Kald af PingService via SOAPUI

Author: Integration Expert Team (IET)
Owner: Integration Expert Team (IET)

1. Dokumenthistorik

Revisioner

Dato for denne version: 09.04.2014	Dato for næste version *ukendt*

Version	Dato	Ændringer	Ændringer markeret
0.1	09.04.2014	Første version	N

Indholdsfortegnelse

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.

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.

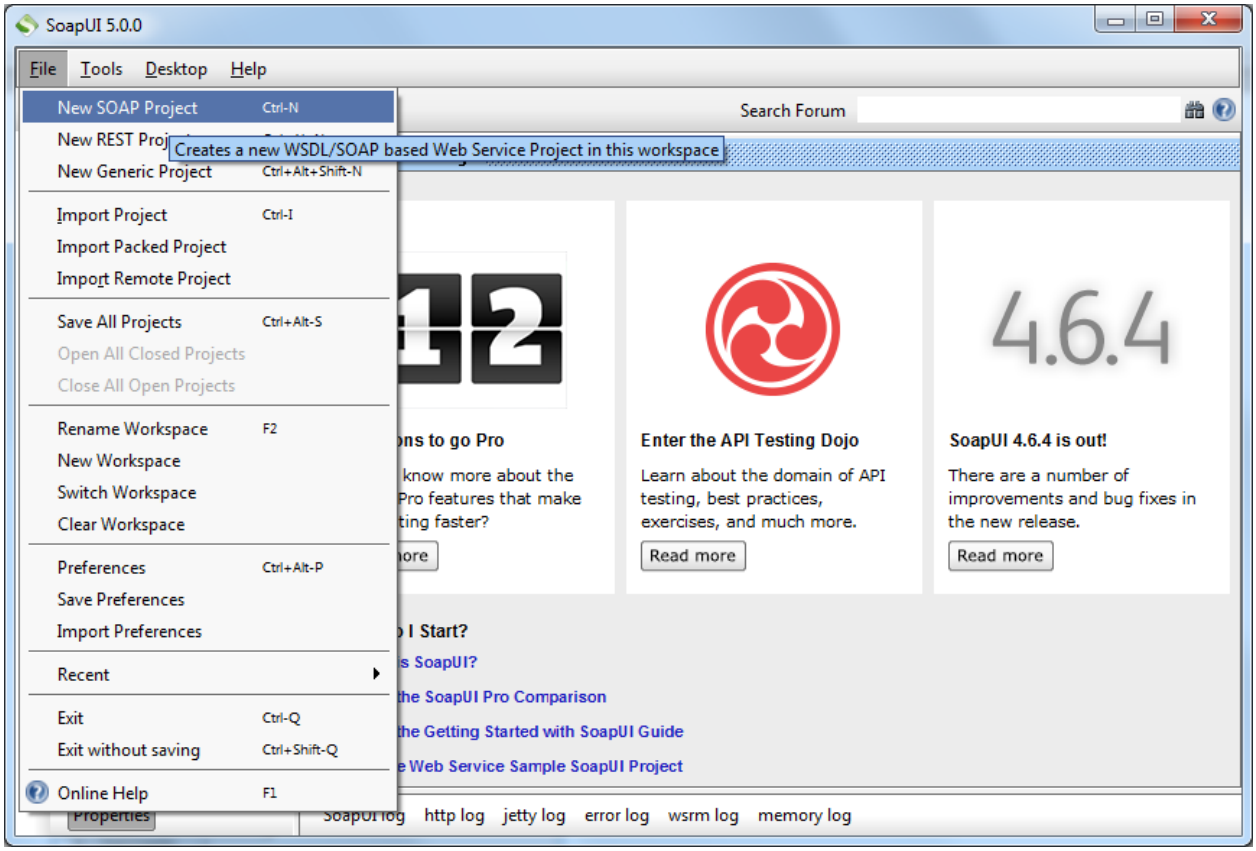
Desuden skal anvenderen have et virksomheds test certifikat (TDC OCES Systemtest CA II eller TRUST2408 Systemtest VIII CA) udstedt af DanID.

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.

4. Opret projekt

Begynd med at oprette et nyt projekt:

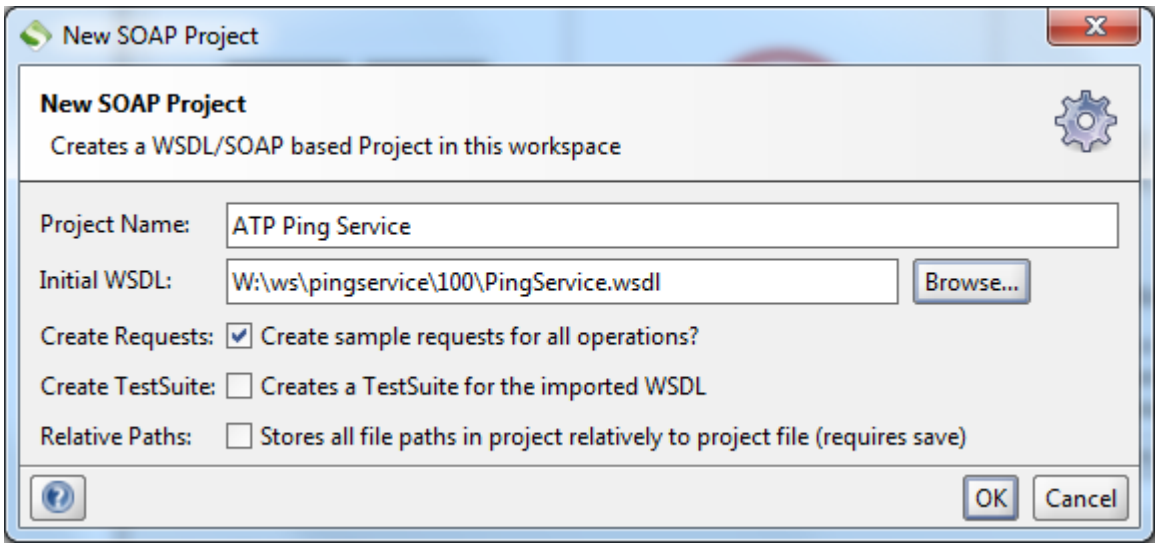


Project Name: Navngiv projektet.

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

Create Requests: sæt hak.

Tryk OK.



5. WS-Security Configurations

Dobbeltklik på projektet.

Vælg fanebladet WS-Security Configurations.

