ETSI TS 103 523-3 V1.3.1 (2019-08)

TECHNICAL SPECIFICATION

CYBER;
Middlebox Security Protocol;
Part 3: Enterprise Transport Security

Reference
RTS/CYBER-0027-3v131

Keywords
cyber 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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

Contents

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 standards adopted in the 1986-1995 period in multiple bodies and IETF 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 TLS protocols.

The present document is one of a series of MSP implementation profiles that support these capabilities, while allowing enterprise operators and users to stay in control of access to their data. It sets forth an MSP profile, "Enterprise Transport Security", for use in enterprise networks and data centres that meets mandatory capabilities for the Middlebox Security Protocol (MSP) [i.1].

Introduction

The present document specifies an MSP profile for enterprise network and data centre domains: Enterprise Transport Security. This is an implementation variant of Transport Layer Security (TLS) protocol version 1.3 [2].

TLS 1.3 is a recent version in a series of TLS protocol standards [i.6] and [i.3]. 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. lateral movement, 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.

The Enterprise Transport Security profile therefore uses longer-lived static Diffie-Hellman keys that are re-used across multiple sessions; enterprises could implement automated key rotation in order to reduce the rotation cycle time. 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.

The Enterprise Transport Security profile also requires the server to report visibility information in its certificate, to indicate to the client that Transport Layer Security 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 circumstances in which visibility information is not suitable and in which the client operator has been informed by other means that connections can be inspected; in such circumstances, annex A can be used. annex A, which is optional, specifies a variant of the Enterprise Transport Security profile where the visibility information is not sent.

EXAMPLE: Annex A can be used when the client and server are wholly within a private enterprise network and the client operator has already been notified by alternative means, such as a condition of access to the network, that connections can be inspected.

The Enterprise Transport Security profile is compatible with any TLS 1.3 compliant client. Annex B, which is optional, defines the concept of an "Enterprise Transport Security aware client" whereby a TLS 1.3 client provides additional capabilities in relation to Enterprise Transport Security visibility.

1 Scope

The present document specifies the "Enterprise Transport Security" profile to enable secure communication sessions between network endpoints whilst enabling network operations. The Enterprise Transport Security (ETS) profile enables use of Transport Layer Security (TLS) version 1.3 [2] in, for example, compliance constrained environments.

The present document describes three Enterprise Transport Security architectures:

- In the first architecture, both the TLS 1.3 client and the Enterprise Transport Security server are located inside the enterprise.
- In the second architecture, the server is an Enterprise Transport Security server inside the enterprise and the TLS 1.3 client is external to the enterprise. TLS 1.3 is terminated at the enterprise edge such that Enterprise Transport Security is used only inside the enterprise.
- In the third architecture, the TLS 1.3 server is external to the enterprise and the TLS 1.3 client is internal to the enterprise. TLS 1.3 is again terminated at the network edge such that Enterprise Transport Security is used only inside the enterprise.

The Diffie-Hellman key exchange and visibility information for indicating the Enterprise Transport Security profile 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 "Enterprise Transport Security aware client" are defined in annex B, which is optional. The means by which the Enterprise Transport Security endpoints share the Diffie-Hellman key with key consumers is specified, and examples are provided.

The present document describes a variant of the Enterprise Transport Security profile in annex A for circumstances in which visibility information is not suitable and in which the client operator has been informed by other means that connections can be inspected. The means by which the client operator is informed is out of scope.

The present document also includes the security assurances made by the Enterprise Transport Security profile, based on the security assurances of TLS 1.3. Annex C gives details of the MSP profile capabilities that are applicable to the Enterprise Transport Security profile, 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 profile capabilities to the Enterprise Transport Security profile 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".

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

[9] Recommendation ITU-T X.509 (10/2016) | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[10] IETF RFC 2818: "HTTP Over TLS".

[11] FIPS 180-4: "Secure Hash Standard (SHS)".

[12] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[13] IETF RFC 8551: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification".

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".

[i.6] Nelson & Heimann: "SDNS Architecture and End-to-End Encryption", CRYPTO' 89 Proceedings, pp 356-366; Ruth Nelson, SDNS Services and Architecture, Proceedings of the 10th National Computer Security Conference, Sept. 1987, pp 153-157.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms 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

Enterprise Transport Security (ETS): MSP profile described in the present document that instantiates an Enterprise Transport Security session

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

3.2 Symbols

Void.

