

**ONVIF<sup>TM</sup>**

**ONVIF Specification Version 2.5  
Release Notes**

© 2008-2014 by ONVIF™ All rights reserved.

Recipients of this document may copy, distribute, publish, or display this document so long as this copyright notice, license and disclaimer are retained with all copies of the document. No license is granted to modify this document.

THIS DOCUMENT IS PROVIDED "AS IS," AND THE CORPORATION AND ITS MEMBERS AND THEIR AFFILIATES, MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THIS DOCUMENT ARE SUITABLE FOR ANY PURPOSE; OR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

IN NO EVENT WILL THE CORPORATION OR ITS MEMBERS OR THEIR AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, ARISING OUT OF OR RELATING TO ANY USE OR DISTRIBUTION OF THIS DOCUMENT, WHETHER OR NOT (1) THE CORPORATION, MEMBERS OR THEIR AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR (2) SUCH DAMAGES WERE REASONABLY FORESEEABLE, AND ARISING OUT OF OR RELATING TO ANY USE OR DISTRIBUTION OF THIS DOCUMENT. THE FOREGOING DISCLAIMER AND LIMITATION ON LIABILITY DO NOT APPLY TO, INVALIDATE, OR LIMIT REPRESENTATIONS AND WARRANTIES MADE BY THE MEMBERS AND THEIR RESPECTIVE AFFILIATES TO THE CORPORATION AND OTHER MEMBERS IN CERTAIN WRITTEN POLICIES OF THE CORPORATION.

# 1. Summary

The ONVIF 2.5 release 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

The following functionality has been added to the service specification:

- Off-device key generation

### 2.2 Analytics Service

The Specification has been extended to support Query Rules. Query Rules allows a client to define queries on streamed metadata of multimedia streams. The client subscribes to the topic associated with the rule to receive notifications from a device.

### 2.3 Core Specification and Recording Control Service

New APIs are introduced to the Device Management Service to cover configuration functions for storage. New APIs are also introduced to Recording Control Service to export the recordings.

### 2.4 Imaging Service

Configuration data is enhanced to cover configuration of Tone Compensation and Defogging features.

## 2.5 Media Services

The Configuration and Streaming of compressed Metadata has been added to the Media Service and the Streaming Specifications.

## 2.6 PTZ Service

Support for acceleration control has been added including fine grain preset tour configurations.

### 3. Changes

Find below all errata from Version 2.4 to 2.5 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.

#### 1322 Add capabilities for to signal whether GetStatus returns MoveStatus and Position elements

In the PTZ Service Specification, Sect. 5.3.5 replace the following

- Position (optional) – Specifies the absolute position of the PTZ unit together with the space references. The default absolute spaces of the corresponding PTZ configuration shall be referenced within the position element.
- MoveStatus (optional) – Indicates if the Pan/Tilt/Zoom device unit is currently moving, idle or in an unknown state.
- Error (optional) – States a current PTZ error.

with

- Position (optional) – Specifies the absolute position of the PTZ unit together with the space references. The default absolute spaces of the corresponding PTZ configuration shall be referenced within the position element. This information shall be present if the device signals support via the capability StatusPosition.
- MoveStatus (optional) - Indicates if the Pan/Tilt/Zoom device unit is currently moving, idle or in an unknown state. This information shall be present if the device signals support via the capability MoveStatus. The state Unknown shall not be used during normal operation, but is reserved to initialization or error conditions.
- Error (optional) – States a current PTZ error condition. This field shall be present if the MoveStatus signals Unkown.

