ONVIF®

Security Baseline Device Test Specification

Version 26.06

June 2026

REVISION HISTORY

Vers.	Date	Description
26.06	Feb 11, 2026	Initial version

Table of Contents

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 Specifications ([ONVIF Network Interface Specs]) and ONVIF Conformance Process Specification ([ONVIF Conformance]) requirements. In addition, the test cases are to be basic inputs for some Profiles and Add-Ons 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 Security Baseline Device Test Specification acts as a supplementary document to the [ONVIF Network Interface Specs], illustrating test cases need to be executed and passed. In addition, this specification acts as an input document to the development of test tool that 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 Security Baseline Device Test Specification ([ONVIF Baseline Device Test Spec]) 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 is to provide test cases to test individual requirements of ONVIF devices defined in ONVIF Security Baseline Specification ([ONVIF Baseline]).

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).
- Full coverage of network protocol implementation test for HTTP, HTTPS, RTP, RTSP, and TLS protocols.

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 Baseline Device Test Spec] covers the [ONVIF Baseline], which is a block of [ONVIF Network Interface Specs] which contains security baseline requirements.

This specification covers the following [ONVIF Baseline] versions:

- 26.06

The following use cases are covered:

- Key Generation Use Case (see Section 5.2)
- Certificate Upload Use Case (see Section 5.3)
- PKCS#8 Upload Use Case (see Section 5.4)
- PKCS#12 Upload Use Case (see Section 5.4)
- TLS Handshake Use Case (see Section 5.4)
- JWT Authentication Use Case (see Section 5.6)
- Recording To Object Storage Use Case (see Section 5.7)

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 Specifications:

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

- [ONVIF Baseline] ONVIF Security Baseline Specification:

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

- [ONVIF Security Configuration Service] ONVIF Security Configuration Specifications:

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

- [ONVIF Base Test] ONVIF Base Device Test Specifications:

  https://www.onvif.org/profiles/conformance/device-test/

- [ONVIF Feature Discovery] ONVIF Device Feature Discovery Specification:

  https://www.onvif.org/profiles/conformance/device-test/

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 defines terms that are specific to the ONVIF Security Configuration Service and tests. For a list of applicable general terms and definitions, please see [ONVIF Base Test].

Key	A key is an input to a cryptographic algorithm. Sufficient randomness of the key is usually a necessary condition for the security of the algorithm. This specification supports both RSA and ECC key pairs as keys.
Key Pair	A key that consists of a public key and (optionally) a private key.
Key Pair Algorithm	A key pair algorithm is used in this specification to indicate to the algorithm of key or key pair. This specification supports both RSA and ECC key pair algorithms.
Key Pair Generation Parameters	A key pair generation parameters is used in this specification as representing of generation parameters for several key pair algorithms. This specification supports both RSA and ECC key pair generation parameters.
RSA key pair	A key pair that is accepted as input by the RSA algorithm.
ECC key pair	A key pair that is accepted as input by the ECC algorithm.
RSA key pair generation Parameters	A key pair generation parameters that is accepted as input by the RSA key pair generation algorithm.
ECC key pair generation parameters	A key pair generation parameters that is accepted as input by the ECC key pair generation algorithm.
Digital Signature	A digital signature for an object allows to verify the object's authenticity, i.e., to check whether the object has in fact been created by the signer and has not been modified afterwards. A digital signature is based on a key pair, where the private key is used to create the signature and the public key is used for verification of the signature.
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 (the certification authority) to allow for verifying its authenticity.
Certification Path	A certification path is a sequence of certificates in which the signature of each certificate except for the last certificate can be verified with the subject public key in the next certificate in the sequence.
Certification Authority	A certification authority is an entity that issues certificates to subject entities.

Alias	An alias is a name for an object on the device that is chosen by the client and treated transparently by the device.

3.3 Abbreviations

This section describes abbreviations used in this document.

CA Certification Authority

CSR Certificate Signing Request (also called Certification Request)

SHA Secure Hashing Algorithm

TLS Transport Layer Security

4 Test Overview

This section provides information the test setup procedure and required prerequisites, and the test policies that should be followed for test case execution.