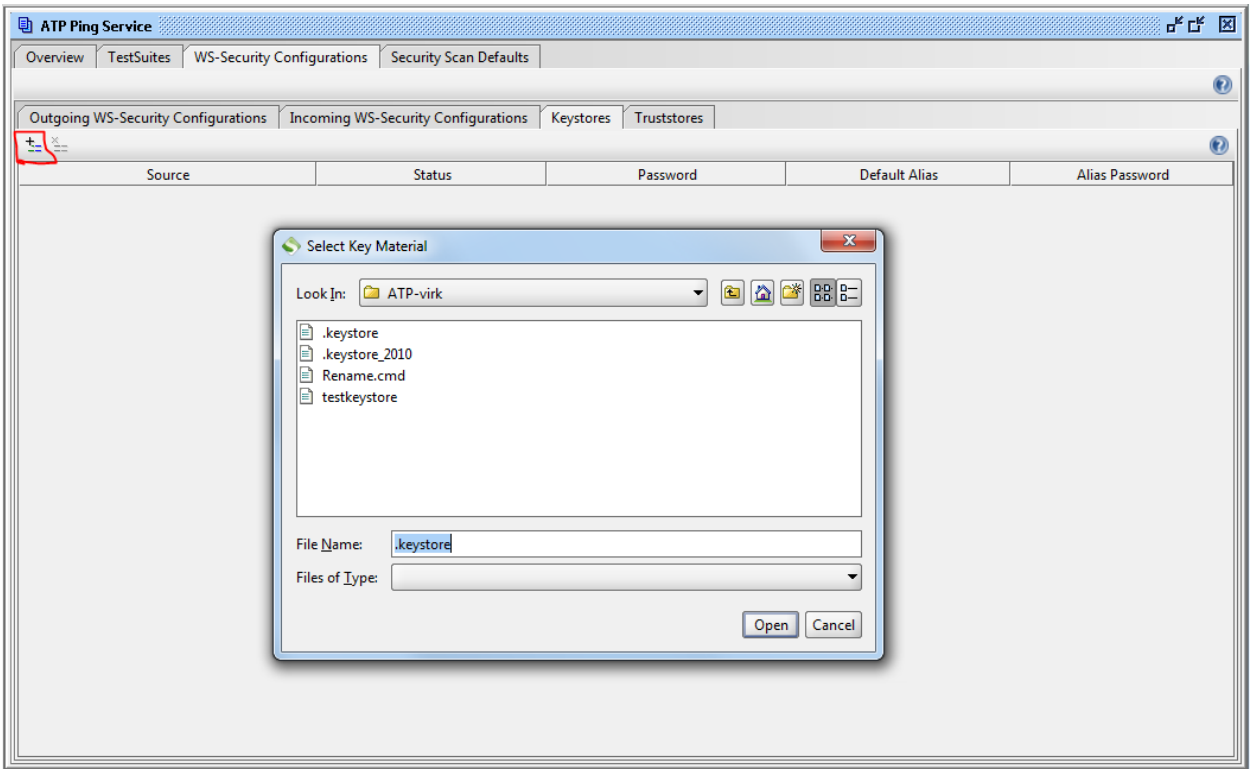
5.1 Opret Keystore

Vælg fanebladet Keystores

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

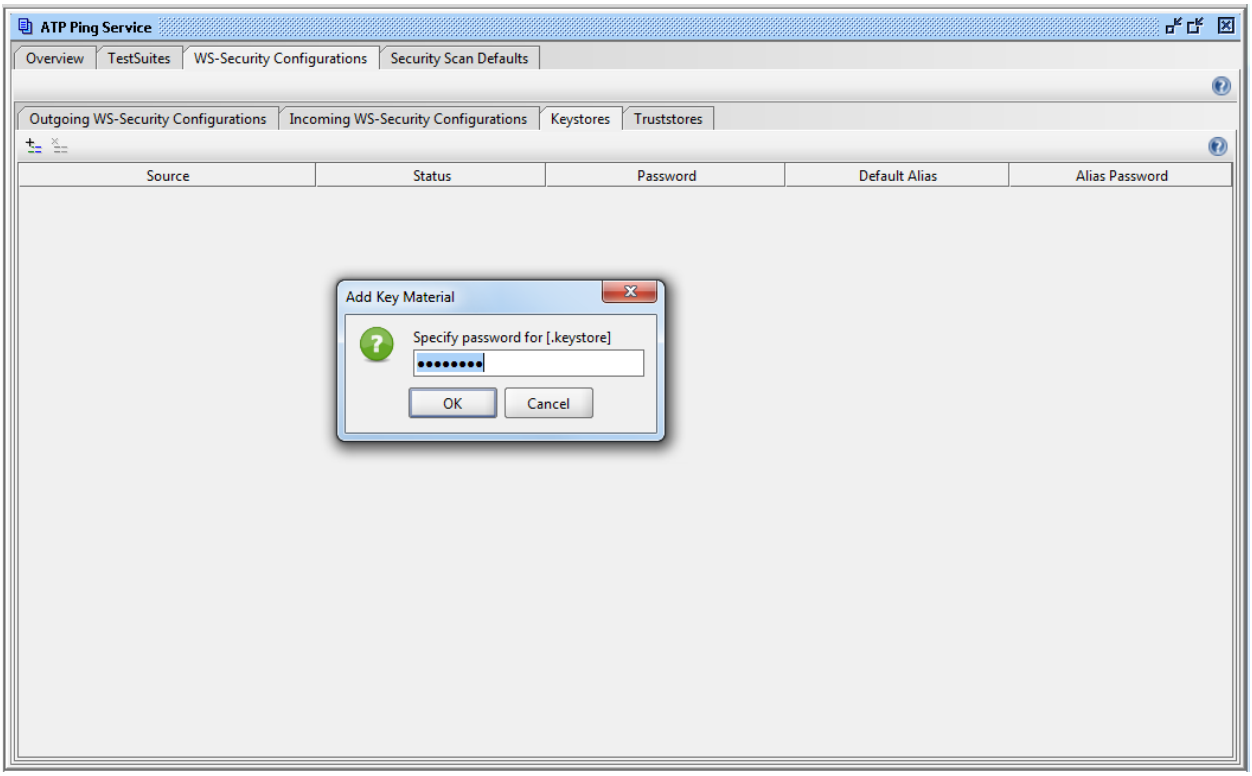
Angiv den keystore der indeholder virksomhedens test certifikat (TDC OCES Systemtest CA II eller TRUST2408 Systemtest VIII CA) udstedt af DanID

Tryk Open.



Indtast password for keystore.

Tryk OK.



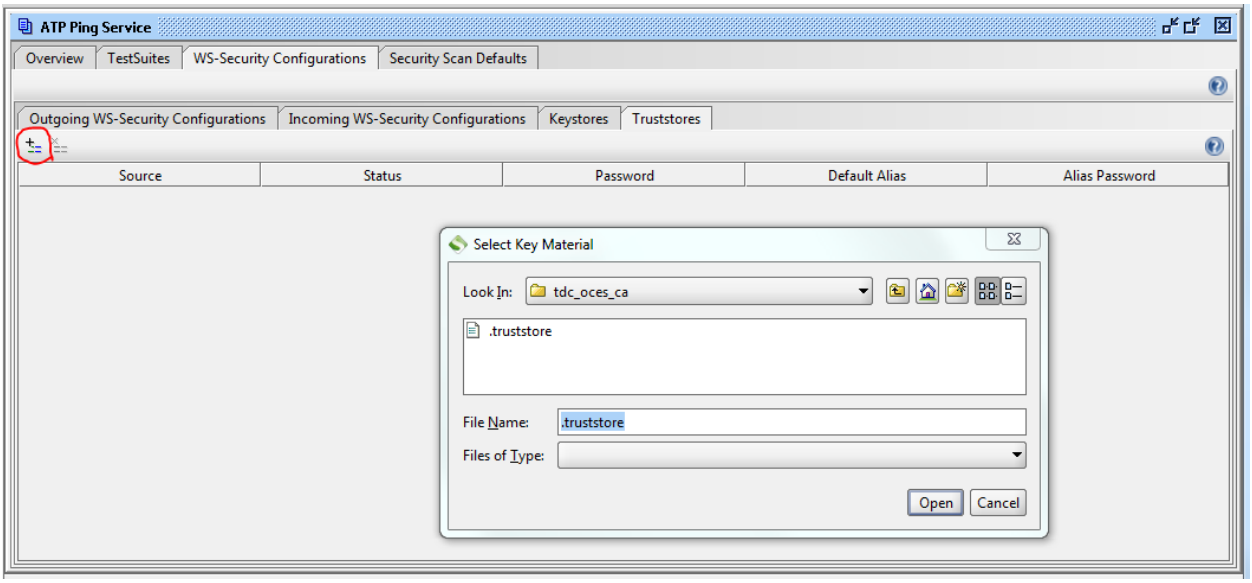
5.2 Opret Truststore

Vælg fanebladet Truststores.

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

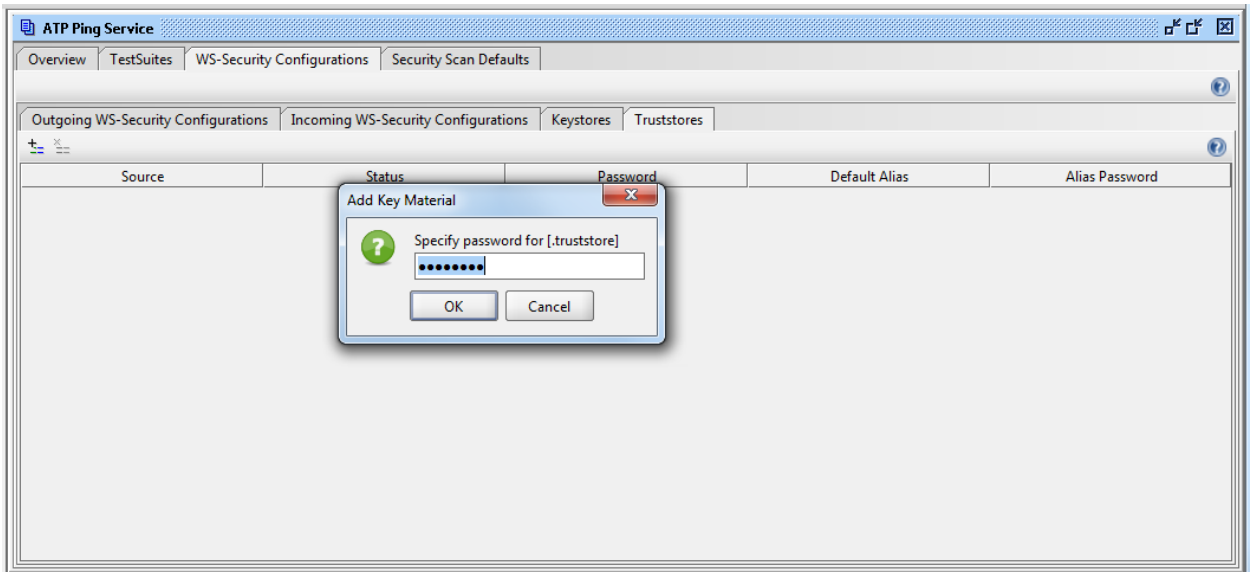
Angiv den truststore som indeholder ATP's public key, eller alternativt rodcertifikatet, alt efter hvad man ønsker at autentificerer svar beskederne ud fra. (Begge dele kan fås fra ATP)

Tryk Open.



Indtast password for truststore.

Tryk OK.



