Adobe® Flash® Access™

August 2011

Version 3.0

Certificate Enrollment Guide

Adobe® Flash® Access™ 3.0 Certificate Enrollment Guide

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

Last updated 8/27/2011

Contents

Obtaining certificates

Use the Adobe® Flash® Access™ Certificate Enrollment site to obtain digital certificates for use with the Flash Access SDK.

About certificates

The Adobe Flash Access SDK is available in the following configurations:

- Flash Access Production SDK
- Flash Access Evaluation SDK
- Flash Access Trial SDK

To use the Flash Access SDK to create a licensing and packaging server, you must obtain digital certificates from Adobe. Digital certificates (also referred to as *certificates*) bind an entity, such as an individual, organization, or system, to a specific public and private key pair. Digital certificates can be thought of as electronic credentials that verify the identity of an individual, system, or organization.

To allow maximum flexibility and enhanced security in your deployment options, the Flash Access SDK requires 4 certificates:

- License Server certificate

  The SDK uses this certificate to sign content licenses issued to Flash® Player and Adobe® AIR® clients.

- Packager certificate

  The SDK uses this certificate to generate DRM metadata when packaging (encrypt) content.

- Transport certificate

  The SDK uses this certificate to secure the communication between the clients and licensing server.

- Domain CA certificate

  Customers who want to implement a domain server need the Domain CA certificate. Unlike the other certificates, the Domain CA certificate is not issued by Adobe.

Note: *For the Evaluation SDK and the Trial SDK, the License Server, Packager, and Transport certificates are combined into a single certificate.*

Prerequisites

To use the Certificate Enrollment site to request certificates you need to know the following:

- How public key infrastructure (PKI) works
- How to generate key pairs and secure your private keys
- How to generate a certificate signing request (CSR)
- How to convert PKCS#7 into PKCS#12, PEM, and DER files

About certificate enrollment roles

The certificate enrollment process requires at least two employees: an Administrator and a Requester. The Flash Access SDK licensee appoints an Account Administrator. There can be only one Account Administrator. The Account Administrator can designate one Secondary Administrator.

Administrators can designate up to five Requestors. Requestors are employees at your company who request and deploy certificates. Administrators approve the certificate requests. Each Adobe ID account can have only one role.

The following are the abilities of each role:

Account Administrator

- 1 Account Administrator per license.
- Add a Requesters
- Add a Secondary Administrator
- Edit the telephone information and challenge phrase of the requester company
- Remove Requesters and Secondary Administrator
- Approve or reject certificate requests
- Revoke issued certificates

Secondary Administrator

- 1 Secondary Administrator per license.
- Add Requesters
- Edit the telephone information and challenge phrase of the requester company
- Remove Requesters
- Approve or reject certificate requests
- Revoke issued certificates

Requester

- Up to 5 Requesters per license.
- Request certificates

Add Requesters and a Secondary Administrator

Add a Requester

A Flash Access licensee can have up to five requesters. It is advised, however, to limit the number of Requesters to the individuals who are developing the Flash Access solution. The Requesters are responsible for storing the private key in a secure location.

1. An administrator logs on to the Certificate Enrollment site with a valid AdobeID that contains the domain name of the licensee.
2. On the Home page, click Add a Requester.

3 On the User accounts tab, do one of the following:

- Add user.

  If the employee has an Adobe account, enter the e-mail address. Click Add and continue.

- Invite user.

  If the employee doesn't have an Adobe account, invite them to create one. Enter the e-mail address and name of the employee and click Send an invitation. The site sends an e-mail invitation to the invitee. The e-mail contains a link to adobe.com where the invitee can create an account. The invitee must use the e-mail address to which the invitation was sent.

Note: *The administrator does not receive notification when a user has created an account. Check the User accounts tab on the Certificate Enrollment site to see whether an invitee has created an account.*

4 If you added a user, the role section screen in the User accounts tab opens. Do the following:

- Confirm that the user's information is correct.
- Enter the company phone number and challenge phrase.

  The user must know this phrase to verify their account.

- For User type, select Requester.
- Click Save.

