[MS-DVRE]:
Device Registration Enrollment Protocol

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
08/08/2013	1.0	New	Released new document.

Contents

1 Introduction

The Device Registration Enrollment Protocol provides a lightweight mechanism for registering personal or corporate-owned devices with a workplace.

Whereas the discovery of information needed to register devices is obtained by use of the Device Registration Discovery Protocol [MS-DVRD], the Device Registration Enrollment Protocol, defined in this specification, makes use of that information to register a device in the device registration service.

Sections 1.8, 2, and 3 of this specification are normative and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in RFC 2119. Sections 1.5 and 1.9 are also normative but cannot contain those terms. All other sections and examples in this specification are informative.

1.1 Glossary

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

ACL
Active Directory
Coordinated Universal Time (UTC)
distinguished name (DN)
globally unique identifier (GUID)
GUID
Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)
SID
SOAP action
SOAP body
SOAP fault
SOAP header
SOAP message
user principal name (UPN)
UTC (Coordinated Universal Time)
WSDL message
WSDL operation

The following terms are specific to this document:

JSON Web token: A type of token that includes a set of claims encoded as a JSON object. For more information, see [IETFDRAFT-JWT].

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. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[IETFDRAFT-JWT] Internet Engineering Task Force (IETF), "JSON Web Token (JWT)", draft-ietf-oauth-json-web-token-08, April 2013, http://tools.ietf.org/html/draft-ietf-oauth-json-web-token-08

[MS-ADA1] Microsoft Corporation, "Active Directory Schema Attributes A-L".

[MS-ADA2] Microsoft Corporation, "Active Directory Schema Attributes M".

[MS-ADA3] Microsoft Corporation, "Active Directory Schema Attributes N-Z".

[MS-ADSC] Microsoft Corporation, "Active Directory Schema Classes".

[MS-DVRD] Microsoft Corporation, "Device Registration Discovery Protocol".

[MS-WSTEP] Microsoft Corporation, "WS-Trust X.509v3 Token Enrollment Extensions".

[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

[RFC2616] Fielding, R., Gettys, J., Mogul, J., et al., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999, http://www.ietf.org/rfc/rfc2616.txt

[RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", RFC 4211, September 2005, http://www.rfc-editor.org/rfc/rfc4211.txt

[RFC5280] Cooper, D., Santesson, S., Farrell, S., et al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008, http://www.ietf.org/rfc/rfc5280.txt

[SOAP1.2-1/2003] Gudgin, M., Hadley, M., Mendelsohn, N., et al., "SOAP Version 1.2 Part 1: Messaging Framework", W3C Recommendation, June 2003, http://www.w3.org/TR/2003/REC-soap12-part1-20030624

[SOAP1.2-2/2003] Gudgin, M., Hadley, M., Mendelsohn, N., et al., "SOAP Version 1.2 Part 2: Adjuncts", W3C Recommendation, June 2003, http://www.w3.org/TR/2003/REC-soap12-part2-20030624

[WSA1.0-WSDLBinding] W3C, "WS-Addressing 1.0 WSDL Binding Namespace", W3C Recommendation, http://www.w3.org/2006/05/addressing/wsdl/

[WSDL] Christensen, E., Curbera, F., Meredith, G., and Weerawarana, S., "Web Services Description Language (WSDL) 1.1", W3C Note, March 2001, http://www.w3.org/TR/2001/NOTE-wsdl-20010315

[WSDLSOAP] Angelov, D., Ballinger, K., Butek, R., et al., "WSDL 1.1 Binding Extension for SOAP 1.2", W3c Member Submission, April 2006, http://www.w3.org/Submission/wsdl11soap12/

[WSFederation] Kaler, C., Nadalin, A., Bajaj, S., et al., "Web Services Federation Language (WS-Federation)", Version 1.1, December 2006, http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf

If you have any trouble finding [WSFederation], please check here.

[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

[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

[XMLNS] Bray, T., Hollander, D., Layman, A., et al., Eds., "Namespaces in XML 1.0 (Third Edition)", W3C Recommendation, December 2009, http://www.w3.org/TR/2009/REC-xml-names-20091208/

[XMLSCHEMA1] Thompson, H.S., Beech, D., Maloney, M., and Mendelsohn, N., Eds., "XML Schema Part 1: Structures", W3C Recommendation, May 2001, http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/

[XMLSCHEMA2] Biron, P.V., and Malhotra, A., Eds., "XML Schema Part 2: Datatypes", W3C Recommendation, May 2001, http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/

1.2.2 Informative References

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

1.3 Overview

The Device Registration Enrollment Protocol provides for issuance of X.509v3 digital certificates, and is intended for use as a lightweight device registration server. The server is known in WS-Trust [WSTrust1.3] terminology as a security token service (STS). The protocol is based loosely on [MS-WSTEP].

This document defines and uses the following term:

Directory Server: Refers to the directory database that will store the device-object record and policy information for the server.

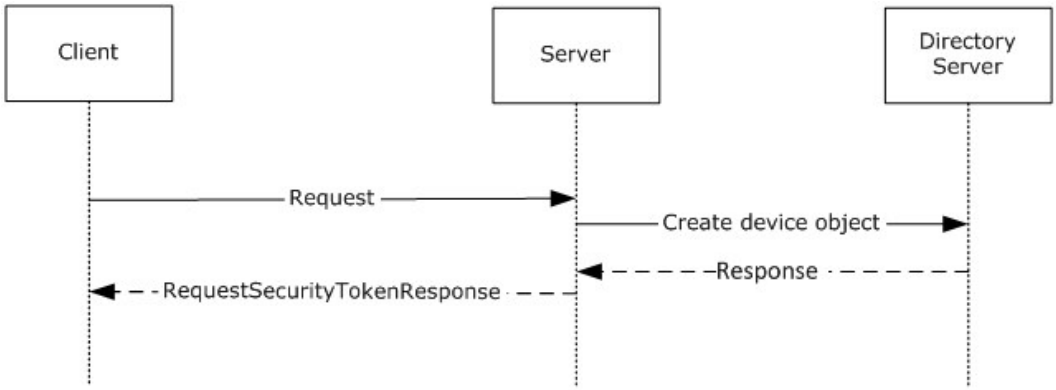

Figure 1: Typical sequence diagram for Device Registration

1.4 Relationship to Other Protocols

The following figure shows the Device Registration Enrollment protocol stack diagram.

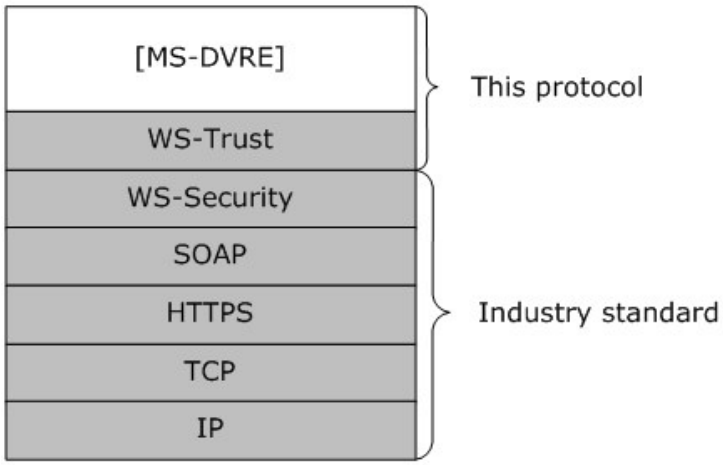

Figure 2: Device Registration Enrollment protocol stack

The Device Registration Enrollment protocol makes use of the **Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)** and SOAP protocols for messaging and security.

1.5 Prerequisites/Preconditions

The Device Registration Enrollment protocol issues X.509v3 certificates that have a corresponding relationship with a device object represented in a directory server. A server implementation of the protocol requires the functionality of a certificate authority and a directory server.

