[MS-WSSEC]:
Web Services:
Security Policy Assertions Format

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft Open Specification Promise or the Community Promise. If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
09/25/2009	0.1	Major	First Release.
11/06/2009	0.1.1	Editorial	Revised and edited the technical content.
12/18/2009	0.1.2	Editorial	Revised and edited the technical content.
01/29/2010	0.1.3	Editorial	Revised and edited the technical content.
03/12/2010	0.1.4	Editorial	Revised and edited the technical content.
04/23/2010	0.1.5	Editorial	Revised and edited the technical content.
06/04/2010	0.1.6	Editorial	Revised and edited the technical content.
07/16/2010	1.0	Major	Significantly changed the technical content.
08/27/2010	1.0	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2010	1.0	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	1.0	No change	No changes to the meaning, language, or formatting of the technical content.
01/07/2011	1.0	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	1.0	No change	No changes to the meaning, language, or formatting of the technical content.
03/25/2011	1.0	No change	No changes to the meaning, language, or formatting of the technical content.
05/06/2011	1.0	No change	No changes to the meaning, language, or formatting of the technical content.
06/17/2011	1.1	Minor	Clarified the meaning of the technical content.
09/23/2011	1.1	No change	No changes to the meaning, language, or formatting of the technical content.
12/16/2011	2.0	Major	Significantly changed the technical content.
03/30/2012	2.0	No change	No changes to the meaning, language, or formatting of the technical content.
07/12/2012	2.0	No change	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	2.0	No change	No changes to the meaning, language, or formatting of the technical content.

Date	Revision History	Revision Class	Comments
01/31/2013	2.0	No change	No changes to the meaning, language, or formatting of the technical content.
08/08/2013	2.0	No change	No changes to the meaning, language, or formatting of the technical content.
11/14/2013	2.0	No change	No changes to the meaning, language, or formatting of the technical content.

Contents

1 Introduction 5
1.1 Glossary 5
1.2 References 5
1.2.1 Normative References 6
1.2.2 Informative References 7
1.3 Overview 7
1.4 Relationship to Protocols and Other Structures 7
1.5 Applicability Statement 8
1.6 Versioning and Localization 8
1.7 Vendor-Extensible Fields 8

2 Structures 9
2.1 mssp:RsaToken 9
2.2 mssp:MustNotSendCancel 9
2.3 mssp:RequireClientCertificate 10
2.4 mssp:SslContextToken 11

3 Structure Examples 12
3.1 mssp:RsaToken policy assertion 12
3.2 mssp:SslContextToken policy assertion 12

4 Security Considerations 13

5 Appendix A: Product Behavior 14

6 Change Tracking 15

7 Index 16

1 Introduction

Web Services Policy 1.2 – Framework (WS-Policy) [WS-Policy] defines a framework for allowing Web services to express their constraints and requirements. Such constraints and requirements are expressed as policy assertions. The Web Services Security Policy Language (WS-SecurityPolicy) [WSSP] defines a set of security policy assertions for use with the [WS-Policy] framework with respect to security features provided in WSS: SOAP Message Security. This document defines additional policy assertions that can be used together with policy assertions defined in [WSSP] to express constraints and requirements that cannot be expressed with just the policy assertions defined in [WSSP].

Sections 1.7 and 2 of this specification are normative and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in RFC 2119. All other sections and examples in this specification are informative.

1.1 Glossary

The following terms are defined in [MS-GLOS]:

.Net Framework

The following terms are specific to this document:

claim: As defined in [WSS] and [WSS1].

policy: As defined in [WSSP].

Policy Assertion: As defined in [WSSP].

initiator: As defined in [WSSP].

token assertion: As defined in [WSSP].

RequestSecurityToken: The SOAP message format as defined by [WSTrust].

security context token: Security token type as defined by [WSSP].

security token: As defined in [WSS] and [WSS1].

Security Token Service (STS): A Web service that issues security tokens. That is, it makes assertions based on evidence that it trusts for consumption by whoever trusts it.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

References to Microsoft Open Specifications documentation do not include a publishing year because links are to the latest version of the documents, which are updated frequently. References to other documents include a publishing year when one is available.