  The Requester receives an e-mail stating that their Flash Access account registration has been completed.

5 If you invited a user, do the following:

- Log on to the Certificate Enrollment site.
- Select the User accounts tab.
- Locate the user in the Invitations Sent section and click Authorize.

  Note: *If there isn't an Authorize link in the Actions column, the invitee hasn't created an Adobe account yet.*

- Confirm that the Requester's information is correct.
- Enter the company phone number and challenge phrase.

  The Requester must know this phrase to verify their account.

- For User type, select Requester.
- Click Save.

  The user receives an e-mail stating that their Flash Access account registration has been completed.

Create a Secondary Administrator

The Account Administrator can create a Secondary Administrator. There can be only one secondary administrator. The Account Administrator can promote the Secondary Administrator to Account Administrator. This action demotes the Account Administrator to the role of Secondary Administrator.

1 The Account Administrator logs on to the Certificate Enrollment site with a valid Adobe ID that contains the domain name of the licensee.

2 On the User accounts tab, do one of the following:

- Add user.

  If the employee has an Adobe account, enter the e-mail address. Click Add and continue.

- Invite user.

If the employee doesn't have an Adobe account, invite them to create one. Enter the e-mail address and name of the employee and click Send an invitation. The site sends an e-mail invitation to the invitee. The e-mail contains a link to adobe.com where the invitee can create an account. The invitee must use the e-mail address to which the invitation was sent.

Note: *The administrator does not receive notification when a user has created an account. Check the User accounts tab on the Certificate Enrollment site to see whether an invitee has created an account.*

3 If you added a user, the role section screen in the User accounts tab opens. Do the following:

- Confirm that the user's information is correct.
- Enter the company phone number and challenge phrase.

  The user must know this phrase to verify their account.
- For User type, select Administrator.

  Note: *To swap Account Administrator and Secondary Administrator roles, select Make default administrator.*
- Click Save.

  The administrator receives an e-mail stating that their Flash Access account registration has been completed.

4 If you invited a user, do the following:

- Log on to the Certificate Enrollment site.
- Select the User accounts tab.
- Locate the user in the Invitations Sent section and click Authorize.

  Note: *If there isn't an Authorize link in the Actions column, the invitee hasn't created an Adobe account yet.*
- Confirm that the user's information is correct.
- Enter the company phone number and challenge phrase.

  The user must know this phrase to verify their account.
- For User type, select Administrator.

  Note: *To swap Account Administrator and Secondary Administrator roles, select Make default administrator.*
- Click Save.

  The user receives an e-mail stating that their Flash Access account registration has been completed.

Request certificates

To use the Flash Access SDK Production SDK, repeat the following steps to request each certificate (License Server, Packager, and Transport). The Evaluation SDK and the Trial SDK use a single certificate.

Generate a Certificate Signing Request (Requester)

Note: *The examples provided in this document use OpenSSL. You can also use other utilities. Use these examples for reference only. For information about generating key pairs and storing keys and certificates in your Hardware Security Module (HSM), see the documentation for your HSM.*

1 Generate a key pair.

To use a utility such as OpenSSL, open a Command Window and enter the following:

```
openssl genrsa -des3 -out mycompany-license.key 1024
```

Note: *Adobe recommends including certificate type (lic, pkgr, trans, trial, or eval) in the key name. This naming convention makes it easier when you deploy them on your license and packaging servers. This example uses "mycompany-license.key". For the Evaluation and Trial versions, use "mycompany-eval.key" and "mycompany-trial.key".*

2 Enter a password to protect the private key. Passwords should contain at least 12 characters. The characters should include a mixture of uppercase and lowercase ASCII characters and numbers.

To use OpenSSL to generate a strong password, open a Command Window and enter the following:

```
openssl rand -base64 8
```

3 Generate a Certificate Signing Request (CSR).

To use OpenSSL to generate a CSR, open a Command Window and enter the following:

```
openssl req -new -key mycompany-license.key -out mycompany-license.csr -batch
```

4 You are prompted to enter the password for the private key.

5 Create a back-up copy of your private key and password

If you lose the private key or if it's compromised, contact the Adobe Certificate Administrator to revoke your certificate and request a new one.

