Digital Signatures System Overview

Outline

- Benefits of a Digital Signatures system
- How the system secures documents from post-approval changes
- How everyone knows that your signature is actually your signature
- What your responsibilities are with regard to the use of Digital Signatures
- Where you can go for additional information

Features of a Digital Signature System

- Efficiency, Speed, Accuracy
  - No more print, sign, scan
  - Simply draw a rectangle on a PDF document, insert your USB token and enter your password

- Key Security Features – guarantees:
  - Authenticity of signature - Ensures that you and only you can put your digital signature to a document
  - Integrity of document – Verifies that the document you signed has not changed since you signed it
  - Non-repudiation - Ensures that you cannot deny signing a document

Key Concept:
If electronic/digital signatures are used on GxP documents (predicate rules), they must be 21 CFR Part 11 and/or Eudralex Chapter 4 Annex 11 compliant.

This Digital Signature Solution

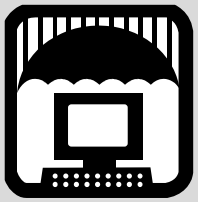
Technology

Commercial Trusted Certificate Services

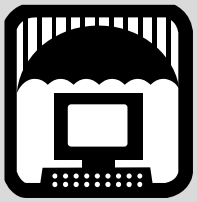
Safenet Hardware Token with Your Digital ID

Adobe Reader and Acrobat

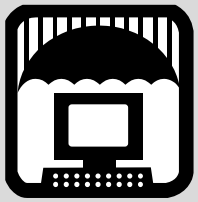
Internal Controls



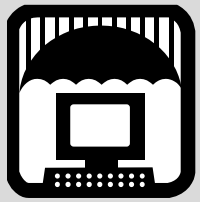
Digital Signature Policy



Digital Signature Installation Steps



Digital Signature SOP



Validation Plans, Tests, Report

TECHNOLOGY

Technology

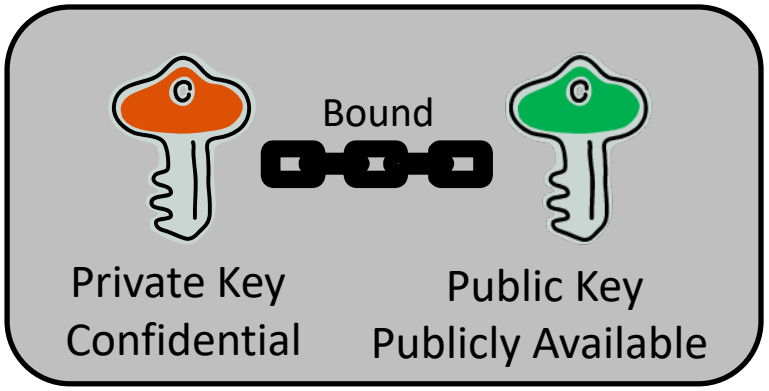
Commercial Trusted Certificate Services

Safenet Hardware Token with Your Digital ID

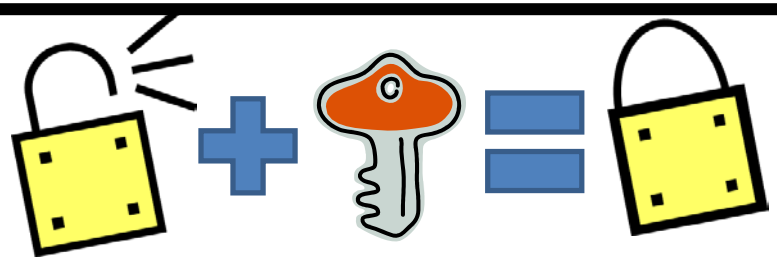
Adobe Reader and Acrobat

Digital Signature Technology

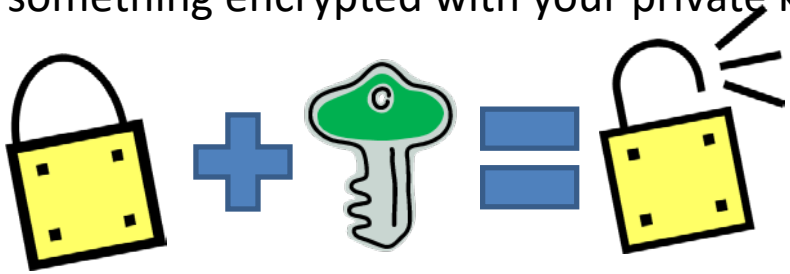
Each user has a unique private/public key pair that are bound together and work uniquely together to encrypt and decrypt information.