A reference marked "(Archived)" means that the reference document was either retired and is no longer being maintained or was replaced with a new document that provides current implementation details. We archive our documents online [Windows Protocol].

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.rfc-editor.org/rfc/rfc2119.txt

[WMPolicy1.5/Att] Vedamuthu, A., Orchard, D., Hirsch, N., et al., "Web Services Policy 1.5 - Attachment", W3C Recommendation, September 2007, http://www.w3.org/TR/2007/REC-ws-policy-attach-20070904/

[WS-Policy] Siddharth, B., Box, D., Chappell, D., et al., "Web Services Policy 1.2 - Framework (WS-Policy)", April 2006, http://www.w3.org/Submission/2006/SUBM-WS-Policy-20060425/

[WSS] OASIS, "Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)", February 2006, http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[WSS1] Nadalin, A., Kaler, C., Hallam-Baker, P., et al., "Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)", March 2004, http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

[WSSC] OpenNetwork, Layer7, Netegrity, Microsoft, Reactivity, IBM, VeriSign, BEA Systems, Oblix, RSA Security, Ping Identity, Westbridge, Computer Associates, "Web Services Secure Conversation Language (WS-SecureConversation)", February 2005, http://schemas.xmlsoap.org/ws/2005/02/sc

[WSSC1.3] Lawrence, K., Kaler, C., Nadalin, A., et al., "WS-SecureConversation 1.3", March 2007, http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.html

[WSSC1.4] OASIS Standard, "WS-SecureConversation 1.4", February 2009, http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.4/os/ws-secureconversation-1.4-spec-os.doc

[WSSP] Della-Libera, G., Gudgin, M., Hallam-Baker, P., et al., "Web Services Security Policy Language (WS-SecurityPolicy)", July 2005, http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-secpol/ws-secpol.pdf

[WSSP1.2/10.1] OASIS Standard, "WS-SecurityPolicy 1.2 - 10.1 Trust13 Assertion", July 2007, http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.html#_Toc161826576

[WSSP1.3] OASIS Standard, "WS-SecurityPolicy 1.3", February 2009, http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/os/ws-securitypolicy-1.3-spec-os.doc

[WSTrust] IBM, Microsoft, Nortel, VeriSign, "WS-Trust V1.0", February 2005, http://specs.xmlsoap.org/ws/2005/02/trust/WS-Trust.pdf

[WSTrust1.3] Lawrence, K., Kaler, C., Nadalin, A., et al., "WS-Trust 1.3", March 2007, http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html

[WSTrust1.4] OASIS Standard, "WS-Trust 1.4", February 2009, http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.doc

[WSTSPNego] Alexander, J., Gajjala, V., Gavrylyuk, K., et al., "Application Note: Using WS-Trust for Simple and Protected Negotiation Protocol", September 2007, http://schemas.xmlsoap.org/ws/2005/02/trust/spnego/WSTrustForSPNego.pdf

1.2.2 Informative References

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary".

1.3 Overview

[WS-Policy] defines a framework for allowing Web services to express their constraints and requirements. Such constraints and requirements are expressed as policy assertions. The [WSSP] defines a set of security policy assertions for use with the [WS-Policy] framework with respect to security features provided in WSS: SOAP Message Security, [WSS], [WSS1], [WSTrust], [WSTrust1.3], [WSTrust1.4], [WSSC], [WSSC1.3], and [WSSC1.4].

This document defines additional policy assertions that can be used together with policy assertions defined in [WSSP] to express constraints and requirements that cannot be expressed with just the policy assertions defined in [WSSP].

There are two kinds of policy assertions defined in this document. The first kind provides new security token policy assertions that can be used to express requirements for security tokens that are not expressible with policy assertions defined by [WSSP]. The following two policy assertions belong to this category:

- mssp:RsaToken
- mssp:SslContextToken

The second kind of policy assertion is used as a nested policy assertion, providing additional requirements for the parent policy assertion under which it is nested. The following two policy assertions belong to this category:

- mssp:MustNotSendCancel
- mssp:RequireClientCertificate

Some of the policy assertions defined in this document (specifically, mssp:RsaToken, mssp:MustNotSendCancel, and mssp:RequireClientCertificate) predate policy assertions that were subsequently defined by the [WSSP1.2/10.1] and [WSSP1.3] standards. This is indicated, where applicable, in the particular policy assertion description in section 2 in this document.