And add the following capabilities in ptz.wsdl

```
<xs:attribute name="MoveStatus" type="xs:boolean">
  <xs:annotation>
    <xs:documentation>Indicates that the PTZVector includes MoveStatus
information.</xs:documentation>
  </xs:annotation>
</xs:attribute>
<xs:attribute name="StatusPosition" type="xs:boolean">
  <xs:annotation>
```

```
<xs:documentation>Indicates that the PTZVector includes Position
information.</xs:documentation>
</xs:annotation>
</xs:attribute>
```

## 1343 Some fault codes caused by sender side

In the Advanced Security Service, Table 16 (AddServerCertificateAssignment),

- replace  
env:Receiver  
ter:InvalidArgVal  
ter:CertificationPathID

env:Receiver  
ter:InvalidArgVal  
ter:NoPrivateKey

with

env:Sender  
ter:InvalidArgVal  
ter:CertificationPathID

env:Sender  
ter:InvalidArgVal  
ter:NoPrivateKey

In the Advanced Security service, Table 17 (RemoveServerCertificateAssignment),

- replace  
env:Receiver  
ter:InvalidArgVal  
ter:OldCertificationPathID

with

env:Sender  
ter:InvalidArgVal  
ter:OldCertificationPathID

In the Advanced Security Service, Table 18 (ReplaceServerCertificateAssignment),

- replace  
env:Receiver

ter:InvalidArgVal  
ter:OldCertificationPathID

env:Receiver  
ter:InvalidArgVal  
ter:NewCertificationPathID

env:Receiver  
ter:InvalidArgVal  
ter:NoPrivateKey

with

env:Sender  
ter:InvalidArgVal  
ter:OldCertificationPathID

env:Sender  
ter:InvalidArgVal  
ter:NewCertificationPathID

env:Sender  
ter:InvalidArgVal  
ter:NoPrivateKey

## 1413 Don't put normative requirement in the method table

Move the following paragraph in Table 33 to new paragraph in Sect. 5.5.4 in ONVIF Media Service specification.

If a video encoder configuration is specified, the options shall concern that particular configuration. If a media profile is specified, the options shall be compatible with that media profile. If no tokens are specified, the options shall be considered generic for the device. A separate Options structure shall be reported for each supported codec.

## 1417 onvif.xsd has incorrect reference namespace

In onvif.xsd, replace

```
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
```

with

```
xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
```

And also replace

```
<xs:import namespace="http://schemas.xmlsoap.org/soap/envelope/"
schemaLocation="http://schemas.xmlsoap.org/soap/envelope/" />
```

with

```
<xs:import namespace="http://www.w3.org/2003/05/soap-envelope"
schemaLocation="http://www.w3.org/2003/05/soap-envelope" />
```

## 1430 Syntax correction in Core Specification 7.3.2.2

In ONVIF Core specification, Sect. 7.3.2.2.1, change the third last paragraph

A device may have other scope URIs. These URIs are not restricted of ONVIF defined scopes.

to

A device may have other scope URIs. These URIs are not restricted to ONVIF defined scopes.

Also remove the last paragraph in this section.

## 1443 Mandatory requirement on SDP descriptions for Metadata

Replace the first paragraph in Streaming specification, Sect. 5.2.1.1.3

In the case of a metadata stream, the SDP description “application” should be used in the DESCRIBE response for media type and “vnd.onvif.metadata” should be used for encoding a name.

with

In the case of a metadata stream, the SDP description “application” shall be used in the DESCRIBE response for media type and “vnd.onvif.metadata” shall be used for encoding a name.

## 1457 Correction required in VideoParameters event message description

Replace the following part of event message description example in ONVIF Recording Search service specification, Sect. 5.19,

```
<tt:ElementItemDescription Name="VideoRateControl?" Type="tt:RateControl"/>
```

with

```
<tt:ElementItemDescription Name="VideoRateControl" Type="tt:VideoRateControl"/>
```



## 1467 Add event to monitor water in washers

Add the following section as 8.8.8 in ONVIF Core specification.

### 8.8.8 Liquid level

If measurements of the level of the liquid inside a washer tank are supported, a device should signal whether the level is under the warning threshold using the LowLiquid event.

