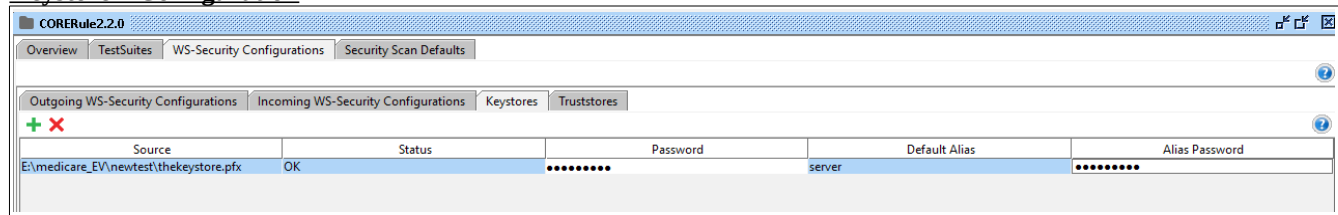


Converted the server certificate .pem to .pfx (public key)

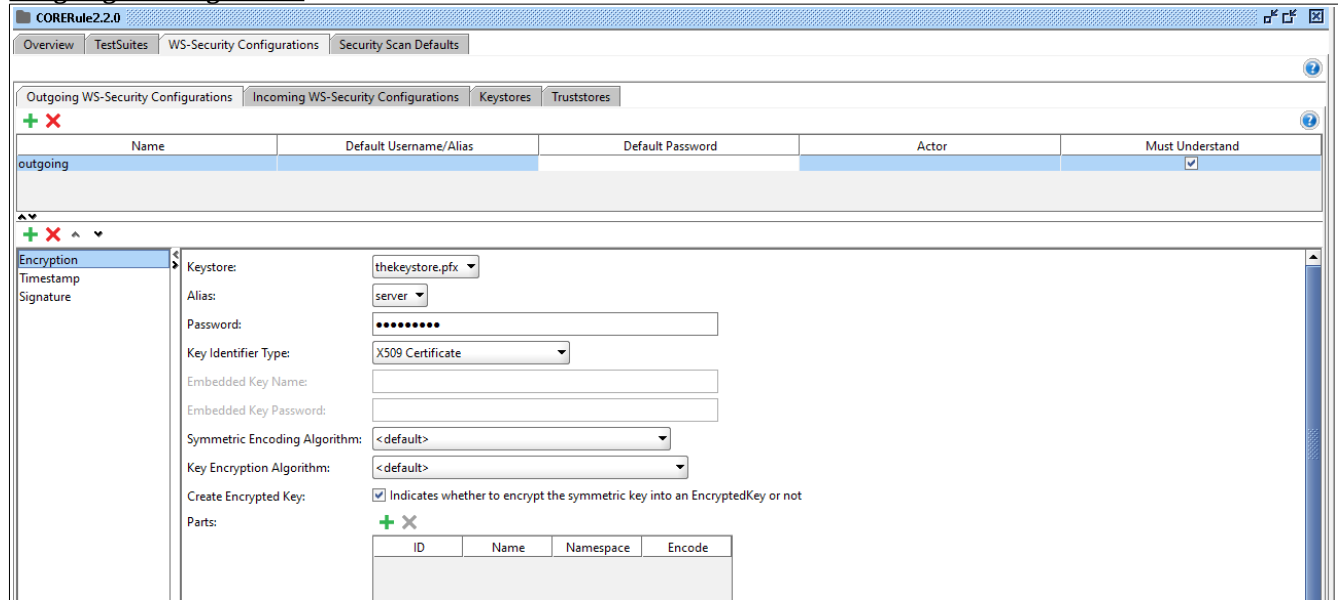
Keystore – Configuration



The screenshot shows the 'Keystores' tab in the 'Security Scan Defaults' section of CORERule2.2.0. A table lists the configured keystores:

Source	Status	Password	Default Alias	Alias Password
E:\medicare_EV\newtest\thekeystore.pfx	OK	server