5.3 Opret Outgoing WSS Configuration

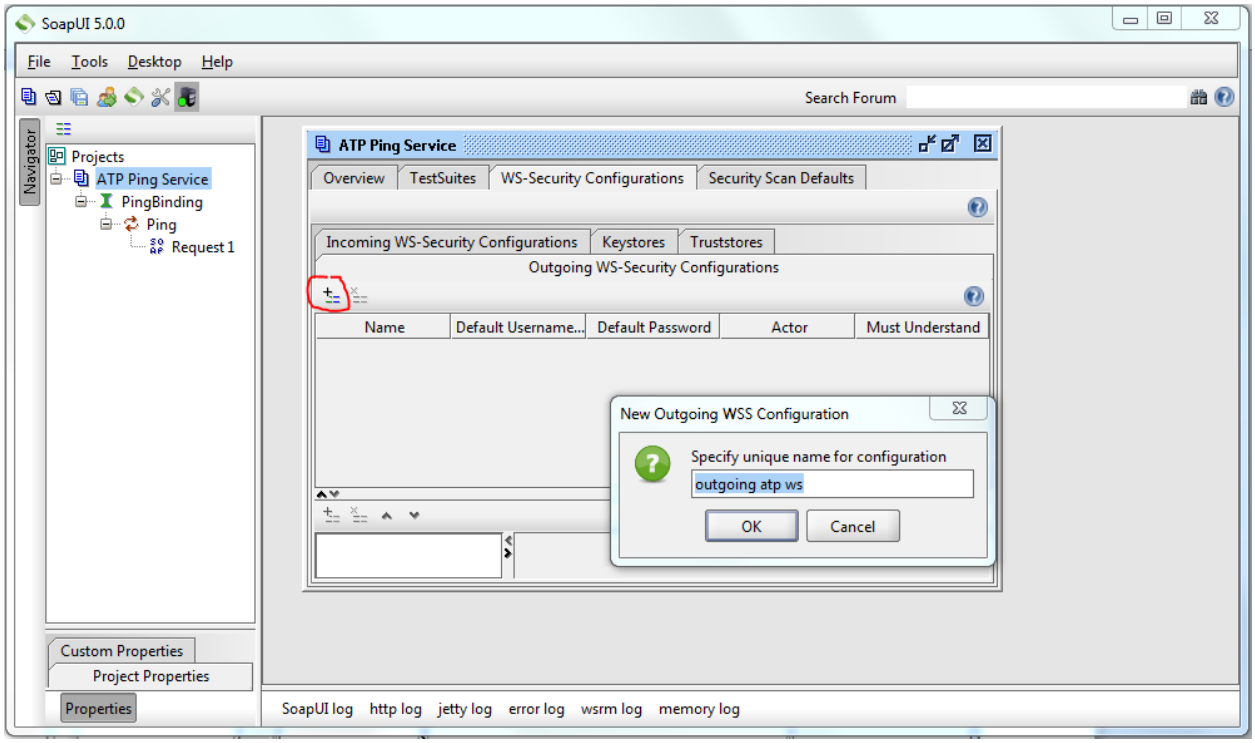
Vælg fanebladet Outgoing WSS Configurations.

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.

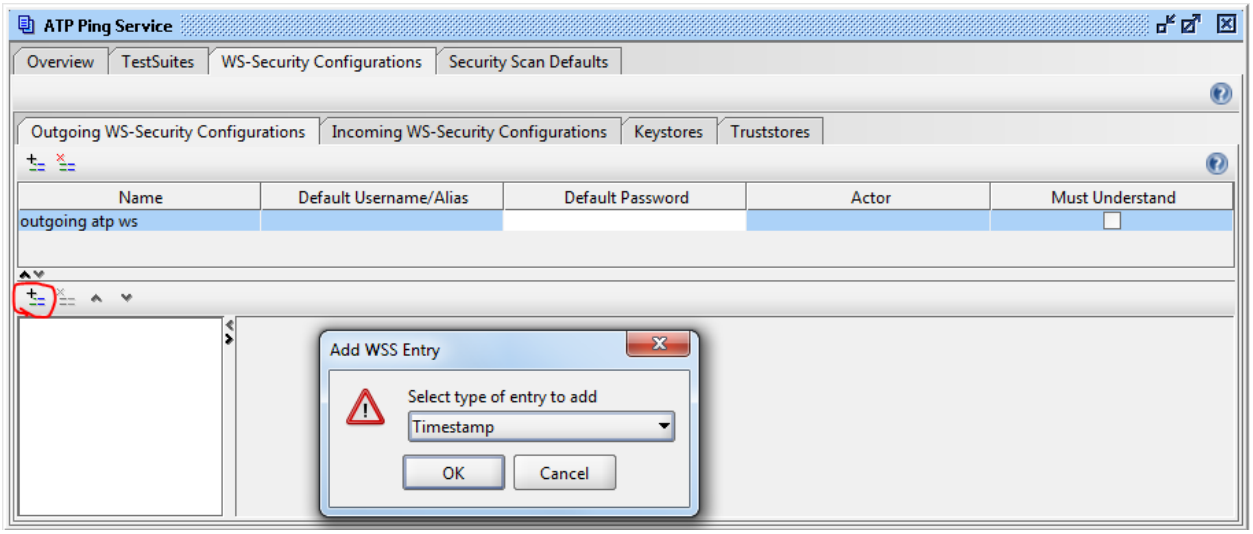
Kald af PingService via SOAPUI



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

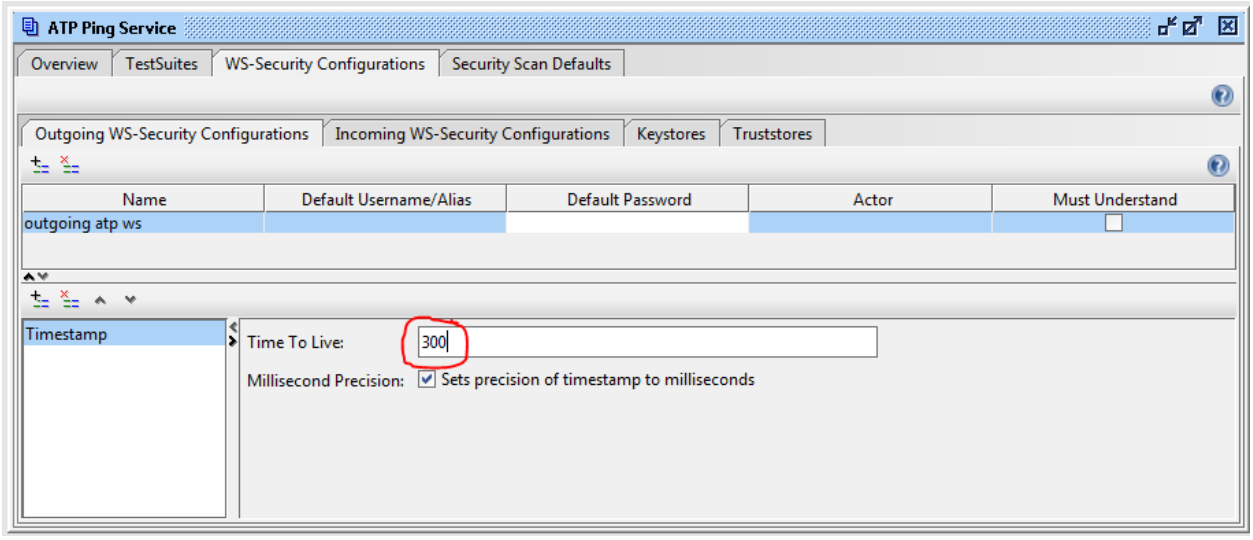
Vælg typen Timestamp.

Tryk OK.



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

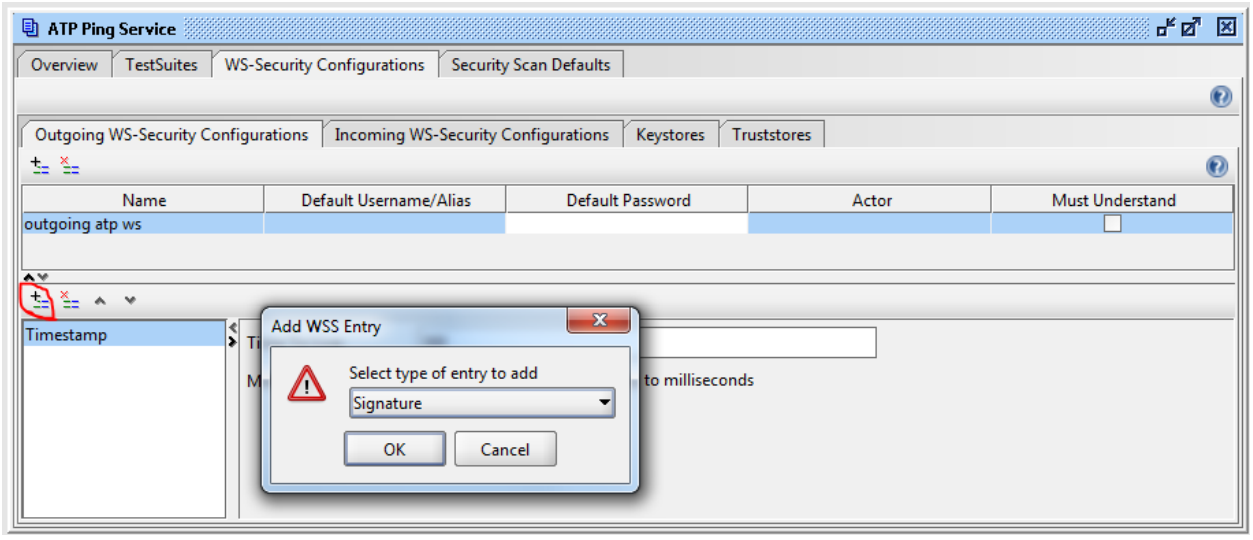
Kald af PingService via SOAPUI



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

Vælg typen Signature.

