ETSI White Paper No. 43

Redefining Network Security: The Standardized Middlebox Security Protocol (MSP)

First edition – March 2021

ISBN No. 979-10-92620-37-7

Authors:

Tony Rutkowski & Roger Eriksson

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

Contents

About the authors

Tony Rutkowski
Middlebox Security Protocol Group Rapporteur, ETSI Member

Over the past several years, Tony Rutkowski has been active in many diverse security standards bodies, including being the rapporteur for ETSI TC CYBER's Middlebox Security Protocol Group. He is an engineer-lawyer, with a 45-year career spanning technical and legal domains in both the Internet and telecom worlds, in the U.S. and internationally. Positions held have spanned the private sector (VeriSign, SAIC, General Magic, Sprint International, Horizon House, Pan American Engineering, General Electric, Evening News Association), government (Federal Communications Commission, the International Telecommunication Union, Cape Canaveral City Council), academia (Internet Society, MIT, and NY Law School), and consultation in NGI Associates.

Dr. Roger Eriksson

Roger Eriksson holds a Ph.D. in electrical engineering from University of Lund. Roger has for more than 25 years worked in the field of cybersecurity holding different positions, such as security architect, project manager, development manager and responsible for security approvals. The past three years Roger has been involved in ETSI (Cyber) and has been rapporteur for the work item: Middlebox Security Protocol, Part 1: Profile Capability Requirements.

Executive Summary

This White Paper describes the high-level technical features, motivations and use cases for ETSI TC CYBER's new middlebox standards, known collectively as the 'Middlebox Security Protocols' or 'MSP'.

The Middlebox Security Protocol standards suite redefines middlebox operations and network security. MSP comprises three Parts so far: TS 103 523, Part 1 [1] is a framework that defines the security properties of MSP; TS 103 523, Part 2 [2] is a protocol that specifies user-controlled access to data and fine-grained control over middlebox access; TS 103 523, Part 3 [3] is a protocol driven by industry need to still perform vital data centre operations, after changes to a major internet protocol (TLS) removed this important functionality.

MSP enables a new way of performing network security with middleboxes, retaining the important functionality that middleboxes provide, whilst giving users: visibility of what is happening with their communications, control over who accesses it, and the opportunity to audit their data.

Middleboxes are of significant R&D community interest – both commercial and academic – leveraged by the MSP group and built to become MSP. MSP was created by industry, for industry; it protects user privacy, specifies methods for a new generation of proxies, enables vital data centre operations, and puts users back in control of their data.

1 Introduction

The Middlebox Security Protocol (MSP) series is a set of **new generation of middlebox protocols** that improve the current proxy status quo, allowing middleboxes to **perform vital functions securely** and whilst keeping up with the rapid pace of technical development.

All parts showcase an innovative approach to network security, allowing middleboxes to protect networks through layered defence and to protect enterprises with transparency and access control at the centre of their design – an improvement to current MITM proxy deployments. The MSP standards allow users and deployers to make choices about use of middleboxes in a connection: to protect user privacy, to allow data loss prevention and defence of user data from theft, privacy-infringing applications and malware.

The set of Middlebox Security Protocol standards are delivered in different Parts, to allow for future MSP profiles, and a variety of use cases and technical requirements:

- MSP Part 1 (TS 103 523-1 [1]) formally sets out **security requirements for middlebox protocols**. It ensures **data protection**, that endpoints have **access control** of middleboxes, and **transparency** (that endpoints retain knowledge of permitted parties in a connection).
- MSP Part 2 (TS 103 523-2 [2]) - (TLMSP) defines a protocol that is designed to put users back in control of their data, by allowing **fine-grained control** over middlebox access to content. TLMSP creates an **authenticated end-to-end encrypted** session, and authorising additional parties to access controlled portions of encrypted data.
- MSP Part 3 (TS 103 523-3 [3]) - (ETS) requires **transparency** of middleboxes on a network, so user endpoints know of, and agree to, their presence. This gives users awareness of the cyber defence measures protecting their data. ETS **enables data centres to perform the functions they need to operate**: load-balancing, DDoS protection, malware prevention, and more.

1.1 Why middleboxes?

The term "middlebox" can refer to a variety of devices, use cases and functions; in the MSP series, however, "middleboxes" are specifically devices that perform functions higher up the stack, at the security layer or for security-specific functions. Such **middleboxes are essential to the operation of modern and legacy networks alike**; they include company firewalls, intrusion detection systems, and data loss prevention systems; functions range from compliance, load-balancing, troubleshooting and personal data protection to IP filtering, faster content delivery and monitoring for cyber security.

Endpoint security alone is not enough to protect networks, for many reasons. With more connectivity than ever, only one device needs to be successfully attacked to compromise a network. IoT devices may not be patched; battery-constrained devices may not have the power to provide their own protection; legacy devices may no longer be supported with the latest patches; and more.

Middleboxes now represent perhaps the most active and innovative sector of network technology research, and product development today with search engines **showing more than 10,000 published academic papers** over the past decade and hundreds of new ones appearing every month. These published papers, treating middlebox and transport cryptographic protocols, represent **one of the most critically important developments and challenges in the cyber security field today**.