1.4 Relationship to Protocols and Other Structures

The policy assertions defined in this document are used in conjunction with policy assertions defined in [WSSP] to express security constraints and requirements of a web service with respect to the SOAP messages exchanged between the service and its client.

The policy assertions defined in this document, together with policy assertions defined by [WSSP], describe how the security features provided by [WSS1], [WSS], [WSTrust], [WSTrust1.3], [WSTrust1.4], [WSSC], [WSSC1.3], [WSSC1.4], and [WSTSPNego] should be used to satisfy the security constraints and requirements of the Web service.

1.5 Applicability Statement

The policy assertions defined in this document apply to Web services that wish to express security requirements and constraints for which the policy assertions defined in [WSSP] are not sufficient. Specifically, the following protocol requirements and constraints can be expressed using the policy assertions defined in this document:

- Requirement for an RSA key pair to be provided by the initiator as a security token.
- Requirement for a secure conversation token to be obtained by the initiator using TLS binary negotiation as defined by [WSTSPNego].
- Requirement for an X.509 certificate to be provided by the initiator as part of the TLS binary negotiation, as defined by [WSTSPNego].
- Expressing the fact that the **Security Token Service (STS)** used to obtain the security context token does not support SCT/Cancel RequestSecurityToken messages.

1.6 Versioning and Localization

The policy assertions defined in this document exist in a single version only. They do not have an associated version number, and there are currently no plans to produce another version in the future.

Every [WS-Policy] policy assertion is identified by its fully qualified XML node name (QName), which consists of a namespace URI and a local name parts. The namespace URI used by assertions defined in this document is "http://schemas.microsoft.com/ws/2005/07/securitypolicy", and the corresponding XML namespace prefix used for this namespace is "mssp".

1.7 Vendor-Extensible Fields

The policy assertions defined in this document do not contain any vendor-extensible fields.

2 Structures

2.1 mssp:RsaToken

The mssp:RsaToken policy assertion predates the [WSSP1.2/10.1] standard. It is equivalent to the sp12:KeyValueToken policy assertion when used together with sp12:RsaKeyValue nested assertion. The sp12:KeyValueToken and sp12:RsaKeyValue assertions are defined in [WSSP1.2/10.1] and in [WSSP1.3], section 5.4.11.

This policy assertion MUST NOT be used together with any policy assertions defined by [WSSP1.2/10.1] or [WSSP1.3], and can only be used together with policy assertions defined by [WSSP].

The mssp:RsaToken policy assertion represents a security token assertion that can be used in the same context as any other security token assertion defined in [WSSP], section 6.3.

The mssp:RsaToken policy assertion expresses a requirement for an arbitrary RSA key pair to be used as a security token. Usually the mssp:RsaToken policy assertion is used as a nested policy assertion of the sp:EndorsingSupportingTokens policy assertion, defined in [WSSP], section 9.3, to express a requirement for the initiator to prove possession of an arbitrary RSA key pair by creating a signature using that RSA key pair, covering the primary message signature.

Here is the XML schema definition of the mssp:RsaToken policy assertion element:

```
<xs:schema targetNamespace="http://schemas.microsoft.com/ws/2005/07/securitypolicy"
           elementFormDefault="qualified"
           xmlns:tns="http://schemas.microsoft.com/ws/2005/07/securitypolicy"
           xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">

  <xs:import namespace="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
             schemaLocation="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/ws-
securitypolicy.xsd"/>

  <xs:element name="RsaToken" type="sp:TokenAssertionType"/>

</xs:schema>
```

This assertion does not contain any fields besides those inherited from sp:TokenAssertionType and documented in [WSSP].

