

Using a Clusterable Cache with WS-Security Asymmetric Binding Policy

SOA | software™



Copyright

Copyright © 2014 SOA Software, Inc. All rights reserved.

Trademarks

SOA Software, Policy Manager, Portfolio Manager, Repository Manager, Service Manager, Community Manager, SOA Intermediary for Microsoft and SOLA are trademarks of SOA Software, Inc. All other product and company names herein may be trademarks and/or registered trademarks of their registered owners.

SOA Software, Inc.

SOA Software, Inc.
12100 Wilshire Blvd, Suite 1800
Los Angeles, CA 90025
(866) SOA-9876
www.soa.com
info@soa.com

Disclaimer

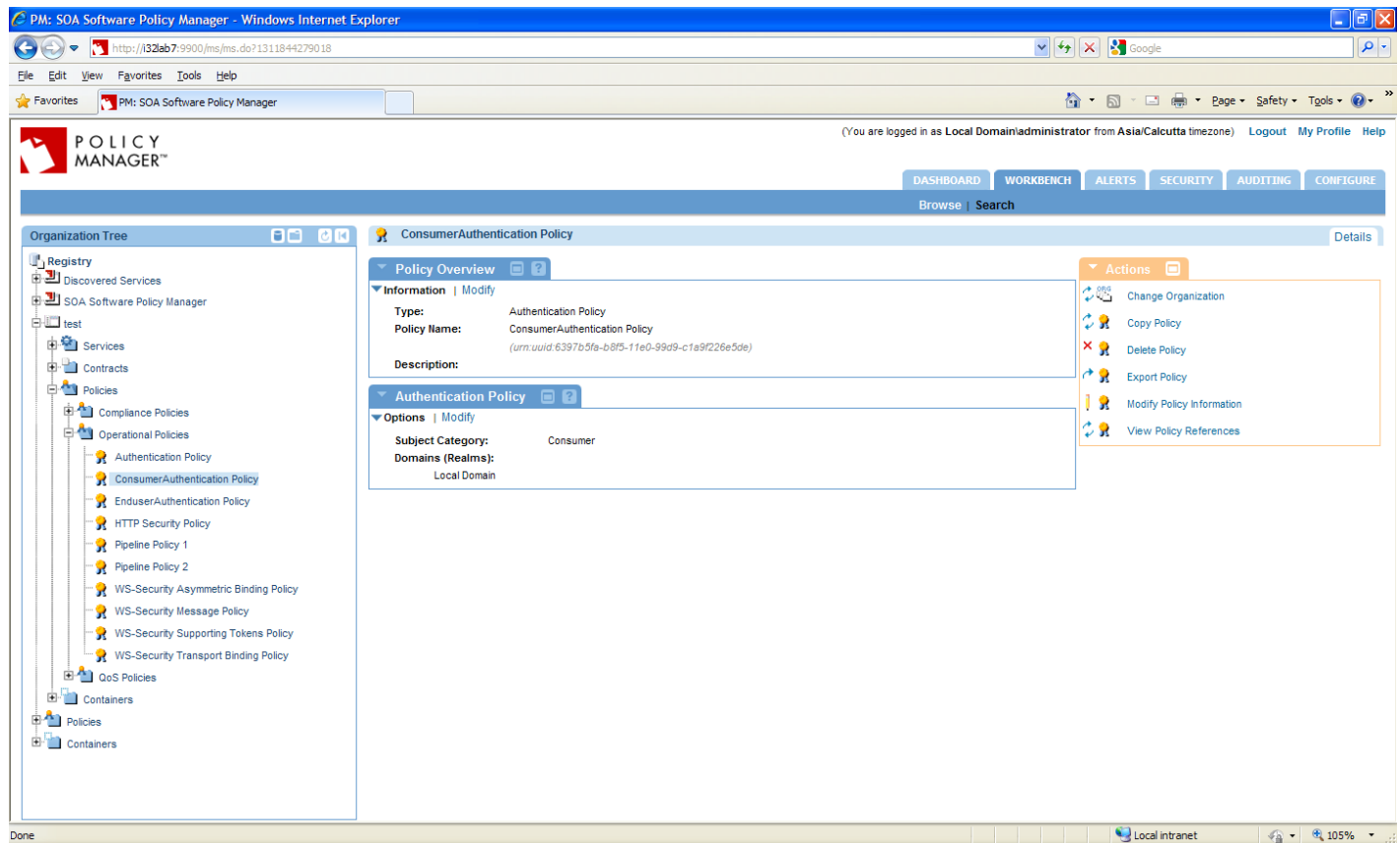
The information provided in this document is provided “AS IS” WITHOUT ANY WARRANTIES OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY. SOA Software may make changes to this document at any time without notice. All comparisons, functionalities and measures as related to similar products and services offered by other vendors are based on SOA Software’s internal assessment and/or publicly available information of SOA Software and other vendor product features, unless otherwise specifically stated. Reliance by you on these assessments / comparative assessments is to be made solely on your own discretion and at your own risk. The content of this document may be out of date, and SOA Software makes no commitment to update this content. This document may refer to products, programs or services that are not available in your country. Consult your local SOA Software business contact for information regarding the products, programs and services that may be available to you. Applicable law may not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Using a Clusterable Cache with the WS-Security Asymmetric Binding Policy Usage Scenarios

This document provides illustrates how to use clusterable caching with the WS-Security Asymmetric Binding Policy.

- 1 Launch the Policy Manager Management Console and create a physical service.
- 2 Virtualize this physical service and host it on Cluster with at least two Network Director (ND) nodes.
- 3 Perform the required steps for setting up a clusterable cache and using in the com.soa.policy.handle.wssp.noncecache and com.soa.grid property as illustrated in the Using a Clusterable Cache topic (http://docs.soa.com/ag/performance/using_clusterable_cache.htm)
- 4 Assign Detailed Auditing, Consumer Authentication, Enduser Authentication, WS-Security Asymmetric Binding, WS-Security Supporting Tokens and WS-Security Message Policies to virtual service.

Consumer Authentication Policy Configuration:



End-user Authentication Policy Configuration:

The screenshot displays the SOA Software Policy Manager web application running in a Windows Internet Explorer browser. The address bar shows the URL: `http://132ab7:9900/fms/fms.do?1311844279018`. The browser's Favorites bar shows "PM: SOA Software Policy Manager".

The application interface includes a top navigation bar with tabs: DASHBOARD, WORKBENCH, ALERTS, SECURITY, AUDITING, and CONFIGURE. Below this is a "Browse | Search" bar. The main content area is titled "EnduserAuthentication Policy" and features a "Details" link.

On the left, the "Organization Tree" shows a hierarchy: Registry > Discovered Services > SOA Software Policy Manager > test > Services > Contracts > Policies > Operational Policies > Authentication Policy > EnduserAuthentication Policy. The "Authentication Policy" node is highlighted.

The main panel displays the "Policy Overview" for "EnduserAuthentication Policy". It includes the following information:

- Policy Overview**
 - Information | Modify**
 - Type: Authentication Policy
 - Policy Name: EnduserAuthentication Policy
 - Description: (urn:uuid:6f5aba63-b8f5-11e0-99d9-c1a9f226e5de)
 - Authentication Policy | Modify**
 - Options | Modify
 - Subject Category: End-User
 - Domains (Realms): Local Domain

On the right, the "Actions" menu includes the following options:

- Change Organization
- Copy Policy
- Delete Policy
- Export Policy
- Modify Policy Information
- View Policy References

The status bar at the bottom shows the URL: `javascript:openobj('operationalpolicy', 'urn:uuid:6f5aba63-b8f5-11e0-99d9-c1a9f226e5de', 'EnduserAuthentication Policy', treeO` and the local intranet address.

WS-Security Asymmetric Binding Policy Configuration:

The screenshot displays the SOA Software Policy Manager web application in a Windows Internet Explorer browser. The interface is divided into several sections:

- Organization Tree (Left):** A hierarchical view of the policy structure. The path 'Policies > Operational Policies > WS-Security Asymmetric Binding Policy' is selected.
- Policy Overview (Top Center):**
 - Information:**
 - Type: WS-Security Asymmetric Binding Policy
 - Policy Name: WS-Security Asymmetric Binding Policy (urn:uuid:s72ce359-b8f5-11e0-99d9-c1a9f226e5de)
 - Description:
 - Options:**
 - WS-SecurityPolicy Version: 1.1
 - Security Header Layout: Lax
 - Include Timestamp: true
 - Encrypt Before Signing: false
 - Encrypt Signature: false
 - Protect Tokens: false
 - Only Sign Entire Headers and Body: true
 - WS-Security 1.1 Options:**
 - Must Support Key Identifier Reference: true
 - Must Support Issuer Serial Reference: true
 - Must Support External URI Reference: false
 - Must Support Embedded Token Reference: false
 - Must Support Thumbprint Reference: true
 - Require Signature Confirmation: false
 - Must Support Encrypted Key Reference: true
 - WS-Trust 1.0 Options:**
 - Must Support Client Challenge: false
 - Must Support Server Challenge: false
 - Require Client Entropy: true
 - Require Server Entropy: true
- Actions (Right):** A list of available actions for the selected policy:
 - Change Organization
 - Copy Policy
 - Delete Policy
 - Export Policy
 - Modify Policy Information
 - View Policy References

The browser's address bar shows the URL: `http://132.167.9900/ms/ms.do?1311844279018`. The status bar at the bottom indicates 'Local intranet' and a zoom level of 105%.

