VIRGINIA
IT AGENCY

Commonwealth of Virginia

Enterprise Architecture Standard (EA-225)

Enterprise Solution Architecture [ESA]

Computer-based Signature Standard

vita.virginia.gov

September 12, 2022

Revision History

Computer-based Requirements: Version History		
Revision	**Date**	**Description**
1.0	03-03-2021	Initial document created
1.1	08-04-2022	Added distinction between E-Signature and Digital Signature.
1.2	08-31-2022	Amended ESG-04 to qualify retention period.
1.3	09-12-2022	Amended per CIO comments.

Review Process
This requirements document was posted on the Virginia Information Technology Agency's (VITA) Online Review and Comment application (ORCA). All agencies, stakeholders, and the public were encouraged to provide their comments through ORCA. All comments were evaluated, and individual commenters were notified of action(s) taken.

Requirements and agency Exceptions
The requirements included within this document are mandatory. Agencies deviating from these requirements must request an exception for each desired deviation, and receive an approved *enterprise Architecture Exception* via Archer, prior to developing, procuring, or deploying such technology, or not complying with a requirement specified in this document. The instructions for completing and submitting an exception request are contained within the *Commonwealth enterprise Architecture Policy*.

Glossary
As appropriate, terms and definitions used in this document are in the COV ITRM IT Glossary. The COV ITRM IT Glossary is available on the VITA website.

Contents

Introduction 4
Purpose 4
Scope 4
Authority 4
Solution Business Requirements 5
Design/Architecture 6
Availability/Performance 6
Capacity 6
Continuity 6
Integration/Interoperability 6
Technology 7
Security 7
Glossary 9

Introduction

Vision & Strategy	
Vision	
Commonwealth of Virginia (COV) Knowledge Workers shall be able to securely transmit documents for legal electronic signature at any time, from any device, from anywhere within the continental United States.	
Strategy	
Objective 1	Provide an electronic document signing capability for COV that meets the legal requirements for electronic signatures.
Objective 2	Provide a document authentication capability for COV that meets the legal requirements for digital signatures.
Objective 3	Provide access to e-signature capabilities and features independent of form factor, i.e. desktop, web, or mobile, at any time, from anywhere.

Purpose

The intent of these requirements is to guide the purchase, design, implementation, and on-going operation of COV IT services and utilized technologies. For further information on the perspectives, please reference the most recent version of the enterprise Solution Architecture (ESA) Requirements.

These requirements contain best practices and set a standard, but this document shall not be construed to provide a basis for questioning the validity or legal effect of an e-signature; an e-signature may be valid and binding even if the e-signature, or the solution used to record it, does not meet all the requirements in this document.

Scope

This standard is applicable to all Executive Branch state agencies (hereinafter collectively referred to as "agencies") that are responsible for the management, development, purchase and use of information technology resources in the Commonwealth of Virginia. This standard does not apply to research projects, research initiatives, or instructional programs at public institutions of higher education

Computerized signature refers to software solutions that provide COV

- Digital form capture of wet ink signatures
- Authentication for government records using Public Key Infrastructure (PKI)

These requirements do not prohibit the use of general-purpose software and communications tools for electronically signing documents, but these requirements should be used to assess whether such fewer formal processes or more general purpose tools are appropriate and sufficient for legal and business needs.

In addition to the requirements below all COV IT technology solutions comply with the standards found on the VITA Policies Standards & Guidelines page.

Authority

Code of Virginia, §2.2-2007	Powers of the CIO
Code of Virginia, §2.2-2007.1	Additional duties of the CIO relating to information technology planning and budgeting

Code of Virginia, §2.2-2009(A)	Additional duties of the CIO relating to security of government information
Code of Virginia, §2.2-2012(A)	Additional powers and duties related to the procurement of information technology
Code of Virginia, § 2.2-3818	Standards for authentication of electronic government records

Solution Business Requirements

General Provisions

ESG-01 COV computerized signature services shall provide a platform for the e-signature of electronic documents that ensures:

- A signing party demonstrates a clear intent to sign, or may opt out
- A signing party consents to do business electronically
- Signature verification and unalterable capture of signing parties' names, emails, public IP addresses, signing events, timestamps, signing location and completion status
- A digital audit trail for every envelope that captures the name, email address, authentication method, public IP address, envelope action, and timestamp
- Association of signature with the record
- Record retention for each signed document

ESG-02 COV computerized signature services shall provide a platform for the digital signature of electronic documents, providing high confidence to a recipient that a message was created by a known sender and that the message was not altered in transit.

ESG-03 COV computerized signature services shall track who has opened, signed or approved a document.

ESG-04 COV computerized signature services shall keep an end-to-end log of each document signing transaction for the applicable records retention period.

ESG-05 COV computerized signature services shall support white-labelling to allow agencies to apply agency-specific branding to document signing workflows and forms.

ESG-06 COV computerized signature services shall provide reporting that tracks progress of transactions.

ESG-07 COV computerized signature services shall provide descriptive, diagnostic, and predictive analytics of document signing transactions.

ESG-08 COV computerized signature services shall provide the ability to create signing workflows that can acquire optional signatures.