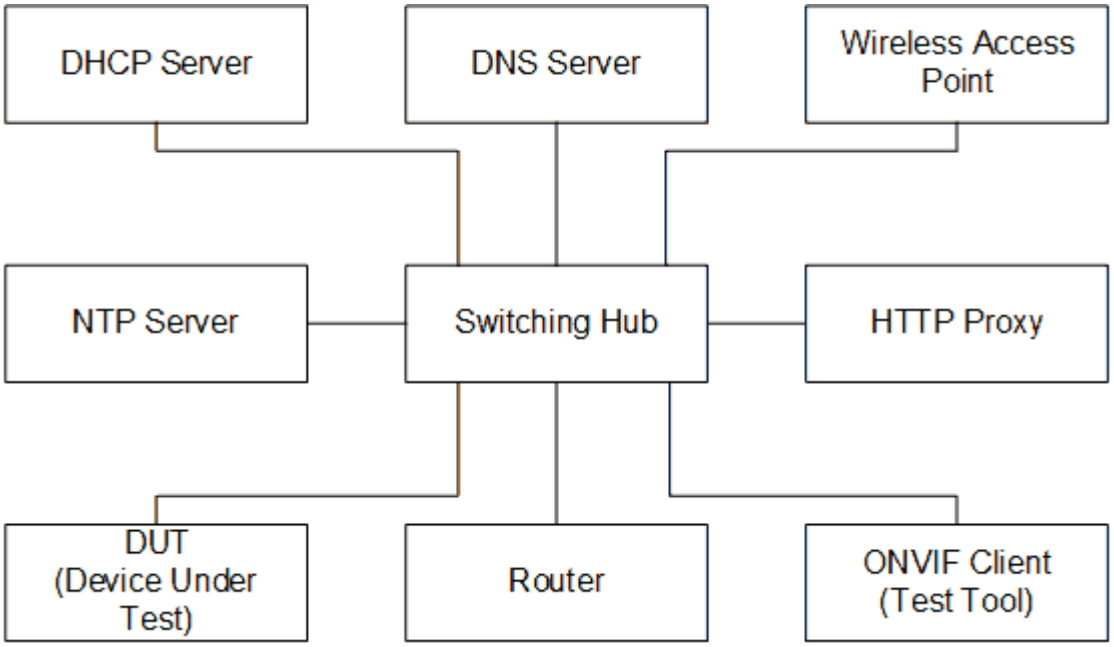
4.1 Test Setup

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:

- The DUT shall be configured with an IPv4 address.
- The DUT shall be IP reachable in the test configuration.
- The DUT shall be able to be discovered by the Test Tool.
- 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.
- The DUT time and Test tool time shall be synchronized with each other either manually or by a common NTP server.
- The ONVIF Client supports both WS-Security Username Token profile and HTTP digest authentication as authentication functionalities and selects the authentication method to use based on the procedure defined in Sect. 3.3.6 (Authentication method selection as a testing framework) of [ONVIF Base Test Spec].
- The user account that is used by the ONVIF Client for issuing commands to the DUT has administrative rights.
- The ONVIF Client shall have access to a certification authority.
- The DUT shall have enough free storage capacity for RSA key pairs that is required for test cases (see test cases pre-requisites for more information).
- The DUT shall have enough free storage capacity for ECC key pairs that is required for test cases (see test cases pre-requisites for more information).
- The DUT shall have enough free storage capacity for certificates that is required for test cases (see test cases pre-requisites for more information).

- The DUT shall have enough free storage capacity for certification paths that is required for test cases (see test cases pre-requisites for more information).
- The DUT shall have enough free storage capacity for server certificate assignment that is required for test cases (see test cases pre-requisites for more information).

4.3 Test Policy

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

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

4.3.1 General Policy

Test cases includes the following test policies specific to the test case execution of all functional blocks:

- Test cases will check which [ONVIF Baseline] version(s) shall be supported by the DUT are defined by procedure described at [ONVIF Feature Discovery].
- Test cases will check the DUT capabilities to verify that required capability is supported.
- If requirement support is not possible to verify only with capabilities check (there are not related capability), test cases will perform functional testing to check the requirement.
- For some sections existing test cases covered by other Test Specifications could be used, so section will contain links to this test cases.

Note: functional testing for the functionalities is covered by other ONVIF Device Test Specifications.

