

# GlobalSign Enterprise Solutions

CFR 21 Part 11 Audit Support

Using GlobalSign's PDF Signing Certificates



## Table of Contents

Introduction .....	3
GlobalSign's PDF Signing Certificates.....	3
Title CFR 21 Part 11 Audit Support .....	3
Subpart A – General Provisions.....	3
Section 11.1 Scope .....	3
Section 11.2 Implementation.....	4
Section 11.3 Definitions .....	4
Subpart B – Electronic Records .....	5
Section 11.10 Controls for Closed Systems.....	5
Section 11.30 Controls for Open Systems.....	13
Section 11.50 Signature Manifestations .....	14
Section 11.70 Signature/Record Linking .....	14
Section 11.100 General Requirements .....	15
Section 11.200 Electronic Signature Components and Controls .....	17
Section 11.300 Controls for Identification Codes/Passwords.....	18
Appendices.....	19
Appendix A – Configure Reason Code in Adobe Acrobat .....	19
Appendix B – Purchasing Individual PDF Signing Certificates .....	20
Appendix C - Purchasing Multiple PDF Signing Certificates .....	22
Step 1 – Establishing an EPKI Account .....	22
Step 2 – Registering Users for PDF Signing Certificates .....	24
Step 3 – Installing Your Certificate.....	28
Conclusion.....	29
GlobalSign Contact Information.....	29

## Introduction

Biotechnology, pharmaceutical, drug and medical manufactures regulated by the FDA need to be aware of the federal regulations surrounding the protection and privacy of consumer data, management of electronic documents and the acceptance requirements for electronic documents and signatures.

The FDA has imposed various regulations in response to soaring costs associated with managing the distribution, storage, and retrieval of records. Additionally, security concerns around hand written signatures emerged as it became increasingly evident that these signatures, including the content they were assigned to, could be easily falsified.

Title CFR 21 Part 11 regulates electronic records and electronic signatures or ERES. Part 11 in particular outlines the criteria for which ERES are considered trusted, reliable, and equivalent to paper records. The following guide walks through the regulations and provides explanations on how implementing electronic signatures using GlobalSign's PDF Signing Certificates can help organizations meet some of the requirements associated with CFR 21 Part 11.

## GlobalSign's PDF Signing Certificates

GlobalSign's PDF Signing Certificates; Adobe Approved Trust List (AATL) and Adobe's Certified Document Services (predecessor to the AATL) produce explicitly trusted signatures in Adobe Reader and Acrobat Standard and Professional software. The type of certificate license you will require will depend on the number of users and volume of PDF documents which will require signatures:

- **Individual:** ideal for an individual with the need to sign PDFs (<2,000 signatures per year). If this is the solution you are looking for please proceed to [Appendix B: Purchasing Individual PDF Signing Certificates](#).
- **Enterprise PKI (EPKI):** ideal for organizations with multiple individuals with the need to sign PDFs and have the added benefit of managing all certificates in a central location. This centralizes lifecycle management including issuing, renewing, revoking, and reissuing. If this is the solution you are looking for please proceed to the next step, [Appendix C: Purchasing Multiple PDF Signing Certificates](#).

## Title CFR 21 Part 11 Audit Support

The following sections go through the regulations outlined in Title CFR 21 Part 11 which are related to and/or directly addressed by the usage of GlobalSign's PDF Signing Solutions. It is important to note, complete Title CFR 21 Part 11 compliance will require other resources and organization activity beyond the use of GlobalSign's certificates.

The following text is taken directly from the Title CFR 21 Part 11 guidelines. The complete regulations can be found on the [U.S. Food and Drug Administration \(FDA\) website](#).

## CFR 21 Part 11 Requirements mapping to GlobalSign PDF Signing service.

### Subpart A – General Provisions

#### Section 11.1 Scope

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service

Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically accepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

(f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

[62 FR 13464, Mar. 20, 1997, as amended at 69 FR 71655, Dec. 9, 2004]

## **Section 11.2 Implementation**

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

- (1) The requirements of this part are met; and
- (2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

*Note: It is the responsibility of the client to determine document applicability to CFR 21 Part 11.*

## **Section 11.3 Definitions**

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

- (1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).
- (2) Agency means the Food and Drug Administration.
- (3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
- (4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

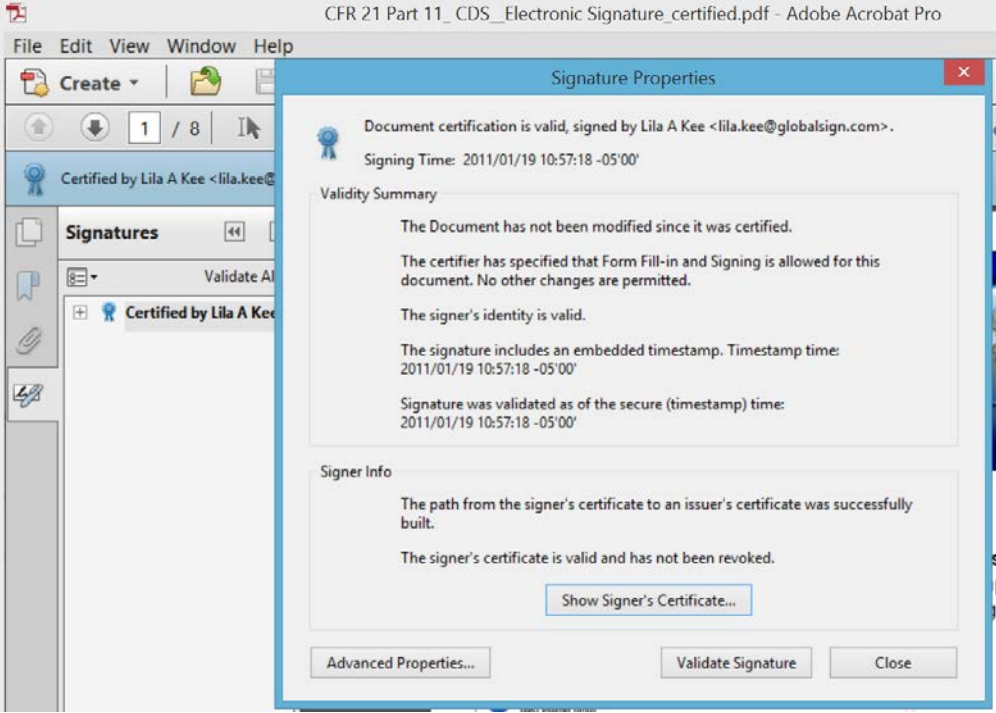
(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

## **Subpart B – Electronic Records**

### **Section 11.10 Controls for Closed Systems**

<p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:</p>
---

<p>(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<ol style="list-style-type: none"> <li>1. Organization to perform periodic checks.</li> <li>2. Adobe Acrobat using PDF Signing certificates implements Data Integrity by: The hash of the entire file is computed, using the bytes specified by the real ByteRange value <ul style="list-style-type: none"> <li>– Using a hash algorithm SHA-256. Acrobat always computes the hash for a document signature over the entire PDF file, starting from byte 0 and ending with the last byte in the physical file, but excluding the signature value bytes.</li> <li>– The hash value is encrypted with the signer's private key and a hex-encoded PKCS#7 object signature object is generated.</li> </ul> </li> </ol> <p>To validate a signature, the validator simply retrieves the signer's certificate and compares it to their own list of trusted certificates:</p> <ol style="list-style-type: none"> <li>1. The recipient's application generates a one-way hash of the document using the same algorithm the signer used, excluding the signature value.</li> <li>2. The encrypted hash value in the document is decrypted using the signer's public key.</li> <li>3. The decrypted hash value is compared to the locally generated hash value.</li> <li>4. If they are identical, the signature is reported as known.</li> </ol>
<p>(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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.</p>	<p>Organization to document storage and retrieval methods for documents, policy, and procedures.</p> <p>Adobe Acrobat PDFs signed with PDF Signer digital signatures produce human readable and tamper evident PDFs</p>