PM: SOA Software Policy Manager - Windows Internet Explorer

http://132lab7:9900/ms/ms.do?1311844279018

File Edit View Favorites Tools Help

PM: SOA Software Policy Manager

(You are logged in as Local Domain\administrator from Asia/Calcutta timezone) [Logout](#) [My Profile](#) [Help](#)

POLICY MANAGER™

DASHBOARD WORKBENCH ALERTS SECURITY AUDITING CONFIGURE

Browse | Search

Organization Tree

- Registry
 - Discovered Services
 - SOA Software Policy Manager
 - test
 - Services
 - Contracts
 - Policies
 - Compliance Policies
 - Operational Policies
 - Authentication Policy
 - ConsumerAuthentication Policy
 - EnduserAuthentication Policy
 - HTTP Security Policy
 - Pipeline Policy 1
 - Pipeline Policy 2
 - WS-Security Asymmetric Binding Policy**
 - WS-Security Message Policy
 - WS-Security Supporting Tokens Policy
 - WS-Security Transport Binding Policy
 - QoS Policies
 - Containers
 - Policies
 - Containers

WS-Security Asymmetric Binding Policy

Details

Must Support Server Challenge:	false
Require Client Entropy:	true
Require Server Entropy:	true
Must Support Issued Tokens:	true
Security Algorithm Configuration:	
Algorithm Suite:	TripleDesRsa15
Canonicalization:	Exclusive
XPath Version:	Not Specified
SOAP Normalization:	false
STR Transform:	false
Initiator Token:	
Token Type:	X.509
Version:	X.509 v3 Token Profile 1.0
Subject Category:	Consumer
Token Inclusion:	Always to Recipient
Key Identifier:	false
Issuer Serial:	false
Embedded Token:	false
Thumbprint:	true
Recipient Token:	
Token Type:	X.509
Version:	X.509 v3 Token Profile 1.0
Subject Category:	Service
Token Inclusion:	Always to Initiator
Key Identifier:	false
Issuer Serial:	false
Embedded Token:	false
Thumbprint:	true

Done

Local intranet 105%

WS-Security Supporting Tokens Policy Configuration:

The screenshot displays the SOA Software Policy Manager interface within a Windows Internet Explorer browser. The address bar shows the URL: `http://132ab7:9900/jms/ms.do?1311844279018`. The browser's title bar reads "PM: SOA Software Policy Manager - Windows Internet Explorer".

The application interface includes a top navigation bar with tabs: DASHBOARD, WORKBENCH, ALERTS, SECURITY, AUDITING, and CONFIGURE. Below this is a "Browse | Search" bar. The main content area is titled "WS-Security Supporting Tokens Policy" and features a "Details" link.

On the left, an "Organization Tree" shows a hierarchy: Registry > Discovered Services > SOA Software Policy Manager > test > Services > Contracts > Policies > Operational Policies > Authentication Policy > ConsumerAuthentication Policy > EnduserAuthentication Policy > HTTP Security Policy > Pipeline Policy 1 > Pipeline Policy 2 > WS-Security Asymmetric Binding Policy > WS-Security Message Policy > **WS-Security Supporting Tokens Policy** > WS-Security Transport Binding Policy > QoS Policies > Containers > Policies > Containers.

The main configuration area is divided into two sections:

- Policy Overview** (Information | Modify):
 - Type: WS-Security Supporting Tokens Policy
 - Policy Name: WS-Security Supporting Tokens Policy (urn:uuid:b9214b4f-b8f5-11e0-99d9-c1a9f226e5de)
 - Description:
- WS-Security Supporting Tokens Policy** (Options | Modify):
 - WS-SecurityPolicy Version: 1.1
 - Signed: false
 - Endorsing: false
 - Encrypted: false
 - Allowed Tokens:

Token Choice: 1	
Token Type:	Username
Version:	UsernameToken Profile 1.0
Subject Category:	End-User
Token Inclusion:	Always to Recipient

On the right, an "Actions" menu provides the following options: Change Organization, Copy Policy, Delete Policy, Export Policy, Modify Policy Information, and View Policy References.


The bottom status bar indicates "Done" and "Local intranet" with a zoom level of 105%.

WS-Security Message Policy Configuration:

The screenshot displays the SOA Software Policy Manager web application running in a Windows Internet Explorer browser. The address bar shows the URL `http://132.167.9900/ms/ms.do?1311844279018`. The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The application's navigation bar features tabs for DASHBOARD, WORKBENCH, ALERTS, SECURITY, AUDITING, and CONFIGURE. The main content area is titled "WS-Security Message Policy" and includes a "Details" link. On the left, an "Organization Tree" shows the hierarchy: Registry > Discovered Services > SOA Software Policy Manager > test > Services > Contracts > Policies > Operational Policies > WS-Security Message Policy. The main configuration panel for "WS-Security Message Policy" (Version: 1.1) includes sections for Options, Signature, Encryption, and Required Content. The Signature section shows "Include Body: true", "Headers: None", "Elements: None", and "Namespace Prefixes: None". The Encryption section shows "Include Body: true", "Headers: None", "Elements: None", and "Namespace Prefixes: None". The Required Content section indicates "Policy content not defined." On the right, a sidebar contains links for "Export Policy", "Modify Policy Information", and "View Policy References". The status bar at the bottom indicates the user is logged in as "Local Domainadministrator" from the "Asia/Calcutta" timezone, with a "Local intranet" connection and a zoom level of 105%.

5 Assign PKI keys and certificate to the virtual service:

SOA Software Policy Manager - Manage PKI Keys (Service Identities) Wizard - Windows Internet Explorer



Select Key Management Option

The "Manage PKI Keys (Service Identities) Wizard" provides key management options that allow you to generate public and private keys to facilitate service access. A service can be assigned a single key identity and can be deployed in multiple Management Point Containers. The "Select Key Management Option" screen provides options for managing the key configuration of the current object (service).

The "Service Identity Details" section displays a summary of key information about the object type including "Type," "Service Name," and "Service Key."

The "PKI Keys Details" section displays the "Public Key" that has been generated and assigned to the object. If keys have not been generated and assigned, the "None Found" message displays.

The "Certificate Details" section displays a summary of information for the certificate assigned to the current object. Assigned certificates can be generated or imported using this wizard. Certificate information presented includes Subject DN, Issuer DN, Serial Number, Effective Date, and Expiration Date. If a certificate has not been assigned, the "None Found" message displays.

The "Key Management Options" section provides functions for performing key and certificate management for the current object. Option categories include "Generate," "Import," "Export,"

Service Identity Details

Type: Managed Virtual Service

Service Name: EchoService_vs0

Service Key: uddi:67e9f41c-b8e2-11e0-9de8-8f9f507f7930

PKI Keys Details

Public Key: MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQCCVzRLFHAQqeO
zJRU0NjeAwEsAclrlqkDFGTU9eQG1t4JG4bh4ybpqTFa/viX 4B+3rlfvhGuzb8roCFfg
k9ezHt+e3nW89326SvjOTJhqY
57ervd9vHprbEelccpEvGd2s2jc5vS74GXQ1BXGSwgbHsFHGbN 2T0iIMgxe/dT9QIDAQAB

Certificate Details

Subject DN: EMAILADDRESS=sss@soa.com, CN=i32linux5.soa.local, OU=SOA, O=SOA, L=Hys, ST=AP, C=IN

Issuer DN: CN=inwqa-ca, DC=inwqa, DC=local

Serial Number: 566727787272682625564746

Effective Date/Time: 12/15/2010 10:35:40 GMT Expiration Date/Time: 12/15/2011 10:45:40 GMT

Private Key: true

Key Management Options

Generate Options

☐ Generate PKI Keys

☐ Generate X.509 Certificate

☐ Generate PKI Keys and X.509 Certificate

☐ Generate Certificate Signing Request (CSR)

