[MS-XWDVSEC]:
Web Distributed Authoring and Versioning (WebDAV) Protocol Security Descriptor Extensions

---

Revision Summary

Date	Revision History	Revision Class	Comments
04/04/2008	0.1		Initial Availability.
04/25/2008	0.2		Revised and updated property names and other technical content.
06/27/2008	1.0		Initial Release.
08/06/2008	1.01		Updated references to reflect date of initial release.
09/03/2008	1.02		Updated references.
12/03/2008	1.03		Revised and edited technical content.
03/04/2009	1.04		Revised and edited technical content.
04/10/2009	2.0		Deprecated for Exchange 2010.
07/15/2009	3.0	Major	Changes made for template compliance.
11/04/2009	3.1.0	Minor	Updated the technical content.
02/10/2010	3.2.0	Minor	Updated the technical content.
05/05/2010	3.3.0	Minor	Updated the technical content.
08/04/2010	3.4	Minor	Clarified the meaning of the technical content.
11/03/2010	3.5	Minor	Clarified the meaning of the technical content.
03/18/2011	3.6	Minor	Clarified the meaning of the technical content.
08/05/2011	3.6	No change	No changes to the meaning, language, or formatting of the technical content.
10/07/2011	3.6	No change	No changes to the meaning, language, or formatting of the technical content.
01/20/2012	4.0	Major	Significantly changed the technical content.
04/27/2012	4.0	No change	No changes to the meaning, language, or formatting of the technical content.
07/16/2012	4.0	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2012	4.1	Minor	Clarified the meaning of the technical content.

Table of Contents

1 Introduction

The Web Distributed Authoring and Versioning (WebDAV) Protocol Security Descriptor Extensions extend the **WebDAV** protocol to request and set **security descriptors**. A security descriptor contains security information associated with an entity, such as the entity's owner, which users can access the entity, and so on.

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]:

access control entry (ACE)
access control list (ACL)
access mask
discretionary access control list (DACL)
flags
GUID
Hypertext Transfer Protocol (HTTP)
security identifier (SID)
XML

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

mailbox
Messaging Application Programming Interface (MAPI)
permission
public folder
security descriptor
security principal
store
Web Distributed Authoring and Versioning Protocol (WebDAV)
WebDAV client
WebDAV server
XML namespace
XML schema definition (XSD)

The following terms are specific to this document:

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 technical documents, which are updated frequently. References to other documents include a publishing year when one is available.

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.

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

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

[MS-ADTS] Microsoft Corporation, "Active Directory Technical Specification".

[MS-DTYP] Microsoft Corporation, "Windows Data Types".

[MS-OXCFOLD] Microsoft Corporation, "Folder Object Protocol Specification".

[MS-OXPROPS] Microsoft Corporation, "Exchange Server Protocols Master Property List".

[MS-SAMR] Microsoft Corporation, "Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)".

[MS-WSO] Microsoft Corporation, "Windows System Overview".

[MS-XWDEXT] Microsoft Corporation, "Web Distributed Authoring and Versioning (WebDAV) Core Extensions".

[RFC2068] Fielding, R., Gettys, J., Mogul, J., et al., "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2068, January 1997, http://www.ietf.org/rfc/rfc2068.txt

[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

[RFC2518] Goland, Y., Whitehead, E., Faizi, A., et al., "HTTP Extensions for Distributed Authoring - WebDAV", RFC 2518, February 1999, http://www.ietf.org/rfc/rfc2518.txt

[W3C-XMLNote] Layman, A., Jung, E., Maler, E., et al., "XML-Data", W3C Note, January 1998, http://www.w3.org/TR/1998/NOTE-XML-data-0105

[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/

[XMLSCHEMA1/2] Thompson, H.S., Ed., Beech, D., Ed., Maloney, M., Ed., and Mendelsohn, N., Ed., "XML Schema Part 1: Structures Second Edition", W3C Recommendation, October 2004, http://www.w3.org/TR/xmlschema-1/

[XMLSCHEMA2/2] Biron, P.V., Ed. and Malhotra, A., Ed., "XML Schema Part 2: Datatypes Second Edition", W3C Recommendation, October 2004, http://www.w3.org/TR/xmlschema-2

1.2.2 Informative References

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

[MS-OXGLOS] Microsoft Corporation, "Exchange Server Protocols Master Glossary".

[MS-OXPROTO] Microsoft Corporation, "Exchange Server Protocols System Overview".

1.3 Overview

As specified in [RFC2518], a **WebDAV client** can retrieve and set properties on a **WebDAV server**. A server can implement a property that represents a security descriptor in **XML**. A client retrieves and sets the security descriptor property on a server by using the WebDAV Protocol Security Extensions. The client can grant or deny access rights to a **security principal** for an entity by adding or removing **access control entries (ACEs)** from the security descriptor's **discretionary access control list (DACL)**.

For example, the client might be an e-commerce application that sells access to research reports. After a customer pays for access to a given report, the application retrieves the security descriptor for the appropriate document, updates it to grant access to the security principal that represents the customer, and sets it on the server. For examples of how a client retrieves and sets the security descriptor, see section 4.

1.4 Relationship to Other Protocols

The security descriptor property is based on WebDAV, as specified in [RFC2518] section 13.

These extensions use the WebDAV extensions specified in [MS-XWDEXT] sections 2.2.1.17 and 2.2.1.18 to get and set the security descriptor property.

For conceptual background information and overviews of the relationships and interactions between this and other protocols, see [MS-OXPROTO].

1.5 Prerequisites/Preconditions

The WebDAV server and WebDAV client applications are required to implement the WebDAV protocol, as specified in [RFC2518], so that the client can set properties on the server.

1.6 Applicability Statement

WebDAV clients can use these extensions to get or set the security descriptor for an entity. For example, a client with sufficient **permission** could determine whether to allow various security principals access to a particular entity.