	<p>CFR 21 Part 11_ CDS_Electronic Signature_certified.pdf - Adobe Acrobat Pro</p>
<p>(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p>Organization to document record retention and retrieval methods, policy, and procedures.</p> <p>Adobe Reader and Acrobat default signature validations requires validation based on revocation check made at time of initial signature. This check is captured in the signature properties of the signed PDF. The signature will remain valid even past the signer and TSA certificate expiration date therefore supporting long term validation.</p>

Signature Verification Preferences

☒ Verify signatures when the document is opened

☐ When document has valid but untrusted signatures, prompt to review and trust signers

Verification Behavior

When Verifying:

☒ Use the document-specified method; prompt if unavailable

☐ Use the document-specified method; if unavailable, use default method

☐ Always use the default method: Adobe Default Security

☒ Require certificate revocation checking to succeed whenever possible during signature verification

☐ Ignore document validation information

Verification Time

Verify Signatures Using:

☒ Time at which the signature was created

☐ Secure time (timestamp) embedded in the signature

☐ Current time

☒ Use expired timestamps

Verification Information

Automatically add verification information when saving signed PDF:

☒ Ask when verification information is too big

☐ Always

☐ Never

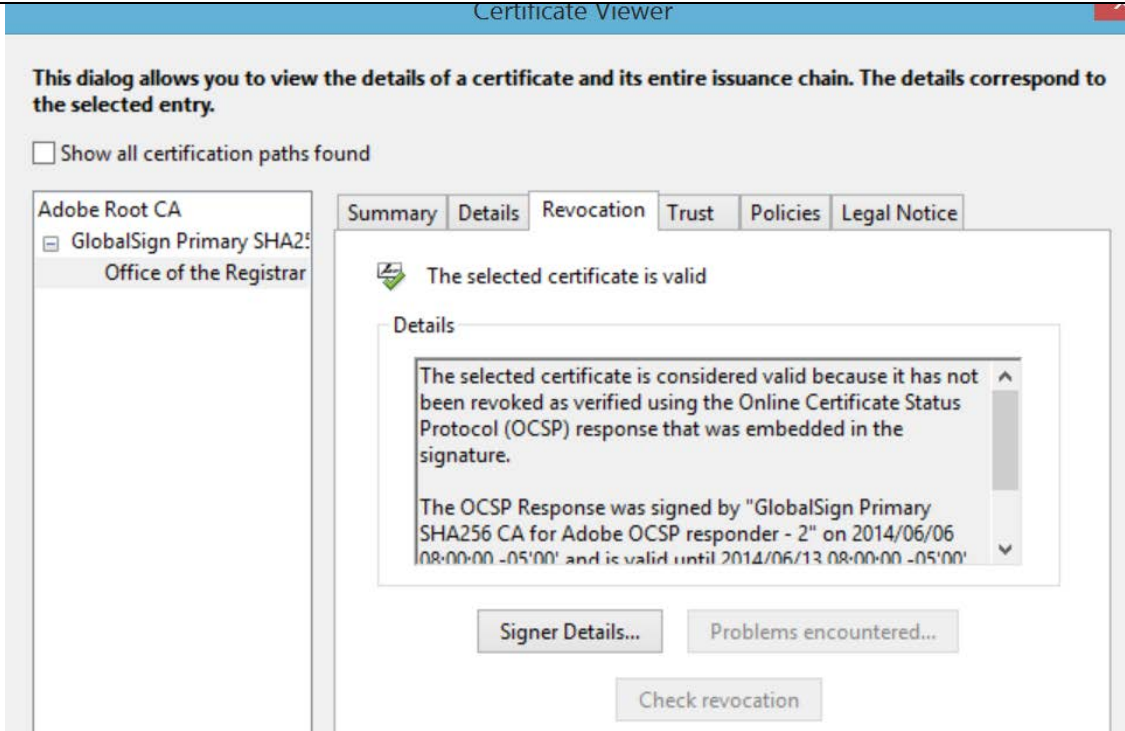
Windows Integration

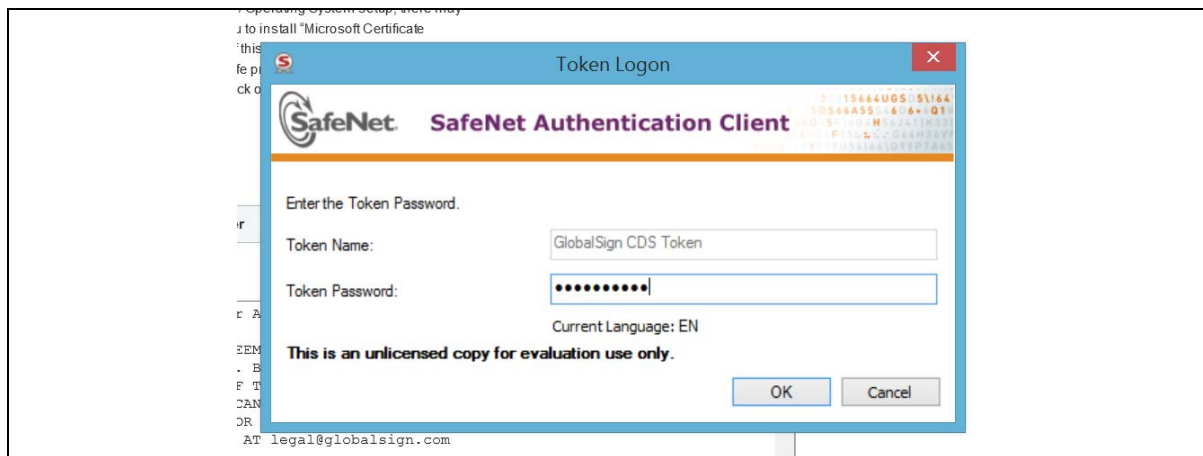
Trust ALL root certificates in the Windows Certificate Store for:

☐ Validating Signatures

☐ Validating Certified Documents

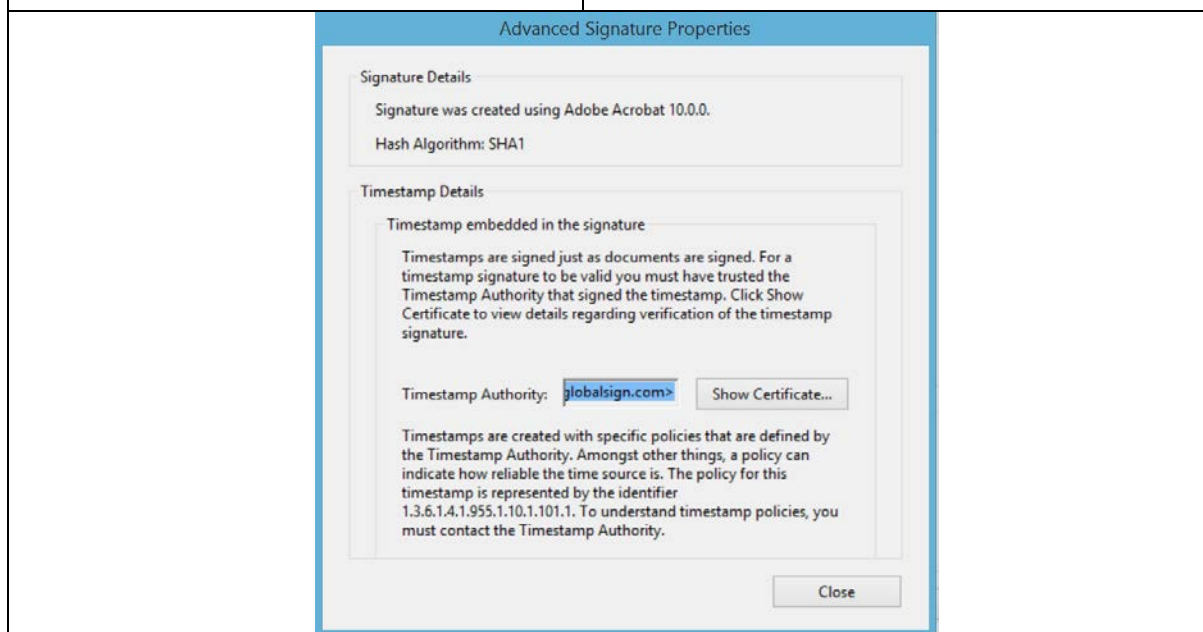


	
(d) Limiting system access to authorized individuals.	<p>Organization should only issue PDF Signing digital certificates onto GlobalSign furnished SafeNet eTokens to authorized individuals using internal HR or other identity verification policies. Once an authorized user is identified, the Organization EPKI administrator, acting as a local Registration Authority will register the user for a PDF Signer certificate and furnish a SafeNet USB eToken to perform the on token key generation and subsequent certificate installation.</p>