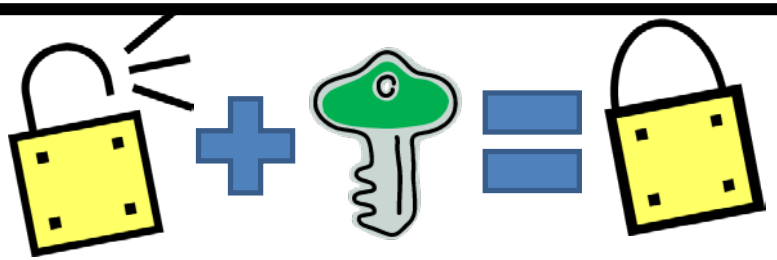


Your **private key** is confidential. It's physically stored on a hardware token that you keep. There is no backup. If you lose your hardware token or forget your token password, you need a new one just like a drivers license.

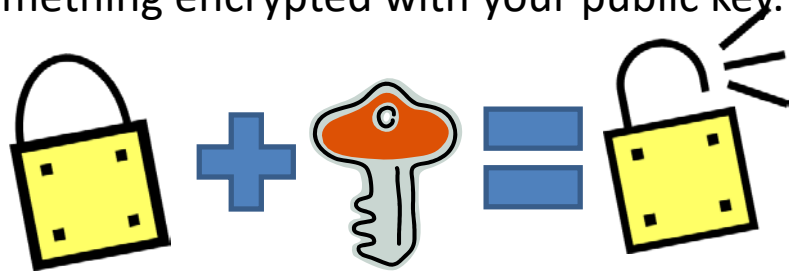


Only your public key can decrypt (unlock) something encrypted with your private key.

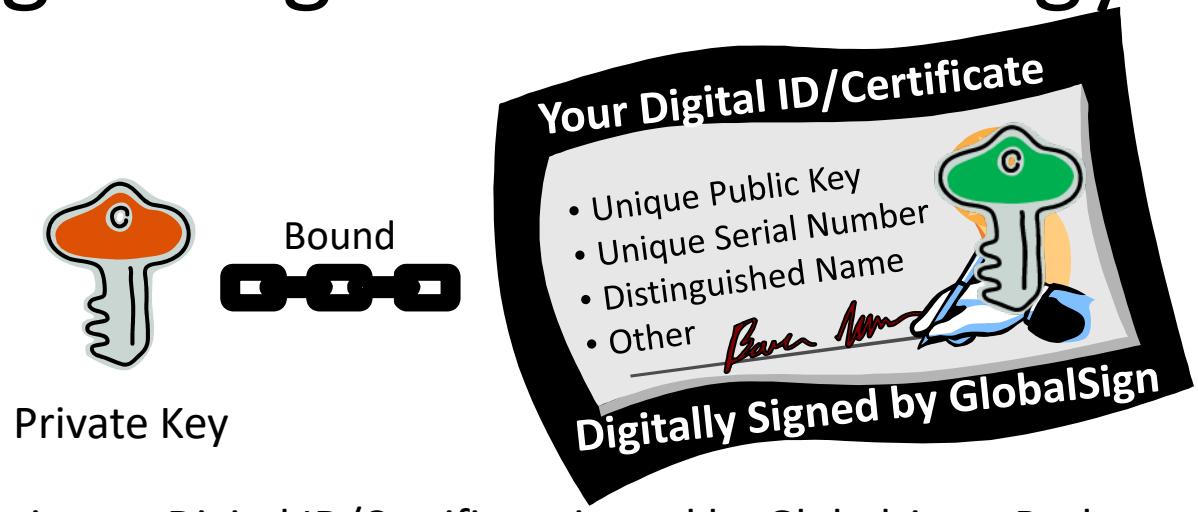




Only your private key can decrypt (unlock) something encrypted with your public key.