1.2 Why create the Middlebox Security Protocol (MSP)?

MSP were **driven by industry need** for future-proof, secure systems with troubleshooting capabilities. ETSI published a Technical Report (ETSI TR 103 421 [4]) recommending standards-based middlebox solutions to the evolving needs of industry and networks. **Middleboxes are a crucial part of network function and defence** today, including proxies, firewalls and intrusion detection systems.

Increasingly, users want control of their data and to protect it, both from malware and from ‘legitimate’ software that harvests user data without consent. Users should be able to choose their defensive posture, including giving access to defence middleboxes. A protocol that doesn't permit this protection removes a potential defence layer against theft of user data, with insufficient means for users to prevent the bypass.

However, middlebox deployments often raise complex and multi-layered questions around the security, privacy and trust of using middleboxes; Man-In-The-Middle (MITM) proxies used today break both authentication and end-to-end encryption without endpoint awareness, which is unsatisfactory for many use cases. So **a new middlebox solution was needed and created – that solution is MSP**.

2 What does MSP do?

The series of MSP specifies middlebox protocols that are more applicable than traditional MITM proxy methods; MSP facilitates similar functions but does so with stronger security properties. The MSP series:

- specifies required security properties of middleboxes (TS103 523 Part 1 [1])
- restricts data access on a fine-grained scale, enabling the security principle of least privilege (TS 103 523 Part 2 [2])
- enables data centre operations, such as: load-balancing, troubleshooting, malware detection, investigation of network attacks, and more, on encrypted networks (TS 103 523 Part 3 [3]).

2.1 Implementations and running code

Previous ETSI Security Weeks have featured MSP hackathons [1 (2019), 2 (2018)], welcoming implementers to read the specifications, test out the MSP source code on the ETSI Forge (ETS and TLMSP), and try out creative projects with MSP. Here, some of the outputs are described at a high level – created just in three days:

- A client-side TLMSP middlebox that understands PII data (e.g. names, banking details) and controls access to that data, preventing other middleboxes from reading the PII. The original message then continues through the network with the sensitive data withheld (from enterprise firewalls, for example), while the server can still reconstruct the original message.
- A personal cyber defence middlebox on a Raspberry Pi, resulting in a portable middlebox for users.
- Use in Industrial IoT to update inventories, utilizing TLMSP's audit functionality to log resources accurately, review which factory used which items, and issue alerts for resource levels.
- Implementation of ETS Wireshark parsing, enabling troubleshooting and analysis of the connection.
- A language filter middlebox, to protect vulnerable people from abusive language in messaging applications. If abuse is found, it is removed, and the endpoint receives the redacted message, fully aware that data has been removed.

But MSP has more use cases than these – read the standards and discover how you could use MSP.

3 Overview of the MSP standards

MSP is a multi-part specification, currently comprising three parts:

Part 1: Middlebox Security Protocols Framework and Template Requirements **(TS 103 523-1)**

MSP brings an opportunity to set a new standard of security and privacy; Part 1 does this through the MSP Framework. The MSP Framework allows the MSP series to be extensible and allows MSP profiles to be consistently analysed for security, allowing flexibility for individual profiles, whilst maintaining a high security standard across the set of Middlebox Security Protocols. The framework is based on four important principles:

1) Data Protection (DP): protecting data from network attackers and malicious actors.
2) Transparency (T): having knowledge of which parties have what access to the data.
3) Access Control (AC): allowing endpoints meaningfully to grant access to parties with this knowledge.
4) Good Citizen (GC): preventing complexity that adds DDoS attack vectors to the network.

Part 2: Transport Layer MSP, profile for fine-grained access control **(TS 103 523-2)**

TLMSP is an MSP profile that allows varied (fine-grained) permissions and accesses to different middleboxes. This MSP profile controls whether the data can be modified or not, gives the client and server visibility of what the proxies are doing, and protects proxies from malicious clients or servers. TLMSP gives user-controlled access to data, details how the profile works and the mechanisms that ensure endpoints have awareness of middleboxes on the connection and their permitted access level.

Part 3: Profile For Enterprise Network and Data Centre Access Control (TS 103 523-3)

Known as Enterprise Transport Security (ETS), ETS was driven by, and fulfils, an industry need to upgrade from TLS 1.2, whilst retains vital system security and system hygiene functions such as troubleshooting, doing network management, data centre operations and investigation of attacks on encrypted networks.

3.1 MSP Part 1: MSP Framework and Template Requirements (TS 103 523-1)

Part 1 provides a framework for assessing the security of MSP profiles, and a common set of requirements for all MSP profiles to meet (Template Requirements). Achieving an extensible and common security baseline for all MSP profiles is a challenge, when MSP profiles span complex and interacting requirements, some of which are listed in Table 1.

