

Kald af PingService via SOAPUI

Kald af PingService via SOAPUI

Author: Integration Expert Team (IET)

Owner: Integration Expert Team (IET)

Kald af PingService via SOAPUI

1. Dokumenthistorik

Revisioner

Dato for denne version: 09.04.2014	Dato for næste version <i>ukendt</i>
------------------------------------	--------------------------------------

Version	Dato	Ændringer	Ændringer markeret
0.1	09.04.2014	Første version	N

Kald af PingService via SOAPUI

Indholdsfortegnelse

1.	Dokumenthistorik.....	2
2.	Indledning.....	4
3.	Forudsætninger.....	5
4.	Opret projekt.....	6
5.	WS-Security Configurations.....	7
5.1	Opret Keystore.....	7
5.2	Opret Truststore.....	8
5.3	Opret Outgoing WSS Configuration.....	9
5.4	Opret Incoming WSS Configuration.....	14
6.	Opsætning af Request.....	16
6.1	Tilføj wsa headers.....	16
6.2	Specificer Endpoint.....	18
6.3	Anvend Incoming WSS configuration.....	19
6.4	Anvend Outgoing WSS Configuration.....	21
7.	Send Request.....	23

Kald af PingService via SOAPUI

2. Indledning

Dette dokument er lavet som en vejledning til at skabe hul igennem til ATP's PingService udstillet under ATP's Web Service Provider profil. Kan man gennemføre dette kald ved man derfor, at man opfylder de generelle krav beskrevet i profilen.

Det er hensigten at et sådan hul igennem kald, kan hjælpe som reference når anvender laver den egentlige system implementering til kald af servicen.

Den klient vi har valgt at anvende og beskrive brugen af i dette dokument er SOAPUI version 5.0.0.



Kald af PingService via SOAPUI

3. Forudsætninger

Der skal være oprettet en IntegrationsAftale med ATP om brug af webservicen, herunder udveksling af et "Teknisk bilag til Integrationsaftale", hvori der indgår kontakt oplysninger, information om de anvendte certifikater, samt hvilke IP net, kaldet kan komme fra.

Desuden skal anvenderen have et virksomheds test certifikat (TDC OCES Systemtest CA II eller TRUST2408 Systemtest VIII CA) udstedt af DanID.

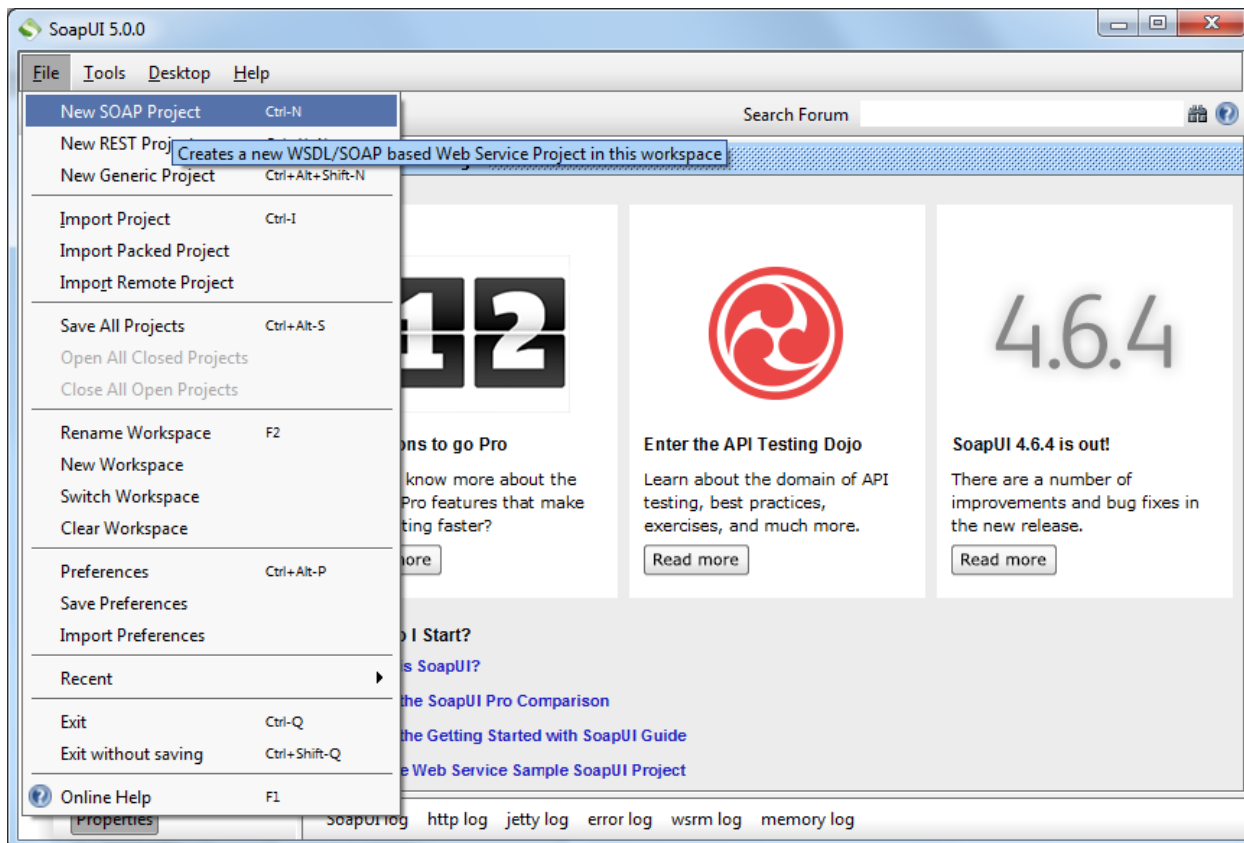
For at kunne autentificere svaret skal anvender have enten ATPs public key, eller rodcertifikatet, alt efter hvilken form for autentificering man ønsker at foretage.

PingService.wsdl medsendt fra ATP i forbindelse med oprettelsen af IntegrationsAftalen.

Kald af PingService via SOAPUI

4. Opret projekt

Begynd med at oprette et nyt projekt:

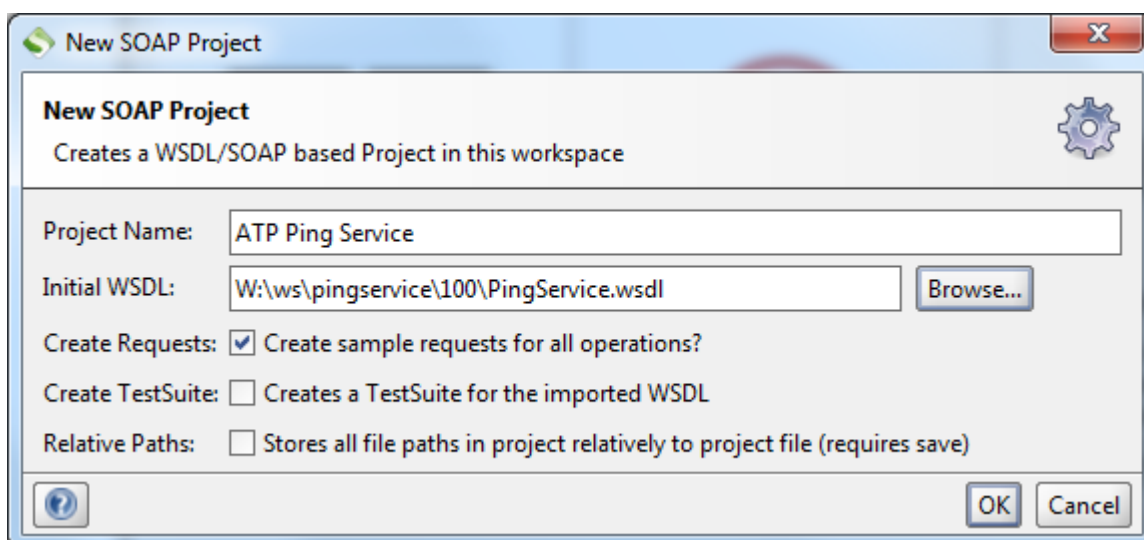


Project Name: Navngiv projektet.

Initial WSDL: Der henvises til den PingService.wsdl ATP har medsendt i aftalen.

Create Requests: sæt hak.

Tryk OK.



Kald af PingService via SOAPUI

5. WS-Security Configurations

Dobbeltklik på projektet.

Vælg fanebladet WS-Security Configurations.

