ONVIF®

Export File Format Device Test Specification

Version 21.06

June 2021

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

Vers.	Date	Description
21.06	Mar 03, 2021	First Issue.
21.06	Mar 11, 2021	Update after review.

Table of Contents

1 Introduction 5

1.1 Scope 5

1.2 Export File Format 6

2 Normative references 7

3 Terms and Definitions 9

3.1 Conventions 9

3.2 Definitions 9

3.3 Abbreviations 9

4 Test Overview 10

4.1 Test Setup 10

4.1.1 Network Configuration for DUT 10

4.2 Prerequisites 11

4.3 Test Policy 11

4.3.1 Export Format 11

5 Export File Format 13

5.1 Export Format 13

5.1.1 EXPORT FILE FORMAT VALIDATION 13

A Helper Procedures and Additional Notes 17

A.1 SurveillanceExportBox Format 17

A.2 RSASSA-PSS Signature Validation 17

1 Introduction

The goal of the ONVIF test specification set is to make it possible to realize fully interoperable IP physical security implementation from different vendors. The set of ONVIF test specification describes the test cases need to verify the [ONVIF Network Interface Specs] and [ONVIF Conformance] requirements. In addition, the test cases are to be basic inputs for some Profile specification requirements. It also describes the test framework, test setup, pre-requisites, test policies needed for the execution of the described test cases.

This ONVIF Export File Format Device Test Specification acts as a supplementary document to the [ONVIF Network Interface Specs], illustrating test cases need to be executed and passed. And this specification acts as an input document to the development of test tool, which will be used to test the ONVIF device implementation conformance towards ONVIF standard. This test tool is referred as ONVIF Client hereafter.

1.1 Scope

This ONVIF Export File Format Device Test Specification defines and regulates the conformance testing procedure for the ONVIF conformant devices. Conformance testing is meant to be functional black-box testing. The objective of this specification to provide test cases to test individual requirements of ONVIF devices according to ONVIF Export File Format Specification which is defined in [ONVIF Network Interface Specs].

The principal intended purposes are:

- Provide self-assessment tool for implementations.
- Provide comprehensive test suite coverage for [ONVIF Network Interface Specs].

This specification **does not** address the following:

- Product use cases and non-functional (performance and regression) testing.
- SOAP Implementation Interoperability test i.e. Web Service Interoperability Basic Profile version 2.0 (WS-I BP 2.0).
- Network protocol implementation Conformance test for HTTP, HTTPS, RTP and RTSP protocol.
- Poor streaming performance test (audio/video distortions, missing audio/video frames, incorrect lib synchronization etc.).

  Wi-Fi Conformance test

The set of ONVIF Test Specification will not cover the complete set of requirements as defined in [ONVIF Network Interface Specs]; instead, it will cover its subset.

This ONVIF Export File Format Device Test Specification covers requirements for export file format, which is a functional block of [ONVIF Network Interface Specs]. The following section gives a brief overview of each functional block and its scope.

1.2 Export File Format

Export File Format cases cover verification of exported file format defined in [ONVIF Export File Format Specification].

2 Normative references

- [ONVIF Conformance] ONVIF Conformance Process Specification:

  https://www.onvif.org/profiles/conformance/

- [ONVIF Profile Policy] ONVIF Profile Policy:

  https://www.onvif.org/profiles/

- [ONVIF Network Interface Specs] ONVIF Network Interface Specification documents:

  https://www.onvif.org/profiles/specifications/

- [ONVIF Core Specs] ONVIF Core Specification:

  https://www.onvif.org/profiles/specifications/

- [ONVIF Export File Format Spec] ONVIF Export File Format Specification:

  https://www.onvif.org/profiles/specifications/

- ISO/IEC 14496-12 Information technology — Coding of audiovisual objects – Part 12: ISO base media file format

  https://www.iso.org/obp/ui/#iso:std:iso-iec:14496:-12:ed-5:v1:en

- ISO/IEC 23000-10 Information technology – Multimedia application format – Part 10: Surveillance application format

