

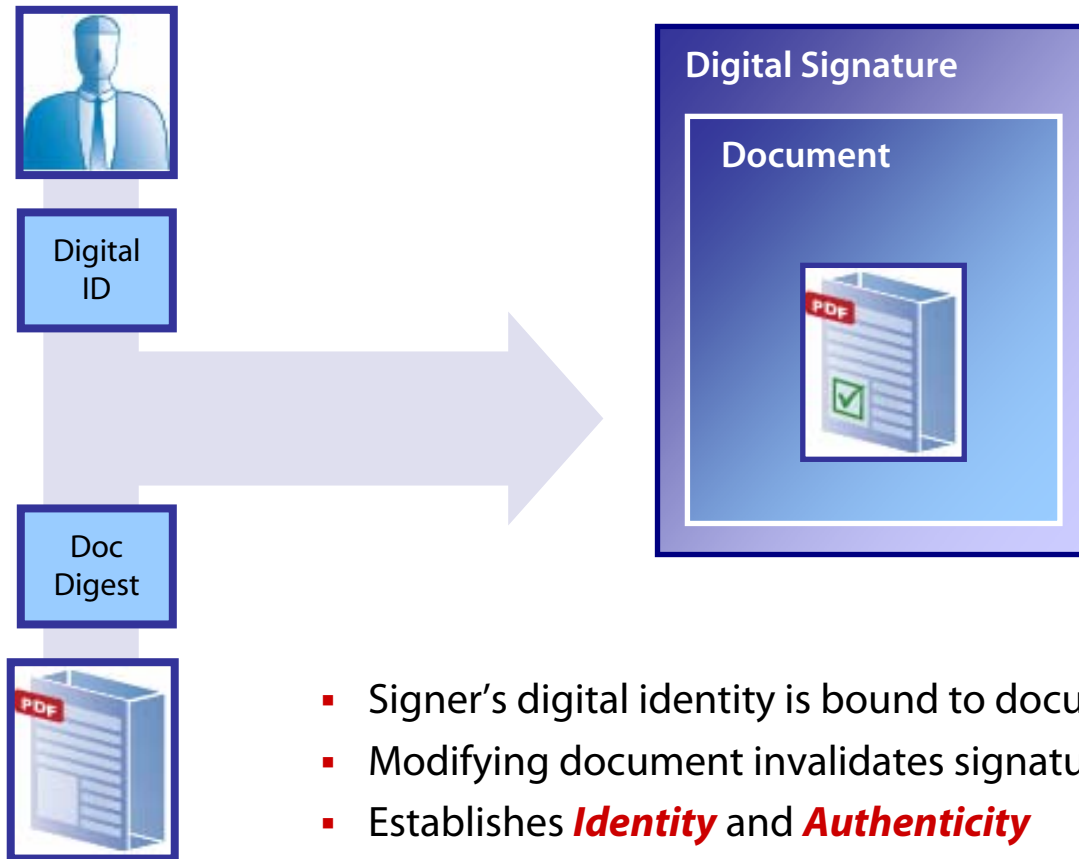
SAFE Digital Signatures in PDF

Ed Chase

Adobe Systems



Digital Signatures in PDF



- Signer's digital identity is bound to document
- Modifying document invalidates signature (*tamper evidence*)
- Establishes **Identity** and **Authenticity**

