ONVIF®

TLS Configuration Add-on Specification

RELEASE CANDIDATE

Version RC 1.4

July 2023

REVISION HISTORY

Vers.	Date	Description	Contributors
RC 1.0	May 2021	Just a draft example of what a Feature Specification could look like to be used as discussion material.	Refer to Contributors table
RC 1.1	November 2021	Edits based on review at the 2021 November ONVIF Meeting in Lisbon.	Attendees at the WG meeting
RC 1.2	June 2022	Branding edits based on feedback from the Communication Committee. Changed November version to 1.1 to simplify versioning.	Michael Adam
RC 1.3	November 2022	Edits based on review at the 2022 November ONVIF Meeting in Casablanca. • AddServerCertificateAssignment made mandatory for clients.	Attendees at the WG meeting
RC 1.4	February 2023	Edits based on WG Meeting and CC Feedback: • AddServerCertificateAssignment made optional with footnote. • Add GetServices and GetServiceCapabilities to function lists per CTT/DTT review. • Update some language per Communication Committee. • Expanded Section 6 with more detailed use cases.	Michael Adam

CONTRIBUTORS

Company	Contributors
Axis Communications AB	Baldvin Gislason Bern Johan Svensk
Genetec Inc.	Jean-Francois Levesque
Motorola Solutions	Michael Adam
Honeywell	Venki Aravapalli

Table of Contents

ONVIF® **1**

TLS CONFIGURATION ADD-ON SPECIFICATION RELEASE CANDIDATE **1**

1 SCOPE **6**

2 NORMATIVE REFERENCES **6**

2.1 NORMATIVE REFERENCES 6

3 TERMS AND DEFINITIONS **6**

3.1 DEFINITIONS 6

4 TECHNICAL SPECIFICATION VERSION REQUIREMENT **7**

5 REQUIREMENT LEVELS **7**

6 OVERVIEW **8**

6.1 USE CASES 8
6.1.1 Initial configuration *8*
6.1.2 Update configuration *8*

7 MANDATORY FEATURES (NORMATIVE) **9**

7.1 DISCOVERY 9
7.1.1 Device requirements *9*
7.1.2 Client requirements *9*
7.1.3 Function list for devices *9*
7.1.4 Function list for clients *9*
7.2 TLS CONFIGURATION 9
7.2.1 Device requirements *9*
7.2.2 Client requirements *10*
7.2.3 TLS server configuration function list for devices *11*
7.2.4 TLS server configuration function list for clients *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

Add-on	See [ONVIF Profile Policy]
Profile	See [ONVIF Profile Policy]
ONVIF device	Networked hardware appliance or software program that exposes one or multiple ONVIF Web Services
ONVIF client	Networked hardware appliance or software program that uses ONVIF Web Services.
TLS	Transport Layer Security
CSR	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 concept of the Add-on.

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 workflow is 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. Using the CA certificate and signed certificate, upload them to the camera with 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 between 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 by listing capabilities via the GetServiceCapabilities operation.**
- **Device shall declare support via the "Addons" list using the following text string:**

  TLSServerConfiguration

7.1.2 Client requirements

- **Client shall be able to list add-ons via 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

7.2 TLS configuration

Manage TLS server, certification path, certificate, and key configurations.

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.**
- **Device shall support TLS server certificate assignment as defined by the "TLSServerSupported" capability.**
- **Device shall support the "SetNetworkProtocols" function to enable/disable TLS.**

7.2.2 Client requirements

Client shall support the following Security Configuration Service capabilities:

- **Client shall support key configuration as defined by both the "RSAKeyPairGeneration" capability.**
- **Client shall support retrieval of key generation status with either the "GetKeyStatus" function or with "tns1:Advancedsecurity/Keystore/KeyStatus" event notification. Client shall support certificate configuration as defined by the "PKCS10ExternalCertificationWithRSA" capability.**
- **Client shall support certification path configuration as defined by "TLSServerSupported" capability.**
- **Client shall support TLS server certificate assignment as defined by the "TLSServerSupported" capability.**
- **Client shall support the "SetNetworkProtocols" function to enable/disable TLS**.

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.