Topic: tns1:Monitoring/Washer/LowLiquid

```
<tt:MessageDescription IsProperty="true">
<tt:Data>
<tt:SimpleItemDescription Name="IsLow" Type="xs:boolean"/>
</tt:Data>
</tt:MessageDescription>
```

## 1471 Clarify Backup/Restore expectations

Replace the following sentence in ONVIF Core specification, Sect. 8.3.3

The exact format of the backup configuration data is outside the scope of this specification.

with

The format of the backup configuration data is vendor specific. It is expected that after completion of the restore operation the device is working on the same configuration as that of the time the configuration was backed up. Note that the configuration of static IP addresses may differ.

Device vendors may put restrictions on the functionality to be restored. The detailed behavior is outside the scope of this specification.

## 1478 Requirements for Default access policy

Add the following paragraph in ONVIF Core specification. Sect. 5.12.2.4

A device that signals support for the Default Access Policy via the respective capability shall support at least one user of each user level Administrator, Operator and User.

## 1481 Link tev:SubscriptionPolicy to tev:CreatePullPointSubscription

Replace in event.wsdl:

```
<xs:complexType name="SubscriptionPolicy">
  <xs:sequence>
    <xs:any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="ChangedOnly" type="xs:boolean">
    < />
  <xs:anyAttribute processContents="lax"/>
</xs:complexType>
```

by

```
<xs:element name="ChangedOnly">
  <xs:complexType/>
</xs:element>
```

Replace in the Core Specification Section 9.1.1:

- ChangedOnly A pullpoint should not provide Initialized nor Deleted events for Properties.

by

- tev:ChangedOnly A pullpoint shall not provide Initialized or Deleted events for Properties.

## 1482 firmware upgrade - does not change configuration

Add the following sentence in ONVIF Core specification, both Sect. 8.3.9 and 8.3.10.

After applying a firmware upgrade the device shall keep the basic network configuration like IP address, subnet mask and gateway or DHCP settings unchanged. Additionally a firmware upgrade shall not change user credentials.

## 1483 Define additional events

Add the following in ONVIF Core specification, Sect. 8.8.5

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:Device/HardwareFailure/TemperatureCritical
<tt:MessageDescription IsProperty="true">
<tt:Data>
```

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

Add the following section as 8.8.9 in ONVIF Core specification.

#### 8.8.8 Mechanical failure

The following event should be generated with true value when a cooling fan fails.

Topic: tns1:Device/HardwareFailure/FanFailure

```
<tt:MessageDescription IsProperty="true">
<tt:Source>
<tt:SimpleItemDescription Name="Token" Type="tt:ReferenceToken"/>
</tt:Source>
<tt:Data>
<tt:SimpleItemDescription Name="Failed" Type="xs:boolean"/>
</tt:Data>
</tt:MessageDescription>
```

The following event should be generated with true value when a power supply fails.

Topic: tns1:Device/HardwareFailure/PowerSupplyFailure

```
<tt:MessageDescription IsProperty="true">
<tt:Source>
<tt:SimpleItemDescription Name="Token" Type="tt:ReferenceToken"/>
</tt:Source>
<tt:Data>
<tt:SimpleItemDescription Name="Failed" Type="xs:boolean"/>
</tt:Data>
</tt:MessageDescription>
```

The following event should be generated with true value when a mass storage device fails.

Topic: tns1:Device/HardwareFailure/StorageFailure

```
<tt:MessageDescription IsProperty="true">
<tt:Source>
<tt:SimpleItemDescription Name="Token" Type="tt:ReferenceToken"/>
</tt:Source>
<tt:Data>
<tt:SimpleItemDescription Name="Failed" Type="xs:boolean"/>
</tt:Data>
</tt:MessageDescription>
```

## 1488 Align Start FirmwareUpgrade spec with wsdl

Change the following data type definition in ONVIF Core specification, Table 48.

