

Secured Signing for 21CFR Part 11 Compliance

Electronic Signatures at Organization ABC

Organization ABC operates in a regulated environment and is subject to compliance with numerous US Government regulations governed by the Food & Drug Administration (FDA).

This document is provided to explain the use of the User Based PKI digital signatures on various documents at Organization ABC business operations. For all digitally signed documents at Organization ABC, the electronic version upload to Secured Signing secured storage is considered the *source* document and all printed documents are for working use only.

PKI Based Digital Signature Technology

Organization ABC achieves FDA 21 CFR Part 11 Standard data integrity compliance using digital signature technology like the same PKI based systems used throughout the US Federal Government.

PKI provides each user (signer) with a key-pair, a Private Key and a Public Key used in every signature. The Private Key, as the name implies, is kept private and stored securely in HSM; the Private Key is used for signing, thereby adding a digital "fingerprint" to the document. The Public Key (from which the Private Keys were created) is made widely available to any person who wishes to use it for validating the sender's digital signature.

The value of digital signatures from an electronic record standpoint is that signed documents "stand on their own" as self-contained, portable, electronic records. Recipients anywhere in the world simply open the signed document (the Private Key is hashed to the document) in order to verify the contents authenticity (who signed) and data integrity (what was signed). Hence, signed documents can be used as electronic evidence for audits to prove unique ID and intent of signer and guarantee that the data has not been altered since the signature was added.

The signed document is sealed with signer's Digital signature, any content alteration invalidates the Digital signature, this provides the highest level of document security, Signer's Identity, Intent and document data Integrity. For more information about Digital Signature Technology have a look at <https://www.securedsigning.com/resources/intro-to-digital-signatures>

21 CFR Part 11 areas covered by the system include:

PART 11 -- ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart B--Electronic Records

11.10 Controls for closed systems

Secured Signing is dealing with electronic documents that meet these requirements using the latest applicable industry standards. Authenticity and integrity are provided by using strong PKI Digital Signatures and the system uses encryption for all documents in rest, data is protected. The document upload is protected using an HTTPS with True Business ID certificate and AES encrypted TLS/SSL session.

<p><i>(a) Validation of systems to ensure accuracy</i></p>	<p>A Secured Signing Paid User/ account login to secured signing, use SSO or username and password and upload the document, the system converts all documents to PDF or uses the original PDF. There is one copy of the document in our system.</p> <p>A user who wishes to sign will position the signature on the page and click sign. A PKI digital signature process is embedded in the PDF file. The Digital signature includes; signer's details, time stamp, graphical image, job title, and reason for signing. All this info can be verified by anyone that receives the signed PDF, only a PDF reader is required to verify signed PDF.</p> <p>The Digital Signature meets ISO 32000 PDF standards and ETSI PAdES signature standards.</p>
<p><i>(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.</i></p>	<p>Any signed documents can be viewed with any PDF reader, by any person.</p>
<p><i>(c) Protection of records</i></p>	<p>Secured Signing uses the latest standards recommended by the US National Institute of Standards and Technology (NIST) namely SHA-384 hashing and RSA 4096-bit digital signatures. The signature supports LTV so you can verify the signed document even when the user's signing key has expired.</p>
<p><i>(d) Limiting system access to authorized individuals.</i></p>	<p>A signer who is part of the organisation and has a paid account can use password or Single Sign On in order to access the document for signing.</p>


	Invitees and external users can use SMS two-factor authentication to access document for signature.
<i>(e) Audit trails.</i>	Each signing process has an audit trail/document log with all signing actions. Each line in the log has the action, the persons role in the process and time stamp.
<i>(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.</i>	Secured Signing's workflow allows the signer to reroute the signing process to authorised person, decline to sign, review before signing, and sign. Each action added to document log for audit down the track
<i>(g) Use of authority checks to ensure that only authorized individuals can use the system</i>	A core function of Secured Signing is to enforce user authentication and data access permissions to maintain trust and data integrity.
<i>(h) Use of device</i>	Secured Signing can be used with any device to access a document for signature, due to only one copy of the document being in our system, what you see on screen is the document you are going to sign.
<i>(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education</i>	The system has user guides, and videos on how to use the system, as well as an intuitive user interface, with tooltips along the way.

11.30 Controls for open systems

<i>Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality</i>	Secured Signing meets these requirements using the latest applicable industry standards. Authenticity and integrity are provided by using strong digital signatures and the system uses encryption for all documents in rest. When documents are uploaded, they are protected using a secure HTTPS with True Business ID certificate TLS/SSL
---	--

11.50 Signature manifestations

Signed electronic records shall clearly indicate printed name of signer, date & time and reason for signing.

