Scope	E-Signature Security Procedures
Author	ETS-ISO
Purpose	To securely implement the electronic signature policy for electronic acquisitions and business operations. These procedures ensure that the electronic signed document is an original copy.

Introduction:

These security procedures apply to all business operations of the Department of General Services. The security procedures are best practices that will be applied to electronic signature (e-Signature) workflows but will be customized depending on the needs of program areas.

The security procedures discussed here are intended to pair with business procedures to allow for DGS program areas to use e-Signatures for acquisitions and other business processes. There are generally three types of security authentication. Only two will be discussed in this document. The third type of authentication requires the use of cryptography to produce a digital certificate. It is not discussed since digital certificates are rarely needed in DGS business processes.

A. The following is the first type of security authentication and is relevant for e-Signatures that are implemented with software tools that provide a complete audit trail for every transaction or workflow launched for e-Signing. Commonly used applications are DocuSign and Adobe Sign.

At each stage of the business process, the following security procedures apply:

I. Identification (Provisioning users):

1. Business program identifies approvers and reviewers prior to sending the document for e-Signature and verifies contact information, especially the approver's name and email address.
2. Business program users log in to the e-Signature tool with credentials and initiates document package.
3. Business program analyst creates a workflow in the e-Signature tool, that can be launched from a managed template, adds names and email addresses for approvers, creates one-time access code (if used), and initiates the e-Signature tool approval workflow.
4. Each required electronic signee, which could include the approving Vendor, Program Approver, Sender Approver, or other, will receive a separate email from the business program containing a link or code to access the document for review or approval.

II. Authentication (1-2 factor authentication may be used to provide identity assurance):

1. The approver and reviewer is authenticated when using the credentials provided by the business program to log into the e-Signature tool
    - The minimum method to be used will be "access link or code" or "email authentication";
    - "SMS" may be used for a high-dollar amount or type of contract.

III. Authorization (Role-based access):

1. Access will be granted upon successful authentication (roles assigned within DGS and set up in the e-Signature tool).
2. When authorization is validated, approver reviews document package and signs.
3. Users may be restricted from editing or deleting recipients via the e-signature tool settings.
4. A signature frame is enabled by ETS for recognition of the e-Signature tool and the signature ID.

IV. Accountability (The traceability of actions performed on a system to a specific system user, process, or

device):

1. Audit trail from the e-Signature tool is captured throughout the process for all actions.
2. Audit trail is protected from corruption using an e-Signature protected by a secure certificate provided by the vendor
3. Audit trail is made available on demand for all stakeholders.
4. Auditable events are captured throughout the entire process.
5. The e-Signature tool enables the following auditable events: User name, date (created, sent, and viewed), time (time zone, hh:mm:ss), location (when possible), requisition number, user/approver

V. Non-repudiation (The process of providing the authenticity of a signature):

1. The e-Signature tool ensures non-repudiation mechanisms are in place throughout the process from creation of the envelope, to viewing, and signing of the document.
2. the e-Signature tool ensures the signatures are hashed and their value can be verified in the e-Signature tool Trust Authority.
3. The e-Signature tool ensures x.509 version 3 certificates, digital checksums, Advanced Encryption Standards (AES) 256-bit encryption, and digital audit trails, which maintains the document's integrity.

VI. Availability (Accessibility and Recoverability):

1. The e-Signature tool sends notifications to ETS regarding downtime due to maintenance or disruption. In accordance to Adobe Sign Support SLA information, the response time after a service request has been received are as follows:
    - Level 1 – Critical : 30 minutes
    - Level 2 – Urgent : 1 hour
    - Level 3 – Important : 4 hours
    - Level 4 – Minor : 1 business day
2. The e-signature tool maintains secure replication of data in real-time at three U.S. Data centers.
3. ETS enforces recovery point objective (the maximum targeted period in which data might be lost) of less than 5 minutes.
4. All parties, both approvers and reviewers, in the electronic signing process will receive copies of the completed package via email from the e-Signature tool.

VII. Retention (Recordkeeping):

1. DGS will upload unaltered copies of the completed electronic acquisition contract to an approved electronic document repository. At least one unaltered copy must remain accessible for the period prescribed by the applicable document retention policy along with its certificate of signing created by the e-Signature tool.

B. The following is the second type of security authentication and is relevant for e-Signatures that are implemented with Adobe Acrobat. This type of e-Signature is free to all DGS employees and is generally sufficient for internal state transactions. It can also be used for public transactions if deemed appropriate by the stakeholders.

At each stage of the business process, the following security procedures apply:

I. Identification (Provisioning users):

1. Business program identifies approvers prior to sending the document for e-Signature and verifies contact information, especially the approver's name and email address.
2. Business program users set up the document to enable Adobe Acrobat e-Signatures.
3. Business program analyst sends the document for e-Signature via email. For various approvers, one

email at a time may have to be sent unless an automated workflow for document routing is utilized.

4. Each required electronic signee, which could include the approving Vendor, Program Approver, Sender Approver, or other, will receive a separate email from the business program with the document for signing attached.
5. Each required approver will have to send the document back to the business program via email.

II. Authentication (1-2 factor authentication may be used to provide identity assurance):

1. The approver is authenticated when the approver's name and email used to send the document matches what is on record in the Identification stage.

III. Accountability (The traceability of actions performed on a system to a specific system user, process, or device):

1. A limited audit trail from Adobe Acrobat may include the date and time stamped by each approver's computer upon signing, and email address of the signer.

IV. Retention (Recordkeeping):

1. The business program is responsible to upload unaltered copies of the completed and signed electronic contract to an approved electronic repository that will be accessible for the duration prescribed by the applicable document retention policy.

Glossary:

DGS	Department of General Services	**ISO**	Information Security Office
AES	Advanced Encryption Standard, the global standard for encryption adopted by the United States	**SMS**	Short Message Service (text message)
ETS	Enterprise Technology Solutions	**Signature Frame**	A frame and unique ID placed around the signature to make it easy to recognize the signature was created by an e-signature tool
Encryption	Conversion of plaintext to cipher text through the use of a FIPS validated cryptographic algorithm [FIPS 140-2]	**x.509**	X.509 is a standard format for public key certificates, digital documents that securely associate cryptographic key pairs with identities such as websites, individuals, or organizations.

Revision History:

Version ID	Date of Change	Author	Rationale
1.0	7/13/2018	ISO Office	Initial Draft
1.1	8/10/2018	ISO Office	Final Draft
1.2	9/3/2020	ISO Office	Revised Draft
1.3	11/5/2020	ISO Office, ESaaS Unit	Final Draft