(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

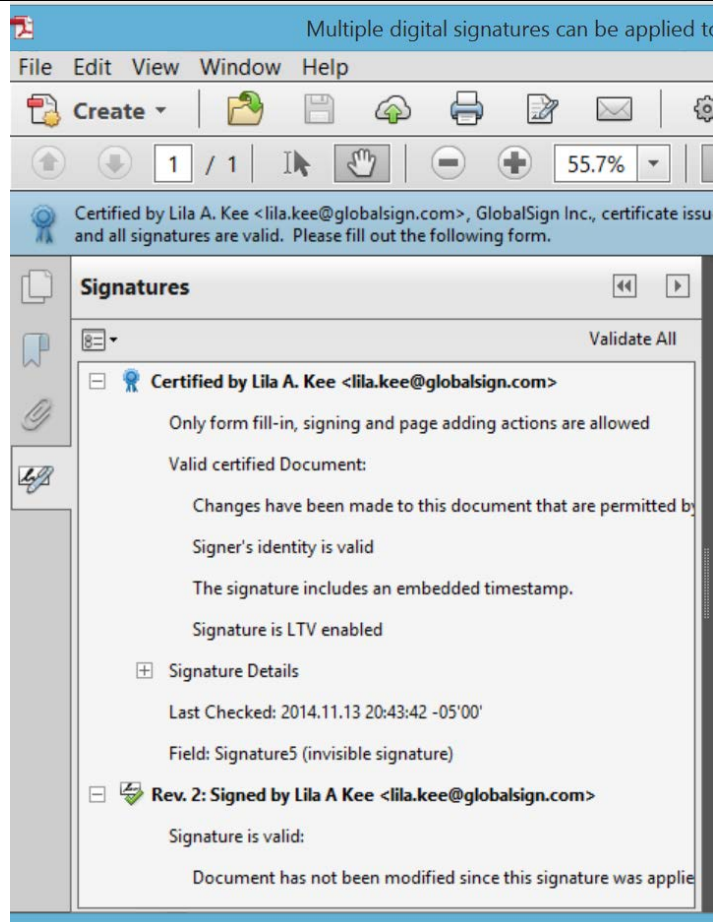
GlobalSign RFC 3161 trusted time clock is utilized in lieu of signer's local system clock. Organization is responsible for audit trail outside of PDF signatures.



(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Organization to document system checks.

Adobe Acrobat-Reader Signature panel provides exact order of signature sequence and document status after each signature was applied.



(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

Organization to document policy around how systems are accessed and utilized to perform electronic signatures by only authorized personnel.

*Following is an example:*

Internal vetting of personnel or non-organization Contingent workers assigned to Organization is done in the context of <XXX's> overall Human Resource (HR) and Security programs. Only current employees or contingent workers with active assignments in the Organization are eligible to receive a digital certificate issued by the Organization. Their identity is confirmed by the presence of their Employee Identification Badge. All employees are issued a photo identification badge and are requested to wear it at all times when inside the Organization facility. The Organization launched a program of Pre-Employment Background Screening. Screening has been implemented to verify the backgrounds of all job candidates to whom contingent job offers are made. A standard background screen includes Social Security verification, verification of highest level of education, and criminal conviction records. Optional background screens may also be requested based on the candidate's duties: employment, professional license/certification, and driving record. Organization also requires background checks and

	<p>identity verification be completed on contract personnel working at Organization locations.</p> <p><i>Note the use of Adobe seed values is one method to add further controls around signatures.</i></p> <p><a href="http://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf">http://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf</a></p>
<p><b>6.3.15 Controlling signature workflows via seed values</b></p> <p>PDF's support for seed values provides authors with field-level control over document behavior once it has been routed to the signer. A seed value specifies an attribute and attribute value, and the author can control whether the specified parameter is optional or required for any particular field.</p> <p>For example, you can use seed values to limit a user's choices when signing a particular signature field, such as requiring signing with a certificate issued by a particular CA. When a signer signs a "seeded" field, the author-specified behaviors are automatically invoked and enforced.</p> <p>If a field dictionary contains an SV entry referencing a seed value dictionary then that dictionary is used when the field is signed. An Ff entry specifies whether the other entries in the dictionary shall be honoured or whether they are merely recommendations. Acrobat's default handler supports all the seed values defined by the PDF standard. Acrobat provides APIs for seeding fields.</p>	
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Per organization policy.
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Per organization training policy.
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	<p>Organization to develop and administer written policies to individuals.</p> <p>GlobalSign certificate enrollment requires individual to accept certain obligations outlined in the Subscriber Agreement such as reporting compromises, providing truthful information. Organization can add additional obligation associated with company policy to this agreement through the EPKI Administrator interface.</p>

Here you may add additional subscriber terms to the Mandatory GlobalSign Subscriber Agreement.

GlobalSign Subscriber Agreement - Version 3.2

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY CANCEL THE ORDER WITHIN SEVEN (7) DAYS OF THE AVAILABILITY OF THE CERTIFICATE FOR A FULL REFUND. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT [legal@globalsign.com](mailto:legal@globalsign.com)

This GlobalSign Subscriber Agreement (the "Agreement") between GlobalSign and the Applicant or Subscriber is effective as of the date of the application for the Certificate (the "Effective Date").

1.0 Definitions and Incorporation by Reference

The following definitions are used throughout this Agreement:

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

Application Software Supplier: A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.

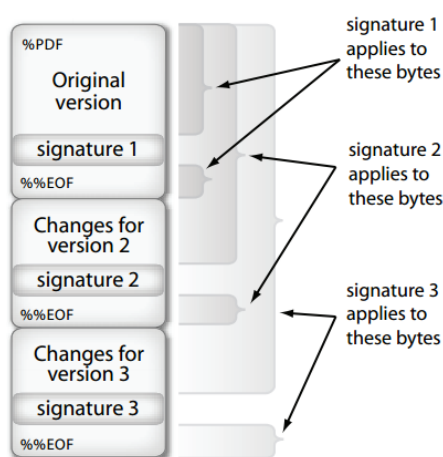
Authority Information Access: A Certificate extension that indicates how to

Back
Next

(k) Use of appropriate controls over systems documentation including:	
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	Organization specific
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Organization specific  Adobe provides an audit trail of changes to the PDF after each signature.

Each additional signature will cover the entire PDF file, from byte 0 to the last byte, excluding only the signature value for the current signature value. Figure 5 shows how signatures are created for a file with three signatures.

**Figure 5 Multiple signatures and incremental updates**



## Section 11.30 Controls for Open Systems

### Regulation:

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.

**Response:**


To address **Section 11.30** please reference the response in [Section 11.10](#).

Additionally, encryption can be added to PDF documents in one of two ways:

1. Encrypt with Certificates via Public Key Infrastructure technology: <http://blogs.adobe.com/security/2011/08/pdf-encryption-options.html>
2. Encrypt with Passwords: <https://helpx.adobe.com/acrobat/using/securing-pdfs-passwords.html>

GlobalSign PDF Signing certificate use strong cryptography based on 2048 RSA keys and SHA-256 Hashing algorithms. Private signing keys are stored on minimum FIPS 140-2 level 2 cryptographic hardware.