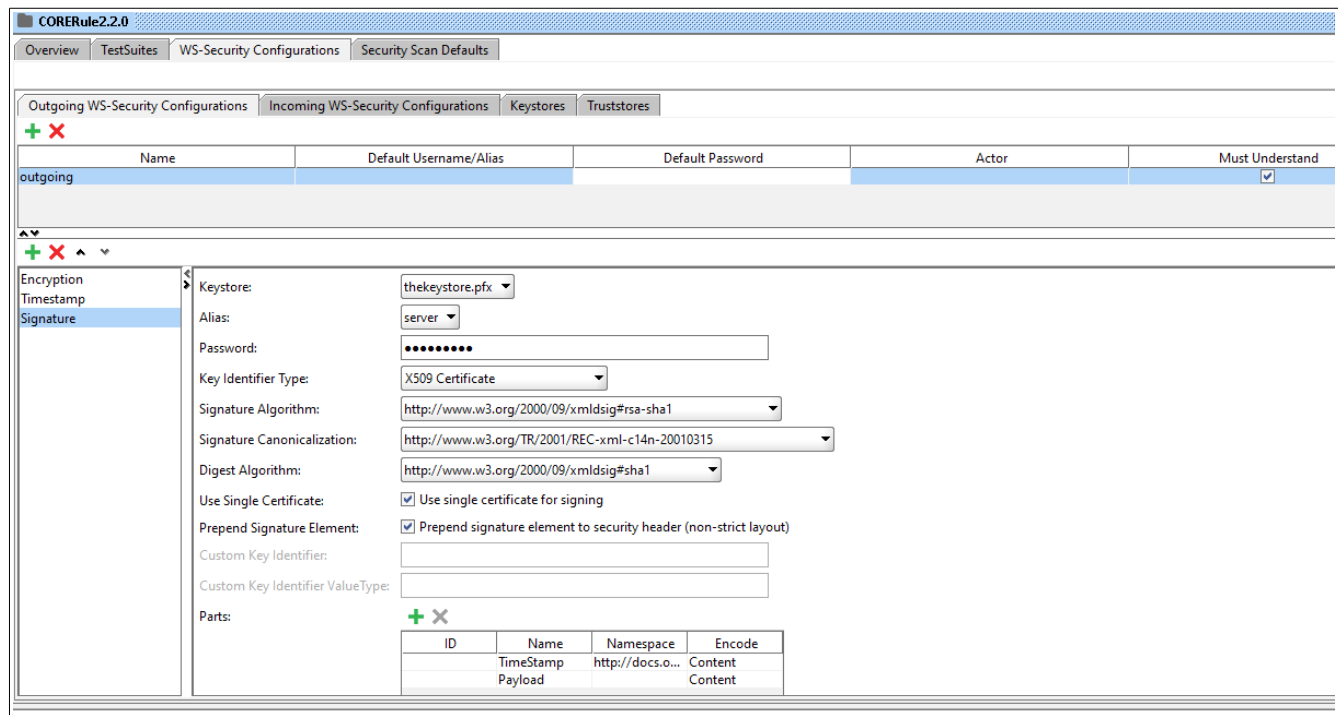
Outgoing – Configuration



The screenshot shows the 'Encryption' configuration for the 'outgoing' profile. The configuration is as follows:

- Keystore: thekeystore.pfx
- Alias: server
- Password:
- Key Identifier Type: X509 Certificate
- Embedded Key Name: (empty)
- Embedded Key Password: (empty)
- Symmetric Encoding Algorithm: <default>
- Key Encryption Algorithm: <default>
- Create Encrypted Key: Indicates whether to encrypt the symmetric key into an EncryptedKey or not

The 'Parts' table is empty.



The screenshot shows the 'Signature' configuration for the 'outgoing' profile. The configuration is as follows:

- Keystore: thekeystore.pfx
- Alias: server
- Password:
- Key Identifier Type: X509 Certificate
- Signature Algorithm: http://www.w3.org/2000/09/xmldsig#rsa-sha1
- Signature Canonicalization: http://www.w3.org/TR/2001/REC-xml-c14n-20010315
- Digest Algorithm: http://www.w3.org/2000/09/xmldsig#sha1
- Use Single Certificate: Use single certificate for signing
- Prepend Signature Element: Prepend signature element to security header (non-strict layout)
- Custom Key Identifier: (empty)
- Custom Key Identifier ValueType: (empty)

The 'Parts' table contains the following entries:

ID	Name	Namespace	Encode
	TimeStamp	http://docs.o...	Content
	Payload		Content

Incoming – Configuration

Projects

- CORERule2.2.0
 - CoreSoapBinding
 - BatchResultsAckSubmitTransact
 - BatchResultsRetrievalTransactor
 - BatchSubmitAckRetrievalTransactor
 - BatchSubmitTransactor
 - GenericBatchReceiptConfirmatic
 - GenericBatchRetrievalTransactor
 - GenericBatchSubmissionTransactor
 - RealTimeTransactor
 - Request 1

CORERule2.2.0

Overview TestSuites WS-Security Configurations Security Scan Defaults

Outgoing WS-Security Configurations Incoming WS-Security Configurations Keystores Truststores

Name	Decrypt Keystore	Signature Keystore	Password
incoming	thekeystore.pfx	thekeystore.pfx	*****

Response

Request 1

https://soap.hets-270-271.cms.gov/eligibility/realtime/soap

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header><wssc:Security xmlns:wssc="http://docs.oasis-open.org/wssc/ns/2004/01/soap-header">
    <wssc:Reference URI="#Body-b91db7a0-6b78-4316-bf90-385cefed1fab"/>
  </soap:Header>
  <soap:Body wsu:Id="id-5A6CADF59266D29AF9156932350225578" xmlns:wsu="http://www.w3.org/2003/05/soap-envelope">
    <ns1:COREEnvelopeRealTimeRequest xmlns:ns1="http://www.cagb.org/2019/09/realtime">
      <PayloadType>X12_270_Request_005010X279A1</PayloadType>
      <ProcessingMode>RealTime</ProcessingMode>
      <PayloadID>d5cf23d4-240d-1d9e-b7d5-ab0f9185296b</PayloadID>
      <TimeStamp>2019-09-16T05:34:33Z</TimeStamp>
      <SenderID>W802294900</SenderID>
      <ReceiverID>CMS</ReceiverID>
      <CORERuleVersion>2.2.0</CORERuleVersion>
      <Payload>ISA*00*          *00*          *ZZ*W8022949
    </ns1:COREEnvelopeRealTimeRequest>
  </soap:Body>
</soap:Envelope>
```