  https://www.iso.org/obp/ui/#iso:std:iso-iec:23000:-10:ed-2:v1:en

- NIST FIPS 180-4 Secure Hash Standard

  https://csrc.nist.gov/publications/detail/fips/180/4/final

- ISO/IEC 14888-2 Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms

  https://www.iso.org/obp/ui/#iso:std:iso-iec:14888:-2:ed-2:v1:en

- IETF RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1

  https://tools.ietf.org/rfc/rfc3447.txt

- ITU-T Recommendation X.690 (2008) | ISO/IEC 8825-1:2008, Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER),Canonical Encoding Rules (CER)and Distinguished Encoding Rules (DER)

  https://www.itu.int/rec/T-REC-X.690-200811-S

3 Terms and Definitions

3.1 Conventions

The key words "shall", "shall not", "should", "should not", "may", "need not", "can", "cannot" in this specification are to be interpreted as described in [ISO/IEC Directives Part 2].

3.2 Definitions

This section describes terms and definitions used in this document.

Profile See ONVIF Profile Policy.

ONVIF Device Computer appliance or software program that exposes one or multiple ONVIF Web Services.

ONVIF Client Computer appliance or software program that uses ONVIF Web Services.

Device Test Tool ONVIF Device Test Tool that tests ONVIF Device implementation towards the ONVIF Test Specification set.

Certificate A certificate as used in this specification binds a public key to a subject entity. The certificate is digitally signed by the certificate issuer to allow for verifying its authenticity.

Signature A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document.

3.3 Abbreviations

This section describes abbreviations used in this document.

SHA Secure Hashing Algorithm.

4 Test Overview

This section describes about the test setup and prerequisites needed, and the test policies that should be followed for test case execution.

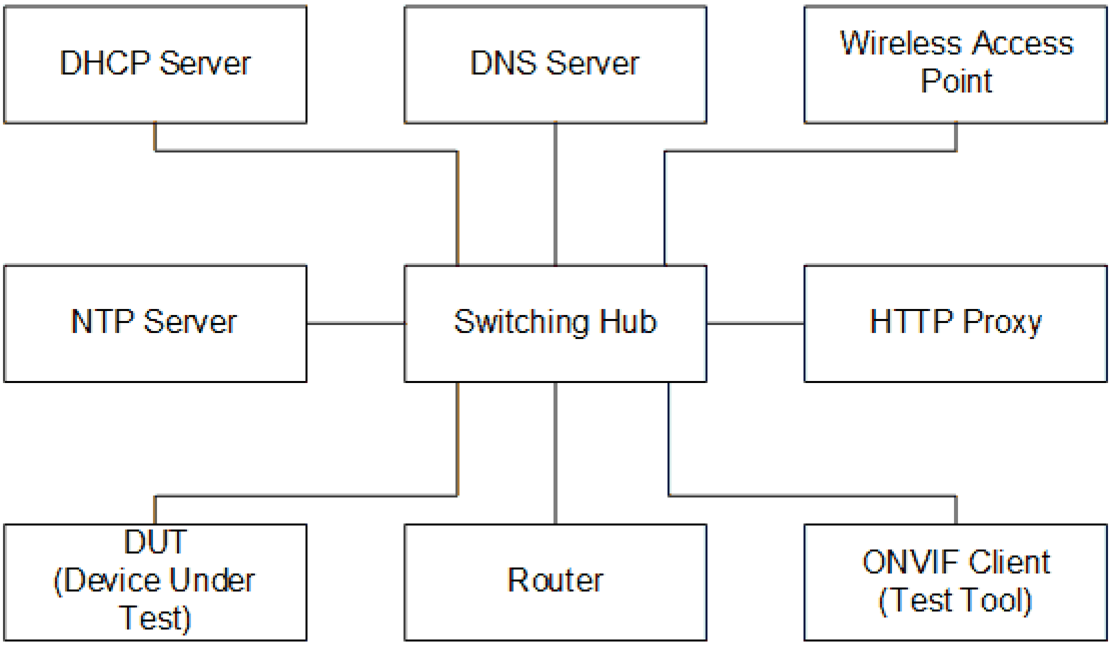
4.1 Test Setup

4.1.1 Network Configuration for DUT

The generic test configuration for the execution of test cases defined in this document is as shown below (Figure 4.1).

Based on the individual test case requirements, some of the entities in the below setup may not be needed for the execution of those corresponding test cases.

Figure 4.1. Test Configuration for DUT



DUT: ONVIF device to be tested. Hereafter, this is referred to as DUT (Device Under Test).