5 Security Baseline Test Cases

5.1 Capabilities

5.1.1 Check Supported Capabilities

Test Case ID: BASELINE-1-1-1

Specification Coverage: Asymmetric Encryption Schemes and Key Agreement (ONVIF Security Baseline Specification), Signatures (ONVIF Security Baseline Specification), Private Key Encryption (ONVIF Security Baseline Specification)

Feature under test: Key Generation Baseline

WSDL Reference: advancedsecurity.wsdl

Test Purpose:

- To verify that if DUT supports RSA key pair generation, DUT supports Key length required by ONVIF Security Baseline.
- To verify that if DUT supports ECC key pair generation, DUT supports elliptic Curve required by ONVIF Security Baseline.
- To verify that DUT supports signatures required by ONVIF Security Baseline.
- To verify that if DUT supports PKCS#12 upload, DUT supports private key encryption required by ONVIF Security Baseline.
- To verify that if DUT supports PKCS#8 upload, DUT supports private key encryption required by ONVIF Security Baseline.

Pre-Requisite:

- Security Configuration Service is received from the DUT.

Test Configuration: ONVIF Client and DUT

Test Procedure:

1. Start an ONVIF Client.
2. Start the DUT.
3. ONVIF Client gets the security configuration service capabilities by following the procedure mentioned in Annex A.1 with the following input and output parameters:

- out *capSecurity* - Security Configuration Service Capabilities

4. If *capSecurity*.RSAKeyPairGeneration = true or *capSecurity*.KeyPairGeneration contains **RSA**:

   4.1. ONVIF Client checks which RSA key lengths (*rsaLengths*) the DUT shall support depending on required Security Baseline versions by the rules defined in Section 6.1.

   4.2. If *capSecurity*.KeystoreCapabilities.RSAKeyLengths does not contains all items listed in *rsaLengths*, FAIL the test and skip other steps.

5. If *capSecurity*.ECCKeyPairGeneration = true or *capSecurity*.KeyPairGeneration contains **ECC**:

   5.1. ONVIF Client checks which ECC elliptic curves (*ellipticCurves*) the DUT shall support depending on required Security Baseline versions by the rules defined in Section 6.2.

   5.2. If *capSecurity*.KeystoreCapabilities.EllipticCurves does not contains all items listed in *ellipticCurves*, FAIL the test and skip other steps.

6. ONVIF Client checks which signature algorithms (*signatureAlgorithms*) the DUT shall support depending on required Security Baseline versions by the rules defined in Section 6.3.

7. If *capSecurity*.KeystoreCapabilities.SignatureAlgorithms does not contains all items listed in *signatureAlgorithms* with parameters, FAIL the test and skip other steps.

8. If *capSecurity*.PKCS12CertificateWithRSAPrivateKeyUpload = true or *capSecurity*.PKCS12 = true or *capSecurity*.PKCS8RSAKeyPairUpload = true or *capSecurity*.PKCS8 = true:

   8.1. ONVIF Client checks which password based encryption algorithms (*passwordBasedEncryptionAlgorithms*) the DUT shall support depending on required Security Baseline versions by the rules defined in Section 6.4.

   8.2. If *capSecurity*.KeystoreCapabilities.PasswordBasedEncryptionAlgorithms does not contains all items listed in *passwordBasedEncryptionAlgorithms*, FAIL the test and skip other steps.

Test Result:

PASS –

- The DUT passes all assertions.

FAIL –

- The DUT does not pass all assertions.

5.2 Key Generation Use Case

Security Baseline test cases related to Key Generation use case are covered with the following test cases from other sections/test specifications:

- BASELINE-1-1-1

5.3 Certificate Upload Use Case

Security Baseline test cases related to Key Generation use case are covered with the following test cases from other sections/test specifications:

- BASELINE-1-1-1
- BASELINE-3-1-1

5.3.1 Check Upload Certificate Without Private Key

Test Case ID: BASELINE-3-1-1

Specification Coverage: Asymmetric Encryption Schemes and Key Agreement (ONVIF Security Baseline Specification)

Feature under test: Certificates Baseline

WSDL Reference: advancedsecurity.wsdl

Test Purpose:

- Check that DUT upload certificates with keys pair parameters that required by ONVIF Security Baseline for certificates without private key only.

Pre-Requisite:

- Security Configuration Service is received from the DUT.

Test Configuration: ONVIF Client and DUT

Test Procedure:

1. Start an ONVIF Client.
2. Start the DUT.
3. ONVIF Client gets the security configuration service capabilities by following the procedure mentioned in Annex A.1 with the following input and output parameters:
   - out *capSecurity* - Security Configuration Service Capabilities

4. ONVIF Client checks which key pairs for certificate upload with public key only (*keyPairTypesList*) the DUT shall support depending on required Security Baseline versions by the rules defined in Section 6.3.