<p>(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</p>	
<p>(1) The printed name of the signer;</p>	<p>Signed by: Stu Wood Tester Reason: I am approving this document Date & Time: 05 Apr, 2020 11:55:34 AM</p>
<p>(2) The date and time when the signature was executed; and</p>	<p>The signature includes, signer's full name, time stamp, the time signature was applied to the document, with offset to signers local time zone. The signer's job title and reason are part of the signature block.</p>
<p>(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.</p>	<p>The system provides the list of reasons that appear in the process, or the signer can type in any reason.</p>
<p>(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).</p>	<p>Review before signing process can be added to signing process to be sure document has been read before signed. The way we are implementing PKI Digital signatures, means that most of signature information is visible on the printed PDF.</p>

11.70 Signature/record linking

<p>Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.</p>	<p>A Digital Signature is always linked to the document and to the person who is signing. ISO 32000 defines the way in which digital signatures are applied to PDF documents. Any change to the document protected by a digital signature invalidates the signature. It will show red X with a message signature is invalid in any PDF reader that is following Digital Signature standards.</p>
--	--

Subpart C--Electronic Signatures

11.100 General requirements

<p>(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.</p>	<p>Each signer has unique signing keys, as well as document hashing based on SHA384 RSA creating a unique document fingerprint that is signed by the unique signer's signing key.</p>
<p>(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual</p>	<p>Secured signing provides a process to issue a certificate to a register user. Based on user directory or email address, names and Mobile phone number. KYC process in place</p>
<p>(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic</p>	<p>The system, as part of the signing process notifies the signer that they have agreed to use electronic signature technology and it is</p>

<i>signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.</i>	a legally binding equivalent of traditional handwritten signatures.
---	---

11.200 Electronic signature components & controls

Employ at least two distinct identification components; Continuous sessions.

<i>(a) Electronic signatures that are not based upon biometrics shall:</i>	Secured signing uses the following methods: <ul style="list-style-type: none"> • Email address and passcode • Email address and password • Email address and SMS OTP • AAD SSO • ADFS SSO
<i>(1) Employ at least two distinct identification components such as an identification code and password.</i>	In order to access a document for signing, signer needs the email address plus passcode, or email address and password, or email address and SMS OTP. Both tokens allow a signer to access the document signing process.
<i>(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.</i>	The system requires users to access again with their credentials when the signer is invited to sign a different document at a different time. In the case of multiple documents in the same pack, the user access can once to sign each document, one by one, however a time process is in place, if they timeout the signer needs to login again.
<i>(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.</i>	
<i>(2) Be used only by their genuine owners; and</i>	User authentication process in place before allowing the use of signer's signing key
<i>(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</i>	Each signer must access the document using their unique link that is connected to their email address and passcode for example. This link presents the signer with their own unique authentication process to verify and if passed they are able to sign.
<i>(b) Electronic signatures based upon biometrics shall be designed to ensure that</i>	Handwritten graphical image is part of the digital signature block. Secured Signing provides a tool to capture/draw graphical

<i>they cannot be used by anyone other than their genuine owners.</i>	signatures, this can be considered a biometric signature as well.
---	---

11.30 Controls for identification codes/passwords

Authenticity & integrity of electronic records from the point of their creation to the point of their receipt.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

<i>(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.</i>	Fully supported, with strong password and notification of a strong or weak password. For higher levels of security, SMS OTP can be used in order to access document for signing process.
<i>(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).</i>	
<i>(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.</i>	Secured Signing has full management of the issuing and storage of signing keys. It is a remote managed PKI System. Revoke key, CRL is all in place as part of our solution. All user key management is embedded in our solution and the end user doesn't need to worry about that.
<i>(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.</i>	All signing keys are within HSM without ability to export or to run outside of the HSM. By revoking the signer, or deleting a user from the organisation their key will be revoked and no new documents can be signed.
<i>(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.</i>	Entire system has a centralised approach for PKI signing keys. None of the keys can be lost by the signer. The signer has remote access to use their signing keys based on their credentials.

Organization ABC Digital Signature Solution

Organization ABC uses a digital signature solution named Secured Signing

Secured signing provides all of the features of PKI Based Digital Signatures described above, plus it provides additional features as required by 21 CFR Part 11. For example:

- All digital signatures include the user's full name, a time/date stamp and force a "reason for signing" to be entered. The digital signature also includes the display of the "graphical" or handwritten signature of the individual. In addition, the digital signatures contain a wealth of information about each signer in the certificate of each signer contained in the digital signature.
- The Private Keys (used for signing) and associated certificate (used for identification) are stored in a security appliance HSM deep behind firewalls. Hence, the digital signature keys and certificates are secure.
- The digital signatures can only be applied after the user successfully authenticates using a unique two form Username plus Password combination, or other options available.
- Each digital signature in a document covers the entire documents; reviewers can verify that the data covered by a signature has not been altered since the signature was applied. Each signature operations are in the document log. Certain file formats, such as PDF, also provide a full audit log or revision history associated with each contained signature; the exact status of the document contents can be viewed at the time of which each signature was applied.

Related Policies and Procedures

Organization ABC Electronic Records System

To minimize the risk of a signed document accidentally being changed within Organization ABC; a digitally signed document is moved and stored into an appropriate directory which has 'create and read only' rights. The source document is controlled in accordance with documented procedures, the same as for all electronic records that are subject to regulatory requirements. These procedures include backup and archiving.

Identity Proofing

Organization ABC has procedures in place to ensure that the identity of the individual has been established before they are setup and given the ability to use the digital signature system. Since the electronic signature system is being used by internal and external users, Organization ABC has an employee policy in place that describes the accepted use of digital signatures. For Secured Signing system to generate a Private Key and certificate for an individual, that individual needs to be approved and entered into the Organization ABC employee database (Microsoft Active Directory system) or Azure AD SSO.

Organization ABC informs all users that the digital signatures are intended to be a legally binding equivalent of traditional handwritten signatures in accordance with 21 CFR part 11 clause 11.100 c.