Import Options

Export Options

☐ Export X.509 Certificate

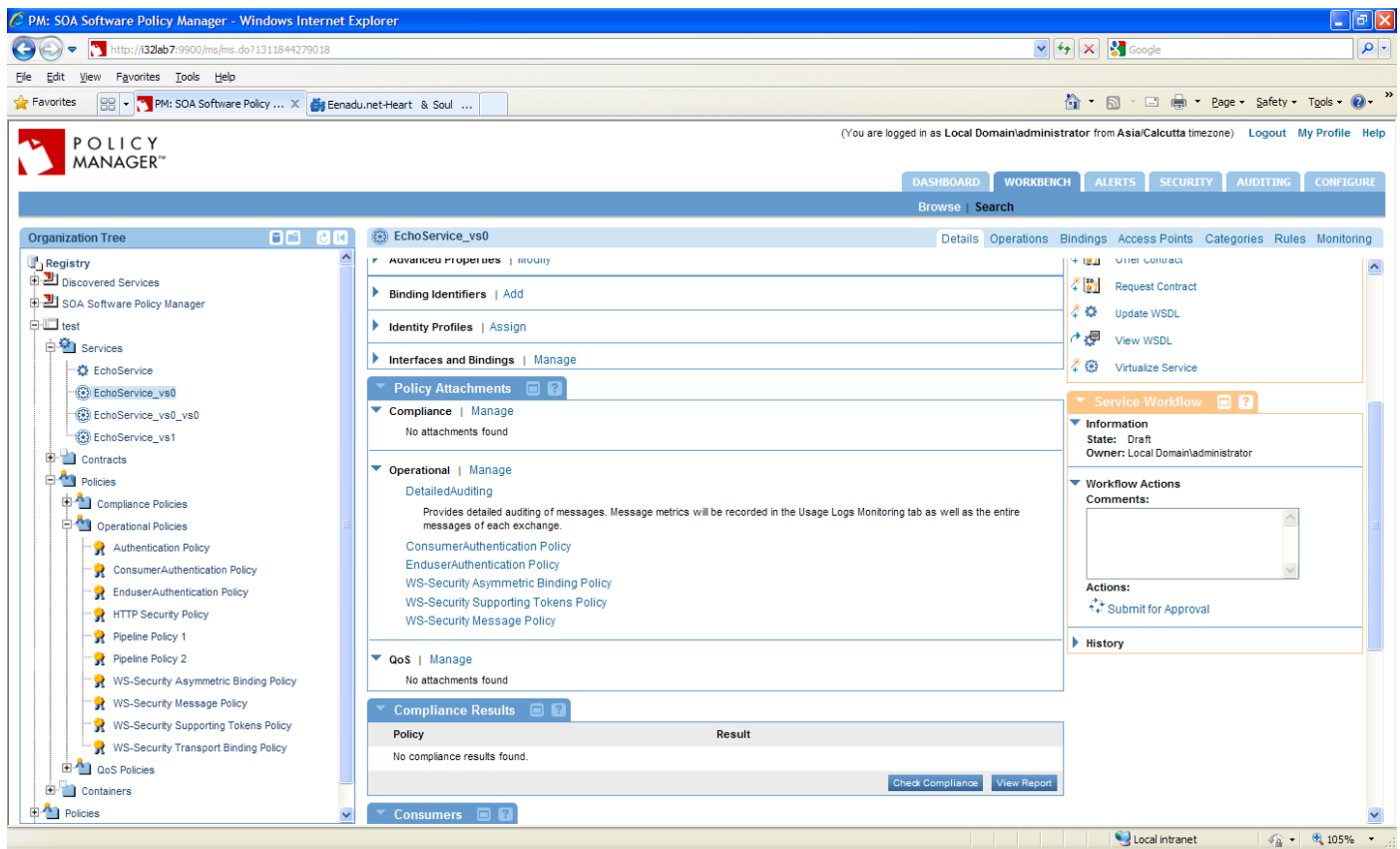
Delete Options

☐ Delete PKI Keys and X.509 Certificate

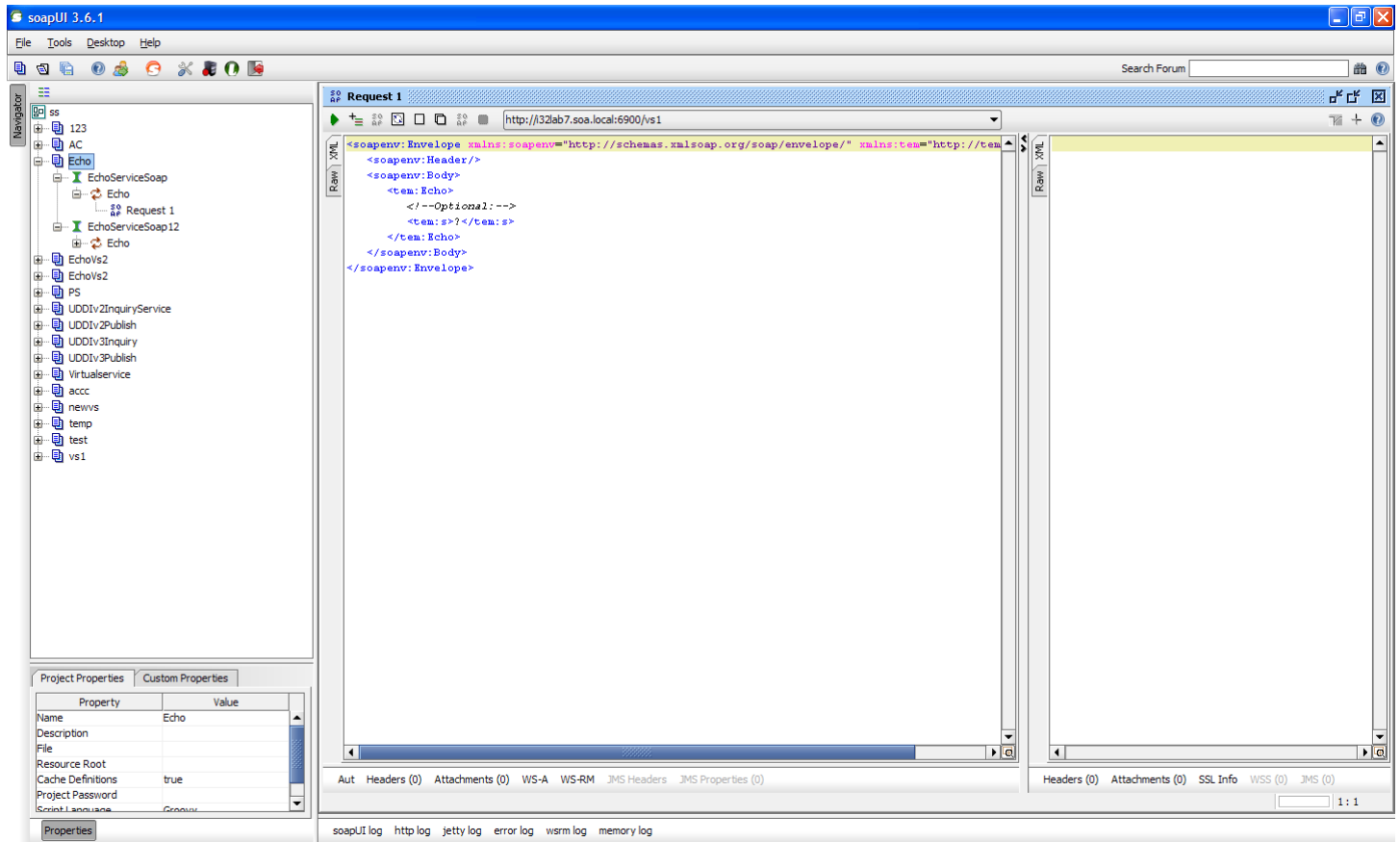
< Back Next > Finish > Cancel

Done Local intranet 105%

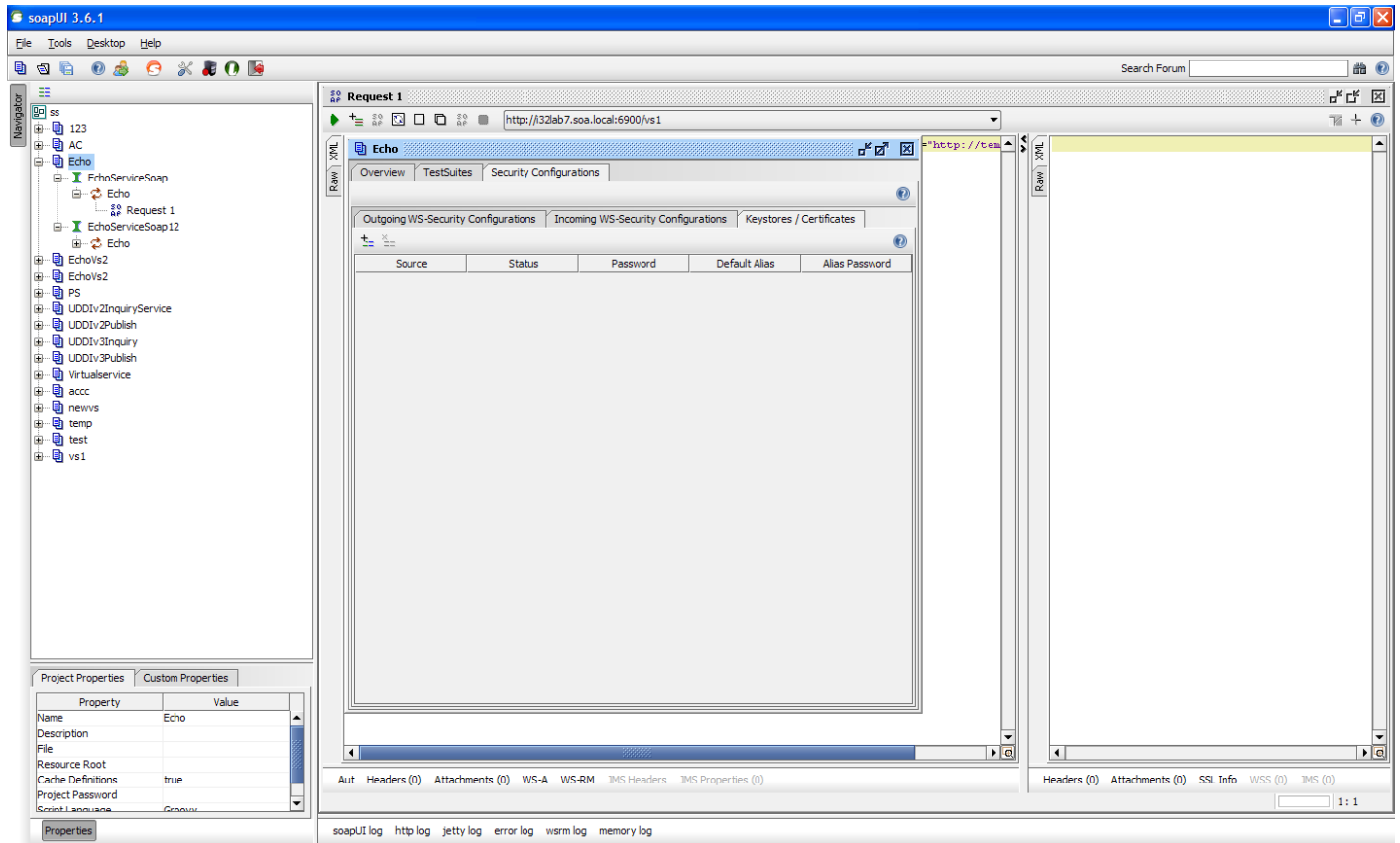
- 6 Assign Detailed Auditing, Consumer Authentication, Enduser Authentication, WS-Security Asymmetric Binding, WS-Security Supporting Token and WS-Security Message Policies to the virtual service.

