

ONVIF™ Security Baseline Specification

Version 26.06

June, 2026



Copyright © 2008-2026 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.

CONTENTS

1	Scope	4
2	Normative References	4
3	Definitions	5
4	Overview	5
5	Asymmetric Encryption Schemes and Key Agreement	5
6	Symmetric Encryption Schemes	6
7	Hash Functions	6
8	Signatures	6
9	Key Derivation	7
10	Private Key Encryption	7
11	JWT	7
Annex A	TLS Cipher Reference (Informative)	8
Annex B	Hybrid Public Key Encryption (Informative)	9
Annex C	Secure Streaming using SRTP (Informative)	10
Annex D	Revision History	11

1 Scope

This document defines the security baseline for ONVIF specifications. Its content is based on state-of-the-art technology as published by NIST or BSI.

Note, that any updates to this specification require a review of implications on technical, profile and add-on specifications. Publication of updates to this document must be synchronized with ONVIF Technical and Technical Service Committees.

2 Normative References

NIST FIPS 180-4 Secure Hash Standard (SHS)

<<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>>

NIST FIPS 186-5 Digital Signature Standard (DSS) - February 3, 2023

<<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf>>

BSI – Technical Guideline, Cryptographic Mechanisms: Recommendations and Key Lengths - January 31, 2025

<https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=9>

RFC 4055 - Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

<<https://datatracker.ietf.org/doc/html/rfc4055>>

RFC 4868 - Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec

<<https://datatracker.ietf.org/doc/html/rfc4868>>

RFC 5116 - An Interface and Algorithms for Authenticated Encryption

<<https://datatracker.ietf.org/doc/html/rfc5116>>

RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

<<http://www.ietf.org/rfc/rfc5280.txt>>

RFC 5480 - Elliptic Curve Cryptography Subject Public Key Information

<<https://datatracker.ietf.org/doc/html/rfc5480>>

RFC 5758 - Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA

<<https://datatracker.ietf.org/doc/html/rfc5758>>

RFC 5869 - HMAC-based Extract-and-Expand Key Derivation Function (HKDF)

<<https://datatracker.ietf.org/doc/html/rfc5869>>

RFC 7292 - PKCS #12: Personal Information Exchange Syntax v1.1

<<https://datatracker.ietf.org/doc/html/rfc7292>>

RFC 7714 - AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP)

<<https://datatracker.ietf.org/doc/html/rfc7714>>

RFC 7519 - JSON Web Token (JWT)

<<https://datatracker.ietf.org/doc/html/rfc7519>>

RFC 8017 - PKCS #1: RSA Cryptography Specifications Version 2.2

<<https://datatracker.ietf.org/doc/html/rfc8017>>

RFC 8018 - PKCS #5: Password-Based Cryptography Specification Version 2.1

<<https://datatracker.ietf.org/doc/html/rfc8018>>

RFC 8439 - ChaCha20 and Poly1305 for IETF Protocols

<<https://datatracker.ietf.org/doc/html/rfc8439>>

RFC 9579 - Use of Password-Based Message Authentication Code 1 (PBMAC1) in PKCS #12 Syntax

<<https://datatracker.ietf.org/doc/html/rfc9579>>

ANSI X9.62 - Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)

<<https://webstore.ansi.org/standards/ascx9/ansix9622005>>

3 Definitions

Asymmetric Encryption	Encryption with public and private key pair.
Hash	Method to create a unique fingerprint of a large data set.
Signature	Private key signed hash that can be verified with the corresponding public key.

4 Overview

The content of this document is based on state-of-the-art technology as published by the American institute NIST and the German department BSI. Note, that any updates to this specification require a review of implications on technical, profile and add-on specifications.

Publication of updates must be synchronized with ONVIF Technical and Technical Service Committees

5 Asymmetric Encryption Schemes and Key Agreement

Baseline for asymmetric encryption and key agreement schemes that a device shall support when it signals support for the algorithm.

