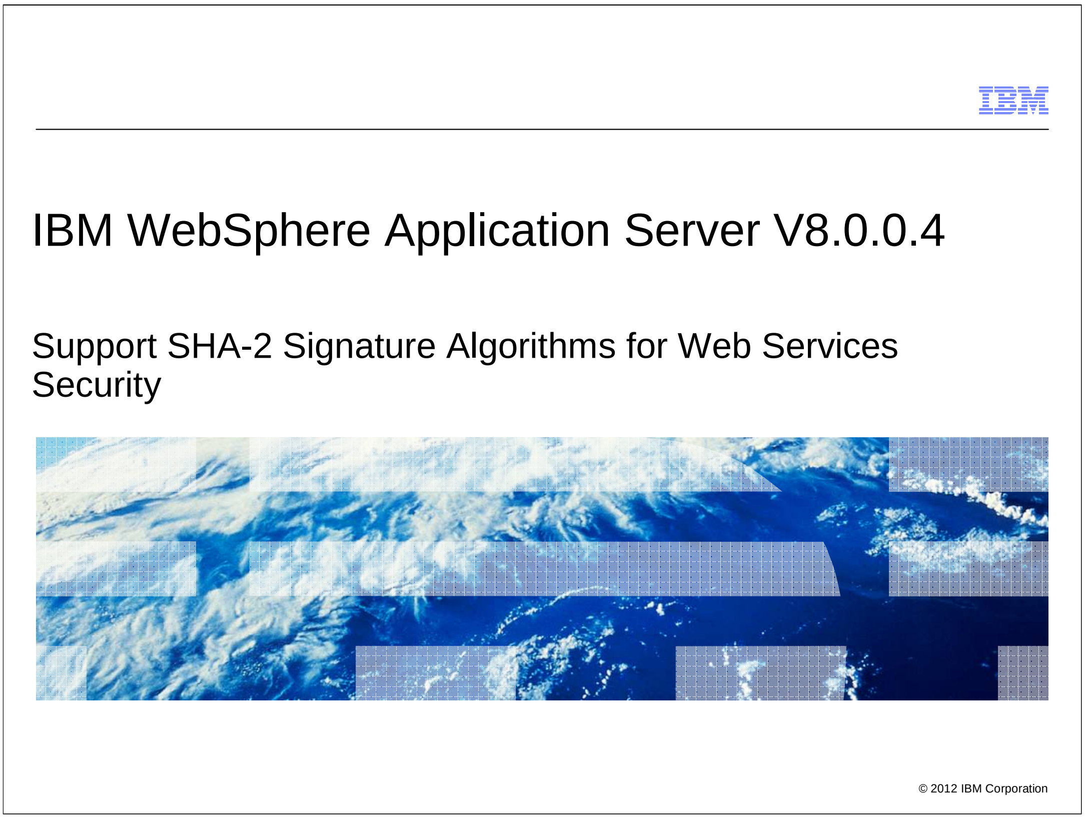
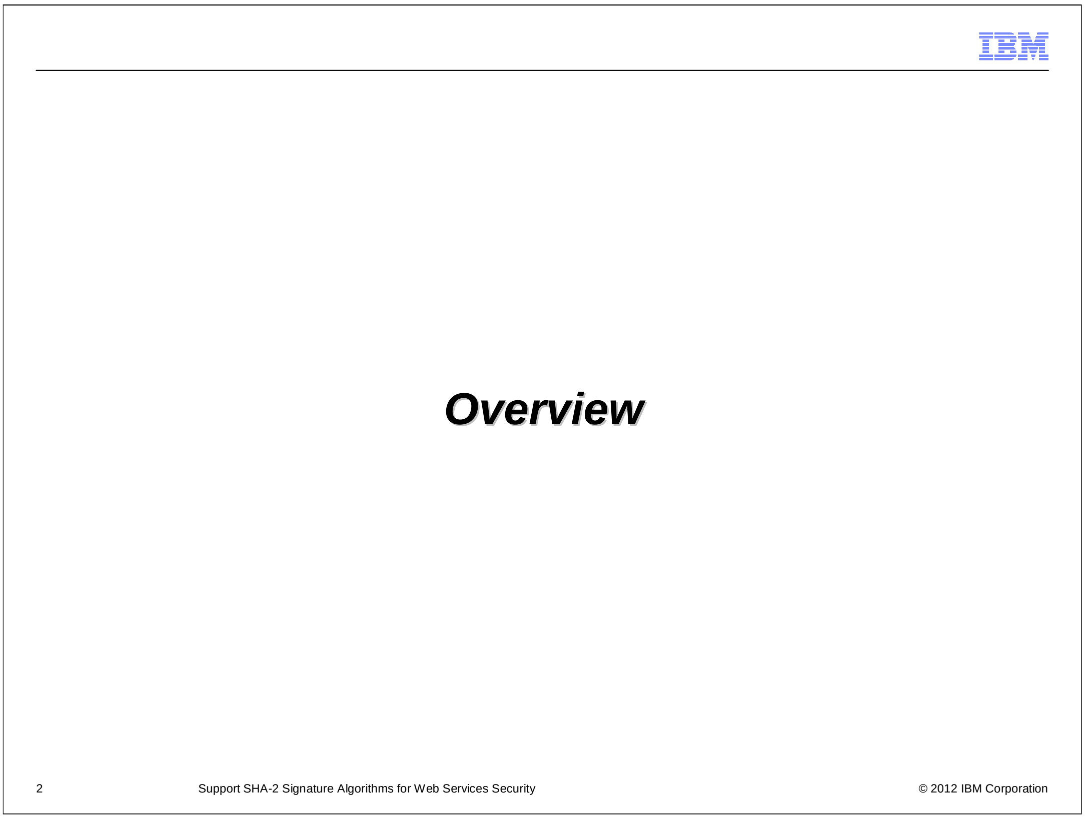