1.7 Versioning and Capability Negotiation

This security descriptor property exposes no new versioning capabilities beyond the base protocol of WebDAV and the **Revision** field of the **SECURITY_DESCRIPTOR** structure, as specified in [MS-DTYP].

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

There is no standards assignment for this property beyond those assigned for the base WebDAV protocol, as specified in [RFC2518].

2 Messages

2.1 Transport

Messages are transported by using **HTTP**, as specified in [RFC2518] and [RFC2068].

2.2 Message Syntax

The security descriptor property adds to the set of WebDAV properties, as specified in [RFC2518] section 13. The WebDAV Protocol Security Extensions use the WebDAV extensions specified in [MS-XWDEXT] sections 2.2.1.17 and 2.2.1.18 to get and set this property. This property is an XML representation of a security descriptor. The type of this property is specified by using **XML schema definition (XSD)** grammar, as specified in [XMLSCHEMA1/2]. This property is represented by the **descriptor** XML element, which extends the **security_descriptor** element defined in the http://schemas.microsoft.com/security/ **XML namespace**. The XSD for this property is defined as follows.

```
<?xml version="1.0" encoding="utf-8" ?>
<xs:schema xmlns:S="http://schemas.microsoft.com/security/"
           xmlns:D="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/"
           attributeFormDefault="qualified"
           elementFormDefault="qualified"
           targetNamespace="http://schemas.microsoft.com/security/"
           xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <!--  Bool is defined to be either 1 or 0 -->
  <xs:simpleType name="bool">
    <xs:restriction base="xs:boolean">
      <xs:pattern value="0|1" />
    </xs:restriction>
  </xs:simpleType>

  <!--  Globally Unique Identifier [MS-DTYP] -->
  <xs:simpleType name="guid">
    <xs:restriction base="xs:string">
      <xs:pattern value="\{[0-9A-Fa-f]{8}-[0-9A-Fa-f]{4}-[0-9A-Fa-f]{4}-[0-9A-Fa-f]{4}-[0-9A-
Fa-f]{12}\}" />
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="type_string">
    <xs:restriction base="xs:string">
      <xs:enumeration value="user" />
      <xs:enumeration value="group" />
      <xs:enumeration value="domain" />
      <xs:enumeration value="alias" />
      <xs:enumeration value="well_known_group" />
      <xs:enumeration value="deleted_account" />
      <xs:enumeration value="invalid" />
      <xs:enumeration value="unknown" />
      <xs:enumeration value="computer" />
    </xs:restriction>
  </xs:simpleType>

  <xs:element name="display_name" type="xs:string" />
  <xs:element name="ad_object_guid" type="S:guid" />
  <xs:element name="type" type="S:type_string" />
```

```
  <xs:element name="nt4_compatible_name" type="xs:string" />
  <xs:element name="string_sid" type="xs:string" />

  <xs:complexType name="NT_Sid">
    <xs:sequence>
      <xs:element minOccurs="0" ref="S:string_sid" />
      <xs:element minOccurs="0" ref="S:nt4_compatible_name" />
      <xs:element minOccurs="0" ref="S:type" />
      <xs:element minOccurs="0" ref="S:ad_object_guid" />
      <xs:element minOccurs="0" ref="S:display_name" />
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="sid">
    <xs:sequence>
      <xs:element name="sid" type="S:NT_Sid" />
    </xs:sequence>
  </xs:complexType>

  <xs:element name="access_mask">
    <xs:simpleType>
      <xs:restriction base="xs:hexBinary">
        <xs:minLength value="1" />
        <xs:maxLength value="8" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>

  <xs:complexType name="ace_T">
    <xs:sequence>
      <xs:element ref="S:access_mask" />
      <xs:element name="sid" type="S:NT_Sid" />
    </xs:sequence>
    <xs:attribute name="inherited" type="S:bool" />
  </xs:complexType>

  <xs:complexType name="inheritable_ace_T">
    <xs:complexContent mixed="false">
      <xs:extension base="S:ace_T">
        <xs:attribute name="no_propagate_inherit" type="S:bool" />
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>

  <xs:complexType name="aces">
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="unbounded" name="access_allowed_ace"
type="S:ace_T" />
      <xs:element minOccurs="0" maxOccurs="unbounded" name="access_denied_ace" type="S:ace_T"
/>
      <xs:element minOccurs="0" maxOccurs="unbounded" name="system_audit_ace" type="S:ace_T"
/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="inheritable_aces">
    <xs:sequence>
      <xs:element minOccurs="0" maxOccurs="unbounded" name="access_allowed_ace"
type="S:inheritable_ace_T" />
```

```
      <xs:element minOccurs="0" maxOccurs="unbounded" name="access_denied_ace"
type="S:inheritable_ace_T" />
      <xs:element minOccurs="0" maxOccurs="unbounded" name="system_audit_ace"
type="S:inheritable_ace_T" />
    </xs:sequence>
  </xs:complexType>

  <xs:element name="revision" type="xs:unsignedInt" />

  <xs:complexType name="acl">
    <xs:all minOccurs="0">
      <xs:element ref="S:revision" />
      <xs:element name="effective_aces" type="S:aces" />
      <xs:element name="subcontainer_inheritable_aces" type="S:inheritable_aces" />
      <xs:element name="subitem_inheritable_aces" type="S:inheritable_aces" />
    </xs:all>
  </xs:complexType>

  <xs:element name="audit_always" type="S:acl" />
  <xs:element name="audit_on_failure" type="S:acl" />
  <xs:element name="audit_on_success" type="S:acl" />

  <xs:element name="sacl">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="S:revision" />
        <xs:element ref="S:audit_always" />
        <xs:element ref="S:audit_on_failure" />
        <xs:element ref="S:audit_on_success" />
      </xs:sequence>
      <xs:attribute name="defaulted" type="S:bool" />
      <xs:attribute name="protected" type="S:bool" />
      <xs:attribute name="autoinherited" type="S:bool" />
    </xs:complexType>
  </xs:element>

  <xs:element name="dacl">
    <xs:complexType>
      <xs:complexContent mixed="false">
        <xs:extension base="S:acl">
          <xs:attribute name="defaulted" type="S:bool" />
          <xs:attribute name="protected" type="S:bool" />
          <xs:attribute name="autoinherited" type="S:bool" />
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>

  <xs:element name="primary_group">
    <xs:complexType>
      <xs:complexContent mixed="false">
        <xs:extension base="S:sid">
          <xs:attribute name="defaulted" type="S:bool" />
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>

  <xs:element name="owner">
```

```
    <xs:complexType>
      <xs:complexContent mixed="false">
        <xs:extension base="S:sid">
          <xs:attribute name="defaulted" type="S:bool" />
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>

  <xs:element name="security_descriptor">
    <xs:complexType>
      <xs:complexContent mixed="false">
        <xs:extension base="D:microsoft.security_descriptor">
          <xs:attribute name="from_mapi_tlh" type="S:bool" />
        </xs:extension>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>
</xs:schema>

<!--  The base microsoft security descriptor -->
<xs:schema xmlns:S="http://schemas.microsoft.com/security/"
           xmlns:D="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/"
           attributeFormDefault="qualified"
           elementFormDefault="qualified"
           targetNamespace="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/"
           xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:complexType name="microsoft.security_descriptor">
    <xs:all minOccurs="0">
      <xs:element ref="S:revision" />
      <xs:element ref="S:owner" />
      <xs:element ref="S:primary_group" />
      <xs:element ref="S:dacl" />
      <xs:element ref="S:sacl" />
    </xs:all>
  </xs:complexType>
</xs:schema>

<!--  The schema of the actual descriptor property
      This is the property that can be asked for via WebDAV  -->

<xs:schema xmlns:S="http://schemas.microsoft.com/security/"
           xmlns:D="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/"
           attributeFormDefault="qualified"
           elementFormDefault="qualified"
           targetNamespace=
              "http://schemas.microsoft.com/exchange/security/"
           xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="descriptor">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="S:security_descriptor" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

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	Namespace URI	Reference
S	http://schemas.microsoft.com/security/	
D	urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/	[W3C-XMLNote]
xs	http://www.w3.org/2001/XMLSchema	[XMLSCHEMA1/2]
(none)	http://schemas.microsoft.com/security/	

2.2.2 PidTagSecurityDescriptorAsXml Property

Data type: **PtypString**