Table 1

Secure and controlled exposure of traffic observables	Ability to institute desired defence measures	Sufficient observable information for acquisition and analysis for defence measures
Sufficient performance metrics	Ability to scale	Ease of deployment
Minimal impact on existing client and server implementations	Minimal threat exposure	Suitability for architecture location (transport path versus data centre)

Each MSP profile described in future Parts can be entirely different, but each profile is required to fulfil the properties in the MSP Part 1 framework. The framework is based on four important principles:

1) *Data Protection (DP): protecting data from network attackers and malicious actors.*
2) *Transparency (T): having knowledge of which parties have what access to the data.*
3) *Access Control (AC): allowing endpoints meaningfully to grant access to parties with this knowledge.*
4) *Good Citizen (GC):* preventing complexity that adds DDoS attack vectors to the network.

All MSP requirements and full details are available in the Technical Specification (TS 103 523-1 [1]).

3.2 MSP Part 2: Transport Layer MSP, profile for fine-grained access control (TS 103 523-2)

There is an industry need for proxies that do not break security or needlessly infringe privacy. Existing proxies often break security – like MITM proxies that prevent the use of certificate pinning and EV certificates – and some encryption protocols may even be blocked by the proxies, forcing users onto insecure protocols. Yet network operators, service providers, enterprises, small businesses and individuals want to be able to grant proxy access to data proportionately. This tension needs a solution.

One solution is TLMSP.

TLMSP defines a profile that allows endpoints to create an authenticated end-to-end encrypted session, and authorise middleboxes to access portions of the encrypted traffic. Endpoints control granting of access to middleboxes and control their permissions, prior to the sending of any application layer traffic. No middleboxes can be added or have permissions granted without endpoints agreeing to both their presence and their permission level. Full details are available in the Technical Specification (**TS 103 523-2** [2]).

3.3 MSP Part 3: Profile For Enterprise Network and Data Centre Access Control (TS 103 523-3)

MSP Part 3, also called Enterprise Transport Security (ETS), was driven by an industry need to upgrade from TLS 1.2, whilst retaining capability to perform vital data centre operations. Such required operations and functionality include troubleshooting, network management, and investigation of network attacks.

MSP Part 3 (TS 103 523-3 [3]) specifies an implementation variant of TLS 1.3. This provides a strict improvement to security from TLS 1.2, and is needed because TLS 1.3 removes vital functionality: semi-static key exchange is not supported, which prevents passive decryption of TLS 1.3 sessions at any scale. However, there are operational circumstances where passive decryption of sessions by authorized middleboxes is necessary.

Such situations generally occur 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 – and access to the unencrypted packet data is required for operational reasons, either in real-time or after the session has ended, such as troubleshooting, compliance, load-balancing, intrusion detection, or prevention of DDoS attacks.

To enable these operations, ETS specifies use of a semi-static Diffie-Hellman key – the server does not change its private key for each session, but may change it daily or weekly instead. Clients have visibility that this semi-static method is being used, and of the policy describing how the server will use the keys.

There are limited but essential circumstances where the visibility information provided in the session is not suitable; this case is described in Annex A of TS 103 523 Part 3 [3], which creates an exception of ETS where this visibility information is not sent in limited essential circumstances. When ETS is widely supported, the Annex A exception will be deprecated, as Annex A is not fully MSP-compliant according to the security requirements and framework laid out in TS 103 523 Part 1 [1].

ETS allows network operators of data centres and enterprises to meet their service agreements and legal mandates; prevents users being forced to revert to older, less secure protocols; and allows data centre operators and users to control access to their data.

Full details and motivations are available in the Technical Specification (TS 103 523-3 [3]).

4 Summary

MSP enables a new way of performing network security with middleboxes, retaining the important functionality that middleboxes provide, whilst specifying the next generation of middlebox protocols. MSP's security framework gives users transparency of what is happening with their data, control over who accesses their data, and provides protocols that address, rather than ignore, industry use cases.

- MSP Part 1 (TS 103 523-1 [1]) stipulates a new benchmark of security and privacy for middleboxes.

- MSP Part 2 (TS 103 523-2 [2]) combines academic research with industry innovation to create an advanced protocol.
- MSP Part 3 (TS 103 523-3 [3]) solves vital operational issues caused by emerging standards.

MSP was created by industry, for industry, specifying ground-breaking protocols for the next generation of proxy technologies.

Annex A: References

[1] ETSI TS 103 523-1 V1.1.1: “CYBER; Middlebox Security Protocol; Part 1: MSP Framework and Template Requirements”.

[2] ETSI TS 103 523-2 V1.1.1: “CYBER; Middlebox Security Protocol; Part 2: Transport layer MSP, profile for land gained access control”.

[3] ETSI TS 103 523-3 V1.3.1: “CYBER; Middlebox Security Protocol; Part 3: Enterprise Transport Security”.

[4] ETSI TR 103 421 V1.1.1: “CYBER; Network Gateway Cyber Defence”.

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

This White Paper is issued for information only. It does not constitute an official or agreed position of ETSI, nor of its Members. The views expressed are entirely those of the author(s).

ETSI declines all responsibility for any errors and any loss or damage resulting from use of the contents of this White Paper.

ETSI also declines responsibility for any infringement of any third party's Intellectual Property Rights (IPR), but will be pleased to acknowledge any IPR and correct any infringement of which it is advised.