# IBM WebSphere Application Server V8.0.0.4

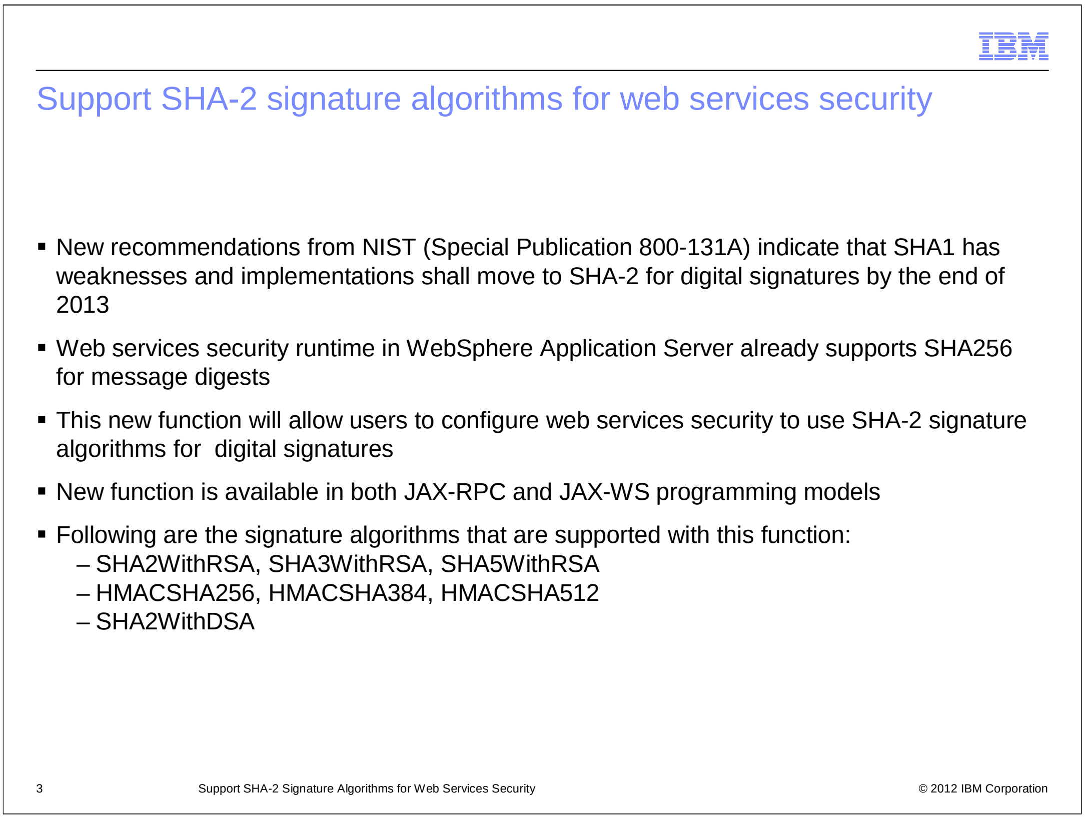
## Support SHA-2 Signature Algorithms for Web Services Security