This protocol requires that the following state changes be made to **Active Directory**.

1. Create a single instance of the **ms-DS-Device-Registration-Service-Container** class in the directory.
2. Set the **ms-DS-Registration-Quota** attribute of the **ms-DS-Device-Registration-Service-Container** object to 10.
3. Set the **ms-DS-Maximum-Registration-Inactivity-Period** attribute of the **ms-DS-Device-Registration-Service-Container** object to 90.
4. Set the **ms-DS-IsEnabled** attribute of the **ms-DS-Device-Registration-Service-Container** object to TRUE.
5. Set the **ms-DS-Device-Location** attribute of the **ms-DS-Device-Registration-Service-Container** object to a **distinguished name (DN)** of a container location in the directory.
6. Generate a certificate signing certificate. The certificate and private key MUST be stored in the **ms-DS-Issuer-Certificates** attribute of the **ms-DS-Device-Registration-Service-Container** object. See section 2.3.1.

   The public portion of the certificate MUST be stored in the **ms-DS-Issuer-Certificates-Public** attribute of the **ms-DS-Device-Registration-Service-Container** object. See section 2.3.2.

7. Set the following directory **ACL** entries:

    1. Grant the server read access to the **ms-DS-Device-Registration-Service-Container** object.

    2. Grant the server read/write access to **ms-DS-device** objects.

1.6 Applicability Statement

The Device Registration Enrollment protocol is applicable only for requests for device registration.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

The Device Registration Enrollment protocol does not include any vendor-extensible fields.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

The Device Registration Enrollment protocol operates over the following transports:

- Web Services: SOAP 1.2 ([SOAP1.2-1/2003] and [SOAP1.2-2/2003]) over HTTPS over TCP/IP ([RFC2616])

The protocol MUST operate on the following URI endpoint.

Web service	Location
Enrollment Web Service	https://<server>:<server port>/EnrollmentServer/DeviceEnrollmentWebService.svc

The protocol MUST use the HTTPS transport.

2.2 Common Message Syntax

This section contains common definitions used by this protocol. The syntax of the definitions uses the XML schema as defined in [XMLSCHEMA1] and [XMLSCHEMA2], and the Web Services Description Language as defined in [WSDL].

2.2.1 Namespaces

This specification defines and references various XML namespaces by using the mechanisms specified in [XMLNS]. Although this specification associates a specific XML namespace prefix for each XML namespace that is used, the choice of any particular XML namespace prefix is implementation-specific and not significant for interoperability.

Prefix	NameSpaces URI	Reference
q2	http://schemas.datacontract.org/2004/07/Microsoft.DeviceRegistration	
xsd	http://www.w3.org/2001/XMLSchema	[XMLSCHEMA1]
wsaw	http://www.w3.org/2006/05/addressing/wsdl	[WSA1.0-WSDLBinding]
soap12	http://schemas.xmlsoap.org/wsdl/soap12/	[WSDLSOAP]
tns	http://schemas.microsoft.com/windows/pki/2009/01/enrollment	This specification
wsdl	http://schemas.xmlsoap.org/wsdl/	[WSDL]
q1	http://schemas.microsoft.com/Message	
ac	http://schemas.xmlsoap.org/ws/2006/12/authorization	[WSFederation]
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd	[WSS]
wst	http://docs.oasis-open.org/ws-sx/ws-trust/200512	[WSTrust1.3]

2.2.2 Messages

This specification does not define any common XML schema message definitions.

2.2.3 Elements

This specification does not define any common XML schema element definitions.

2.2.4 Complex Types

This specification does not define any common XML schema complex type definitions.

2.2.5 Simple Types

This specification does not define any common XML schema simple type definitions.

2.2.6 Attributes

This specification does not define any common XML schema attribute definitions.

2.2.7 Groups

This specification does not define any common XML schema group definitions.

2.2.8 Attribute Groups

This specification does not define any common XML schema attribute group definitions.

2.2.9 Common Data Structures

This specification does not define any common XML schema data structures.

2.3 Directory Service Schema Elements

The protocol accesses the following Directory Service schema classes and attributes listed in the following table.

For the syntactic specifications of the following <Class> or <Class><Attribute> pairs, refer to:

Active Directory Domain Services (AD DS) ([MS-ADA1], [MS-ADA2], [MS-ADA3], and [MS-ADSC]).

Class	Attribute
ms-DS-Device	alt-Security-Identities ms-DS-Device-ID ms-DS-Device-OS-Type ms-DS-Device-OS-Version ms-DS-Registered-Users ms-DS-Is-Enabled ms-DS-Approximate-Last-Use-Time-Stamp ms-DS-Registered-Owner ms-DS-Display-Name

Class	Attribute
ms-DS-Device-Registration-Service-Container	ms-DS-Issuer-Certificates ms-DS-Issuer-Certificates-Public ms-DS-Registration-Quota ms-DS-Maximum-Registration-Inactivity-Period ms-DS-Device-Location ms-DS-IsEnabled
user	objectGuid
domain	objectGuid
nTDSDSA	invocationId

2.3.1 ms-DS-Issuer-Certificates

The **ms-DS-Issuer-Certificates** attribute is a multi-valued OCTET_STRING attribute. Each value of the attribute is stored as a Binary blob containing the following formatted data:

"**[time]**:**[binary value of an X.509 certificate]**"

Where **[time]** is timestamp formatted as an integer representing the number of 100-nanosecond intervals that have elapsed since 12:00:00 midnight, January 1, 0001 and **[binary value of an X.509 certificate]** is the contents of an X.509 certificate [RFC5280] stored as an encrypted binary blob.

2.3.2 ms-DS-Issuer-Certificates-Public

The **ms-DS-Issuer-Certificates-Public** attribute is a multi-valued OCTET_STRING attribute. Each value of the attribute is stored as a binary blob containing an X.509 certificate [RFC5280].

2.3.3 alt-Security-Identities

The **alt-Security-Identities** attribute is a multi-valued UNICODE_STRING attribute. The value is formatted as:

X509:<SHA1-TP-PUBKEY>**[thumbprint]**+**[certificate]**

Where **[thumbprint]** is the SHA1 hash of a certificate public key and **[certificate]** is the base64 encoded X.509 certificate [RFC5280].

3 Protocol Details

3.1 IWindowsDeviceEnrollmentService Server Details

The **IWindowsDeviceEnrollmentService** hosts a message endpoint that receives **RequestSecurityToken** messages (section 3.1.4.1). When received, the server processes the client request, creates and signs an X.509 certificate [RFC5280], and then contacts the directory server to create a device object. Upon receiving a response from the directory server, a response is generated, and the server sends either a **RequestSecurityTokenResponse** message (section 3.1.4.1.1.2) or a **SOAP fault**. When the message has been sent to the client, the server returns to the waiting state.

Figure 3: State model for security token service

The items of information that are communicated between the server and the directory server are specified in subsequent sections of this document.

Authentication

The WS-Trust X509v3 Enrollment Protocol Extensions [MS-WSTEP] use the authentication provisions in WS-Security [WSS] to enable the X509v3 Security Token issuer to authenticate the X509v3

Security Token requestor. The following information defines the schema used to express the credential descriptor for each supported credential type.

- Token Authentication

  The token credential is provided in a request message by using the WS-Trust BinarySecurityToken definition as defined in section 3.1.4.1.2.3.

3.1.1 Abstract Data Model

None.

3.1.2 Timers

StaleDeviceCleanup: A periodic timer that is used to remove unused devices. This timer triggers activity at a random time, once every 24 hours.

3.1.3 Initialization

The following initialization steps MUST be performed each time the server service starts:

1. Read the **ms-DS-IsEnabled** attribute of the **ms-DS-Device-Registration-Service-Container** object. If the value is FALSE, the server service MUST shut down.

2. The web service on the server MUST be listening for requests from the client.

3.1.4 Message Processing Events and Sequencing Rules

The following table summarizes the list of all **WSDL operations** as defined by this specification.