3.3 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
ETS	Enterprise Transport Security
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
MSP	Middlebox Security Protocol
RSA	Rivest-Shamir-Adleman
TLS	Transport Layer Security

4 Enterprise Transport Security for the MSP framework

4.1 MSP requirements mapping

MSP Part 1 [i.1] defines 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 [i.1] requirements to the Enterprise Transport Security 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 the Enterprise Transport Security profile 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.

Enterprise Transport Security 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. The Enterprise Transport Security profile is also single-context, as access is granted, or not granted, only to the entire data stream.

4.2 Enterprise Transport Security architectures

4.2.1 Enterprise Transport Security with enterprise clients and servers

Figure 4.1 depicts the Enterprise Transport Security implementation architecture when both the TLS 1.3 [2] client and the Enterprise Transport Security server are located in the Enterprise.

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.

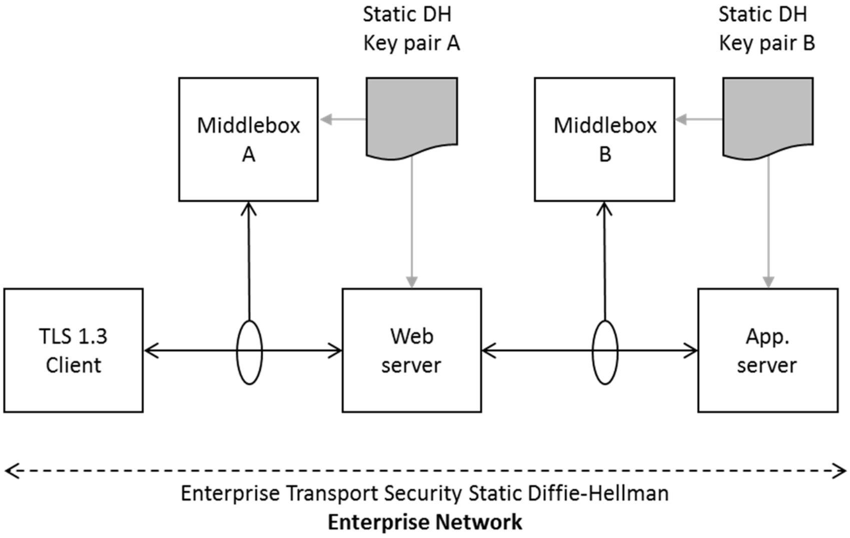

Figure 4.1: Enterprise Transport Security architecture with enterprise client and server

4.2.2 Enterprise Transport Security with enterprise servers

Figure 4.2 depicts the Enterprise Transport Security implementation architecture when the TLS 1.3 client is outside the enterprise and the Enterprise Transport Security server is located in the Enterprise. 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.

The firewall terminates the Internet TLS 1.3 sessions and uses the Enterprise Transport Security profile 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.