Tryk OK.



Vælg keystore.

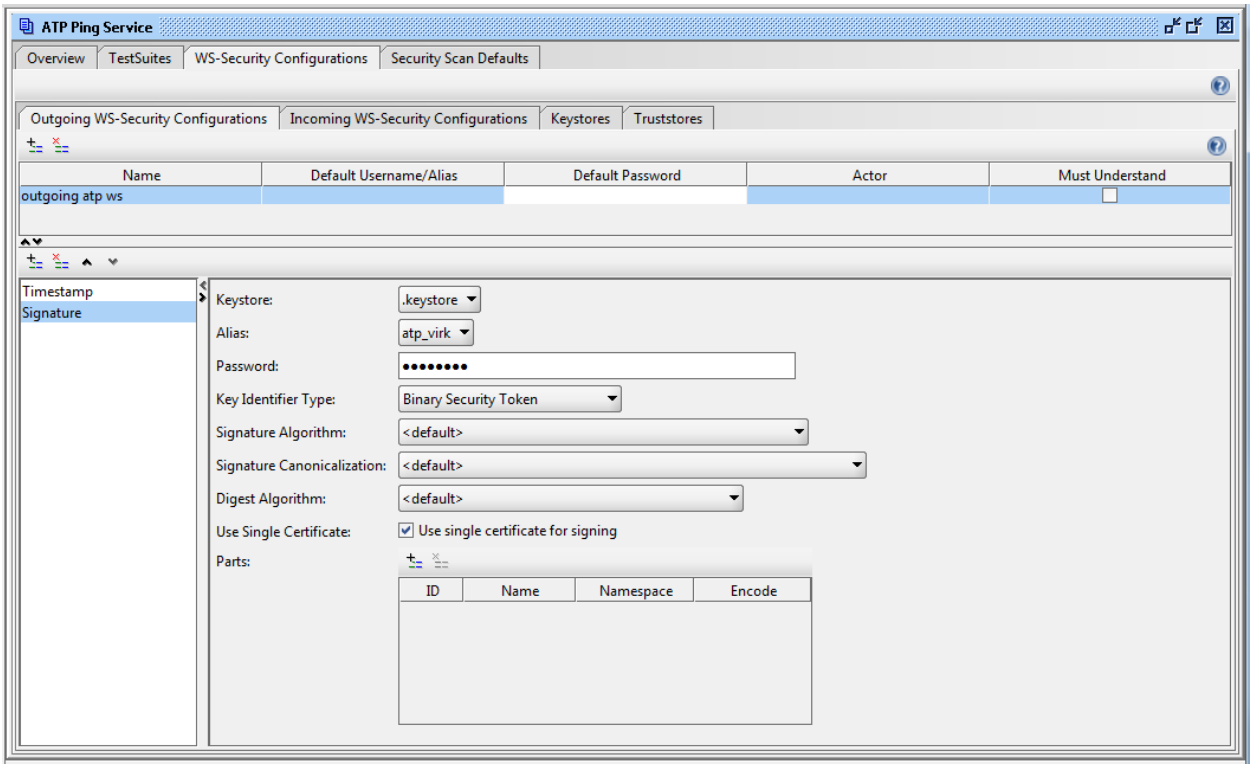
Vælg Alias.

Indtast Password (til keystore).

Key Identifier Type: sættes til ”Binary Security Token”

Use Single Certificate: sæt hak.

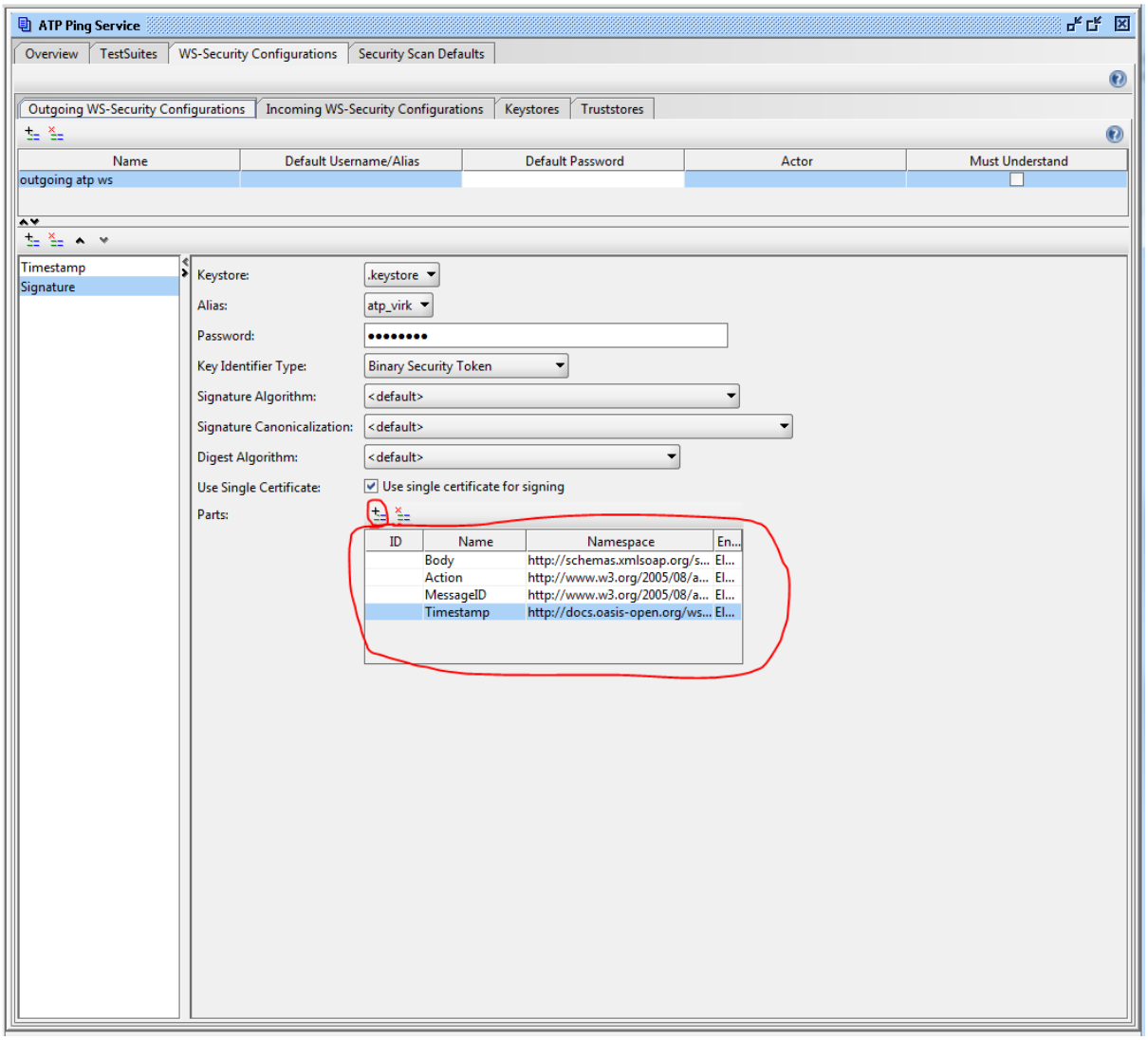
Kald af PingService via SOAPUI



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

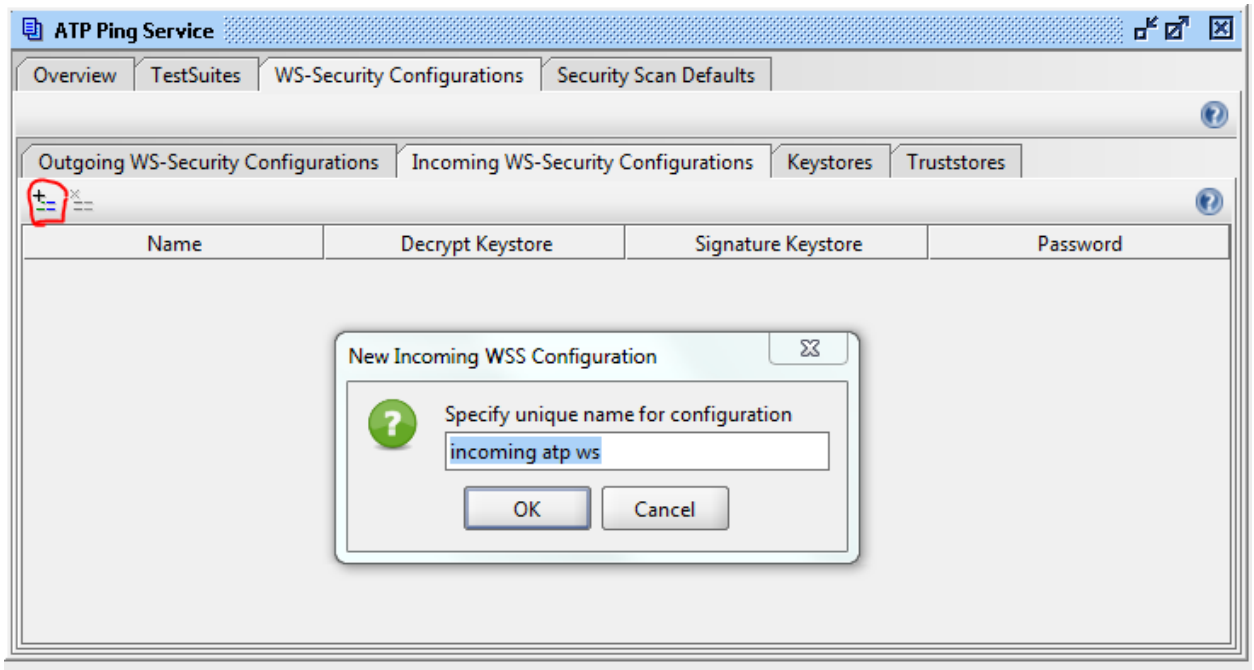
5.4 Opret Incoming WSS Configuration

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.

