ETSI TS 104 107 V9.0.0 (2025-05)

Publicly Available Specification (PAS); O-RAN Security Protocols Specifications (O-RAN.WG11.Security-Protocols-Specification.O-R003-v09.00)

CAUTION

The present document has been submitted to ETSI as a PAS produced by O-RAN Alliance and approved by the ETSI Technical Committee Mobile Standards Group (MSG).

Reference
DTS/MSG-001159

Keywords
O-RAN, protocol, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by O-RAN Alliance and approved by ETSI Technical Committee Mobile Standards Group (MSG).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document specifies security protocols as to be used for O-RAN compliant implementation.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE 1: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

NOTE 2: All specifications issued by IETF referenced in the present document are valid in the latest version which the IETF declares as valid. Any updates to valid RFCs have to be considered and implemented, if applicable.

[1] Void.

[2] IETF RFC 4252: "The Secure Shell (SSH) Authentication Protocol".

[3] Void.

[4] Void.

[5] IANA: "Secure Shell (SSH) Protocol Parameters".

[6] O-RAN ALLIANCE TS: "O-RAN Management Plane Specification".

[7] Void.

[8] IANA: "Transport Layer Security (TLS) Parameters", Retrieved 2021-01-21.

[9] Void.

[10] O-RAN-WG1.O1-Interface-v04.00: "O-RAN Operations and Maintenance Interface Specification v04.00".

[11] IETF RFC 6668: "SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol", July 2012.

[12] IETF RFC 8268: "More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH)", December 2017.

[13] IETF RFC 8308: "Extension Negotiation in the Secure Shell (SSH) Protocol", March 2018.

[14] IETF RFC 8332: "Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol", March 2018.

[15] IETF RFC 8709: "Ed25519 and Ed448 Public Key Algorithms for the Secure Shell (SSH) Protocol", February 2020.

[16] Void.

[17] Void.

[18] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[19] Void.

[20] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

[21] Void.

[22] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[23] IETF RFC 9147: "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3".

[24] IETF RFC 6083: "Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[25] Void.

[26] ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310)".

[27] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[28] 3GPP TS 33.401 (V16.0.0): "3GPP System Architecture Evolution (SAE); Security architecture (Release 15)".

[29] ETSI TS 133 501 (V16.6.0): "5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.6.0 Release 16)".

[30] Void.

[31] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[32] Void.

[33] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

[34] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[35] IETF RFC 6749: "The OAuth 2.0 Authorization framework".

[36] IETF RFC 7519: "JSON Web Token (JWT)".

[37] IETF RFC 7515: "JSON Web Signature (JWS)".

[38] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)".

[39] IETF RFC 4211: "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)".

[40] NIST: "Cryptographic Standards and Guidelines".

[41] Void.

[42] FIPS 186 series: "Digital Signature Standard (DSS)", National Institute of Standards and Technology.

[43] Void.

[44] FIPS 197: "Advanced Encryption Standard (AES)", National Institute of Standards and Technology.

[45] Void.

[46] Void.

[47] FIPS 202: "NIST Permutation-Based Hash and Extendable-Output Function".

[48] NIST SP 800-131A: "Transitioning the Use of Cryptographic Algorithms and Key Lengths".

[49] Void.

[50] IETF RFC 8017: "PKCS #1: RSA Cryptography Specifications Version 2.2".

[51] Void.

[52] IANA: "Transport Layer Security (TLS) Parameters", Accessed May 7, 2022.

[53] Void.

[54] IETF RFC 6125: "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)".

[55] IETF RFC 7633: "X.509v3 Transport Layer Security (TLS) Feature Extension".

[56] CA-Browser-Forum-BR-1.8.0: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", August 2021.

[57] Void.

[58] Void.

[59] Void.

[60] IETF RFC 7093: "Additional Methods for Generating Key Identifiers Values".

[61] Void.

[62] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[63] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[64] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[65] SFTPv3: "SFTP Industry Best Practice".

[66] IETF RFC 4217: "Securing FTP with TLS".

[67] ETSI TS 128 532: "5G; Management and orchestration; Generic management services (3GPP TS 28.532)".

[68] ETSI TS 128 537: "5G; Management and orchestration; Management capabilities (3GPP TS 28.537)".

[69] IETF RFC 9110: "HTTP Semantics".

[70] IETF RFC 4253: "The Secure Shell (SSH) Transport Layer Protocol".

[71] IETF RFC 9325: "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)".

[72] IETF RFC 3279: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[73] FIPS 180-4: "Secure Hash Standard (SHS)", National Institute of Standards and Technology.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

[i.2] Mozilla Wiki: "Security/Server Side TLS", 2 January 2020. .