```
xs:duration UploadDelay [0][1]
xs:duration ExpectedDownTime [0][1]
```

to

```
xs:duration UploadDelay [1][1]
xs:duration ExpectedDownTime [1][1]
```

## 1472 Fix HttpFirmwareUpgrade annotation

Change the following annotation in devicemgmt.wsdl

```
<xs:documentation>Indicates support for system backup through
MTOM.</xs:documentation>
```

to

```
<xs:documentation>Indicates support for firmware upgrade through
HTTP.</xs:documentation>
```

## 1490 Incorrect access policy for SystemReboot

Change the default access policy in Table 51 in ONVIF Core specification from ACTUATE to UNRECOVERABLE.

## 1491 Incorrect access policy for GetSystemSupportInformation

Change the default access policy in Table 50 in ONVIF Core specification from READ\_SYSTEM to READ\_SYSTEM\_SECRET.

## 1492 Typo in DeviceIo table 26

Correct all the occurrences of "SerialConfiguration" to "SerialPortConfiguration" in ONVIF Device IO service specification, Table 26 as follows.

Replace the table title

GetSerialConfigurationOptions

with

GetSerialPortConfigurationOptions.

Replace the title block

GetSerialConfigurationOptions

With

GetSerialPortConfigurationOptions.

Replace

GetSerialConfigurationOptions-Request

With

GetSerialPortConfigurationOptions-Request.

Replace

GetSerialConfigurationOptions-Response

With

GetSerialPortConfigurationOptions-Response.

## 1502 Max Username and Password capabilities

In section 8.1.2.3 add the following two capabilities:

- MaxUsernameLength Maximum number of characters supported for the username by CreateUsers.
- MaxPasswordLength Maximum number of characters supported for the password by CreateUsers and SetUser.

## 1509 Fix typo in advancedsecurity.wsd

In advancedsecurity.wsd, element DistinguishedName, add a documentation block for the first anyAttribute:

```
<xs:element minOccurs="0" name="anyAttribute">
  <xs:annotation>
    <xs:documentation>Required extension point. It is recommended
      to not use this element, and instead use GenericAttribute and
      the numeric Distinguished Name Attribute
      Type.</xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:any minOccurs="0" maxOccurs="unbounded" namespace="##any"
        processContents="lax"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:sequence>
<xs:anyAttribute processContents="lax"/>
```

## 1515 Clarify frequency of constantly changing property events

Replace Section 8.8.1 in ONVIF Core specification with

If a device supports monitoring of processing unit usage, it should provide the processing unit usage monitoring event to inform a client about its current processing unit usage in percent. The value shall be the usage average over a time interval. It is recommended to use a time interval of five seconds to avoid flooding the event queue with excessive processing unit usage events.

Topic: tns1:Monitoring/ProcessorUsage

```
<tt:MessageDescription IsProperty="true">
  <tt:Source>
    <tt:SimpleItemDescription Name="Token" Type="tt:ReferenceToken"/>
  </tt:Source>
  <tt>Data>
    <tt:SimpleItemDescription Name="Value" Type="xs:float"/>
  </tt>Data>
</tt:MessageDescription>
```

Replace Section 8.8.5 Relative Humidity part with

If measurements of environmental conditions are supported a device should provide the following events.

The following event specifies the relative humidity in percent. It is recommended to use a time interval of sixty seconds or a 1% change to avoid flooding the event queue with excessive

relative humidity events. An event shall be sent if either the interval or percent change occurs.

```
Topic: tns1:Monitoring/EnvironmentalConditions/RelativeHumidity
<tt:MessageDescription IsProperty="true">
  <tt:Data>
    <tt:SimpleItemDescription Name="Status" Type="xs:float"/>
  </tt:Data>
</tt:MessageDescription>
```

#### Replace Section 8.8.5 Temperature part with

The following event specifies the operating temperature of the device in degree Celsius. It is recommended to use a time interval of sixty seconds or a 5% change to avoid flooding the event queue with excessive temperature change events. An event shall be sent if either the interval or percent change occurs.

```
Topic: tns1:Monitoring/EnvironmentalConditions/Temperature
<tt:MessageDescription IsProperty="true">
  <tt:Data>
    <tt:SimpleItemDescription Name="Status" Type="xs:float"/>
  </tt:Data>
</tt:MessageDescription>
```

#### Also replace Section 8.8.6 with

If measurements of the battery level are supported a device should provide the data using the BatteryCapacity event. It is recommended to use a 2% change to avoid flooding the event queue with excessive battery capacity change events.

