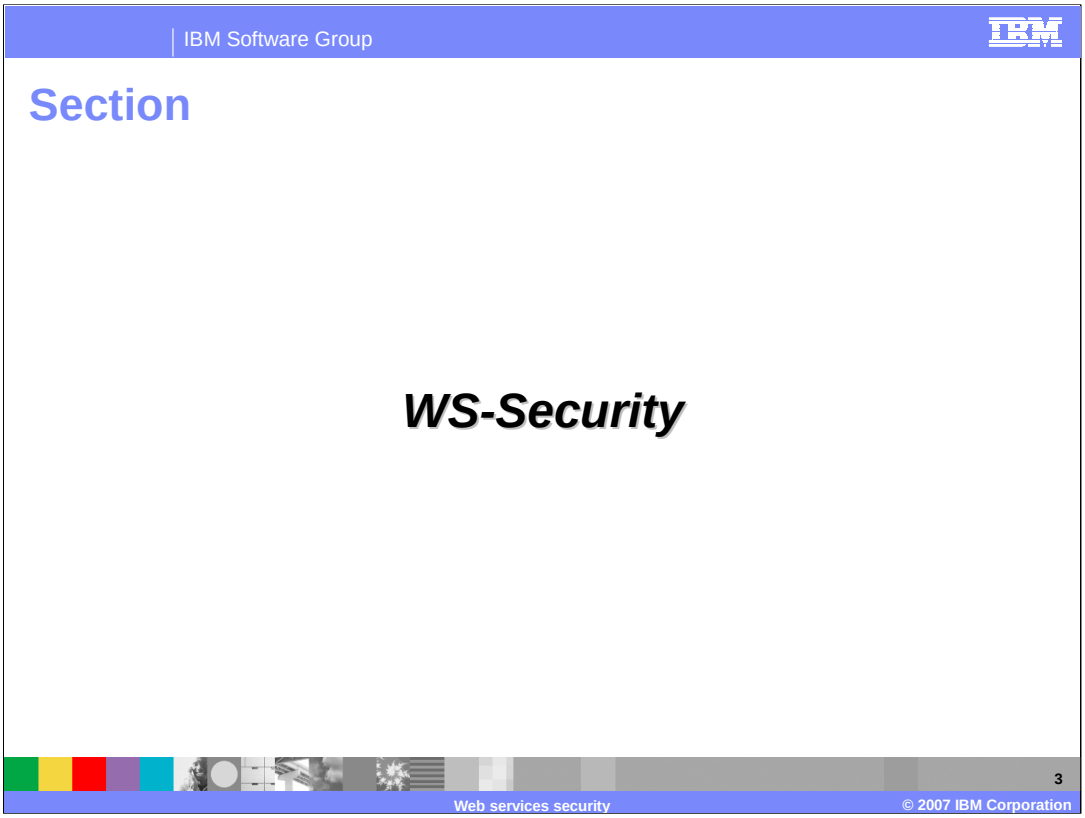
This presentation will explain the new policy sets feature for WS-Security in the feature pack for Web services.

Agenda

- WS-Security
- Problem determination

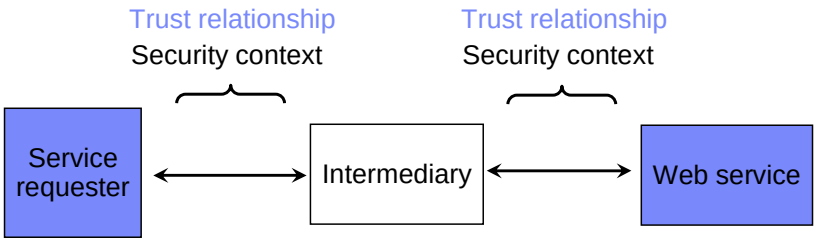
This presentation begins by explaining the policy set support for WS-Security in the Feature Pack for Web Services. This support is specific to the JAX-WS programming model.



This section explains the enhancements for Web Services Security in the Feature Pack for Web Services.