```
</Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-core-schema#sha256"/>
  <DigestValue>FPFw/zBD89icG7NG/G7ULS6JxLyLEngk7Nu6SDsJAw=</DigestValue>
</Reference>
<Reference URI="#Body-b91db7a0-6b78-4316-bf90-385cefed1fab">
  <Transforms>
    <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-core-schema#sha256"/>
  <DigestValue>h2D+IqkIkWlxg5zIHqyrbzqsM072oAs6QvZbecB2s=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>gQR/omybRj2To3WQWJpRpElkWRhGIRL2tqAt3kezrtPQpG1wy8GRbjI
</SignatureValue>
<KeyInfo>
  <wssc:SecurityTokenReference xmlns:wssc="http://docs.oasis-open.org/wssc/ns/2004/01/soap-header">
    <wssc:Reference URI="#SecurityToken-ba71224c-8c5d-4c5b-9236-385cefed1fab"/>
  </wssc:SecurityTokenReference>
</KeyInfo>
</Signature>
</wssc:Security>
</soap:Header>
<soap:Body wsu:Id="Body-b91db7a0-6b78-4316-bf90-385cefed1fab" xmlns:wsu="http://www.w3.org/2003/05/soap-envelope">
  <cor:COREEnvelopeRealTimeResponse>
    <PayloadType>CoreEnvelopeError</PayloadType>
    <ProcessingMode>RealTime</ProcessingMode>
    <PayloadID>d5cf23d4-240d-1d9e-b7d5-ab0f9185296b</PayloadID>
    <TimeStamp>2019-10-24T09:13:45.072Z</TimeStamp>
    <SenderID>CMS</SenderID>
    <ReceiverID>W802294900</ReceiverID>
    <CORERuleVersion>2.2.0</CORERuleVersion>
    <ErrorMessage>The signature could not be verified.</ErrorMessage>
  </cor:COREEnvelopeRealTimeResponse>
```

Header Connection

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header><wssc:Security xmlns:wssc="http://docs.oasis-open.org/wssc/ns/2004/01/soap-header">
    <wssc:Reference URI="#Body-b91db7a0-6b78-4316-bf90-385cefed1fab"/>
  </soap:Header>
  <soap:Body wsu:Id="id-5A6CADF59266D29AF9156932350225578" xmlns:wsu="http://www.w3.org/2003/05/soap-envelope">
    <ns1:COREEnvelopeRealTimeRequest xmlns:ns1="http://www.cagb.org/2019/09/realtime">
      <PayloadType>X12_270_Request_005010X279A1</PayloadType>
      <ProcessingMode>RealTime</ProcessingMode>
      <PayloadID>d5cf23d4-240d-1d9e-b7d5-ab0f9185296b</PayloadID>
      <TimeStamp>2019-09-16T05:34:33Z</TimeStamp>
      <SenderID>W802294900</SenderID>
      <ReceiverID>CMS</ReceiverID>
      <CORERuleVersion>2.2.0</CORERuleVersion>
      <Payload>ISA*00*          *00*          *ZZ*W8022949
    </ns1:COREEnvelopeRealTimeRequest>
  </soap:Body>
</soap:Envelope>
```

```
</Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-core-schema#sha256"/>
  <DigestValue>FPFw/zBD89icG7NG/G7ULS6JxLyLEngk7Nu6SDsJAw=</DigestValue>
</Reference>
<Reference URI="#Body-b91db7a0-6b78-4316-bf90-385cefed1fab">
  <Transforms>
    <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-core-schema#sha256"/>
  <DigestValue>h2D+IqkIkWlxg5zIHqyrbzqsM072oAs6QvZbecB2s=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>gQR/omybRj2To3WQWJpRpElkWRhGIRL2tqAt3kezrtPQpG1wy8GRbjI
</SignatureValue>
<KeyInfo>
  <wssc:SecurityTokenReference xmlns:wssc="http://docs.oasis-open.org/wssc/ns/2004/01/soap-header">
    <wssc:Reference URI="#SecurityToken-ba71224c-8c5d-4c5b-9236-385cefed1fab"/>
  </wssc:SecurityTokenReference>
</KeyInfo>
</Signature>
</wssc:Security>
</soap:Header>
```

Header	Value
Connection	close
#status#	HTTP/1.1 403 Forbidden
WWW-Authenticate	default
X-Backside-Transport	FAIL FAIL
Content-Type	application/soap+xml

Not Yet Configured
Authorization has not been set for protected services.
Use the *Authorization* drop down to configure.