

# ONVIF<sup>®</sup>

# TLS Configuration Add-on Specification

Version 1.0

December 2023

©2008-2023 by ONVIF: Open Network Video Interface Forum. 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.

## REVISION HISTORY

<b>Vers.</b>	<b>Date</b>	<b>Description</b>	<b>Contributors</b>
1.0	December, 2023	Original Release version 1.0	Refer to Contributors table

## CONTRIBUTORS

<b>Company</b>	<b>Contributors</b>
Axis Communications AB	Baldvin Gislason Bern Johan Svensk Sriram Bhetanabottla
Genetec Inc.	Jean-Francois Levesque
Motorola Solutions	Michael Adam Todd Johnson
Honeywell	Venki Aravapalli Giri Guntipalli
Bosch Security Systems B.V.	Hans Busch André Eichhorn

## Table of Contents

<b>ONVIF®</b>	<b>1</b>
<b>TLS CONFIGURATION ADD-ON SPECIFICATION</b>	<b>1</b>
<b>1 SCOPE</b>	<b>6</b>
<b>2 NORMATIVE REFERENCES</b>	<b>6</b>
2.1 NORMATIVE REFERENCES	6
<b>3 TERMS AND DEFINITIONS</b>	<b>6</b>
3.1 DEFINITIONS	6
<b>4 TECHNICAL SPECIFICATION VERSION REQUIREMENT</b>	<b>7</b>
<b>5 REQUIREMENT LEVELS</b>	<b>7</b>
<b>6 OVERVIEW</b>	<b>8</b>
6.1 USE CASES	8
6.1.1 <i>Initial configuration</i>	8
6.1.2 <i>Update configuration</i>	8
<b>7 MANDATORY FEATURES (NORMATIVE)</b>	<b>9</b>
7.1 DISCOVERY	9
7.1.1 <i>Device requirements</i>	9
7.1.2 <i>Client requirements</i>	9
7.1.3 <i>Function list for devices</i>	9
7.1.4 <i>Function list for clients</i>	9
7.2 TLS CONFIGURATION	10
7.2.1 <i>Device requirements</i>	10
7.2.2 <i>Client requirements</i>	10
7.2.3 <i>TLS server configuration function list for devices</i>	11
7.2.4 <i>TLS server configuration function list for clients</i>	12

# 1 Scope

This document defines the mandatory and conditional features required by an ONVIF device and ONVIF client that support the Feature Set of the TLS Configuration Add-on.

## 2 Normative references

This section defines the normative references applicable to this specification.

### 2.1 Normative references

- **ONVIF Profile Policy**  
< <http://www.onvif.org/profiles> >
- **ONVIF Network Interface Specifications**  
< <https://www.onvif.org/profiles/specifications/> >

## 3 Terms and definitions

This section provides common terms and definitions used in this specification.

### 3.1 Definitions

<b>Add-on</b>	See [ONVIF Profile Policy]
<b>Profile</b>	See [ONVIF Profile Policy]
<b>ONVIF device</b>	Networked hardware appliance or software program that exposes one or multiple ONVIF Web Services
<b>ONVIF client</b>	Networked hardware appliance or software program that uses ONVIF Web Services
<b>TLS</b>	Transport Layer Security
<b>CSR</b>	Certificate Signing Request

## 4 Technical specification version requirement

Implementation of ONVIF Network Interface Specifications, version 22.06 or later is required for conformance to TLS configuration add-on.

## 5 Requirement levels

Each feature in this document has a requirement level for device and client that claims conformance to TLS configuration add-on and contains a function list that states the function's requirement level for device and client that implement that feature.

The requirement levels for features are:

- **Mandatory = Feature that shall be implemented by an ONVIF device or ONVIF client.**

The requirement levels for functions are:

- **Mandatory = Function that shall be implemented by an ONVIF device or ONVIF client.**
- **Optional = Function that may be implemented by an ONVIF device or ONVIF client.**

Function lists use the following abbreviations:

- **M = Mandatory**
- **O = Optional**

All functions shall be implemented as described in the corresponding [ONVIF Network Interface Specifications].

## 6 Overview

This section explains the basic motivation for defining the TLS Add-on specification.

Secure communication between ONVIF clients and ONVIF devices is a key market demand. One important aspect of secure communication is the possibility to encrypt the communication using Transport Layer Security, or TLS.

An ONVIF device conformant to TLS configuration add-on is an ONVIF device that can be configured to use TLS.

An ONVIF client conformant to TLS configuration add-on is an ONVIF client that can configure an ONVIF device to use TLS.

### 6.1 Use cases

This section defines the anticipated typical usage of the Add-on.

#### 6.1.1 Initial configuration

An end user utilizes a client to configure TLS settings on a device to prepare for encrypted and trusted communication between clients and the configured device.

The Add-on does not specify the exact workflow for this process, however an example Interface (or function) call sequence could be as follows:

1. Query **GetServices** and **GetServiceCapabilities** to verify device support.
2. Use **CreatePKCS10CSR** to request a Certificate Signing Request from the device
3. Sign the CSR using a Certificate Authority.
4. Upload CA certificate and signed certificate to the camera using **UploadCertificate**
5. Use the Certificate ID(s) to create a certification path with **CreateCertificationPath**
6. Assign the certification path using **Add/ReplaceServerCertificateAssignment**
7. Enable the HTTPS port on the device (if not already enabled)

Steps 2-4 can be replaced with **CreateSelfSignedCertificate** to create a self signed certificate for use on the camera.

#### 6.1.2 Update configuration

An end user utilizes a client to update the TLS settings on a device, such as deploying a new certificate, to enable the device to continue to operate in an encrypted and trusted environment.

