Driving IP-based physical security through global standardization

ONVIF™

ONVIF Specification Version 2.6
Release Notes

1. Summary

The ONVIF 2.6release incorporates a number of major enhancements and minor clarifications for better interoperability among ONVIF conformant clients and devices. The changes themselves are described in details in the list below chapters 2 and 3.

2. Additions

This release adds the following functionality to the set of ONVIF Network Interface Specifications:

2.1 Advanced Security Service

Certificate based client authentication has been added to the service specification:

2.2 Access Rules Specification

This specification defines the web service interface for integration with physical access control systems. This includes discovering components and support of the configuration of the access rules components. The access rules service specification, which constitutes the access profiles and policies. The access rules service provides the access authorization for a credential.

2.3 Credential Service Specification

This specification defines the web service interface for integration with physical access control systems. This includes discovering components and support of the configuration of the credentials components.

2.4 Schedule Service Specification

This specification defines the web service interface for interaction with ONVIF devices which support time management features such as schedules and special days (sometimes referred to as holidays).

3. Changes

Find below all errata from Version 2.5 to 2.6 in order to improve interoperability. The numbers correspond to the Change Request ticket numbers and are not necessarily continuously ascending.

If not noted otherwise the changes refer to the Core specification.

1552 Define required cryptographic protocols options only at one place

In the Advanced Security Service, define mandatory cryptographic algorithms in Sect. 5.4.4 only and delete redundant information from the API definitions as follows.

In Create PKCS#10 Certification Request (Sect. 5.2.6.3.1), delete

> A device that supports this command shall as minimum support the sha1WithRSAEncryption signature algorithm as specified in [RFC 3279] and the sha256WithRSAEncryption signature algorithm as specified in [RFC 4055].

In Create Self-Signed Certificate (Sect. 5.2.6.3.2), delete

> A device that supports this command shall as minimum support the sha1WithRSAEncryption signature algorithm as specified in [RFC 3279] and the sha256WithRSAEncryption signature algorithm as specified in [RFC 4055].

In Upload Certificate (Sect. 5.2.6.3.3), delete

> A device that supports this command shall as minimum support the sha1WithRSAEncryption signature algorithm as specified in [RFC 3279] and the sha256WithRSAEncryption signature algorithm as specified in [RFC 4055].

1555 Some fault descriptions are different between command API table and table 24.

In the Advanced Security Service, make the following changes:

In Table 4 (CreateRSAKeyPair command),ter:MaximumNumberOfKeysReached, replace

> The device does not have enough storage space to store the key pair to be generated.

by

> The keystore does not have enough storage space to store the key pair that has to be generated.

In Table 12 (Upload Certificate command), ter:MaximumNumberOfKeysReached, replace

> The device does not have enough storage space to store the key pair that has to be generated.

by

> The keystore does not have enough storage space to store the key pair that has to be generated.

In Table 29 (Advanced Security service specific fault codes), add a row

> env:Receiver, ter:Action, ter:KeyLength ; Key length not supported ; The specified key length is not supported by the device.

In Table 7 (GetPrivateKeyStatus command), ter:InvalidKeyType, replace

The key stored under the requested KeyID does not identify a key pair.

by

The key stored in the keystore under the requested KeyID is of an invalid type.

In Table 9 (DeleteKey command), ter:ReferenceExists, replace

A reference exists for the specified key.

by

A reference exists for the object that is to be deleted.

In Table 20 (DeleteCertificationPath command), ter:ReferenceExists, replace

A reference exists for the specified certification path.

by

A reference exists for the object that is to be deleted.

In Table 10 (CreatePKCS10CSR command), ter:KeyID, replace

No key is stored under the requested KeyID or the key specified by the requested Key ID is not an asymmetric key pair.

by

No key is stored under the requested KeyID.

In Table 11 (CreateSelfSignedCertificate command), ter:KeyID, replace

No key is stored under the requested KeyID or the key specified by the requested Key ID is not an asymmetric key pair.

by

No key is stored under the requested KeyID.

In Table 12 (Upload Certificate command), ter:MaximumNumberOfCertificatesReached, replace

The device does not have enough storage space to store the certificate to be uploaded.

by

The device does not have enough storage space to store the certificate to be created.