Point to point security

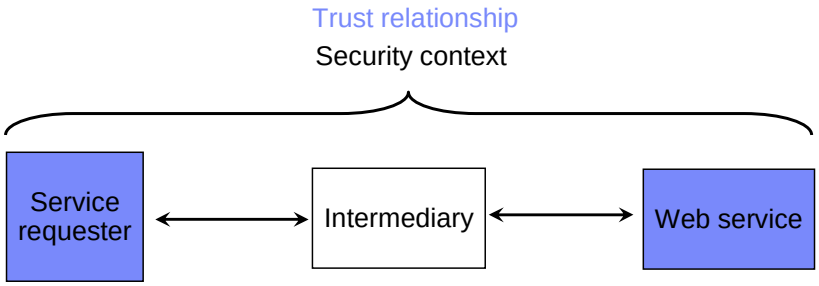
- HTTPS focuses on transport level security
  - Secures point to point communications
  - Maintains security context between endpoints



Traditionally Web services security has focused on securing point to point communications. HTTPS has often been used to maintain the security context between messaging endpoints. In cases where there are network intermediaries such as proxies, there are separate trust relationships associated for the separate point to point communications. This approach has worked well for securing remote procedure call based Web services.

Message level security

- Message level security provides end to end security
  - Provides message integrity, confidentiality and the ability to send security tokens
  - Useful for securing long running message exchanges



For messaging-based Web services, focusing on point to point security can add significant overhead, and so message level security is preferred. Message level security focuses on securing the entire end to end communication within a single security context. This is done through a combination of message integrity, confidentiality and use of security tokens to verify messages. This is an optimal security method for securing the type of long running message exchanges that are more common in messaging based Web Services.

Security enhancements

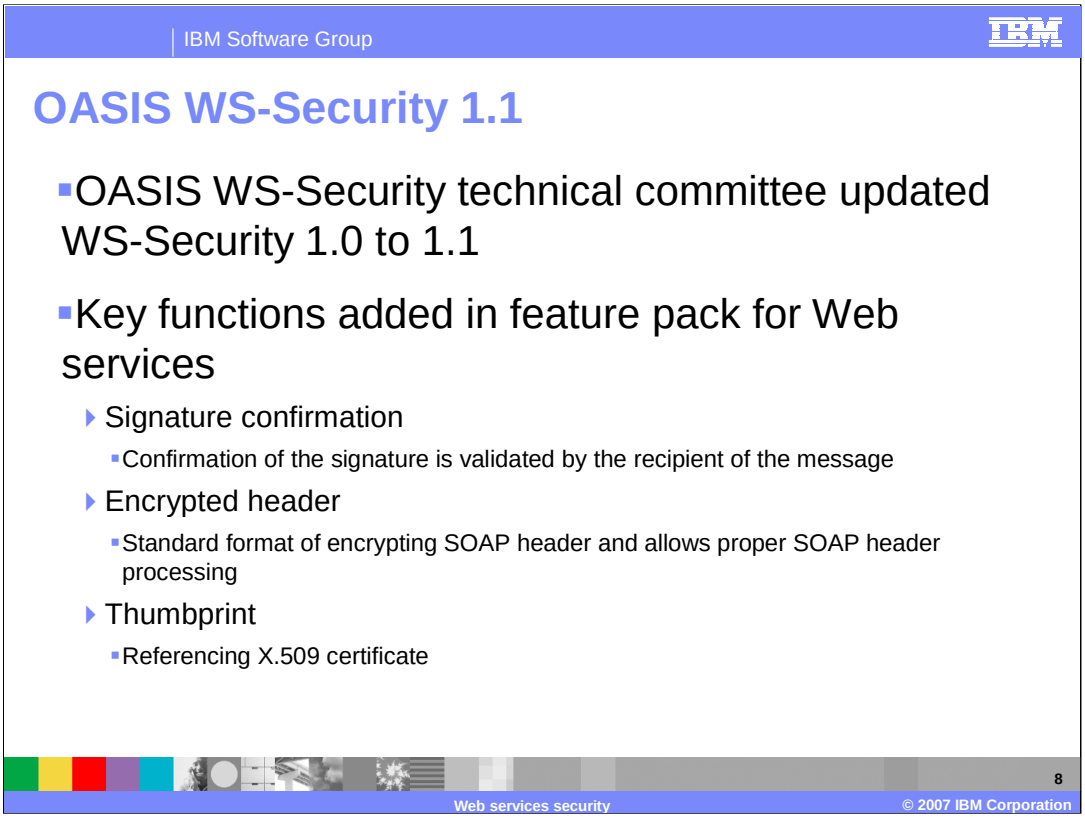
- WS-Security 1.0 and 1.1 standards define a framework to provide message level security to SOAP messages
  - XML digital signature to provide integrity protection
  - XML encryption to provide confidentiality protection
  - Flexible token framework for attaching security tokens with SOAP messages to provide authentication
- WS-Secure Conversation (WS-SC) defines the mechanism for establishing secure context for long running message exchanges

