



CYBER;
Middlebox Security Protocol;
Part 3: Profile for enterprise network and
data centre access control

Full Standard Preview
ETSI TS 103 523-3 V1.1.1 (2018-10)
https://standards.iteh.ai/catalog/standards/sls/70a252a-3e6b-4a48-97a7-dde0b7dae939/etsi-ts-103-523-v1-1-2018-10

ReferenceDTS/CYBER-0027-3

Keywordscyber 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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2018.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M logo is protected for the benefit of its Members.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary	4
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	7
3 Definitions and abbreviations.....	7
3.1 Definitions.....	7
3.2 Abbreviations	7
4 The eTLS MSP profile	8
4.1 MSP requirements mapping	8
4.2 eTLS implementation architecture	8
4.2.1 eTLS with enterprise servers	8
4.2.2 eTLS with enterprise clients	9
4.3 eTLS protocol.....	9
4.3.1 Normal TLS 1.3 Diffie-Hellman key exchange	9
4.3.2 eTLS Diffie-Hellman key exchange	10
4.3.3 Visibility information	10
4.3.4 Directly installed keys	11
4.3.5 Centrally managed keys.....	11
4.3.6 Asymmetric key package.....	11
4.3.7 Protecting the key package	13
4.3.8 Transferring keys	13
4.3.8.1 Protocol overview	13
4.3.8.2 Transfer initiated by the key manager.....	13
4.3.8.3 Transfer initiated by the key consumer	13
5 Security.....	15
Annex A (informative): Middlebox visibility information variant.....	16
Annex B (normative): Requirements for an eTLS Aware client	17
Annex C (informative): Mapping MSP desired capabilities to eTLS	18
History	20

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.1].

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.

Executive summary

Requirements - such as legal mandates and service agreements - exist for enterprise network and data centre operators and service providers, organizations, and small businesses to be able to observe and audit the content and metadata of encrypted sessions transported across their infrastructures [i.2]. The original TLS protocol standard adopted in 1994 and its subsequent versions up to and including TLS 1.2, provided for these capabilities [i.3] and [1]. The latest version of the protocol, TLS 1.3, does not provide for these capabilities [2]. Where these capabilities do not exist, this new encryption protocol could be blocked altogether at the enterprise gateway, forcing users to revert to older, less secure protocols.

The present document is one of a series of implementation profiles that, to achieve these required capabilities, puts the enterprise operators and users in control of the access to their data for cyber defence and prevents unauthorized access. It sets forth a "Profile for an enterprise network and data centre access control" called eTLS that meets several desired capabilities for the Middlebox Security Protocol MSP [i.1].

Introduction

The present document specifies an implementation variant of Transport Layer Security (TLS) version 1.3 [2] - which is the latest version in a series of TLS protocol standards extending back to 1994 [i.3] and [1]. This implementation variant is denoted eTLS ("enterprise TLS") because one of its primary use cases is in enterprise networks and data centres.

TLS 1.3 [2] introduces several significant changes compared with TLS 1.2 [1]. One of these changes is the removal of support for RSA key exchange and static Diffie-Hellman key exchange. The primary key exchange mechanism in TLS 1.3 is ephemeral Diffie-Hellman. Ephemeral Diffie-Hellman prevents passive decryption of TLS 1.3 sessions at any scale. However, there are operational circumstances where passive decryption of TLS sessions by authorized entities is a requirement. The decryption may need to be performed in real-time, or the packets may need to be stored and decrypted post-capture.

Situations requiring passive decryption of TLS sessions generally occur in environments where both the client and server, and by inference the data being exchanged over the TLS session, are under the control of the same entity. TLS encryption is often stipulated by internal or external security policies, but access to the unencrypted packet data is required for operational reasons, including:

- Application health monitoring and troubleshooting.
- Intrusion detection.
- Detection of malware activity, e.g. command and control, and data exfiltration traffic.
- Detection of advanced distributed denial of service (DDoS) attacks.
- Compliance audits.