Digital Signature Technology



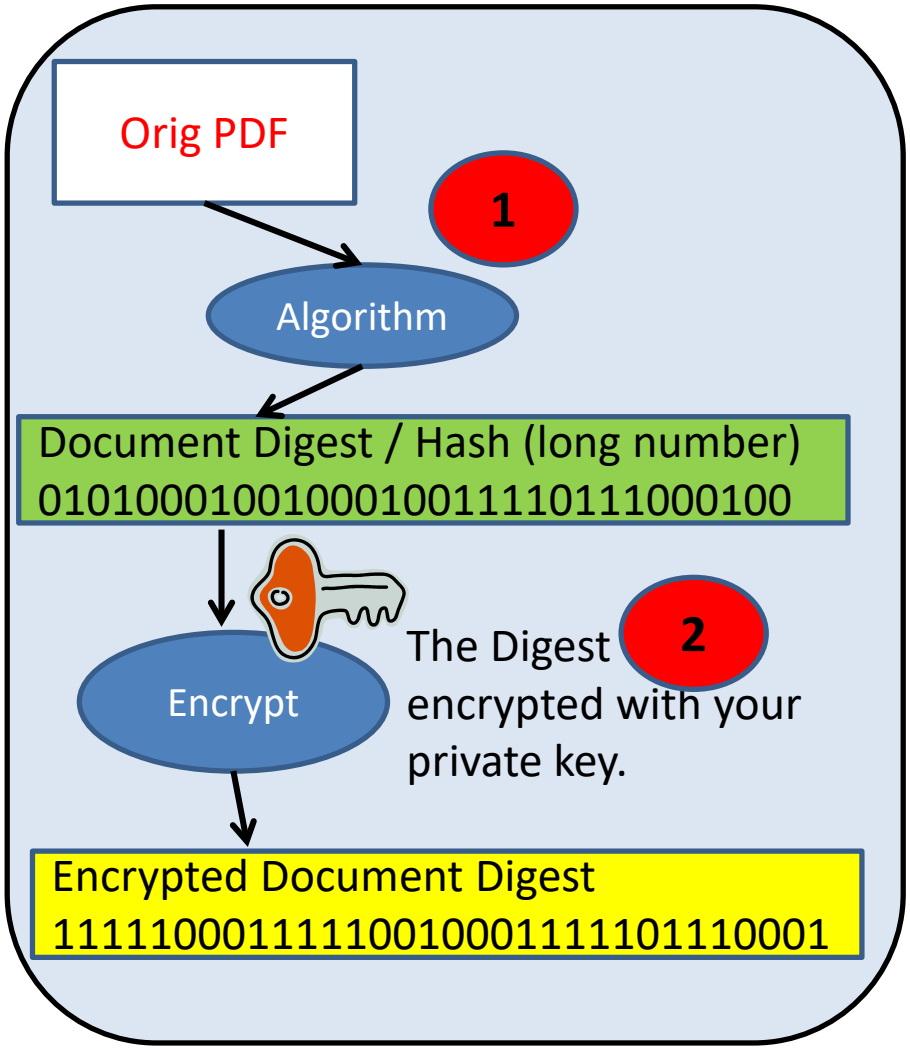
Your public key is on a Digital ID/Certificate issued by Globalsign. Both your private key and your Digital ID/Certificate are stored on your token.

Your Digital ID/Certificate also contains other information as compliant with the industry standard: X.509.

Globalsign, as a Certificate (ID) Authority also DIGITALLY SIGNS your ID attesting to the authenticity of the private/public key pair represents the ID owner (YOU) .

Your Digital ID/Certificate (**but not your private key**) is inserted into every PDF document that you sign .

You Sign a Document



New PDF has 3 components

Orig PDF

Your Public Key in a Digital ID signed by GlobalSign

Encrypted Document Digest

Your Colleagues Open Your Signed Document

From previous slide

PDF with 3 components

Orig PDF

Your Public Key in a Digital ID signed by GlobalSign

Encrypted Document Digest

1

Orig PDF

Adobe Reader independently calculates a Document Digest

Algorithm

Document Digest / Hash
01010001001000100111101110001000

2

Your public key is the only number that that can decrypt the Encrypted Document Digest.

Encrypted Document Digest

decrypt

Document Digest / Hash
01010001001000100111101110001000

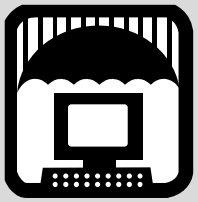
3

Match?

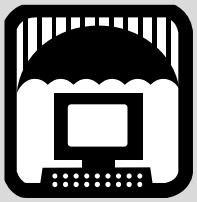
If they match, then document has not changed.