[i.3] OWASP Cheat Sheet Series: "TLS Cipher String Cheat Sheet", 2020.

[i.4] NIST Special Publication 800-52.2: "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations", Kerry McKay (NIST), David Cooper (NIST), August 2019. .

[i.5] 3GPP TR 33.821 (V9.0.0): "Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE) (Release 9)".

[i.6] BSI TR-02102-1: "BSI Technical Guideline - Designation: Cryptographic Mechanisms: Recommendations and Key Lengths", 2022-01.

[i.7] NIST SP 800-38 series: "Recommendation for Block Cipher Modes of Operation".

[i.8] NIST SP 800-186: "Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters".

[i.9] NIST SP 800-57: "Recommendation for Key management".

[i.10] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.11] Void.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 121 905 [i.1] and the following apply.

NOTE: An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in ETSI TR 121 905 [i.1].

CA	Certification Authority
CMP	Certificate Management Protocol
DH	Diffie–Hellman
DPD	Dead Peer Detection
DTLS	Datagram Transport Layer Security
ESP	Encapsulating Security Payload
FTPES	Explicit SSL File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IPsec	Internet Protocol security
NAT	Network Address Translation
NE	Network Element
NETCONF	Network Configuration protocol
PKI	Public Key Infrastructure
RA	Registration Authority
SA	Security Association
SFTP	SSH File Transfer Protocol
SPD	Security Policy Database
SSH	Secure Shell
TLS	Transport Layer Security

4 Security protocols specifications for O-RAN compliant implementation

4.1 SSH

4.1.1 General requirements

O-RAN and 3GPP interfaces that implement authentication, confidentiality and integrity using SSH shall:

- Support SSHv2 [1] and [70].
- Disable by default cryptographically insecure ciphers as specified in clauses 4.1.2.1, 4.1.2.3 and 4.1.2.4 of the present document.
- Enable an O-RAN deployer to configure SSH to offer less secure ciphers using standard SSH configurations to enable backward compatibility with older SSH implementations.
- Enable remote shell access only if required by the interface. If remote shell access is enabled, disable remote login as root or equivalent highest privileged user. Such access shall be limited to the local system console only. Root user shall not be allowed to login to the system remotely.

Entities providing O-RAN components that support SSH for authentication, confidentiality or integrity shall:

- Stay current with SSH [5].
- Provide an upgrade path for changes to the SSH protocol and ciphers [5].

4.1.2 Required ciphers

4.1.2.0 Introduction

O-RAN requires the following ciphers when using SSH. For more information see [2], [5], [11], [12], [13], [14] and [15]. See the Security chapter of the O-RAN Working Group 4 Management Plane Specification for the M-plane mandated SSH ciphers [6].

4.1.2.1 Key agreement

Note that the present document uses the IANA cipher naming convention [5].

- Required
    a. ecdsa-sha2-nistp256
    b. ecdsa-sha2-nistp384
    c. ecdsa-sha2-nistp521
    d. ssh-ed25519
- Optional
    a. ssh-ed448
- Shall not be implemented
    a. ssh-rsa
    b. ssh-dss

4.1.2.2 Symmetric algorithms for encrypting transferred data

- Required
    a. aes256-gcm
    b. aes128-gcm
    c. aes256-ctr
    d. aes192-ctr
    e. aes128-ctr

4.1.2.3 Key exchange algorithms (KexAlgorithms)

- Required
    a. ecdh-sha2-nistp521
    b. ecdh-sha2-nistp384
    c. ecdh-sha2-nistp256
    d. diffie-hellman-group-exchange-sha256
    e. curve25519-sha256
- Shall not be implemented
    a. Diffie-hellman-group1-sha1

4.1.2.4 Message Authentication Codes (MACs)

- Required
  a. hmac-sha2-512-etm
  b. hmac-sha2-512
  c. hmac-sha2-256-etm
  d. hmac-sha2-256
  e. umac-128
- Shall not be implemented
  a. hmac-sha1

4.2 TLS

4.2.1 General requirements

4.2.1.0 Introduction

O-RAN interfaces that implement authentication, confidentiality and integrity using Transport Layer Security (TLS) shall:

- Support TLS 1.2 [18].
- Configure the TLS 1.2 Intermediate server ciphers as specified in [i.2] and [8].
- Support TLS 1.3 [18] and [i.4].
- Enable an O-RAN deployer to configure TLS 1.2 to offer less secure ciphers using standard TLS configurations to enable backward compatibility with weaker TLS ciphers.
- Disable by default cryptographically insecure ciphers identified in [8] and [i.3].