WSDL Operation	Description
RequestSecurityToken	The RequestSecurityToken operation is the sole operation in the Device Registration Enrollment Protocol. It provides the mechanism for device registration requests.

3.1.4.1 RequestSecurityToken

The client calls the **RequestSecurityToken** method to register a device.

This operation is specified by the following WSDL.

```
<wsdl:operation name="RequestSecurityToken">
  <wsdl:input
wsaw:Action="http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RST/wstep"
message="tns:IWindowsDeviceEnrollmentService_RequestSecurityToken_InputMessage"/>
  <wsdl:output
wsaw:Action="http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RSTRC/wstep"
message="tns:IWindowsDeviceEnrollmentService_RequestSecurityToken_OutputMessage"/>
  <wsdl:fault
wsaw:Action="http://schemas.microsoft.com/windows/pki/2009/01/enrollment/IWindowsDeviceEnroll
mentService/RequestSecurityTokenWindowsDeviceEnrollmentServiceErrorFault"
name="WindowsDeviceEnrollmentServiceErrorFault"
message="tns:IWindowsDeviceEnrollmentService_RequestSecurityToken_WindowsDeviceEnrollmentServ
iceErrorFault_FaultMessage"/>
</wsdl:operation>
```

The **IWindowsDeviceEnrollmentService_RequestSecurityToken_InputMessage** message consists of a single object definition: the client request. The client request is made by using the acceptable SOAP actions and values as defined in sections section 3.1.4.1.1 and section 3.1.4.1.2.

3.1.4.1.1 Messages

The following table summarizes the set of **WSDL message** definitions that are specific to this operation.

Message	Description
IWindowsDeviceEnrollmentService_RequestSecurityToken_InputMessage	A request to register a device.
IWindowsDeviceEnrollmentService_RequestSecurityToken_OutputMessage	A response containing the signed certificate.
IWindowsDeviceEnrollmentService_RequestSecurityToken_WindowsDeviceEnrollmentServiceErrorFault_FaultMessage	An error message object.

3.1.4.1.1.1 IWindowsDeviceEnrollmentService_RequestSecurityToken_InputMessage Message

A WSDL message containing the request for the **RequestSecurityToken** WSDL operation.

The **SOAP action** value is:

```
http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RST/wstep
```

The **IWindowsDeviceEnrollmentService_RequestSecurityToken_InputMessage** Message contains the elements that are part of a client request to a server.

The following elements MUST be included in the **SOAP header**.

- **wsse:Security:** Defined in section 3.1.4.1.2.2.

  This element MUST be a child of the <s:Header> element.

- **wsse:BinarySecurityToken:** Defined in section 3.1.4.1.2.3. The ValueType attribute MUST be urn:ietf:params:oauth:token-type:jwt. The EncodingType attribute MUST be http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd#base64binary. The <wsse:BinarySecurityToken> element must contain a base64 encoded **JSON Web token** (JWT) [IETFDRAFT-JWT]. The JWT MUST contain the following claims:

Claim	Description
http://schemas.microsoft.com/authorization/claims/PermitDeviceRegistrationClaim.	Whether the security authority has granted permission for the user to register devices.
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	The **user principal name (UPN)** of the user that authenticated to the web service.

This element MUST be a child of the <wsse:Security> element.

The following elements MUST be included in the **SOAP body**.

- **wst:RequestSecurityToken:** Defined in section 3.1.4.1.2.4.

  This element MUST be a child of the <s:Body> element.

- **wst:RequestType:** Defined in section 3.1.4.1.2.5. The <wst:RequestType> element MUST be http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue.

  This element MUST be a child of the <wst:RequestSecurityToken> element.

- **wst:TokenType**: Defined in section 3.1.4.1.2.6. For the X.509 enrollment extension to WS-Trust, the <wst:tokentype> element MUST be http://schemas.microsoft.com/5.0.0.0/ConfigurationManager/Enrollment/DeviceEnrollmentToken .

  This element MUST be a child of the <wst:RequestSecurityToken> element.

- **wsse:BinarySecurityToken:** Defined in section 3.1.4.1.2.3. The ValueType attribute MUST be http://schemas.microsoft.com/windows/pki/2009/01/enrollment#PKCS10. The EncodingType attribute MUST be http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd#base64binary. The <wsse:BinarySecurityToken> element must contain a base64 encoded X.509 Certificate Request [RFC4211]. The Certificate Request MUST use a SHA1 hash type, 2048 bit key, and include the client authentication key usage.

  This element MUST be a child of the <wst:RequestSecurityToken> element.

- **ac:AddtionalContext:** Defined in section 3.1.4.1.2.7. The <ac:AdditionalContext> element MUST contain three <ac:ContextItem> child elements to represent the device type, OS version, and device display name.

  This element MUST be a child of the <wst:RequestSecurityToken> element.

- **ac:ContextItem:** Defined in section 3.1.4.1.2.8. The request MUST contain the following information in <ac:ContextItem> elements as child elements of the <ac:AdditionalContext> element.

Name attribute	Description
The literal string "DeviceType"	The <ac:Value> element contains the device type.

Name attribute	Description
The literal string: "ApplicationVersion"	The <ac:Value> element contains the OS version installed on the device.
The literal string: "DeviceDisplayName"	The <ac:Value> element contains the friendly name of the device.

```
<wsdl:message name="IWindowsDeviceEnrollmentService_RequestSecurityToken_InputMessage">
  <wsdl:part name="messageRequest" type="q1:MessageBody"/>
</wsdl:message>
```

3.1.4.1.1.2 IWindowsDeviceEnrollmentService_RequestSecurityToken_OutputMessage Message

A WSDL message containing the response for the **RequestSecurityToken** WSDL operation.

The SOAP action value is:

```
http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RSTRC/wstep
```

The **IWindowsDeviceEnrollmentService_RequestSecurityToken_OutputMessage** message contains the elements that are part of a server response to a client.

The following elements MUST be included in the SOAP body.

- **wst:RequestSecurityTokenResponseCollection:** Defined in section 3.1.4.1.2.9.

  This element MUST be a child of the <s:Body> element.

- **wst:RequestSecurityTokenResponse**: Defined in section 3.1.4.1.2.10.

  This element MUST be a child of the <wst:RequestSecurityTokenResponseCollection> element.

- **wst:TokenType:** Defined in section 3.1.4.1.2.6. The <wst:TokenType> element MUST be http://schemas.microsoft.com/5.0.0.0/ConfigurationManager/Enrollment/DeviceEnrollmentToken.

  This element MUST be a child of the <wst:RequestSecurityTokenResponse> element.

- **wst:RequestedSecurityToken:** Defined in section 3.1.4.1.2.11.

  This element MUST be a child of the <wst:RequestSecurityTokenResponse> element.

- **wsse:BinarySecurityToken:** Defined in section 3.1.4.1.2.3. The ValueType attribute MUST be http://schemas.microsoft.com/5.0.0.0/ConfigurationManager/Enrollment/DeviceEnrollmentProvisionDoc. The EncodingType attribute MUST be http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd#base64binary. The <wsse:BinarySecurityToken> element MUST contain a base64 encoded XML document formatted as a Provisioning Document (section 3.1.4.1.2.12). The XML document MUST contain an X.509 Certificate [RFC5280].

  This element MUST be a child of the <wst:RequestSecurityToken> element.

- **ac:AdditionalContext:** Defined in section 3.1.4.1.2.7.

This element MUST be a child of the <wst:RequestSecurityTokenResponse> element.

- **ac:ContextItem:** Defined in section 3.1.4.1.2.8. The request MUST provide the following information in <ac:ContextItem> elements as child elements of the <ac:AdditionalContext> element.