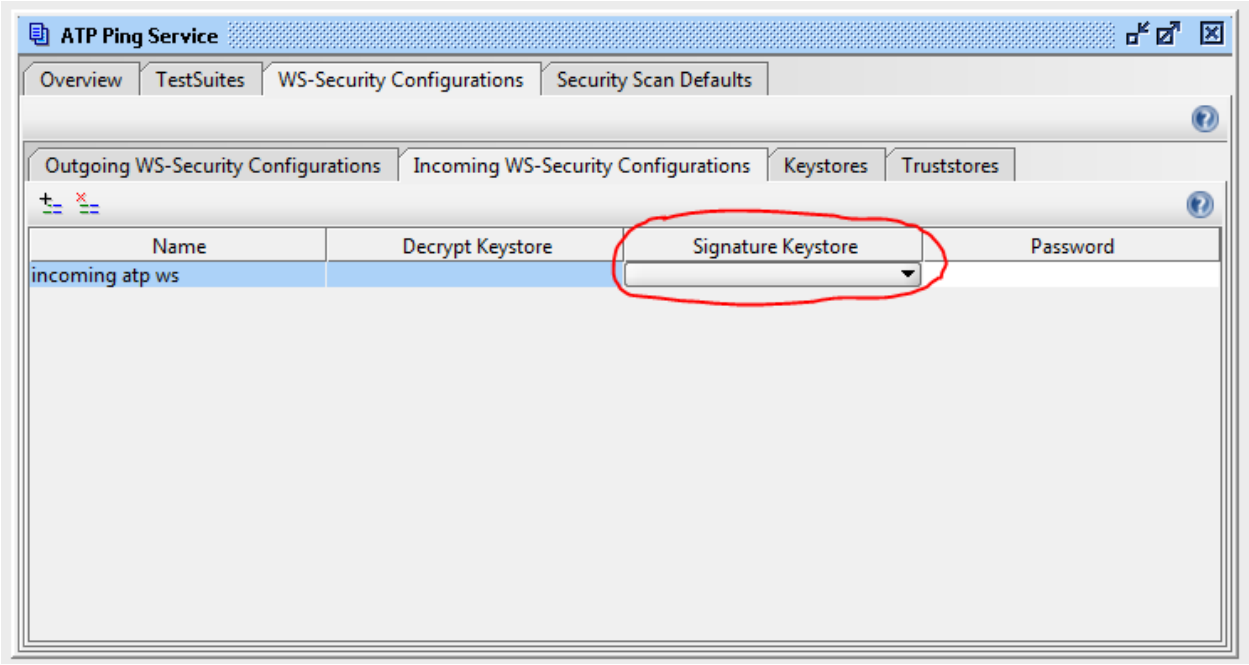


Angiv ”Signature Keystore” for konfigurationen.

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



6. Opsætning af Request

6.1 Tilføj wsa headers

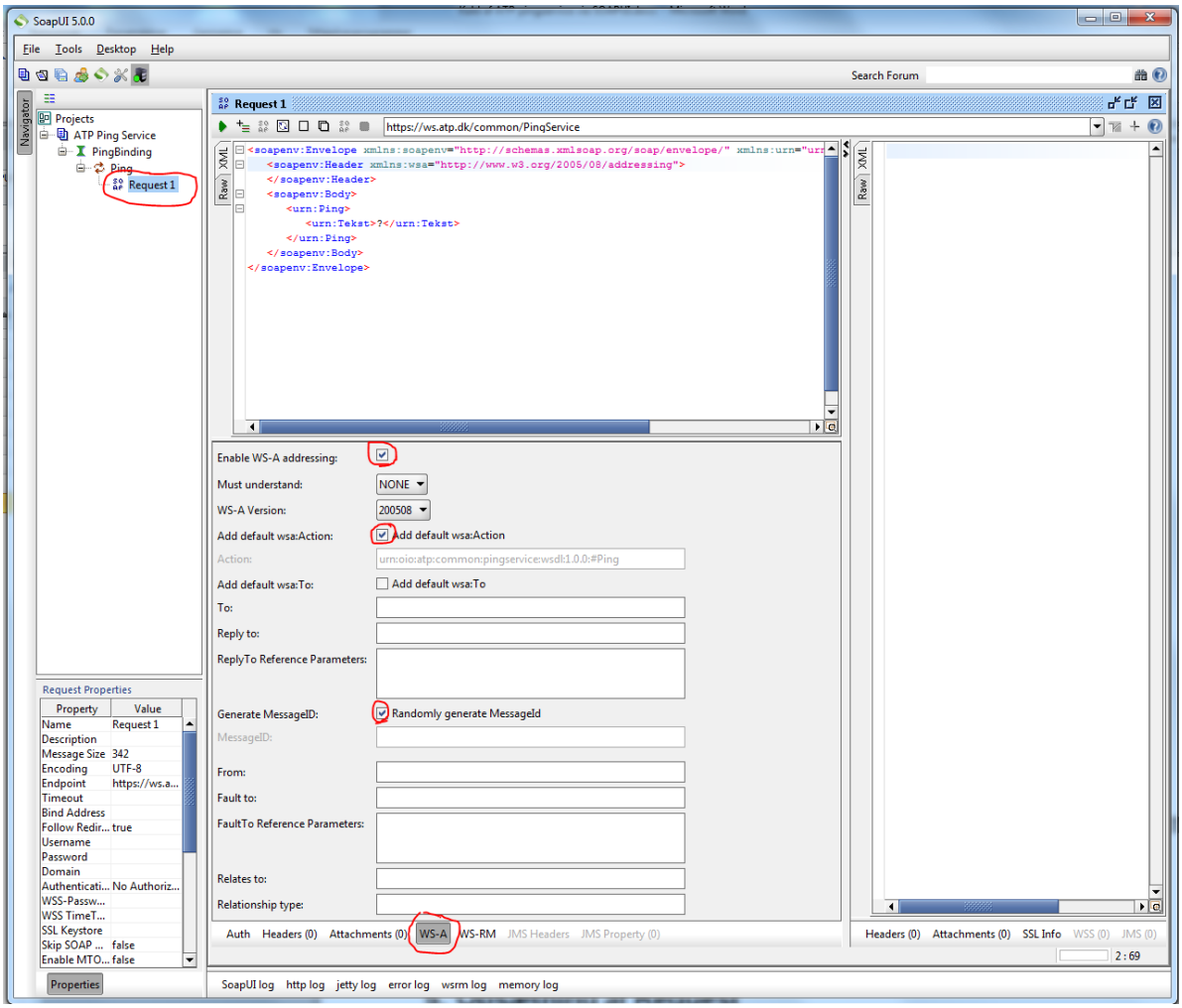
Dobbelt klik på Request 1 for at få request vinduet frem.

Forneden vælg WS-A (se billede nedenfor).