Entities providing O-RAN components that support TLS for authentication, confidentiality or integrity shall:

- Stay current with the latest release of the TLS software used to implement the protocol, such as OpenSSL.
- Provide an upgrade path for new software releases.

Any version of SSL and any version of TLS below 1.2, shall not be supported.

Entities providing O-RAN components that support TLS shall support mutual certificate-based authentication, i.e. client authentication shall be supported in TLS communications, also referred as mutual TLS authentication.

- A TLS server supporting TLS 1.2 shall request a certificate from the client as specified in [18] clause 7.4.4 and validate the certificate that is being returned from the client using the structure defined in [18] clause 7.4.2.
- A TLS server supporting TLS 1.3 shall request a certificate from the client as specified in [18] clause 4.3.2 and validate the certificate that is being returned from the client.

See the Security chapter of the O-RAN Working Group 4 Management Plane Specification for the M-plane mandated TLS ciphers [6].

4.2.1.1 Specific requirements

In addition, one-way TLS authentication may be supported with server certificate exchanged as specified in [18] clause 7.4.2 (TLS 1.2) or [18] clause 4.4.2 (TLS 1.3).

4.2.2 TLS Protocol profiles specifications

TLS 1.2 used on all interfaces except the Open Fronthaul interfaces shall support the TLS 1.2 profiles as defined by ETSI TS 133 210 [20] clause 6.2.3. See Chapter 5.4 Security in [6] for the M-plane mandated TLS ciphers [6].

TLS 1.3 used on all interfaces except the Open Fronthaul interfaces shall support the TLS 1.3 profiles as defined by ETSI TS 133 210 [20] clause 6.2.2. See Chapter 5.4 Security in [6] for the M-plane mandated TLS ciphers [6].

Use of a cipher suite in TLS shall be configurable. Broken ciphers should be removed from the list of negotiable ciphers.

O-RAN specified protocols using TLS may support additional TLS ciphers recommended by IANA [52].

4.2.3 Certificate Profile for TLS Entity

The present clause addresses the certificate profile requirements for the TLS entities that may behave either as client, server, or both. The structure of the TLS certificate profile described in this clause under Table 4-1 provides requirements based on the ETSI TS 133 310 [26], CA-browser forum [56] and NIST Special Publication 800-52.2 [i.4]. The TLS entity certificate profile shall be applied to all nodes and interfaces that use the TLS protocol for secured communication in the O-RAN network except the Open Fronthaul interfaces:

- The TLS entity certificates shall adhere to the certificate profile outlined in Table 4-1, based on their respective roles.
- The CA responsible for handling the certificate signing request shall ensure compliance in accordance with the certificate profile specified in clause 4.2.3.
- The common rules for all certificates defined in ETSI TS 133 310 [26], clause 6.1.1, clause 6.1.3.a shall apply.
- The CA-browser forum [56] has the following requirement for the certificate operational and key usage periods. Certificates issued on or after 1 September 2020 shall not have a Validity Period greater than 397 days.
- Certificate Policies: Certificate policies shall be crafted using the guidelines defined in IETF RFC 3647 [63].
- subjectAltName shall (for TLS server certificates) contain at least one FQDN(Hostname) and shall not contain only IP Address as described in IETF RFC 6066 [22]. As per IETF RFC 6125 [54], an application service shall be identified by a name or names carried in the subject field (i.e. a CN-ID) and/or in one of the following identifier types within subjectAltName entries (DNS-ID, SRV-ID. URI-ID).
- Optional and non-critical TLS Feature Extension: IETF RFC 7633 [55] defines a certificate extension that indicates that clients expect stapled OCSP responses with a value of "status_request (5)" for the certificate and aborts the handshake ("hard-fail") if such a response is not available. As per IETF RFC 9325 [71] TLS servers should support the following as a best practice: OCSP IETF RFC 6960 [62] and OCSP stapling using the status_request extension defined in IETF RFC 6066 [22]. The exact mechanism for embedding the status_request extension differs between TLS 1.2 and 1.3. As a matter of local policy, server operators may request that CAs issue must-staple IETF RFC 7633 [55] certificates for the server and/or for client authentication.
- Extensions: Mandatory Critical Key Usage:
  - digitalSignature for both TLS client and Server certificates. This applies for RSA signature certificate, ECDSA signature certificate, or DSA signature certificate.
  - When using RSA IETF RFC 3279 [72] with TLS 1.2, the keyEncipherment shall be set.
  - When using DH [72] or ECDH [72] with TLS 1.2, the keyAgreement shall be set.

The following table captures the certificate profile for the TLS entity that may behave as a client, server or both.