The **PidTagSecurityDescriptorAsXml** property ([MS-OXPROPS] section 2.1062) exposes a security descriptor that represents an entity's security attributes in XML. These attributes specify who owns the entity, who can access it, what they can do with it, what level of audit logging can be applied to the entity, and what kind of restrictions apply to the use of the security descriptor. The security descriptor is a limited XML version of the **SECURITY_DESCRIPTOR** structure, as specified in [MS-DTYP]. The content of the security descriptor is specified by the **security_descriptor** element, as specified in section 2.2.3. The schema that specifies the possible values for the **security_descriptor** element is specified in section 2.2.

Note that the XML security descriptor format does not have a way of transmitting the **SECURITY_INFORMATION** structure, as specified in [MS-DTYP], which is needed to set the security descriptor on the entity. Instead, the **SECURITY_INFORMATION** structure is derived from the presence or absence of fields in the XML security descriptor. For example, to set only the DACL on an entity, this property is set with only a DACL in it.

It is possible for a WebDAV client to get this property on an entity when (1) the client created the entity, (2) the client has administrator rights, (3) the entity is in the client's **mailbox**, and (4) the entity is in a **public folder**.

It is possible for a client to set this property on an entity when (1) the client created the entity, (2) the client has administrator rights, (3) the entity is in the client's mailbox, and (4) the entity is in a public folder on which the client has owner permissions.

2.2.3 security_descriptor Element

Name: security_descriptor

Namespace: http://schemas.microsoft.com/security/

Type: microsoft.security_descriptor (section 2.2.4)

Description: The **security_descriptor** element contains the type of the security descriptor specified in section 2.2.2. This element extends the **microsoft.security_descriptor** type adding a **bool** attribute of **from_mapi_tlh**.

2.2.3.1 from_mapi_tlh Attribute

Name: **from_mapi_tlh**

Namespace: http://schemas.microsoft.com/security/

Type: bool (section 2.2.20)

Description: The **from_mapi_tlh** attribute indicates that the entity for which this security descriptor applies is from a **store** that is accessible by using WebDAV clients that have the **Messaging Application Programming Interface (MAPI)** enabled.

The absence of this attribute implies that its value is 0. This attribute is applicable only when it is set by the WebDAV server. The WebDAV server MUST ignore this attribute if it is set by a client.

2.2.4 microsoft.security_descriptor Type

Name: microsoft.security_descriptor

Namespace: urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/

Description: The **microsoft.security_descriptor** type is the base security descriptor on which the WebDAV server's security descriptor is based.

2.2.5 revision Element

Name: revision

Namespace: http://schemas.microsoft.com/security/

Type: unsignedInt, as specified in [XMLSCHEMA2/2] section 3.3.22

Description: The **revision** element represents the revision of the **microsoft.security_descriptor** type, as specified in section 2.2.4. If this element is present, its value MUST be set to 1. The absence of this element implies that its value is 1.

2.2.6 owner Element

Name: owner

Namespace: http://schemas.microsoft.com/security/

Description: The **owner** element contains the **security identifier (SID)**, as specified in section 2.2.16, that specifies the owner of the entity to which the security descriptor is associated. This element can be present. The value of this element is semantically the same as that of the **Owner** member of the **SECURITY_DESCRIPTOR** structure as specified in [MS-DTYP].

2.2.6.1 defaulted Attribute

Name: defaulted

Namespace: http://schemas.microsoft.com/security/

Type: bool (section 2.2.20)

Description: The **defaulted** attribute is set when the owner was established by default means. This attribute MUST be present for the **owner** element, as specified in section 2.2.6. The value of this

attribute is semantically the same as that specified in [MS-DTYP], relating to the **OD** flag in the **Control** field of the **SECURITY_DESCRIPTOR** structure.

2.2.7 primary_group Element

Name: primary_group

Namespace: http://schemas.microsoft.com/security/

Description: The **primary_group** element contains the SID that specifies the group of the entity to which the security descriptor is associated. This element MUST be present for the **owner** element, as specified in section 2.2.6. The value of this element is semantically the same as that specified for the **Group** member of the **SECURITY_DESCRIPTOR** structure in [MS-DTYP].

2.2.7.1 defaulted Attribute

Name: defaulted

Namespace: http://schemas.microsoft.com/security/

Type: bool (section 2.2.20)

Description: The **defaulted** attribute is set when the group was established by default means. This attribute MUST be present for the **primary_group** element, as specified in section 2.2.7. The value of this attribute is semantically the same as that specified in [MS-DTYP], relating to the **GD** flag in the **Control** field of the **SECURITY_DESCRIPTOR** structure.

2.2.8 dacl Element

Name: dacl

Namespace: http://schemas.microsoft.com/security/

Description: The **dacl** element indicates the DACL. The DACL contains ACEs that grant or deny access to principals or groups. The value of this element is semantically the same as that specified for the **Dacl** member of the **SECURITY_DESCRIPTOR** structure in [MS-DTYP].

2.2.8.1 defaulted Attribute

Name: defaulted

Namespace: http://schemas.microsoft.com/security/

Type: bool (section 2.2.20)

Description: The **defaulted** attribute is set when the DACL represented by the **dacl** element, as specified in section 2.2.8, was established by default means. This attribute MUST be present for the **dacl** element. The value of this attribute is semantically the same as that specified in [MS-DTYP], relating to the **DD** flag in the **Control** field of the **SECURITY_DESCRIPTOR** structure.

2.2.8.2 protected Attribute

Name: protected

Namespace: http://schemas.microsoft.com/security/

Type: bool (section 2.2.20)

Description: The **protected** attribute is set when the DACL represented by the **dacl** element, as specified in section 2.2.8, SHOULD be protected from inherit operations. This attribute MUST be present for the **dacl** element. The value of this attribute is semantically the same as that specified in [MS-DTYP], relating to the **PD** flag in the **Control** field of the **SECURITY_DESCRIPTOR** structure.

2.2.8.3 autoinherited Attribute

Name: autoinherited

Namespace: http://schemas.microsoft.com/security/

Type: bool (section 2.2.20)

Description: The **autoinherited** attribute is set when the **access control list (ACL)** was created through inheritance. This attribute MUST be present for the **dacl** element, as specified in section 2.2.8. The value of this attribute is semantically the same as that specified in [MS-DTYP], relating to the **DI** flag in the **Control** field of the **SECURITY_DESCRIPTOR** structure.

2.2.9 sacl Element

Name: sacl

Namespace: http://schemas.microsoft.com/security/

Description: The **sacl** element indicates the system **ACL**. This element contains auditing ACEs. The value of this element is semantically the same as that specified for system ACL<1> in [MS-DTYP].

2.2.9.1 revision Element

Name: revision

Namespace: http://schemas.microsoft.com/security/

Type: unsignedInt, as specified in [XMLSCHEMA2/2] section 3.3.22

Description: The **revision** element MUST be present for the **sacl** element, as specified in section 2.2.9. This element serves the same purpose as the **AclRevision** field specified in [MS-DTYP] and shares the same appropriate values.

2.2.9.2 audit_always Element

Name: audit_always

Namespace: http://schemas.microsoft.com/security/

Type: acl (section 2.2.10)

Description: The **audit_always** element contains the set of ACEs to generate audit messages for access attempts. The value of this element is semantically the same as that specified in [MS-DTYP], relating to the **FAILED_ACCESS_ACE_FLAG** and **SUCCESSFUL_ACCESS_ACE_FLAG** flags.

2.2.9.3 audit_on_failure Element

Name: audit_on_failure

Namespace: http://schemas.microsoft.com/security/

Type: acl (section 2.2.10)

Description: The **audit_on_failure** element contains the set of ACEs to generate audit messages for failed access attempts. This element is used in place of the **FAILED_ACCESS_ACE_FLAG** flag of the **AceFlags** field in the **ACE_HEADER** structure specified in [MS-DTYP] and has the same semantic meaning.

2.2.9.4 audit_on_success Element

Name: audit_on_success

Namespace: http://schemas.microsoft.com/security/

Type: acl (section 2.2.10)

Description: The **audit_on_success** element contains the set of ACEs to generate audit messages for successful access attempts. This element is used in place of the **SUCCESSFUL_ACCESS_ACE_FLAG** flag of the **AceFlags** field in the **ACE_HEADER** structure specified in [MS-DTYP] and has the same semantic meaning.

2.2.9.5 defaulted Attribute

Name: defaulted

Namespace: http://schemas.microsoft.com/security/

Type: bool (section 2.2.20)