Sæt hak ved EnableWS-A addressing

Sæt hak ved Add default wsaAction

Sæt hak ved GenerateMessageID

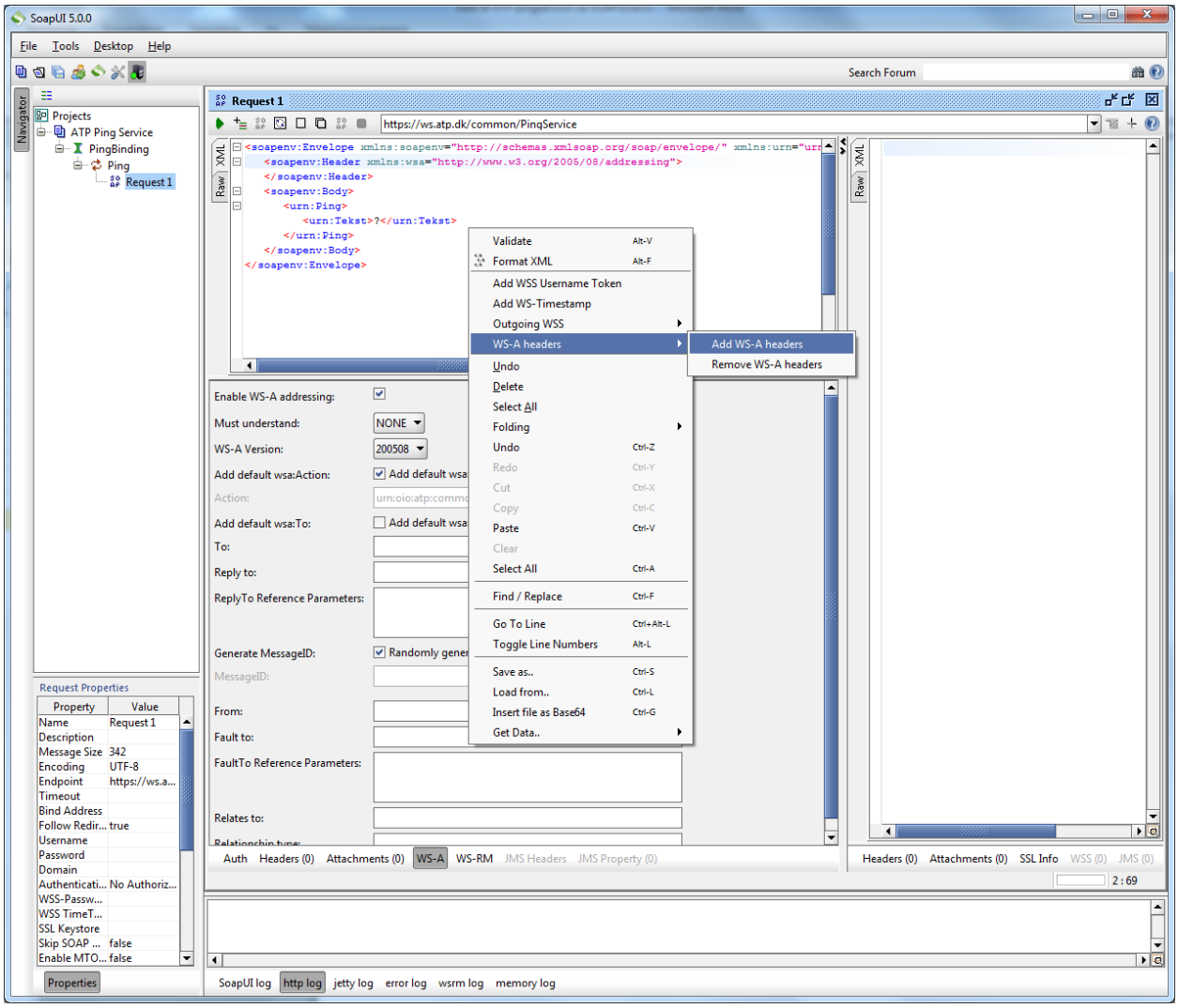


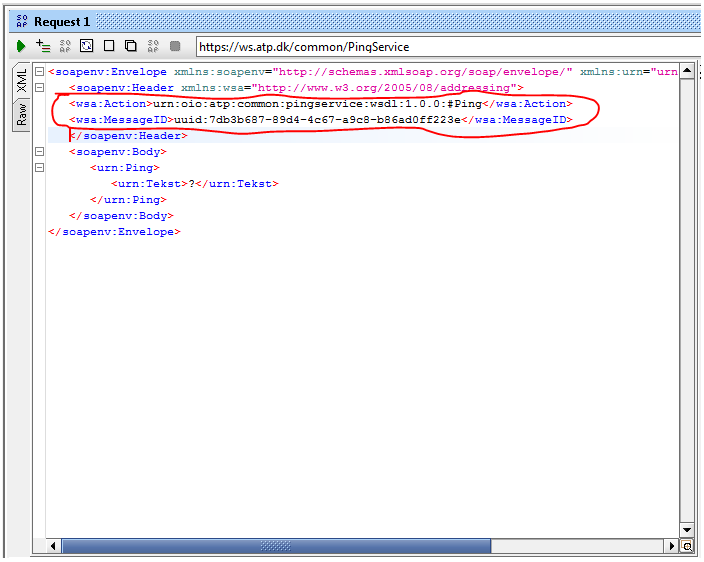
Højreklik i requesten.

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

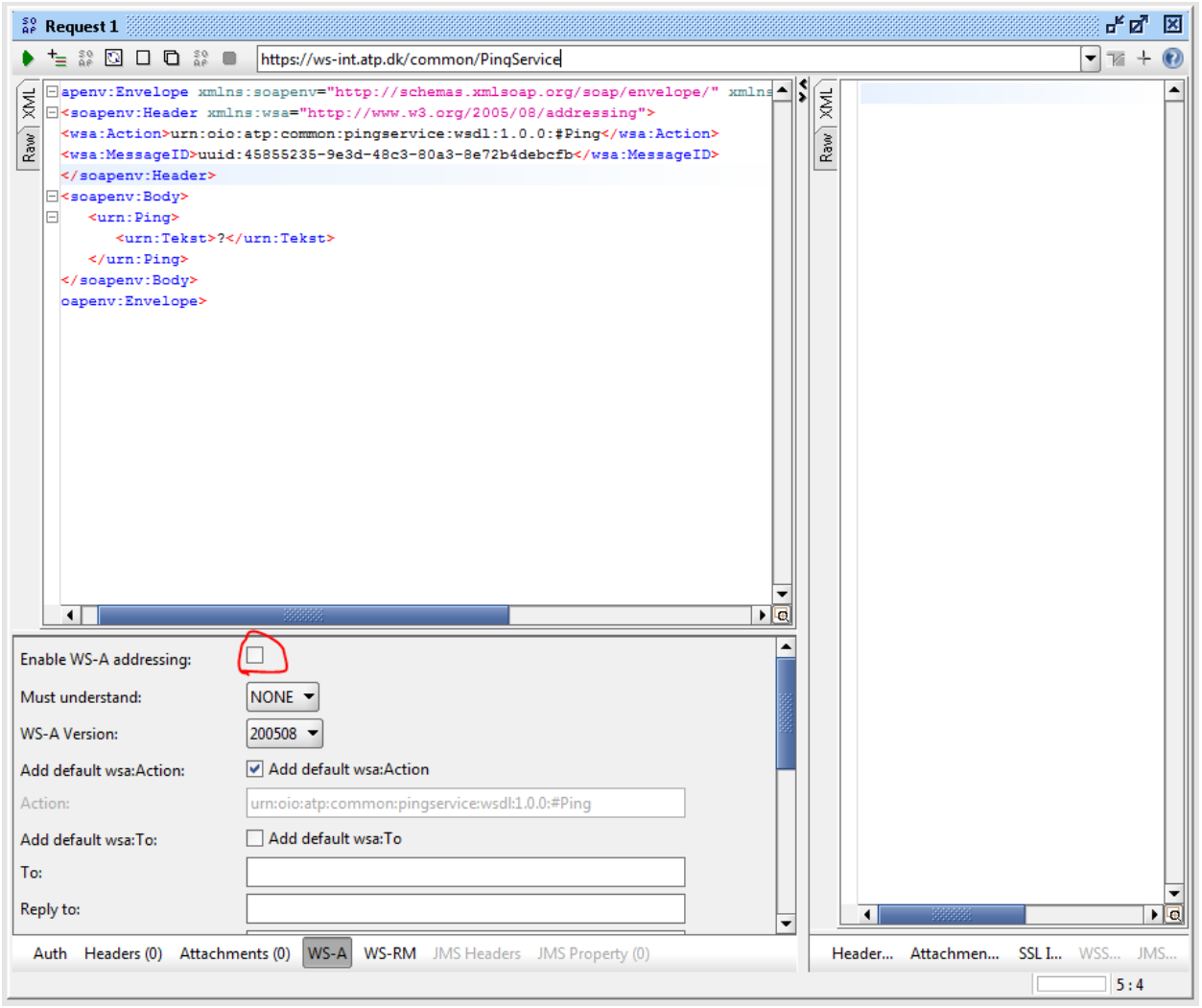




Forneden vælg WS-A (se billede nedenfor).