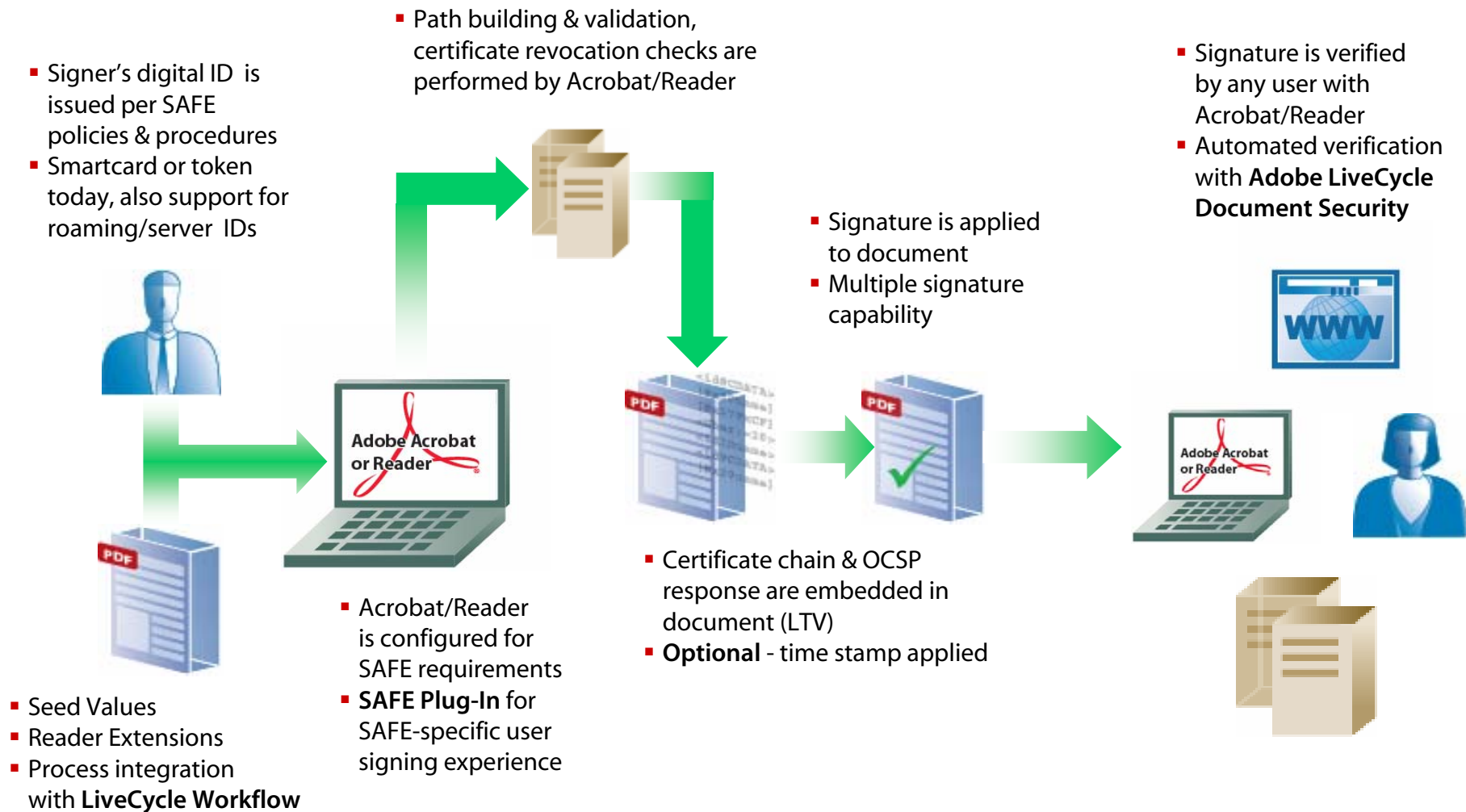
PDF and Digital Signatures – Standards Support

Since Adobe Acrobat 4.0 - 1999

- PKI standards-based digital signatures
 - NIST PKITS & DOD JTIC approved (Acrobat & Reader)
- Highly customizable (JavaScript & *Seed Values*)
- Any hardware or software x.509 cert
 - Windows cert store, Acrobat, or PKCS#11
 - Roaming/server certificate support (8.0)
- Signatures are in the document
- Built-in to Acrobat & Reader (w/LCRE)
 - Revocation checking & embedding - OCSP & CRL
 - Secure Time Stamp support (RFC 3161)
 - Path building and validation w/bridge support - AIA extension IC acquisition support in 7.0.7 and up
 - Modification Detection & Prevention (MDP) - Multiple signatures w/"Roll-back" versioning
 - Long-Term Validation (LTV) – Include cert revocation info
 - New in 8 – signature preview mode, new signing UI
- **Adobe Acrobat, Reader, and LiveCycle Document Security are now certified SAFE compliant**



The SAFE Signing Process with Adobe Acrobat & Reader



The SAFE Plug-In for Acrobat & Reader

- **Simplifies SAFE-enabled configuration and signing in Acrobat and Reader 7**
- Easier for end-users
 - Inserts a "SAFE-Signature" button in Acrobat
 - Signers don't need to select a digital ID, signature appearance, or reason for signing
 - All either pre-configured in deployment or by user on first use of plug-in
 - On or off-line signing
- Easier to deploy
 - Packaged with Acrobat/Reader via *IntallShield Tuner* for enterprise deployment
 - Plug-in is application-level JavaScript on user's system
 - Also includes: registry settings, logos and appearance files for SAFE, and trusted identity files for individual customers