Note: *Adobe recommends using an HSM to protect your private key and password.*

Request a certificate (Requester)

1 Log onto the Certificate Enrollment site.

The user who requests a certificate must be a Requester.

2 On the Request tab, select the type of certificate (License Server, Packager or Transport).

Note: *This option is not shown for the Evaluation and Trial SDK versions. Those SDK versions use one certificate.*

3 Do one of the following:

- Upload the CSR file.
- Copy the CSR information from the CSR and paste it into the form.

Note: *To copy the CSR information, select the text between, not including, the beginning tag (-----BEGIN CERTIFICATE REQUEST-----) and end tag (-----END CERTIFICATE REQUEST-----).*

4 Click the Submit Request button.

An e-mail is sent to the Account and Secondary Administrators for review. The Requester is CC'd.

Approve a certificate (Account or Secondary Administrator)

1 Log onto the Certificate Enrollment site.

2 Select the Certificates tab.

3 Review the request to verify that the request is valid.

4 If the request is valid, click Approve. You may also add a comment.

An e-mail is sent to the Requester stating that the request has been approved by one of the company administrators. A copy of this e-mail is sent to the company and Adobe administrators.

5 If the request is not valid, click Reject and enter a comment in the confirmation dialog.

An e-mail is sent to the Requester stating that the request has been rejected by one of the company administrators. A copy of this e-mail is sent to the company administrators.

Certificate delivery

When an administrator approves a certificate request, Adobe verifies the identity of the Requester. Adobe contacts the Requester at the telephone number listed in their profile.

The Adobe administrator attempts to contact the Requester twice within a three-day period. If the Adobe administrator cannot contact the Requester, they leave a message requesting a call-back or they provide a time when they will call again. If the Adobe administrator is not able to reach the Requester, an e-mail is sent to the administrators.

Note: *Only the Account and Secondary administrators can change the company telephone number and the challenge phrase of the Requester.*

If the identity of the Requester is verified, the Requester receives an e-mail containing the PKCS#7 file (p7b).

The Requester can copy the PKCS#7 content from the e-mail body and save it to a file or use the file that is attached to the e-mail. Adobe recommends that when you save the PKSC#7 file, you use the base name that you used to generate the private key and CSR file.

Note: *The file sent to the Requester contains only the certificate. The file does not contain private key information.*

Obtaining Domain CA certificates

Unlike the License Server, Packager or Transport certificate, the Domain CA certificate is not issued by Adobe. You can obtain this certificate from a Certificate Authority, or you can generate a self-signed certificate to use for this purpose. The Domain CA certificate should use a 1024-bit key and contain the standard attributes required in a CA certificate:

- Basic Constraints extension with the `CA flag` set to true
- Key Usage extension specifying Certificate Signing is allowed

For example, using OpenSSL, a self-signed CA certificate can be generated as follows:

1. Create a file called `ca-extensions.txt` containing:

```
keyUsage=critical,keyCertSign
basicConstraints=critical,CA:TRUE
subjectKeyIdentifier=hash
```

2. Generate key:

```
openssl genrsa -des3 -out domain-ca.key 1024
```

3. Generate CSR:

```
openssl req -new -key domain-ca.key -out domain-ca.csr
```

4. Generate certificate:

```
openssl x509 -req -days 365 -in domain-ca.csr -signkey domain-ca.key -out domain-ca.cer -
extfile ca-extensions.txt
```

5. Generate password:

```
openssl rand -base64 8
```

6. Generate PFX:

```
openssl pkcs12 -export -inkey domain-ca.key -in domain-ca.cer -out domain-ca.pfx
```

Deploy certificates

To add certificates to the Flash Access properties files, convert the PKCS#7 file to a PFX file using the private key and generate either a PEM file or a DER file.

- When a credential (certificate and private key) is required, the Flash Access command line tools and Adobe HTTP Dynamic Streaming packagers require a PFX file. The SDK, Reference Implementation, and Flash Access Server for Protected Streaming can accept a PFX file and can also use a credential stored on an HSM.
- When only a certificate is required, most Flash Access components can use a PEM file, DER file, or a certificate on an HSM. The Adobe HTTP Dynamic Streaming packagers only accept DER files for certificates.