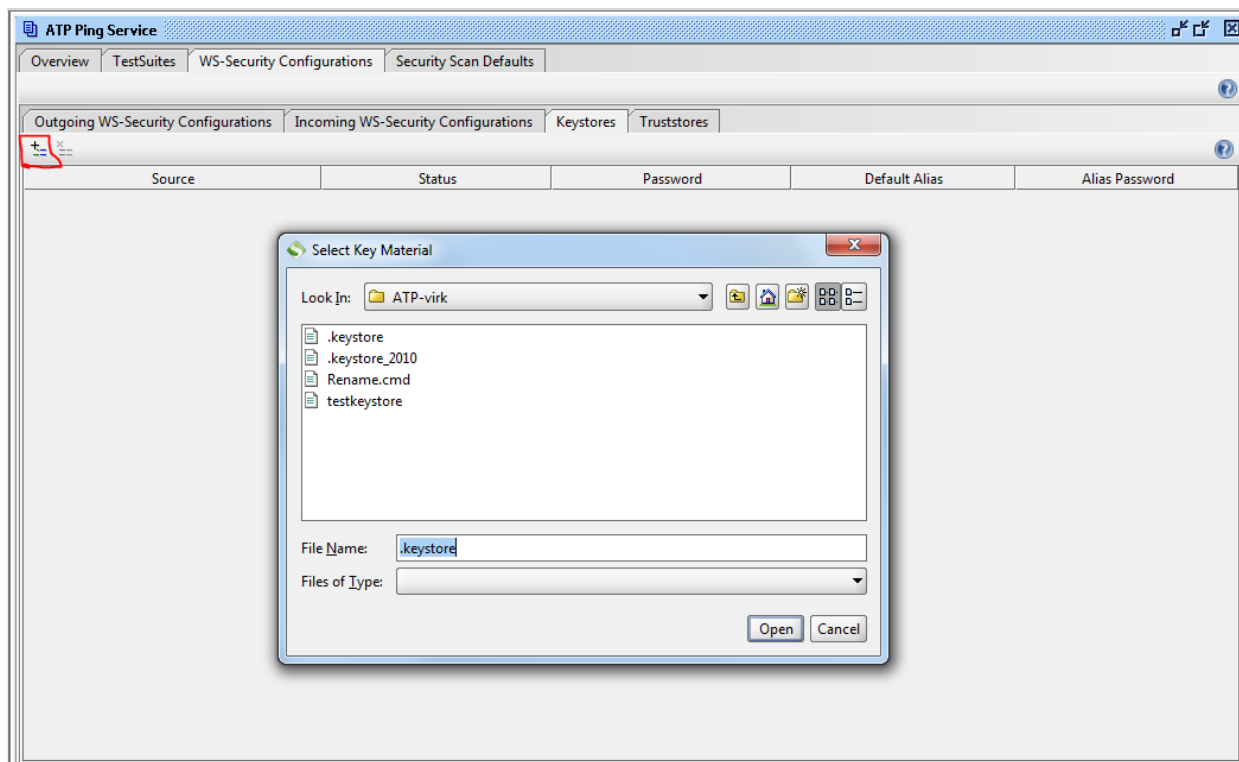
5.1 Opret Keystore

Vælg fanebladet Keystores

Tilføj en ny Keystore ved at klikke på plusset (markeret med rød ring på billedet herunder).

Angiv den keystore der indeholder virksomhedens test certifikat (TDC OCES Systemtest CA II eller TRUST2408 Systemtest VIII CA) udstedt af DanID

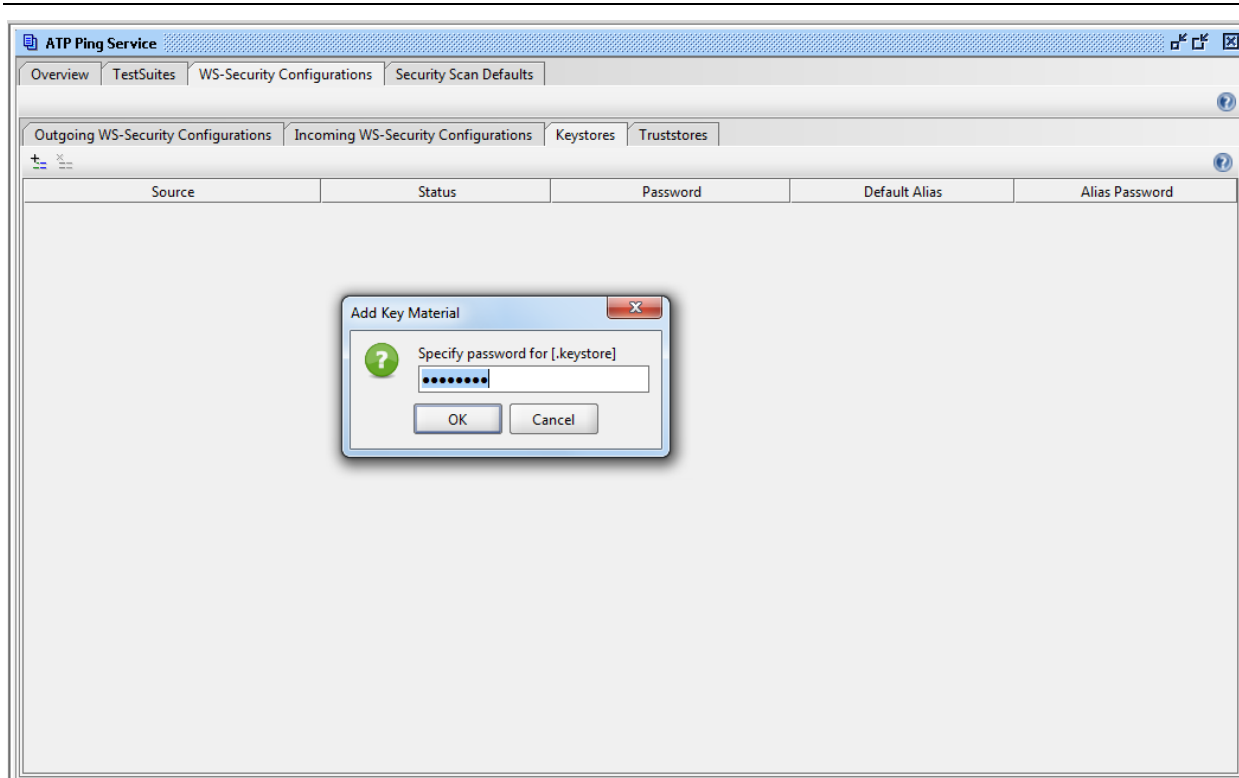
Tryk Open.



Indtast password for keystore.

Tryk OK.

Kald af PingService via SOAPUI



5.2 Opret Truststore

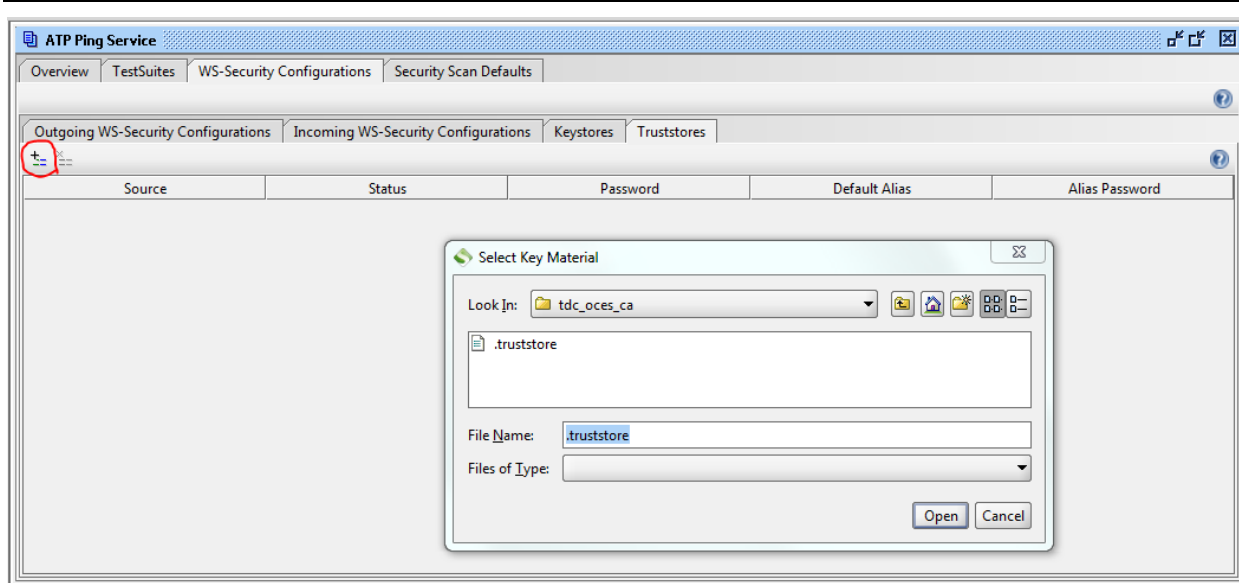
Vælg fanebladet Truststores.

Tilføj en ny Truststore ved at klikke på pluset (markeret med rød cirkel på billedet herunder).