In Table 12 (Upload Certificate command), ter:UnsupportedSignatureAlgorithm, replace

The signature algorithm that the signature of the supplied certificate is based on is not supported by the device.

by

The specified signature algorithm is not supported by the device.

In Table 17 (CreateCertificationPath command), ter:MaximumNumberOfCertificationPathsReached, replace

The device does not have enough storage space to store the certification path to be created.

by

The maximum number of certification paths that may be assigned to the TLS server simultaneously is reached.

In Table 17 (CreateCertificationPath command), ter:CertificateID, replace

For at least one of the supplied certificate IDs, there exists no certificate in the device’s keystore.

by

No certificate is stored under the requested CertificateID.

In Table 21 (AddServerCertificateAssignment command), ter:NoPrivateKey, replace

> The key pair that is associated with the first certificate in the certification path (i.e., the server certificate) does not have an associated private key.

by

> The key pair that is associated with the first certificate in the certificate chain does not have an associated private key.

In Table 23 (ReplaceServerCertificateAssignment command), ter:NoPrivateKey, replace

> The key pair that is associated with the first certificate in the new certification path (i.e., the server certificate), does not have an associated private key.

by

> The key pair that is associated with the first certificate in the certificate chain does not have an associated private key.

1571 Update Streaming spec about GZIP payload format

Replace the following text in ONVIF Streaming specification

> The Metadata payload is an XML document with root node tt:MetaDataStream. There is no limitation on the size of the XML document.

with

> The Metadata payload is an XML document with root node tt:MetaDataStream. There is no limitation on the size of the XML document. If GZIP compression is used the payload starts with a GZIP header according to RFC 1952 followed by the compressed data. A marker bit signals the end of the compressed data.

Add the following normative reference in Chapter 2.

> GZIP file format specification version 4.3
> <http://tools.ietf.org/html/rfc1952>

1581 Monitoring Event default time

Add the following text in Section 8.8.4 in ONVIF Core specification

> A device shall report the time of 1970-01-01T00:00:00Z when notifying the Initialized state of a property event that has never occurred. This applies e.g. to LastReset, LastClockSynchronization and Backup/Last.

1582 In section 4.6, reference in Appendix A. is wrong

Replace the following text in Section 4.6 in ONVIF Core specification

A fully standardized event requires standardized notifications. However, the notification topics will, to a large extent, depend on the application needs. This specification defines a set of basic notification topics that a device is recommended to support, see Appendix A. In addition, for some services, this specification extends the basic notification topics with mandatory events.

with

A fully standardized event handling requires standardized notifications. However, the notification topics will, to a large extent, depend on the application needs. This specification defines a set of basic notification topics.

1583 KeyID is not unique in GetAllCertificates

In advancedsecurity.wsdl, element <xs:simpleType name="KeyID">, replace

<xs:restriction base="xs:ID"/>

with

<xs:restriction base="xs:NCName"/>

In advancedsecurity.wsdl, element <xs:simpleType name="CertificateID">,

replace

<xs:restriction base="xs:ID"/>

with

<xs:restriction base="xs:NCName"/>

In advancedsecurity.wsdl, element <xs:simpleType name="CertificationPathID">,

replace

<xs:restriction base="xs:ID"/>

with

<xs:restriction base="xs:NCName"/>

In advancedsecurity.wsdl, element <xs:simpleType name="PassphraseID">,

replace

<xs:restriction base="xs:ID"/>

with

<xs:restriction base="xs:NCName"/>

1585 Remove old part in 9.11.2

Remove the following part in Section 9.11.2 in ONVIF Core specification

(the description can be downloaded from http://www.onvif.org/onvif/ver10/topics/topicns.xml)