This presentation describes the support of SHA-2 signature algorithms in web service security included in IBM WebSphere Application Server V8.0.0.4.



## Overview

This feature provides the support of SHA-2 signature algorithms in web service security. With this feature, web service client can sign SOAP message with SHA-2 signature algorithm, and web service provider can verify SOAP message signature signed with SHA-2 signature algorithm.

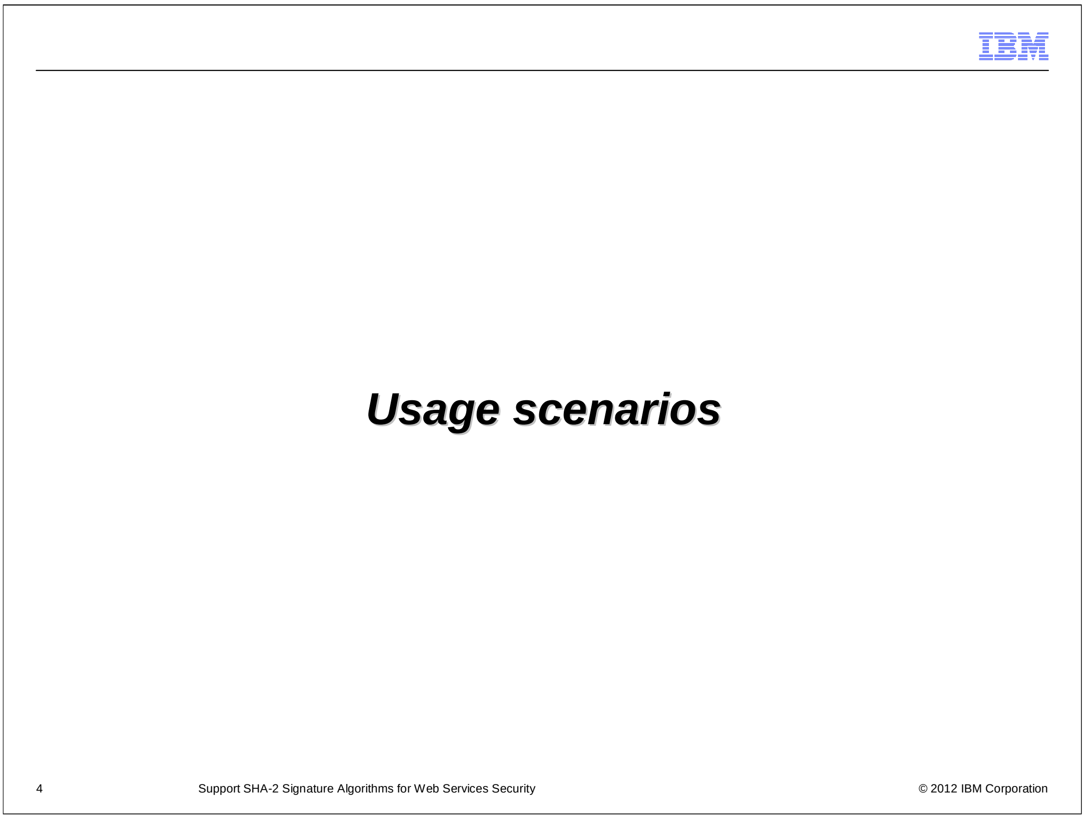


## Support SHA-2 signature algorithms for web services security

- New recommendations from NIST (Special Publication 800-131A) indicate that SHA1 has weaknesses and implementations shall move to SHA-2 for digital signatures by the end of 2013
- Web services security runtime in WebSphere Application Server already supports SHA256 for message digests