Angiv den truststore som indeholder ATP's public key, eller alternativt rodcertifikatet, alt efter hvad man ønsker at autentificerer svar beskederne ud fra. (Begge dele kan fås fra ATP)

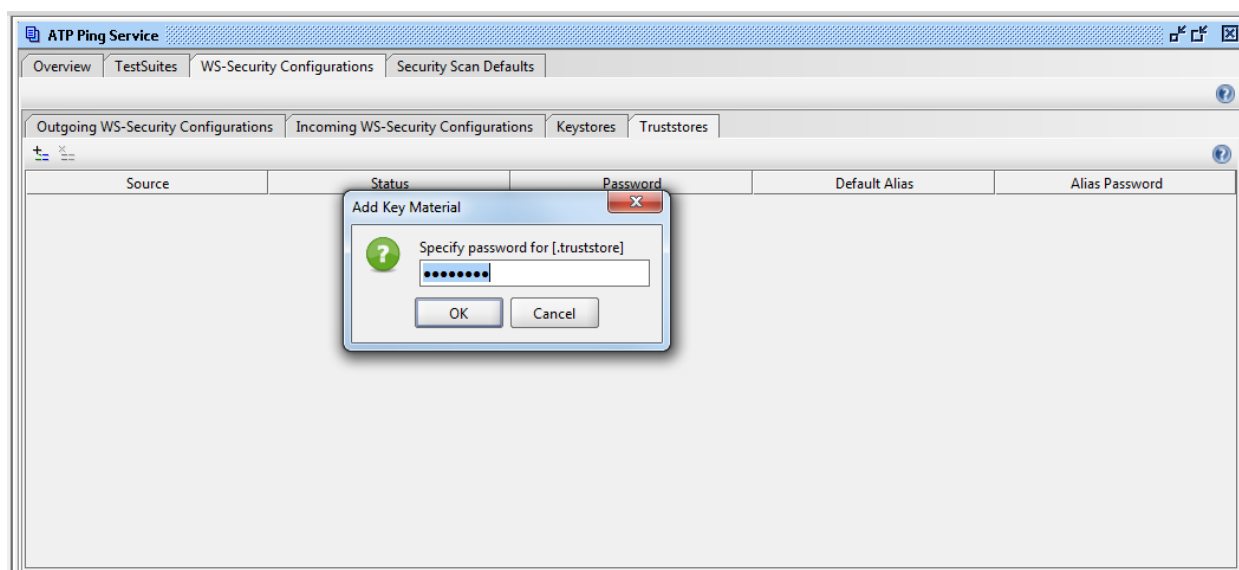
Tryk Open.

Kald af PingService via SOAPUI



Indtast password for truststore.

Tryk OK.



5.3 Opret Outgoing WSS Configuration

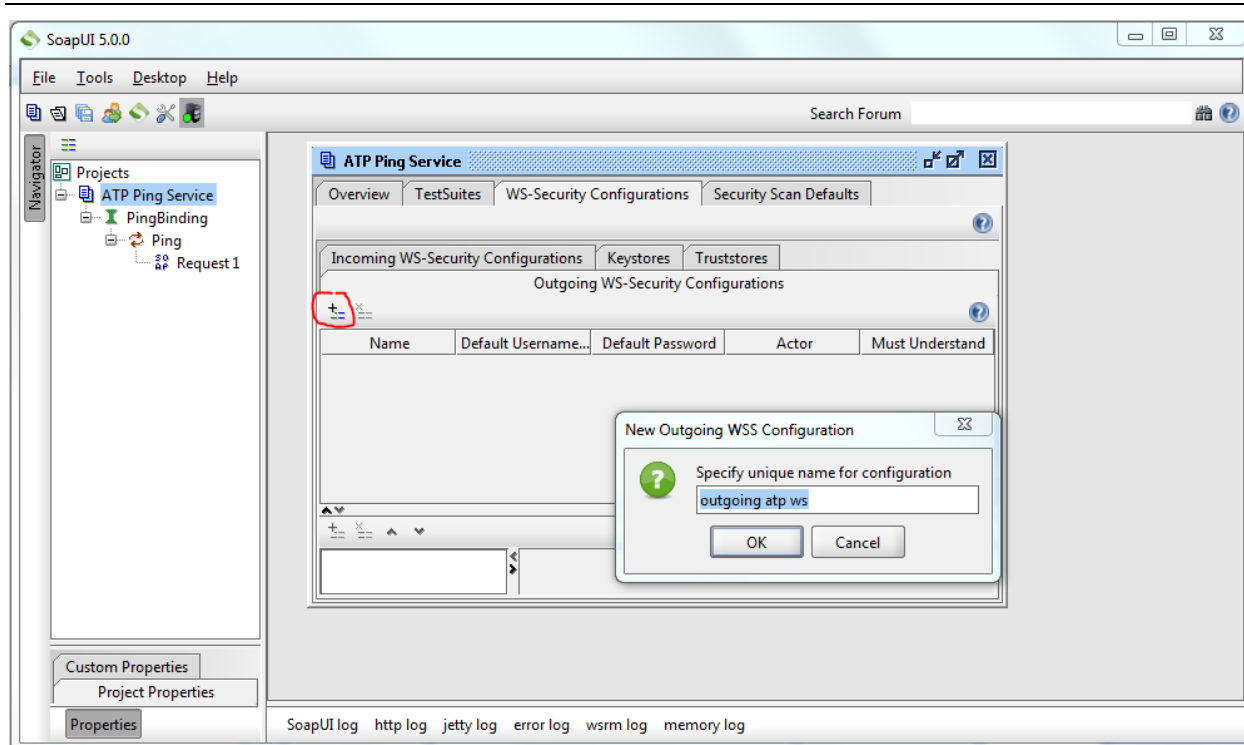
Vælg fanebladet Outgoing WSS Configurations.

Tilføj en ny "Outgoing WSS Configuration" ved at klikke på plusset (markeret med rød cirkel på billedet herunder).

Angiv et navn for konfigurationen f.eks. "outgoing atp ws"

Tryk OK.

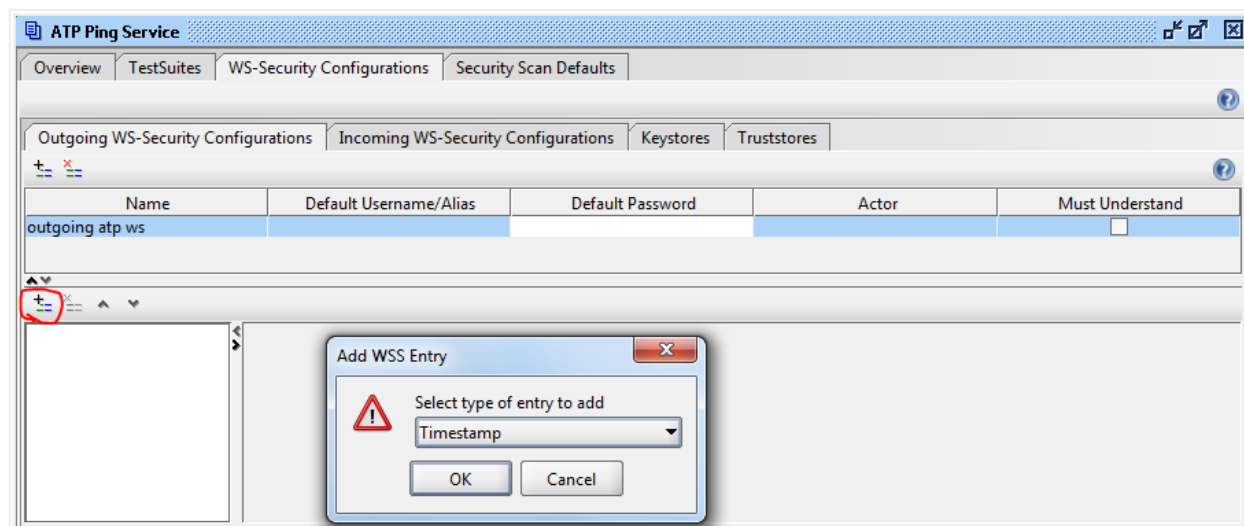
Kald af PingService via SOAPUI



Tilføj en ny WSS entry ved at klikke på plusset (markeret med rød cirkel på billedet herunder).

