Non-functional
ARCH11.1	Architecture	IMT Standards Conformance	e-Signatures should conform to applicable GoA IMT standards such as its metadata standard	Technical / Solution	Non-functional
ARCH11.2	Architecture	IMT Standards Conformance	e-Signatures should conform to applicable GoA EA principles	Technical / Solution	Non-functional
ARCH11.3	Architecture	International Standards Conformance	e-Signature solutions should conform to applicable international standards	Technical / Solution	Non-functional
ARCH12.0	Architecture	Infrastructure	e-Signature solutions must support common GoA IMT infrastructure	Technical / Solution	Non-functional
ARCH12.1	Architecture	Endpoints	e-Signatures must be able to be captured on and published to common endpoint technologies in use by GoA, the public and GoA partners	Technical / Solution	Non-functional
ARCH12.1.1	Architecture	Endpoint Operating Systems	e-Signatures must be able to be captured on and published to common endpoint operating systems (Windows, MacOS, iOS, Android) in use by GoA, the public and GoA partners	Technical / Solution	Non-functional

ARCH12.1.2	Architecture	Browsers	e-Signatures must be able to be captured on and published to common endpoint web browsers in use by GoA, the public and GoA partners where the web is a target channel	Technical / Solution	Non-functional
ARCH12.1.2	Architecture	Disconnected Endpoints	e-Signature solutions must function when endpoints are disconnected. Graceful degradation in functionality is acceptable if functionality, such as identity or signature verification, requires access to a remote resource that is unavailable while disconnected -- normal processing should continue when re-connected.	Technical / Solution	Non-functional
ARCH12.2	Architecture	Server Operating Systems	e-Signatures must be able to be processed on common server operating systems in use by GoA	Technical / Solution	Non-functional
ARCH12.3	Architecture	Channel-Specific Technologies	e-Signatures must be able to be processed on common channel-specific technologies (IVR, e-mail, etc.) in use by GoA	Technical / Solution	Non-functional
ARCH12.4	Architecture	Channel-Specific Technologies	e-Signature solutions must support standard GoA data storage technologies	Technical / Solution	Non-functional
ARCH13.0	Architecture	Robustness	e-Signatures solutoins must be able to deal with varying network bandwidth, computing loads, etc.	Technical / Solution	Non-functional
ARCH14.0	Architecture	Supportability	e-Signatures solutoins must be supportable using GoA standard support and IMT change management / maintenance processes	Technical / Solution	Non-functional

ARCH15.0	Architecture	Integrability	e-Signature solutions must be able to integrate with GoA standard technologies and application development stacks	Technical / Solution	Non-functional
ARCH15.0	Architecture	Interoperability	e-Signature solutions should be interoperable, allowing the use of the signature, including validation of the signature, beyond the original capturing system	Technical / Solution	Non-functional
ARCH16.0	Architecture	Security	e-Signature solutions must be assessable for security threats, risks and vulnerabilities via standard GoA processes	Technical / Solution	Non-functional
ARCH17.0	Architecture	Privacy	e-Signature solutions must be assessable for privacy risks and impacts via standard GoA processes	Technical / Solution	Non-functional
ARCH18.0	Architecture	Cloud	e-Signature solutions should support the use of the cloud as an IaaS, PaaS or SaaS platform	Technical / Solution	Non-functional
ARCH18.1	Architecture	M365	e-Signature solutions should be compatible with the Microsoft M365 platform	Technical / Solution	Non-functional