- This new function will allow users to configure web services security to use SHA-2 signature algorithms for  digital signatures
- New function is available in both JAX-RPC and JAX-WS programming models
- Following are the signature algorithms that are supported with this function:
  - SHA2WithRSA, SHA3WithRSA, SHA5WithRSA
  - HMACSHA256, HMACSHA384, HMACSHA512
  - SHA2WithDSA

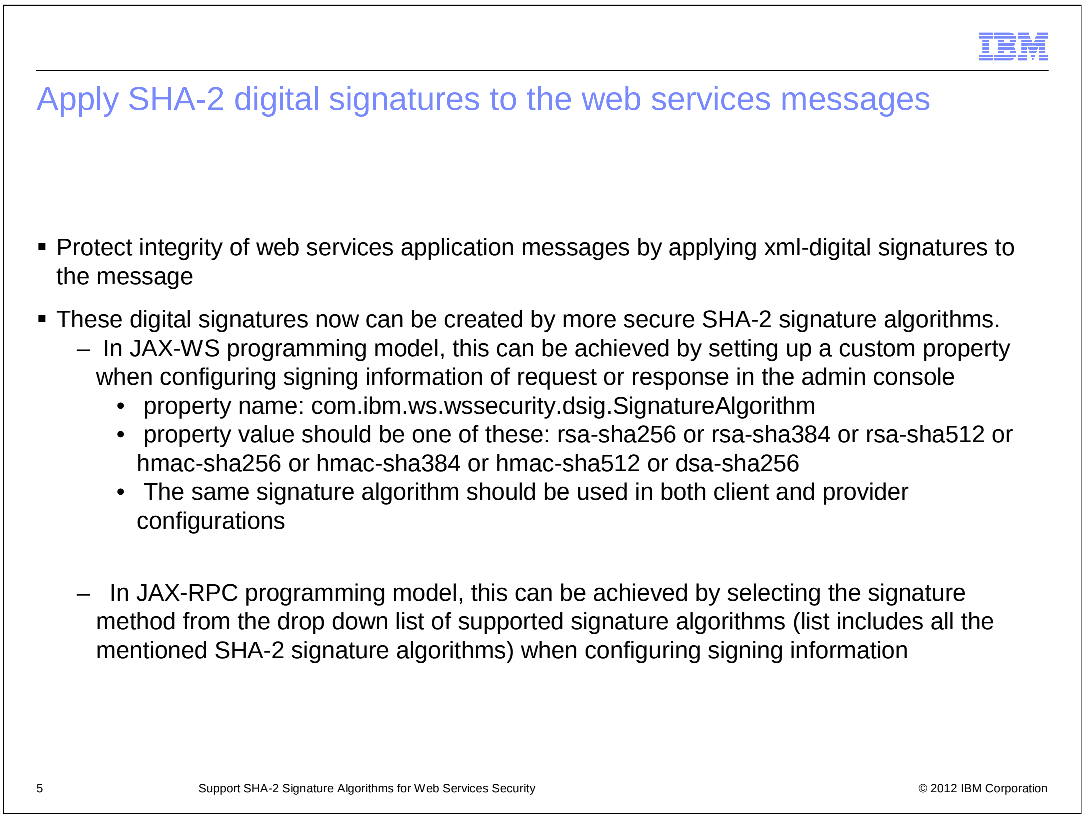
National Institute of Standards and Technology (NIST) originates the series of publications to coordinate the requirements and standards for cryptographic modules. The NIST publication SP800-131 requires longer key lengths, strong digital signature algorithms and cryptographic algorithms. It further requires all implementations move to use the stronger SHA-2 from SHA-1 digital signatures by the end of 2013.