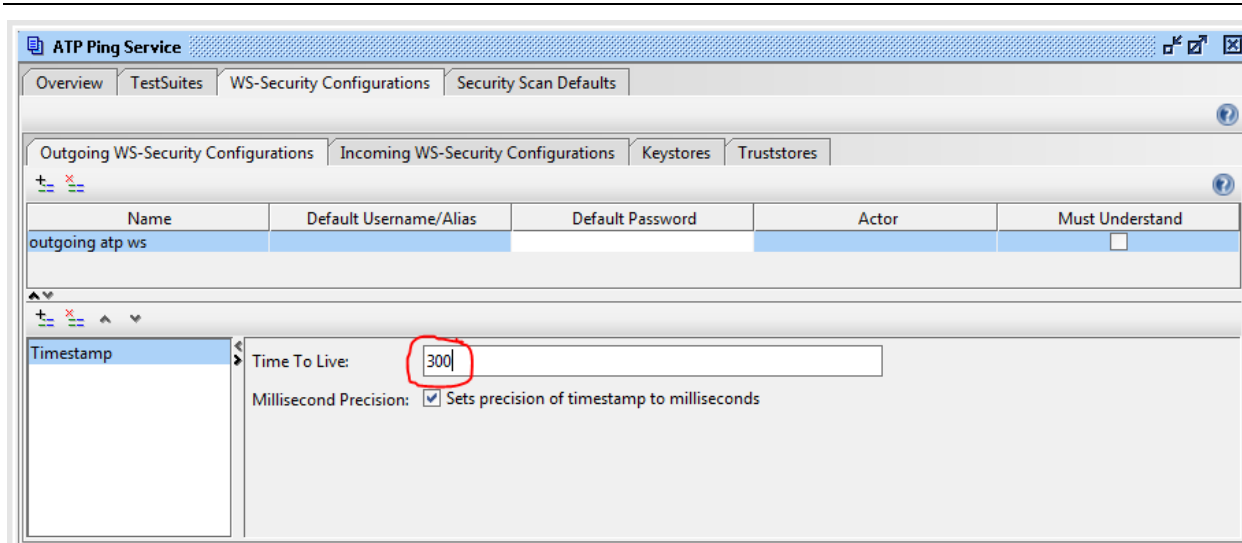
Vælg typen Timestamp.

Tryk OK.



Sæt Time To Live: til 300 (atp godtager ikke Timestamps ældre end 5 min.)

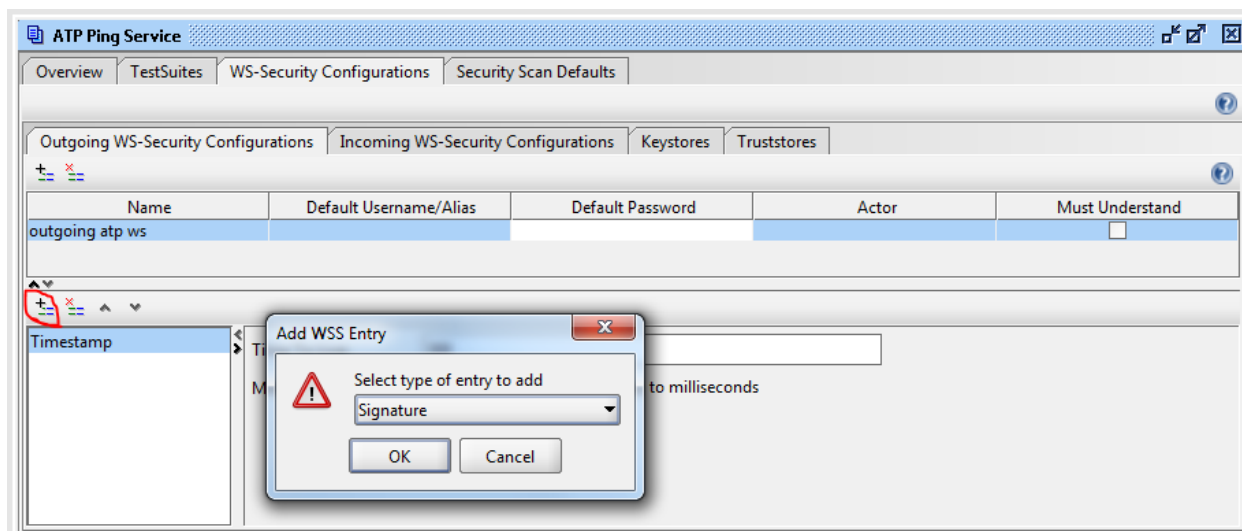
Kald af PingService via SOAPUI



Tilføj en ny WSS entry ved at klikke på plusset (markeret med rød cirkel på billedet herunder).

Vælg typen Signature.

Tryk OK.



Vælg keystore.

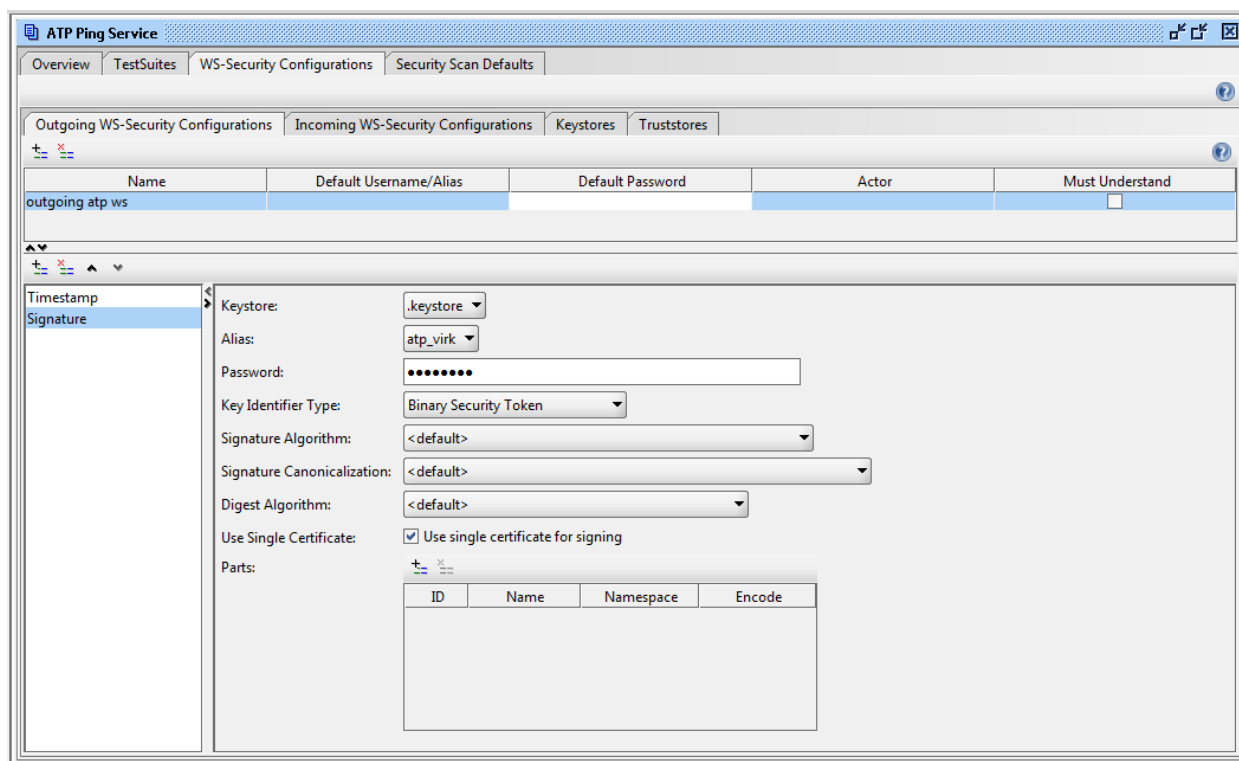
Vælg Alias.

Indtast Password (til keystore).

Key Identifier Type: sættes til "Binary Security Token"

Use Single Certificate: sæt hak.