One possible approach to passively decrypting TLS 1.3 sessions is to export the ephemeral keys generated for each TLS session to middleboxes. However, this approach has several significant limitations. Firstly, it is very difficult to ensure that the exported ephemeral keys will arrive at the middlebox in sufficient time to allow decryption in real-time. Secondly, the keys need to be correlated with every stored packet session in anticipation of post-capture decryption. For these reasons, this approach does not scale to the needs of a data centre.

eTLS therefore uses longer-lived static Diffie-Hellman keys that are re-used across multiple sessions; keys could be rotated daily or weekly. This ensures that the keys can be distributed to real-time decryption middleboxes in advance, and it greatly reduces the number of keys to be stored and correlated with packet storage systems.

eTLS requires the server to report visibility information in its certificate, to indicate to the client that eTLS is in use with a particular static Diffie-Hellman public key, and to describe the set of entities or roles or domains, or any combination of these, for which the policy of the party signing the certificate allows sharing of the corresponding private key.

There are limited but essential circumstances in which the visibility information is not suitable; this case is described in annex A, which creates an exception of eTLS where this visibility information is not sent. When there is sufficient support of eTLS, then the annex A exception will be deprecated, as annex A is not fully MSP-compliant.

eTLS is compatible with any TLS 1.3 compliant client. Annex B defines the concept of an "eTLS Aware Client" whereby a TLS 1.3 client provides additional capabilities that use the eTLS visibility information to control when eTLS sessions are to be accepted.

1 Scope

The present document specifies a protocol to enable secure communication sessions between network endpoints and one or more enterprise networks or between data centre middleboxes using encryption, whilst enabling network operations. The present document specifies an implementation variant of Transport Layer Security (TLS) version 1.3, called "eTLS" [2].

The present document describes two eTLS architectures; one for the situation where the originating server is an eTLS server inside the enterprise; and one for the situation where the originating server is a TLS 1.3 server outside the enterprise. The Diffie-Hellman key exchange and visibility information for negotiating the eTLS protocol setup is specified.

The actions of the client on receiving the visibility information and structure of the policy included in the visibility information are not normatively defined; however, capabilities for an "eTLS aware client" are defined in annex B. The means by which eTLS endpoints share the Diffie-Hellman key with key consumers is specified, and examples are provided.

The present document describes a variant of eTLS in annex A, which is not fully MSP compliant and to be used in only essential cases, as visibility information is not supported.

The present document also includes the security guarantees made by eTLS, based on the security guarantees of TLS 1.3. Annex C details description of applicable MSP protocol profile requirements to eTLS, taken from the draft specification of ETSI TS 103 523-1 [i.1], such that this MSP Part may be a standalone document. A final mapping of MSP protocol profile requirements to eTLS is left to a future version of the present document.

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 at <https://docbox.etsi.org/Reference>.

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 are necessary for the application of the present document.

- [1] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".
- [2] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".
- [3] IETF RFC 5958: "Asymmetric Key Packages".
- [4] IETF RFC 7906: "NSA's Cryptographic Message Syntax (CMS) Key Management Attributes".
- [5] IETF RFC 3279: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- [6] IETF RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".
- [7] IETF RFC 5915: "Elliptic Curve Private Key Structure".
- [9] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- [10] Recommendation ITU-T X.509 (10/2016) | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

- [11] IETF RFC 2818: "HTTP Over TLS".
- [12] FIPS 180-4: "Secure Hash Standard".
- [13] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

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 are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI TS 103 523-1: "CYBER; Middlebox Security Protocol; Part 1: Capability Requirements".
- [i.2] S. Fenter: "Why Enterprises Need Out-of-Band TLS Decryption", IETF, 2018.
- [i.3] Recommendation ITU-T X.274 (1994) | ISO/IEC 10736:1995: "Transport Layer Security Protocol".
- [i.4] IETF RFC 5652: "Cryptographic Message Syntax (CMS)".
- [i.5] IETF RFC 5083: "Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