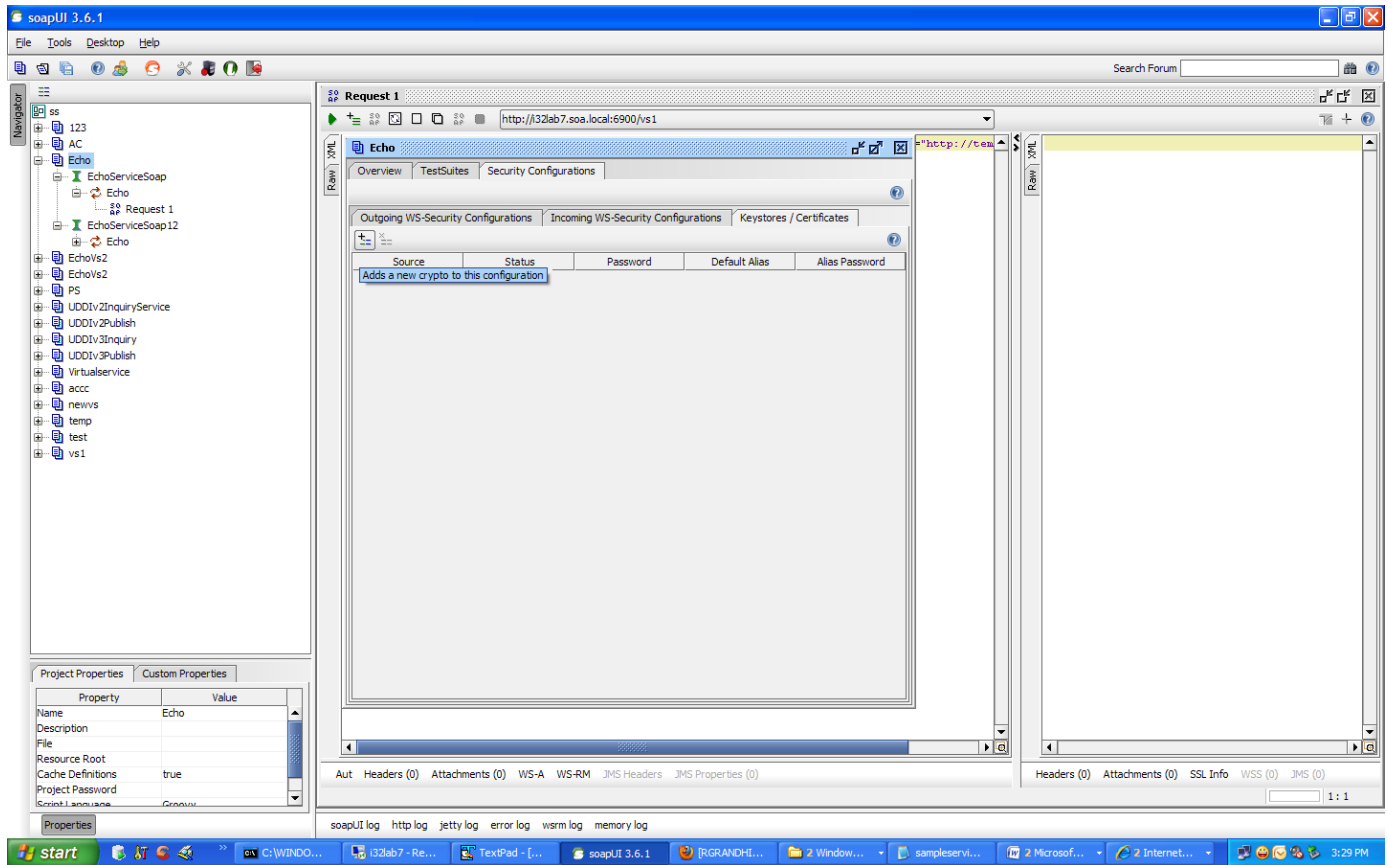


7 Create a project in SOAP UI using the virtual service WSDL URL.

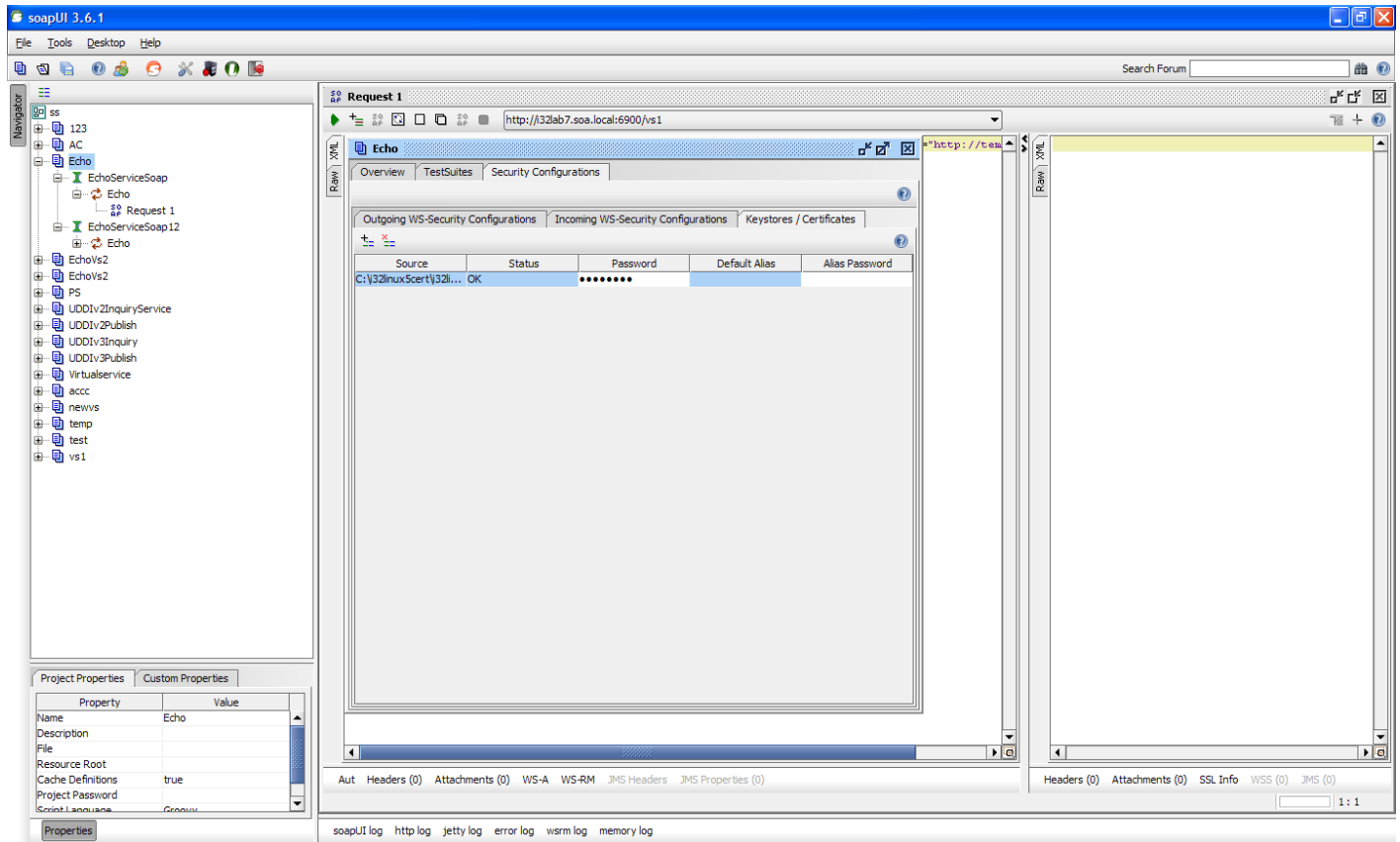


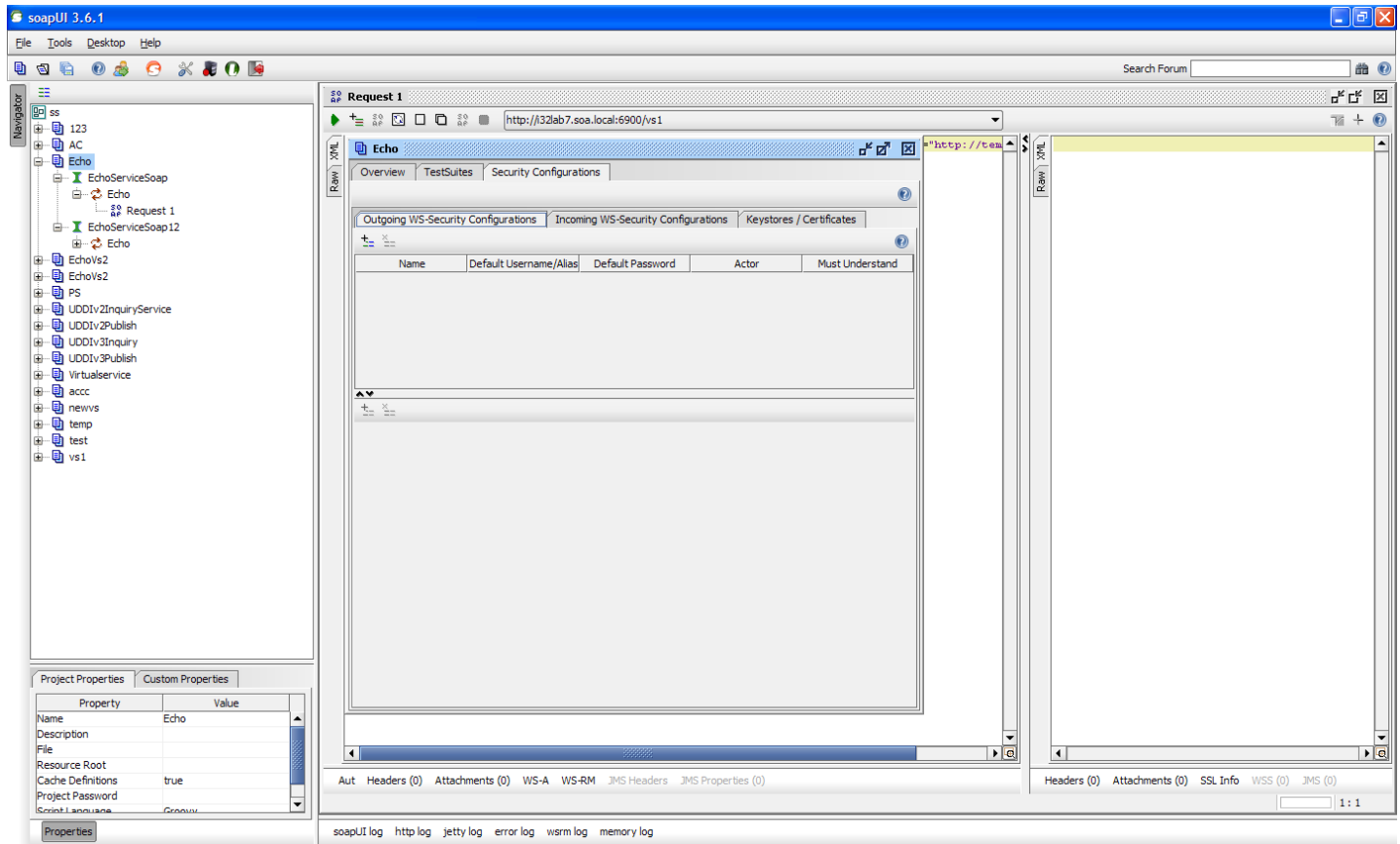
8 Double click on a project (e.g., "Echo").