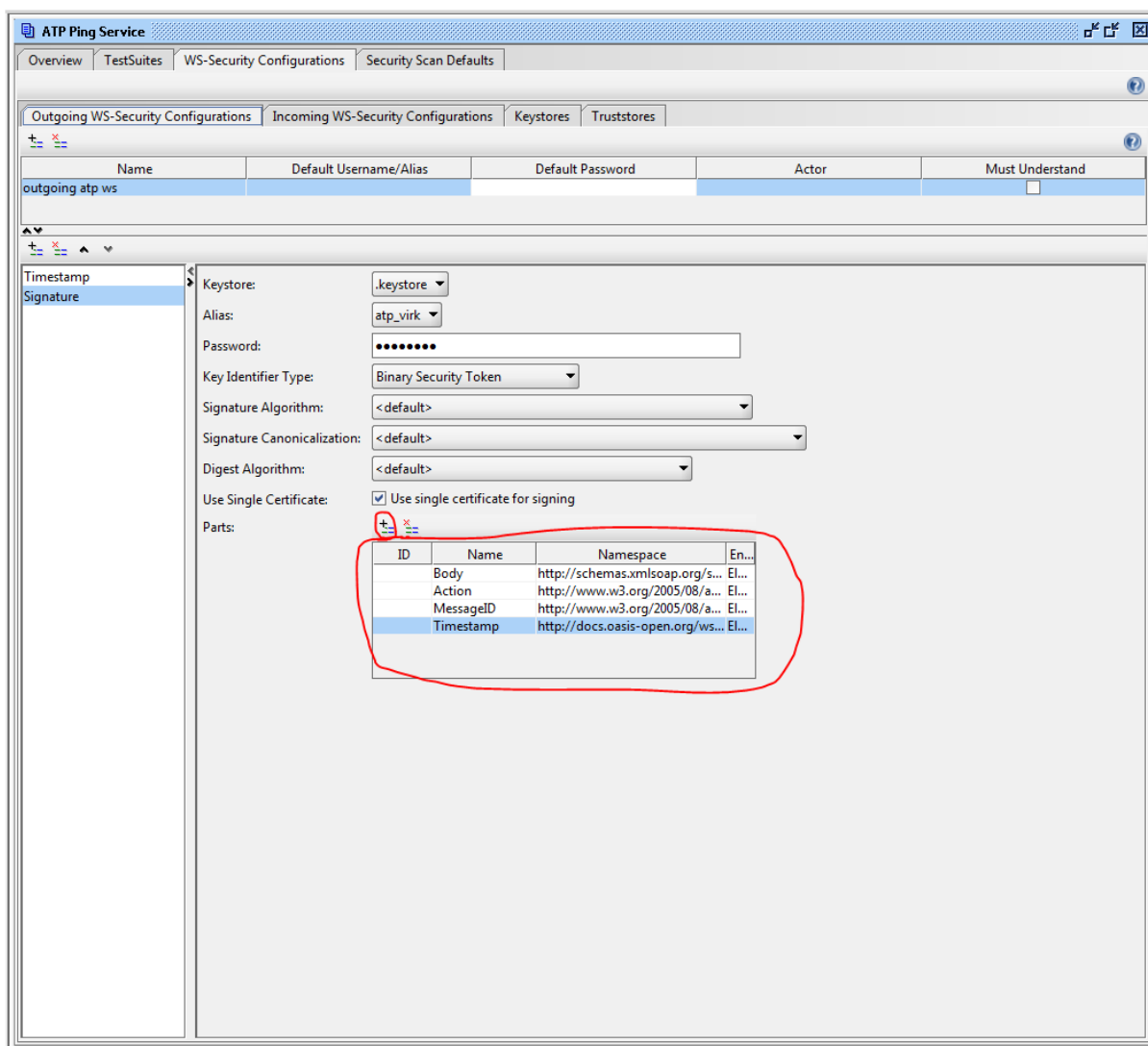
Kald af PingService via SOAPUI



Så skal det defineres hvilke dele af beskeden der skal signeres. Det gøres ved at tilføje "Parts".

Tilføj 4 nye "Parts" ved at klikke på plusset (markeret med rød cirkel på billedet herunder).

Kald af PingService via SOAPUI



Udfyld med følgende værdier (vær opmærksom på store/små bogstaver i navnet):

ID	Name	Namespace	Encode
	Body	http://schemas.xmlsoap.org/soap/envelope/	Element
	Timestamp	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	Element
	Action	http://www.w3.org/2005/08/addressing	Element
	MessageID	http://www.w3.org/2005/08/addressing	Element

Kald af PingService via SOAPUI

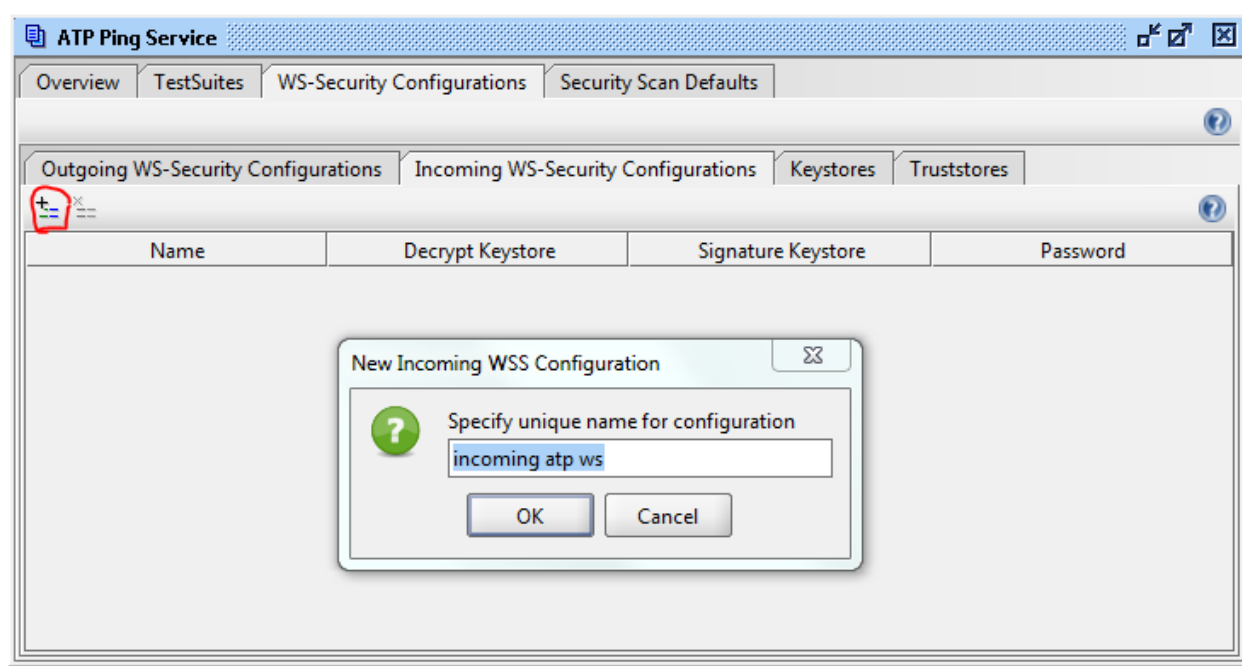
5.4 Opret Incoming WSS Configuration

Vælg fanebladet Incoming WS-Security Configurations.

Tilføj en ny "Incoming WSS Configuration" ved at klikke på plusset (markeret med rød cirkel på billedet herunder).

Angiv et navn for konfigurationen f.eks. "incoming atp ws"

Tryk OK.

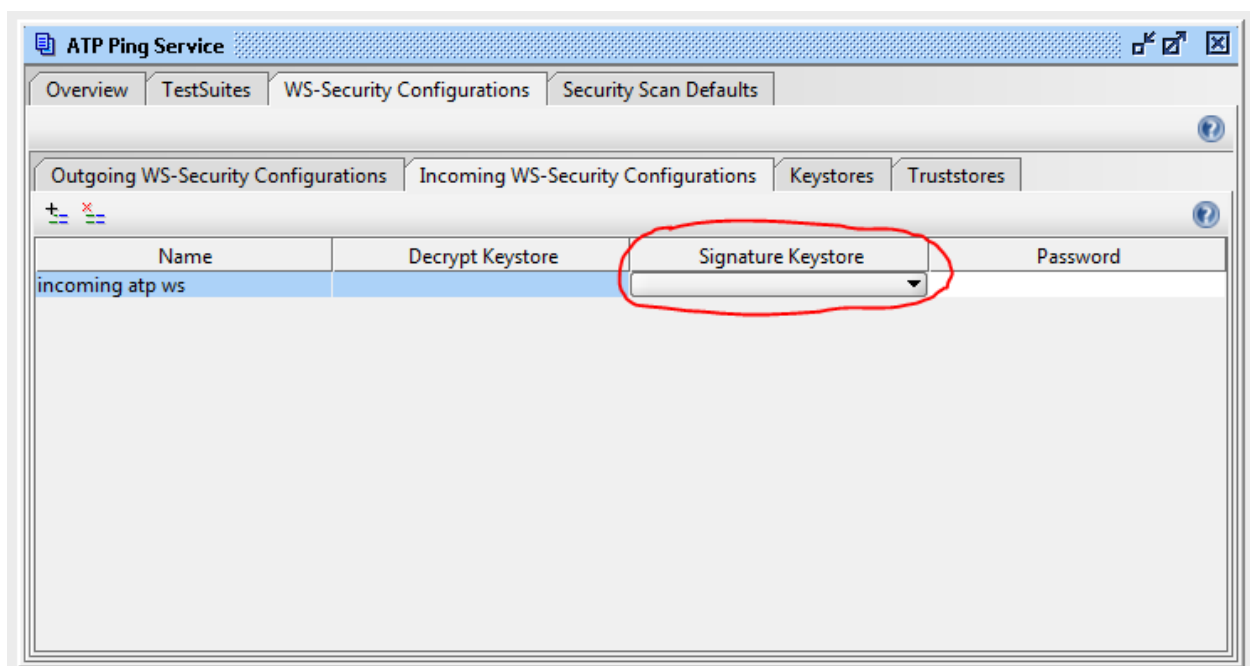


Angiv "Signature Keystore" for konfigurationen.

Det skal være den truststore hvor ATP's public key er gemt eller alternativt rodcertifikatet. Se 5.2.

På denne måde kan man via konfigurationen angive hvordan signaturen på det indkomne svar skal autentificeres.