Table 4-1: TLS Client and Server Certificate Profile

ORAN TLS Client and Server Certificate Profile			
Version		v3.	
Serial Number		Shall be Unique Positive Integer in the context of the issuing CA	
Subject DN		(C=<country>), O=<Organization Name>, CN=<Some distinguishing name>. Organization and CN can be in UTF8 format. Note that C is optional element. cn=<hostname>, (ou=<servers>), dc=<domain>, dc=<domain>. Note that ou is an optional element.	
Validity Period		1 year or less.	
Signature		See clause 6.1.1 of ETSI TS 133 310 [26] for the list of supported signature algorithms.	
Subject Public Key Info		See clause 6.1.1 of ETSI TS 133 310 [26] for the list of supported public key types.	
Extensions	**Mandatory**	**Criticality**	**Value**
keyUsage	TRUE	TRUE	digitalSignature for TLS clients and servers.
extendedKeyUsage	FALSE	FALSE	id-kp-clientAuth TLS clients.
			id-kp-serverAuth for TLS servers.
			Entities that may be both client and server will have both OIDs set.
certificatePolicies	FALSE	FALSE	If added, then, it should be populated with a CP Object Identifier(OID). These OIDs correspond to specific policies established by the certificate issuer.
authorityKeyIdentifier	FALSE	FALSE	This is same as the subjectKeyIdentifier of the Issuer's certificate. CA utilizes the method as defined in clause 2 of IETF RFC 7093 [60].
subjectKeyIdentifier	FALSE	FALSE	This is calculated by the issuing CA utilizing method as defined in clause 2 of IETF RFC 7093 [60].
cRLDistributionPoint	TRUE	FALSE	distributionPoint According to IETF RFC 5280 [64] this indicates if the CRL is available for retrieval using access protocol and location with HTTP URI or LDAP.
subjectAltName	TRUE	TRUE	Multiple subjectAltNames are permitted and has been defined above
authorityInfoAccess	FALSE	FALSE	id-ad-caIssuers According to IETF RFC 5280 [64] id-ad-caIssuers describes the referenced description server and the access protocol and location, for example, using one or multiple HTTP and/or LDAP URIs. The referenced CA issuers description is intended to aid certificate users in the selection of a certification path that terminates at a point trusted by the certificate user
			id-ad-ocsp According to IETF RFC 5280 [64] id-ad-ocsp defines the location of the OCSP responder using HTTP URI.

ORAN TLS Client and Server Certificate Profile			
Extensions	**Mandatory**	**Criticality**	**Value**
TLS feature extension	FALSE	FALSE	id-pe-tlsfeature: status_request(5)" This can be used according to IETF RFC 7633 [55] to prevent downgrade attacks that are not otherwise prevented by the TLS protocol; IETF RFC 7633 [55] also defines a certificate extension that indicates that clients expects stapled OCSP responses with a value of "status_request(5)" for the certificate and aborts the handshake ("hard-fail") if such a response is not available.

4.3 Support NETCONF over secure Transport

TLS requirements for use with NETCONF on the O1 interface [10] are specified in clause 4.2.

TLS requirements for use with NETCONF on the Open Fronthaul M-plane are specified in clause 5.4 of the O-RAN WG4 Management Plane Specification [6].

4.4 DTLS

4.4.1 General requirements

O-RAN and 3GPP interfaces that implement mutual authentication, integrity protection, replay protection and confidentiality protection using DatagramTransport Layer Security (DTLS) shall:

- Support DTLS 1.2 [23];
- Support DTLS for Stream Control Transmission Protocol [24];

and should support DTLS 1.3 [23].

DTLS 1.0 shall not be supported.

NOTE: IETF RFC 6083 [24] specifies a user message limit of approximately 16 kbytes, which does not align with the unlimited user message size that exists when SCTP is used without DTLS. There could be applications messages exceeding the limit, preventing the use of DTLS over SCTP, so enforcing unsecured SCTP.

Entities providing O-RAN components that support DTLS for authentication, confidentiality or integrity shall:

- Stay current with the latest release of the DTLS software used to implement the protocol, such as OpenSSL.
- Provide an upgrade path for new software releases.

Pre-shared keys in the authentication mechanisms should not be used.

4.4.2 DTLS 1.2 profiling

DTLS 1.2 is based on TLS 1.2, so all requirements defined in clause 4.2 in the present document for TLS 1.2 shall apply to DTLS as well.

3GPP control plane interfaces in O-RAN system implementing DTLS 1.2 shall support all requirements defined in the profiling for TLS 1.2 specified in ETSI TS 133 210 [20], clause 6.2.3.