1586 ONVIF topic namespace

Replace the following part in Section 9.7.1 in ONVIF Core specification

The following root topics are defined in the ONVIF Namespace. All notifications referring to these topics shall use the Message Format as described in Section 9.5.2.

```
<wstop:TopicNamespace name="ONVIF"
 targetNamespace="http://www.onvif.org/ver10/topics" >
<wstop:Topic name="Device"/>
<wstop:Topic name="VideoSource"/>
<wstop:Topic name="VideoEncoder"/>
<wstop:Topic name="VideoAnalytics"/>
<wstop:Topic name="RuleEngine"/>
<wstop:Topic name="PTZController"/>
<wstop:Topic name="AudioSource"/>
<wstop:Topic name="AudioEncoder"/>
<wstop:Topic name="UserAlarm"/>
<wstop:Topic name="MediaControl"/>
<wstop:Topic name="RecordingConfig"/>
<wstop:Topic name="RecordingHistory"/>
<wstop:Topic name="VideoOutput"/>
<wstop:Topic name="AudioOutput"/>
<wstop:Topic name="VideoDecoder"/>
<wstop:Topic name="AudioDecoder"/>
<wstop:Topic name=”Receiver”/>
<wstop:Topic name=”Monitoring”/>
</wstop:TopicNamespace>
```

with

All notifications referring to topics in the ONVIF topic namespace shall use the Message Format as described in Section 9.5.2.

9.2 Notification Streaming Interface

Remove the entire Section 9.2 in ONVIF Core specification and add the following text in ONVIF Media Service specification.

> The [WS-BaseNotification] defines the element wsnt:NotificationMessage to pack the Message Payload, the Topic and the ProducerReference. The structure of this message is the same as that for direct notification requests (the format is described in Section 9.4 of ONVIF Core specification). Multiple instances of the wsnt:NotificationMessage elements can be placed within a metadata document introduced in the Real-time Viewing section.
>
> There is no explicit SubscriptionReference with streaming notifications. Therefore, the wsnt:NotificationMessage shall not contain the SubscriptionReference element.

Remove old part in Section 5.1.2

Remove the following text in Section 5.1.2 in ONVIF Core specification.

> The service requirements for the different device types are defined in the device type specifications.

5.11.2 SerialPortConfiguration

Remove the whole Section 5.11.2 in ONVIF Device IO Service specification.

RemoveServerCertificateAssignment Behavior

In Advanced Security Service v1.1, Sect. 5.3.2.2 (Remove Server Certificate Assignment), append the paragraph

> If the TLS server on the device is enabled, the device shall produce a ReferenceExists fault and shall not remove the server certificate assignment."

In Advanced Security Service v1.1, Table 22 (RemoveServerCertificateAssignment command), append a row

> env:Sender
> ter:InvalidArgVal
> ter:ReferenceExists
> |
> A reference exists for the object that is to be deleted.

1593 Ambiguity in wsaw:Action and soapAction URL in Event WSDL

Replace the following part in event.wsdl

```
<soap:operation soapAction="
http://www.onvif.org/ver10/events/wsdl/EventPortType/GetServiceCapabilities "/>
```

with

```
<soap:operation
soapAction=" http://www.onvif.org/ver10/events/wsdl/EventPortType/GetServiceCapabi
litiesRequest "/>
```

1602 Additions for EXI to Media Service specification

According to the introduction of EXI metadata compression, add related parts into ONVIF Media Service specification.as follows.

2. Normative references

5.10 Metadata configuration

5.10. 1 Efficient XML Interchange (EXI)

1603 Additions for EXI to onvif.xsd

Add the following in MetadataCompressionType in onvif.xsd

```
<xs:enumeration value="EXI"/>
```

1604 Additions for EXI to media.wsdl

Add the following attribute in Capabilities in media.wsdl

```
<xs:attribute name="EXICompression" type="xs:boolean">
  <xs:annotation>
    <xs:documentation>Indicates the support for the Efficient XML Interchange (EXI)
binary XML format. </xs:documentation>
  </xs:annotation>
</xs:attribute/>
```

1605 Addition for EXI to Streaming specification

Add the following bullets in Section 5.2.1.1.3 in ONVIF Streaming specification.

- "vnd.onvif.metadaa.exi.onvif" for EXI using ONVIF default compression parameters
- "vnd.onvif.metadata.exi.ext" for EXI using compression parameters that are sent in-band

1565 Clarify device requirements on certificate fields

In the Advanced Security Service specification v1.1, Table 28 (Requirements implied by Capabilities), append the row

Capability: X.509Versions | Implied Requirements: If X.509v3 is supported, the device shall support the distinguished name attribute types country, organization, organizational unit, distinguished name qualifier, state or province name, common name, and serial number.