Convert files

Using a utility such as OpenSSL and the private key the Requester generates the PKCS#12 (pfx) and PEM/DER files by entering the following commands from a Command Window:

1 Convert PKCS#7 file to a temporary PEM file.

To use OpenSSL, open a Command Window and enter the following:

```
openssl pkcs7 -in mycompany-license.p7b -inform DER -out mycompany-license-temp.pem -outform
PEM -print_certs
```

Note: *This temporary PEM contains your certificate and the certificates for Intermediate CAs. Use these certificates to generate the PFX file.*

2 Convert the temporary PEM file to a PFX file.

To use OpenSSL, open a Command Window and enter the following:

```
openssl pkcs12 -export -inkey mycompany-license.key -in mycompany-license-temp.pem -out
mycompany-license.pfx -passin pass:private_key_password -passout pass:pfx_password
```

3 Convert the temporary PEM file to a final PEM file.

To use OpenSSL, open a Command Window and enter the following:

```
openssl x509 -in mycompany-license-temp.pem -inform PEM -out mycompany-license.pem -outform PEM
```

Note: *Although not required, Adobe recommends using different passwords for the private key (private_key_password) and the PFX (pfx_password).*

This final PEM file contains only your certificate.

4 Convert the PEM file to a DER file.

To use OpenSSL, open a Command Window and enter the following:

```
openssl x509 -in mycompany-license.pem -inform PEM -out mycompany-license.der -outform DER
```

Note: *DER files are required only for the HTTP Dynamic Streaming packagers.*

Deploying certificates

1 To avoid having the PFX password available in cleartext on the License Server, the Reference Implementation and Flash Access Server for Protected Streaming require the password to be encrypted when specified in the configuration file. See *`Using the Flash Access Reference Implementations`* or *`Using the Flash Access Server for Protected Streaming`* for instructions on running the scrambling utilities. The Reference Implementation and Flash Access Server for Protected Streaming each includes its own scramble utility, and the encrypted passwords are not interchangeable between these two License Server implementations.

2 To deploy the certificates and scrambled password to your license and packaging servers, see *Using the Flash Access Reference Implementations* or *Using the Flash Access Server for Protected Streaming*.

Storing keys

Adobe recommends that content publishers store cryptographic private keys for signing and encryption in a secure, tamper-proof hardware device. Keys that are stored in software are more susceptible to compromise than keys that are stored in hardware. For example, if a software key is leaked, the key or file that contains the key is typically copied, making it difficult to detect the breach. Keys that are stored on hardware are less vulnerable to undetected compromise.

Hardware security modules (HSMs) are dedicated hardware devices that store and protect cryptographic keys. For more information, see *Storing keys* in *Adobe Flash Access Secure Deployment Guidelines*.

Renew certificates

There are different certificate renewal restrictions based on your Flash Access SDK configuration:

- Flash Access Production SDK

  Adobe provides the initial set of certificates for the Flash Access Production SDK free of charge when you purchase a support contract. If you don't have a support contract, you can purchase renewal certificates. This set of certificates is valid for two years.

- Flash Access Evaluation SDK

  The certificate set for this SDK is valid for one year and cannot be renewed.

- Flash Access Trial SDK

  The Flash Access Trial SDK is valid for three months. Adobe provides one set of renewal certificates free of charge.

Before a set of certificates expires, Adobe sends an e-mail to the original requester reminding the requester to apply for a new set of certificates. The company administrators are copied on these reminder emails.

The administrators and requester receive an e-mail 8 and 4 weeks before the rroduction certificates expire. The renewal notification e-mail will be sent out 2 weeks before expiration for the Trial version. Within this renewal window requesters can submit requests for new certificates.

To continue using the Flash Access SDK after the second set of certificates has expired, purchase a higher SDK configuration. For example, upgrade from the Trial to the Evaluation or Production configurations. Upgrade from the Evaluation configuration to the Production configuration.