ONVIF Client (Test Tool): Tests are executed by this system and it controls the behavior of the DUT. It handles both expected and unexpected behavior.

HTTP Proxy: provides facilitation in case of RTP and RTSP tunneling over HTTP.

Wireless Access Point: provides wireless connectivity to the devices that support wireless connection.

DNS Server: provides DNS related information to the connected devices.

DHCP Server: provides IPv4 Address to the connected devices.

NTP Server: provides time synchronization between ONVIF Client and DUT.

Switching Hub: provides network connectivity among all the test equipments in the test environment. All devices should be connected to the Switching Hub. When running multiple test instances in parallel on the same network, the Switching Hub should be configured to use filtering in order to avoid multicast traffic being flooded to all ports, because this may affect test stability.

Router: provides router advertisements for IPv6 configuration.

4.2 Prerequisites

The pre-requisites for executing the test cases described in this Test Specification are:

1. The DUT shall be configured with an IPv4 address.
2. The DUT shall be IP reachable [in the test configuration].
3. The DUT shall be able to be discovered by the Test Tool.
4. The DUT shall be configured with the time i.e. manual configuration of UTC time and if NTP is supported by the DUT, then NTP time shall be synchronized with NTP Server.
5. The DUT time and Test tool time shall be synchronized with each other either manually or by common NTP server

4.3 Test Policy

This section describes the test policies specific to the test case execution of each functional block.

The DUT shall adhere to the test policies defined in this section.

4.3.1 Export Format

The test policies specific to the test case execution of Export File Format functional block:

- DUT shall support exporting of media file according to ONVIF format. Exported file shall contain:
    - At least one Video track;
    - Meta Box container (meta);

- SurveillanceExportBox (suep);

- AFIdentificationBox (sumi);

- Protection Box (ipro) with RSASSA-PSS signature.

Please, refer to Section 5.1 for Export Format Test Cases.

5 Export File Format

5.1 Export Format

5.1.1 EXPORT FILE FORMAT VALIDATION

Test Case ID: EXPORT_FORMAT-1-1-1

Specification Coverage: Export Format (ONVIF Export File Format Spec)

Feature Under Test: ONVIF file format for exported media

WSDL Reference: None

Test Purpose: To verify that file format for exported media corresponds to mandatory requerement from ONVIF Export File Format Spec

Pre-Requisite: File with exported media is provided in the Device Test Tool user interface. It contains at least one Video track.

Test Configuration: ONVIF Client and DUT

Test Procedure:

1. ONVIF Client retrieves file with exported media from user interface.
2. Set *exportedFile* := file with exported media from user interface.
3. ONVIF Client parses *exportedFile*.
4. ONVIF Client checks that *exportedFile* contains at least one video track
   - 4.1. If *exportedFile* does not contain at least one track (moov/trak), FAIL the test.
   - 4.2. If at least one track (moov/trak/mdia) does not have 'hdlr' box with type value = 'vide', FAIL the test.
5. If *exportedFile* does not contain Meta Box container (*meta*), FAIL the test.
6. ONVIF Client checks *meta* structure
   - 6.1. If *meta* does not contain SurveillanceExportBox with box type = 'suep', FAIL the test.
   - 6.2. If *meta* contains more than one SurveillanceExportBox with box type = 'suep', FAIL the test.

6.3. ONVIF Client parses SurveillanceExportBox box according to order described in Annex A.1 and checks information provided inside