With this new function, web service security will have the capability to create or verify SOAP digital signatures using more secure SHA-2 signature algorithms.



## Usage scenarios

WebSphere application server web service security can be configured to use the more secured SHA-2 signature algorithm  to sign SOAP message, or to verify SOAP signature.

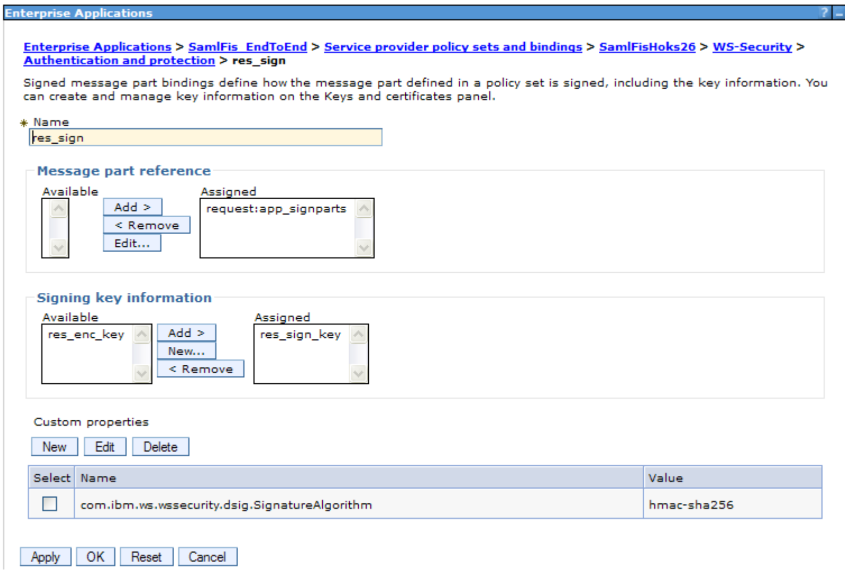


## Apply SHA-2 digital signatures to the web services messages

- Protect integrity of web services application messages by applying xml-digital signatures to the message
- These digital signatures now can be created by more secure SHA-2 signature algorithms.
  - In JAX-WS programming model, this can be achieved by setting up a custom property when configuring signing information of request or response in the admin console
    - property name: com.ibm.ws.wssecurity.dsig.SignatureAlgorithm
    - property value should be one of these: rsa-sha256 or rsa-sha384 or rsa-sha512 or hmac-sha256 or hmac-sha384 or hmac-sha512 or dsa-sha256
    - The same signature algorithm should be used in both client and provider configurations
  - In JAX-RPC programming model, this can be achieved by selecting the signature method from the drop down list of supported signature algorithms (list includes all the mentioned SHA-2 signature algorithms) when configuring signing information

Both JAX-WS web service and JAX-RPC web service support SHA-2 signature algorithms. In JAX-WS, you use custom property com.ibm.ws.wssecurity.dsig.SignatureAlgorithm to the required signature algorithm when configuring signing information. The allowed algorithm values are rsa-sha256, rsa-sha384, rsa-sha512, hmac-sha256, hmac-sha512, hmac-sha384, and dsa-sha256. In JAX-RPC, you can select the desired SHA-2 algorithm from a list available algorithms when configuring signing information.

## JAX-WS signing configuration using sha-2 algorithm



Enterprise Applications

Enterprise Applications > SamlFis_EndToEnd > Service provider policy sets and bindings > SamlFisHoks26 > WS-Security > Authentication and protection > res_sign

Signed message part bindings define how the message part defined in a policy set is signed, including the key information. You can create and manage key information on the Keys and certificates panel.