1-sided: middlebox traffic observability enabled unilaterally by one endpoint such that the other endpoint is not able to reject or negotiate the traffic observability, other than by ceasing the communication

eTLS: MSP profile described in the present document

single-context: access is granted, or not granted, only to the entire data stream, not to portions of the data stream

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASN	Abstract Syntax Notation
CMS	Cryptographic Message Syntax
DDOS	Distributed Denial Of Service
DER	Distinguished Encoding Rules
eTLS	enterprise TLS
HTTP	HyperText Transfer Protocol
MSP	Middlebox Security Protocol
RSA	Rivest-Shamir-Adleman
TLS	Transport Layer Security

4 The eTLS MSP profile

4.1 MSP requirements mapping

MSP Part 1 [i.1] will define several Capability Requirements that are demanded of a profile wishing to comply with the MSP framework. The full and complete mapping of MSP Part 1 requirements to eTLS, the profile described in the current document, is left to a future revision of the present document when MSP Part 1 [i.1] is finalized. However, desired capabilities of MSP profiles are mapped to relevant properties of eTLS in annex C.

For any mapping, an MSP profile needs categorizing as a 1-sided or 2-sided profile with single or fine-grained context, as defined in the planned MSP Part 1 [i.1]. This categorization determines the mandatory and optional requirements that the MSP profile needs to satisfy.

eTLS is a 1-sided MSP profile, as only one endpoint will be using a static Diffie-Hellman key, and so that endpoint unilaterally enables traffic observability. eTLS is also single-context, as access is granted, or not granted, only to the entire data stream.

4.2 eTLS implementation architecture

4.2.1 eTLS with enterprise servers

Figure 4.1 depicts the eTLS implementation architecture when used with enterprise servers. TLS connections to clients that are external to an enterprise network or data centre may be made using TLS 1.3 [2], using forward secrecy and enhanced protections.

The firewall terminates the Internet TLS 1.3 sessions and uses eTLS between the firewall and the web server, with the firewall acting as the TLS client. Middlebox A is authorized to inspect the traffic flowing between the firewall and the web server. It therefore receives a passive copy of these packets along with a copy of the static Diffie-Hellman public/private key pair (A) used by the web server.

EXAMPLE 1: Middlebox A decrypts the traffic in real-time to perform intrusion detection.

The web server acts as a TLS client in its connection to the application server. In this case, Middlebox B is authorized to inspect the traffic flowing between the two servers, and it decrypts the TLS sessions using the application server's static Diffie-Hellman public/private key pair (B).

EXAMPLE 2: Middlebox B decrypts the traffic in real-time to provide application health monitoring, but also stores the encrypted packets so they can be decrypted at a later date for compliance and auditing purposes.

