Driving IP-based physical security through global standardization

ONVIF™

ONVIF Specification Version 2.4.2
Release Notes

1. Summary

The ONVIF 2.4.2 release incorporates 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

In this maintenance release, there is no new service addition in the network specification set.

3. Changes

Find below all errata from Version 2.4.1 to 2.4.2 in order to improve interoperability. The numbers correspond to the Change Request ticket numbers and are not necessarily continuously ascending.

Note that three changes to the advanced security methods CreatePKCS10CSR, CreateSelfSignedCertificate and UploadCertificate include newer options that may not be supported by devices implemented according to the first two releases of the respective specification.

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

1050 Clarification for rotate feature

In section 5.23.8 in ONVIF Media service specification, add the following.

What resolutions a device supports shall be unaffected by the Rotate parameters.
OSDs shall be unaffected by the Rotate parameters.

If a device is configured with Rotate=AUTO, the device shall take control over the Degree parameter and automatically update it so that a client can query current rotation.

The device shall automatically apply the same rotation to its pan/tilt control direction if the following condition is true.

- if Reverse=AUTO in PTControlDirection
- or if the device doesn’t support Reverse in PTControlDirection

1229 Clarification on Response of EndSearch for FindRecordings - Search Session

In section 5.16 in ONVIF Recording Search service specificatoin, replace the following sentence

> If the search was completed the original EndPoint supplied by the Find operation shall be returned. This operation is mandatory to support for a device implementing the recording search service.

By

> If the search was completed the original EndPoint supplied by the Find operation shall be returned. When issuing EndSearch on a FindRecordings request the EndPoint is undefined and shall not be used since the FindRecordings request doesn't have StartPoint/EndPoint.

1238 Inconsistency between SetScopes and AddScopes

In section 8.3.15 in ONVIF Core Specification, remove a row which refers to ter:ScopeOverwrite from table 52.

In section 8.3.14 in ONVIF Core Specification, replace the following paragraph

> Fixed scope parameters cannot be altered through the device management interface but are permanent device characteristics part of the device firmware configurations. The scope type is indicated in the scope list returned in the get scope parameters response. Configurable scope parameters can be set throught the set and add scope parameters operations, see Section 8.3.14 and Section 8.3.15. The device shall support retrieval of discovery scope parameters through the GetScopes command. As some scope parameters are mandatory, the client always expects a scope list in the response.

By

> Fixed scope parameters are permanent device characteristics and cannot be removed through the device management interface. The scope type is indicated in the scope list returned in the get scope parameters response. A device shall support retrieval of discovery scope parameters through the GetScopes command. As some scope parameters are mandatory, the device shall return a non-empty scope list in the response.

1241 Clarification required for GetServicesResponse

In section 8.1.2.1 in ONVIF Core specification, add the following paragraph.

> The version in GetServicesResponseshall contain the specification version number of the corresponding service that is implemented by a device.

1244 Clarification for the behavior in SetHostnameFromDHCP

In section 8.2.3 in ONVIF Core specification, add the following sentences in the second paragraph.

A device shall accept the command independent whether it is currently using DHCP to retrieve its IPv4 address or not. Note that the device is not required to retrieve its hostname via DHCP while the device is not using DHCP for retrieving its IP address. In the latter case the device may fall back to the statically set hostname.

1268 Allow sets of AttributeTypeAndValue in RelativeDistinguishedNames

Expand tas:DistinguishedName to allow entry of multi-valued RDNs. First, define a MultiValuedRDN type: Add

<xs:complexType name=MultiValuedRDN">
<xs:annotation>
<xs:documentation>A multi-valued RDN</xs:documentation>
</xs:annotation>
<xs:sequence>
<xs:element minOccurs="0" maxOccurs="unbounded" name="Attribute"
type="tas:DNAttributeTypeAndValue">
<xs:annotation>
<xs:documentation>A list of types and values defining a multi-valued RDN</xs:documentation>
</xs:annotation>
</xs:element>
</xs:sequence>
</xs:complexType>

Then at the end of the tas:DistinguishedName definition, after GenericAttribute and before anyAttribute, add

<xs:element minOccurs="0" maxOccurs="unbounded" name="MultiValuedRDN"
type="tas:MultiValuedRDN">
<xs:annotation>
<xs:documentation>A multi-valued RDN</xs:documentation>
</xs:annotation>
</xs:element>