Description: The **defaulted** attribute is set when the system ACL was established by default means. This attribute MUST be present for the **sacl** element, as specified in section 2.2.9. The value of this attribute is semantically the same as that specified in [MS-DTYP], relating to the **SD** flag in the **Control** field of the **SECURITY_DESCRIPTOR** structure.

2.2.9.6 protected Attribute

Name: protected

Namespace: http://schemas.microsoft.com/security/

Type: bool (section 2.2.20)

Description: The **protected** attribute is set to protect the system ACL from inherit operations. This attribute MUST be present for the **sacl** element, as specified in section 2.2.9. The value of this attribute is semantically the same as that specified in [MS-DTYP], relating to the **PS** flag in the **Control** field of the **SECURITY_DESCRIPTOR** structure.

2.2.9.7 autoinherited Attribute

Name: autoinherited

Namespace: http://schemas.microsoft.com/security/

Type: bool (section 2.2.20)

Description: The **autoinherited** attribute is set when the system ACL was created by inheritance. This attribute MUST be present for the **sacl** element, as specified in section 2.2.9. The value of this

attribute is semantically the same as that specified in [MS-DTYP], relating to the **SI** flag in the **Control** field of the **SECURITY_DESCRIPTOR** structure.

2.2.10 acl Type

Name: acl

Namespace: http://schemas.microsoft.com/security/

Description: The **acl** type contains a list of ACEs. This is analogous to the **ACL** type, as specified in [MS-DTYP].

2.2.10.1 revision Element

Name: revision

Namespace: http://schemas.microsoft.com/security/

Type: unsignedInt, as specified in [XMLSCHEMA2/2] section 3.3.22

Description: The **revision** element indicates the version of the **acl** type, as specified in section 2.2.10. This element MUST exist. This element serves the same purpose as the **AclRevision** field specified in [MS-DTYP] and shares the same appropriate values.

2.2.10.2 effective_aces Element

Name: effective_aces

Namespace: http://schemas.microsoft.com/security/

Type: aces (section 2.2.11)

Description: The **effective_aces** element contains a list of ACEs that affect the entity. This element can exist if the ACL contains one or more ACEs.

2.2.10.3 subcontainer_inheritable_aces Element

Name: subcontainer_inheritable_aces

Namespace: http://schemas.microsoft.com/security/

Type: inheritable_aces (section 2.2.12)

Description: The **subcontainer_inheritable_aces** element contains a list of ACEs such that child entities that are containers, such as folders, inherit these ACEs as effective ACEs. This element can exist if the ACL contains one or more ACEs. This is semantically the same as each **ACE** within this element having the **CONTAINER_INHERIT_ACE** flag set on the **AceFlags** field of the **ACE_HEADER** structure, as specified in [MS-DTYP].

2.2.10.4 subitem_inheritable_aces Element

Name: subitem_inheritable_aces

Namespace: http://schemas.microsoft.com/security/

Type: inheritable_aces (section 2.2.12)

Description: The **subitem_inheritable_aces** element contains a list of ACEs such that noncontainer child entities, such as attachments, inherit these ACEs as effective ACEs. This element can exist if the ACL contains one or more ACEs. This is semantically the same as each ACE within this element having the **OBJECT_INHERIT_ACE** flag set on the **AceFlags** field of the **ACE_HEADER** structure, as specified in [MS-DTYP].

2.2.11 aces Type

Name: aces

Namespace: http://schemas.microsoft.com/security/

Description: The **aces** type contains a list of non-inheritable ACEs. All the ACEs in this type are semantically the same as the **ACE_INHERITED_OBJECT_TYPE_PRESENT** flag not being set on an ACE, as specified in [MS-DTYP].

2.2.11.1 access_allowed_ace Element

Name: access_allowed_ace

Namespace: http://schemas.microsoft.com/security/

Type: ace_T (section 2.2.13)

Description: The **access_allowed_aces** element allows access to an entity for a specific trustee identified by a SID. This element can exist if a trustee is allowed access to an entity. This element is only allowed within the **dacl** element, as specified in section 2.2.8. This ACE is semantically the same as the **ACCESS_ALLOWED_ACE** structure, as specified in [MS-DTYP].

2.2.11.2 access_denied_ace Element

Name: access_denied_ace

Namespace: http://schemas.microsoft.com/security/

Type: ace_T (section 2.2.13)

Description: The **access_denied_ace** element denies access to an entity for a specific trustee identified by a SID. This element can exist if a trustee is denied access to an entity. This element is only allowed within the **dacl** element, as specified in section 2.2.8. This ACE is semantically the same as the **ACCESS_DENIED_ACE** structure, as specified in [MS-DTYP].

2.2.11.3 system_audit_ace Element

Name: system_audit_ace

Namespace: http://schemas.microsoft.com/security/

Type: ace_T (section 2.2.13)

Description: The **system_audit_ace** element can exist if a trustee is monitored for attempts to access a specific entity. This element is only allowed within the **sacl** element, as specified in section 2.2.10. This ACE follows the same semantics as the **SYSTEM_AUDIT_ACE** structure, as specified in [MS-DTYP].

2.2.12 inheritable_aces Type

Name: inheritable_aces

Namespace: http://schemas.microsoft.com/security/

Description: The **inheritable_aces** type contains a list of inheritable ACEs. How these ACEs are inherited is declared by the usage of the **inheritable_aces** type in either the **subitem_inheritable_aces** element, as specified in section 2.2.10.4, or the **subcontainer_inheritable_aces** element, as specified in section 2.2.10.3.

2.2.12.1 access_allowed_ace Element

Name: access_allowed_ace

Namespace: http://schemas.microsoft.com/security/

Type: inheritable_ace_T (section 2.2.14)

Description: The **access_allowed_ace** element allows access to an entity for a specific trustee identified by a SID. This element can exist if a trustee is allowed access to an entity. This element is allowed only within the **dacl** element, as specified in section 2.2.8. This ACE is semantically the same as the **ACCESS_ALLOWED_ACE** structure, as specified in [MS-DTYP].

2.2.12.2 access_denied_ace Element

Name: access_denied_ace

Namespace: http://schemas.microsoft.com/security/

Type: inheritable_ace_T (section 2.2.14)

Description: The **access_denied_ace** element denies access to an entity for a specific trustee identified by a SID. This element can exist if a trustee is denied access to an entity. This element is only allowed within the **dacl** element, as specified in section 2.2.8. This ACE is semantically the same as the **ACCESS_DENIED_ACE** structure, as specified in [MS-DTYP].

2.2.12.3 system_audit_ace Element

Name: system_audit_ace

Namespace: http://schemas.microsoft.com/security/

Type: inheritable_ace_T (section 2.2.14)

Description: The **system_audit_ace** element can exist if a trustee is monitored for attempts to access a specific entity. This element is only allowed within the **sacl** element, as specified in section 2.2.10. This ACE is semantically the same as the **SYSTEM_AUDIT_ACE** structure, as specified in [MS-DTYP].

2.2.13 ace_T Type

Name: ace_T

Namespace: http://schemas.microsoft.com/security/

Description: The **ace_T** type is the type for ACEs, as specified in section 2.2.11.

2.2.13.1 access_mask Element

Name: access_mask

Namespace: http://schemas.microsoft.com/security/

Type: access_mask (section 2.2.15)

Description: The **access_mask** element encodes the rights to an entity for a security principal. This element MUST exist on all ACEs. The actual **flags** for encoding these rights are specified in section 2.2.15.

2.2.13.2 sid Element

Name: sid

Namespace: http://schemas.microsoft.com/security/

Type: NT_Sid (section 2.2.17)

Description: The **sid** element identifies a security principal. This element MUST exist on all ACEs. This element is semantically the same as the **SID** type, as specified in [MS-DTYP].

2.2.13.3 inherited Attribute

Name: inherited

Namespace: http://schemas.microsoft.com/security/

Type: bool (section 2.2.20)

Description: The **inherited** attribute indicates that the ACE was inherited. This attribute MUST exist. This attribute is semantically the same as the **INHERITED_ACE** flag in the **AceFlags** field of the **ACE_HEADER** structure, as specified in [MS-DTYP].

2.2.14 inheritable_ace_T Type

Name: inheritable_ace_T

Namespace: http://schemas.microsoft.com/security/

Description: The **inheritable_ace_T** type is the base type for all inheritable ACEs. ACEs of this type are the equivalent of having the specific **CONTAINER_INHERIT_ACE** or **OBJECT_INHERIT_ACE** flags set in the **AceFlags** field of the **ACE_HEADER** structure as specified in [MS-DTYP].

The **inheritable_ace_T** type extends the base **ace_T** type, as specified in section 2.2.13.

2.2.14.1 no_propagate_inherit Attribute

Name: no_propagate_inherit

Namespace: http://schemas.microsoft.com/security/

Type: bool (section 2.2.20)