## Section 11.50 Signature Manifestations

<b>(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:</b>	
(1) The printed name of the signer;	<p>PDF Signing example using GlobalSign CDS certificate</p>  <p>Digitally signed by Lila A Kee  DN: c=US, st=NH, l=Portsmouth,  o=GlobalSign, Inc., cn=Lila A Kee,  email=lila.kee@globalsign.com  Reason: I approve this request  Date: 2014.11.14 11:21:04 -05'00'</p>
(2) The date and time when the signature was executed; and	See screen shot above. Note timestamp is based off GlobalSign RFC 3161 compliant trusted Time-stamping clock.
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	See screen shot above, specifically "Reason". See <a href="#">Appendix A</a> for an overview of how to add a reason (meaning) code to a signature.
<b>(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).</b>	
<p>See screen shot above. Note all information is in human readable format.  The record is embedded in the PDF (not detached).</p>	

## Section 11.70 Signature/Record Linking

**Regulation:**

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.

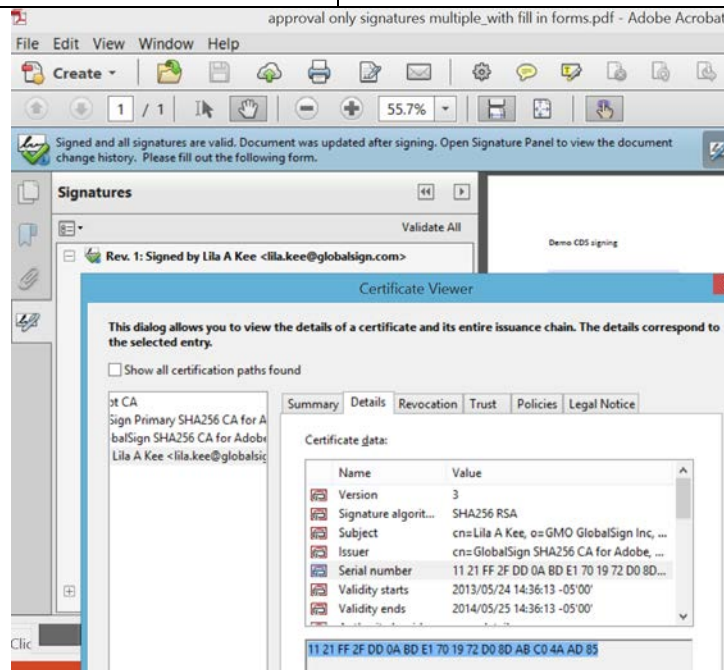
**Response:**

Adobe Signatures are linked to PDFs through recording all cryptographic and other related functions in the signature properties embedded in the Signature Panel of the PDF.

**Section 11.100 General Requirements**

(a) Each electronic signature shall be unique to one individual and shall not be reused by or reassigned to anyone else.

Signatures are cryptographically tied to a verified identity (GlobalSign as the RA for the organization and the Organization as the LRA for the individual). A unique serial number and Issuing CA tied to the subject distinguish name included in the digital certificate binds the individual's identity to the signature.



(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.


The organization verifies the individual through its normal HR or contracting processes. Here the organization would specify how that is does i.e. background check, examination of government furnished ID, references, etc.



	<p>Verified individuals are often depicted in the Organization's directory e.g. Active Directory. The EPKI Administrator follows the appropriate identity verification process e.g. check employee badge, directory, manager etc. and issues certificates to approved individuals.</p>																
<div> <h3>Certificate Identity Details</h3> <table> <tr> <td>Common Name <small>Required</small></td><td>Julie Olinski</td></tr> <tr> <td>Organization</td><td>GMO GlobalSign Inc</td></tr> <tr> <td>Organizational Unit</td><td></td></tr> <tr> <td>Country</td><td>United States - US</td></tr> <tr> <td>Email Address <small>Required</small></td><td>julie.olinski@globalsign.com</td></tr> <tr> <td>Pickup Password <small>Required</small></td><td> <div>*****</div> <div>           Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9)           <div>             Password Generation             <div></div> </div> </div> <div>When the password automatic operation generation button is pressed, a random password automatic construction is set.</div> </td></tr> <tr> <td>Pickup Password (re-enter) <small>Required</small></td><td>*****</td></tr> <tr> <td>Memo</td><td> <div>           I examined Julie's employee badge checked active status in directory and obtained approval from her manager         </div> </td></tr> </table> <div> <div>Back</div> <div>Next</div> </div> </div>		Common Name <small>Required</small>	Julie Olinski	Organization	GMO GlobalSign Inc	Organizational Unit		Country	United States - US	Email Address <small>Required</small>	julie.olinski@globalsign.com	Pickup Password <small>Required</small>	<div>*****</div> <div>           Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9)           <div>             Password Generation             <div></div> </div> </div> <div>When the password automatic operation generation button is pressed, a random password automatic construction is set.</div>	Pickup Password (re-enter) <small>Required</small>	*****	Memo	<div>           I examined Julie's employee badge checked active status in directory and obtained approval from her manager         </div>
Common Name <small>Required</small>	Julie Olinski																
Organization	GMO GlobalSign Inc																
Organizational Unit																	
Country	United States - US																
Email Address <small>Required</small>	julie.olinski@globalsign.com																
Pickup Password <small>Required</small>	<div>*****</div> <div>           Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9)           <div>             Password Generation             <div></div> </div> </div> <div>When the password automatic operation generation button is pressed, a random password automatic construction is set.</div>																
Pickup Password (re-enter) <small>Required</small>	*****																
Memo	<div>           I examined Julie's employee badge checked active status in directory and obtained approval from her manager         </div>																
(c) Persons using electronic signatures shall prior to or at the time of such use certify to the agency that the electronic signatures in their system used on or after August 20 1997 are intended to be the legally binding equivalent of traditional handwritten signatures.	Submit certification																
(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature to the Office of Regional Operations (HFC-100) 5600 Fishers Lane Rockville MD 20857.	Submit certification																
(2) Persons using electronic signatures shall upon agency request provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Provide necessary information upon request																

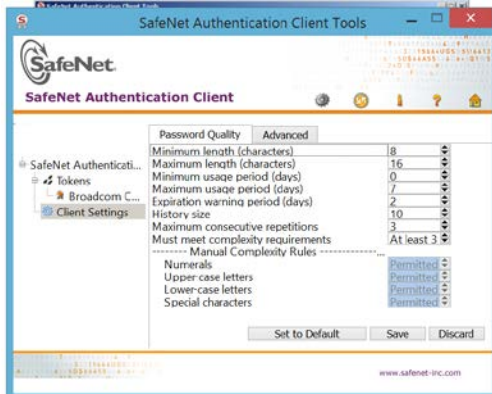


## Section 11.200 Electronic Signature Components and Controls

(a) Electronic signatures that are not based upon biometrics shall:	
(1) Employ at least two distinct identification components such as an identification code and password.	Signers must authenticate with both a PIN and a physical USB token before signing. Prior to accessing Acrobat, user should also be required to log in with desktop password or alternative
	
