



# Adobe® Electronic Signature Survey

In order to support interoperability testing across Adobe LiveCycle® ES, Adobe Acrobat® and Adobe Reader®, and help us to determine the next direction for our products, we are offering you the ability to participate in this Electronic Signature Survey.

There are three parts to this Survey. The first part asks you to sign a signature field with your signature credential. The second asks you a series of questions about your use of electronic signatures, and the third concerns technical details about your signature credential. Please note that all submissions on this Electronic Signature Survey are optional.

**IMPORTANT NOTICE:** All information you provide as part of the Electronic Signature Survey will only be used to test the compatibility of Adobe's LiveCycle ES, Adobe Acrobat and Adobe Reader products with the signatures collected by way of this Electronic Signature Survey and to understand the ways in which signatures are used in our products, helping guide Adobe's electronic signature product strategy. Adobe will retain the information you submit as part of the Electronic Signature Survey as long as reasonably necessary but solely for testing and product development purposes as noted above. The information you provide as part of the Electronic Signature Survey will not be publicly disclosed. If at any time you wish to have the information you submit via the Electronic Signature Survey removed from Adobe's database, please send an email to [signaturesurvey@adobe.com](mailto:signaturesurvey@adobe.com).

When you have completed the Electronic Signature Survey, please click the 'Submit' button in the upper right hand corner of the screen to send your survey results via email to Adobe's product team or email the file directly to [signaturesurvey@adobe.com](mailto:signaturesurvey@adobe.com). Thank you for participating in the Adobe Electronic Signature Survey!

## *Part One - Signature*

Please click the signature field below (marked with a red flag) to apply a digital signature using your organization's or your individual signature credential. These signatures will be used by our product and quality teams to ensure that current and future versions of our products interoperate effectively with a wide variety of signatures.

***Sign Here:***

## *Part Two - Signature Usage*

**All questions are optional.** We welcome you to complete the optional questions below that provide information about the environment and organization that issued the credential that signed this document and provide us with even more insight into your use of signatures and how we can make our products better fit your needs in the future. (If you have multiple CAs, please sign another copy of this document.)

General Questions about Usage and Deployment

1. What stage is electronic signature deployment at, within your organization?

- No plans (only me)    RFP    Department Pilot    Organization Pilot    Production

2. How many users are currently signing documents at your organization?

- None (only me)    <50    50-250    250-1000    1000-10000    10000+

3. How many users are currently validating signed (but not necessarily signing) documents?

- None (only me)    <50    50-250    250-1000    1000-10000    10000+

4. What types of electronic signatures are you implementing? Click all that apply.

- Browser-based e-signatures (click-thru)
- Handwritten electronic signatures (tablet PC / signing pad)
- Certified documents (one way publishing of documents via digital signature)
- Recipient digital signatures (click on all details/ use cases that apply below)
- Sign-only (no form fields)
  - Fill-in fields, Sign
  - Fill-in fields, Sign1, Sign2
  - Fill-in fields, Sign1, Fill-in more fields, Sign2
  - OTHER \_\_\_\_\_

5. How does your organization store your signing credential?

- Software (on local PC)
- Roaming or Centralized Storage of ID
- Smartcard
- USB Token
- Server HSM
- OTHER (please describe) \_\_\_\_\_

6. How does your organization protect your signing credential?

No authentication required

PIN code

Complex password

OTP (one time password) token

Biometrics (fingerprint, voice, iris, etc)

OTHER (please describe) \_\_\_\_\_

7. Do you have a need to sign documents on mobile devices?

Yes (Please list platform: \_\_\_\_\_ )

No

8. How long do your signed documents need to be archived?

No requirement

1-7 years

8-30 years

31-100 years

101+ years

9. What products does your organization use to apply signatures with this credential (click all that apply):

Adobe Acrobat

Adobe Reader

Adobe LiveCycle Digital Signatures

Microsoft Office

OTHER (please list) \_\_\_\_\_

10. What products does your organization use to validate digital signatures from this credential (click all that apply):

Adobe Acrobat

Adobe Reader

Adobe LiveCycle Digital Signatures

Microsoft Office

OTHER (please list) \_\_\_\_\_

11. What desktop operating systems are primarily used in your organization to sign/validate with this credential (click all that apply):

Windows Vista

- Windows XP
- Windows 2000
- Other Windows \_\_\_\_\_
- Mac OS X 10.5
- Other Mac OS X \_\_\_\_\_
- Linux
- OTHER \_\_\_\_\_

12. Do people outside your organization sign documents with this credential? That is, do you provide these credentials to partners, consultants, etc.?

- Yes       No

13. Do people outside your organization validate documents signed with this credential? That is, do you use this credential to do business / communicate with third parties, partners, customers, etc.

- Yes       No

14. Do you also issue digital certificate credentials for web browser authentication?

- Yes, a different credential       Yes, this same credential       No

15. Do you also issue digital certificate credentials for encryption?

- Yes, a different credential       Yes, this same credential       No

## *Part Two – Technical Questions*

This set of questions relates to the credential that signed above.

1. Name of Root CA in this credential path: \_\_\_\_\_
2. Name of ICA(s) in this credential path: \_\_\_\_\_

3. Which of the following revocation mechanisms are used to validate this credential?

- CRL
- OCSP
- OTHER \_\_\_\_\_

4. Do you use RFC 3161 timestamping?

Yes       No, other format: \_\_\_\_\_       No timestamps used

5. What RSA key sizes do you support for digital signatures?

512     1024     2048     4096     OTHER \_\_\_\_\_

6. What hashing algorithms do you support for digital signatures

MD5     SHA1     SHA256     SHA384     SHA512     OTHER \_\_\_\_\_

7. Do you currently utilize ECDSA?

Yes       No

8. Is this certificate authority cross-certified with another bridge or CA? Check all that apply.

Federal Bridge (At level: \_\_\_\_\_)

CertiPath (At level: \_\_\_\_\_)

SAFE (At level: \_\_\_\_\_)

Higher Ed Bridge (At level: \_\_\_\_\_)

Other \_\_\_\_\_

9. Is this CA "Qualified" as per the EU Signature Directive and local regulations?

Yes (Country(ies): \_\_\_\_\_)       No

10. How many end-entity credentials are currently active in this CA? \_\_\_\_\_

11. How many end-entity credentials have been revoked in this CA? \_\_\_\_\_