The Feature Pack for Web Services has several security enhancements. Support for the WS-Security 1.0 and 1.1 specifications provide a framework for securing SOAP messages through XML digital signature, XML encryption and a token framework for attaching security tokens to SOAP messages for authentication purposes. Support for the WS-secure conversation specification provides security for long running message exchanges.

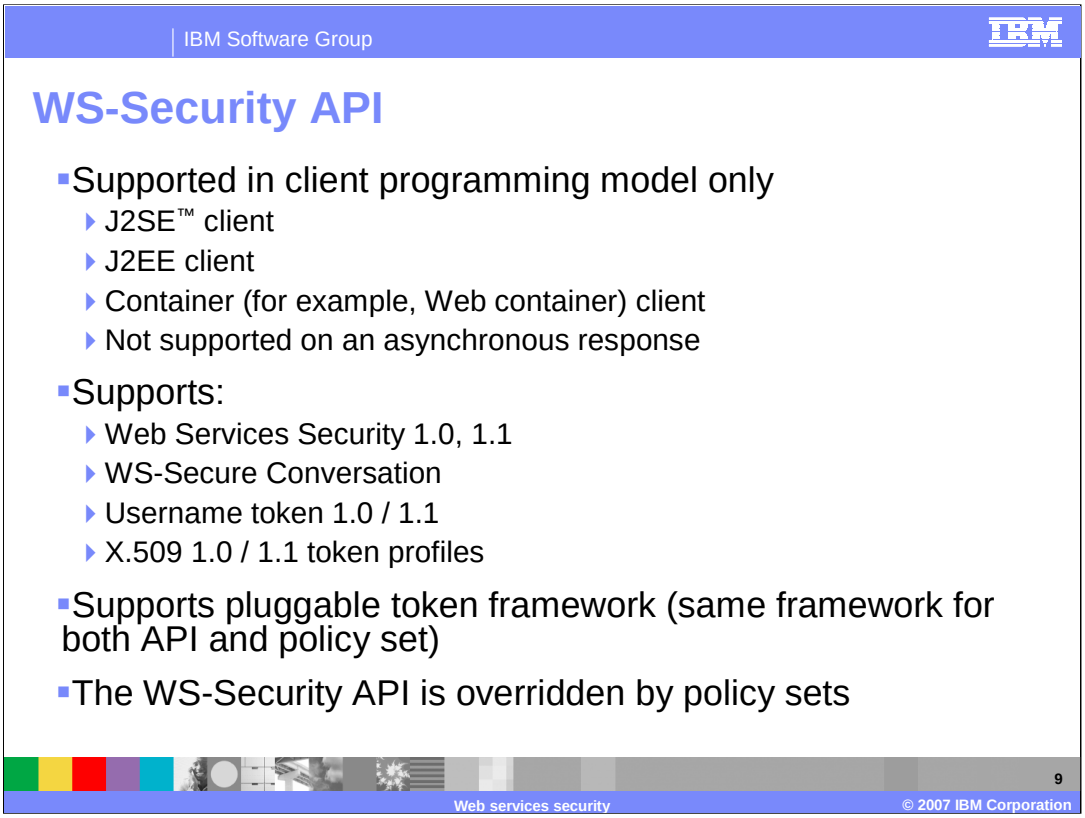
Secure conversation

- Built on top of OASIS WS-Security 1.0 / 1.1
  - WS-Security focuses on message protection and authentication, not a security context
- Web Services-Secure Conservation (WS-SC) defines:
  - A mechanism for establishing and sharing security context using the WS-Trust protocol
  - Deriving cryptographic keys from security contexts
    - Using symmetric cryptography (more efficient than asymmetric cryptography)
  - Enabling a secure conversation
    - Beneficial to secure reliable messaging