1273 Typo in wsdl documentation

There are mistakes in the documentation for notValidBefore and notValidAfter. In advancedSecurity.wsdl, change

The X.509 not validValidBefore information

to

The X.509 not valid before information

Change

The X.509 not validValidAfter information

to

The X.509 not valid after information

1276 Additional fault codes for CreatePKCS10CSR and CreateSelfSignedCertificate

In Table 24 (Advanced Security service specific fault codes), add

env:Sender
ter:InvalidArgVal
ter:InvalidSubject
Subject invalid
The specified subject is invalid or incomplete.
env:Sender
ter:InvalidArgVal
ter:InvalidAttribute
Attribute invalid
The specified attribute is invalid or incomplete.
env:Sender
ter:InvalidArgVal
ter:InvalidDateTime
dateTime invalid
The specified dateTime is invalid.

In Sect. 5.2.6.2.1 (Create PKCS#10 Certification Request), append to the paragraph starting with "The signature algorithm parameter determines"

If the specified subject is invalid or incomplete, a Subject invalid fault shall be produced and no CSR shall be created. If an attribute is invalid or incomplete, an Attribute invalid fault shall be produced and no CSR shall be generated.

In Table 6 (CreatePKCS10CSR command), add

env:Sender
ter:InvalidArgVal
ter:InvalidSubject
& The specified subject is invalid or incomplete.

env:Sender
ter:InvalidArgVal
ter:InvalidAttribute
& The specified attribute is invalid or incomplete.

In Sect. 5.2.6.2.2 (Create Self-Signed Certificate), add before the paragraph starting with "The notValidBefore parameter"

If the specified subject is invalid or incomplete, a Subject invalid fault shall be produced and no certificate shall be created.

In Sect. 5.2.6.2.2 (Create Self-Signed Certificate), append to the paragraph starting with "The notValidBefore parameter"

If the notValidBefore parameter is invalid, an invalid DateTime fault shall be produced and no certificate shall be generated.

If the notValidAfter parameter is invalid, an invalid DateTime fault shall be produced and no certificate shall be generated.

In Table 7 (CreateSelfSignedCertificate command), add

env:Sender
ter:InvalidArgVal
ter:InvalidSubject
& The specified subject is invalid or incomplete.
env:Sender
ter:InvalidArgVal
ter:InvalidDateTime
& A specified dateTime is invalid.

1290 PullMessages several active requests from a client

In section 9.2.2 in ONVIF Core specification, add the following paragraph in the last paragraph.

A device should return an error (UnableToGetMessagesFault) when receiving a PullMessages request for a subscription where a blocking PullMessage request already exists.

1292 Clarification for requirement of audio recording

In section 5.4 in ONVIF Recording Control service specification, replace the following sentence

The new recording shall be created with one video, one audio and one metadata track.

By

The new recording shall be created with a track for each supported TrackType see section 5.21.

In section 5.21, also replace the following

Encoding Indication which encodings are supported for recording. The list may contain one or more enumeration values of tt:VideoEncoding and tt:AudioEncoding.

By

Encoding Indication which encodings are supported for recording. The list may contain one or more enumeration values of tt:VideoEncoding and tt:AudioEncoding. If device does not support audio recording tt:AudioEncoding shall not be listed.

In section 5.21, add the following capability.

MetadataRecording Indication if the device supports to record metadata.

In recording.wsdl, add the following capability

```
<xs:attribute name="MetadataRecording" type="xs:boolean">
<xs:annotation>
      <xs:documentation>Indication if the device supports
recordingmetadata.</xs:documentation></xs:annotation>
</xs:attribute>
```

1298 Add informative example section for Recording Job priorities

In Annex A in ONVIF Recording Control service specification, replace the following

Annex A. Revision History

By

Annex B. Revision History

Newly introduce Annex A as follows.

Annex A. Example scenario for Recording Job Priority (Informative)

This annex describes a scenario for Multiple Recording Jobs configured to record data into a single recording.

As described in Section 5.3.3, "If there are two recording jobs with the same priority, the device shall record the data corresponding to the recording job that was activated the latest."