4.4.3 Certificate profiling

Certificate requirements defined in clause 4.2 in the present document for TLS 1.2 shall apply to DTLS as well.

3GPP control plane interfaces in O-RAN system implementing DTLS 1.2 shall support certificate profiling as given in clause 6.1.3a of ETSI TS 133 310 [26].

DTLS client certificates shall be directly signed by the DTLS client CA in the operator domain that the DTLS client belongs to. DTLS server certificates shall be directly signed by the DTLS server CA in the operator domain that the DTLS server belongs to.

4.5 IPSec

4.5.1 Overview

4.5.1.0 Supported IPsec capabilities

O-RAN and 3GPP interfaces that implement authentication, confidentiality and integrity using IPsec shall support IPsec according to [27]. The supported IPsec capabilities in this clause follow [20] for interworking purposes and further apply requirements given in [26], [28], [29] and [i.5].

4.5.1.1 Supported IPsec capabilities

Services that SHALL be supported (see also [29], section 9.8.2):

- Confidentiality, can be enabled/disabled (via ENCR_NULL)
- Integrity protection, always enabled
- Data origin authentication, always enabled
- Anti-replay protection, can be enabled/disabled
- Extended sequence numbers, can be enabled/disabled

Protocol that SHALL be supported: ESP ([31], as profiled by [20]):

- IPsec mode: Tunnel mode
- Copying the DSCP value from the inner IP-header to the outer IP-header for encrypted packets
- For encrypted packets the DSCP value of the inner packet will be copied to the outer packet
- NAT traversal

ESP encryption transforms that SHALL be supported (including authenticated encryption transforms, see also [20], section 5.3.3) as defined in [i.5] (the ones marked with 'MUST').

ESP authentication transforms that SHALL be supported according to [20], subsection 5.3.4:

- IKE endpoint Identification that SHALL be supported, according to [26], subsection 6.2.1b: IP address
- Fully Qualified domain name (FQDN) (if DNS is supported

Authentication that SHALL be supported:

- X.509v3 digital certificates provided by a Certificate Authority solution

Authentication that MAY be supported:

- Pre-shared Keys

NOTE: Pre-shared keys should not be used.

Key exchange that SHALL be supported:

- IKEv2 [33] profile as described in [26]

- Certificate-based authentication according to [26]
- Certificates according to the profile described by [26]
- DH group 19
- (Optional) DH group 20

Security Association multiplicity that SHALL be supported:

- Multiple IKE SAs (multiple IPsec tunnels)
- Multiple IPsec SAs
- Multiple IPsec SAs per IPsec tunnel

IKE SA(s) and IPSEC SA(s) SHALL be regularly re-established:

- When the full sequence number space of an IPSEC SA(s) is used, the transmission for that SA SHALL stop.
- Dead-Peer-Detection (DPD) SHALL be supported as defined in [34].
- Each node SHALL support a traffic narrowing function for the traffic selector ([34]): If the traffic selector notified from the peer (e.g. Security GW or neighbouring node) is wider than the Local/Remote Address range in the SPD information set on the node side, the peers set the traffic selector values to the narrower range.

4.5.2 Parallel usage of IPsec and other secure transport protocols

Implementations SHALL support IPSec configuration with one or more dedicated connections in parallel with other secure transport protocols.

EXAMPLE: It should be possible to run SSH or TLS connections within an IPsec tunnel or in parallel to IPsec tunnel(s).

4.5.3 Responder mode and Initiator/Responder mode support

Implementations SHALL support a configurable option per IKE Security Association to use "Responder mode" instead of "Responder/Initiator mode".

Responder mode is applied to IKE SA establishment only. The introduction of "Responder mode" does not change the IKE SA rekeying behaviour: Each node shall be able to operate as initiator and responder in IKE_SA rekeying.

4.6 CMPv2

Certificate Management Protocol version 2 (CMPv2) is based on Internet X.509 Public Key Infrastructure (PKI) Certificate Management Protocol (CMP) specified in IETF RFC 4210 [38] and IETF RFC 4211 [39].

ETSI TS 133 310 [26] specifies the use of CMPv2 used by base stations to obtain an operator-signed certificate using a secured communication based on the vendor-signed certificate in the base station and a vendor root certificate pre-installed in the CA/RA server.

Certificates may be installed at initial system initialization or obtained through certificate enrolment with the operator's PKI. Certificate enrolment may be supported with the CMPv2 protocol between the Network Element (NE) and the operator's CA as defined in ETSI TS 133 310 [26]. A PNF that supports CMPv2 shall use the CMPv2 profile defined in ETSI TS 133 310 [26], clause 9.5. The CA/RA server may include the trust anchor for the operator issued certificate and the appropriate certificate chains in the initialization response message.