Generally, this follows the workflow described in 6.1.1, however a client would leverage the **Add/Update/Remove** functions as necessary.



## 7 Mandatory features (normative)

The mandatory features section lists all the features that are guaranteed to be supported by a device and client that are both conformant to the Add-on.

### 7.1 Discovery

This section describes the operations related to device discovery.

#### 7.1.1 Device requirements

- Device shall support listing capabilities via the **GetServices** and **GetServiceCapabilities** operation.
- Device shall declare the Add-on support via **GetServices** and **GetServiceCapabilities** response “**Addons**” list using the following text string:

**TLSServerConfiguration**

Potential subsequent versions will append major version information to this text string.

#### 7.1.2 Client requirements

- Client shall be able to list add-ons via **GetServices** or **GetServiceCapabilities** as specified in the **Core Specification**.

#### 7.1.3 Function list for devices

Discovery		Device MANDATORY	
Function	Service	Requirement	
GetServices	Device Management	M	
GetServiceCapabilities	Device Management	M	

#### 7.1.4 Function list for clients

Discovery		Client MANDATORY	
Function	Service	Requirement	
GetServices	Device Management	O	
GetServiceCapabilities	Device Management	O	

Note: GetServices and GetServiceCapabilities are optional for this add-on, but one or the other will be implicitly required as mandatory for a supported profile.

## 7.2 TLS configuration

The TLSConfiguration is a set of interfaces needed to configure functionality related to TLS server, managing certificates, certification paths and keys on the device.

### 7.2.1 Device requirements

Device shall support the following **Security Configuration Service** capabilities:

- Device shall support key configuration as defined by the "**RSAKeyPairGeneration**" capability.
- Device shall support key generation status with both the "**GetKeyStatus**" function and with "**tns1:Advancedsecurity/Keystore/KeyStatus**" event notification.
- Device shall support "**MaximumNumberOfKeys**" capability of at least 16 to allow flexibility in certificate configuration.
- Device shall support certificate configuration as defined by each of the "**SelfSignedCertificateCreationWithRSA**" and the "**PKCS10ExternalCertificationWithRSA**" capabilities.
- Device shall support "**MaximumNumberOfCertificates**" capability of at least 16 to allow flexibility in certification path configuration.
- Device shall support certification path configuration as defined by the "**TLSServerSupported**" capabilities as described in the **Security Service Specification Capability-Implied Requirements**.
- Device shall support TLS server certificate assignment as defined by the "**TLSServerSupported**" capability as described in the **Security Service Specification Capability-Implied Requirements**.
- Device shall support the "**SetNetworkProtocols**" function to enable/disable TLS.

### 7.2.2 Client requirements

- Client shall be able to do key management using "**CreateRSAKeyPair and DeleteKey**" operations as described in the **Security Service Specification**.
- Client shall be able to verify key status using "**GetKeyStatus**" service or subscribing to event "**tns1:Advancedsecurity/Keystore/KeyStatus**" as defined in the **Security Service Specification**.
- Client shall be able to do certificate management using "**CreatePKCS10CSR, UploadCertificate, DeleteCertificate, CreateCertificationPath and DeleteCertificationPath**" operations as described in the **Security Service Specification**.
- Client shall be able to do TLS Server Operations using "**ReplaceServerCertificateAssignment**" operation as described in the **Security Service Specification**.
- Client shall be able to enable/disable TLS using "**SetNetworkProtocols**" operation as described in the **Security Service Specification**.

### 7.2.3 TLS server configuration function list for devices

TLS Server Configuration		Device MANDATORY	
Function	Service	Requirement	
AddServerCertificateAssignment	Security	M	
CreateCertificationPath	Security	M	
CreatePKCS10CSR	Security	M	
CreateRSAKeyPair	Security	M	
CreateSelfSignedCertificate	Security	M	
DeleteCertificate	Security	M	
DeleteCertificationPath	Security	M	
DeleteKey	Security	M	
GetAllCertificates	Security	M	
GetAllCertificationPaths	Security	M	
GetAllKeys	Security	M	
GetAssignedServerCertificates	Security	M	
GetCertificate	Security	M	
GetCertificationPath	Security	M	
GetKeyStatus	Security	M	
GetServiceCapabilities	Security	M	
tns1:Advancedsecurity/Keystore/KeyStatus	Event	M	
RemoveServerCertificateAssignment	Security	M	
ReplaceServerCertificateAssignment	Security	M	
SetNetworkProtocols	Device	M	
UploadCertificate	Security	M	

### 7.2.4 TLS server configuration function list for clients

TLS Server Configuration		Client MANDATORY
Function	Service	Requirement
AddServerCertificateAssignment	Security	O**
CreateCertificationPath	Security	M
CreatePKCS10CSR	Security	M
CreateRSAKeyPair	Security	M
CreateSelfSignedCertificate	Security	O
DeleteCertificate	Security	M
DeleteCertificationPath	Security	M
DeleteKey	Security	M
GetAllCertificates	Security	O
GetAllCertificationPaths	Security	O
GetAllKeys	Security	O
GetAssignedServerCertificates	Security	O
GetCertificate	Security	O
GetCertificationPath	Security	O
GetServiceCapabilities	Security	O
GetKeyStatus	Security	M*
tns1:Advancedsecurity/Keystore/KeyStatus	Event	
RemoveServerCertificateAssignment	Security	O
ReplaceServerCertificateAssignment	Security	M
SetNetworkProtocols	Device	M
UploadCertificate	Security	M

\* Client shall support at least one of the listed methodologies to obtain the status for the key generation.

\*\* Clients are recommended to support this function for Devices that do not have a pre-installed certificate.