

Adobe Signature Solutions

Sudha Iyer

Senior Product Manager, Adobe Systems

5/21/2008

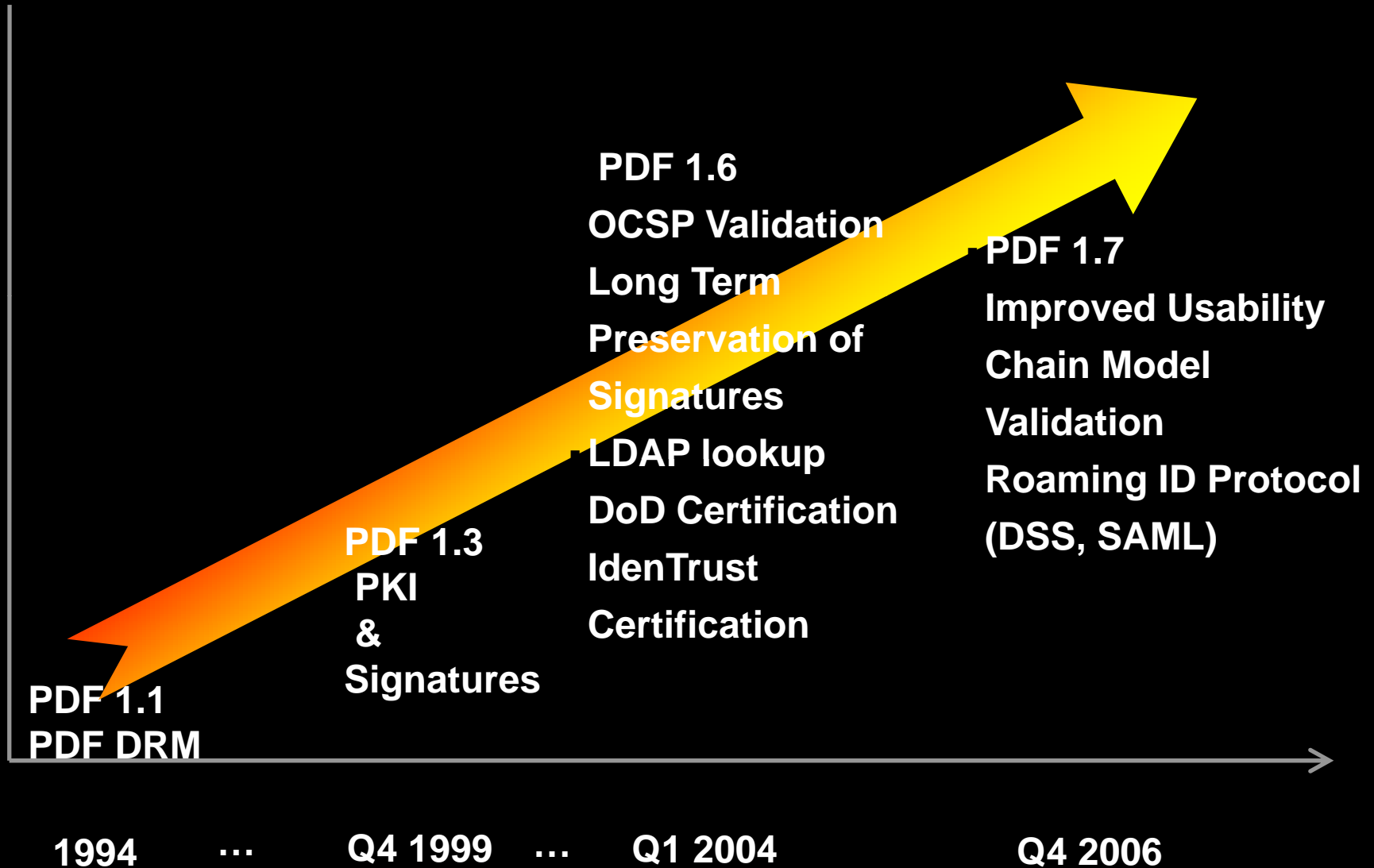


Agenda

- Value Proposition of Signatures in PDF
- Examples from current usage
- Any questions



Evolution of Signatures in PDF



PDF Signature Platform

1. Usability

- Fidelity
- Intuitive interface

2. Versatile

- SDK and Plug in model encourages a number of localized implementations
- AdHoc/Enterprise workflows
- Validate in free reader
- PDF Signatures and XML Signatures

3. Standards Based

- ISO 32000, PKI standards



PKI Industry Standards in PDF supported by Adobe Acrobat, Adobe Reader

- RFC 2315/3279 compliant signature formats
- RFC 3280/NIST compliant Path validation and CRL checking
- RFC 2560/Identrus compliant OCSP revocation checking
- Federal Bridge CA compliant Cross-certificate support
- RFC 3161 compliant time stamping
- Smart Card support using PKCS#11
 - Standard PC/SC card readers, CAPI support
- Standard Hashing algorithms, MD5, SHA1, SHA-256, SHA-384, SHA-512, RIPEMD160
- Include FIPS 140-2 Level 2 compliant crypto libraries

Security Certifications

1. NIST PKI Test Suite (PKITS) Compliant
 - We pass the 240+ tests
2. US Federal Bridge Cross Certification
 - In progress



DEFENSE INFORMATION SYSTEMS AGENCY
JOINT INTEROPERABILITY TEST COMMAND
P.O. BOX 12798
FORT HUACHUCA, ARIZONA 85670-2798

IN REPLY
REFER TO: Networks and Transport Division (JTE)

John Landwehr
Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704

Dear Mr. Landwehr:

The Joint Interoperability Test Command (JITC) has completed Department of Defense (DOD) Public Key Infrastructure (PKI) testing of Adobe Reader 7.0.