4.7 OAuth 2.0

4.7.1 Overview

The authorization framework described in clause 4.7 of the present document uses the OAuth 2.0 framework as specified in IETF RFC 6749 [35]. It allows the service producers to authorize the requests from service consumers, and the service consumers to obtain authorization credentials ("token endpoint").

Interfaces requiring the use of OAuth 2.0 for authorization purposes shall support the functionality according to clause 4.7 of the present document.

Following options have been introduced to guarantee interoperability and align with the existing OAuth 2.0 authorization framework in ETSI TS 133 501 [29] (i.e. Service Based Architecture).

4.7.2 Basic Parameterization

4.7.2.1 General

Client access token authorization grants shall be supported with type Client Credentials Grant, as described in clause 4.4 of IETF RFC 6749 [35]. Mutual TLS authentication, as specified in the present document (clause 4.2.1), is the mechanism selected by O-RAN for this security procedure.

In addition, still aligned with Client Credential Grant as described in section 4.4. of IETF RFC 6749 [35], Client Id and Client Secret may be supported for client authentication. In this case, one-way TLS may be used (certificate on server side).

Access tokens shall be JSON Web Tokens (JWT) as described in IETF RFC 7519 [36] and shall be secured with digital signatures based on JSON Web Signature (JWS) as described in IETF RFC 7515 [37].

The 'scope' attribute as described in clause 3.3 of IETF RFC 6749 [35] shall be used to specify the allowed services per type of service producer. A more granular level of authorization may be defined by adding additional scope information with the token (e.g. to authorize specific operations, or access to particular resources or datasets), which requires to be verified by the service producer.

OAuth 2.0 roles, as defined in clause 1.1 of IETF RFC 6749 [35], are as follows:

- OAuth 2.0 Authorization server: new security function in O-RAN architecture; or provided by existing OAuth 2.0 infrastructure in the network.
- OAuth 2.0 client: every API service consumer in O-RAN system (e.g. rApp, xApps).
- OAuth 2.0 resource owner/server: every API service producer in O-RAN system (e.g. Near-RT RIC platform).

4.7.2.2 Registration process

OAuth 2.0 resource servers (API service producers) shall be registered with the OAuth 2.0 Authorization server. Service producers may include additional scope information related to specific allowed service operations and resources per client type.

Before initiating the authorization protocol, OAuth 2.0 clients shall be registered with the OAuth 2.0 Authorization server. To achieve that, information about the service consumer instance and its type shall be made available in the OAuth 2.0 Authorization server. The registration process is subject to implementation procedures of the operator, with the following consideration on authentication procedure:

OAuth 2.0 clients shall be capable to authenticate securely with the authorization server and client type shall be "confidential" as specified in clause 2.1 of IETF RFC 6749 [35].

Strong authentication mechanisms based on digital certificates shall be supported.

In addition, client authentication mechanism based on client Id and Client Secret may be supported.

4.7.2.3 Access Token request process

4.7.2.3.0 Server requirements

After TLS mutual authentication procedure between the OAuth 2.0 client and OAuth 2.0 Authorization server, or one-way TLS authentication with server certificate and client authentication based on Client Id and Client Secret has been executed, the Authorization server exposes a 'Token Endpoint' where the Access Token request service can be requested by OAuth 2.0 client.

The following procedure depicts the procedure of the OAuth 2.0 client to obtain an access token from the OAuth 2.0 authorization server.

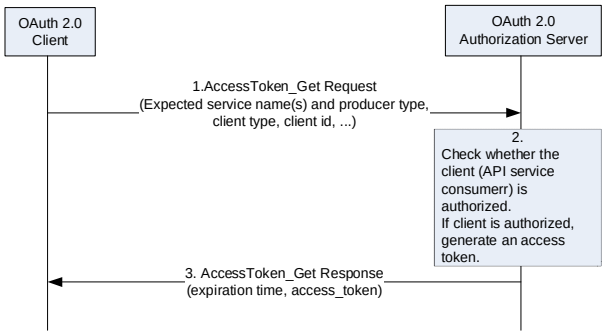

Figure 4-1: Access Token request

The OAuth 2.0 Client shall request an access token from the OAuth 2.0 Authorization server. For this operation the client shall send a HTTP POST request to the authorization server ('Token endpoint'), as described in IETF RFC 6749 [35], clause 3.2. The message, i.e. the body of the HTTP POST request, shall include the identifier of the client instance making the request, the 'scope' parameter indicating the expected services, and optionally additional scope information with more granular information about resources and operations on the resources, and optionally the type of client ('confidential') and the expected OAuth 2.0 resource owner/server. The message may include as well information referring to instance(s) of specific resource owner(s)/server(s) if required.