Name attribute	Description
The literal string: "UserPrincipalName"	The <ac:Value> element contains the value of the http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn claim in the JWT that was sent to the server (section 3.1.4.1.1.1).

```
<wsdl:message name="IWindowsDeviceEnrollmentService_RequestSecurityToken_OutputMessage">
  <wsdl:part name="RequestSecurityTokenResult" type="q1:MessageBody"/>
</wsdl:message>
```

3.1.4.1.1.3 IWindowsDeviceEnrollmentService_RequestSecurityToken_WindowsDeviceEnrollmentServiceErrorFault_FaultMessage Message

A WSDL message containing a fault for the **RequestSecurityToken** WSDL operation.

The SOAP action value is:

```
http://schemas.microsoft.com/windows/pki/2009/01/enrollment/IWindowsDeviceEnrollmentService/RequestSecurityTokenWindowsDeviceEnrollmentServiceErrorFault
```

The **IWindowsDeviceEnrollmentService_RequestSecurityToken_WindowsDeviceEnrollmentServiceErrorFault_FaultMessage** message contains the SOAP fault associated with an error in the request from the client to the server.

WindowsDeviceEnrollmentServiceError: Defined in section 3.1.4.1.2.1. The object MUST be included in the <s:Detail> element of a SOAP fault.

```
<wsdl:message
name="IWindowsDeviceEnrollmentService_RequestSecurityToken_WindowsDeviceEnrollmentServiceErrorFault_FaultMessage">
  <wsdl:part name="detail" element="tns:WindowsDeviceEnrollmentServiceError"/>
</wsdl:message>
```

3.1.4.1.2 Elements

The following table summarizes the WSDL element definitions that are specific to this operation.

Element	Description
WindowsDeviceEnrollmentServiceError	An object returned by the web service when an error occurs.
wsse:Security	As described in [WSS].
wsse:BinarySecurityToken	As described in [WSS].

Element	Description
wst:RequestSecurityToken	As described in [WSTrust1.3].
wst:RequestType	As described in [WSTrust1.3].
wst:TokenType	As described in [WSTrust1.3].
ac:AdditionalContext	As described in [WSFederation].
ac:ContextItem	As described in [WSFederation].
wst:RequestSecurityTokenResponseCollection	As described in [WSTrust1.3].
wst:RequestSecurityTokenResponse	As described in [WSTrust1.3].
wst:RequestedSecurityToken	As described in [WSTrust1.3].
Provisioning Document	An XML document containing a configuration profile for a mobile device.

3.1.4.1.2.1 WindowsDeviceEnrollmentServiceError

```
<xsd:element name="WindowsDeviceEnrollmentServiceError" nillable="true"
type="q2:WindowsDeviceEnrollmentServiceError"/>
```

3.1.4.1.2.2 wsse:Security

The <wsse:Security> element is defined in [WSS].

3.1.4.1.2.3 wsse:BinarySecurityToken

The <wsse:BinarySecurityToken> element is defined in [WSS].

3.1.4.1.2.4 wst:RequestSecurityToken

The <wst:RequestSecurityToken> element is defined in WS-Trust 1.3 [WSTrust1.3], section 3.1.

3.1.4.1.2.5 wst:RequestType

The <wst:RequestType> element is defined in [WSTrust1.3] section 3.1. It is an instance of a <wst:RequestTypeOpenEnum> object as defined in [WSTrust1.3] XML schema definition (XSD).

3.1.4.1.2.6 wst:TokenType

The <wst:TokenType> element is defined in [WSTrust1.3], section 3.1.

3.1.4.1.2.7 ac:AdditionalContext

The <ac:AdditionalContext> element is defined in [WSFederation]. It is used to provide additional information in a wst:RequestSecurityToken message.

3.1.4.1.2.8 ac:ContextItem

The <ac:ContextItem> element is defined in [WSFederation]. It is a child element of <ac:AdditionalContext> and is used to provide additional information in a wst:RequestSecurityToken message. See sections 3.1.4.1.1.1 and 3.1.4.1.1.2 for additional requirements.

3.1.4.1.2.9 wst:RequestSecurityTokenResponseCollection

The <wst:RequestSecurityTokenResponseCollection> element is defined in [WSTrust1.3], section 3.1.

3.1.4.1.2.10 wst:RequestSecurityTokenResponse

The <wst:RequestSecurityTokenResponse> element is defined in [WSTrust1.3], section 3.1.

3.1.4.1.2.11 wst:RequestedSecurityToken

The <wst:RequestedSecurityToken> element is defined in [WSTrust1.3], section 3.1.

3.1.4.1.2.12 Provisioning Document Schema

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="NewDataSet" xmlns="" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:msdata="urn:schemas-microsoft-com:xml-msdata">
  <xs:element name="characteristic">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="parm" minOccurs="0" maxOccurs="unbounded">
          <xs:complexType>
            <xs:attribute name="name" type="xs:string" />
            <xs:attribute name="value" type="xs:string" />
          </xs:complexType>
        </xs:element>
        <xs:element ref="characteristic" minOccurs="0" maxOccurs="unbounded" />
      </xs:sequence>
      <xs:attribute name="type" type="xs:string" />
    </xs:complexType>
  </xs:element>
  <xs:element name="wap-provisioningdoc">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="characteristic" minOccurs="0" maxOccurs="unbounded" />
      </xs:sequence>
      <xs:attribute name="version" type="xs:string" />
    </xs:complexType>
  </xs:element>
  <xs:element name="NewDataSet" msdata:IsDataSet="true" msdata:UseCurrentLocale="true">
    <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element ref="characteristic" />
        <xs:element ref="wap-provisioningdoc" />
      </xs:choice>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

3.1.4.1.3 Complex Types

The following table summarizes the XML Schema complex type definitions that are specific to this operation.

ComplexType	Description
WindowsDeviceEnrollmentServiceError	An object returned by the web service when an error occurs.

3.1.4.1.3.1 WindowsDeviceEnrollmentServiceError

Namespace: http://schemas.datacontract.org/2004/07/Microsoft.DeviceRegistration

```
<xsd:complexType name="WindowsDeviceEnrollmentServiceError">
  <xsd:sequence>
    <xsd:element minOccurs="0" maxOccurs="1" name="ErrorType" nillable="true"
type="q2:WinDeviceEnrollmentServiceErrorType"/>
    <xsd:element minOccurs="0" maxOccurs="1" name="Message" nillable="true"
type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>
```

ErrorType:

Message:

3.1.4.1.4 Simple Types

The following table summarizes the XML Schema simple type definitions that are specific to this operation.

SimpleType	Description
WinDeviceEnrollmentServiceErrorType	An object returned by the web service when an error occurs.

3.1.4.1.4.1 WinDeviceEnrollmentServiceErrorType

An object returned by the web service when an error occurs.

Namespace: http://schemas.datacontract.org/2004/07/Microsoft.DeviceRegistration

```
<xsd:simpleType name="WinDeviceEnrollmentServiceErrorType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="InvalidParameter"/>
    <xsd:enumeration value="SqlError"/>
    <xsd:enumeration value="CertificateAuthorityError"/>
    <xsd:enumeration value="DirectoryAccountError"/>
    <xsd:enumeration value="AuthenticationError"/>
    <xsd:enumeration value="AuthorizationError"/>
    <xsd:enumeration value="UnknownError"/>
  </xsd:restriction>
</xsd:simpleType>
```

The following table specifies the allowable values for **WinDeviceEnrollmentServiceErrorType:**

Value	Meaning
InvalidParameter	An invalid parameter was sent to the web service.
SqlError	An error occurred with the database.
CertificateAuthorityError	An error occurred with the Certificate Authority.
DirectoryAccountError	An error occurred with the Directory Service.
AuthenticationError	An error occurred while authenticating the user.
AuthorizationError	An error occurred while authorizing the user.
UnknownError	An unknown error occurred.

3.1.4.2 Processing Rules

An incoming **SOAP message** MUST be processed to evaluate the SOAP actions and authentication information.