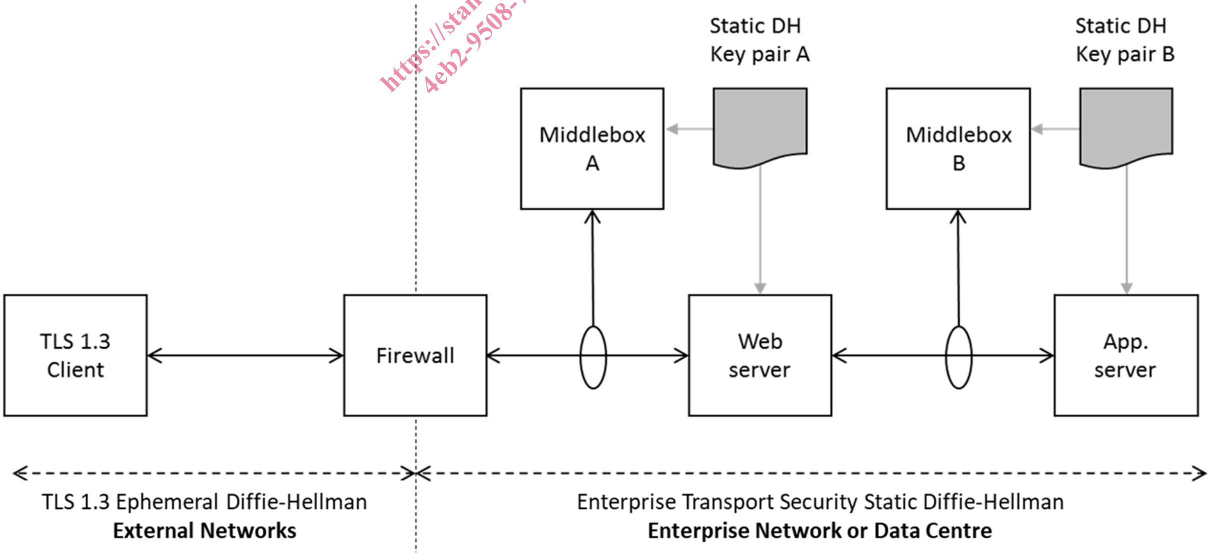
Static DH
Key pair A
Static DH
Key pair B
Middlebox
A
Middlebox
B
TLS 1.3
Client
Firewall
Web
server
App.
server
TLS 1.3 Ephemeral Diffie-Hellman
External Networks
Enterprise Transport Security Static Diffie-Hellman
Enterprise Network or Data Centre

Figure 4.2: Enterprise Transport Security architecture with enterprise servers

4.2.3 Enterprise Transport Security with enterprise clients

Figure 4.3 depicts the Enterprise Transport Security implementation architecture when enterprise clients are used with a TLS 1.3 server outside the enterprise. TLS connections to servers that are external to an enterprise network may be made using TLS 1.3 [2], using forward secrecy.

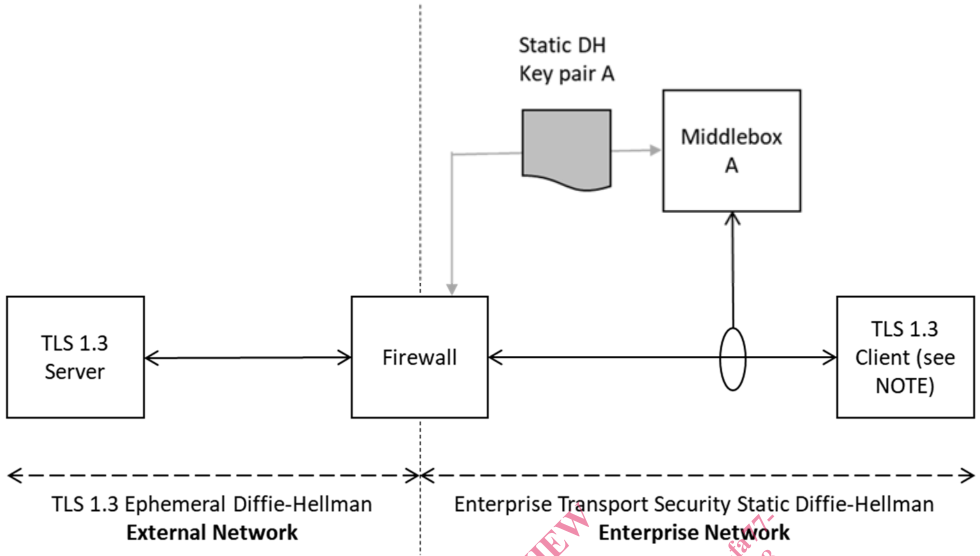
Static DH
Key pair A
Middlebox A
TLS 1.3 Server
Firewall
TLS 1.3 Client (see NOTE)
TLS 1.3 Ephemeral Diffie-Hellman
External Network
Enterprise Transport Security Static Diffie-Hellman
Enterprise Network

Figure 4.3: Enterprise Transport Security architecture with enterprise clients

The firewall terminates the enterprise network sessions that are using Enterprise Transport Security, with the firewall acting as the Enterprise Transport Security 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 Enterprise Transport Security server.

NOTE: Although the client is participating in an Enterprise Transport Security 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 The Enterprise Transport Security profile

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 nonce, 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.