Description: The **no_propagate_inherit** attribute declares that an inherited ACE is not inheritable. This attribute MUST exist. This attribute is semantically the same as the **NO_PROPAGATE_INHERIT_ACE** flag as specified in [MS-DTYP] for the **AceFlags** field flags **CONTAINER_INHERIT_ACE** and **OBJECT_INHERIT_ACE**.

2.2.15 access_mask Element

Name: access_mask

Namespace: http://schemas.microsoft.com/security/

Type: hexBinary [XMLSCHEMA2/2] section 3.2.15, but limited to between one and eight digits

Description: The **access_mask** element is a 32-bit set of flags that are used to encode the user rights to an entity. An **access mask** is used both to encode the rights to an entity assigned to a security principal and to encode the requested access when opening an entity. This element MUST exist for all ACEs. A bit set to 1 specifies that the allowed or denied right is granted. The unused lower bits MUST be ignored. The lower 16 bits are as follows.

MSB															**LSB**
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
				V	DOI	WOP	WA	RA		E	WP	RP	AM	WB	RB

Value	Meaning
RB	Read body
WB	Write body
AM	Append message
RP	Read property
WP	Write property
E	Execute
RA	Read attributes
WA	Write attributes
WOP	Write own property
DOI	Delete own item
V	View item

2.2.16 sid Type

Name: sid

Namespace: http://schemas.microsoft.com/security/

Description: The **sid** type contains the SID that uniquely identifies a security principal. This type wraps an **NT_Sid** type, as specified in section 2.2.17, with a **sid** element.

2.2.17 NT_Sid Type

Name: NT_Sid

Namespace: http://schemas.microsoft.com/security/

Description: The **NT_Sid** type is the XML representation of a SID. It can contain several pieces of information about the security identifier.

If the WebDAV client retrieves the XML representation from the WebDAV server, the following elements will appear in the representation of the **NT_Sid** type (as long as they are available):

- **string_sid** (section 2.2.17.1)
- **nt4_compatible_name** (section 2.2.17.2)
- **type** (section 2.2.17.3)
- **ad_object_guid** (section 2.2.17.4)
- **display_name** (section 2.2.17.5)

In some cases, the server returns less information. For example, if the SID cannot be looked up, the server returns only the **string_sid** element. For some built-in NT accounts, the server returns only the **string_sid**, **nt4_compatible_name**, and **type** elements.

If the WebDAV client sets the XML representation, it does not have to give all the elements, providing that one of the following elements is sufficient:

- **string_sid**
- **nt4_compatible_name**
- **ad_object_guid**
- **display_name**

The server will use only one of the elements that the client gives it to determine the SID. The server SHOULD use the element that is easiest to compute and least prone to ambiguity. The order based on ease of computation is (1) **string_sid**, (2) **nt4_compatible_name**, (3) **ad_object_guid**, and (4) **display_name**. As a last resort, the client can use the **display_name** element, but because it is not unique, this is not recommended.

2.2.17.1 string_sid Element

Name: string_sid

Namespace: http://schemas.microsoft.com/security/

Type: string [XMLSCHEMA2/2] section 3.2.1

Description: The **string_sid** element identifies a security principal. This element can exist for any SID. This is the string representation of the **SID** type, as specified in [MS-DTYP].

2.2.17.2 nt4_compatible_name Element

Name: **nt4_compatible_name**

Namespace: http://schemas.microsoft.com/security/

Type: string [XMLSCHEMA2/2] section 3.2.1

Description: The **nt4_compatible_name** element identifies a security principal. This element can exist for any SID. This element contains a security principal as either a fully qualified account name, such as contoso/someone, or a user principal name, such as someone@contoso. as specified in [MS-WSO].

2.2.17.3 type Element

Name: type

Namespace: http://schemas.microsoft.com/security/

Type: type_string (section 2.2.18)

Description: The **type** element specifies the type of SID. This element can exist for any SID. The enumeration of values is specified in section 2.2.18.

2.2.17.4 ad_object_guid Element

Name: ad_object_guid

Namespace: http://schemas.microsoft.com/security/

Type: guid (section 2.2.19).

Description: The **ad_object_guid** element identifies a security principal. This element can exist for any SID. The value of this element is a string representation of the **objectGuid** property specified in [MS-ADA3]. This property is included so that WebDAV clients that allow users to pick an entry from the directory service, as specified in [MS-ADTS], can specify the entry by giving the **objectGuid** property.

2.2.17.5 display_name Element

Name: display_name

Namespace: http://schemas.microsoft.com/security/

Type: string [XMLSCHEMA2/2] section 3.2.1

Description: The **display_name** element identifies a security principal. This element can exist for any SID. The value of this element is a display name that WebDAV clients can display in the UI. It comes from the **PidTagDisplayName** property ([MS-OXCFOLD] section 2.2.2.2.2.4). It can also be read from the directory service as **displayName**, as specified in [MS-ADA1]. Use of this element to identify a security principal is not recommended because the value is not unique.

2.2.18 type_string Type

Name: type_string

Namespace: http://schemas.microsoft.com/security/

Description: The **type_string** type specifies the type of SID contained in the **NT_Sid** type, as specified in section 2.2.17. This type can be one of the values listed in the following table.

Value	Meaning
user	A user SID
group	A group SID
domain	A domain SID
alias	An alias SID
well_known_group	A SID for a well-known group
deleted_account	A SID for a deleted account
invalid	A SID that is not valid
unknown	A SID of unknown type
computer	A SID for a computer

These values are semantically the same as those found in the enumeration **SID_NAME_USE**, as specified in [MS-SAMR].

2.2.19 guid Type

Name: guid

Namespace: http://schemas.microsoft.com/security/

Description: The **guid** type is a **GUID** that identifies a security principal. This type is semantically the same as the **GUID** structure, as specified in [MS-DTYP]. The value of the **guid** type MUST be enclosed by curly braces, for example: "{41a1a32a-4d0f-41ab-ad0c-fb344ef368fd}".

2.2.20 bool Type

Name: bool

Namespace: http://schemas.microsoft.com/security/

Type: Boolean [XMLSCHEMA2/2]

Description: The **bool** type has the same meaning as specified in [XMLSCHEMA2/2] but is constrained to the values of 0 (zero) and 1.

3 Protocol Details

3.1 WebDAV Client Details

The security descriptor property that the WebDAV client retrieves from the WebDAV server can contain more information than what is required of the client to set it. Section 2.2.2 specifies that the client does not need to set the entire security descriptor to modify the DACL. Additionally, the security descriptor property can contain multiple security principal identifiers for the **NT_Sid** type, as specified in section 2.2.17.

The client can generate all of the security principal identifiers when sending the security descriptor property to the server. It is recommended that the client generate the most precise identifier, as specified in section 2.2.17, to avoid ambiguous identifiers.

3.1.1 Abstract Data Model

None.

3.1.2 Timers

None.

3.1.3 Initialization

None.

3.1.4 Higher-Layer Triggered Events

No additional higher-layer triggered events exist beyond those in [RFC2518], and the behavior of any existing higher-layer triggered events is unchanged by this extension.

3.1.5 Message Processing Events and Sequencing Rules

The sequence rules are those that are found for any property, as specified in [RFC2518] section 13.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2 WebDAV Server Details

The WebDAV server MUST generate all available security principal identifiers when sending the security descriptor property to the WebDAV client. The client can generate all the security principal identifiers when sending the security descriptor property to the server, but the server MUST use the most precise identifier that is received from the client, as specified in section 2.2.17.

3.2.1 Abstract Data Model

None.

3.2.2 Timers

None.

3.2.3 Initialization

None.

3.2.4 Higher-Layer Triggered Events

No additional higher-layer triggered events exist beyond those specified in [RFC2518], and the behavior of any existing higher-layer triggered events is unchanged by this extension.

3.2.5 Message Processing Events and Sequencing Rules

The sequence rules are those that are found for any property, as specified in [RFC2518] section 13.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

4 Protocol Examples

4.1 Retrieving the Security Descriptor Property

The security descriptor property can be retrieved using a standard WebDAV **PROPFIND** method request, as specified in [RFC2518], by asking for the **descriptor** element.

For example, the **descriptor** element might look as follows.