* Name: res_sign

**Message part reference**

Available: (none)

Assigned: request:app_signparts

**Signing key information**

Available: res_enc_key

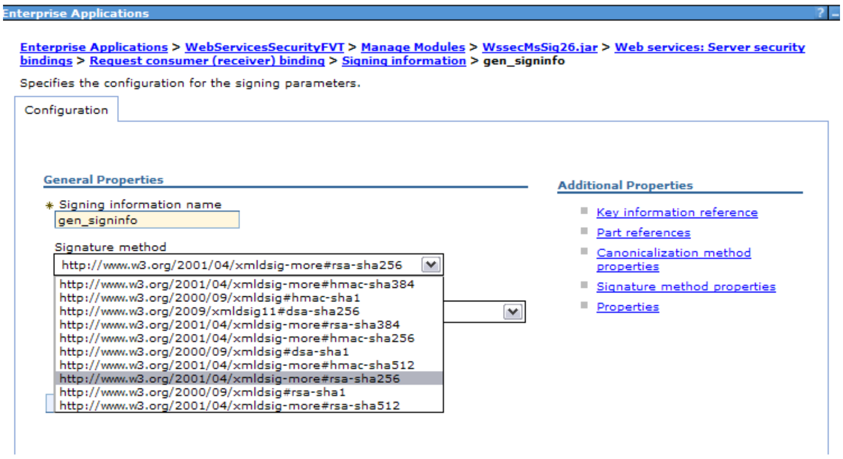
Assigned: res_sign_key

Custom properties

| Select | Name | Value |
|---|---|---|
| □ | com.ibm.ws.wssecurity.dsig.SignatureAlgorithm | hmac-sha256 |

This slide shows an admin console screen capture of JAX-WS configuration and how it is setup to use SHA-2 signature algorithm. The custom property com.ibm.ws.wssecurity.dsig.SignatureAlgorithm indicates which signature algorithm to use.

# JAX-RPC signing configuration



Enterprise Applications > WebServicesSecurityFVT > Manage Modules > WssecMsSig26.jar > Web services: Server security bindings > Request consumer (receiver) binding > Signing information > gen_signinfo

Specifies the configuration for the signing parameters.

**General Properties**

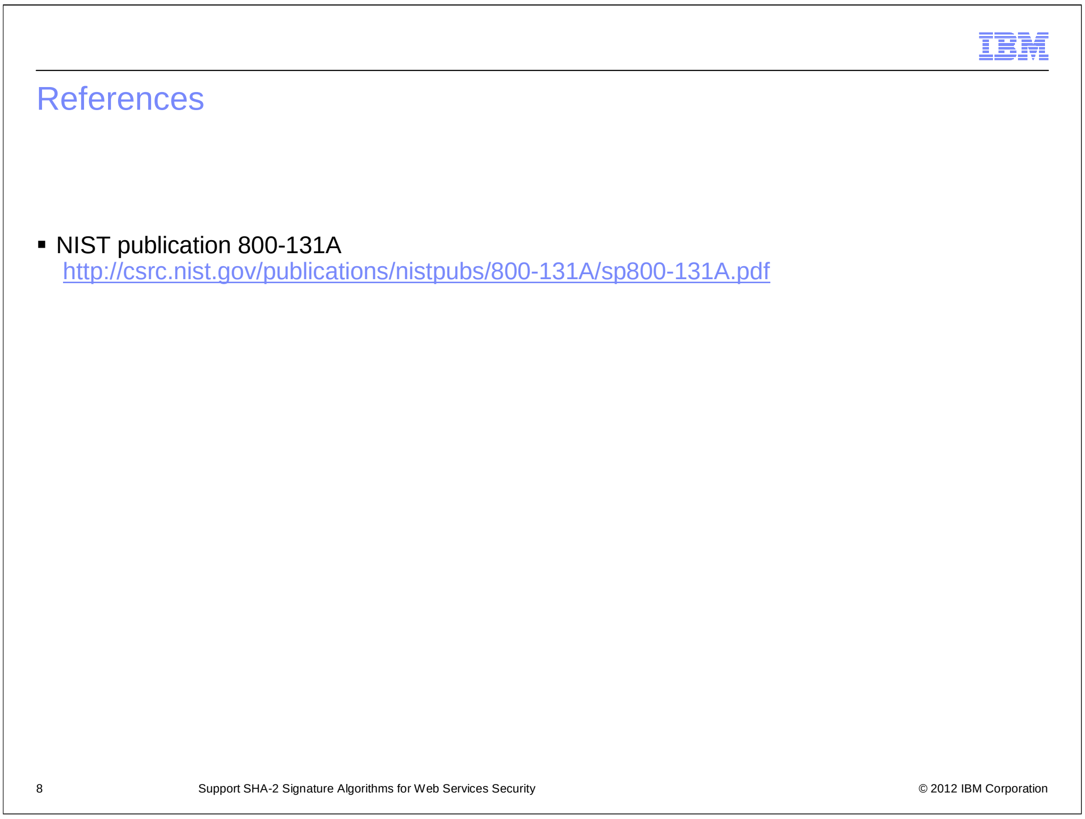
* Signing information name: gen_signinfo