4.7.2.3.1 Server requirements

- The OAuth 2.0 Authorization server shall verify that the input parameters in the access token (e.g. client type) match with the corresponding ones in the public certificate of the client, or those in the client profile previously registered.
- If the client is authorized, the Authorization server shall generate an access token with appropriate scope as defined in clause 3.3 of IETF RFC 6749 [35] included.
- The Authorization server shall digitally sign the generated access token based on a private key as described in IETF RFC 7515 [37]. If the client is not authorized, the Authorization server shall not issue an access token to that client. If the authorization is successful, the Authorization server shall send the access token to the client ('200 OK'), otherwise it shall reply based on OAuth 2.0 error response defined in IETF RFC 6749 [35].
- The success response should include in addition the expiration time for the token as indicated in IETF RFC 6749 [35].
- The response shall include information to identify the resource owner(s)/server(s) if they differ from the related information included in the token request.

4.7.2.4 Service access request based on token verification

Once the client is in possession of a valid access token, it may proceed with the request of service access towards the service producer (OAuth 2.0 resource owner/server).

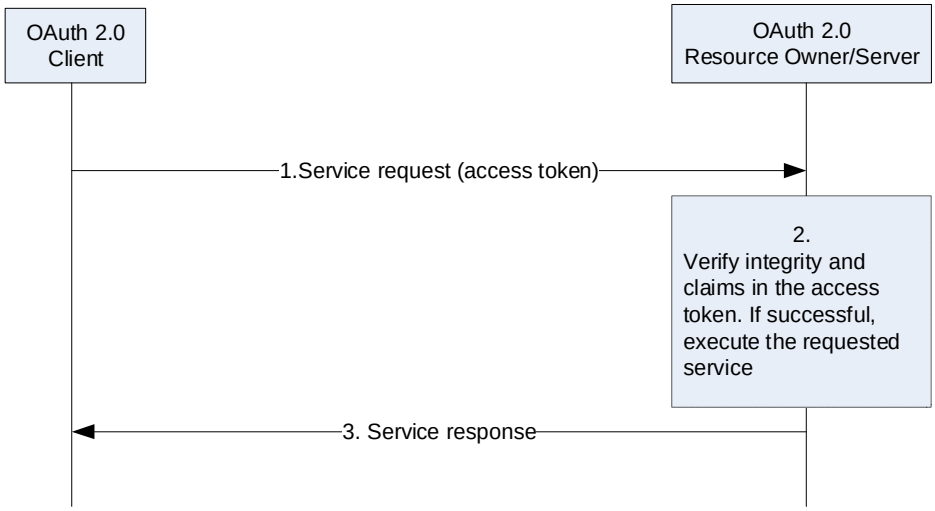

Figure 4-2: Service request

1. The OAuth 2.0 client requests service from the OAuth 2.0 resource owner/server. The OAuth 2.0 client shall include the access token in the request. The OAuth 2.0 client and OAuth 2.0 resource owner/server shall authenticate each other via mutual TLS, as defined in the present document (clause 4.2.1) In addition, one-way TLS authentication with certificate only on server side may be supported, as defined in the clause 4.2.1.
2. The OAuth 2.0 resource owner/server shall verify the token:
   i. It ensures the integrity of the token by verifying the signature using the OAuth 2.0 Authorization server's public key.
   ii. If the integrity check is successful, the OAuth 2.0 resource owner/server shall verify the claims.
3. If the verification is successful, the OAuth 2.0 resource owner/server shall execute the requested service and respond back to the OAuth 2.0 client. Otherwise, it shall send a proper error response. If the HTTP protocol is used, that error response shall be based on the OAuth 2.0 error response defined in IETF RFC 6749 [35].

5 Cryptographic operations

Table 5-1 outlines the main cryptographic operations involved in the protection of (1) App/VNF/CNF packages for ensuring their integrity, authenticity and confidentiality (for sensitive artifacts) during delivery, onboarding, and instantiation phases, (2) the communication channel over O-RAN interfaces in terms of authenticity, confidentiality and integrity, and (3) the stored assets within O-RAN system. It contains the allowed list of algorithms, key sizes and standards according to BSI [i.6] and NIST [40], [48], [i.9] cryptographic guidelines.