(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.	SafeNet Authentication Client (SAC) can be configured so the PIN (password) is required each time the Token is being accessed while in a Windows authenticated desktop.
(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.	<p><b>Defining Automatic Logoff</b></p> <p>You can determine whether tokens are automatically logged off following a period of token inactivity, even if the tokens are not disconnected.</p> <p>After a token is logged off, the user must enter the Token Password again before the token contents can be accessed.</p> <p><b>To define the automatic logoff setting:</b></p> <ol style="list-style-type: none"> <li>1. Open SafeNet Authentication Client Tools <i>Advanced View</i>. See <i>Opening the Advanced View</i> on page 14.</li> <li>2. In the left pane, select <b>Client Settings</b>.</li> <li>3. In the right pane, select the <b>Advanced</b> tab.</li> <li>4. In the <i>Automatic logoff after token inactivity</i> drop-down list, select one of the following: <ul style="list-style-type: none"> <li>◆ <b>Never:</b> The Token Password must be entered once, and the token remains logged on as long as it remains connected.</li> <li>◆ <b>Always:</b> The Token Password must be entered each time the token contents are accessed.</li> <li>◆ <b>After:</b> The Token Password must be entered if the number of minutes set in the text box has passed since the last token activity. Set the number of minutes in the text box (1 - 254).</li> </ul> </li> <li>5. Do one of the following: <ul style="list-style-type: none"> <li>◆ To save your changes, click <b>Save</b>.</li> <li>◆ To ignore your changes, click <b>Discard</b>.</li> </ul> </li> </ol>
(2) Be used only by their genuine owners; and	USB tokens are furnished to individuals and not to be shared. Each Token has a serial number that should be assigned and recorded to the individual. Only the individual has knowledge of the Token PIN.
(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.	GlobalSign configures USB tokens to require the individual log on to the token with their unique PIN. Unsuccessful attempts greater than 9 will permanently lock out the user. Replacement certificates are free of charge, therefore locked out tokens can be initialized by the user or Administrator and replacement certificates enrolled through EPKI reissue function.

<p>Certificate action information</p> <table border="1"> <thead> <tr> <th>Action details</th><th>Action date</th><th>Result</th><th>User Id</th></tr> </thead> <tbody> <tr> <td>ORDER_REQUEST</td><td>10/03/2014 10:42:41(GMT-05:00)</td><td>SUCCESS</td><td>PAR12694_lakee1</td></tr> <tr> <td>CERT_ISSUE_WAIT</td><td>10/03/2014 10:46:02(GMT-05:00)</td><td>SUCCESS</td><td>PAR12694_lakee1</td></tr> <tr> <td>CERT_ISSUE</td><td>10/03/2014 10:52:20(GMT-05:00)</td><td>SUCCESS</td><td>PAR12694_lakee1</td></tr> </tbody> </table> <p> <a href="#">Revoke Certificate</a> <a href="#">Reissue Certificate</a> <a href="#">Mail History</a> </p>		Action details	Action date	Result	User Id	ORDER_REQUEST	10/03/2014 10:42:41(GMT-05:00)	SUCCESS	PAR12694_lakee1	CERT_ISSUE_WAIT	10/03/2014 10:46:02(GMT-05:00)	SUCCESS	PAR12694_lakee1	CERT_ISSUE	10/03/2014 10:52:20(GMT-05:00)	SUCCESS	PAR12694_lakee1	<p>(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.</p>	<p>Not applicable to PDF Signing certificates.</p>
Action details	Action date	Result	User Id																
ORDER_REQUEST	10/03/2014 10:42:41(GMT-05:00)	SUCCESS	PAR12694_lakee1																
CERT_ISSUE_WAIT	10/03/2014 10:46:02(GMT-05:00)	SUCCESS	PAR12694_lakee1																
CERT_ISSUE	10/03/2014 10:52:20(GMT-05:00)	SUCCESS	PAR12694_lakee1																

## Section 11.300 Controls for Identification Codes/Passwords

<p><b>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:</b></p>			
<p>(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</p>		<p>Organization policy.</p>	
<p>(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).</p>		<p>The Password Quality feature enables the administrator to set certain complexity and usage requirements for Token Passwords. The SafeNet Authentication Client allows for forced periodic password reset and password strength.</p> 	
<p>(c) Following loss management procedures to electronically de-authorize 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.</p>		<p>GlobalSign configures USB tokens to require the individual log on to the token with their unique PIN. Unsuccessful attempts greater than 9 will permanently lock out the user. Replacement certificates are free of charge, therefore locked out tokens can be initialized by the user or Administrator and replacement certificates enrolled through EPKI.</p> <p>Lost or suspected compromised keys should be immediately reported to the EPKI Administrator who shall immediately revoke the user's certificate through the EPKI Portal. GlobalSign provides for 10% spare USB token for immediate re-</p>	

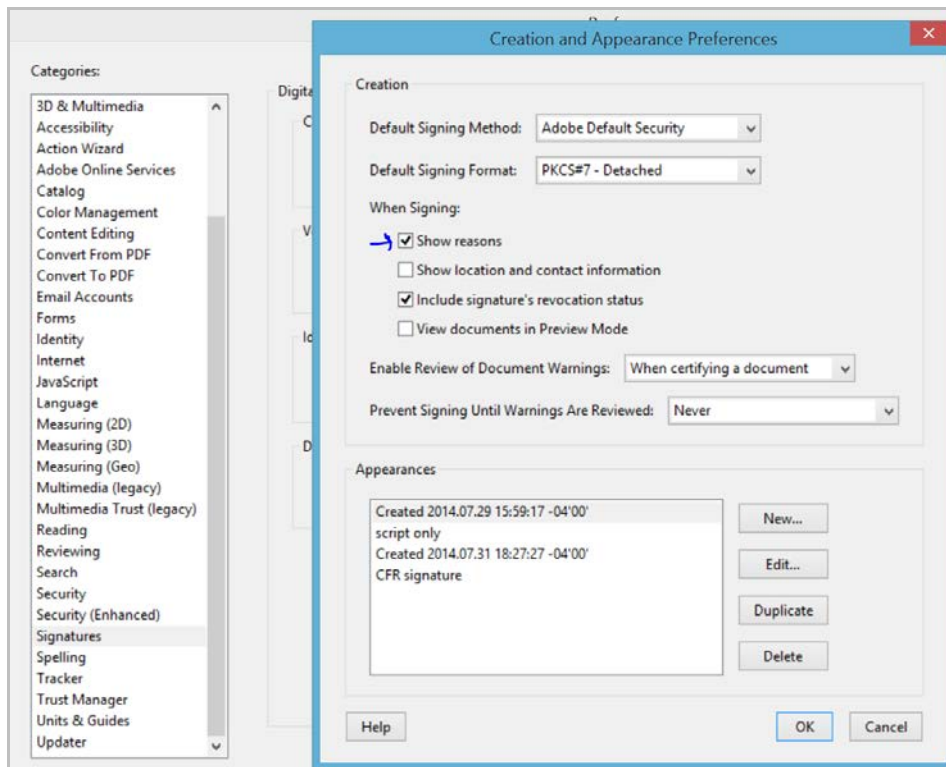
	provisioning of the signing credential																
<div>Certificate action information</div> <table><tr><th>Action details</th><th>Action date</th><th>Result</th><th>User Id</th></tr><tr><td>ORDER_REQUEST</td><td>10/03/2014 10:42:41(GMT-05:00)</td><td>SUCCESS</td><td>PAR12694_lakeef</td></tr><tr><td>CERT_ISSUE_WAIT</td><td>10/03/2014 10:46:02(GMT-05:00)</td><td>SUCCESS</td><td>PAR12694_lakeef</td></tr><tr><td>CERT_ISSUE</td><td>10/03/2014 10:52:20(GMT-05:00)</td><td>SUCCESS</td><td>PAR12694_lakeef</td></tr></table> <div><a href="#">Revoke Certificate</a> <a href="#">Reissue Certificate</a> <a href="#">Mail History</a></div>		Action details	Action date	Result	User Id	ORDER_REQUEST	10/03/2014 10:42:41(GMT-05:00)	SUCCESS	PAR12694_lakeef	CERT_ISSUE_WAIT	10/03/2014 10:46:02(GMT-05:00)	SUCCESS	PAR12694_lakeef	CERT_ISSUE	10/03/2014 10:52:20(GMT-05:00)	SUCCESS	PAR12694_lakeef
Action details	Action date	Result	User Id														
ORDER_REQUEST	10/03/2014 10:42:41(GMT-05:00)	SUCCESS	PAR12694_lakeef														
CERT_ISSUE_WAIT	10/03/2014 10:46:02(GMT-05:00)	SUCCESS	PAR12694_lakeef														
CERT_ISSUE	10/03/2014 10:52:20(GMT-05:00)	SUCCESS	PAR12694_lakeef														
(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.	<p>GlobalSign configures USB tokens to require the individual log on to the token with their unique PIN. Unsuccessful attempts greater than 9 will permanently lock out the user. Replacement certificates are free of charge, therefore locked out tokens can be initialized by the user or Administrator and replacement certificates enrolled through EPKI.</p> <p>Revoked certificates will no longer be able to produced trusted signatures. Signatures produced prior to revocation as long as the revocation check was embedded at time of authorship will remain valid.</p>																
(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.	Not applicable to PDF Signing.																