2.2 mssp:MustNotSendCancel

The mssp:MustNotSendCancel policy assertion predates the [WSSP1.2/10.1] standard. It is equivalent to the sp12:MustNotSendCancel policy assertion defined as a nested policy assertion for sp12:SpnegoContextToken, and sp12:SecureConversationToken policy assertions in [WSSP1.2/10.1] (section 5.4.5) and [WSSP1.3] (section 5.4.7).

This policy assertion MUST NOT be used together with any policy assertions defined by [WSSP1.2/10.1] or [WSSP1.3] and can only be used together with policy assertions defined by [WSSP].

Presence of the mssp:MustNotSendCancel policy assertion indicates that the STS issuing the security context token for which this assertion is listed as a nested policy assertion does not support SCT/Cancel RequestSecurityToken messages, as defined in [WSSC].

Here is the XML schema definition of the mssp:MustNotSendCancel policy assertion element:

```
<xs:schema targetNamespace="http://schemas.microsoft.com/ws/2005/07/securitypolicy"
           elementFormDefault="qualified"
           xmlns:tns="http://schemas.microsoft.com/ws/2005/07/securitypolicy"
           xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">

  <xs:import namespace="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
             schemaLocation="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/ws-
securitypolicy.xsd"/>

  <xs:element name="MustNotSendCancel" type="sp:QNameAssertionType"/>

</xs:schema>
```

This policy assertion does not define any extra fields.

2.3 mssp:RequireClientCertificate

The mssp:RequireClientCertificate policy assertion predates the [WSSP1.2/10.1] standard. It is equivalent to the sp12:RequireClientCertificate policy assertion defined as a nested assertion for sp12:HttpsToken policy assertion in [WSSP1.2/10.1] and [WSSP1.3], section 5.4.10.

The presence of the mssp:RequireClientCertificate policy assertion indicates that the client MUST provide a X.509 certificate when negotiating the SSL/TLS session.

This assertion is used as a nested policy assertion for mssp:SslContextToken policy assertion defined in section 2.4 of this document.

The XML schema definition for the mssp:RequireClientCertificate policy assertion element is as follows:

```
<xs:schema targetNamespace="http://schemas.microsoft.com/ws/2005/07/securitypolicy"
           elementFormDefault="qualified"
           xmlns:tns="http://schemas.microsoft.com/ws/2005/07/securitypolicy"
           xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">

  <xs:import namespace="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
             schemaLocation="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/ws-
securitypolicy.xsd"/>

  <xs:element name="RequireClientCertificate" type="sp:QNameAssertionType"/>

</xs:schema>
```

This policy assertion does not define any extra fields.

2.4 mssp:SslContextToken

The mssp:SslContextToken policy assertion represents a security token assertion that can be used in the same context as any other security token assertion defined in [WSSP], section 6.3.

The mssp:SslContextToken policy assertion represents a requirement for a security context token obtained by executing a multi-leg RST/RSTR TLSNEGO binary negotiation with the Web service, as defined in [WSTSPNego].

Here is the XML schema definition for the mssp:SslContextToken policy assertion element:

```
<xs:schema targetNamespace="http://schemas.microsoft.com/ws/2005/07/securitypolicy"
           elementFormDefault="qualified"
           xmlns:tns="http://schemas.microsoft.com/ws/2005/07/securitypolicy"
           xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">

  <xs:import namespace="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
             schemaLocation="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/ws-
securitypolicy.xsd"/>

  <xs:element name="SslContextToken" type="sp:TokenAssertionType"/>

</xs:schema>
```

The mssp:SslContextToken policy assertion can be used with the following nested policy assertions:

sp:RequireDerivedKeys: The presence of this nested policy assertion sets the [Derived Keys] properties for this token to "true". These properties are defined in [WSSP], section 6.2.1.

mssp:MustNotSendCancel: The presence of this nested policy assertion indicates that the STS issuing the security context token after successful TLSNEGO binary negotiation does not support SCT/Cancel RequestSecurityTokenMessages. This policy assertion is defined in section 2.2 of this document. mssp:MustNotSendCancel and sp12:MustNotSendCancel nested policy assertions MUST NOT be used at the same time. This nested policy assertion MUST be used when mssp:SslContextToken policy assertion is used together with policy assertions defined in [WSSP].

