

Digital Autopen for Federal Register Documents Playbook

Standard Operating Procedure Template

**March 2023**

**FINAL**

**Federal Chief Information Security Officer Council**

**Identity, Credential, and Access Management Subcommittee**

**Delegated Digital Signature Working Group**

**Federal Register Signing**

**I. Authority**

1. [Name of delegation policy with the date and subsection] delegates authority to the [office with delegated authority] to sign Federal Register documents. The [office with delegated authority] may delegate this authority, in writing, only to the [positions].
2. Once delegated, only the [positions] for [office with delegated authority] are authorized to use the delegated signature authority. Because the delegation and sub-delegation are to the respective positions, the delegations do not need to be reissued when a new [authorizing sponsor] starts, or should new officials be appointed to serve in the abovementioned positions.
3. The delegation identifies the total number of approved delegates, not to exceed two (a primary and alternate).

**II. Process**

The digital autopen is used to affix the [authorizing sponsor] signature on a document. Before using the digital autopen to affix the [authorizing sponsor] signature, the user must ensure the following:

1. The [authorizing sponsor] approved the underlying document using a decision document. The [authorizing sponsor] may verbally approve a document in exigent circumstances. In that event, the [office of delegated authority] must note this verbal approval on the decision document. The decision document will note if [the authorizing sponsor] directs a digital autopen approval. A template for the decision document is attached.
2. The [digital autopen recipient] digitally signing the document must verify the [authorizing sponsor] prior approval of the underlying document and the approval for the [digital autopen recipient] to affix the [authorizing sponsor] signature.
3. The digital autopen cannot be used to affix the signature before the [authorizing sponsor] has approved the underlying document (for example, no “sign and hold”). See the [FICAM Playbook Digitally Sign an Office of the Federal Register Document](https://playbooks.idmanagement.gov/playbooks/signfedregister/) for the latest instructions on digitally signing a Microsoft Word document.

**III. Security and Logs**

[office with delegated authority] will maintain a physical or digital log of digital autopen use. The digital autopen recipient will capture the following information in the log:

1. Document Number of the Underlying Decision Document.
2. Date and time of the digital autopen use.
3. Name of the digital autopen recipient affixing the [authorized sponsor]’s signature.
4. Check box to verify that the [authorizing sponsor] approved the underlying decision document.
5. Check box to verify that the [authorizing sponsor] directed the use of the digital autopen and by what method (direct or verbally transmitted) and noted on the decision document.

**Digital Autopen Certificate**

**I. Authorities**

1. Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors
2. Federal Information Processing Standards (FIPS) Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors;
3. X.509 Certificate Policy for the U.S. Federal Public Key Infrastructure (PKI) Common Policy Framework
4. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-157, Guidelines for Derived PIV Credentials.

**II. Process**

The [agency] digital autopen certificate is only used to affix the [authorizing sponsor] signature on a *Federal Register* document. The [office with delegated authority] must ensure the following before requesting a digital autopen.

1. The user signs the User Agreement with their PIV card. See attached sample User Agreement. The user must comply with all requirements of the User Agreement.
2. The [office with delegated authority] attaches the delegation authority and signed User Agreement to an issuance request form to the [security office].
3. The [security office] verifies the person is a federal employee, is in a position in the [office with delegated authority] named in the [Name of delegation policy with date and subsection], and has signed the user agreement.
4. The [security office] verifies that this request doesn't exceed the maximum authorized delegates.
5. The [security office] sends a request with attachments to the certificate issuer.
6. The [security office] retains this package for auditable purposes.
7. The certificate issuer verifies the information and coordinates with the user for certificate issuance.
8. According to the User Agreement, the user receives and protects the digital autopen certificate.

**III. Security and Logs**

Secure the digital autopen certificate following the User Agreement. The following artifacts create an auditable trail of delegation and certificate issuance.

1. [Name of delegation policy with date and subsection]
2. Signed User Agreement
3. Signed Certificate Issuance Request

**Other Information**

1. The [office with delegated authority] should periodically review the logs to maintain them properly.
2. The [office with delegated authority] should coordinate any changes to this Standard Operating Procedure with the Office of the General Counsel.

Approved:

|  |  |  |
| --- | --- | --- |
| [Name][Title] |  | Date |

Attachment:

1. Decision Document
2. Sample User Agreement
3. Issuance Request