## Appendices

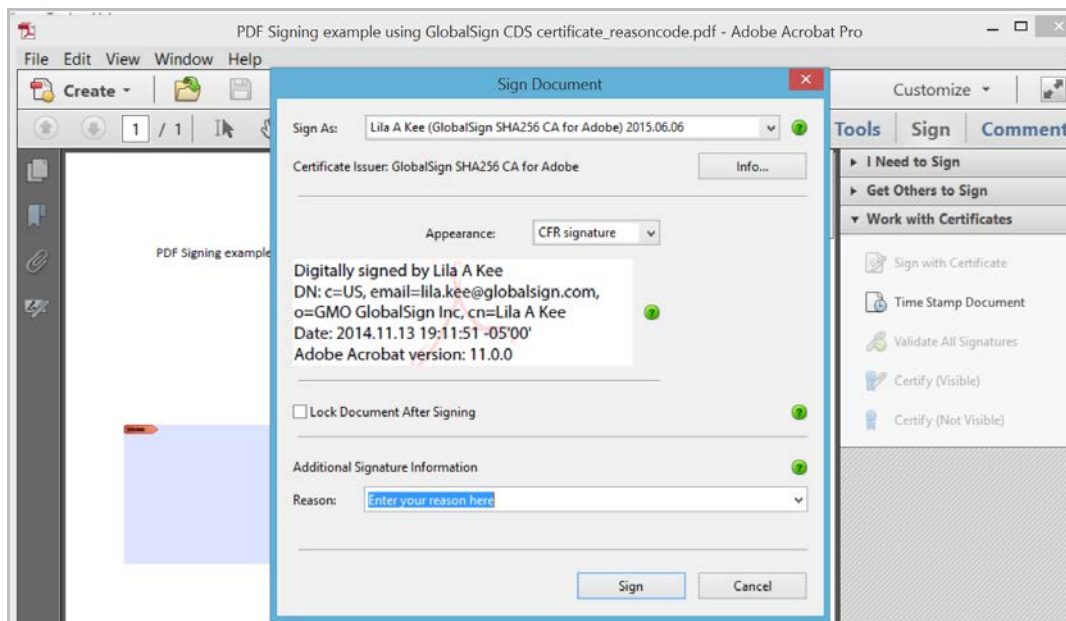
### Appendix A – Configure Reason Code in Adobe Acrobat

The following screenshots display how you can configure Adobe Acrobat to include a reason (meaning) code with the signature. This is required in Section 11.50 Signature Manifestations.

#### Creation and Appearance Preferences



### Sign Document – Reason Field



## Appendix B – Purchasing Individual PDF Signing Certificates

The type of certificate license you will require will depend on the number of users and volume of PDF documents which will require signatures. This section is to explain the ordering process for individuals with the need to sign PDFs (<2,000 signatures per year). If you are looking for a greater volume of certificates please review the section on [GlobalSign Certificates](#).

1. Navigate to <https://www.globalsign.com/pdf-signing/> . Click **Buy Now**
2. Click **Select Individual** Certificates
3. Select your region from the dropdown menu and click **Select & Continue**.
4. Your order will then be processed and the **Certificate Application** will appear. Complete all required information of the application and click **Next**. *Note: this is not the vetted certificate information.*

Account Details	
Please specify details for your account. Your account contact will receive notices regarding your Certificate application and will be the main contact associated with your GlobalSign Certificate Center (GCC) account. If you are applying on behalf of someone else, enter their details, and you can specify an additional Technical Contact for yourself later in the application process.	
First Name <small>Required</small>	<input type="text"/>
Middle Name or Initial	<input type="text"/>
Last Name <small>Required</small>	<input type="text"/>
Email Address <small>Required</small>	<input type="text"/> <small>Please check email is accurate, this email address will be used in the application process</small>
Phone Number <small>Required</small>	<input type="text"/> <small>e.g. 603-570-7060 or 01622 786766</small>
Fax Number	<input type="text"/> <small>e.g. 603-570-7059 or 01622 662255</small>
Organization Name <small>Required</small>	<input type="text"/> <small>Specify the Organization Registered Name in full, including Inc, Ltd, NV, Plc etc</small>
Department	<input type="text"/>
Street Address 1 <small>Required</small>	<input type="text"/> <small>e.g. Two International Drive</small>
Street Address 2	<input type="text"/> <small>e.g. Suite 330</small>
City <small>Required</small>	<input type="text"/>
State / County <small>Required</small>	<input type="text"/>

You will also need to choose a username and password. An account number (PAR####) will be appended to the username you choose. Click **Next** to continue.

GlobalSign Certificate Center (GCC) Login Details	
Your GCC account allows you to manage all your GlobalSign Certificates and provides fast access to ordering additional products and renewing, reissuing and revoking current Certificates. Please create a memorable Username and Password.	
Username <small>Required</small>	<input type="text"/> <small>Username is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9)</small>
Password <small>Required</small>	<input type="password"/> <small>Password is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9)</small>
Password(re-enter) <small>Required</small>	<input type="password"/>
<input type="button" value="Next"/>	

5. Confirm your account information and review the Terms of Service Agreement. Be sure to double check that all information is entered correctly. Click **Next** to continue.
6. Choose a validity period to be applied to your license pack (1-3 years). Click **Next**.

- Next, complete the **Certificate Identity Details**. These details will be vetted and included as the certified identity within your issued certificate.

**Important** - make sure the details entered are correct as GlobalSign will vet the details you include.

**Important** - Establish a one-time Pickup Password. **You will need this password to install** the certificate onto your device. If you forget this password, you will need to resubmit your order. Please copy it somewhere safe.

**Optional** - Add an additional technical contact (this is commonly used when you are applying on behalf of someone else).

Click **Next** to continue.

### Create Temporary Pickup Password

Please create a temporary pickup password. You will only need this during the installation process. This is not the same as your account password.

If you forget this password you will need to resubmit your order. Please copy it somewhere safe.

Pickup Password <b>Required</b>	<input type="password"/>
Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9)	
Pickup Password (re-enter) <b>Required</b>	<input type="password"/>

☒ **Required** I have copied this password to a safe location

### Specify an Additional Technical Contact

If you are applying on behalf of someone else, you may specify an additional Technical Contact. The Technical Contact is typically the person who is responsible for the application process and collection of the issued Certificate. Click the Enter Technical Contact Details link to create the additional contact.

If you are applying for yourself, you do not need an additional Technical Contact, so please click Next.

NOTE: For PersonalSign 3 Pro applications the issued certificate will not be sent to the Technical Contact.

[Enter Technical Contact Information](#)

- Complete the payment details.
- Confirm the details you have entered and agree to the **DocumentSign Subscriber Agreement**. Click **Next** to continue.
- A confirmation email will now be sent to the email address you provided earlier. To approve the application, you need to click the approval link within the approval email. Only if you approve the application will the certificate be issued.
- Review the application details and **APPROVE** the application.

Once you have successfully ordered your PDF Signing Certificate and your application will be sent to our vetting team. Vetting your application details can take **up to 2-3 business days**. Once the vetting process is complete, you will receive an email notifying you of its completion. Once the vetting process is complete please proceed to [Step 3 – Installing Your Certificate](#).