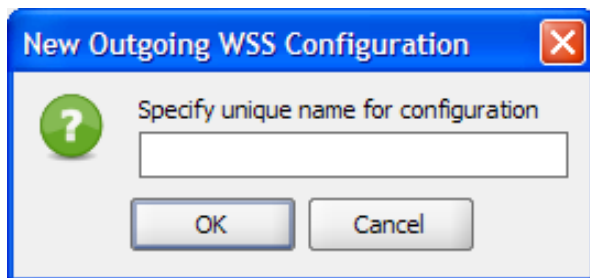
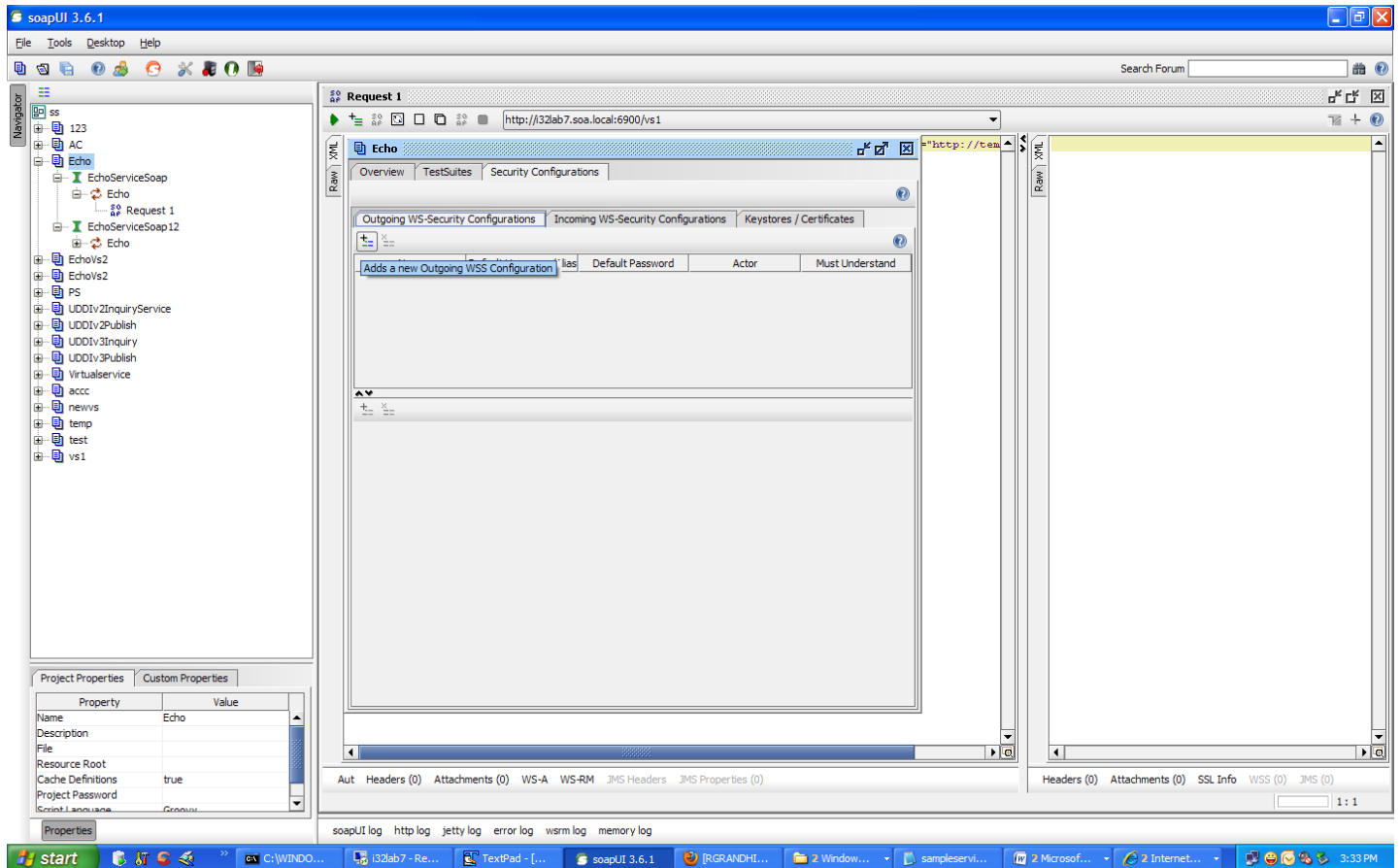
9 Navigate to **Security Configurations** → **Keystores/Certificates**.

10 Click **Adds a new crypto to this configuration.**

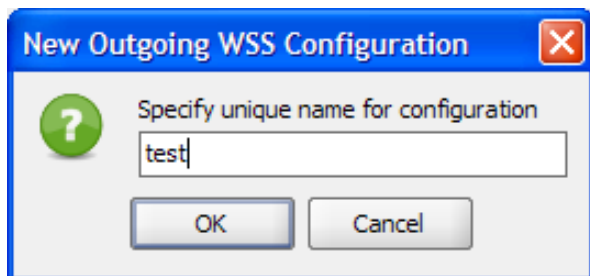
11 Assign a valid jks.