If the user has authenticated successfully by using the provided authentication information, message processing MUST continue. If the authentication fails, the server MUST respond with a SOAP fault.

If any other SOAP action is defined, the server MUST respond with a SOAP fault.

3.1.4.2.1 New Request Processing

For this type of message, a server has syntax constraints on the request message.

1. The server MUST check for the http://schemas.microsoft.com/authorization/claims/PermitDeviceRegistrationClaim claim in the JWT. If the claim is not present, or if the value of this claim is not TRUE, the server MUST respond with a SOAP fault.

2. The server MUST query for all **ms-DS-Device** objects whose **ms-DS-RegisteredUsers** attribute contains the **SID** of the authenticating user.

   The server MUST read the integer value of the **ms-DS-Registration-Quota** attribute of the **ms-DS-Device-Registration-Service-Container** object stored on the directory server.

   If the value of the **ms-DS-Registration-Quota** attribute is not zero and the total count of device objects that are registered to the user is greater than the integer stored in the **ms-DS-Registration-Quota** attribute, the server MUST respond with a SOAP fault.

3. The server MUST add the following OIDs and values to the X.509 Certificate Request [RFC4211] contained in the <wsse:BinarySecurityToken> element in the SOAP body of the client request.

OID	Value
1.2.840.113556.1.5.284.2	The server MUST generate a **globally unique identifier (GUID)** and include it as the value.
1.2.840.113556.1.5.284.3	The objectGuid of the user object ([MS-ADSC] section 2.263) on the directory server that corresponds to the authenticating user.

OID	Value
1.2.840.113556.1.5.284.4	The objectGuid of the domain object ([MS-ADSC] section 2.41) on the directory server.
1.2.840.113556.1.5.284.1	The invocationId ([MS-ADA1] section 2.314) of the nTDSDSA object for the directory server.

4. The server MUST sign the request by using the issuer certificate stored in the **ms-DS-Issuer-Certificates** attribute of the **ms-DS-Device-Registration-Service-Container** object with the most recent timestamp (see section 2.3.1). The server MUST use SHA256 as the signature algorithm.

5. The server MUST send a request to the directory server to create a device record as an instance of the **ms-DS-Device** class as a child of the container specified in the **ms-DS-Device-Location** attribute of the **ms-DS-Device-Registration-Service-Container** object.

   The device record MUST contain:

   - The **GUID** generated by the server in step 3, stored as the **ms-DS-Device-ID** attribute.
   - The SHA1 hash of the certificate thumbprint plus certificate public key, stored as the **alt-Security-Identities** attribute.
   - The device type that corresponds to the device type sent in the request (section 3.1.4.1.1.1), stored as the **ms-DS-Device-OS-Type** attribute.
   - The device operating system version that corresponds to the device operating system sent in the request (section 3.1.4.1.1.1), stored as the **ms-DS-Device-OS-Version** attribute.
   - The SID of the user account that authenticated to the web service, stored as the **ms-DS-Registered-Users** attribute.
   - The SID of the user account that authenticated to the web service, stored as the **ms-DS-Registered-Owner** attribute.
   - Set the **ms-DS-Is-Enabled** attribute to true.
   - The friendly name of the device that corresponds to the display name sent in the request (section 3.1.4.1.1.1), stored as the **ms-DS-Display-Name** attribute.

6. The server MUST send a SOAP response to the client. See section 3.1.4.1.1.2 for details on the response.

3.1.5 Timer Events

StaleDeviceCleanup: (section 3.1.2)

If the integer value of the **ms-DS-Maximum-Registration-Inactivity-Period** attribute of the **ms-DS-Device-Registration-Service-Container** is zero, the server MUST stop processing and MUST NOT delete any **ms-DS-Device** objects from the directory.

Otherwise, the server MUST query the directory for all **ms-DS-Device** objects. For each **ms-DS-Device** object, the server MUST calculate the time difference (as a count of days) between the local server **Coordinated Universal Time (UTC)** and the time stored in the **ms-DS-Approximate-Last-Use-Time-Stamp** attribute of the **ms-DS-Device** object.

If the count (as days) is greater than the integer value of the **ms-DS-Maximum-Registration-Inactivity-Period** attribute of the **ms-DS-Device-Registration-Service-Container** and the local server **UTC** time is greater than the time stored in the **ms-DS-Approximate-Last-Use-Time-Stamp** attribute of the **ms-DS-Device** object, the server MUST delete the **ms-DS-Device** object.

3.1.6 Other Local Events

None.

4 Protocol Examples

In the following message sequence, the token authentication headers have been included in the message sequences for clarity.