```
<d:descriptor  xmlns:d="http://schemas.microsoft.com/exchange/security/">
  <S:security_descriptor xmlns:S="http://schemas.microsoft.com/security/"
xmlns:D="urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/" D:dt="microsoft.security_descriptor"
S:from_mapi_tlh="1">
    <S:revision>1</S:revision>
    <S:owner S:defaulted="0">
      <S:sid>
        <S:string_sid>S-1-5-21-2082262111-2968666075-236047801-1111</S:string_sid>
        <S:type>user</S:type>
        <S:nt4_compatible_name>ELZCHU-DOM\bob</S:nt4_compatible_name>
        <S:ad_object_guid>{138bfc4d-48e0-4d29-9de6-643ecb7314f1}</S:ad_object_guid>
        <S:display_name>bob</S:display_name>
      </S:sid>
    </S:owner>
    <S:primary_group S:defaulted="0">
      <S:sid>
        <S:string_sid>S-1-5-21-2082262111-2968666075-236047801-513</S:string_sid>
        <S:type>group</S:type>
        <S:nt4_compatible_name>ELZCHU-DOM\Domain Users</S:nt4_compatible_name>
        <S:ad_object_guid>{f2a02601-c596-4fd2-9543-d770ba31d9e5}</S:ad_object_guid>
      </S:sid>
    </S:primary_group>
    <S:dacl S:defaulted="1" S:protected="0" S:autoinherited="1">
      <S:revision>2</S:revision>
      <S:effective_aces>
        <S:access_allowed_ace S:inherited="1">
          <S:access_mask>1f0fbf</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-5-21-2082262111-2968666075-236047801-500</S:string_sid>
            <S:type>user</S:type>
            <S:nt4_compatible_name>ELZCHU-DOM\Administrator</S:nt4_compatible_name>
            <S:ad_object_guid>{41a1a32a-4d0f-41ab-ad0c-fb344ef368fd}</S:ad_object_guid>
            <S:display_name>Administrator</S:display_name>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_allowed_ace S:inherited="1">
          <S:access_mask>1f0fbf</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-5-7</S:string_sid>
            <S:type>well_known_group</S:type>
            <S:nt4_compatible_name>NT AUTHORITY\ANONYMOUS LOGON</S:nt4_compatible_name>
            <S:ad_object_guid>{ff158509-ee41-4c44-98c1-affd7edf6a83}</S:ad_object_guid>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_allowed_ace S:inherited="1">
          <S:access_mask>1f0fbf</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-1-0</S:string_sid>
            <S:type>well_known_group</S:type>
```