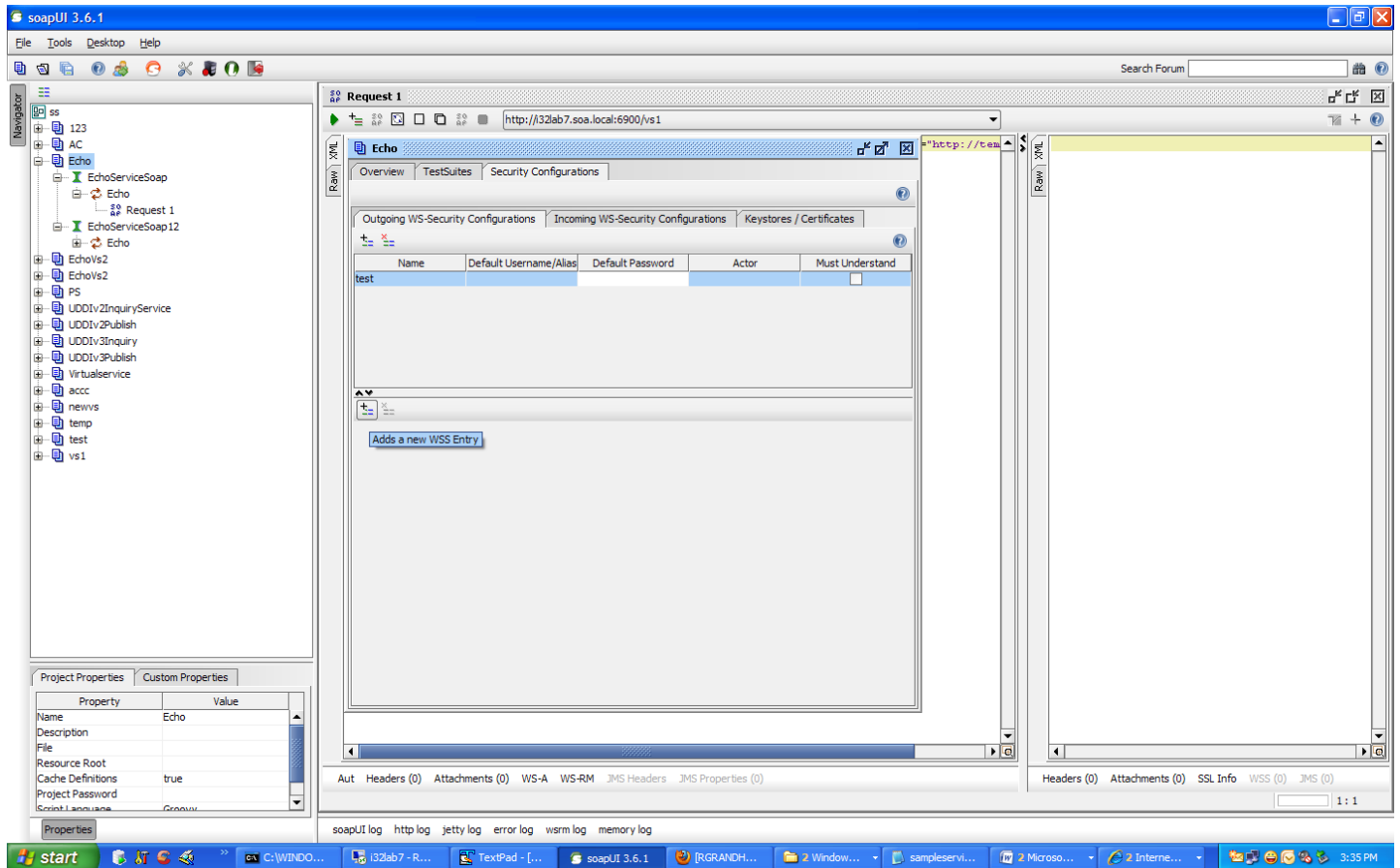


12 Click **Outgoing WS-Security Configurations**.

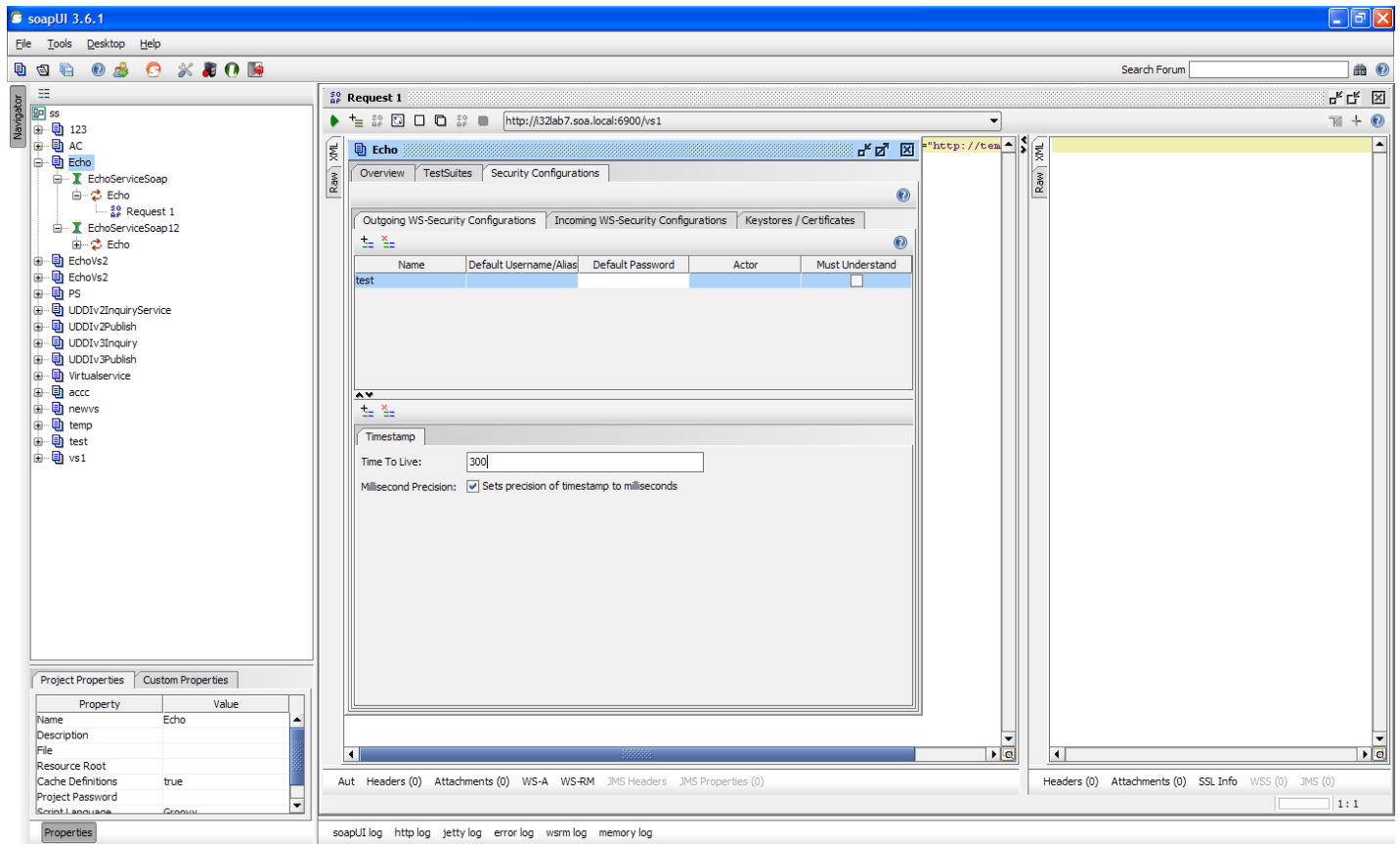
13 Click **Adds a new Outgoing WSS Configuration**.

14 Enter unique name.

15 Click **OK**.

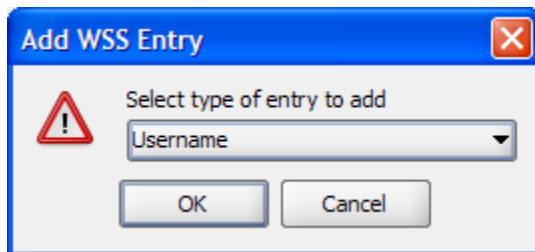
16 Click **Adds a new WSS Entry**.17 Select "Time stamp" and click **OK**.