4.1 RequestSecurityToken Request/Response Message Sequence

4.1.1 Client RequestSecurityToken Message

```
<s:Envelope
  xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://www.w3.org/2005/08/addressing"
  xmlns:u="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd"
  xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd"
  xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
  xmlns:ac="http://schemas.xmlsoap.org/ws/2006/12/authorization">
  <s:Header>
    <a:Action

s:mustUnderstand="1">http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RST/wstep
    </a:Action>
    <a:MessageID>
      urn:uuid:0d5a1441-5891-453b-becf-a2e5f6ea3749
    </a:MessageID>
    <a:ReplyTo>
      <a:Address>
        http://www.w3.org/2005/08/addressing/anonymous
      </a:Address>
    </a:ReplyTo>
    <a:To
s:mustUnderstand="1">https://sts.contoso.com/EnrollmentServer/DeviceEnrollmentWebService.svc
    </a:To>
    <wsse:Security
      s:mustUnderstand="1">
      <wsse:BinarySecurityToken
        ValueType="urn:ietf:params:oauth:token-type:jwt"
        EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary">
        ZXlKMGVYQWlPaUpLVjFRaUxDSmhiR2NpT2lKU1V6STFOaUlzSW5nM
        WRDSTZJblpSZW1KbFozRnJTa3RtVFVkVlZVeENTRFp6UkY4emMyUm
        haeUo5LmV5SmhkV1FpT2lKMWNtNDZiWE10WkhKek9uTjBjeTVqYjI
        1MGIzTnZMbU52YlNJc0ltbHpjeUk2SW1oMGRIQTZMeTl6ZEhNdVky
        OXVkRzl6Ynk1amIyMHZZV1JtY3k5elpYSjJhV05sY3k5MGNuVnpkQ
        0lzSW01aVppSTZNVE0yTmpNeE56Z3pNeXdpWlhod0lqb3hNelkyTX
        pJeE5ETXpMQ0pxZEdraU9pSmZOakF6T1RKa01EZ3RPR1psT0MwMFk
        ySmlMV0U1TTJNdE1HVXhPRFk1TW1VelptTmhMVEpCTmpreFJVVkNP
        REE1TlVZeFFUUTVOa0ZHUXpJMU56VTJRalV4UWtZMklpd2lkWEJ1S
        WpvaVpHRnVRR052Ym5SdmMyOHVZMjl0SWl3aVlYVjBhR2x1YzNSaG
        JuUWlPaUl5TURFekxUQTBMVEU0VkRJd09qUXpPalV6TGpJMU9Gb2l
        MQ0poZFhSb2JXVjBhRzlrSWpwYkltaDBkSEE2THk5elkyaGxiV0Z6
        TG0xcFkzSnZjMjltZEM1amIyMHZkM012TWpBd09DOHdOaTlwWkdWd
        WRHbDBlUzloZFhSb1pXNTBhV05oZEdsdmJtMWxkR2h2WkM5d1lYTn
        pkMjl5WkNJc0luVnlianB2WVhOcGN6cHVZVzFsY3pwMFl6cFRRVTF
        NT2pJdU1EcGhZenBqYkdGemMyVnpPbEJoYzNOM2IzSmtVSEp2ZEdW
        amRHVmtWSEpoYm5Od2IzSjBJbDBzSW5CeWFXMWhjbmxuY205MWNIT
        nBaQ0k2SWxNdE1TMDFMVEl4TFRJek56Z3lOemN5TkRZdE1qWTRNak
```

```
          EzTkRNeE9TMDBNelUwTnpReE1UVXROVEV6SWl3aVozSnZkWEJ6YVd
          RaU9sc2lVeTB4TFRVdE1qRXRNak0zT0RJM056STBOaTB5TmpneU1E
          YzBNekU1TFRRek5UUTNOREV4TlMwMU1UTWlMQ0pUTFRFdE1TMHdJa
          XdpVXkweExUVXRNekl0TlRRMUlpd2lVeTB4TFRVdE1pSXNJbE10TV
          MwMUxURXhJaXdpVXkweExUVXRNVFVpWFN3aWNISnBiV0Z5ZVhOcFp
          DSTZJbE10TVMwMUxUSXhMVEl6TnpneU56Y3lORFl0TWpZNE1qQTNO
          RE14T1MwME16VTBOelF4TVRVdE1URXdOU0lzSW01aGJXVWlPaUpYU
          lVOUFRsUlBVMDljWEdSaGJpSXNJbmRwYm1GalkyOTFiblJ1WVcxbE
          lqb2lWMFZEVDA1VVQxTlBYRnhrWVc0aUxDSm9kSFJ3T2k4dmMyTm9
          aVzFoY3k1dGFXTnliM052Wm5RdVkyOXRMM2R6THpJd01USXZNVEl2
          WTJ4aGFXMXpMMkZrWkdsMGFXOXVZV3hoZFhSb2RtVnlhV1pwWTJGM
          GFXOXViV1YwYUc5a2N5STZJbWgwZEhBNkx5OXpZMmhsYldGekxtMX
          BZM0p2YzI5bWRDNWpiMjB2ZDNNdk1qQXdPQzh3Tmk5cFpHVnVkR2w
          wZVM5aGRYUm9aVzUwYVdOaGRHbHZibTFsZEdodlpDOXdZWE56ZDI5
          eVpDSXNJbWgwZEhBNkx5OXpZMmhsYldGekxtMXBZM0p2YzI5bWRDN
          WpiMjB2ZDNNdk1qQXhNaTh4TWk5amJHRnBiWE12WVdSa2FYUnBiMj
          VoYkdGMWRHaDJaWEpwWm1sallYUnBiMjUxYzJWa0lqb2labUZzYzJ
          VaUxDSmxibVJ3YjJsdWRIQmhkR2dpT2lJdllXUm1jeTl2WVhWMGFE
          SXZkRzlyWlc0aUxDSmhjSEJwWkdWdWRHbG1hV1Z5SWpvaWJYTXRZW
          EJ3T2k4dmQybHVaRzkzY3k1cGJXMWxjbk5wZG1WamIyNTBjbTlzY0
          dGdVpXd3ZJaXdpYUhSMGNEb3ZMM05qYUdWdFlYTXViV2xqY205emI
          yWjBMbU52YlM5aGRYUm9iM0pwZW1GMGFXOXVMMk5zWVdsdGN5OVFa
          WEp0YVhSRVpYWnBZMlZTWldkcGMzUnlZWFJwYjI0aU9pSjBjblZsS
          W4wLmhTem9VVllrVXZ6cjhsX19PeXA4RFdEZi1SOUhHZ3UySG5ndG
          Jnb1Z6ang0a01jMTZLWjNLZzhlM0hYLVRvWk9jZ0VoLXZqYzljY0t
          KMXNYYWZLLVVVc1FGZXV4bDNCSzNFbVJmSFVyXy00MTY3M0RIT1dM
          cTNTXzVWd3JhU3NnVXN4OWtqU01EV3MwcGl1WGZURHhLZzc5T2UwR
          i1HRVNCcm5UQk5GZjdVZ3VKRTVaSGpRenJtTEh2bElSVzJ4dTY3ZT
          loWjZhY1VyeEF6azhmSzhiTS1heGlaZWFnX0RxbTRQSExEMnU2ekd
          BeFlRQmQyNWR3ZmZ4Wk84bkRZajRxVjJiOEFzZjZSMUVWbnBxYWEw
          eXhCTENHcDRuV3NJazJBUW8xaWNIMWoxbEYtc2NVMmJpNU1VcFZhT
          1gxRHJ0RnNyTW1RWUtjWno4U2NJRzRqcFhWZw==
        </wsse:BinarySecurityToken>
      </wsse:Security>
    </s:Header>
    <s:Body>
      <wst:RequestSecurityToken>
        <wst:TokenType>

  http://schemas.microsoft.com/5.0.0.0/ConfigurationManager/Enrollment/DeviceEnrollmentToken
        </wst:TokenType>
        <wst:RequestType>
          http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
        </wst:RequestType>
        <wsse:BinarySecurityToken
          ValueType="http://schemas.microsoft.com/windows/pki/2009/01/enrollment#PKCS10"
          EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
  secext-1.0.xsd#base64binary">
          MIICcTCCAV0CAQAwMDEuMCwGA1UEAxMlQjFDNDNDRDAtMTYyNC0
          1RkJCLThFNTQtMzRDRjE3REZEM0ExADCCASIwDQYJKoZIhvcNAQ
          EBBQADggEPADCCAQoCggEBALrqvyhxKTchE5I5L/dFjnjG25ary
          zFmYJ0JJb6ZvaZeueaZKFAJyCGZE1xq0SwHYK9rTvXWSibF6mXW
          w6PJ6Zyd2LEjzgQBGd7iU+vtbwRy7bmYgJEMCILbdpabrYYg/IQ
          RBQpUIe/SxnwKi0RdID2N0T6IwktJjCWJeRI6xr3Cj74MU9wrrM
          SJ3NKaf3eD6iwsEYsU0sEe2ijsiz0Px+Ajmct9Ukq9VLmk34PIK
          EX5RzRYanfshEbr7U7GP9gZKZyIm9kfZjRK057LDuYCKNNzV2hF
          dxkT81PYvnmoYLCeNpYNSJTR/GfYYMkTT3EZVboxN8oTAXQLwfq
          UKfYRNvMCAwEAAaAAMAkGBSsOAwIdBQADggEBAC3JnACsgu3z4r
          fij+Ggxw6wgFzS8gJPkPU4rnylGwICGVnYZIEM/Ny5RsKVZglwY
```

```
        ZIkz4/UumG7NfdKKOqLeFtS3TQMagqdNqv8ehy7BmNglo5HkHrS
        tJi1hsTzhPXtfBgZxDiA5MJUDiZyOfbJSlZckVXyKkyKCbJ1Avm
        ZXIWt10mYvIBzFHVpE5KaZU1sPI/M3td1XYXSgO3kgYvB7jBKUI
        WNjnMPxvPYOjYp0OUiTNtpLozjd1MuCXth9is2OA21t7INKeVzP
        bE01TTcD5JfRQtj9jtk1PNdqd3cp1FgazrbidVjzlqBcEHUndnD
        7WJ2S0QbmscESftupf4nAic=
      </wsse:BinarySecurityToken>
      <ac:AdditionalContext xmlns="http://schemas.xmlsoap.org/ws/2006/12/authorization">
        <ac:ContextItem Name="DeviceType">
          <ac:Value>Windows</ac:Value>
        </ac:ContextItem>
        <ac:ContextItem Name="ApplicationVersion">
          <ac:Value>6.2.9200.0</ac:Value>
        </ac:ContextItem>
        <ac:ContextItem Name="DeviceDisplayName">
          <ac:Value>WEClient.contoso.com</ac:Value>
        </ac:ContextItem>
      </ac:AdditionalContext>
    </wst:RequestSecurityToken>
  </s:Body>
</s:Envelope>
```