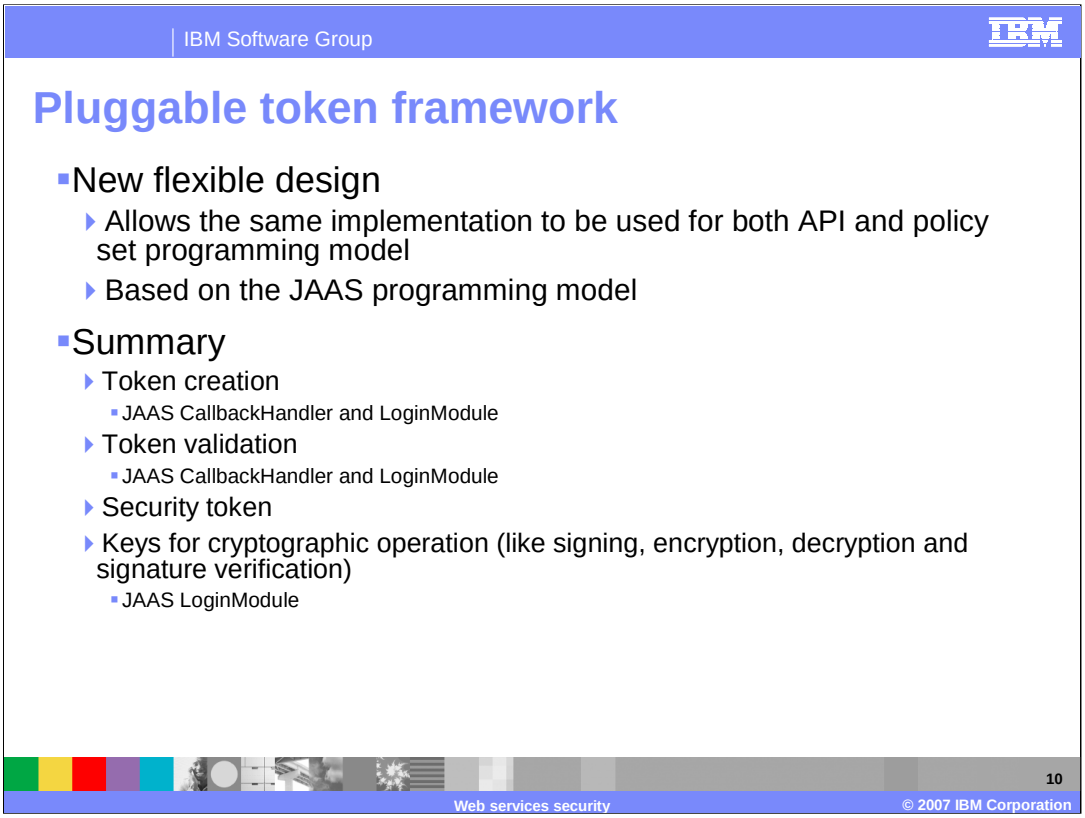
The Web Services Secure Conversation specification is built on top of the WS-Security 1.0 and 1.1 specifications. WS-Security focuses on message protect and authentication, but not on providing a security context. WS-Secure Conversation adds to this and defines a way to establish and share a security context based on the WS-Trust specification. WS-Secure Conversation can derive cryptographic keys from the security context using symmetric cryptography. This helps to enable a secure conversation for messaging based Web Services which is beneficial for securing reliable messaging services.



The OASIS WS-Security group has updated the specification to 1.1. The Feature Pack for Web Services adds support for several key functions from this specification, including; signature confirmation, the ability to encrypt SOAP headers, and the ability to add a thumbprint that references an X.509 certificate.



The Feature Pack for Web Services includes an API that can be used to add WS-Security on Web Services clients. The WS-Security API uses default values for most of the parameters. These defaults can be overridden where needed, but it requires fewer lines of code to perform basic tasks. The API supports the WS-Security 1.0 and 1.1 specifications, WS-Secure Conversation, username tokens and X.509 tokens. The WS-Security API also works with the pluggable token framework. When using policy sets, configurations specified by the API will be overridden; policy sets take precedence over the API.