5. For each key pair type (*keyPairType*) from *keyPairTypesList* repeat the following steps:

   5.1. Create key pair (out *keyPair*) with new public key and private key with the following properties:

   - *keyPairType*

   5.2. ONVIF Client selects signature algorithm by following the procedure mentioned in Annex A.2 with the following input and output parameters:

   - in *cap* - DUT capabilities
   - in *keyPairType*.Algorithm - key pair algorithm
   - out *signatureAlgorithm* - signature algorithm

   5.3. ONVIF Client creates an X.509 self-signed CA certificate (*CAcert*) that is compliant to [RFC 5280] and has the following properties:

   - version := v3
   - signature := *signatureAlgorithm*
   - validity := not before 19700101000000Z and not after 99991231235959Z
   - subject := "CN=ONVIF TT,C=US"
   - public key := *keyPair*.publicKey
   - private key to be used := *keyPair*.privateKey

   5.4. ONVIF Client invokes **UploadCertificate** with parameters

   - Certificate := *CAcert*
   - Alias := "ONVIF_Test"
   - PrivateKeyRequired := false

   5.5. The DUT responds with a **UploadCertificateResponse** message with parameters

   - CertificateID =: *certificateID*
   - KeyID =: *keyPairID*

5.6. ONVIF Client deletes certificate and key pair by following the procedure mentioned in Annex A.3 with the following input and output parameters:

- in *certificateID* - certificate ID
- in *keyPairID* - key pair id

Test Result:

PASS –

- The DUT passes all assertions.

FAIL –

- DUT did not send **UploadCertificateResponse** message.

5.4 PKCS#8 Upload Use Case

Security Baseline test cases related to PKCS#8 Upload use case are covered with the following test cases from other sections/test specifications:

- BASELINE-1-1-1

5.5 PKCS#12 Upload Use Case

Security Baseline test cases related to PKCS#12 Upload use case are covered with the following test cases from other sections/test specifications:

- BASELINE-1-1-1

5.6 TLS Handshake Use Case

Security Baseline test cases related to TLS Handshake Use Case use case are covered with the following test cases from other sections/test specifications:

- DUT as TLS Server
  - ADVANCED_SECURITY-3-2-8
  - ADVANCED_SECURITY-3-2-6
- DUT Connection to External Server
  - Uplink Remote Client

  - UPLINK-1-1-2
  - UPLINK-1-2-1
- DUT Connection to Signaling Server
  - MEDIA2_RTSS-7-1-1

5.7 JWT Authentication Use Case

Security Baseline test cases related to JWT Authentication Use Case use case are covered with the following test cases from other sections/test specifications:

- MEDIA2_RTSS-7-1-5
- MEDIA2_RTSS-7-1-8
- UPLINK-3-1-3
- UPLINK-3-1-7
- DEVICE-10-2-3
- DEVICE-10-2-4

5.8 Recording To Object Storage Use Case

Security Baseline test cases related to Recording To Object Storage Use Case use case are covered with the following test cases from other sections/test specifications:

- RECORDING-2-2-15
- RECORDING-2-2-16

6 Security Baseline Requirements

6.1 RSA Key Lengths

Depending on [ONVIF Baseline] version(s) that shall be supported values defined in the table Table 6.1 to be added to required list.

Table 6.1. RSA Key Lengths for Baseline Versions

RSA Key Length	Security Baseline Versions
3072	26.06

6.2 ECC Elliptic Curves

Depending on [ONVIF Baseline] version(s) that shall be supported values defined in the table Table 6.2 to be added to required list.

Table 6.2. ECC Elliptic Curves for Baseline Versions

ECC Elliptic Curve	Security Baseline Versions
secp256r1	26.06
secp384r1	26.06

6.3 Signature Algorithms

Depending on [ONVIF Baseline] version(s) that shall be supported values defined in the table Table 6.3 to be added to required list.