18 Enter time to live as "300" milliseconds.

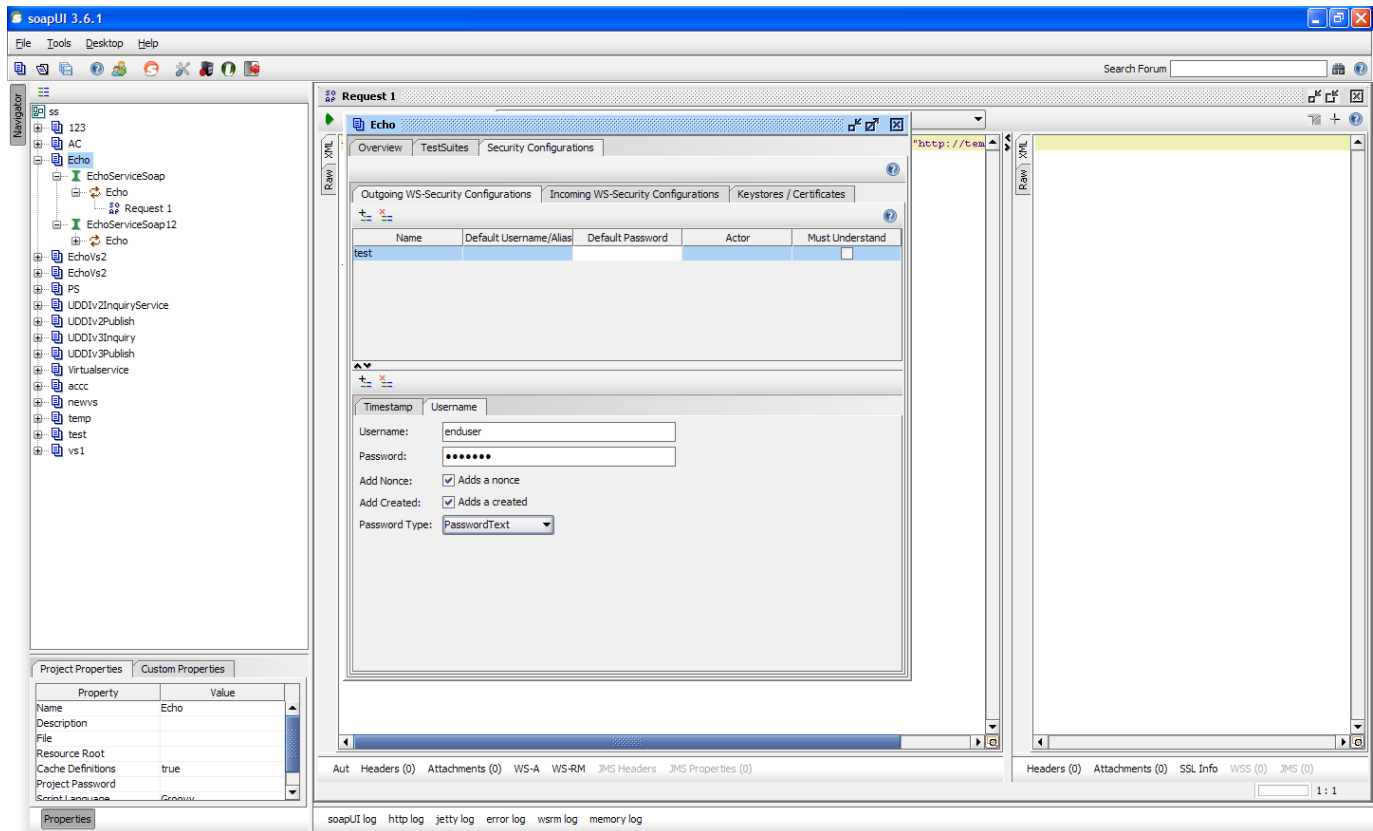


19 Click **Adds a new WSS Entry**.

20 Select WSS Entry type as "Username" and click **OK**.

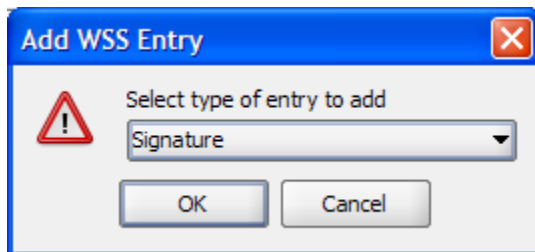


21 Configure "Username" as illustrated below.

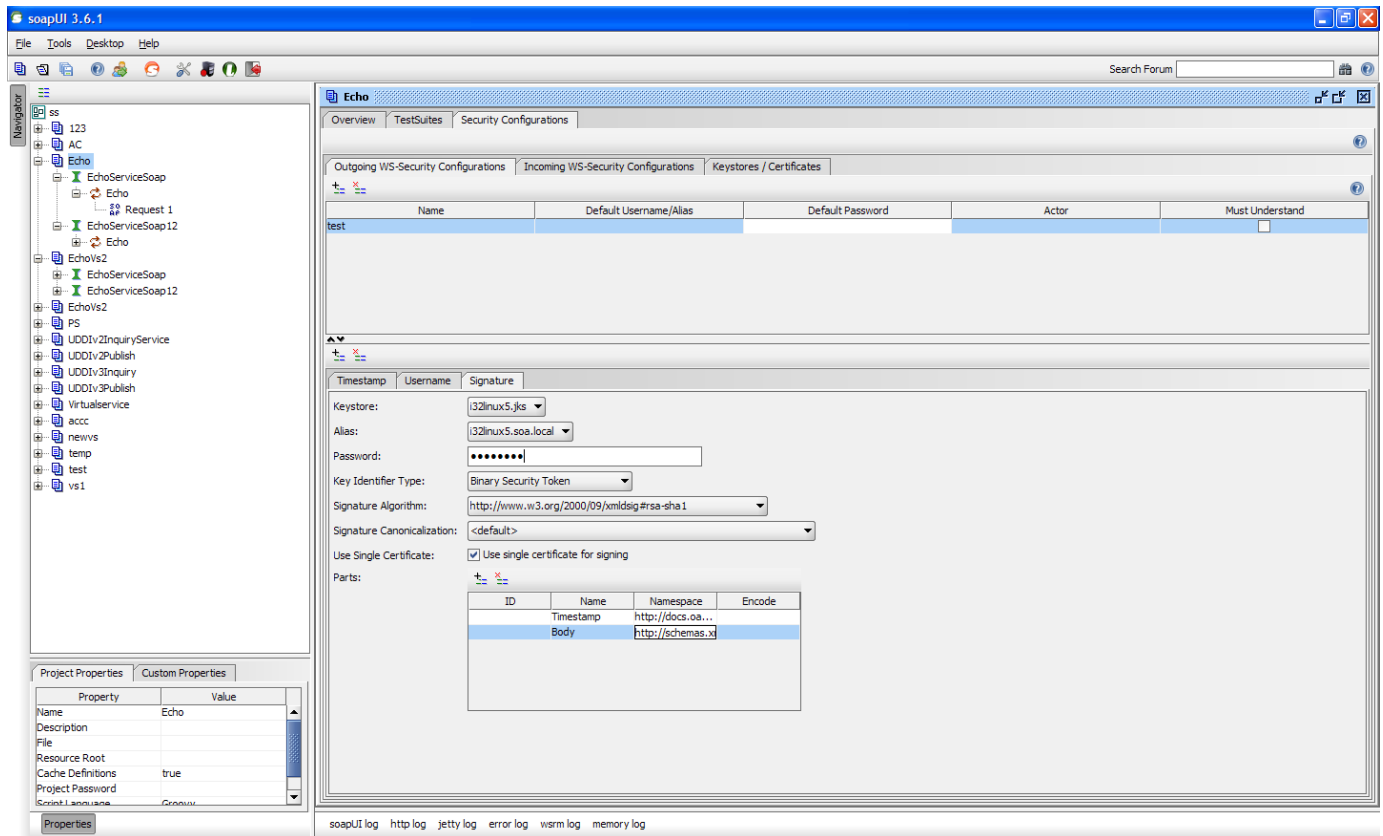


22 Click on **Adds a new WSS Entry**.

23 Select WSS type as "Signature" and click **OK**.



24 Configure signature as illustrated below.



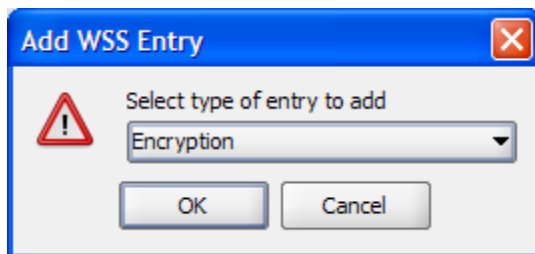
Name Name space

Timestamp <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd>

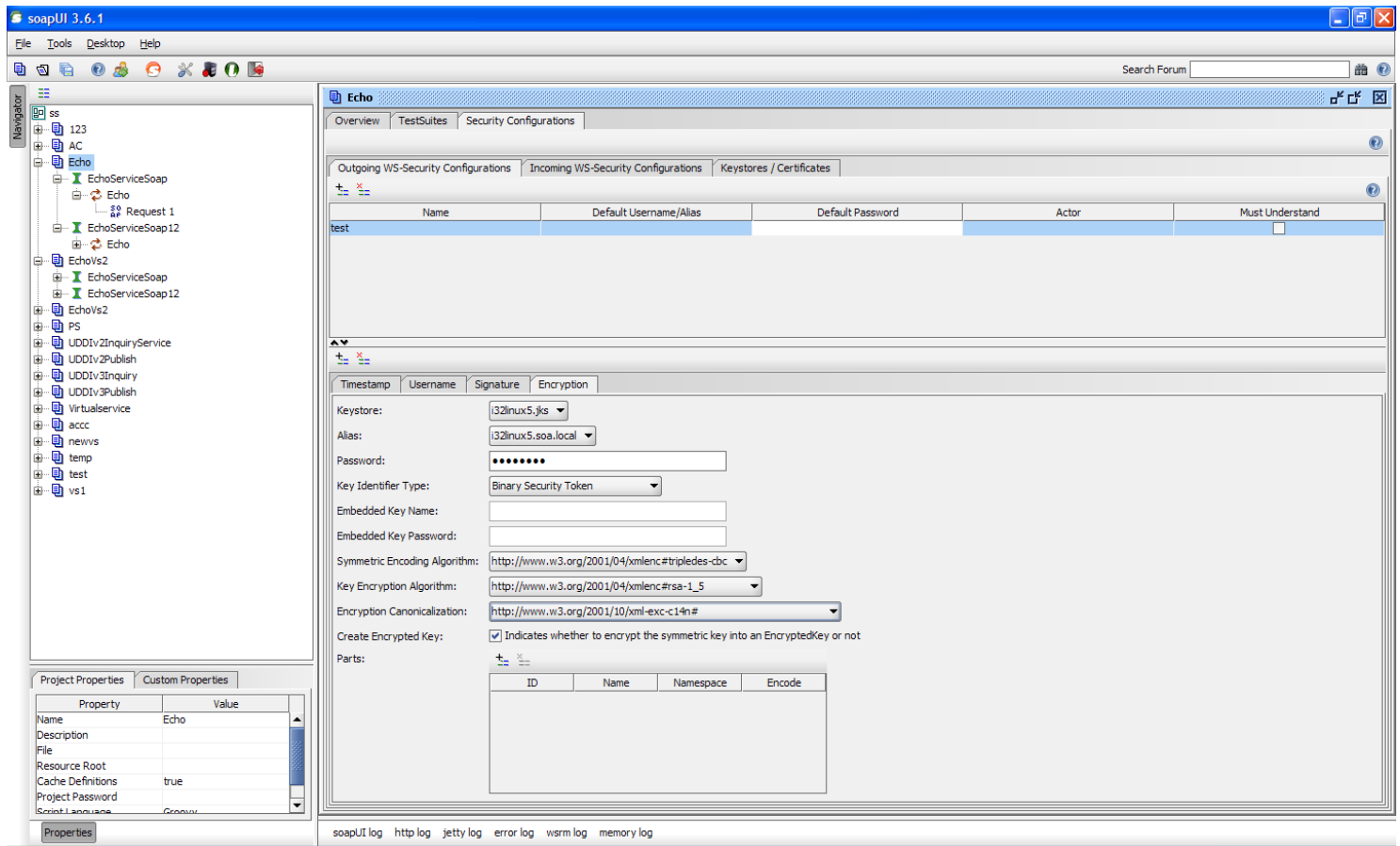
Body <http://schemas.xmlsoap.org/soap/envelope/>

25 Click **New WSS Entry**.

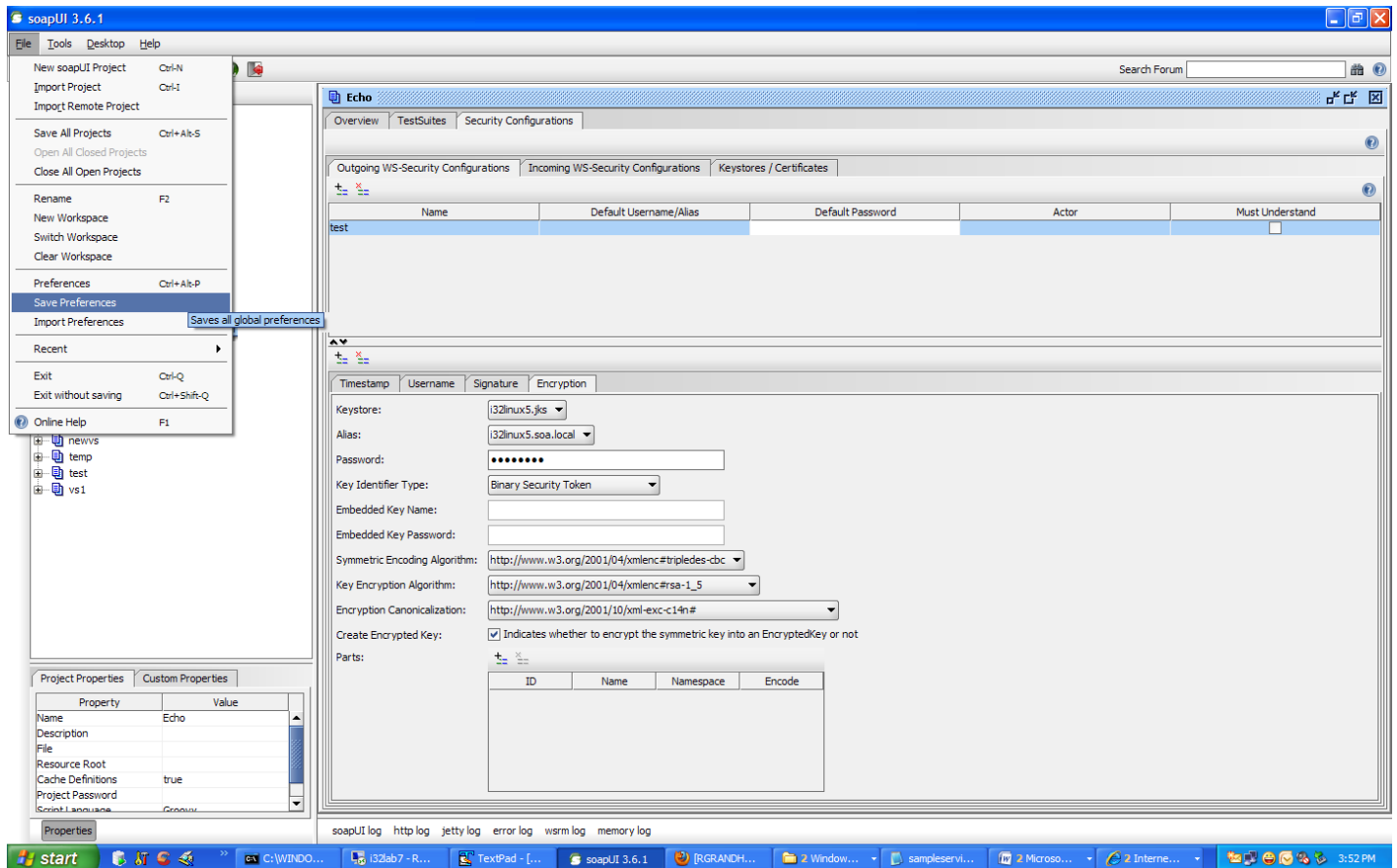
26 Select WSS type as "Encryption" and click **OK**.