Accordingly, a device supporting Multiple Recording Jobs is required to change the Job Modes of Recording Jobs with respect to Priority, as described below :

Step 1: A Recording Job ‘J1’ with Priority ‘1’ is created in 'Active' mode
Job Modes of Recording Jobs after Step 1:
Recording Job ‘J1’ = ACTIVE

Step 2: A new Recording Job ‘J2’ with Priority ‘1’ is now created in 'Active' mode
Job Modes of Recording Jobs after Step 2:
Recording Job ‘J1’ = IDLE
Recording Job ‘J2’ = ACTIVE

Step 3 : Another Recording Job ‘J3’ with higher Priority ‘2’ is now created in 'Active' mode. Because it has a higher priority than J2, it takes precedence.
Job Modes of Recording Jobs after Step 3:
Recording Job ‘J1’ = IDLE
Recording Job ‘J2’ = IDLE
Recording Job ‘J3’ = ACTIVE

Step 4. Recording Job ‘J3’ is now deleted, 'J1' and 'J2' are both at the highest priority, so Section 5.14 applies, and the device can activate either 'J1' or 'J2'.
Job Modes of Recording Jobs after Step 4, possibility 1:
Recording Job ‘J1’ = ACTIVE
Recording Job ‘J2’ = IDLE
Job Modes of Recording Jobs after Step 4, possibility 2:
Recording Job ‘J1’ = IDLE
Recording Job ‘J2’ = ACTIVE

1299 Infrastructure network defined but not used

In section 3.1 in ONVIF Core specification, remove the term Infrastructure network definition from the the definition table.

1300 Normative reference to xpath is missing

In chapter 2 in ONVIF Core specification, add the following reference.

W3C XML Path Language (XPath) Version 1.0
<http://www.w3.org/TR/xpath/>

1301 Add missing abbreviations

In section 3.2 in ONVIF Core specification, add the following abbreviations.

API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
LAN	Local Area Network
XPath	XML Path Language

1302 Minor editorial fixes

In section 8.2.22.4.2 in ONVIF Core specification, replace the following sentence.

To minimise the risk for compromising the PSK the device should not transmit any PSK to a client, furthermore it shall not return the PSK in a response to a GetNetworkInterfaces operation call.

By

To minimize the risk for compromising the PSK the device should not transmit any PSK to a client, furthermore it shall not return the PSK in a response to a GetNetworkInterfaces operation call.

In section 8.4.13 in ONVIF Core specification, replace the following sentence.

A device that support *onboard* key pair generation that supports either TLS or IEEE 802.1X using client certificate shall support this command.

By

A device that support *onboard* key pair generation and that supports either TLS or IEEE 802.1X using client certificate shall support this command.

In section 8.4.17 in ONVIF Core spefication, replace the following sentence.

A device that support onboard key pair generation may support this command.

By

A device that supports onboard key pair generation may support this command.

In Seek operation section (chapter 9) in ONVIF Core specification, replace the following sentence.

When Seek is used the in forward mode a device shall position the pull pointer to include all NotificationMessages in the persistent storage with a UtcTime attribute greater than or equal to the Seek argument.

By

When Seek is used in the forward mode a device shall position the pull pointer to include all NotificationMessages in the persistent storage with a UtcTime attribute greater than or equal to the Seek argument.

And also replace the following sentence.

When Seek is used in reverse mode a device shall position the pull pointer to include all NotificationMessages in the in the persistent storage with a UtcTime attribute less than or equal to the Seek argument.

By

When Seek is used in reverse mode a device shall position the pull pointer to include all NotificationMessages in the persistent storage with a UtcTime attribute less than or equal to the Seek argument.

In Annex C in ONVIF Core specification, replace the following

The following is an example response for GetServices which

By

The following is an example response for GetServices :

1303 Contradicting requirement in GetUsers behavior

In section 8.4.3 in ONVIF Core specification, replace the following

This operation lists the registered users and along with their user levels. The device shall support retrieval of registered device users and their credentials for authentication through the GetUsers command.

By

This operation lists the registered users and along with their user levels. The device shall support retrieval of registered device users through the GetUsers command.
Furthermore a device shall not return the credentials (password) in the reply.

And also, replace the following sentence in Table 64

i.e, the username password is not included into the response.

By

NOTE: The password is not included in the response even if it is present in the tt:User type.

1304 Ambiguity in RecordingJobConfiguration->Priority

In section 5.3.3 in ONVIF Recording Control service specification, replace the following word

This shall be a positive number.

By

This shall be a non-negative number.

Also apply the same change in section 5.25.14.