Table 6.3. Signature Algorithms for Baseline Versions

Signature Algorithms (oid)	Additional Signature Algorithms Parameters Check	Security Baseline Versions
1.2.840.113549.1.1.11	No additional checks	26.06
1.2.840.113549.1.1.12	No additional checks	26.06
1.2.840.113549.1.1.13	No additional checks	26.06
1.2.840.10045.4.3.2	No additional checks	26.06
1.2.840.10045.4.3.3	No additional checks	26.06
1.2.840.10045.4.3.4	No additional checks	26.06

Signature Algorithms (oid)	Additional Signature Algorithms Parameters Check	Security Baseline Versions
1.2.840.113549.1.1.10	hashAlgorithm = id-sha256	26.06
1.2.840.113549.1.1.10	hashAlgorithm = id-sha384	26.06
1.2.840.113549.1.1.10	hashAlgorithm = id-sha512	26.06

6.4 Password Based Encryption Algorithms

Depending on [ONVIF Baseline] version(s) that shall be supported values defined in the table Table 6.4 to be added to required list.

Table 6.4. Password Based Encryption Algorithms for Baseline Versions

PasswordBasedEncryptionAlgor	Security Baseline Versions	
PBKDF2	26.06	
AES-128-CBC	26.06	

6.5 Public Keys Types For Certificate Upload With Public Key Only

Depending on [ONVIF Baseline] version(s) that shall be supported values defined in the table Table 6.5 to be added to required list.

Table 6.5. Public Keys Types For Certificate Upload With Public Key Only for Baseline Versions

Key Type	Key Parameters	Security Baseline Versions
RSA	Length = 4096	26.06

6.6 TLS Cipher Requirements

Depending on [ONVIF Baseline] version(s) that shall be supported values defined in the table Table 6.6 to be added to required list.

Table 6.6. TLS Cipher for Baseline Versions

Key Algorithm	Cipher	Security Baseline Versions
RSA	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	26.06

Key Algorithm	Cipher	Security Baseline Versions
ECC	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	26.06

6.7 Private Key JWT Authentication Algorithms Requirements

Depending on [ONVIF Baseline] version(s) that shall be supported values defined in the table Table 6.7 to be added to required list.

Table 6.7. Private Key JWT Algorithms for Baseline Versions

Key Type	Parameters	Private Key JWT Algorithms	Security Baseline Versions
RSA	Length = 3072	RS256	26.06
ECC	Curve = secp256r1	ES256	26.06

6.8 Recording Asymmetric Encryption Version 1 Requirements

Depending on [ONVIF Baseline] version(s) that shall be supported values defined in the table Table 6.8 to be added to required list.

Table 6.8. Recording Asymmetric Encryption With RSA for Baseline Versions

OAEP-PSS Digest Algorithms	Security Baseline Versions
id-sha256 (OID 2.16.840.1.101.3.4.2.1)	26.06
id-sha384 (OID 2.16.840.1.101.3.4.2.2)	26.06
id-sha512 (OID 2.16.840.1.101.3.4.2.3)	26.06

6.9 Recording Asymmetric Encryption Version 2 Requirements

Depending on [ONVIF Baseline] version(s) that shall be supported values defined in the table Table 6.9 to be added to required list.

Table 6.9. Recording Symmetric Encryption for Baseline Versions

HPKE KEM Identifiers	HPKE KDF Identifiers	HPKE AEAD Identifiers	Security Baseline Versions
DHKEM(P-256, HKDF-SHA256)	HKDF-SHA256	AES-256-GCM	26.06

Annex A Helper Procedures and Additional Notes

A.1 Get service capabilities for Advanced Security service

Name: HelperGetServiceCapabilities_AdvancedSecurity

Notes: Annex is used at:

- ONVIF Real Time Streaming using Media2 Device Test Specification
- ONVIF Security Configuration Device Test Specification
- ONVIF Base Device Test Specification
- ONVIF Media2 Configuration Device Test Specification
- ONVIF Uplink Device Test Specification
- ONVIF Recording Control Device Test Specification

Procedure Purpose: Helper procedure to get service capabilities.

Pre-requisite: Security Configuration Service is received from the DUT.

Input: None

Returns: The service capabilities (*cap*).

Procedure:

1. ONVIF Client invokes **GetServiceCapabilities** request.
2. The DUT responds with **GetServiceCapabilitiesResponse** message with parameters:
   - Capabilities =: *cap*

Procedure Result:

PASS –

- DUT passes all assertions.

FAIL –

- DUT did not send **GetServiceCapabilitiesResponse** message.