Table 5-1

Cryptographic operations	Algorithms	Key sizes	Applicable standards	Usage	Note
Signature generation and verification	RSASSA-PSS RSA_PKCS1_V1_5	≥ 2048-bits	FIPS 186 [42]	For ensuring the integrity and authenticity of Apps/VNF/CNF packages during delivery, onboarding, and instantiation phases	Existing code should use PKCS #1 v1.5 padding mode for compatibility only. Use of null padding is not recommended.
Signature generation and verification	ECDSA NIST-approved curves (P-256, P-384, or P-521)	≥ 256-bits	FIPS 186 [42], SP 800-186 [i.8]		Parameter key size for DSA shall not allow the following combination: Bit lengths of L and N parameters L = 2048, N = 224 (BSI TR-02102-1 [i.6]).
Symmetric Encryption/Decryption	AES_128, AES_192 and AES_256	128, 192 and 256 bits	FIPS 197 [44], SP 800-38 [i.7] (operation modes)	For ensuring the confidentiality of sensitive artifacts	
Asymmetric Encryption/Decryption	RSAES-OAEP	≥ 2048-bits	IETF RFC 8017 [50]		
Hashing	SHA-2 family (SHA- 224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256) SHA-3 family (SHA3-224, SHA3-256, SHA3-384, and SHA3-512)		FIPS 180-4 [73] for SHA2 FIPS 202 [47] for SHA 3	For ensuring the integrity of Apps/VNF/CNF packages	

The signature operation shall involve X.509-based PKI certificates [i.10].

The following recommendations should be considered:

- For the protection of cryptographic keys, Hardware Security Modules, or HSMs, should be used.
- Along with HSMs, the principle of least privilege should be used with keys, to ensure only users who need the key have access to it.
- In case a legacy system does not support ECDSA, RSA signing algorithms should be used instead. Otherwise, the use of the Elliptic curve signing algorithms is recommended.
- If libraries or frameworks are in use that do not support PSS padding scheme, one of the RSA PKCS1 algorithms should be used instead. Otherwise, the use of one of the RSA PSS algorithms is recommended.
- In general, the largest key size available for an algorithm family should be used:
  - For RSA, the largest supported key size is 4 096 bits.
  - For ECDSA, the largest supported key size is 512 bits.
  - For AES, the largest supported key size is 256 bits.

6 Secure File Transfer protocols

6.1 General

File Transfer management is required in several O-RAN use cases, e.g. for export of log files.

An O-RAN architectural element that implements file management shall support at least one of these secure file transfer protocols: SFTP, FTPES, HTTPS. This is aligned with, for example, how 3GPP specifies File Management in [67] and [68].

SFTP is authenticated with username/password, SSH keys or X.509 certificates. FTPES is authenticated with X.509 certificates. HTTPS is mutually authenticated with X.509 certificates.

6.2 SFTP

6.2.1 General Requirements

O-RAN architectural elements that implement secure file transfer using SFTP shall:

- Support secure connection and authentication using SSHv2 Authentication Protocol [2] with all O-RAN specific requirements from clause 4.1 in the present document.
- Support SFTPv3 as the SFTP Industry Best Practice [65].

6.3 FTPES

6.3.1 General Requirements

O-RAN architectural elements that implement secure file transfer using FTPES shall:

- Support secure connection and authentication using TLS with all O-RAN specific requirements from clause 4.2 in the present document.
- Support FTPES as defined in [66].

6.4 HTTPS

6.4.1 General Requirements

O-RAN architectural elements that implement secure file transfer using HTTPS shall:

- Support secure connection and authentication using TLS with all O-RAN specific requirements from clause 4.2 in the present document.
- Support HTTPS as defined in [69].

Annex A (informative): Change history

Date	Revision	Description
2024.03	09.00	Certificate Profile for O-RAN TLS entity Reference Update
2023.11	08.00	Secure file transfer protocols added SSH Update on no root remote login ssh-ed448 changed to optional Reference on SSH added
2023.07	07.00	Editorial alignments TLS entity certificate profile CMPv2 profile update Introduction of one-way TLS authentication for OAuth2.0
2023.03	06.00	Cryptographic operations update
2022.11	05.00	TLS Cipher update
2022.07.20	04.00	Addition of CMPv2 Update of O-Cloud Image protocols Addition of mTLS Update of OAuth 2.0
2021.11.08	03.00	Update the O-RAN security protocols and specifications to include mandatory support for TLS 1.3
2021.07.05	02.00	Addition of DTLS and IPsec requirements. Alignment of TLS 1.2 and TLS 1.3 profiles with 3GPP TS 33.210. Typographical changes.
2021.04.01	01.00	Initial version of the document with requirements for TLS and SSH.

History

Document history		
V9.0.0	May 2025	Publication