1305 Invert transform y value in the example

In Annex. B2 in ONVIF Analytics service specification, replace the following

```
<tt:Transformation>
       <tt:Translate x="-0.66666" y="-0.6" />
       <tt:Scale x="0.1666666" y="-0.2" />
</tt:Transformation>
```

By

```
<tt:Transformation>
       <tt:Translate x="-0.66666" y="0.6" />
       <tt:Scale x="0.1666666" y="-0.2" />
</tt:Transformation>
```

1308 Update capability reference for auxiliary operation

In section 8.6 in ONVIF Core specification, replace the following paragraph

The supported commands can be retrieved by the AuxiliaryData parameter which derives from GetCapabilities command response. The command transmitted by using this command should match one of the supported commands listed in the AuxiliaryData response. If the capability command response lists only irlampon command, then the SendAuxiliaryCommand argument will be irlampon, which may indicate turning the connected IR lamp on.

By

The commands supported by the device is reported in the AuxiliaryCommands attribute returned by the capabilites commands, see section 8.1.2. The command transmitted by using this command should match one of the commands supported by the device. If for example the capability command response lists only irlampon command, then the SendAuxiliaryCommand argument will be irlampon, which may indicate turning the connected IR lamp on.

1309 GetCapabilites in core specification / wsdl

In section 8.1.2 in ONVIF Core specification, remove the following sentence.

The device shall indicate all its ONVIF compliant capabilities through the GetCapabilities command.

In devicemgmt.wsdl, remove the following sentence from wsdl:documentation in GetZeroConfiguration.

Use GetCapalities to check if zero-zero-configuration is supported.

1311 Wrong explanation of remote discovery capability in wsdl / schema

In onvif.xsd and devicemgmt.wsdl, remove the following from wsdl annotation text in both tt:SystemCapabilities and tds:SystemCapabilities.

see WS-Discovery

1323 MetadataStream documentation error

In section 5.1.2 in ONVIF Streaming specification, replace all the occurrences of

tt:MetaDataStream

By

tt:MetadataStream

And also replace all the occurences of

wsnt:NotficationMessage

By

wsnt:NotificationMessage

1325 Improve Event Specification Section.

Section 9 has been reorganized to improve the overall readability of the section:

Section 9.1 has been moved to 9.3

Section 9.2 has become 9.1

Section 9.3 has become 9.2

Section 9.9 has been moved to 9.1.7

New sections 9.1.3 Renew, 9.1.4 Unsubscribe and 9.1.6 Pull Point Lifecycle have been added in order

to clearly distinguish between informative and normative sections.

1326 Unused simpleElement in advancedsecurity.wsdl

The first simpleElement defined in advancedsecurity.wsdl is ID, restricted to an xs:token. Then the IDs (KeyID, CertificateID, and CertificationPathID) are defined restricted by xs:ID, not by tas:ID. Delete the definition of tas:ID from advancedsecurity.wsdl.

1330 Add reference to corrigendum

In chapter 2 in ONVIF Export File Format specification, add the following reference.

ISO/IEC 23000-10/Cor 2:2014 Information technology – Multimedia application format – Part 10: Surveillance application format - Technical Corrigendum 2

1342 Clarification for RTSP over HTTP port

In section 5.15.1 in ONVIF Media service specification, add the following paragraph.

On a request for transport protocol http a device should return a url that uses the same port as the web service. This enables seamless NAT traversal.

1347 Fix abbreviation section

In section 3.2 in ONVIF Access Control service specification, replace the following respectively.

HTTP	Hypertext Transfer (or Transport) Protocol
REX	Request to exit
TLS	Transport Level Security
VMS	Video Management (or Monitoring) System

By

HTTP	Hypertext Transfer Protocol
REX	Request To Exit
TLS	Transport Layer Security
VMS	Video Management System

1348 A lot of spaces are missing

In various section in ONVIF Access Control service specification, correct the wording something like the following by adding proper space in-between.

bedefined
ONVIFfunctionality
However,futureversions
partofAccess
foraccessing
connectionis
eventsas

1349 Typo in Advanced Security ter:NoPrivateKey description

In table 16 of the Advanced Security Service Specification, replace the following

… certification path (i.e., the server certificate), does not …

By

… certification path (i.e., the server certificate) does not …t

1350 Incorrect grammar in ter:OldCertificationPathID

In several places in the Advanced Security Service Specification, replace

associated to

By

associated with

1351 Incorrect Namespace in Key Status description

In section 5.5.1 in the Advanced Security Service Specification, replace

xs:KeyID

By

tas:KeyID

And also replace

xs:KeyStatus

By

tas:KeyStatus

1355 "AccessPoint" / "Access Point" should be "access point"

In section 3.1 in ONVIF Access Control service specification, correct all the occurrences of either "AccessPoint" or "Access Point" in "Access Point Disable" definition by "access point".