6.3.1. If SurveillanceExportBox does not contain all required fields (see Annex A.1), FAIL the test.

6.3.2. If at least one field value does not correspond to its type (Annex A.1), FAIL the test.

6.4. If *meta* does not contain AFIdentificationBox with box type = 'sumi', FAIL the test.

6.5. If *meta* contains more than one AFIdentificationBox with box type = 'sumi', FAIL the test.

6.6. ONVIF Client parses AFIdentificationBox box and checks information provided inside

6.6.1. If AFIdentificationBox does not contain startTime field with unsigned integer value, FAIL the test.

6.7. For each track fragment (moof/traf) *track*

6.7.1. If *track* does not contain Track Fragment Decode Time box with box type = 'tfdt', FAIL the test.

6.7.2. If *track* contains more than one Track Fragment Decode Time box with box type = 'tfdt', FAIL the test.

7. ONVIF Client checks signature

7.1. If *meta* does not contain Item Protection Box with box type = 'ipro' (*ipro*), FAIL the test.

7.2. If *meta* contains more than one Protection Box with box type = 'ipro', FAIL the test.

7.3. If Protection Count value in *ipro* != 1, FAIL the test.

7.4. If *ipro* does not contain at least one Protection Scheme Info Box with box type = 'sinf', FAIL the test.

7.5. For each Protection Scheme Info Box with box type = 'sinf' (*sinf*)

7.5.1. If *sinf* does not contain Scheme Type Box with box type = 'schm' (*schm*), FAIL the test.

7.5.2. If *sinf* contains more than one Scheme Type Box with box type = 'schm', FAIL the test.

7.5.3. If Scheme Type value in *schm* = 0x6F656666 ("Onvif Export File Format")

7.5.3.1. If Scheme Version value in *schm* != 0x00010000 (1), FAIL the test.

7.5.3.2. If *sinf* contains CorrectStartTimeBox with box type = 'cstb'

7.5.3.2.1. If amout of CorrectStartTimeBox with box type = 'cstb' is more than one, FAIL the test.

7.5.3.2.2. If track_ID field type is not unsigned integer, FAIL the test.

7.5.3.2.3. If track_ID field value = 0, FAIL the test.

7.5.3.2.4. If startTime field type is not unsigned integer, FAIL the test.

7.5.3.3. If *sinf* does not contain Scheme Information Box with box type = 'schi' (*schi*), FAIL the test.

7.5.3.4. If *sinf* contains more than one Scheme Information Box with box type = 'schi', FAIL the test.

7.5.3.5. ONVIF Client checks (*schi*)

7.5.3.5.1. If *schi* does not contain SignatureBox with box type = 'sibo', FAIL the test.

7.5.3.5.2. If *schi* contains more than one SignatureBox with box type = 'sibo', FAIL the test.

7.5.3.5.3. ONVIF Client validates signature in SignatureBox with box type = 'sibo' according to Annex A.2 with the following input and output parameters

- in *sibo* - SignatureBox with box type = 'sibo'

- in *exportedFile* - signed exported file

7.5.3.5.4. If *schi* does not contain CertificateBox with box type = 'cert', FAIL the test.

7.5.3.5.5. If *schi* contains more than one CertificateBox with box type = 'cert', FAIL the test.

7.5.3.6. If *sinf* does not contain at least one Scheme Information Box with box type = 'schi', FAIL the test.

7.6. If at step 7.5 there was no at least one box with type = 'sinf' and with Scheme Type value in 'schm' = 0x6F656666, FAIL the test and skip other steps.

Test Result:

PASS –

- DUT passes all assertions.

FAIL –

- Parsing of file provided in the Device Test Tool user interface was failed.

Annex A Helper Procedures and Additional Notes

A.1 SurveillanceExportBox Format

SurveillanceExportBox shall contain all these fields in the following order:

- ExportUnitName (UTF-8 characters string)
- ExportUnitURL (UTF-8 characters string)
- ExportUnitMAC (UTF-8 characters string)
- ExportUnitTime (integer)
- ExportOperator (UTF-8 characters string)
- For each media track (moov/trak) in *exportedFile*:
  - SourceName (UTF-8 characters string)
  - SourceURL (UTF-8 characters string)
  - SourceMAC (UTF-8 characters string)
  - SourceLine (UTF-8 characters string)

A.2 RSASSA-PSS Signature Validation

Name: HelperRSASSA-PSSsignatureValidation

Procedure Purpose: Helper procedure to validate signature in SignatureBox.

Pre-requisite: None.

Input: SignatureBox with box type = 'sibo' (*sibo*). Signed exported file (*exportedFile*).

Returns: None.

Procedure:

1. If *sibo* does not contain Signature string with RSASSA-PSS signature format (ISO/IEC 14888-2), FAIL the test and skip other steps.
2. If secure hash algorithms of Signature string does not correspond to SHA-256 (as specified in FIPS 180-4), FAIL the test and skip other steps.
3. If an RSA modulus length < 2048 bits, FAIL the test and skip other steps.

4. If Signature does not correspond to hash of *exportedFile*, FAIL the test and skip other steps.

Procedure Result:

PASS –

- DUT passes all assertions.

FAIL –

- None.