CONTROLS

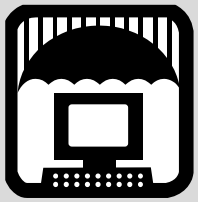
Internal Controls



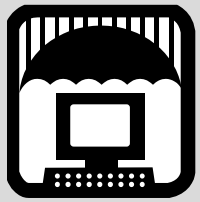
Digital Signature Policy



Digital Signature Installation Steps



Digital Signature SOP



Validation Plans, Tests, Report

Digital Signature Policy

- All users must read the policy.
- Key points of Policy
  - People can use their own digital identities if they meet Company requirements (see QA for requirements).
  - Hardware tokens (USB sticks) must be physically secured when not in use
  - A written copy of your passwords may not be stored with your hardware token
  - Everyone must sign a statement ("wet" signature – original sent to QA) acknowledging they understand the policy

Digital Signature Installation

You will receive installation documentation which provides step by step instructions for initializing your hardware token and signing your first document.

Digital Signature SOP

Key Points

- The organization that has paid for your Digital ID restricts the use of the Digital ID to work performed for this organization.
- Immediately report loss or other compromise of your hardware token to QA.
- Do not share your token password with anyone else (not QA, not Globalsign, not your spouse)
- Immediately report to QA any invalid signature on any work document
- If a document is to be routed to several reviewers, Adobe Acrobat must be used to set up the form and to allow Adobe Readers to sign document (Reader Extension enabled)

Validation Process

Define a set of requirements against which the System will be validated. These requirements include your specific requirements plus all of the Part 11 and Annex 11 requirements.

Per FDA guidance, a risk assessment is performed and the results documented. The risk assessment results in additional requirements for the System (to reduce/mitigate the risks).

Validation Plan describes how requirements are met through (a) procedural controls --- SOP, Forms, and Policy or (b) test/demonstration. The Validation Matrix lists every requirement including Part 11/Annex 11 and specifies how the system will be validated against relevant requirements.

Test plan describes test cases that show the Technology meets requirements. Test cases are defined per the GAMP 'Testing' Good Practice Guide.

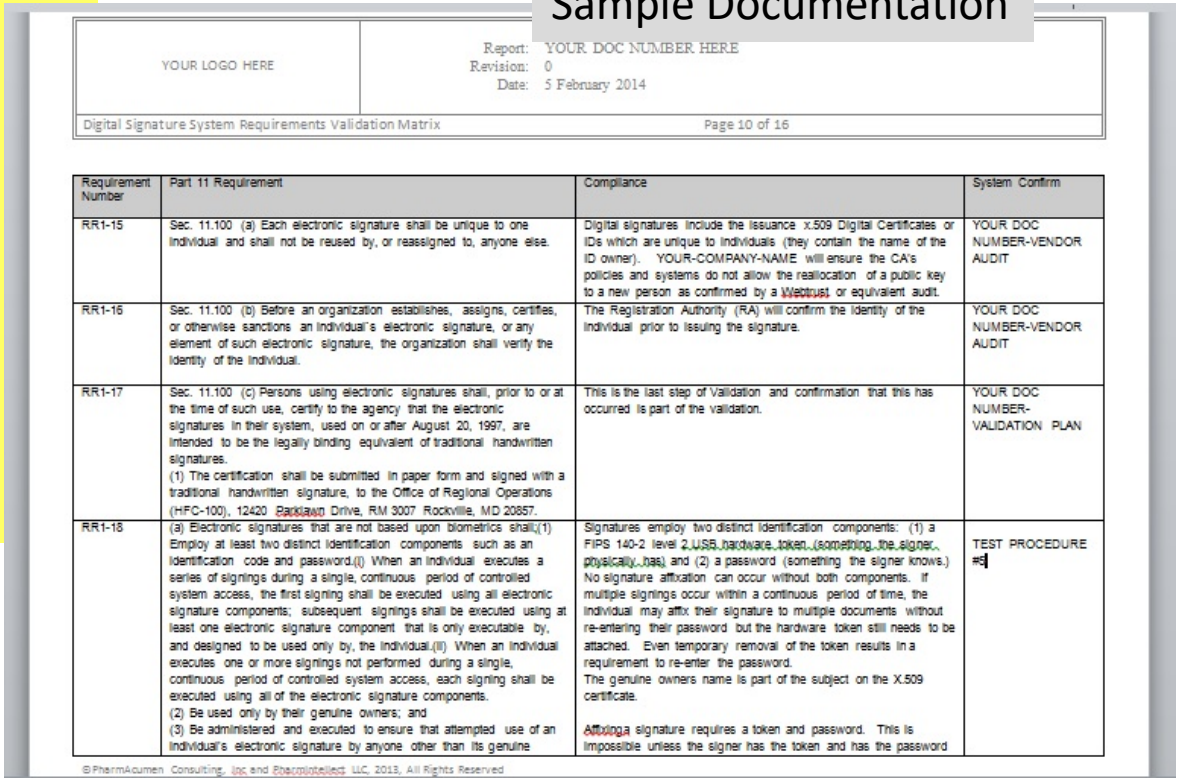
Validation is performed and Test Report written; Digital Identity Vendor Audit performed.