Kald af PingService via SOAPUI



Kald af PingService via SOAPUI

6. Opsætning af Request

6.1 Tilføj wsa headers

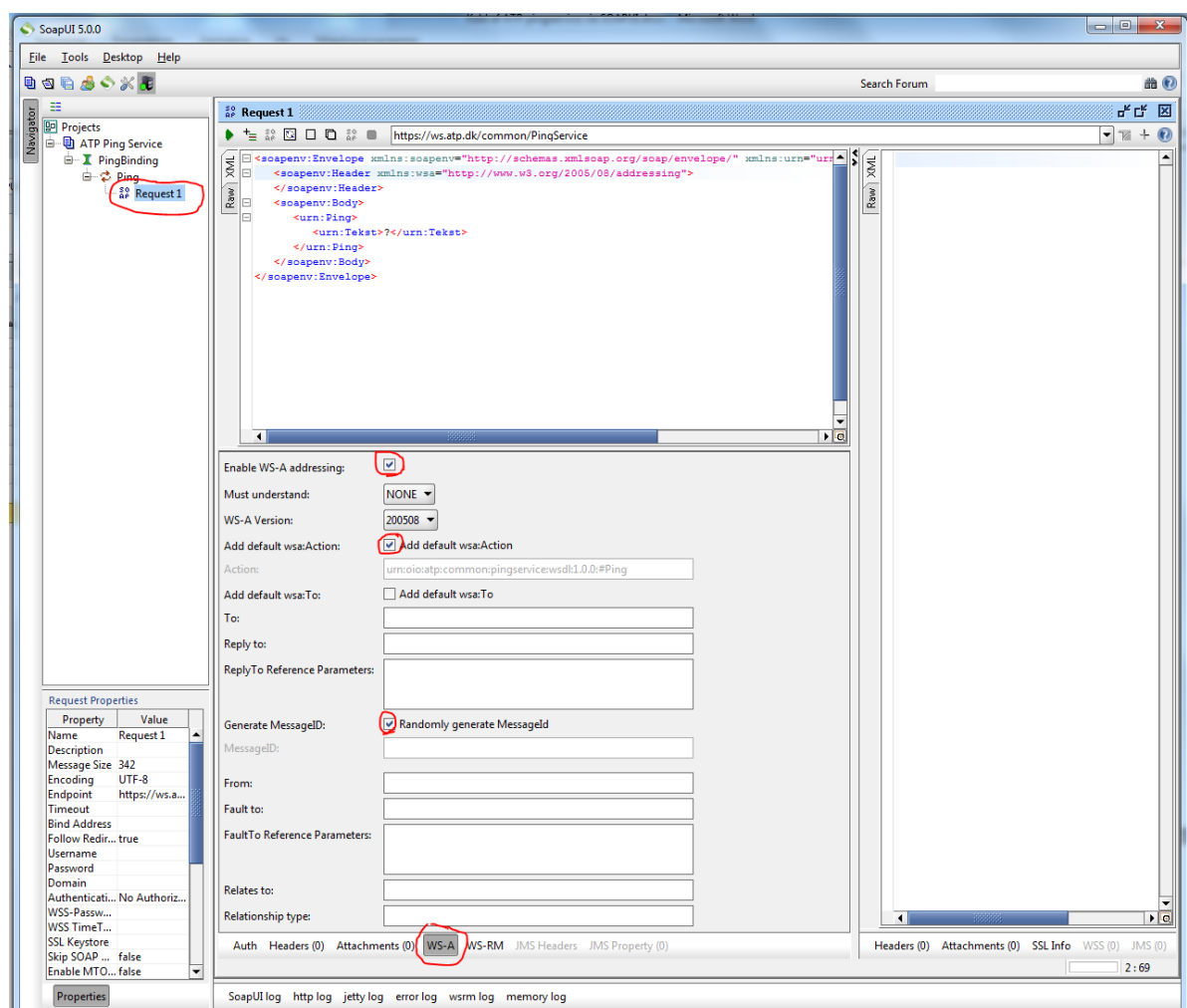
Dobbelt klik på Request 1 for at få request vinduet frem.

Forneden vælg WS-A (se billede nedenfor).

Sæt hak ved EnableWS-A addressing

Sæt hak ved Add default wsaAction

Sæt hak ved GenerateMessageID

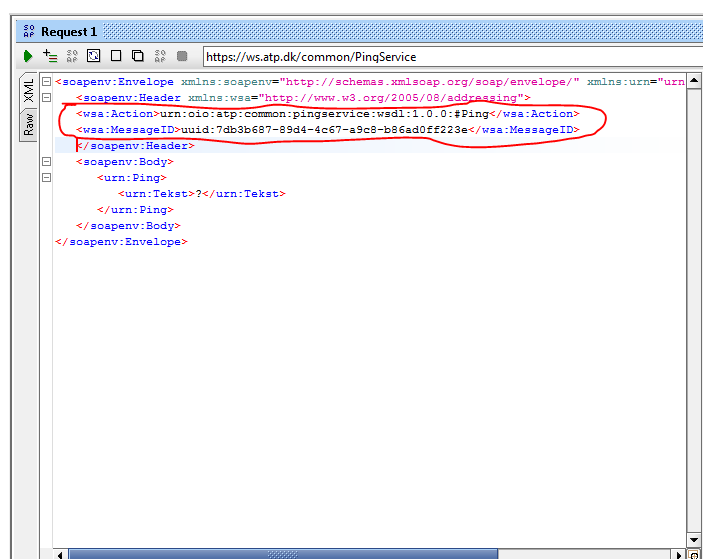
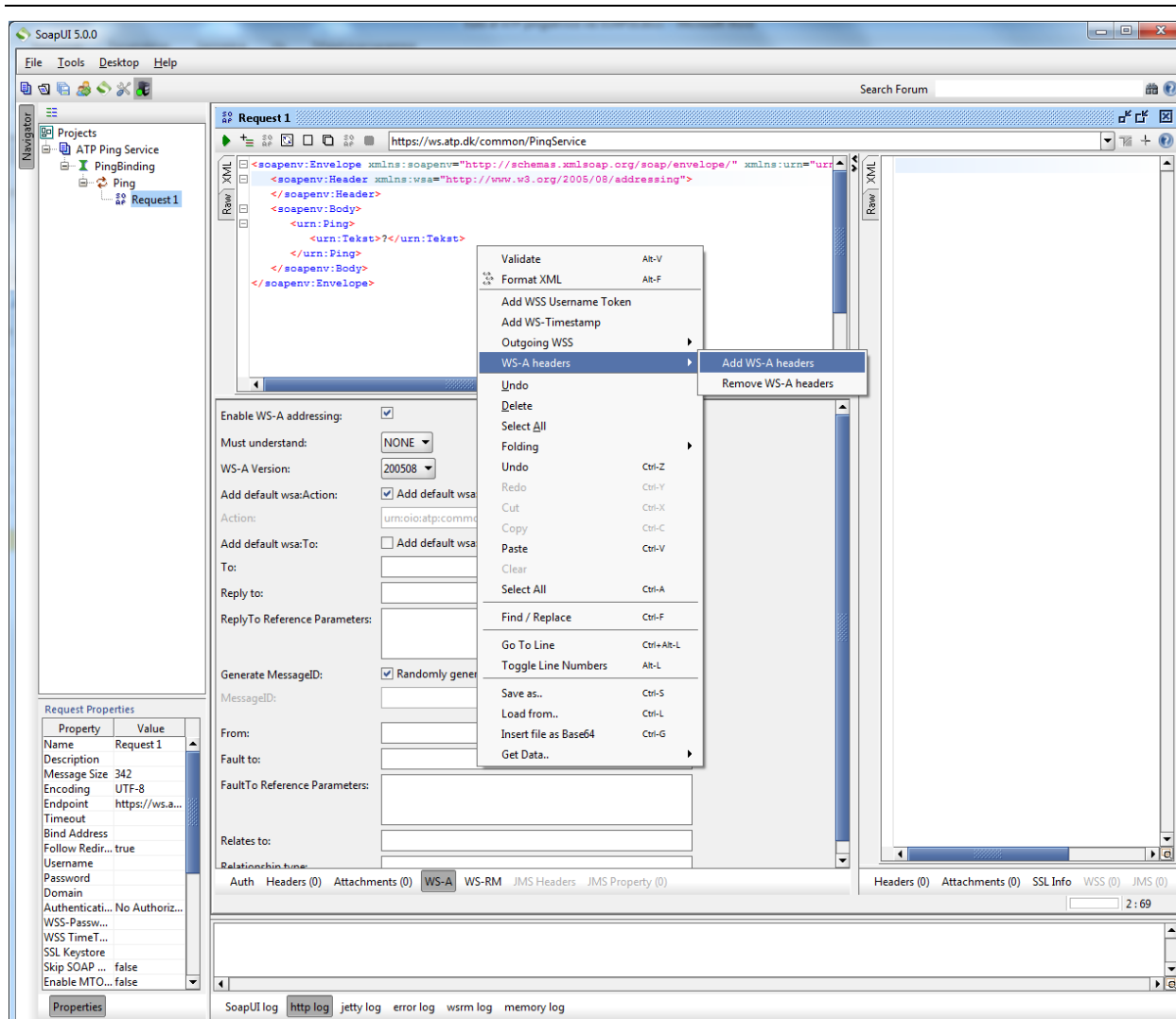


Højreklik i requesten.

Vælg "WS-A headers" i dropdown menuen, og vælg her under "Add W-A headers".