1615 Clarify the meaning of “TLS Server” in Advanced Security Service

In the Advanced Security Service Specification, Sect. 3.1 (Definitions),append a table row

TLS Server | TLS-enabled HTTP server (HTTPS)

1616 Deprecate GetPrivateKeyStatus

In the Advanced Security Service specification v1.1, Sect. 5.2.6.2.4 (Get Private Key Status)

- append the string “(deprecated)” to the headline of the section,
- append a paragraph "This command is deprecated. Use GetAllKeys (see Sect. 5.2.6.2.5) instead.”

In the Advanced Security Service specification v1.1, Sect. 5.4.4 (Capability-implied Requirements),

- capability RSAKeyPairGeneration: Remove "GetPrivateKeyStatus" from the implied requirements,
- capability PKCS8RSAKeyPairUpload: Remove "GetPrivateKeyStatus" from the implied requirements,
- capability PKCS12CertificateWithRSAKeyPairUpload: Remove "GetPrivateKeyStatus" from the implied requirements.

1617 Remove superseded requirements on supported signature algorithms

- In the Advanced Security Service Sect. 5.4.4 (Capability-implied requirements),
- Capability PKCS12CertificateWithRSAPrivateKeyUpload: Delete the requirement
- If true, SignatureAlgorithms shall not be empty

- Capability PKCS10ExternalCertificationWithRSA: Delete the requirement
- If true, SignatureAlgorithms shall not be empty
- Capability SelfSignedCertificateCreationWithRSA: Delete the requirement
- If true, SignatureAlgorithms shall not be empty

1618 Wrong command names in capabilities

In the Advanced Security Service spec v1.1, Sect. 5.4.4 (Capability-implied Requirements), capability TLSServerSupported,replace

AddTLSServerCertificateAssignment

with

AddServerCertificateAssignment

Replace

RemoveTLSServerCertificateAssignment

with

RemoveServerCertificateAssignment

Replace

ReplaceTLSServerCertificateAssignment

with

ReplaceServerCertificateAssignment

1619 Imprecise restrictions on capability

In the Advanced Security Service spec, Sect. 5.4.4 (Capability-implied requirements), "TLSServerSupported and PKCS10ExternalCertificationWithRSA", replace

If both TLSServerSupported and PKCS10ExternalCertificationWithRSA are true

with

If TLSServerSupported is non-empty and PKCS10ExternalCertificationWithRSA is true

1624 Add missing normative reference

Add the following normative reference in Chapter 2 in ONVIF Streaming specification.

IETF RFC 3016, RTP Payload Format for MPEG-4 Audio/Visual Streams <http://tools.ietf.org/html/rfc3016>

1639 Remove Media events from Device IO

Remove Section 5.13.3 Configuration Change in ONVIF Device IO Service specification.

1642 Relay Output Trigger

Replace the following paragraph in Section 5.13.2 in ONVIF Device IO Service specification

> A device that signals RelayOutputs in its capabilities should provide the Trigger event whenever its relay inputs change. An ONVIF compliant device shall use the following topic and message format:

with

> A device that signals RelayOutputs in its capabilities shall provide the Trigger event whenever a relay output state is changed. A device shall use the following topic and message format:

1647 Correct message definition of Media GetServiceCapabilities

Replace the following part in media.wsdl

```
<wsdl:message name="GetServiceCapabilitiesRequest">
    <wsdl:part name="parameter" element="tr2:GetServiceCapabilities"/>
</wsdl:message>
<wsdl:message name="GetServiceCapabilitiesResponse">
    <wsdl:part name="parameter" element="tr2:GetServiceCapabilitiesResponse2"/>
</wsdl:message>
```

with

```
<wsdl:message name="GetServiceCapabilitiesRequest">
    <wsdl:part name="parameters" element="tr2:GetServiceCapabilities"/>
</wsdl:message>
<wsdl:message name="GetServiceCapabilitiesResponse">
    <wsdl:part name="parameters" element="tr2:GetServiceCapabilitiesResponse2"/>
</wsdl:message>
```

1651 Inconsistency of fault codes observed for event filter in event service and search service

Add the following fault code column in Table 7 of Section 5.9 in ONVIF Recording Search Service specification.

env:Sender ter:InvalidArgVal ter:InvalidFilterFault	Provided Search filter expression was not understood or supported by the device.