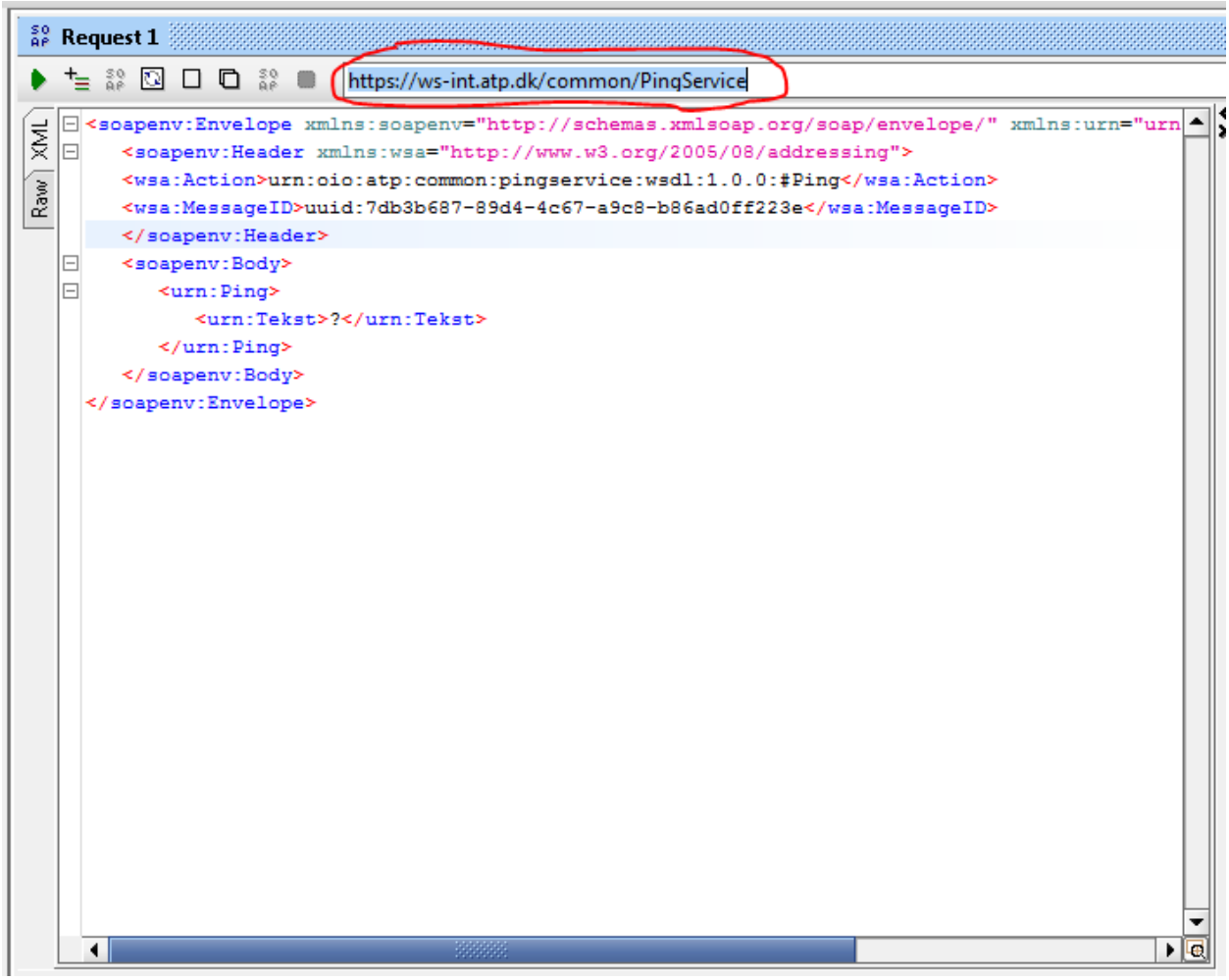
Kald af PingService via SOAPUI

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.



6.3 Anvend Incoming WSS configuration

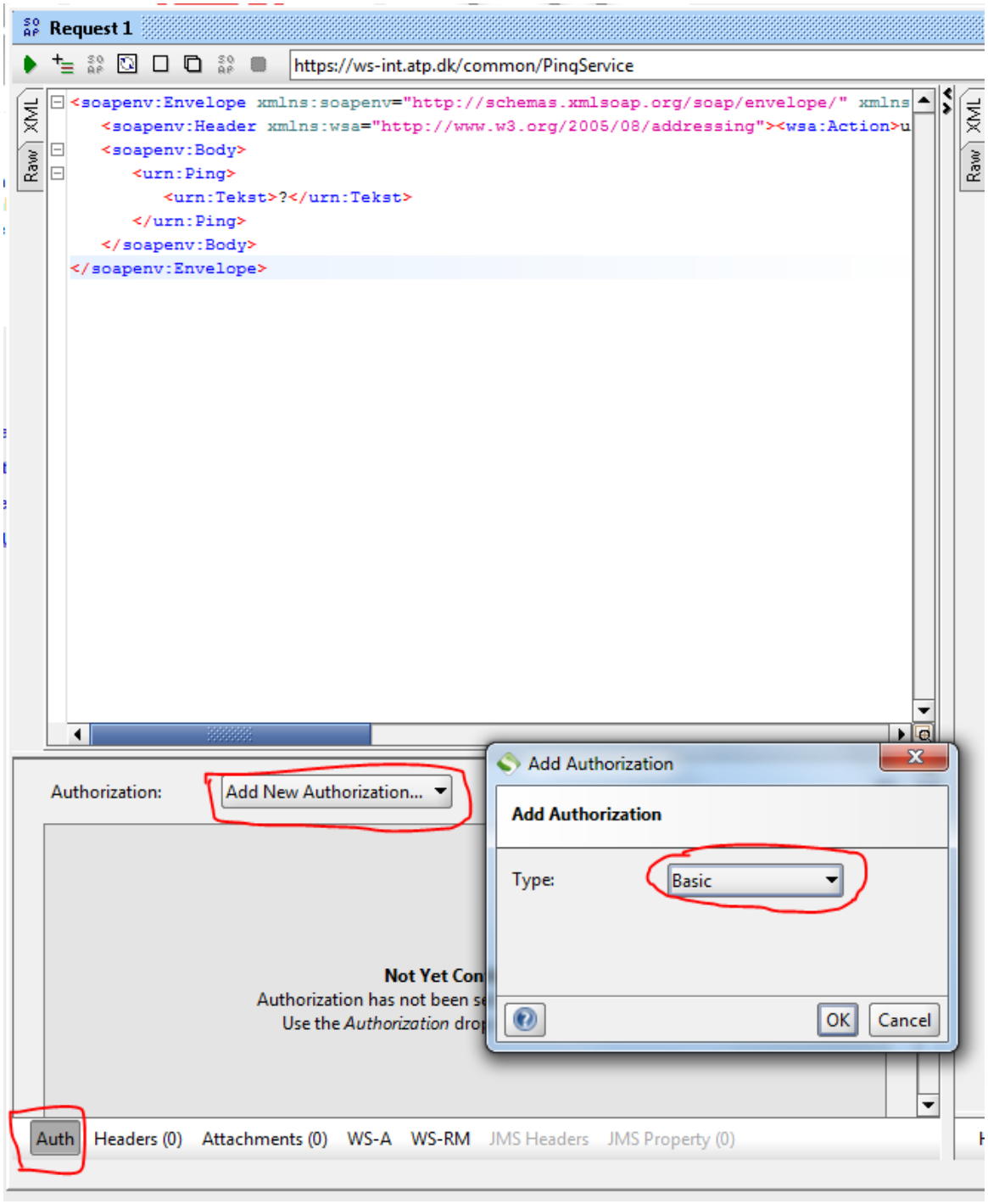
I Request vinduet, forneden vælg ”Auth” (se billede nedenfor).

Vælg ”Add new Authorization…”

Vælg typen “Basic”

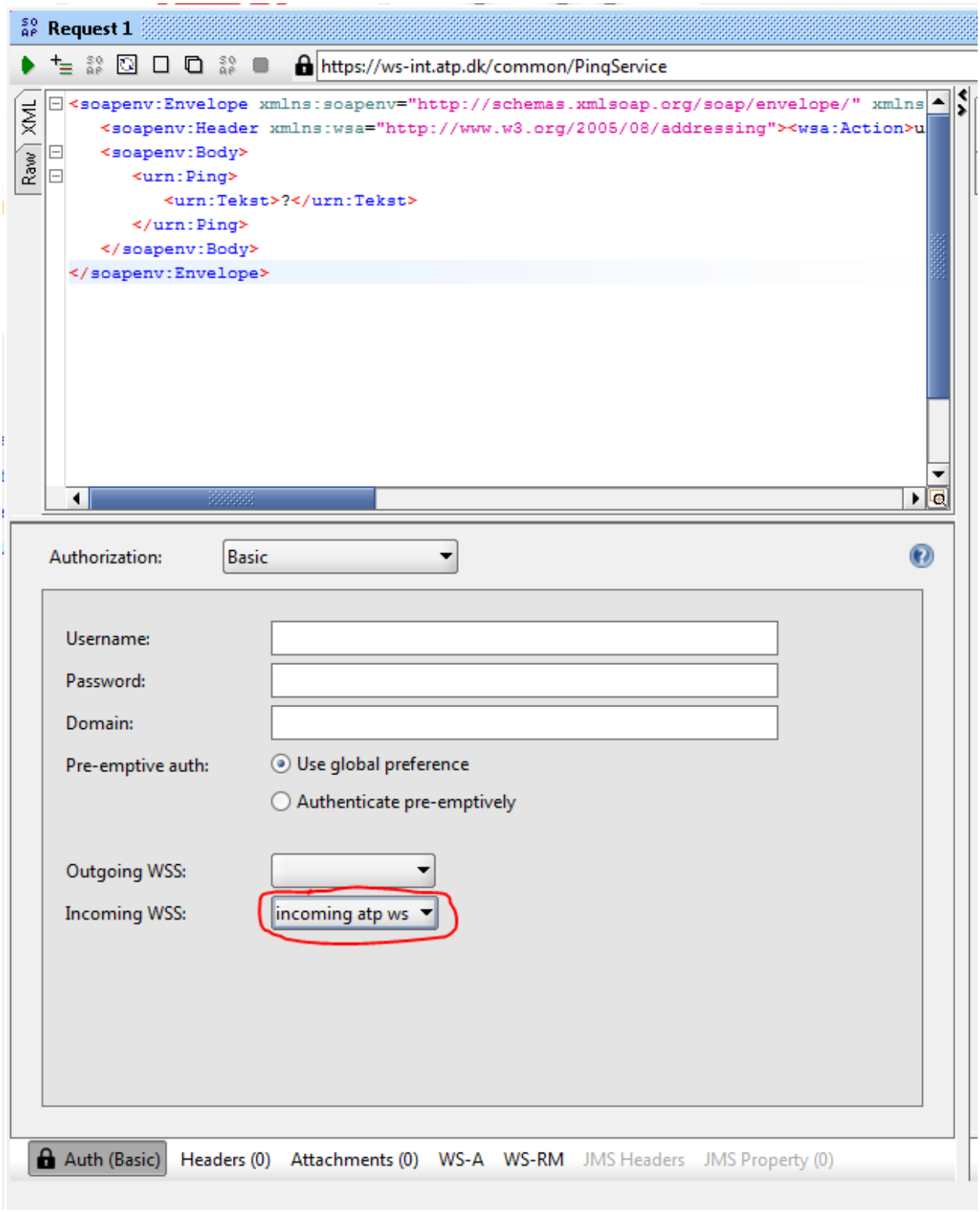
Tryk OK.