På denne måde får man tilføjet Action og MessageID til Headeren.

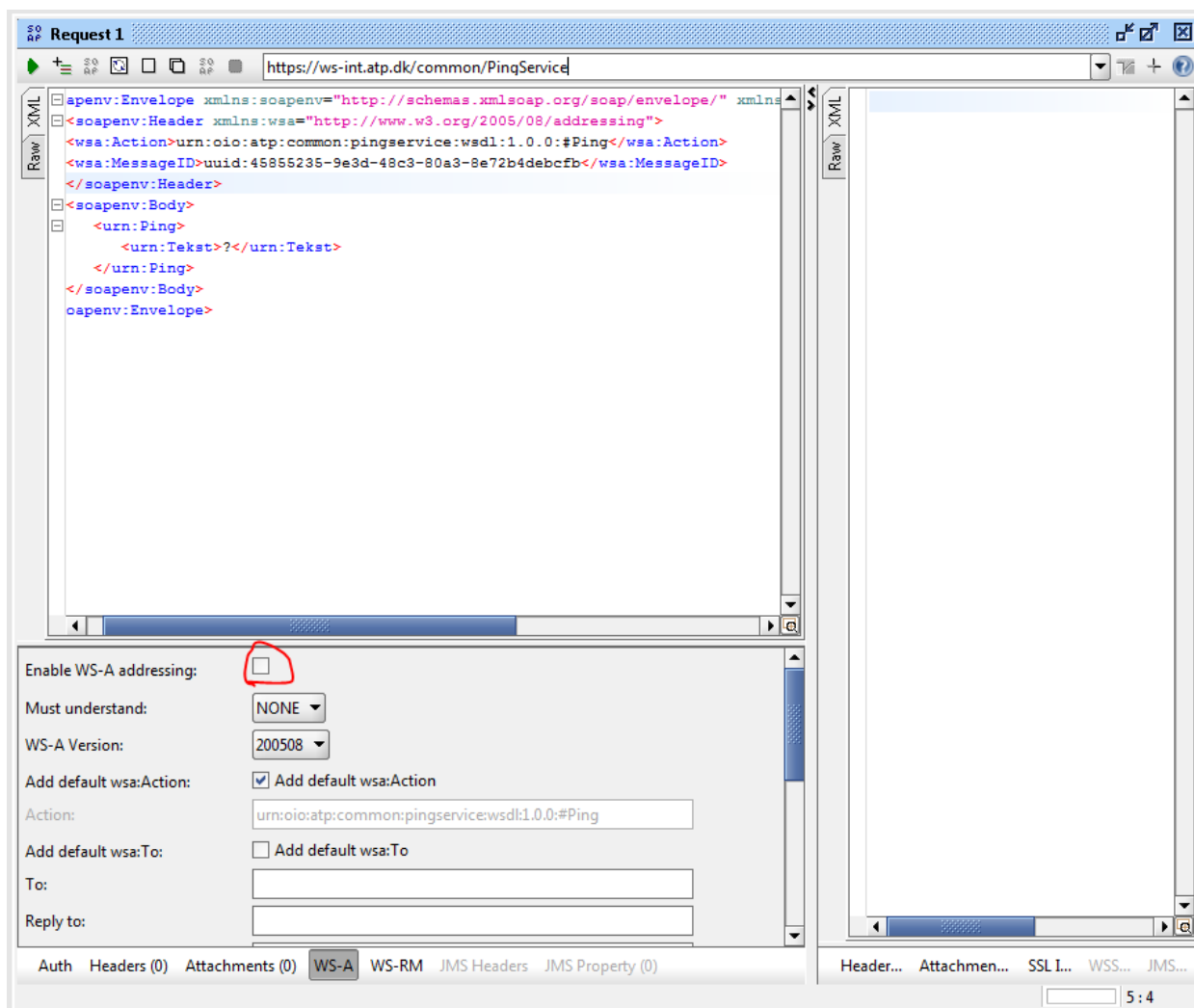
Kald af PingService via SOAPUI



Forneden vælg WS-A (se billede nedenfor).

Kald af PingService via SOAPUI

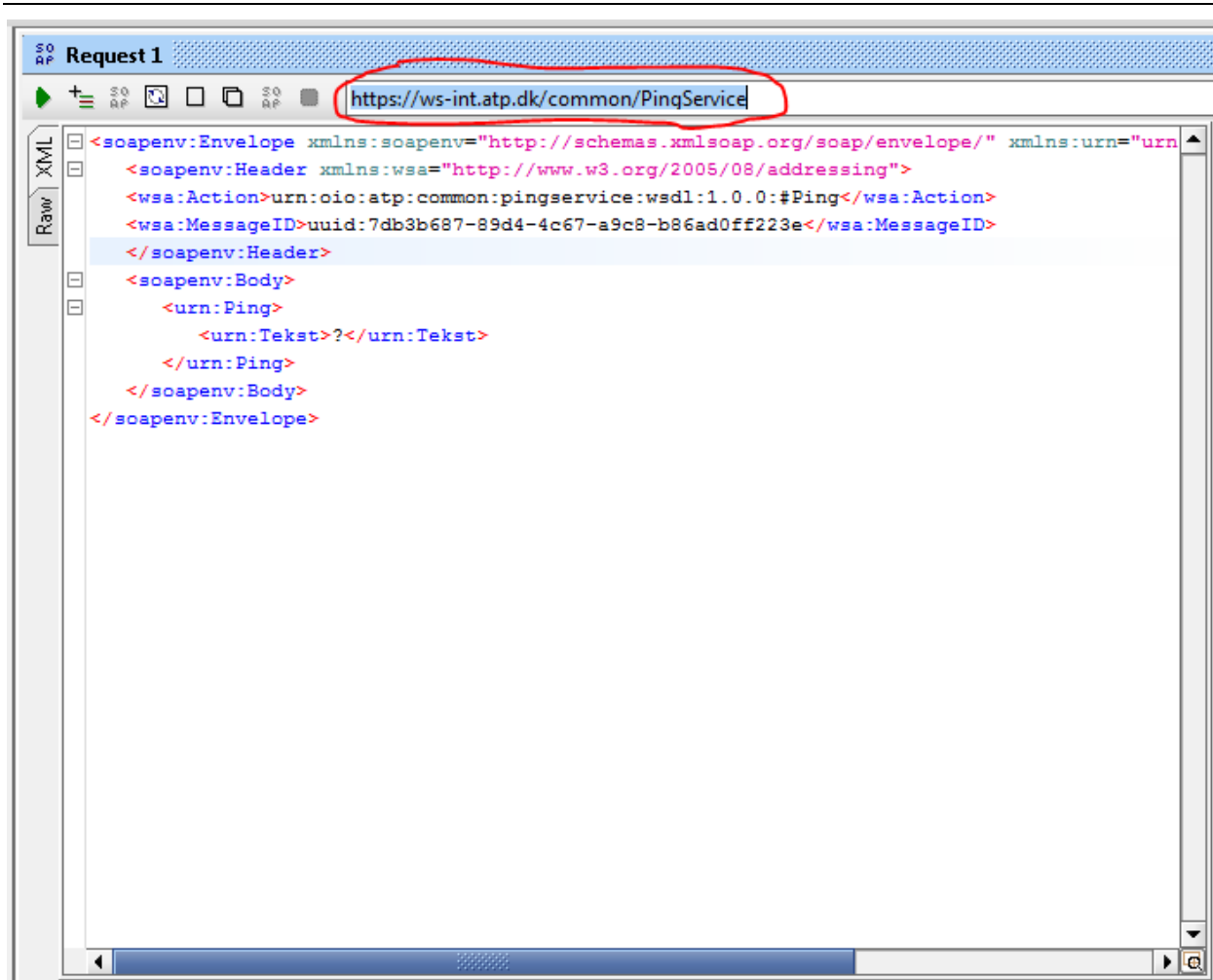
Fjern hak ved EnableWS-A addressing



6.2 Specificer Endpoint

Ændre endpoint så det peger på det miljø man ønsker at ramme, herunder er vist Atp's komponent-test.

Kald af PingService via SOAPUI



6.3 Anvend Incoming WSS configuration

I Request vinduet, forinden vælg "Auth" (se billede nedenfor).

Vælg "Add new Authorization..."

Vælg typen "Basic"

Tryk OK.