4.1.2 Server RequestSecurityToken Response

```
<s:Envelope
  xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">
      http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RSTRC/wstep
    </a:Action>
    <ActivityId
      CorrelationId="0e09fc40-373c-41ee-933a-0e085270a081"
      xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">
      8cca3c03-1ef1-4ecc-83cd-3201fd775596
    </ActivityId>
    <a:RelatesTo>
      urn:uuid:0d5a1441-5891-453b-becf-a2e5f6ea3749
    </a:RelatesTo>
  </s:Header>
  <s:Body>
    <RequestSecurityTokenResponseCollection xmlns="http://docs.oasis-open.org/ws-sx/ws-
trust/200512">
      <RequestSecurityTokenResponse>
        <TokenType>

http://schemas.microsoft.com/5.0.0.0/ConfigurationManager/Enrollment/DeviceEnrollmentToken
        </TokenType>
        <RequestedSecurityToken>
          <BinarySecurityToken
ValueType="http://schemas.microsoft.com/5.0.0.0/ConfigurationManager/Enrollment/DeviceEnrollm
entProvisionDoc"
            EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd#base64binary"
            xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
            PHdhcC1wcm92aXNpb25pbmdkb2MgdmVyc2lvbj0iMS4xIj4
            NCiAgPGNoYXJhY3RlcmlzdGljIHR5cGU9IkNlcnRpZmljYX
```

```
              RlU3RvcmUiPg0KICAgIDxjaGFyYWN0ZXJpc3RpYyB0eXBlP
              SJNeSI+DQogICAgICA8Y2hhcmFjdGVyaXN0aWMgdHlwZT0i
              VXNlciI+DQogICAgICAgIDxjaGFyYWN0ZXJpc3RpYyB0eXB
              lPSJDQjIxMUMxMjQ5MjI5MEU5OUU5OTczOTg5REY3NDk1QT
              AwMzIwMTc3Ij4NCiAgICAgICAgICA8cGFybSBuYW1lPSJFb
              mNvZGVkQ2VydGlmaWNhdGUiIHZhbHVlPSJNSUlFUWpDQ0F5
              NmdBd0lCQWdJUXFWVnRnNEV4MHJaT3o4UkU0MlVqaGpBSkJ
              nVXJEZ01DSFFVQU1JR01NWUdKTUJFR0NnbVNKb21UOGl4a0
              FSa1dBMk52YlRBUkJnb0praWFKay9Jc1pBRVpGZ056ZEhNd
              0ZRWUtDWkltaVpQeUxHUUJHUllIWTI5dWRHOXpiekFkQmdO
              VkJBTVRGazFUTFU5eVoyRnVhWHBoZEdsdmJpMUJZMk5sYzN
              Nd0t3WURWUVFMRXlSak1URTBaVFF5T0MwMU1tVTJMVFJtWk
              RJdE9EVmpNQzFsT0RnNU5ERTJZVE5pTWpVd0hoY05NVE13T
              kRFNE1qQXpPRFUwV2hjTk1qTXdOREUyTWpBME16VTBXakF2
              TVMwd0t3WURWUVFERXlReE1EaGhOVE0xTVMxbU9EbGpMVFE
              yTldFdE9UaGpaUzA0TldZMFpXUXhNekppWXprd2dnRWlNQT
              BHQ1NxR1NJYjNEUUVCQVFBQUE0SUJEd0F3Z2dFS0FvSUJBU
              UM2NnI4b2NTazNJUk9TT1MvM1JZNTR4dHVXcThzeFptQ2RD
              U1crbWIybVhybm1tU2hRQ2NnaG1STmNhdEVzQjJDdmEwNzE
              xa29teGVwbDFzT2p5ZW1jbmRpeEk4NEVBUm5lNGxQcjdXOE
              VjdTI1bUlDUkRBaUMyM2FXbTYyR0lQeUVFUVVLVkNIdjBzW
              jhDb3RFWFNBOWpkRStpTUpMU1l3bGlYa1NPc2E5d28rK0RG
              UGNLNnpFaWR6U21uOTNnK29zTEJHTEZOTEJIdG9vN0lzOUQ
              4ZmdJNW5MZlZKS3ZWUzVwTitEeUNoRitVYzBXR3AzN0lSRz
              YrMU94ai9ZR1NtY2lKdlpIMlkwU3RPZXl3N21BaWpUYzFkb
              1JYY1pFL05UMkw1NXFHQ3duamFXRFVpVTBmeG4yR0RKRTA5
              eEdWVzZNVGZLRXdGMEM4SDZsQ24yRVRiekFnTUJBQUdCRVF
              CKzB0SXJ5dEZ2UlpLT1IzT3V1d1ZSZ2hFQVVWT0tFSno0V2
              thWXpvWDA3Uk1yeWFPQjNUQ0IyakFNQmdOVkhSTUJBZjhFQ
              WpBQU1Cd0dDQ3FHU0liM0ZBVUdCQkJxcldQMUNsZTJUcWRD
              b05ZS3lXNThNQndHQ0NxR1NJYjNGQVVDQkJENHBwWUxocXN
              LUTVqenZaUEtoZUlITUJ3R0NDcUdTSWIzRkFVRUJCQlJVNG
              9RblBoYVJwak9oZlR0RXl2Sk1Cd0dDQ3FHU0liM0ZBVUZCQ
              kFxb3pVZWdtaVdRWVlveitvcTd3TDlNQllHQTFVZEpRRUIv
              d1FNTUFvR0NDc0dBUVVGQndNQ01Cd0dDQ3FHU0liM0ZBVUh
              CQkRjcnFwTkoxR1hTYmdsbEcyRHNxeG1NQndHQ0NxR1NJYj
              NGQVVLQkJEelFSZzVXcjE3UnBWY0hVdTEzcWVHTUFrR0JTc
              09Bd0lkQlFBRGdnRUJBSXAxTTh6bE5CSytVRnNYbzNZTDhB
              eDNSSU9ZcHg1Z1JMdnZhSXZUOWdZUUdiU25NZWozR0N1cWl
              xVHMyc1h0b2Rnb2J5Y1lVeElxTjcxcXgvYmJEbW9iMHpFeE
              dOY3QzNFNaUGkrNVE4V3RhNUJpaFA2QTJKMHk5cUdDam5sZ
              kk2dW1TUC9EQnhsUEg3REVkVzI4VjhJaFBIK3F3Z1Bla0NI
              VzVUVU8ycGdXc0wyaDllT2JmMit1YVI1cTQ5Nk1xR05NQUd
              SVDF0WFNqZUdKZGxhUS93aldldkhISWo3N09jTlJkZXhoN0
              1YalpVNThEMngvdmdVMWY1TmRzdzViYmZ5cCsrTEZOUGZjc
              FY3Q3VqSEU0TEk5T01NcHpCS0x4Q200cGdLS01DVnJLdjk5
              RUZWbFB3STc4RFlZSjhnRUhEbU4rbDRtRk1talcrWUM5NDN
              2Qy9NPSIgLz4NCiAgICAgICAgPC9jaGFyYWN0ZXJpc3RpYz
              4NCiAgICAgIDwvY2hhcmFjdGVyaXN0aWM+DQogICAgPC9ja
              GFyYWN0ZXJpc3RpYz4NCiAgPC9jaGFyYWN0ZXJpc3RpYz4N
              Cjwvd2FwLXByb3Zpc2lvbmluZ2RvYz4=
            </BinarySecurityToken>
          </RequestedSecurityToken>
          <RequestID
  xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollment">0</RequestID>
          <AdditionalContext
            xmlns="http://schemas.xmlsoap.org/ws/2006/12/authorization">
            <ContextItem Name="UserPrincipalName">
              <Value>dan@contoso.com</Value>
```

```
          </ContextItem>
        </AdditionalContext>
      </RequestSecurityTokenResponse>
    </RequestSecurityTokenResponseCollection>
  </s:Body>
</s:Envelope>
```