```
Topic: tns1:Monitoring/BatteryCapacity
<tt:MessageDescription IsProperty="true">
  <tt:Data>
    <tt:SimpleItemDescription Name="onvif:PercentageRemainingCapacity"
      Type="xs:float"/>
  </tt:Data>
</tt:MessageDescription>
```



## 1516 Fix typo in DeviceIO spec

In Table 9 of ONVIF Device IO service specification, replace the title and the first row of  
GetVideoSourceConfiguartionOptions  
with  
GetVideoSourceConfigurationOptions

In Table 9, replace the word  
GetVideoSourceConfiguartionOptions-Response  
with  
GetVideoSourceConfigurationOptions-Response

## 1528 Define capability-implied requirements only at one place.

In the Advanced Security Service Specification, Sect. 5.2.6.1.1 (Create RSA key pair), delete the paragraph “A device signalling support for RSA key pair generation via the RSAKeyPairGeneration capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.1.2 (Get Key Status), delete the paragraph “A device that indicates support for key handling via the MaximumNumberOfKeys capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.1.3 (Get Private Key Status), delete the paragraph “A device that indicates support for RSA key pairs via the RSAKeyPairGenerationcapability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.1.4 (Get All Keys), delete the paragraph “A device that indicates support for key handling via the MaximumNumberOfKeys capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.1.5 (Delete Key), delete the paragraph “A device that indicates support for key handling via the MaximumNumberOfKeys capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.2.1 (Create PKCS#10 Certification Request), delete the paragraph “A device signalling support for creating PKCS#10 certification requests via the PKCS10ExternalCertificationWithRSA capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.2.2 (Create Self-Signed Certificate), delete the paragraph “A device signalling support for creating RSA-based self-signed certificates via the SelfSignedCertificateCreationWithRSA capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.2.3 (Upload Certificate), delete the paragraph “A device signalling support for PKCS#10 External Certification with the PKCS10ExternalCertificationWithRSAcapability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.2.4 (Get Certificate), delete the paragraph

“A device that supports the Create Self Signed Certificate command or the Upload certificate command shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.2.5 (Get All Certificates), delete the paragraph “A device that supports the Create Self Signed Certificate command or the Upload certificate command shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.2.6 (Delete Certificate), delete the paragraph “A device that supports the Create Self Signed Certificate command or the Upload certificate command shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.2.7 (Create Certification Path), delete the paragraph “A device signalling support for TLS via the TLSServerSupported capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.2.8 (Get Certification Path), delete the paragraph “A device signalling support for TLS via theTLSServerSupported capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.2.9 (Get All Certification Paths), delete the paragraph “A device signalling support for TLS via theTLSServerSupported capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.2.6.2.10 (Delete Certification Path), delete the paragraph “A device signalling support for TLS via theTLSServerSupported capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.3.2.1 (Add Server Certificate Assignment), delete the paragraph “A device signalling a TLS server implementation via the TLSServerSupported capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.3.2.2 (Remove Server Certificate Assignment), delete the paragraph “A device signalling a TLS server implementation via the TLSServerSupported capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.3.2.3 (Replace Server Certificate Assignment), delete the paragraph “A device signalling a TLS server implementation via the TLSServerSupported capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.3.2.4 (Get Assigned Server Certificates), delete the paragraph “A device signalling a TLS server implementation via the TLSServerSupported capability shall support this command.”

In the Advanced Security Service Specification, Sect. 5.4.4 (Capability-implied Requirements), Table 23, add to the operations required by capability PKCS10ExternalCertificationWithRSA the operations GetCertificate, GetAllCertificates, and DeleteCertificate.