```
            <S:nt4_compatible_name>\Everyone</S:nt4_compatible_name>
            <S:ad_object_guid>{aa5d6b3e-3546-4f9e-8530-59ad567c6dd8}</S:ad_object_guid>
          </S:sid>
        </S:access_allowed_ace>
      </S:effective_aces>
    </S:dacl>
  </S:security_descriptor>
</d:descriptor>
```

4.2 Setting the Security Descriptor Property

To set the security descriptor property by using the **PROPPATCH** method, as specified in [RFC2518], the WebDAV request XML can look like the following.

```
<?xml version='1.0'?>
<d:descriptor xmlns:d='http://schemas.microsoft.com/exchange/security/'>
  <S:security_descriptor xmlns:data='urn:uuid:c2f41010-65b3-11d1-a29f-00aa00c14882/'
data:dt='microsoft.security_descriptor'>
    <S:dacl xmlns:S="http://schemas.microsoft.com/security/" S:defaulted="0" S:protected="0"
S:autoinherited="0">
      <S:effective_aces>
        <S:access_allowed_ace>
          <S:access_mask>1f0fbf</S:access_mask>
          <S:sid>
             <S:string_sid>S-1-5-21-2082262111-2968666075-236047801-500</S:string_sid>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_allowed_ace>
          <S:access_mask>1f0fbf</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-5-7</S:string_sid>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_allowed_ace>
          <S:access_mask>1208a9</S:access_mask>
          <S:sid>
            <S:ad_object_guid>{9F4AC28A-2FD0-475E-9736-A9AF92E6612F}</S:ad_object_guid>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_allowed_ace>
          <S:access_mask>1200a9</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-1-0</S:string_sid>
          </S:sid>
        </S:access_allowed_ace>
        <S:access_denied_ace>
          <S:access_mask>d0f16</S:access_mask>
          <S:sid>
            <S:string_sid>S-1-1-0</S:string_sid>
          </S:sid>
        </S:access_denied_ace>
      </S:effective_aces>
      <S:subcontainer_inheritable_aces>
        <S:access_allowed_ace>
          <S:access_mask>1208a9</S:access_mask>
          <S:sid>
```