sp12:MustNotSendCancel: The presence of this nested policy assertion has the same effect as the presence of the mssp:MustNotSendCancel policy assertion described earlier. mssp:MustNotSendCancel and sp12:MustNotSendCancel nested policy assertions MUST NOT be used at the same time. This nested policy assertion MUST be used when mssp:SslContextToken policy assertion is used together with policy assertions defined in [WSSP1.2/10.1] or [WSSP1.3].<1>

mssp:RequireClientCertificate: The presence of this nested policy assertion indicates that the client must provide an X.509 certificate during the TLSNEGO binary negotiation. This policy assertion is defined in section 2.3 of this document.

3 Structure Examples

3.1 mssp:RsaToken policy assertion

The following example shows a policy document utilizing the mssp:RsaToken policy assertion used as a nested policy assertion of the sp:EndorsingSupportingTokens policy assertion.

Example 1: RsaToken policy assertion

```
<wsp:Policy  xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy">  <wsp:ExactlyOne>
<wsp:All>      <sp:EndorsingSupportingTokens>        <wsp:Policy>          <mssp:RsaToken
sp:IncludeToken="
http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient"
/>        </wsp:Policy>      </sp:EndorsingSupportingTokens>    </wsp:All>
</wsp:ExactlyOne></wsp:Policy>
```

3.2 mssp:SslContextToken policy assertion

This shows a policy document utilizing mssp:SslContextToken as a protection token for the sp:SymmetricBinding policy assertion. In addition, the mssp:SslContextToken contains sp:RequireDerivedKeys, mssp:MustNotSendCancel and mssp:RequireClientCertificate nested policy assertions.

Example 2: SslContextToken policy assertion

```
<wsp:Policy  xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:mssp="http://schemas.microsoft.com/ws/2005/07/securitypolicy">  <wsp:ExactlyOne>
<wsp:All>      <sp:SymmetricBinding>        <wsp:Policy>          <sp:ProtectionToken>
<wsp:Policy>              <mssp:SslContextToken               sp:IncludeToken="
http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient"
>               <wsp:Policy>                <sp:RequireDerivedKeys/>
<mssp:MustNotSendCancel/>                <mssp:RequireClientCertificate/>
</wsp:Policy>             </mssp:SslContextToken>           </wsp:Policy>
</sp:ProtectionToken>        </wsp:Policy>      </sp:SymmetricBinding>    </wsp:All>
</wsp:ExactlyOne></wsp:Policy>
```

4 Security Considerations

There are no security considerations besides those described in [WSSP].

5 Appendix A: Product Behavior

This document specifies version-specific details in the Microsoft .NET Framework. For information about which versions of .NET Framework are available in each released Windows product or as supplemental software, see **.NET Framework**.

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Microsoft .NET Framework 3.0
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 4.5

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

<1> Section 2.4: .NET Framework 3.0 is not capable of processing or emitting this nested policy assertion.

6 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

7 Index

A

Applicability 8

C

Change tracking 15

D

Details
- mssp:MustNotSendCancel structure 9
- mssp:RequireClientCertificate structure 10
- mssp:RsaToken structure 9
- mssp:SslContextToken structure 11

E

Examples
- mssp:RsaToken policy assertion 12
- mssp:SslContextToken policy assertion 12

F

Fields - vendor-extensible 8

G

Glossary 5

I

Implementer - security considerations 13
Informative references 7

L

Localization 8

M

mssp:MustNotSendCancel structure 9
mssp:RequireClientCertificate structure 10
mssp:RsaToken policy assertion example 12
mssp:RsaToken structure 9
mssp:SslContextToken policy assertion example 12
mssp:SslContextToken structure 11

N

Normative references 6

P

Product Behavior 14

R

References
- informative 7
- normative 6

Relationship to protocols and other structures 7

S

Security - considerations 13
Structures
- mssp:MustNotSendCancel 9
- mssp:RequireClientCertificate 10
- mssp:RsaToken 9
- mssp:SslContextToken 11
- overview 7

T

Tracking changes 15

V

Vendor-extensible fields 8
Versioning 8