Table 1: Asymmetric Key Schemes

Name	Key Length	Comment
RSA	3072 Bit	RSA Baseline
RSA	4096 Bit	Public key usage
secp256r1	256 Bit	EC Baseline
secp384r1	384 Bit	

Table 2: Asymmetric Encryption Algorithm OIDs

Name	OID	Reference
rsaEncryption	1.2.840.113549.1.1.1	RFC 8017
secp256r1	1.2.840.10045.3.1.7	RFC 5480
secp384r1	1.3.132.0.34	RFC 5480

6 Symmetric Encryption Schemes

Symmetric encryption algorithms that a device shall support

Table 3: Symmetric Encryption Schemes

Name	Key Length	Comment
AES-GCM	128 Bit	RFC 5116

7 Hash Functions

Table 4: Hashes

Name	Size	Reference
SHA-2	256 Bit	FIPS 180-4
SHA-2	384 Bit	FIPS 180-4
SHA-2	512 Bit	FIPS 180-4

Table 5: Standalone Hash Algorithm OIDs

Name	OID	Reference
id-sha256	2.16.840.1.101.3.4.2.1	FIPS 180-4
id-sha384	2.16.840.1.101.3.4.2.2	FIPS 180-4
id-sha512	2.16.840.1.101.3.4.2.3	FIPS 180-4

8 Signatures

This chapter defines the signature schemes and their corresponding algorithm OIDs that devices shall support.

Table 6: Signature Schemes

Scheme	Hash	Reference
RSA PKCS1 v1_5	SHA 256, SHA 384, SHA 512	RFC 8017 not recommended
RSASSA-PSS	SHA 256, SHA 384, SHA 512	RFC 8017
ECDSA	SHA 256, SHA 384, SHA 512	RFC 5758, X9.62

The signature algorithm OIDs listed below are applicable to certificate signatures as well as other cryptographic operations such as media signing and general-purpose digital signatures.

Table 7: Signature Algorithm OIDs

Name	OID	Reference
sha256WithRSAEncryption	1.2.840.113549.1.1.11	RFC 4055
sha384WithRSAEncryption	1.2.840.113549.1.1.12	RFC 4055
sha512WithRSAEncryption	1.2.840.113549.1.1.13	RFC 4055

Name	OID	Reference
ecdsa-with-SHA256	1.2.840.10045.4.3.2	RFC 5758, X9.62
ecdsa-with-SHA384	1.2.840.10045.4.3.3	RFC 5758, X9.62
ecdsa-with-SHA512	1.2.840.10045.4.3.4	RFC 5758, X9.62
rsassa-pss	1.2.840.113549.1.1.10	RFC 8017

9 Key Derivation

Table 8: Key Derivation Functions

Name	Reference	Comment
PBKDF2	RFC 8018 & RFC 9579	for passwords
HKDF	RFC 5869	for random keys

10 Private Key Encryption

Requirements for encrypting private keys during certificate upload and creation.

Table 9: Baseline for Encrypting Private Key

Name	Reference	Capability
PBKDF2	RFC 8018	PasswordBasedEncryptionAlgorithms
AES-128-CBC	RFC 7292	

11 JWT

Requirements for JWT signature algorithm.

Table 10: Signature Baseline

Name	Reference
RS256	RFC 7519
ES256	RFC 7519

Annex A.

TLS Cipher Reference (Informative)

This Annex is advocating a small subset of Ciphers as part of the ONVIF standard that readers of this specification can use as an informative guide.

The following small subset of ciphers covering TLS 1.2 / 1.3 are based on the baseline defined in this document and match common practise by Cloudflare, Mozilla, and ciphersuite.info.

While TLS 1.2 and 1.3 are both currently viable, TLS 1.3 is preferred. Do note that the table is not ordered by the strength of the cipher.

Table A.1: TLS 1.3 / 1.2 Cipher list

Minimum Protocol	IANA Name
TLS 1.3	TLS_AES_256_GCM_SHA384
TLS 1.3	TLS_CHACHA20_POLY1305_SHA256
TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS 1.2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Annex B.

Hybrid Public Key Encryption (Informative)

This section lists the HPKE encryption baseline and links them to the relevant IANA registry. The listed algorithms map to the definitions in the normative sections above.

Table B.1: HPKE KEM Identifiers

IANA Registry	Algorithm
0x0010	DHKEM(P-256, HKDF-SHA256)

Table B.2: HPKE KDF Identifiers

IANA Registry	Algorithm
1	HKDF-SHA256

Table B.3: HPKE AEAD Identifiers

IANA Registry	Algorithm
2	AES-256-GCM

Annex C.

Secure Streaming using SRTP (Informative)

This section lists the security baseline for SRTP streaming and links them to the relevant IANA registry. The listed algorithms map to the definitions in the normative sections above.

Table C.1: SRTP Identifiers

Algorithm	Reference
AEAD_AES_128_GCM	RFC 7714

Annex D. Revision History

Rev.	Date	Editor	Changes
25.12	Dec-2025	Hans Busch	First release
26.06	Jun-2026	Ottavio Campana, Sujith Raman.	Editorial fixes.