Kald af PingService via SOAPUI



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

Kald af PingService via SOAPUI



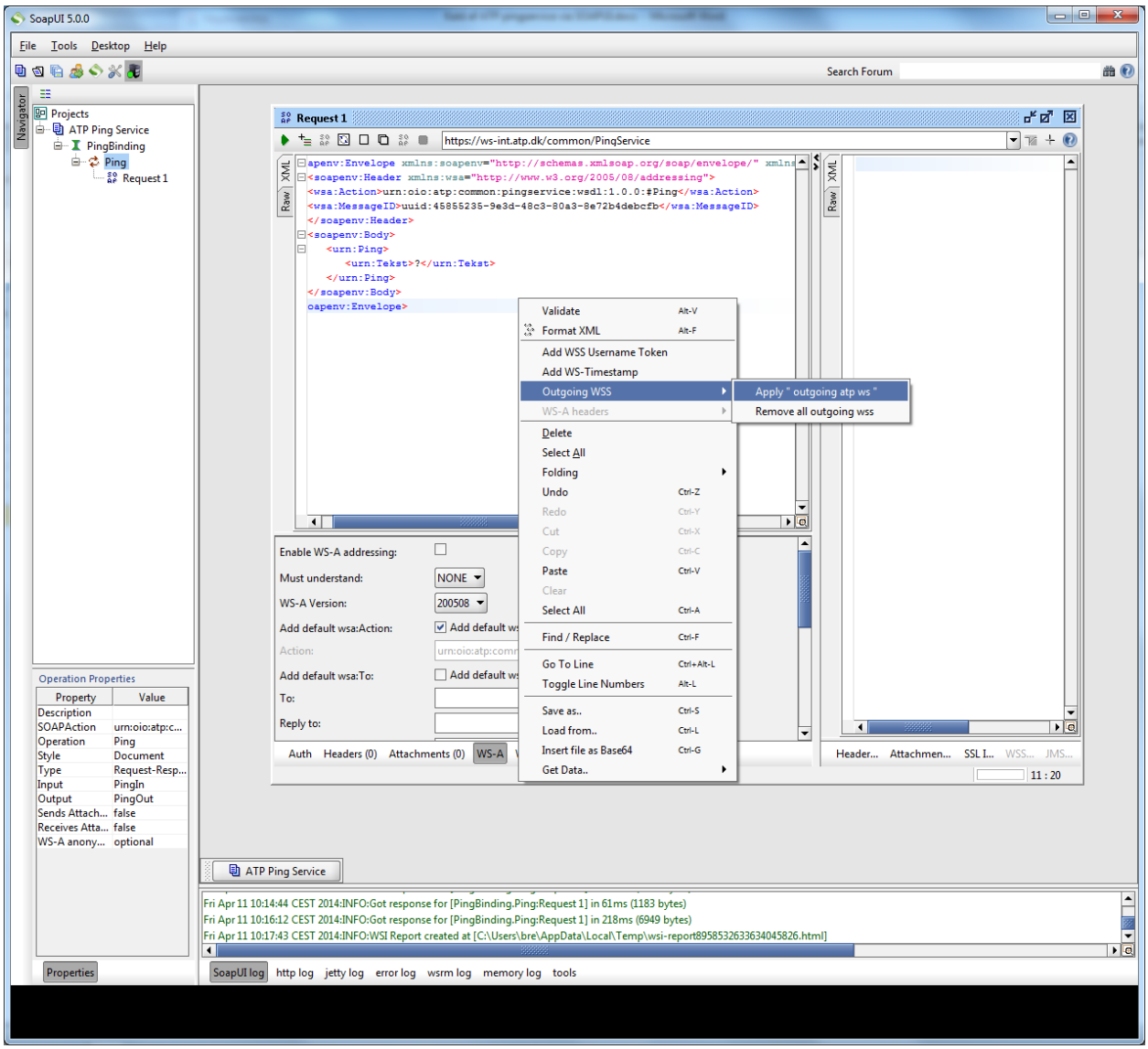
6.4 Anvend Outgoing WSS Configuration

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)

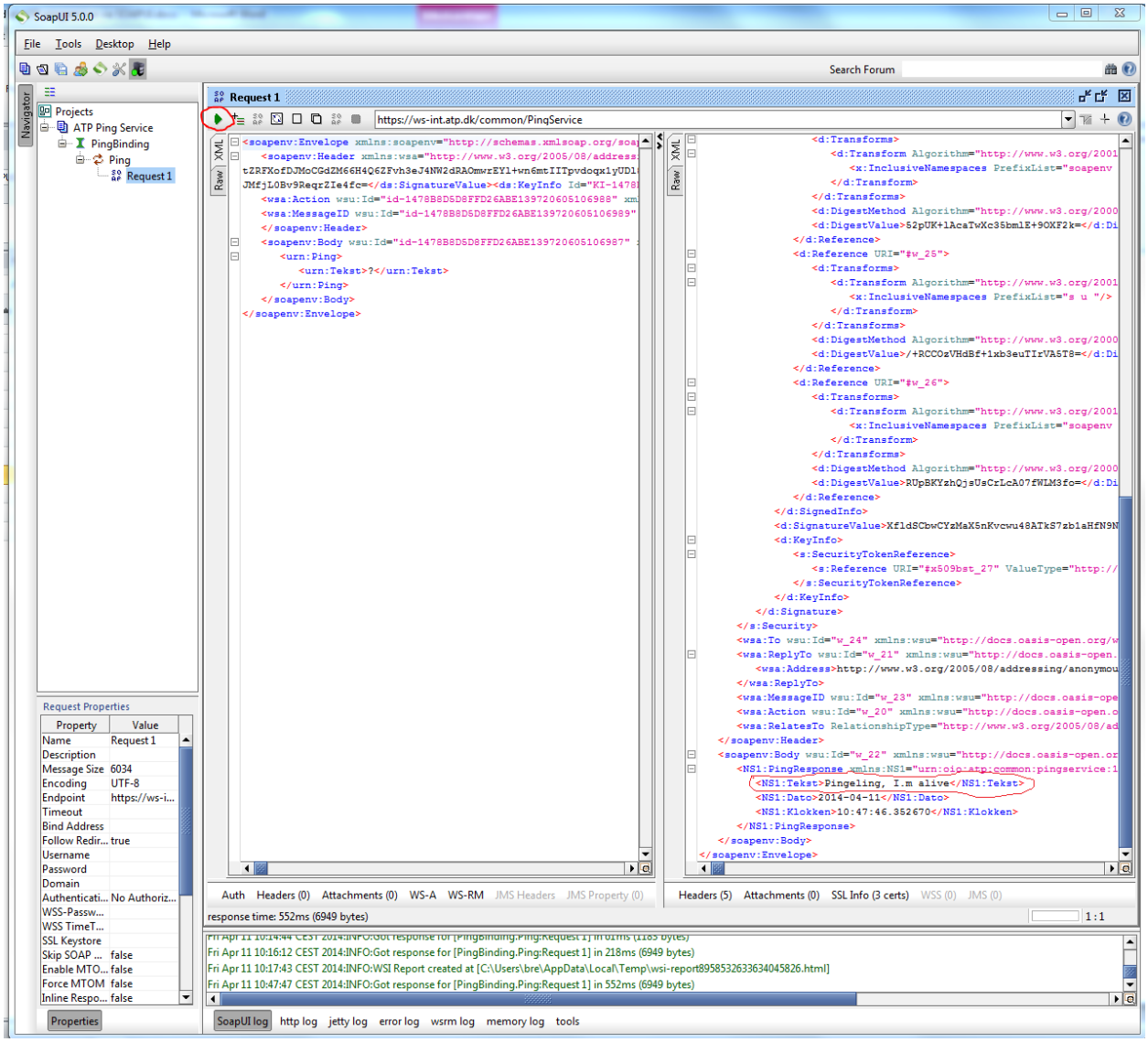


7. Send Request

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.



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”