A.2 Signature Algorithm Selection

Name: HelperSignatureAlgorithmSelection

Notes: Annex is used at:

- ONVIF Real Time Streaming using Media2 Device Test Specification
- ONVIF Security Configuration Device Test Specification
- ONVIF Base Device Test Specification
- ONVIF Uplink Device Test Specification
- ONVIF Recording Control Device Test Specification

Procedure Purpose: Helper procedure to select signature algorithm which will be used for tests based on Device capabilities.

Pre-requisite: Security Configuration Service is received from the DUT.

Input: The service capabilities (*cap*). The key pair algorithm (*keyAlgorithm*).

Returns: The signature algorithm (*signatureAlgorithm*).

Procedure:

1. If *keyAlgorithm* = RSA: ONVIF Client selects signature algorithm (*signatureAlgorithm*) that will be used for the test from the list provided by DUT at *cap*.KeystoreCapabilities.SignatureAlgorithms. Selection is done among the following list of signature algorithms supported by the Client by priority from first to last:
   - 1.2.840.113549.1.1.13 (OID of SHA-512 with RSA Encryption algorithm)
   - 1.2.840.113549.1.1.12 (OID of SHA-384 with RSA Encryption algorithm)
   - 1.2.840.113549.1.1.11 (OID of SHA-256 with RSA Encryption algorithm)
2. If *keyAlgorithm* = ECC: ONVIF Client selects signature algorithm (*signatureAlgorithm*) that will be used for the test from the list provided by DUT at *cap*.KeystoreCapabilities.SignatureAlgorithms. Selection is done among the following list of signature algorithms supported by the Client by priority from first to last:
   - 1.2.840.10045.4.3.4 (OID of SHA-512 with ECC Encryption algorithm)
   - 1.2.840.10045.4.3.3 (OID of SHA-384 with ECC Encryption algorithm)
   - 1.2.840.10045.4.3.2 (OID of SHA-256 with ECC Encryption algorithm)
3. If the previous steps is done with empty signature algorithm (*signatureAlgorithm*): FAIL the procedure.

Procedure Result:

PASS –

- DUT passes all assertions.

FAIL –

- DUT did not return any of signature algorithms listed at step 1 or 2.

A.3 Delete a certificate with corresponding key pair

Name: HelperDeleteCertWithKey

Notes: Annex is used at:

- ONVIF Real Time Streaming using Media2 Device Test Specification
- ONVIF Security Configuration Device Test Specification
- ONVIF Base Device Test Specification

Procedure Purpose: Helper procedure to delete a certificate and related RSA key pair.

Pre-requisite: Security Configuration Service is received from the DUT. Create self-signed certificate by the DUT as indicated by the SelfSignedCertificateCreation or SelfSignedCertificateCreationWithRSA, or PCKS#10 supported by the DUT as indicated by the PKCS10 or PKCS10ExternalCertificationWithRSA capability.

Input: The identifier of the certificate (*certID*) and key pair (*keyID*) to delete.

Returns: None

Procedure:

1. ONVIF Client invokes **DeleteCertificate** with parameters
   - CertificateID := *certID*
2. The DUT responds with **DeleteCertificateResponse** message.
3. ONVIF Client deletes the key pair (in *keyID*) by following the procedure mentioned in Annex A.4.

Procedure Result:

PASS –

- DUT passes all assertions.

FAIL –

- DUT did not send **DeleteCertificateResponse** message.

A.4 Delete a key pair

Name: HelperDeleteKeyPair

Notes: Annex is used at:

- ONVIF Real Time Streaming using Media2 Device Test Specification
- ONVIF Security Configuration Device Test Specification
- ONVIF Base Device Test Specification
- ONVIF Uplink Device Test Specification

Procedure Purpose: Helper procedure to delete a key pair.

Pre-requisite:

- Security Configuration Service is received from the DUT.
- On-board ECC or RSA key pair generation is supported by the DUT as indicated by the RSAKeyPairGeneration capability, or by the ECCKeyPairGeneration capability, or by the KeyPairGeneration capability, which contains RSA or ECC.

Input: The identifier of the key pair (*keyID*) to delete.

Returns: None

Procedure:

1. ONVIF Client invokes **DeleteKey** with parameters
   - KeyID := *keyID*
2. DUT responds with a **DeleteKeyResponse** message.

Procedure Result:

PASS –

- DUT passes all assertions.

FAIL –

- DUT did not send **DeleteKeyResponse** message.