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

Introduction:

These security procedures apply to the initial OBAS pilot, and will be expanded when broadening the scope to other program areas. The security procedures are best practices that will be applied to future e-signature workflows, but will be customized when working with other program areas.

The following security procedures are intended to pair with business procedures to allow for DGS program areas to use e-signatures for acquisitions. The current DGS standard for an electronic signature tool is DocuSign.
At each stage of the business process, the following security procedures apply:

I. **Identification** (Provisioning users):
   1. OBAS identifies vendor during Solicitation process and verifies contact information.
   2. OBAS (internal DGS procurement) users log in to the e-signature tool with credentials and initiates document package.
   3. OBAS analyst creates envelope in the e-signature tool 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. The approving Vendor, Program Approver, and OBAS Approver will receive a separate email from OBAS containing an access code to login.

II. **Authentication** (1-2 factor authentication may be used to provide identity assurance):
   1. The approver is authenticated when using the credentials provided by OBAS to log into the e-signature tool
      a) The minimum method to be used will be “access code” or “email authentication”;
      b) “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 are 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 electronic signature protected by a secure certificate provided by a trusted third party approved by the Secretary of State.
   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

actions, user/approver activities, status, envelope recipients, envelope ID, subject when document is created, viewed, signed, approved, queried, or completed.

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.
    - Maintenance notifications must be made via email to ETS within a reasonable time, no later than 24 hours.
    - the e-signature tool will respond to any incident reports within 15 minutes.
    - the e-signature tool will resolve incident reports within 24 calendar hours from time of reporting.
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 to the electronic acquisition contract will receive copies of the completed package via email from the e-signature tool.
5. SCO receives unaltered copy of the electronic acquisition contract via email from the e-signature tool.

VII. **Retention** (Recordkeeping):
1. DGS will upload unaltered copies of the completed electronic acquisition contract to FI$Cal and ServiceNow. DGS will upload the certificate of signing to ServiceNow.

Glossary:

DGS	Department of General Services	**ISO**	Information Security Office
FI$Cal	Financial Information System for California	**SMS**	Short Message Service (text message)
AES	Advanced Encryption Standard, the global standard for encryption adopted by the United States	**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
ETS	Enterprise Technology Solutions	**SCO**	State Controller's Office
OBAS	Office of Business Acquisitions and Services	**x.509**	A cryptography term used for a standard that defines the format of public key certificates
ServiceNow	A company that provides cloud-based business process workflow automation		

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