Question
Stefan Cronje · Jul 10, 2017

SHA256 Signing with RSA PSS padding

Hi everyone,

I have a project which requires the sending of JSON messages to an external service provider using REST. The service provider requires the message contents to be signed.

Their instructions:

1. Add a header called "Date" with the the date and time in a specific format - done
2. Add the client's certificate password in a field in the header - done
3. Create a string which consist of the {Date}{newline}{Password}{newline}{etc}{Message Body}.
    1. Convert to a UTF8 byte array
    2. SHA256 sign the value with the certificate and private key **and use RSA PSS padding**
    3. Base 64 Encode the value and place it in a Signature field in the header.

I've done the following:

1. Set up X.509 credentials using the certificate and private key files
2. Created the string to sign as per their instruction
3. Performed a $zconvert, 'O', 'UTF8' on the string
4. Used %SYSTEM.Encryption -> RSASHASign() and Base64Encode()

This does not seem to be correct, as the service provider keeps rejecting the messages.

Is there a way to specify the RSA padding to be PSS?
Am I using the wrong method?
Does this method actually use PSS padding and I should look for the problem somewhere else?
Are these methods endian-ness aware?

Thank you in advance.

#Caché #Callout #REST API #SOAP #Encryption