Signature method: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

```
http://www.w3.org/2001/04/xmldsig-more#hmac-sha384
http://www.w3.org/2000/09/xmldsig#hmac-sha1
http://www.w3.org/2009/xmldsig11#dsa-sha256
http://www.w3.org/2001/04/xmldsig-more#rsa-sha384
http://www.w3.org/2001/04/xmldsig-more#hmac-sha256
http://www.w3.org/2000/09/xmldsig#dsa-sha1
http://www.w3.org/2001/04/xmldsig-more#hmac-sha512
http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
http://www.w3.org/2000/09/xmldsig#rsa-sha1
http://www.w3.org/2001/04/xmldsig-more#rsa-sha512
```

Additional Properties
Key information reference
Part references
Canonicalization method properties
Signature method properties
Properties

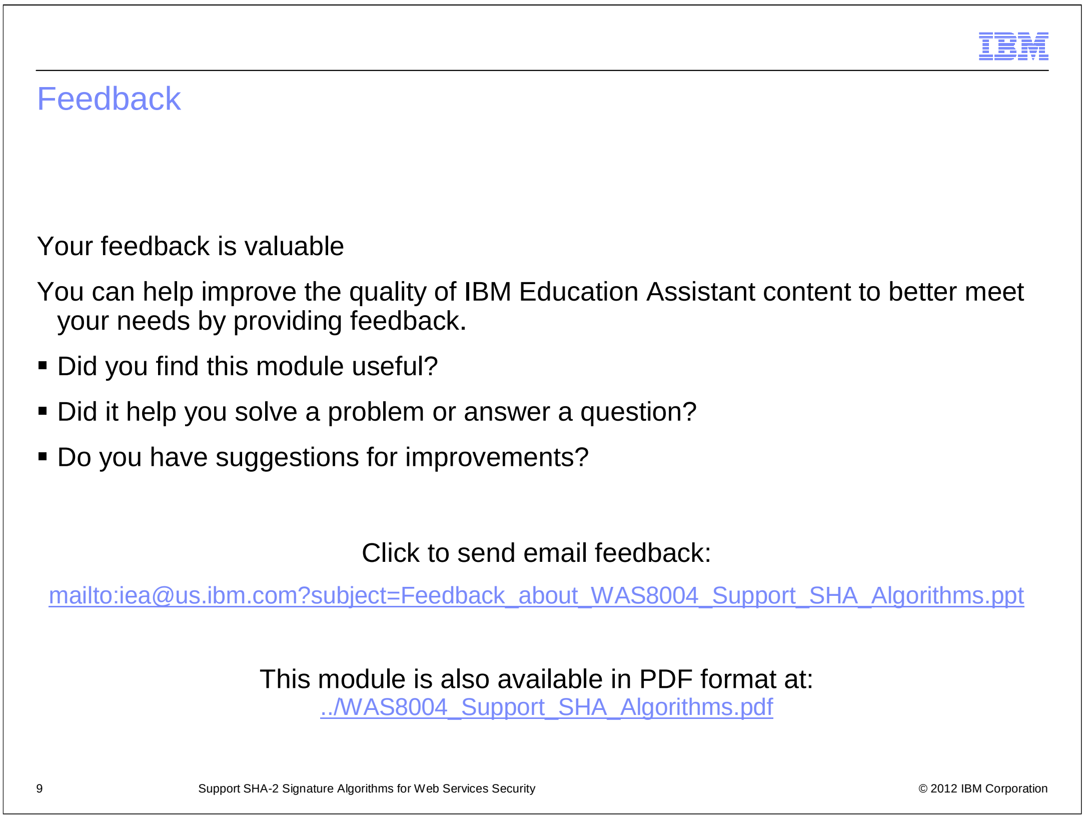
This is a screen capture from JAX-RPC when configuring signing information, and you can choose any available signature from the list.