1352 Aliases in UploadCertificate

Add to table 8 of the ONVIF Advanced Security Service Specification

xs:string KeyAlias[0][1]

In Sect. 5.2.6.2.3 (UploadCertificate), in front of "How the link between the uploaded certificate..."
add

The device shall assign the supplied Alias to the uploaded certificate.
If a new key pair is generated, the device shall assign the supplied KeyAlias to it. Otherwise, the device shall ignore an eventually supplied KeyAlias.

In advancedsecurity.wsdl, definition of element "UploadCertificate"
add after element Alias

```
<xs:element name="KeyAlias" type="xs:string" minOccurs="0>
 <xs:annotation>
  <xs:documentation>The client-defined alias of the key pair
  </xs:documentation>
 </xs:annotation>
</xs:element>
```

1357 Remove empty page

In ONVIF Access Control service specification, remove all the excessive line break which lead to empty page etc..

1358 Update correct section reference

In section 4.3 in ONVIF Access Control service specification, replace the following sentence

Please refer to ONVIF Core specification for details on event delivery mechanism and section 5.1 for the list of events defined by this document.

By

Please refer to ONVIF Core specification for details on event delivery mechanism and section 6 for the list of events defined by this document.

1359 Missing capability of "Misc - AuxiliaryCommands"

In section 8.1.2.2 in ONVIF Core specification, add the following row in Table 12.

Misc AuxiliaryCommands List of commands supported by SendAuxiliaryCommand

1360 Description of ter:InvalidPresetTour different

In section 5.8.5 in ONVIF PTZ service specification, replace the following

The suggested PresetTour includes invalid parameter(s).

By

The requested PresetTour includes invalid parameter(s).

1361 Typo in OperatePresetTour command

In section 5.8.6 in ONVIF PTZ service specification, replace the following from Table 26.

tt:PresetTourToken

By

tt:ReferenceToken

1362 Remove meaningless sentence in ModifyPresetTour command

In section 5.8.5 in ONVIF PTZ service specification, remove the following sentence in the first paragraph.

This is a read-only parameter.

1363 Simplify mandatory requirement

In ONVIF Access Control service specification, replace all the occurrences of

An ONVIF compliant device (that provides the Access Control service) shall implement this method.

By

A device shall support this method.

which are present in 5.1.2, 5.2.2, 5.2.3, 5.3.2, 5.3.3 and 5.4.2.

In section 5.2.1.1, replace the following sentence

An ONVIF compliant device shall provide the following fields for each AccessPoint instance

By

A device shall provide the following fields for each AccessPoint instance

In section 5.3.1.1 and 5.4.1.1, replace the following sentence

An ONVIF compliant device shall provide the following fields for each AccessPoint instance

By

A device shall provide the following fields for each AccessPoint instance

In section 5.5.2 and 5.5.3, replace the following sentence

A device that signals support forDisableAccessPoint capability for a particular AccessPoint instance shall implement this command.

By

A device that signals support for DisableAccessPoint capability for a particular AccessPoint instance shall support this command.

In section 5.5.4, replace the following sentence

A device that signals support forExternalAuthorization capability for a particular AccessPoint instance shall implement this command.

By

A device that signals support for ExternalAuthorization capability for a particular AccessPoint instance shall support this command.

In section 6.2.1, replace the following sentence

an ONVIF compliant device shall provide a corresponding eventmessage as per the following sub-sections.

By

a device shall provide a corresponding event message as per the following sub-sections.

In section 6.8.1, replace the following sentence

An ONVIF compliant device shall use the topics defined in this section associated with the respective message description.

By

A device shall use the topics defined in this section associated with the respective message description.

In section 6.9, replace the following sentence

Whenever configuration data has been changed, added or been removed an ONVIF compliant device shall provide these events to inform subscribed clients.

By

Whenever configuration data has been changed, added or been removed a device shall provide these events to inform subscribed clients.

1364 Missint "not"

In section 6.4.3 in ONVIF Access Control service specification, replace the following setntence

When the device detects that access is taken and the credential can be identified, it shall provide the following event:

By

When the device detects that access is not taken and the credential can be identified, it shall provide the following event:

1365 Missing ":" in table caption

In all the table captions in ONVIF Access Control service specification, correct the following table caption.