Validation Products

The following documents exist and have been reviewed and approved by Quality Assurance

- Digital Signature Requirements and Risk Assessment
- Digital Signature Validation Plan
- Digital Signature System Test Plan
- Digital Signature System Requirements Validation Matrix
- Digital Signature Validation Report
- Digital Identity Vendor Audit

Sample Documentation



YOUR LOGO HERE

Report: YOUR DOC NUMBER HERE
Revision: 0
Date: 5 February 2014

Digital Signature System Requirements Validation Matrix Page 10 of 16

Requirement Number	Part 11 Requirement	Compliance	System Confirm
RR1-15	Sec. 11.100 (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Digital signatures include the issuance x.509 Digital Certificates or IDs which are unique to individuals (they contain the name of the ID owner). YOUR-COMPANY-NAME will ensure the CA's policies and systems do not allow the reallocation of a public key to a new person as confirmed by a Webtrust or equivalent audit.	YOUR DOC NUMBER-VENDOR AUDIT
RR1-16	Sec. 11.100 (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 Registration Authority (RA) will confirm the identity of the individual prior to issuing the signature.	YOUR DOC NUMBER-VENDOR AUDIT
RR1-17	Sec. 11.100 (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. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 12420 Parklawn Drive, RM 3007 Rockville, MD 20857.	This is the last step of Validation and confirmation that this has occurred is part of the validation.	YOUR DOC NUMBER-VALIDATION PLAN
RR1-18	(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.(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.(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. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine	Signatures employ two distinct identification components: (1) a FIPS 140-2 level 2 USB hardware token (something the signer physically has) and (2) a password (something the signer knows.) No signature affixation can occur without both components. If multiple signings occur within a continuous period of time, the individual may affix their signature to multiple documents without re-entering their password but the hardware token still needs to be attached. Even temporary removal of the token results in a requirement to re-enter the password. The genuine owners name is part of the subject on the X.509 certificate. Affixing a signature requires a token and password. This is impossible unless the signer has the token and has the password	TEST PROCEDURE #5

Final Note: GlobalSign IDs are used by the EMA for digitally certifying their documents under their E-signature program.

Leveraging for Ease of Validation

- Adobe
  - Test Report for compliance with NIST Standards for Digital Signature Application (X.509)
  - Compliance with DoD PKI Test Suite
- USB Tokens
  - FIPS 140-2 Validation Certificate (conformance to NIST Standards)

FIPS=Federal Information Processing Standards

- GlobalSign (see next page)
  - WebTrust Audit by Ernst & Young
  - Adobe CDS Audits

Leveraged results –
No need to repeat testing

GlobalSign

- Every major CA is required to undergo a yearly WebTrust audit, which rigorously examines practices such as customer authentication procedures, physical, network and logical security surrounding the certificate issuance infrastructure, handling of customer data and business continuity planning.
- GlobalSign - second longest WebTrust certified CA after VeriSign (now Symantec).

Final Note: GlobalSign IDs are used by the EMA for digitally certifying their documents under their E-signature program.

Are you reading this training material electronically in Reader or Acrobat?

- If yes, I signed this training material. So let's take a look at a signed PDF document first hand.
- Right click on my signature below and select "Show Signature Properties".
- Examine the properties of the signature.
- Look at Advanced Properties – view the info about trusted timestamps.
- Show my certificate.
- Validate my signature.
- Good luck and enjoy!