Question Stephen De Gabrielle · Apr 27, 2017

How to sign certificate requests from a client system?

Hi,

I can't work out how to use the Cache CA Server to process certificate request from external clients!

We are setting up an interface where we use SSL/TLS 'Mutual Authentication' to allow a client system to securely transmit document to our server. (they are off-site and hosting a service for us)

I am not a security expert, but my understanding of setting up mutual authentication where my instance of ensemble is the server, and it is receiving messages from a client is as follows

- 1. I create a CA private key and self-signed certificate (or purchase a cert from one of the big providers)
- 2. Generate the server certificate and private key
- 3. The client generates their own private key and certificate request.
- 4. The client sends me their certificate request (only)
- 5. I use my CA private key and their certificate request to create the client certificate
- 6. I send the Client certificate and my CA certificate to the client.

When the client initiates a connection with my instance of ensemble, the SSL handshake is used to let both parties confirm they are connecting to who they are connecting to*, and establish a secure channel.

While the SSI/TLS configurations facility supports setting up client and server configurations, the Public Key Infrastructure only seems to support signing a certificate request created in the 'InterSystems Public Key Infrastructure (PKI)':

'5. At this point, you have used Caché to create and submit the CSR.' (Submitting a Certificate Signing Request to a Certificate Authority Server at http://docs.intersystems.com/latest/csp/docbook/DocBook.UI.Page.cls?KEY=GCASpki#GCASpkicsrsu bmit)

Unfortunately to do 'Mutual Authentication' we need to sign a certificate request sent by the client system.

I can use OpenSSL to process the certificate request at the command line, but I'd prefer to use the 'InterSystems Public Key Infrastructure (PKI)' facilities if possible.

Is there a folder I should put the certificate request from exteral clients so the Cache CA Server can 'Process pending Certificate Signing Requests' ?

[If the the 'InterSystems Public Key Infrastructure (PKI)' can't be used to sign certificate requests, I'll write a short post on how to do it with OpenSSL on the command line.]

Kind regards,

Stephen

#Ensemble #HealthShare #SSL

Source URL: https://community.intersystems.com/post/how-sign-certificate-requests-client-system