Table X <title of the table>

By

Table X: <title of the table>

1366 Hanging paragraph

In section 5.1, 5.4, 5.5, 6.8 and 6.9 in ONVIF Access Control service specification, add General sub-section and then move the entire content up to the subsequent (sub-)section.

In section 6.8, replace the following

> The device shall provide these events to inform

By

> The device shall provide the status change events to inform

In chapter 6, remove the initial paragraph and then move section 6.1.1 to 6.2.

1367 Remove "(Informative)"

In section 6.1 in ONVIF Access Control service specification, remove "(Informative)" from the section header.

1368 Add normative requirement sentence

In section 5.4.6 in ONVIF Door Control service specification, add the following sentence in the first paragraph.

> A device that signals support for LockDown capability for a particular Door instance shall support this command.

In section 5.4.8, add the following sentence in the first paragraph.

> A device that signals support for LockOpen capability for a particular Door instance shall support this command.

1369 Simplify mandatory requirement

In ONVIF Door Control service specification, replace all the occurrences of the following sentence

> An ONVIF compliant device which provides the Door Control service shall implement this method.

By

> A device shall support this command.

In section 5.3.2, replace the following sentence

> A device implementing the Door Control service shall be capable of reporting the status of a door using a DoorState structure available from the GetDoorState command.

By

> A device shall be capable of reporting the status of a door using a DoorState structure available from the GetDoorState command.

In ONVIF Door Control service specification, replace all the occurrences of the following sentence

> A device that signals support for <*> capability for a particular Door instance shall implement this method

By

> A device that signals support for <*> capability for a particular Door instance shall support this command

1371 Correct fonts

In section 5.6 in ONVIF Core specification, correct fonts in the following sentences.

> The fault codes listed in the tables are the specific fault codes that can be expected from the command, see 5.11.2.2. Any command can return a generic fault, see 5.11.2.2.

1372 User level shouldn't be defined inside default access policy

In ONVIF Core specification, create a new section 5.12.1.1 User Levels and move the following part from the original 5.12.1.1.

> Each user is associated exactly one of the following user levels:
>
> 1. Administrator
> 2. Operator
> 3. User
> 4. Anonymous
>
> Unauthenticated users are placed into the anonymous category and a device shall not allow users to be added to the anonymous user level category.

1373 Remove hanging paragraphs

In ONVIF Core specification, apply the following changes.

Add section 5.1.1 General, containing everything between 5.1 and the old 5.1.1.

Add section 5.6.1 General, containing everything between 5.6 and the old 5.6.1.

Add section 5.11.2.1 General, containing everything between 5.11.2 and the old 5.11.2.1

Add section 7.3.2.2.1 General, containing everything between 7.3.2.2 and the old 7.3.2.2.1

Add section 8.1.2.1 General, containing everything between 8.1.2 and the old 8.1.2.1.

Add section 5.12.1 Authentication, containing everything between 5.12 and the old 5.12.1.

And also update the referenced section numbers accordingly.

1374 Wrong section reference in 7.3.2.3 Hello

In section 7.3.2.3 in ONVIF Core specification, replace the following sentence

The IP addressing configuration principles for a device are defined in 5.12.2.1.1.

By

The IP addressing configuration principles for a device are defined in6.

1375 Access classes shouldn't be defined inside default access policy

In ONVIF Core specification, create a new section Access classes for service requests just before Default access policy section (5.12.1.1) and move the following part from the original section.

·PRE_AUTH

The service shall not require user authentication.

Example: GetEndpointReference

·READ_SYSTEM

The service reads system configuration information from the device.

Example: GetNetworkInterfaces

·READ_SYSTEM_SENSITIVE

The service reads sensitive (but not really confidential) system configuration information from the device.

·READ_SYSTEM_SECRET

The service reads confidential system configuration information from the device.

Example: GetSystemLog

·WRITE_SYSTEM

The service causes changes to the system configuration of the device.

Example: SetNetworkDefaultGateway

·UNRECOVERABLE

The service causes unrecoverable changes to the system configuration of the device.

Example: SetSystemFactoryDefault

·READ_MEDIA

The service reads data related to recorded media.

Example: GetRecordings

·ACTUATE

The service affects the runtime behaviour of the system.