4.1.3 SOAP Fault

```
<s:Envelope
  xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">
      DeviceCapReached
    </a:Action>
    <a:RelatesTo>
      urn:uuid:0d5a1441-5891-453b-becf-a2e5f6ea3749
    </a:RelatesTo>
    <ActivityId
      CorrelationId="a6dd8835-9dc0-44c9-a410-8d897dd113fe"
      xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">
      0174f3f9-58e1-4a44-9a1c-3d15089efc9b
    </ActivityId>
  </s:Header>
  <s:Body>
    <s:Fault>
      <s:Code>
        <s:Value>
          s:Receiver
        </s:Value>
        <s:Subcode>
          <s:Value>
            s:DeviceCapReached
          </s:Value>
        </s:Subcode>
      </s:Code>
      <s:Reason>
        <s:Text xml:lang="en-US">
          WindowsEnrollmentServiceError
        </s:Text>
      </s:Reason>
      <s:Detail>
        <WindowsDeviceEnrollmentServiceError
          xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollment"
          xmlns:xsd="http://www.w3.org/2001/XMLSchema"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
          <ErrorType>
            AuthorizationError
          </ErrorType>
          <Message>
            DeviceCapReached
          </Message>
        </WindowsDeviceEnrollmentServiceError>
      </s:Detail>
    </s:Fault>
  </s:Body>
```

```
</s:Envelope>
```

4.1.4 Provisioning Document Example

```
<wap-provisioningdoc version="1.1">
  <characteristic
    type="CertificateStore">
    <characteristic
      type="My">
      <characteristic
        type="User">
        <characteristic
          type="F0370C64CAF6A46EB0F7214E591639AC05AC0B6E">
          <parm
            name="EncodedCertificate"
            value="MIIELTCCAxmgAwIBAgIQkNAArss5vZ1HypRLTixDuDAJBgUrDgMCHQU
                   AMHgxdjARBgoJkiaJk/IsZAEZFgNuZXQwFQYKCZImiZPyLGQBGRYHd2
                   luZG93czAdBgNVBAMTFk1TLU9yZ2FuaXphdGlvbi1BY2Nlc3MwKwYDV
                   QQLEyQ4MmRiYWNhNC0zZTgxLTQ2Y2EtOWM3My0wOTUwYzFlYWNhOTcw
        </characteristic>
      </characteristic>
    </characteristic>
  </characteristic>
</wap-provisioningdoc>
```

5 Security

5.1 Security Considerations for Implementers

The Device Registration Enrollment Protocol MUST use HTTPS as a transport. Using Secure Sockets Layer (SSL) server certificate verification ensures that the client is communicating with the real server and closes any possible man-in-the-middle attacks.

The input message uses an OAuth 2.0 JSON Web Token for both authentication and authorization. The server must validate that the security token is signed by a trusted identity provider and is within the token validity period, and that the target audience of the token is the server.

5.2 Index of Security Parameters

Security parameter	Section
wsse:BinarySecurityToken	3.1.4.1.1.1

6 Appendix A: Full WSDL

For ease of implementation, the full WSDL and schema are provided in this appendix.

```
<wsdl:definitions
xmlns:q2="http://schemas.datacontract.org/2004/07/Microsoft.DeviceRegistration"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:tns="http://schemas.microsoft.com/windows/pki/2009/01/enrollment"
xmlns:q1="http://schemas.microsoft.com/Message"
targetNamespace="http://schemas.microsoft.com/windows/pki/2009/01/enrollment"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:types>
    <xsd:schema elementFormDefault="qualified"
targetNamespace="http://schemas.microsoft.com/Message">
      <xsd:complexType name="MessageBody">
        <xsd:sequence>
          <xsd:any minOccurs="0" maxOccurs="unbounded" namespace="##any"/>
        </xsd:sequence>
      </xsd:complexType>
    </xsd:schema>
    <xsd:schema elementFormDefault="qualified"
targetNamespace="http://schemas.microsoft.com/windows/pki/2009/01/enrollment">
      <xsd:import
namespace="http://schemas.datacontract.org/2004/07/Microsoft.DeviceRegistration"/>
      <xsd:element name="WindowsDeviceEnrollmentServiceError" nillable="true"
type="q2:WindowsDeviceEnrollmentServiceError"/>
    </xsd:schema>
    <xsd:schema elementFormDefault="qualified"
targetNamespace="http://schemas.datacontract.org/2004/07/Microsoft.DeviceRegistration">
      <xsd:complexType name="WindowsDeviceEnrollmentServiceError">
        <xsd:sequence>
          <xsd:element minOccurs="0" maxOccurs="1" name="ErrorType" nillable="true"
type="q2:WinDeviceEnrollmentServiceErrorType"/>
          <xsd:element minOccurs="0" maxOccurs="1" name="Message" nillable="true"
type="xsd:string"/>
        </xsd:sequence>
      </xsd:complexType>
      <xsd:simpleType name="WinDeviceEnrollmentServiceErrorType">
        <xsd:restriction base="xsd:string">
          <xsd:enumeration value="InvalidParameter"/>
          <xsd:enumeration value="SqlError"/>
          <xsd:enumeration value="CertificateAuthorityError"/>
          <xsd:enumeration value="DirectoryAccountError"/>
          <xsd:enumeration value="AuthenticationError"/>
          <xsd:enumeration value="AuthorizationError"/>
          <xsd:enumeration value="UnknownError"/>
        </xsd:restriction>
      </xsd:simpleType>
    </xsd:schema>
  </wsdl:types>
  <wsdl:message name="IWindowsDeviceEnrollmentService_RequestSecurityToken_InputMessage">
    <wsdl:part name="messageRequest" type="q1:MessageBody"/>
  </wsdl:message>
  <wsdl:message name="IWindowsDeviceEnrollmentService_RequestSecurityToken_OutputMessage">
    <wsdl:part name="RequestSecurityTokenResult" type="q1:MessageBody"/>
  </wsdl:message>
```

```
  <wsdl:message
name="IWindowsDeviceEnrollmentService_RequestSecurityToken_WindowsDeviceEnrollmentServiceErro
rFault_FaultMessage">
    <wsdl:part name="detail" element="tns:WindowsDeviceEnrollmentServiceError"/>
  </wsdl:message>
  <wsdl:portType name="IWindowsDeviceEnrollmentService">
    <wsdl:operation name="RequestSecurityToken">
      <wsdl:input
wsaw:Action="http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RST/wstep"
message="tns:IWindowsDeviceEnrollmentService_RequestSecurityToken_InputMessage"/>
      <wsdl:output
wsaw:Action="http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RSTRC/wstep"
message="tns:IWindowsDeviceEnrollmentService_RequestSecurityToken_OutputMessage"/>
      <wsdl:fault
wsaw:Action="http://schemas.microsoft.com/windows/pki/2009/01/enrollment/IWindowsDeviceEnroll
mentService/RequestSecurityTokenWindowsDeviceEnrollmentServiceErrorFault"
name="WindowsDeviceEnrollmentServiceErrorFault"
message="tns:IWindowsDeviceEnrollmentService_RequestSecurityToken_WindowsDeviceEnrollmentServ
iceErrorFault_FaultMessage"/>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="IWindowsDeviceEnrollmentServiceSoap12"
type="tns:IWindowsDeviceEnrollmentService">
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="RequestSecurityToken">
      <soap12:operation
soapAction="http://schemas.microsoft.com/windows/pki/2009/01/enrollment/RST/wstep"
style="document"/>
      <wsdl:input>
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal"/>
      </wsdl:output>
      <wsdl:fault name="WindowsDeviceEnrollmentServiceErrorFault">
        <soap12:fault name="WindowsDeviceEnrollmentServiceErrorFault" use="literal"/>
      </wsdl:fault>
    </wsdl:operation>
  </wsdl:binding>
</wsdl:definitions>
```

7 Appendix B: Product Behavior

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

- Windows 8.1 operating system
- Windows Server 2012 R2 operating system

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.

8 Change Tracking

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

9 Index

V

W