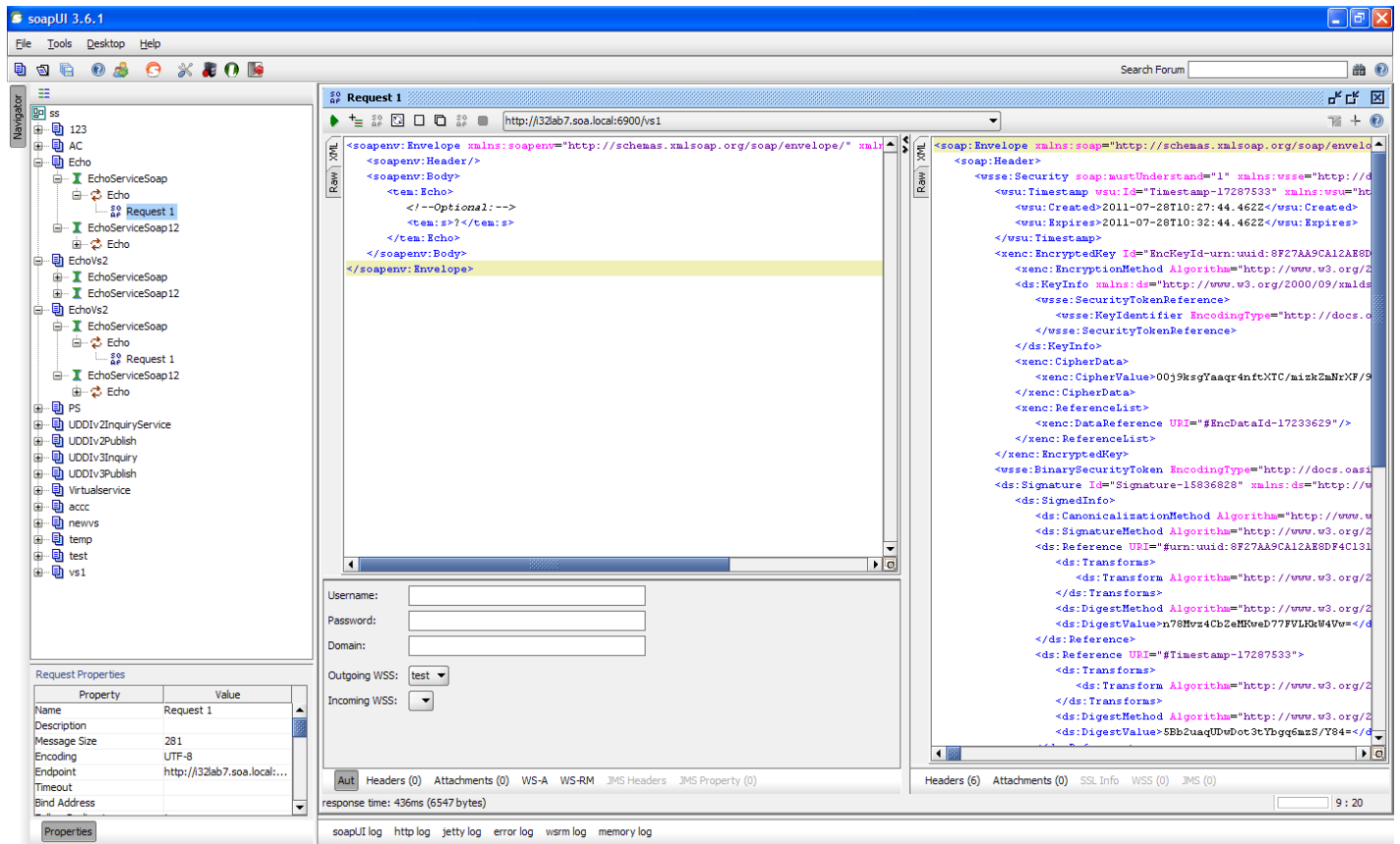
27 Configure Encryption as illustrated below.



28 Save preferences.



29 Select "test" in Outgoing WSS and send a request to the virtual service.



30 Request should get process successfully.

31 Observe recorded message tab.

SOA Software Policy Manager - Usage Data Details - Google Chrome

inwvm04:9900/ms/per_usagedata_nav_frameset.jsp?X-Csrf-Token=FO1V-ZWRG-V9II-001Z-7ZH9-VX17-A

2 of 2

Below is a list of the SOAP messages associated with the Usage record summarized above. Click on any record to see the corresponding message.

Message Date/Time	Record Name	Type
10/22/2014 21:10:15	APPLICATION	Complete request
10/22/2014 21:10:15	APPLICATION	Complete response

Message Details

Raw Format (Includes HTTP Headers): ☒

```

F5E3821F651C8B99721413992415545178" xmlns:xenc="http://www.w3.org/2001/04/xmldsig#"
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmldsig#rsa-1_5"/><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
<wsse:SecurityTokenReference><wsse:Reference URI="#F5E3821F651C8B99721413992415545179" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/></wsse:SecurityTokenReference></ds:KeyInfo><xenc:CipherData>
<xenc:CipherValue>irjwU/cZvYVj7Ot+Yp+4Ns2Vj6cpBoXBwo++VGrX5B8cHeDtBS9tnRo8/vpGdbpPN5RQTaLvcpMZCwQW75Q1vbw8eyly/EutRKln1b
</xenc:CipherValue></xenc:CipherData><xenc:ReferenceList><xenc:DataReference URI="#ED-F5E3821F651C8B99721413992415545180"/>
</xenc:ReferenceList></xenc:EncryptedKey><wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3" wsu:Id="X509-
F5E3821F651C8B99721413992415537173">MIIFBDCCA+ygAwIBAgIKMJu0TAAIAAAfzANBgkqhkiG9w0BAQUFAADBMRUwEwYKCCImZPyLGOBGF
</wsse:BinarySecurityToken><ds:Signature Id="SIG-F5E3821F651C8B99721413992415537177" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
<ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
<ec:InclusiveNamespaces PrefixList="soapenv:tem" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:CanonicalizationMethod>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/><ds:Reference URI="#TS-
F5E3821F651C8B99721413992415535171"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
<ec:InclusiveNamespaces PrefixList="wsse:soapenv:tem" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform></ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>pQpYipHBjQ4MMDMYCAB0kzK+u3M=</ds:DigestValue>
</ds:Reference><ds:Reference URI="#id-F5E3821F651C8B99721413992415537176"><ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
<ec:InclusiveNamespaces PrefixList="tem" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform></ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><ds:DigestValue>4M+TQ4RZX+3nyih2JfNhW5tShcU=</ds:DigestValue>
</ds:Reference></ds:SignedInfo><ds:SignatureValue>lp1mvJJ9TImpzayxmap1CKghffFIOMyzNcu/AzDCmdtKGYt7z9NyZwm9jAckDxgkC49tVJbf
ZoyhsvhqKVEs/xwM0wrQKht/vwy/vi+rtMmW6lZ2OaeMWgQ1AaQsFzthw/0iN+hrjpxvsllryW
Q3XBCHz2Pevglkhqzk=</ds:SignatureValue><ds:KeyInfo Id="KI-F5E3821F651C8B99721413992415537174">
<wsse:SecurityTokenReference wsu:Id="STR-F5E3821F651C8B99721413992415537175"><wsse:Reference URI="#X509-
F5E3821F651C8B99721413992415537173" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
</wsse:SecurityTokenReference></ds:KeyInfo></ds:Signature><wsse:UsernameToken wsu:Id="UsernameToken-
F5E3821F651C8B99721413992415536172"><wsse:Username>a</wsse:Username><wsse:Password Type="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText">s</wsse:Password>
<wsse:Nonce EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary">xAshBkUQrbpQwV/NsWbjwA==</wsse:Nonce><wsu:Created>2014-10-22T15:40:15.536Z</wsu:Created><wsse:UsernameToken>
<wsu:Timestamp wsu:Id="TS-F5E3821F651C8B99721413992415535171"><wsu:Created>2014-10-22T15:40:15.535Z</wsu:Created>
<wsu:Expires>2014-10-22T15:45:15.535Z</wsu:Expires></wsu:Timestamp></wsse:Security></soapenv:Header>
<soapenv:Body wsu:Id="id-F5E3821F651C8B99721413992415537176" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"><xenc:EncryptedData Id="ED-
F5E3821F651C8B99721413992415545180" Type="http://www.w3.org/2001/04/xmldsig#Content" xmlns:xenc="http://www.w3.org/2001/04/xmldsig#"
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmldsig#tripleDES-cbc"/><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
<wsse:SecurityTokenReference wsse11:TokenType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsse11="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.1.xsd"><wsse:Reference URI="#EK-F5E3821F651C8B99721413992415545178"/>
</wsse:SecurityTokenReference></ds:KeyInfo><xenc:CipherData>
<xenc:CipherValue>fx/mZR/VaUwe60vcMeo2JOLFGRU7LzVrk9QDMpz2NMfuEhAysh++45bWX4oc9ftNoAxs5sawYWa7ZdTJ1QT5BSdTKEMiPv26zJkVc

```

- 32 Verify that the wsse:Nonce header passed through the request. Similarly view any continuous requests and make sure that the tokens are unique for various Network Director nodes.