```
            <S:ad_object_guid>{9F4AC28A-2FD0-475E-9736-A9AF92E6612F}</S:ad_object_guid>
          </S:sid>
        </S:access_allowed_ace>
      </S:subcontainer_inheritable_aces>
      <S:subitem_inheritable_aces>
        <S:access_allowed_ace>
          <S:access_mask>1208a9</S:access_mask>
          <S:sid>
             <S:ad_object_guid>{9F4AC28A-2FD0-475E-9736-A9AF92E6612F}</S:ad_object_guid>
          </S:sid>
        </S:access_allowed_ace>
      </S:subitem_inheritable_aces>
    </S:dacl>
  </S:security_descriptor>
</d:descriptor>
```

5 Security

5.1 Security Considerations for Implementers

This extension has no security considerations beyond those described in [RFC2518] section 17, [RFC2068] section 15, and [MS-DTYP].

5.2 Index of Security Parameters

None.

6 Appendix A: 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:

- Microsoft® Exchange Server 2003
- Microsoft® Exchange Server 2007

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 2.2.9: The **sacl** element is not settable in Exchange 2003 and Exchange 2007, but it can appear on items that were upgraded to Exchange 2003 or Exchange 2007.

7 Change Tracking

This section identifies changes that were made to the [MS-XWDVSEC] protocol document between the July 2012 and October 2012 releases. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.
- An extensive rewrite, addition, or deletion of major portions of content.
- The removal of a document from the documentation set.
- Changes made for template compliance.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the language and formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical or language changes were introduced. The technical content of the document is identical to the last released version, but minor editorial and formatting changes, as well as updates to the header and footer information, and to the revision summary, may have been made.

Major and minor changes can be described further using the following change types:

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.

- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.
- New content added for template compliance.
- Content updated for template compliance.
- Content removed for template compliance.
- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated.**

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact protocol@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
1.2.2 Informative References	Added the reference [MS-OXPROTO].	N	Content updated.
1.4 Relationship to Other Protocols	Added informative reference information for overview of relationships between this and other protocols.	N	Content updated.

8 Index

T

V