Example: CreateRecordingJob

Table 7: Access class to user level mapping

	Administrator	Operator	User	Anonymous
PRE_AUTH	X	X	X	X
READ_SYSTEM	X	X	X	
READ_SYSTEM_SENSITIVE	X	X		
READ_SYSTEM_SECRET	X			
WRITE_SYSTEM	X			
UNRECOVERABLE	X			
READ_MEDIA	X	X	X	
ACTUATE	X	X		

Insert the following introduction paragraph.

The service requests are classified into access classes based to their impact. The following access classes are defined:

Also the following paragraph between the bullets and table above.

Table 7 defines for each access class which user levels are allowed access. A user of level c shall be granted access to a service request associated to access class r if and only if an "X" is present in the cell at column c and row r.

1376 Missing normative requirement

In section 5.4.1 in the Advanced Security Service Specification, add

A device shall support this command.

1377 Key Status Event

In section 5.5.1 in the Advanced Security Service Specification, replace

A device should provide information about key status changes through key status events.

By

A device that indicates support for key handling via the MaximumNumberOfKeys capability shall provide information about key status changes through key status events.

A device shall include an OldStatus value unless NewStatus is generating.

And also remove

<xs:annotation>
<xs:documentation>The old status shall be included in the event unless NewStatus=”generating”.
</xs:documentation>
</xs:annotation>

1412 Move formerly proposed clarification sentence to the correct position

In Table 18 in ONVIF Recording Control service specification, move the following sentence to the *Spare* attribute explanation portion.

By setting none of the Spare attribute the device signals that no job can be created.

1378 Mandate support for SHA2

In the Advanced Security Service Specification, Sect. 2 (Normative References), add

RFC 4055
Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
< http://www.ietf.org/rfc/rfc4055.txt>

In the Advanced Security Service Specification, Sect. 5.2.6.2.1 (Create PKCS#10 Certification Request), replace

A device that supports this command shall as minimum support the sha-1WithRSAEncryption signature algorithm as specified in [RFC 3279]. Furthermore, if no signature algorithm is specified in the request, adevice shall use the sha1-withRSAEncryption signature algorithm for creating the signature.

with

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 the Advanced Security Service Specification, Table 6 (CreatePKCS10CSR command), replace

tas:AlgorithmIdentifier SignatureAlgorithm[0][1]

with

tas:AlgorithmIdentifier SignatureAlgorithm[1][1]

In the Advanced Security Service Specification, Sect. 5.2.6.2.2 (Create Self-Signed Certificate), replace

A device that supports this command shall as minimum support the sha-1WithRSAEncryption signature algorithm as specified in [RFC 3279]. Furthermore, if no signature algorithm is specified in the request, a device shall use the sha1-withRSAEncryption signature algorithm for creating the signature.

with

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 the Advanced Security Service Specification, Table 7 (CreateSelfSignedCertificate command), replace

tas:AlgorithmIdentifier SignatureAlgorithm[0][1]

with

tas:AlgorithmIdentifier SignatureAlgorithm[1][1]

In the Advanced Security Service Specification, Sect. 5.2.6.2.3 (Upload Certificate), replace

A device that supports this command shall support sha1-WithRSAEncryption as certificate signature algorithm.

with

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 the Advanced Security Service Specification, Table 25 (configuration options of cryptographic protocols), replace

sha-1WithRSAEncryption

with

sha1WithRSAEncryption，sha256WithRSAEncryption

In the Advanced Security Service Specification, Sect. 6 (Security Considerations), replace

However, since the security of the SHA-1 algorithm is under question, it is strongly recommended that newer implementations of this specification support a signature algorithm

based on SHA-256, e.g., sha256WithRSAEncryption as specified in [RFC 4055].

with

However, since the security of the SHA-1 algorithm is under question, this specification mandates that a signature algorithm based on SHA-256, particularly sha256WithRSAEncryption as specified in [RFC 4055], be supported in addition.

In advancedsecurity.wsdl, element CreatePKCS10CSR, replace

<xs:element name="SignatureAlgorithm" minOccurs="0" type="tas:AlgorithmIdentifier">

with

<xs:element name="SignatureAlgorithm" type="tas:AlgorithmIdentifier">

In advancedsecurity.wsdl, element CreateSelfSignedCertificate, replace

<xs:element name="SignatureAlgorithm" minOccurs="0" type="tas:AlgorithmIdentifier">

with

<xs:element name="SignatureAlgorithm" type="tas:AlgorithmIdentifier">

1379 Fault not mentioned in command specification

In the Advanced Security Service specification, Sect. 5.2.6.2.3 (Upload Certificate), replace

If the key pair that the certificate shall be linked to does not have status ok, an InvalidKeyID fault is produced, and the uploaded certificate is not stored in the keystore.

with

If the key pair that the certificate shall be linked to does not have status ok, an InvalidKeyID fault is produced, and the uploaded certificate is not stored in the keystore.