1660 Recommendation for reasonable performance

Replace the following text in Section 5.3 in ONVIF PTZ Service specification

> This section describes three operations to move the PTZ unit absolutely, relatively or continuously. All operations require a ProfileToken referencing a Media Profile including a PTZConfiguration.
>
> All move commands are non-blocking, meaning they do not wait until the requested move operation has finished. The last move operation can be overwritten by sending another move request.

with

> This section describes three operations to move the PTZ unit absolutely, relatively or continuously. All operations require a ProfileToken referencing a Media Profile including a PTZConfiguration.
>
> All move commands shall be implemented non-blocking, meaning they shall not wait until the requested move operation has finished. The last move operation can be overwritten by sending another move request.
>
> Due to the wide range of physical devices this specification addresses, the specification does not require a specific response time to PTZ move operations. However, a device shall strive for minimal latency regarding PTZ move command request-to-response time. Note that the device controls command delay and video encoding delay; network delay and client delay also affect the user experience but cannot be controlled by the device.

1661 Correct reference in section 9.5

Replace the section reference 9.1.3 with 9.1.5 in the first paragraph in Section 9.5 in ONVIF Core specification.

1662 Correct reference in section 9.6

Replace the following text in Section 9.6 in ONVIF Core specification

> This standard extends the Topic framework defined in the [WS-Topics] specification. Section 9.7.1 describes an ONVIF Topic Namespace. Section 9.7.2 defines an interface to topic properties. This interface shall be implemented by an ONVIF compliant device. Section 9.7.3 incorporates the Message Description Language defined in section 9.5.4 into the TopicSet structure. All topics grown from the ONVIF Topic Namespace describes the type of a topic according to section 9.7.3. This section also defines the Topic Expression Dialects to be supported by a device.

with

> This standard extends the Topic framework defined in the [WS-Topics] specification.
> Section 9.6.1 describes the ONVIF Topic Namespace. Section 9.6.2 incorporates the Message Description Language defined in section 9.4.4 into the TopicSet structure, furthermore section 9.7 defines an interface that allows a client to get this information. A Topic Expression Dialects to be supported by a device is defined in section 9.6.3.

1663 Wrong reference in Section 9

Replace the following text in Section 9 in ONVIF Core specifiction

> ...
> Section 9.7 describes the integration of Topics and section
> 9.9 discusses the handling of faults.
>
> The last section demonstrates the usage of the Real-Time Pull-Point Notification Interface including Message Filtering and Topic Set.
> ...

with

> ...
> Section 9.7 describes the integration of Topics and section
> 9.10 discusses the handling of faults.

Section 9.11 demonstrates the usage of the Real-Time Pull-Point Notification Interface including Message Filtering and Topic Set.

...

1666 Wrongly assigned TemperatureCritical event

Move the following part in Section 8.8.5 in ONVIF Core specification

The following event should be generated with true value when the device reaches a temperature outside the normal range of operation, and should be generated with false value when the device returns to normal temperature range.

Topic: tns1:Monitoring/EnvironmentalConditions/TemperatureCritical

<tt:MessageDescription IsProperty="true">

<tt:Data>

<tt:SimpleItemDescription Name="Critical" Type="xs:boolean"/>

</tt:Data>

</tt:MessageDescription>

to Section 8.8.10 and then update the topic to the following

Topic: tns1:Device /HardwareFailure/TemperatureCritical

Correct all the occurrences of "tns1:Motoring/HardawareFailure/***Failure" into "tns1:Device/Hardware/***Failure"

Remove the following topics in Section 8.8.8

tns1:Device/HardwareFailure/FanFailure

tns1:Device/HardwareFailure/PowerSupplyFailure

tns1:Device/HardwareFailure/StorageFailure

tns1:Device/HardwareFailure/TemperatureCritical

1668 2.5 documentation doesn't mention PTZ MoveStatus or StatusPosition capabilities

The following columns should be added in Section 5.10 in ONVIF PTZ Service specification.

MoveStatus Indicates that the PTZVector includes MoveStatus information.

StatusPosition Indicates that the PTZVector includes Position information.