Adopting the new Connect Certificates

- Background
- Scenarios/Use Cases
  - Scenario 1: Single End point to supporting multiple DocuSign Instances
  - Scenario 2 : Single End point to supporting multiple accounts which may be configured to use either the old or new the new certificate
- Approach
  - Differences Between Old and New Certificate(s)
  - Handle Connect Messages with different certificates
    - For Mutual TLS
      - Apache
      - IIS
    - For Signed SOAP Message

Background

DocuSign is replacing the current DocuSign Connect certificate with three new certificates; one for DocuSign's North American (NA) servers, one for DocuSign's European (EU) servers, and one for DocuSign's DEMO environment. DocuSign has obtained the new certificates and customers that use the current Connect certificate must update the certificate in their systems related to DocuSign Connect. The current certificate, which expires on November 11, 2016, will be decommissioned on October 28, 2016.

This document provides information about the differences between the old and the new certificates, along with tips for customers and partners adopting the new certificates.

The following is a list of important changes with the new certificates:

1. Different certificates for different DocuSign environments
2. Change in the name of the certificate
3. Connect feature being used: Signed SOAP envelope vs Mutual TLS

Scenarios

There are two broad scenarios which determine the amount of work that needs to be done in the near and long term for your system.

Scenario 1: Single endpoint supporting multiple DocuSign instances

In this scenario, the same Connect endpoint is being used to support accounts from multiple DocuSign instances, such as DEMO and Production. For example: any partners who integrate with DocuSign Connect using event Notifications and servicing DEMO and Production instances using the same endpoint URL to receive connect messages.

This scenario is not limited to the transition time between the old certificate and the new one, but to a long term switch since, going forward, DocuSign will use different certificates for different instances.

Scenario 2: Single endpoint supporting multiple accounts that can be configured to use either the old or new the new certificate

The new Connect certificate rollout provides DocuSign administrators a way to easily switch between the new and the old certificates at any time. As a result, the same Connect endpoint may need to support/handle messages sent using either certificate.

This scenario is limited to the transition time between the old certificate and the new one. Customers may need to revisit this again when the new certificate expires in 2018.

In both cases, all endpoints are encouraged to be able to support processing of Connect messages with different certificates.

Approach

In either scenario, the first step is to understand the differences between the old and the new certificates. The next step is to plan for adopting the new certificates.

Differences between Old and New Certificates

The following table illustrates the key differences between the current DocuSign certificate and the new certificates.

Certificate CN (Common Name)	DocuSign Instance(s)	Signature Algorithm	Issuer CN (Common Name)	Serial Number	SHA1 Fingerprint
signedby.DocuSign.net (OLD)	ALL	SHA-1 with RSA Encryption	Symantec Class 3 EV SSL CA - G2	0D 37 62 1A 9C 3A AC 19 7A B1 22 06 54 FA A4 39	E6 7C 12 C5 48 29 BE 72 77 D8 C8 45 66 A3 6F B2 58 A2 C6 D7

connect.DocuSign.net	NA1, NA2, NA3 only	SHA-256 with RSA Encryption	Symantec Class 3 Secure Server CA - G4	67 8E 6D 0F 4D 4A C6 22 D5 BB 95 E9 78 38 E6 04	88 7C 9E FD 3A 62 E6 C5 4B 0D 24 A4 C5 7F 41 E8 75 CA E4 A0
demo.connect.DocuSign.net	DEMO, STAGE only	SHA-256 with RSA Encryption	Symantec Class 3 Secure Server CA - G4	18 19 8F 84 E8 CF 9C 2D E1 36 D1 06 4D 1E 5D E3	D2 81 8C 52 63 A9 8C A6 3C E0 CA D3 59 F9 12 73 6C C3 A0 CE
eu.connect.DocuSign.net	EUPROD (EU) only	SHA-256 with RSA Encryption	Symantec Class 3 Secure Server CA - G4	63 ED F5 44 D1 E0 B8 0D 1E DE 09 5A 12 52 98 71	57 26 4F 53 EE F4 36 4E 61 F2 F4 5B EA 50 A9 03 23 29 06 47

Handling Connect messages with different certificates

The impact of the change depends on how the certificate is being used; for Mutual TLS or for Signed SOAP Messages. Here are some tips for each use case:

For Mutual TLS

If the certificate is primarily being used for Mutual TLS, we recommend that you configure your servers to accept the relevant named certificates from the two different issuers - Note that the new certificates have different issuer.

Apache

If you are using Apache, you can configure it to support multiple certificates by setting the SSLCACertificateFile directive to point to a file containing a concatenation of the permitted CA certs (i.e. from the certificate chain for each client cert, take the CA cert in PEM format and put it in this file). More information setting this up can be found at these links:

https://httpd.apache.org/docs/current/mod/mod_ssl.html

http://httpd.apache.org/docs/current/ssl/ssl_howto.html#allclients

Use the SSLRequire directive/Require expression to limit access to the endpoint to client certificates that match a particular pattern. For example, the CN equals signedby.docusign.net. More information about this can be found at this link:

http://httpd.apache.org/docs/current/mod/mod_ssl.html#sslrequire

IIS

If you are using IIS, you can add multiple CA certificates to the relevant certificate store. Note that this has changed on Windows Server 2012 and Windows 8. The following link goes to an article that describes the old and new behaviors under the "Management of trusted issuers for client authentication" section:

https://technet.microsoft.com/en-us/library/dn786429.aspx

If using the Client Authentication Issuers store, see the "Configuring an application or feature to use the Client Authentication Issuers store" in the above link.

For Signed SOAP Message

If you are signing the Connect messages, then you need to use the certificate included in the message to process the Connect message. Given that the messages might be signed using different certificates, you may have look at the fingerprint of certificate in the Connect message and to determine the correct Connect certificate to use when processing the message. It is highly recommended that the handling of fingerprint & CN are implemented to be configurable as a whitelist and not hardcoded. This will insure future updates are simplified and manageable. Whether you are using Apache or IIS, restricting access to the specific CN must be done programmatically.