If the signature algorithm that the signature of the supplied certificate is based on is not supported by the device, the device shall generate an UnsupportedSignatureAlgorithm fault and shall not store the uploaded certificate nor the contained public key in the keystore.

1380 Non-normative language with certificate trust definition in Upload Certificate

In the Advanced Security Service specification, Sect. 5.2.6.2.3 (Upload Certificate), replace

This operation shall not mark the uploaded certificate as trusted.

with

The device shall not mark the uploaded certificate as trusted.

1381 Non-normative language with certificate trust definition in Create Self-signed Certificate

In the Advanced Security Service specification, Sect. 5.2.6.2.2 (Create Self-signed Certificate), replace

> This operation shall not mark the uploaded certificate as trusted.

with

> The device shall not mark the uploaded certificate as trusted.

1382 Clarify requirements level for capability-implied requirements

In the Advanced Security Service Specification, Table 23 (Requirements implied by Capabilities), replace

> The following table summarizes for each capability the requirements that a device signaling this capability must satisfy.

with

> Table 23 summarizes for each capability the minimum requirements that a device signaling this capability shall satisfy; it should not be seen as a recommendation.

1383 Use "shall" instead of "must" in normative spec parts

In all normative sections of the Advanced Security Service specification, replace

> must

with

> shall

1390 Restriction on DNAttributeValue

In Sect. 5.6 (service specific data types) of the advanced security service specification and the corresponding part in advancedsecurity.wsdl, replace

```
<xs:simpleType name="DNAttributeValue">
<xs:restriction base="xs:string">
<xs:annotation>
<xs:documentation>The distinguished name attribute values shall be encoded in hexadecimal form as specified in RFC 4514.</xs:documentation>
</xs:annotation>
</xs:restriction>
</xs:simpleType>
```

with

<xs:simpleType name="DNAttributeValue">
<xs:restriction base="xs:string">
<xs:annotation>
<xs:documentation>The distinguished name attribute values are encoded in UTF-8 or in hexadecimal form as specified in RFC 4514.
</xs:documentation>
</xs:annotation>
</xs:restriction>
</xs:simpleType>

In Sect. 5.2.6.2.2 (Create Self-Signed Certificate) of the Advanced Security Service Specification, after the paragraph starting with "The Extensions parameter specifies potential X509v3 extensions...", add the paragraphs

Distinguished name attribute values shall be supplied either in UTF-8 or in hexadecimal form as specified in RFC 4514.

If the distinguished name attribute value is supplied in hexadecimal form, the device shall encode the attribute in the format given in the hexadecimal format.

If the distinguished name attribute value is supplied in UTF-8 and the attribute value has a uniquely defined encoding (e.g., CountryName is defined as PrintableString), the device shall encode the attribute as the defined encoding. Otherwise, the device shall encode the attribute value as UTF-8.

In Sect. 5.2.6.2.1 (Create PKCS10 Certification Request) of the Advanced Security Service Specification, after the paragraph starting with "The subject parameter describes the entity...", add the paragraphs

Distinguished name attribute values shall be supplied either in UTF-8 or in hexadecimal form as specified in RFC 4514.

If the distinguished name attribute value is supplied in hexadecimal form, the device shall encode the attribute in the format given in the hexadecimal format.

If the distinguished name attribute value is supplied in UTF-8 and the attribute value has a uniquely defined encoding (e.g., CountryName is defined as PrintableString), the device shall encode the attribute as the defined encoding. Otherwise, the device shall encode the attribute value as UTF-8.

1409 Add newly predefined auxiliary commands

In section 8.6 in ONVIF Core specification, add the following AuxiliaryCommands to control an IR illuminator attached to an ONVIF compliant device.

tt:IRLamp|On – Request to turn ON an IR illuminator attached to the unit.

tt:IRLamp|Off – Request to turn OFF an IR illuminator attached to the unit.

tt:IRLamp|Auto – Request to configure an IR illuminator attached to the unit so that it automatically turns ON and OFF.