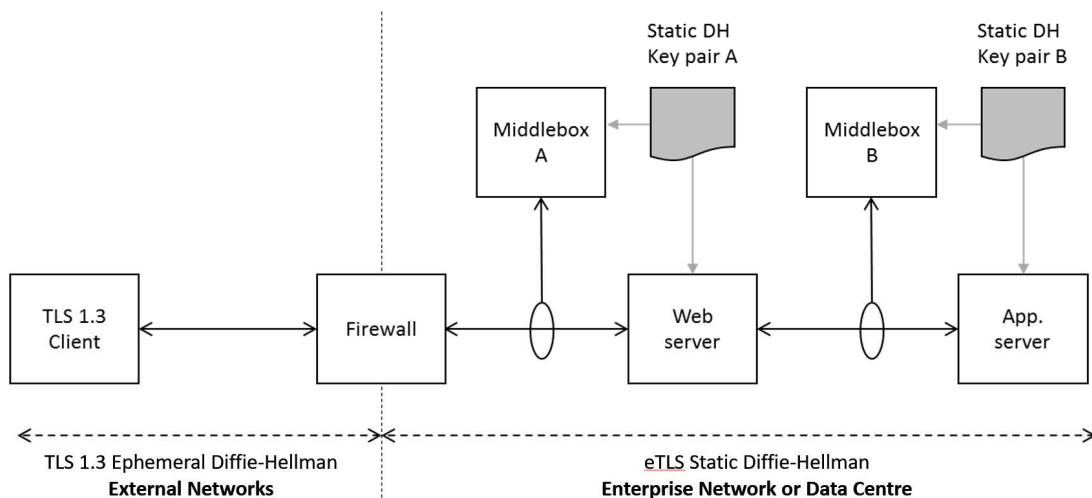


Figure 4.1: eTLS architecture with enterprise servers

4.2.2 eTLS with enterprise clients

Figure 4.2 depicts the eTLS implementation architecture when used with enterprise clients. TLS connections to servers that are external to an enterprise network may be made using TLS 1.3 [2], using forward secrecy and enhanced protections.

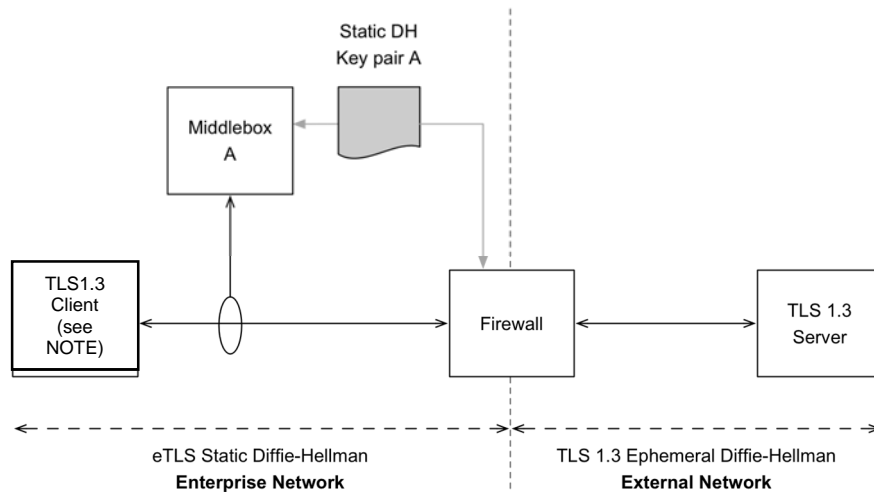


Figure 4.2: eTLS architecture with enterprise clients

The firewall terminates the enterprise network sessions that are using eTLS, with the firewall acting as the eTLS server. The firewall then acts as the TLS 1.3 client and uses TLS 1.3 to communicate to the TLS 1.3 server on the external network. Middlebox A is authorized to inspect the traffic flowing between the client and the firewall. It therefore receives a passive copy of these packets along with a copy of the static Diffie-Hellman public/private key pair (A) used by the firewall, in its role as the eTLS server.

NOTE: Although the client is participating in an eTLS connection, it is a TLS 1.3 compliant client.

EXAMPLE: Middlebox A decrypts the traffic in real-time to perform malware detection or data loss prevention.

4.3 eTLS protocol

4.3.1 Normal TLS 1.3 Diffie-Hellman key exchange

For reference, a description of the normal TLS 1.3 Diffie-Hellman key exchange is included. Unless a pre-shared key is in use, the TLS 1.3 key exchange mechanism proceeds at the start of a new session as follows [2]:

- 1) The client generates an ephemeral Diffie-Hellman public and private key. The public key is transmitted to the server in a "key_share" message with a random client nonce.
- 2) The server generates an ephemeral Diffie-Hellman public and private key. The public key is transmitted to the client in a "key_share" message with a random server nonce.
- 3) The client and server each use a combination of their own private keys and the public key received from the other side of the connection to generate a shared secret.
- 4) The client and server then use the shared secret along with the initial handshake messages, which include the nonces, to generate a set of handshake traffic keys for encryption of the remainder of the handshake.
- 5) During the remainder of the handshake, the server sends its certificate encrypted using a handshake traffic key.
- 6) Upon completion of the handshake, the client and server then use the shared secret along with various elements of the handshake messages, which again include the nonces, to generate a set of application traffic keys for the session.
- 7) The application traffic keys are used to encrypt further data exchanged between the client and server.