***Acrobat 8.0 &
Reader 8.0
DOD Certified***

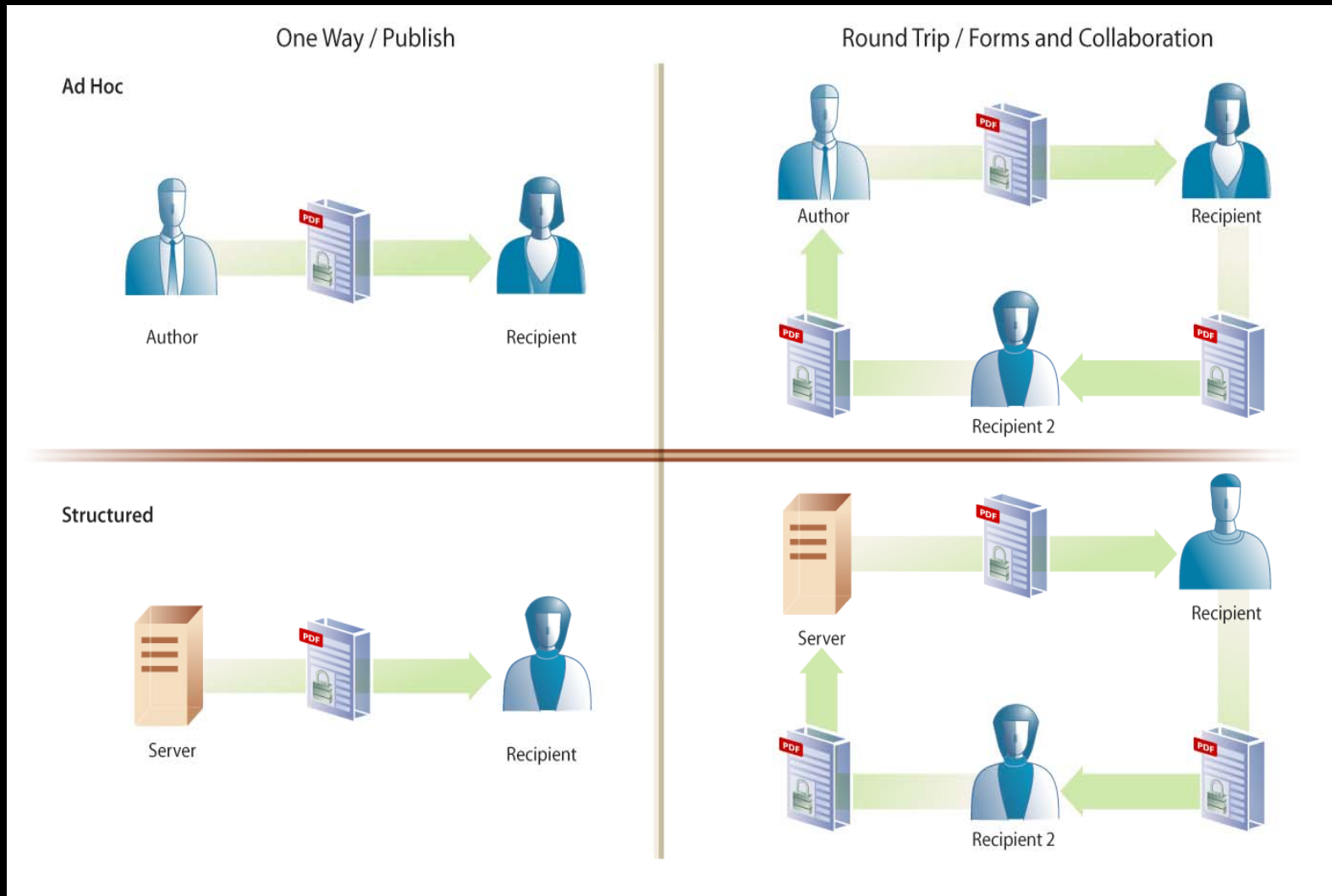
1 Apr

Additional Standards in PDF 1.7

- Industry Standard protocols in use in Roaming Ids
 - RFC 2222 – use SASL over SOAP for authentication messages
 - RFC 2246 – Server authentication over TLS
 - RFC 2616 – SOAP over http
 - WSS:SOAP Message Security
- XML Encryption; XML Digital Signatures [for XFA Forms]
 - W3C Standards

Deployments with PDF Signatures

Structured and Ad Hoc Workflows



Advanced Electronic Signatures, Qualified Electronic Signatures

Demo



Why PDF Signature Solutions?

Improved Business Efficiencies

- **Integration with Existing Business Processes**
- **Meets Compliance Goals**
- **Industry Standard solution**
- **Backward Compatibility**
- **Certified Document Service**



Roaming IDs

What is it?

- Server holds the digital ids on behalf of the user
- Acrobat/Reader client;
- Adobe Partners provide the server

Value Proposition

- On boarding a user with digital id
- Providing true roaming capabilities with no burden of carrying a digital id

Additional Resources

- Adobe Signatures Product Documentation
 - Acrobat, Reader
 - <http://www.adobe.com/devnet/acrobat/security.html>
 - LC ES
 - http://www.adobe.com/devnet/livecycle/pdfs/lc_digital_sig_wp_ue.pdf
- Adobe Security Partner Information
 - http://partners.adobe.com/public/developer/security/index_security_partners.html

Questions?