

## 2 **WS-Trust 1.3 Interoperability Profile:** 3 **Username Token Profile**

### 4 **Working Draft 01** 5 **07 January 2008**

#### 6 **Specification URIs:**

7 urn:mace:switch.ch:doc:wst:profile:upt-200801

#### 8 **This Version:**

9 <http://switch.ch/grid/support/documents/wst-utp-wd01.pdf>

#### 10 **Previous Version:**

11 No previous version

#### 12 **Latest Version:**

13 <http://switch.ch/grid/support/documents/>

#### 14 **Editors:**

15 Chad La Joie, SWITCH

#### 16 **Related Work:**

17 This document relates to the WS-Trust Interoperability Profile [WST-Interop] and the Web  
18 Services Security: Username Token Profile [WSS-U].

#### 19 **Abstract:**

20 This profile provides the semantics for the use of a Username security token within messages  
21 that comply with the WS-Trust Interoperability Profile.

#### 22 **Status:**

23 Working Draft

24 **Table of Contents**

25 1 Introduction.....3  
26 1.1 Notation.....3  
27 1.2 Normative References.....4  
28 2 Username Token Processing.....5  
29 2.1 <wsse:UsernameToken> Usage..... 5  
30 2.2 Username Token Claim Processing..... 5  
31 2.3 Username Token Creation.....5  
32 2.4 Delegation Support.....5  
33 3 Examples (informative).....6  
34

# 1 Introduction

This profile provides the semantics for the use of a Username security token within messages that comply with the WS-Trust Interoperability Profile.

## 1.1 Notation

This specification uses normative text to define an extension to the SAML V2.0 metadata specification.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in [RFC 2119]:

...they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions)...

These keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

Listings of XML schemas appear like this.

Example code listings appear like this.

Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

Prefix	XML Namespace	Comments
ds:	<a href="http://www.w3.org/2000/09/xmldsig#">http://www.w3.org/2000/09/xmldsig#</a>	This is the XML Signature namespace [XMLSig].
wsse:	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd</a>	This is the WS-Security extension 1.0 namespace defined in [WSS].
wst:	<a href="http://docs.oasis-open.org/ws-sx/ws-trust/200512">http://docs.oasis-open.org/ws-sx/ws-trust/200512</a>	This is the WS-Trust 1.3 namespace defined in [WS-Trust].
wsu:	<a href="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd</a>	This is the WS-Security utility namespace defined in [WSS].

This specification uses the following typographical conventions in text: <WSTrustElement>, <ns:ForeignElement>, Attribute, **Datatype**, OtherKeyword.

## 1.2 Normative References

- [RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. See <http://www.ietf.org/rfc/rfc2119.txt>.
- [WSI-BSP]** M. McIntosh, et al. *Basic Security Profile Version 1.0*. Web Services Interoperability Organization, 3 March 2007. See <http://www.wsi.org/Profiles/BasicSecurityProfile-1.0.html>.
- [WSS]** A. Nadalin, et al. *Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)*. OASIS, 1 February 2004. See <http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>.

- 67 **[WSS-U]** A. Nadalin, et al. *Web Services Security: Username Token Profile 1.1*. OASIS, 1  
68 February 2006. See <http://www.oasis->  
69 [open.org/committees/download.php/16782/wss-v1.1-spec-os-](http://www.oasis-open.org/committees/download.php/16782/wss-v1.1-spec-os-UsernameTokenProfile.pdf)  
70 [UsernameTokenProfile.pdf](http://www.oasis-open.org/committees/download.php/16782/wss-v1.1-spec-os-UsernameTokenProfile.pdf).
- 71 **[WS-Trust]** A. Nadalin, et al. *WS-Trust 1.3*. OASIS, 19 March 2007. See <http://docs.oasis->  
72 [open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf](http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf).
- 73 **[WST-Interop]** C. La Joie. *WS-Trust Interoperability Profile*. See
- 74 **[XMLSig]** D. Eastlake, et al. *XML-Signature Syntax and Processing*, World Wide Web  
75 Consortium, February 2002. See <http://www.w3.org/TR/xmlsig-core/>.

## 76 2 Username Token Processing

### 77 Token Identification:

78 <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token->  
79 [profile-1.0](http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0)

### 80 2.1 <wsse:UsernameToken> Usage

81 In order to improve the chance of interoperability when using the WSS: UsernameToken Profile [WSS-U]  
82 defined <wsse:UsernameToken> such tokens MUST also conform to the WS-I Basic Security Profile  
83 1.0 [WSI-BSP], section 11.

### 84 2.2 Username Token Claim Processing

85 When a <wsse:UsernameToken> is used as a claim within a request the following steps are taken to  
86 validate the claim:

- 87 ● If a nonce is present the token service SHOULD verify that the nonce has not be received before,  
88 that is that the message has not been replayed
- 89 ● If a creation timestamp is present the token service SHOULD verify the message does not  
90 exceed a service defined freshness threshold
- 91 ● The password MUST be verified against the user database used by the token service
- 92 ● If the request action was a cancellation the account associated with the username token  
93 SHOULD be deactivated or removed if the token service is the authority for the account.

### 94 2.3 Username Token Creation

95 When a token service issues a username token it MUST produce a token that:

- 96 ● Meets the requirements of WS-I Basic Security Profile 1.0 [WSI-BSP], Section 11
- 97 ● Contain exactly one a cryptographically random <wsse:Nonce> of at least 128 bits
- 98 ● Contain exactly one <wsu:Created> timestamp.

### 99 2.4 Delegation Support

100 Delegation of Username tokens is not supported.

### 101 2.5 Security Considerations

102 A message issuer MUST ensure that a Username token is kept confidential. This may be accomplished  
103 by the use of a transport, such as SSL/TLS, that provides confidentiality. Alternatively the token may be  
104 carried, encrypted, within the <wsse:Security> and the encrypted as described [WSS] section 6.5 and  
105 in accordance with the encryption profile in [WST-Interop].

### 106 3 Examples (informative)

107 The following is an example of a Username token profile.

108 Namespace declarations and base64-encoded content are not shown in the example for the sake of  
109 brevity.

```
110 <wsse:Security wsse:Id="X509SecurityToken">  
111   <wsse:UsernameToken>  
112     <wsse:Username>jsmith</wsse:Username>  
113     <wsse:Password>JoesPassword</wsse:Password>  
114     <wsse:Nonce><!-- Base64-encoded content --></wsse:Nonce>  
115     <wsu:Created>1970-01-01T00:00:00</wsu:Created>  
116   </wsse:UsernameToken>  
117 </wsse:Security>
```