Kald af PingService via SOAPUI

The screenshot displays the SOAPUI interface for a request to `https://ws-int.atp.dk/common/PingService`. The XML view shows a SOAP envelope with a header and a body containing a ping request. A dialog box titled "Add Authorization" is open, showing a dropdown menu for "Type" set to "Basic". The "Add New Authorization..." button in the main interface is also highlighted. The "Auth" tab is selected in the bottom navigation bar.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="urn:PingService" xmlns:wsa="http://www.w3.org/2005/08/addressing">
  <soapenv:Header>
    <wsa:Action>urn:PingService:Ping
  </wsa:Action>
  </soapenv:Header>
  <soapenv:Body>
    <urn:Ping>
      <urn:Tekst>?</urn:Tekst>
    </urn:Ping>
  </soapenv:Body>
</soapenv:Envelope>
```

For Incoming WSS vælg nu i dropdown menuen den Incoming WSS konfiguration der blev oprettet under 5.4.

Kald af PingService via SOAPUI

The screenshot displays the SOAPUI interface. At the top, the address bar shows the URL `https://ws-int.atp.dk/common/PingService`. The main window displays the raw XML of a SOAP request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:urn="http://www.w3.org/2005/08/addressing">  
  <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"><wsa:Action>u</wsa:Action></soapenv:Header>  
  <soapenv:Body>  
    <urn:Ping>  
      <urn:Tekst>?</urn:Tekst>  
    </urn:Ping>  
  </soapenv:Body>  
</soapenv:Envelope>
```

Below the XML view, the configuration panel is visible. The 'Authorization' dropdown is set to 'Basic'. The 'Incoming WSS' dropdown is highlighted with a red circle and contains the text 'incoming atp ws'. Other fields include Username, Password, Domain, Pre-emptive auth (with 'Use global preference' selected), and Outgoing WSS.

At the bottom of the configuration panel, there are tabs for 'Auth (Basic)', 'Headers (0)', 'Attachments (0)', 'WS-A', 'WS-RM', 'JMS Headers', and 'JMS Property (0)'.

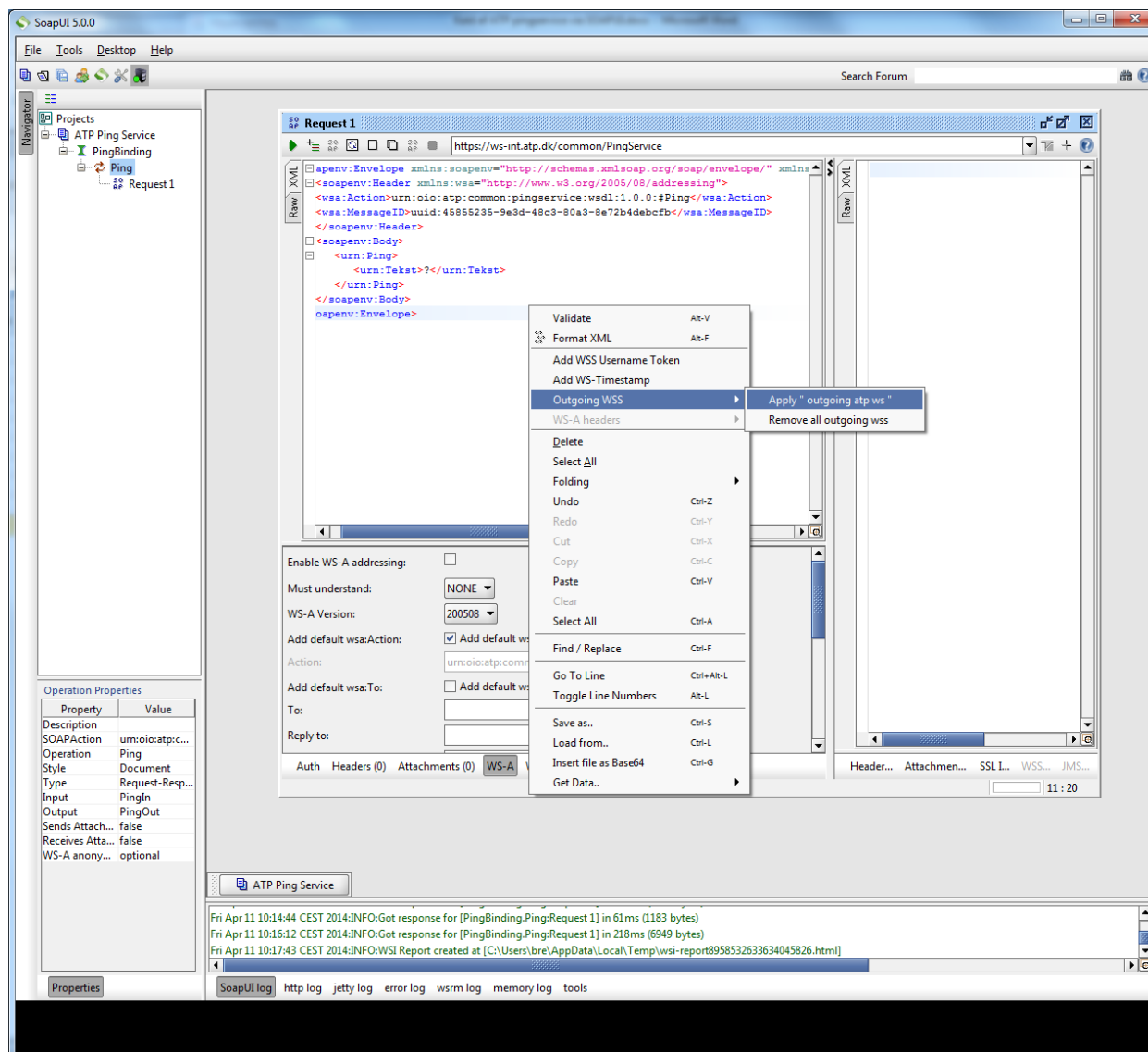
6.4 Anvend Outgoing WSS Configuration

Højre klik i Request1 vinduet.

Kald af PingService via SOAPUI

Vælg "Outgoing WSS" i dropdown menuen, og vælg herunder Apply "outgoing atp ws" (navnet kan variere alt efter hvordan man har navngivet i 5.3).

På denne måde tilføjes Timestamp og de fire dele (Body, Action, MessageID og Timestamp signeres)



Kald af PingService via SOAPUI

7. Send Request

Requesten kan nu afsendes. Klik på grøn pil, markeret med rød cirkel.

Hver opmærksom på at Timestamp forældes efter 5 min.

Hvis alt er sat rigtigt op skal man få svaret "Pingeling, I'm alive", markeret med rød ring.

The screenshot shows the SoapUI 5.0.0 interface. On the left, the 'Request 1' is selected in the Navigator. The main area displays the raw XML of the request and response. The request is a SOAP envelope with a Ping action. The response is a PingResponse with a text element containing 'Pingeling, I m alive'. The 'Request Properties' panel on the left shows details for the request, including the endpoint 'https://ws-int.atp.dk/common/PingService' and the message size '6034'. The bottom status bar shows the response time as 552ms (6949 bytes).

```

<?xml version='1.0' encoding='UTF-8'>
<soap:Envelope xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/'>
  <soap:Header xmlns:wsa='http://www.w3.org/2005/08/addressing'>
    <wsa:Action wsa:Id='id-1478885D8FFD26ABE139720605106988' xmlns:wsa='http://www.w3.org/2005/08/addressing'/>
    <wsa:MessageID wsa:Id='id-1478885D8FFD26ABE139720605106988' xmlns:wsa='http://www.w3.org/2005/08/addressing'/>
  </soap:Header>
  <soap:Body wsa:Id='id-1478885D8FFD26ABE139720605106988' xmlns:wsa='http://www.w3.org/2005/08/addressing'>
    <urn:Ping>
      <urn:Tekst?></urn:Tekst>
    </urn:Ping>
  </soap:Body>
</soap:Envelope>
  
```

```

<?xml version='1.0' encoding='UTF-8'>
<ns1:PingResponse xmlns:ns1='urn:oasis:names:tc:ebxml-core:xsd:ping:2014-04-11'>
  <ns1:Tekst>Pingeling, I m alive</ns1:Tekst>
  <ns1:Data>2014-04-11</ns1:Data>
  <ns1:Klokken>10:47:46.352670</ns1:Klokken>
</ns1:PingResponse>
  
```

Kald af PingService via SOAPUI

8. FejlScenarier

Flere ting kan gå galt under opsætningen.

Alt efter faultcode må man forsøge at finde frem til hvad der er gået galt.

Her et par eksempler:

FailedAuthentication:

Indikerer at det certifikat man kalder med ikke kan trustes af ATP. Det bør undersøges om man har sat keystore rigtigt op, og bruger den rigtige type certifikat.

FailedCheck:

CWWSS5720E: A required message part [http://www.w3.org/2005/08/addressing:MessageID] is not signed.

I dette tilfælde er MessageID ikke signeret, tjek at MessageID er med i listen over de parts der er defineret under Signature i Outgoing WS-Security Configuration, samt at der ikke findes slå fejl.

Prøv evt. at sætte signaturene på igen:

Højreklik på Request vinduet,

vælg først Outgoing WSS og så "Remove all outgoing wss",

vælg så Outgoing WSS og så "Apply outgoing atp ws"

DuplicateMessageID:

Der er kaldt med en tidligere anvendt MessageID.

Prøv med et nyt MessageID.

Højreklik på Request vinduet,

Vælg først Outgoing WSS og så "Remove all outgoing wss",

Ret MessageID i requesten

Vælg så Outgoing WSS og så "Apply outgoing atp ws"