## 1529 GetAllCertificates: Parameter mismatch in spec and wsdl

In the Advanced Security Service Specification, Sect. 5.2.6.2.5 (Get All Certificates),

- replace “This operation returns the IDs of all certificates that are stored in the device’s keystore.”  
With “This operation returns all certificates that are stored in the device’s keystore.”

In the Advanced Security Service Specification, Table 10 (Get All Certificates),

- replace “tas:CertificateID CertificateID [0][unbounded]” with “tas:X509Certificate Certificate [0][unbounded]”.

## 1530 Incorrect Whitespace at various places

In the Advanced Security Service Specification, add/remove whitespace at appropriate places to improve the readability of the document.

## 1531 Clarify requirements on certification path assignments to TLS Server

In the Advanced Security Service Specification, Sect. 5.3.2.1 (Add Server Certificate Assignment), in front of the paragraph starting with “A device signaling a TLS server implementation...”,

- add the paragraph “If the certification path identified by the supplied certification path ID is already assigned to the TLS server, this command shall have no effect.”

## 1532 Contradicting definitions for GetAssignedServerCertificates

In the Advanced Security Service Specification, Sect. 5.3.2.4, replace the first paragraph with "This operation returns the IDs of all certification paths that are assigned to the TLS server on the device."

## 1533 Include protocol options in capability-implied requirements

In the Advanced Security Service Specification,

- delete Sect. 5.8 (Protocol Options).

In the Advanced Security Service Specification, Sect. 5.4.4 (Capability-implied Requirements), capability “PKCS10ExternalCertificationWithRSA”,

- add as implied requirement “If true, the list of supported signature algorithms as indicated by the SignatureAlgorithms capability shall contain at least the algorithms sha1-WithRSAEncryption and sha256WithRSAEncryption.”

In the Advanced Security Service Specification, Sect. 5.4.4 (Capability-implied Requirements), capability “SelfSignedCertificateCreationWithRSA”,

- add as implied requirement “If true, the list of supported signature algorithms as indicated by the

SignatureAlgorithms capability shall contain at least the algorithms sha1-WithRSAEncryption and sha256WithRSAEncryption.”

### 1534 TLSServerSupported capability does not imply certificate handling support

In the Advanced Security Service Specification, Sect. 5.4.4 (Capability-implied requirements), capability TLSServerSupported,

- add the requirement “If not empty, PKCS10ExternalCertificationWithRSA shall be true or SelfSignedCertificateCreationWithRSA shall be true.”

### 1535 Define service-specific data types in wsdl only.

In the Advanced Security Service Specification, Sect. 5.6 (Service specific data types),

- replace the section content with “The service specific data types are defined in advancedsecurity.wsdl.”

### 1536 TLSServerSupported requirement assumes wrong parameter type

In the Advanced Security Service specification, Sect. 5.4.4 (Capability-implied requirements), capability TLSServerSupported,

- replace the requirement “If true, MaximumNumberOfCertificationPaths $\geq$ 2 and MaximumNumberOfTLSCertificationPaths $>$ 0 shall hold.” with  
“If not empty, MaximumNumberOfCertificationPaths $\geq$ 2 and MaximumNumberOfTLSCertificationPaths $>$ 0 shall hold.”

### 1539 Add requirement level indication in the Keep-alive behavior in Real-time pull point function

In Sect. 9.1.1 in ONVIF Core specification, replace the 2nd paragraph of

By default the pull point keep alive is controlled via the PullMessages operation. In this case the default relative timeout of 60 seconds is automatically prolonged by each consecutive PullMessages operation on the pull point.

with

By default the pull point keep alive is controlled via the PullMessages operation. In this case, after a PullMessages response is returned, the subscription should be active for at least the timeout specified in the PullMessages request.

## 1540 Add clarification text in StopMulticastStreaming

In Sect. 5.17.2 in ONVIF Media service specification, add the following sentence in the 1st paragraph.

In case that a device receives the StopMulticastStreaming request whose corresponding multicast streaming is not started, the device should reply with successful StopMulticastStreamingResponse.

## 1559 (typo) Replace doPeriodicNotify in the XML with the isPeriodicNotify

In A.3 Loitering Detector in ONVIF Analytics service specification, replace "doPeriodicNotify" in XML with "isPeriodicNotify".