## Appendix C - Purchasing Multiple PDF Signing Certificates

### Step 1 – Establishing an EPKI Account

If you do not already have a GlobalSign EPKI Account, you will need to register for an EPKI account and setup a Certificate Profile. A Certificate Profile will serve as a pre-vetted organization template containing the organization's identity records (such as organization name, city, state, etc.) that end user certificate requests will be issued from. Verifying the organization's identity associated with a profile typically **takes between 2 and 3 business days**.

If you already have an EPKI Account, please proceed to [Step 2- Registering Users for PDF Signing Certificates](#).

If you do not already have an EPKI Account, please contact your Account Manager or email [sales-us@globalsign.com](mailto:sales-us@globalsign.com) to obtain the EPKI Account signup link.

1. Using the EPKI signup link, register for an EPKI account by entering your account details. *Note: this is not the vetted profile information.*

Account Details	
Please specify details for your account. Your account contact will receive notices regarding your Certificate application and will be the main contact associated with your GlobalSign Certificate Center (GCC) account. If you are applying on behalf of someone else, enter their details, and you can specify an additional Technical Contact for yourself later in the application process.	
First Name <small>Required</small>	<input type="text"/>
Middle Name or Initial	<input type="text"/>
Last Name <small>Required</small>	<input type="text"/>
Email Address <small>Required</small>	<input type="text"/> <small>Please check email is accurate, this email address will be used in the application process</small>
Phone Number <small>Required</small>	<input type="text"/> <small>e.g. 603-570-7060 or 01622 766766</small>
Fax Number	<input type="text"/> <small>e.g. 603-570-7059 or 01622 662255</small>
Organization Name <small>Required</small>	<input type="text"/> <small>Specify the Organization Registered Name in full, including Inc, Ltd, NV, Plc etc</small>
Department	<input type="text"/>
Street Address 1 <small>Required</small>	<input type="text"/> <small>e.g. Two International Drive</small>
Street Address 2	<input type="text"/> <small>e.g. Suite 330</small>
City <small>Required</small>	<input type="text"/>
State / County <small>Required</small>	<input type="text"/>

2. Choose a username and password. An account number (PAR####) will be appended to the username you choose. Click **Next** to continue.

GlobalSign Certificate Center (GCC) Login Details	
Your GCC account allows you to manage all your GlobalSign Certificates and provides fast access to ordering additional products and renewing, reissuing and revoking current Certificates. Please create a memorable Username and Password.	
Username <small>Required</small>	<input type="text"/> <small>Username is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9)</small>
Password <small>Required</small>	<input type="password"/> <small>Password is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9)</small>
Password(re-enter) <small>Required</small>	<input type="password"/>

Next

3. Confirm your account information and review the Terms of Service Agreement. Be sure to double check that all information is entered correctly. Click **Next** to continue.
4. Choose the license pack size of Identity Certificates you wish to purchase. Click **Next**.
5. Choose a validity period to be applied to your license pack (1-3 years).

**Optional** - Add an additional technical contact (this is commonly used when you are applying on behalf of someone else). Click **Next** to complete.

6. Enter the Certificate Profile Details. These details will be vetted and included as the certified identity within your issued certificates. Click **Next** to continue.

**Important** - make sure the details entered are correct as GlobalSign will vet the details you include.

### Certificate Profile Details

These details will be vetted and included as the certified identity within your issued Certificate. Make sure the details entered are correct - we will vet the details you include. To assist you, some details will be pre-populated from previous pages or from your GCC account details, you may overwrite these if needed.

Note: Within the form below you have the ability to define the certificates DistinguishedName (DN). One optional element is a freeform Organizational Unit (OU) description. The OU field allows you to enter a value that suits your business needs with a description such as "Marketing Team Building 5" for example. It is not mandatory to enter this but please note that if you choose to 'Lock a unique OU' then this means that the description you have chosen cannot be used again and is unique to this profile. An example of where you might choose to do this is for client authentication situations where each certificate needs one or two fixed unique strings to allow access such as 'O' and 'OU'.

Organization <small>Required</small>	<input type="text" value="The Max, Inc."/>
Organizational Unit <small>Optional unless locked as unique</small>	<div><input type="text"/> <input type="text"/> <input type="text"/></div> <div><input type="checkbox"/> Lock a unique OU</div>
Locality <small>Optional</small>	<input type="text" value="Bayside"/>
State or Province <small>Optional</small>	<input type="text" value="CA"/>
Country <small>Required</small>	<input type="text" value="United States - US"/>

7. Complete the payment details.
8. Confirm your order details. Review and agree to the EPKI Service Agreement. Click **Next** when finished.
9. The next screen will display your username and information about your profile. Save this information for your records.

### Application Completed

User ID	PAR96168_savedbythebell
License ID	ML201312032352
Profile ID	MP201312031637

Once you have successfully created an EPKI account, your information will be sent to our vetting team. Vetting your organization details can take **up to 2-3 business days**. Once the vetting process is complete, you will receive an email notifying you of its completion.

Once your EPKI account is setup and established, please continue to [Step 2 – Registering Users for PDF Signing Certificates](#).

## Step 2 – Registering Users for PDF Signing Certificates

There are a few options that the EPKI Administrator can use to “invite” users to apply for pre-approved digital certificates:

- **Individual** – Order Certificates: *Ideal for issuing up to 25 Certificates*
- **Multiple** – Order Certificate BULK: *Ideal for issuing more than 25 Certificates*

The following steps will walk you through the individual invite process using the **Order Certificates** function. For additional instructions please view the REGISTER USERS FOR CERTIFICATES VIA EPKI ADMINISTRATOR section of the EPKI Administrator Guide: <https://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf>



1. Login to your GlobalSign Certificate Center (GCC) account at [www.globalsign.com/login/](http://www.globalsign.com/login/).
2. Select the “Enterprise PKI” tab found on the top menu bar.



**Please note:** if this is your first time logging in your menu options will be limited. For first time users, you will need to enroll for an “EPKI Administrator Certificate”, which is an authentication certificate needed to access secure areas of GCC such as the Certificate Management section. Please follow the steps below to enroll for your administrator certificate.

- a. Click the **View Admin Menu Options** link in the left hand menu to start the enrollment process.
- b. Follow the prompted steps to enroll and install your certificate.
- c. If you need further assistance and detailed instructions on how to enroll for your EPKI Administrator Certificate, please see our administrator guide located at <https://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf>

3. In the left hand menu, select **Order Certificates** under My Certificates.



4. Next, select the **Profile** and **License** pack that you want to issue the certificate from. In most cases there will be only one option for each area. Click **Next**.
- 5.

 A screenshot of the 'Product Details' step in the GlobalSign enrollment process. It shows a progress bar with '1. Product Details' and '2. Completed'. Below the progress bar are three steps: 'Select Profile', 'Certificate Identity Details', and 'Confirm Details'. The 'Product Details' section contains two tables. The first table, 'Profile', has columns for Profile ID, BaseDN, Organization, and Organization Unit. The second table, 'License', has columns for Service and License Unused number. A 'Next' button is at the bottom.
 

Profile ID	BaseDN	Organization	Organization Unit
MP20130927	Disabled	GlobalSign, Inc	

Service	License Unused number
Enterprise PKI AATL Signing For Adobe PDF 1 year	1

6. Next, complete the **Certificate Identity Details**.  
Provide the end-user identity details.
  - a. **Important** - Establish a one-time Pickup Password. **The user will need this password to install** the certificate onto their device; you must deliver this Pickup Password in an out-of-band method.

- b. **Optional** - enter a reason or note associated with the registration. This note will appear in the Order History section of EPKI and may be useful for audit purposes.

Click **Next** to continue.