ESG-09 COV computerized signature services shall provide the ability to create signing workflows that can route to signers dynamically based on conditional fields.

ESG-10 COV shall retain ownership of all documents that have been subjected to an e-signature process.

ESG-11 COV computerized signature services shall comply with the Virginia Public Records Act for document retention.

ESG-12 COV computerized signature services shall support Remote Online Notarization (RON).

ESG-13 COV IT e-signature services shall support capturing consent to a COV agency's standard terms and conditions (for example, through clickwrap).

ESG-14 COV computerized signature services shall provide the ability to search and filter documents that have been submitted to the e-signature process.

ESG-15 COV computerized signature services shall provide both remote and in-person signing options.

ESG-16 COV computerized signature services shall provide templates to create signing workflows.

ESG-17 COV computerized signature services shall provide tiers of service to support agencies different business volume needs.

ESG-18 COV computerized signature services shall provide tiers of service to allow agencies to select the volume of API calls they intend to submit in a year.

ESG-19 COV computerized signature services shall process agency API calls and documents submitted for signature that exceed the capacity of their selected tier.

Design/Architecture

ESG-20 COV IT e-signature services shall comply with applicable law[1].

ESG-21 COV computerized signature services shall provide the means to archive signed documents.

ESG-22 COV computerized signature services shall comply with COV Accessibility Standards.

Availability/Performance

ESG-23 COV computerized signature services shall have a minimum availability of 99.9%.

ESG-24 COV computerized signature services shall have an RTO of 24 hours or less, and an RPO of 25 to 48 hours or less.

ESG-25 COV computerized signature services shall comply with COV Data Availability Requirements regarding backup of data.

Capacity

ESG-26 COV computerized signature services shall provide the capacity to support the selected tiers of service for document volume.

ESG-27 COV computerized signature services shall provide the capacity to support the service volume of API calls they intend to submit in a year.

Continuity

ESG-28 COV computerized signature services shall support the guaranteed delivery of documents to all required and optional signers.

Integration/Interoperability

[1] Consult your counsel regarding the law applicable to a particular legal document or e-signature. Two of the most commonly applicable laws are the federal Electronic Signatures in Global and National Commerce Act [ESIGN] and Virginia's enactment of the Uniform Electronic Transactions Act [UETA].

ESG-29 COV computerized signature services shall integrate with the COV certificate authority for the digital signing of electronic documents.

ESG-30 COV IT e-signature services shall provide integration to essential agency business applications (for example, depending on the agency, Oracle PeopleSoft, Microsoft Office 365, or SalesForce).

ESG-31 COV computerized signature services shall provide custom integration to third party solutions through APIs.

Technology

ESG-32 COV computerized signature services shall support the ability to capture signatures from smart devices.

ESG-33 COV computerized signature services shall support the ability to capture signatures when the signer is offline.

ESG-34 COV computerized signature services shall support video conference signing.

ESG-35 COV computerized signature services shall support both serial and parallel signing workflows.

ESG-36 COV computerized signature services shall secure the immutability of signed documents through the application of digital signature encryption.

ESG-37 COV computerized signature services shall not be tightly bound to the software that captures and renders the e-signature, such that if the software is removed, the e-signature for a document remains immutably bound to the document.

Security

ESG-38 COV computerized signature services shall provide real-time identity proofing for users engaged in a signing workflow.

ESG-39 COV computerized signature services shall provide multiple methods for authenticating users engaged in a signing workflow, including:

- Biometric verification
- Certificate-based IDs
- Digipass
- Email
- Government ID verification
- Government smart cards & derived credentials
- Knowledge-based authentication (KBA)
- Login credentials
- Shared secrets
- SMS one-time passwords (OTP)

ESG-40 COV IT e-signature services shall comply with applicable Commonwealth security standards and additional security standards as appropriate, such as those established by the Federal Risk and Authorization Management Program (FedRAMP), the International Organization for Standardization (ISO 27001, ISO 27017, ISO 27018), or the National Institute of Standards and Technology (NIST 800-53r5).

ESG-41 COV IT digital signature services shall comply with the federal FIPS 186-4 Digital Signature Standard (DSS).

Glossary

As appropriate, terms and definitions used in this document are included in the COV ITRM IT Glossary.

Clickwrap

A clickwrap or clickthrough agreement is a prompt that offers individuals the opportunity to accept or decline a digitally mediated policy. Privacy policies, terms of service and other user policies, as well as copyright policies commonly employ the clickwrap prompt.

Digital Signature

A secured signature which works with E-signature and rely on Public Key Infrastructure means it comes with encryption standards. Validation of digital signature is performed by trusted certificate authorities or trust service providers.

E-Signature

A digital form of a wet ink signature which is legally binding and secure but it does not incorporate any coding or standards. It can be a symbol, image, process attached to the message or document to recognize the identity and to give consent on it. When we need to only verify the document we use electronic signature.

Remote Online Notarization (RON)

The process of having a state-licensed notary public notarize a document remotely using electronic signature, identity verification, audio-visual and electronic notarial journal and record keeping technologies.

White-labelling

A white-label product is a product or service produced by one company that other companies rebrand to make it appear as if they had made it. The name derives from the image of a white label on the packaging that can be filled in with the marketer's trade dress