The token processing and pluggable token architecture in the Web Service Security runtime for IBM WebSphere Application Server V6.1 Feature Pack has been redesigned to reuse the same security token interface and JAAS Login Module from the Web Services Security APIs. The same implementation of token creation and validation can be used in both the WS-Security API and the WS-Security SPI in the Web service security runtime.

WS-Security problem determination

- Common mistakes:
  - Mismatch policy and binding configuration between the client and service:
    - For example, if the service policy requires the body to be signed, the client policy must also have the body signed.
  - Cryptographic keys configuration:
    - For example, public key for encryption and private key for decryption, asymmetric and symmetric cryptography
  - XPath configuration
- Trace with these trace strings:
  - com.ibm.websphere.wssecurity.*=all
  - com.ibm.wsspi.wssecurity.*=all
  - com.ibm.ws.wssecurity.*=all

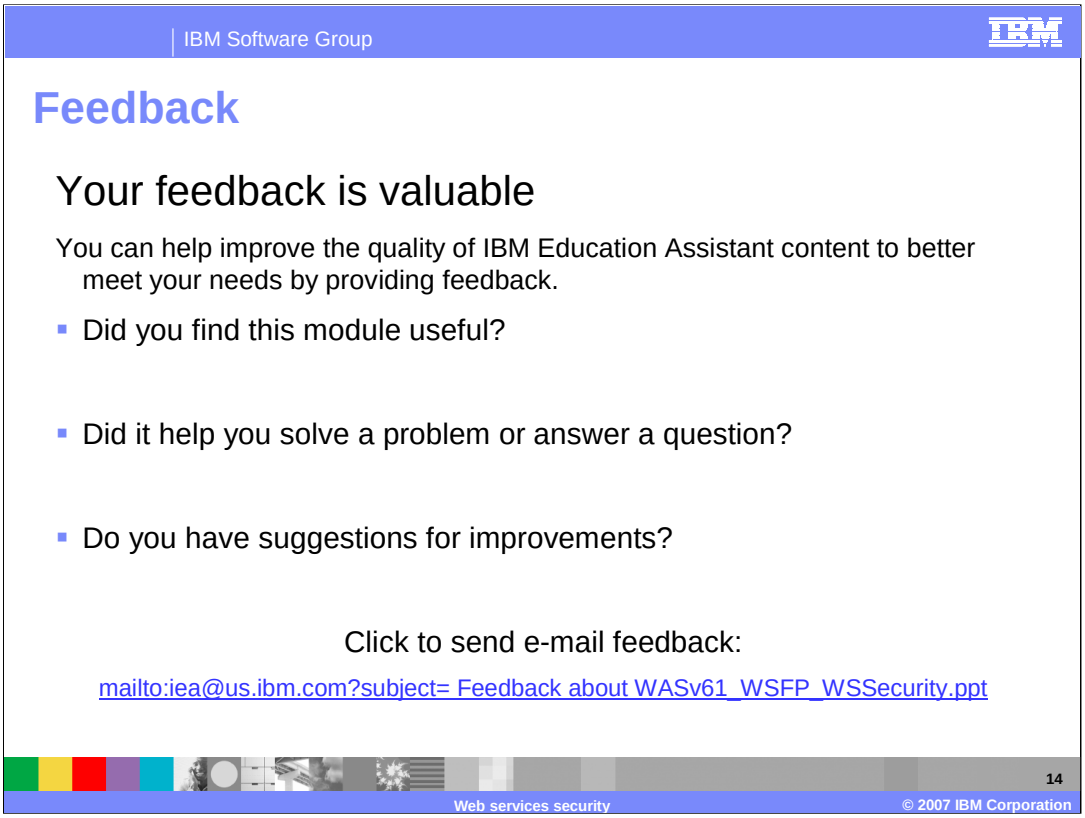
Common mistakes related to Web Service Security often deal with mismatching the policy configuration between the client and the service. When this occurs the client or service may not receive a message with the appropriate encryption or tokens that are expected. The trace strings to use for WS-Security are listed here for reference.

The next section provides a summary of this presentation.

Summary

- The Feature Pack for Web Services provides policy sets for WS-Security and WS-Secure conversation
  - Specific to JAX-WS

This presentation explained the policy set support for WS-Security and WS-Secure Conversation in the Feature Pack for Web Services. This support is specific to the JAX-WS programming model.



You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM WebSphere

J2EE, J2SE, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.