## References

- NIST publication 800-131A
  http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

This slide contains a reference link.



## Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

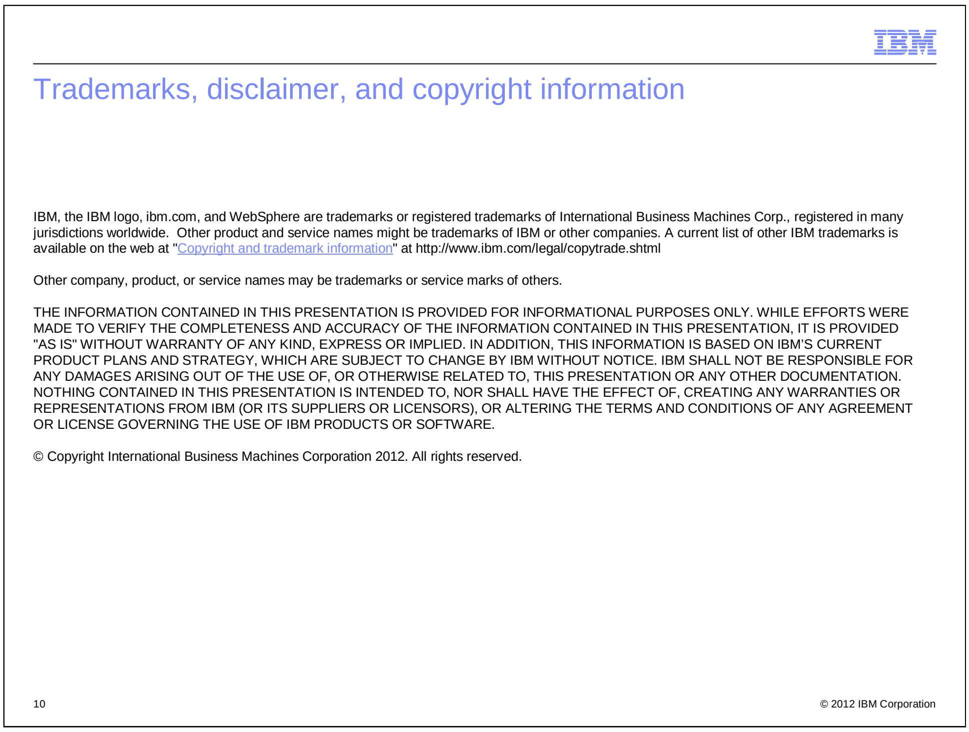
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WAS8004_Support_SHA_Algorithms.ppt

This module is also available in PDF format at:
../WAS8004_Support_SHA_Algorithms.pdf

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



# Trademarks, disclaimer, and copyright information

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.