The screenshot shows a web application interface for 'ENTERPRISE PKI'. At the top, there are tabs for 'SSL CERTIFICATES', 'MANAGED SSL', 'CODE SIGNING, PERSONAL SIGN, PDF SIGNING for ADOBE CDS', and 'ENTERPRISE PKI'. Below the tabs is a 'Product Selection' header. A progress bar shows two steps: '1. Product Details' (active) and '2. Completed'. Below the progress bar is a navigation bar with three buttons: 'Select Profile', 'Certificate Identity Details' (active), and 'Confirm Details'. The main section is titled 'Certificate Identity Details' and contains a form with the following fields:

Common Name <i>Required</i>	<input type="text"/>
Organization	GlobalSign Test
Organizational Unit (Profile)	AD Client Auth Test
Organizational Unit	<input type="text"/>
Locality	Portsmouth
State or Province	NH
Country	United States - US
Email Address <i>Required</i>	<input type="text"/>
Pickup Password <i>Required</i>	<input type="text"/> <small>Password must be a minimum of 8 characters. Alpha-numeric values only (A-Z, 0-9)</small> <a href="#">Password Generation</a> <small>When the password automatic operation generation button is pressed, a random password automatic construction is set.</small>
Pickup Password (re-enter) <i>Required</i>	<input type="text"/>
Memo	<div><div></div><div></div></div>

At the bottom of the form are two buttons: 'Back' and 'Next'. The 'Next' button is highlighted with a green border.

7. Review and confirm registration details. If satisfied, click **Next** to complete the registration.

PAR52316\_kimj Logout [Technical Support Center](#) [Contact Us](#)  
TEL | US +1 877 775 4562 | EMEA +32 16 891900 | UK +44 1622 766786

SSL CERTIFICATES MANAGED SSL CODE SIGNING, PERSONALSIGN, PDF SIGNING for ADOBE CDS ENTERPRISE PKI

## Product Selection

1. Product Details 2. Completed

Select Profile >> Certificate Identity Details >> **Confirm Details**

### Confirm Details

#### Product Details

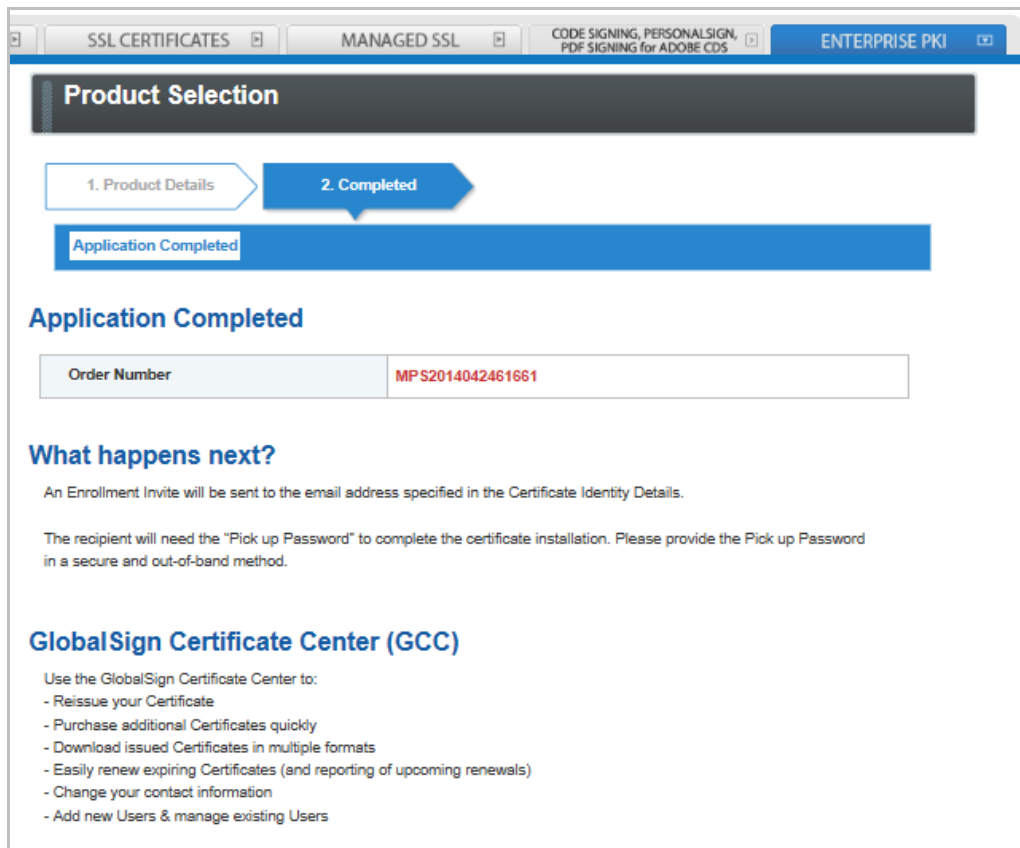
Profile ID	MP201204040879
License ID	ML201404212667

#### Certificate Identity Details

Common Name	PDF Signing
Organization	GlobalSign Test
Organizational Unit	AD Client Auth Test
Locality	Portsmouth
State or Province	NH
Country	United States - US
Email Address	@globalsign.com
Memo	

[Back](#) [Next](#)

The registration is now complete and as indicated the Enrollment Invite will be sent to the email address specified in the Certificate Identity Details. Please continue to [Step 3 – Installing Your Certificate](#) to see how the user will complete the certificate pick-up and installation.



### Step 3 – Installing Your Certificate

Now that you have issued a PDF Signing Certificate it will need to be installed on a USB token. GlobalSign has standardized on offering SafeNet iKey USB tokens which will be shipped to you once the vetting process has been completed.

Once you receive the tokens you will need to take the following steps to complete the installation:

- Install the GlobalSign SafeNet Utility Drivers
- Initialize the USB token and set your USB token password
- Install the GlobalSign certificate on the USB token

*Note the certificate must be installed within thirty (30) days from the date the order was placed.*

For detailed instructions on the steps outlined above please review the GlobalSign PDF Signing Certificates Installation Support guide: <https://support.globalsign.com/customer/en/portal/articles/1999625-download-and-install-aatl-or-cds-certificate>

## Conclusion

Title CFR 21 Part 11 regulates electronic records and electronic signatures or ERES. This regulation has been imposed by the FDA in response to soaring costs associated with managing the distribution, storage, and retrieval of records as well as security concerns around hand written signatures as it has become increasingly evident that these signatures, including the content they were assigned to, could be easily falsified.

Part 11 in particular outlines the criteria for which ERES are considered trusted, reliable, and equivalent to paper records. GlobalSign's PDF Signing certificates can be implemented to address many of the requirements to be Part 11 compliant.

## GlobalSign Contact Information

<b>GlobalSign Americas</b> Tel: 1-877-775-4562 <a href="http://www.globalsign.com">www.globalsign.com</a> <a href="mailto:sales-us@globalsign.com">sales-us@globalsign.com</a>	<b>GlobalSign EU</b> Tel: +32 16 891900 <a href="http://www.globalsign.eu">www.globalsign.eu</a> <a href="mailto:sales@globalsign.com">sales@globalsign.com</a>	<b>GlobalSign UK</b> Tel: +44 1622 766766 <a href="http://www.globalsign.co.uk">www.globalsign.co.uk</a> <a href="mailto:sales@globalsign.com">sales@globalsign.com</a>
<b>GlobalSign FR</b> Tel: +33 1 82 88 01 24 <a href="http://www.globalsign.fr">www.globalsign.fr</a> <a href="mailto:ventes@globalsign.com">ventes@globalsign.com</a>	<b>GlobalSign DE</b> Tel: +49 800 723 798 0 <a href="http://www.globalsign.de">www.globalsign.de</a> <a href="mailto:verkauf@globalsign.com">verkauf@globalsign.com</a>	<b>GlobalSign NL</b> Tel: +31 20 8908021 <a href="http://www.globalsign.nl">www.globalsign.nl</a> <a href="mailto:verkoop@globalsign.com">verkoop@globalsign.com</a>