NEW - SAFE Signing with Adobe *LiveCycle Document Security*

- Signer's digital identity is issued in accordance with SAFE policies
- Still **two-factor** – Smart card or token



- Upload PDF or
- Generate from application files or
- Workflow integration

- User interacts through web application
- No configuration of Reader or Acrobat –
- Reader or Acrobat still required to view documents



- PDF signature processing by **Adobe LiveCycle Document Security**



- Documents are reviewed in Reader
- Precise signature placement
- Path building and validation by server
- Certificate chain & revocation response are embedded in document
- Optional time stamp



Other Options -

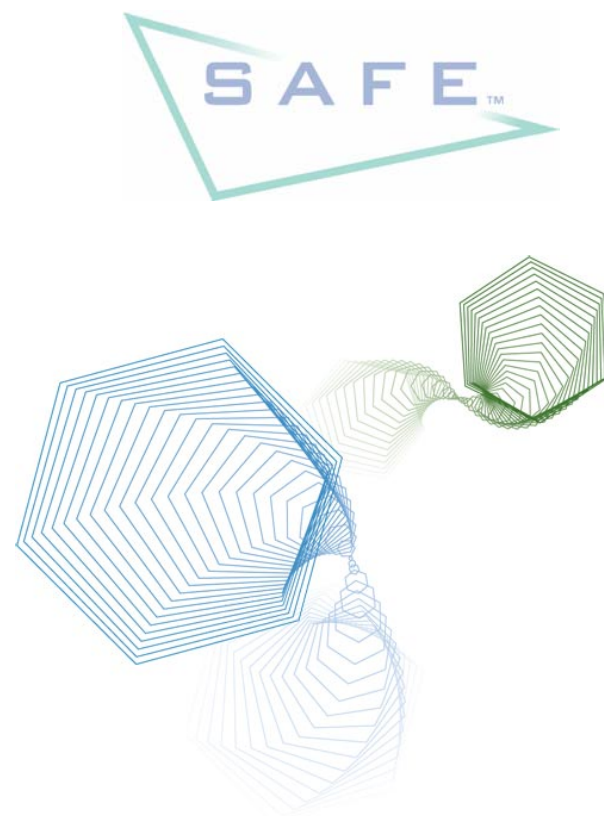
- Multiple signatures
- Order requirements
- Signature designates

- Signed documents can be downloaded or automatically routed
- Signature is verified by any user with Acrobat/Reader



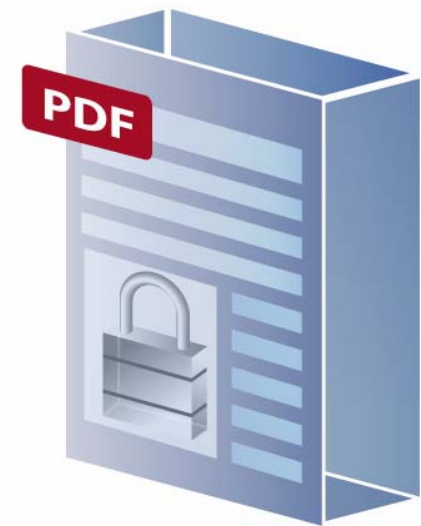
SAFE Signatures with Adobe LiveCycle Document Security

- **Server managed signing with client-side digital IDs and signature generation**
- Easier for end-users
 - Browser-based signing
 - Integrated PDF creation with LiveCycle Generator
 - Precision signature field creation capabilities for users in the browser
 - Notifications, workflow, role, and designated signer options
- Easier to deploy & maintain
 - Central management & logs
 - Integrate with other enterprise applications and content management systems
 - No plug-ins or custom Acrobat/Reader deployments required
 - Built on Adobe LiveCycle by Adobe solution partners



The SAFE Implementation Guide for Acrobat & Reader

- **Deployment information for SAFE signatures in Acrobat & Reader**
- Enterprise deployment information
- Application settings
 - User preferences
 - Registry settings
 - JavaScript
- Document settings
 - Seed values
- Developer resources
- Direct comparison of SAFE Enabled Application (SEA) specifications with Acrobat & PDF functionality



Resources

Ed Chase

Adobe Systems Worldwide Standards

chase@adobe.com