4.3.2 eTLS Diffie-Hellman key exchange

The eTLS key exchange shall use exactly the same messages and procedures to establish a set of session keys as a TLS 1.3 ephemeral Diffie-Hellman key exchange, except for two differences [2].

- 1) the server shall use a static public/private key pair at Step 2 in clause 4.3.1; and
- 2) the server's certificate at Step 5 shall contain visibility information as defined in clause 4.3.3 to indicate to the client that eTLS is in use.

NOTE: Neither the static public key nor the visibility information affects the operation of a TLS 1.3 compliant client, so an eTLS server is therefore fully interoperable with TLS 1.3 compliant clients.

The eTLS server shall be provisioned with a static key pair for each elliptic curve (or finite field length) supported by the server. These key pairs may be shared with middleboxes that are authorized to decrypt sessions from the server as shown in Figure 4.1.

The static key pair shall be:

- 1) installed directly on the server and rotated as necessary, described in clause 4.3.4; or
- 2) downloaded from a central key manager and updated as necessary, described in clause 4.3.5.

4.3.3 Visibility information

In eTLS, the server certificate, as defined in Recommendation ITU-T X.509 [10], shall send visibility information in its certificate that shall:

- 1) Indicate that eTLS is being used.
- 2) Be bound to the static Diffie-Hellman public/private key pair for Step 2 of the eTLS protocol, described in clause 4.3.2. This public/private key pair shall not be the same as the certificate subject's public/private key pair (defined in clause 4.1.2.7 Subject Public Key Info of IETF RFC 5280 [9]), which is used for the signature in the CertificateVerify message (defined in clause 4.4.3 Certificate Verify of IETF RFC 8446 [2]).
- 3) Identify, either generally or specifically, the controlling or authorizing entities or roles or domains, or any combination of these, of any middleboxes that may be allowed access to the eTLS static Diffie-Hellman private key described in clause 4.3.2 of the present document.

The above 3 points describe the Visibility Information field, which shall be defined by the following ASN.1 type:

```
VisibilityInformation ::= SEQUENCE {
    fingerprint      OCTET STRING (SIZE(10)),
    accessDescription UTF8String }
```

where the SHA-256 digest of the static Diffie-Hellman public key as transmitted in the key_share extension of the ServerHello message shall be represented as the vector of 32-bit words (H_0, H_1, \dots, H_7) as defined in FIPS 180-4 [12]. The fingerprint field shall be set to $H_0 || H_1 || (H_2 \gg 16)$, which is the first 80 bits of the digest vector read in big-endian format. The accessDescription field shall be a human-readable text string that identifies, either generally or specifically, the controlling or authorizing entities or roles or domains, or any combination of these, of any middleboxes that may be allowed access to the eTLS static Diffie-Hellman private key.

The Visibility Information field shall be sent as an otherName field entry of the subjectAltName as defined in clause 4.2.1.6 Subject Alternative Name of IETF RFC 5280 [9]. The type-id shall be set to the Object Identifier 0.4.0.3523.3.1 {itu-t(0) identified-organization(4) etsi(0) msp(3523) etls(3) visibility(1)} and the contents of value shall be set to the DER encoding of VisibilityInformation.

Thus fingerprint, in conjunction with the certificate's validity period, binds the certificate to a particular static Diffie-Hellman public/private key pair. The accessDescription allows the endpoints to identify, either generally or specifically, the controlling or authorizing entities or roles or domains, or any combination of these, of any middleboxes that may be given the ability to decrypt data protected by the corresponding eTLS key exchange.

The accessDescription field shall be accurate; a structure for the description may be introduced in a future version of eTLS.