MEF SASE Certification:

Frequently Asked Questions

March 2025, FAQ v1

Summary

This FAQ provides more information about MEF SASE Certification. We address 44 common questions and provide links to additional material that should be of value to a wide range of industry professionals.

Contents

Cybersecurity Markets

1. Why should enterprises be concerned with Cybersecurity?

The risk of major cyberattacks against private and public sector organizations has never been greater. A rapidly growing digital economy, accelerating digital transformation across all industries, the inability of overwhelmed cyber defenses to keep pace with threats, the expanding use of AI by threat actors, a shortage of skilled cybersecurity experts, and geopolitical instability are all contributing to the increasing volume, sophistication, speed, scale, and costs of cyberattacks worldwide. Cybercrime is projected to grow from $8 trillion in 2023 (7.7% of global GDP) to $10.5T by 2025 (9.5% of forecasted global GDP), according to Cybersecurity Ventures.

The cost of global cybercrime grew 14% from $7T in 2022 to $8T in 2023 and is set to climb to $10.5T in 2025, according to Cybersecurity Ventures. The 2023 figure equates to ~$1,310 for each of the Internet's 5.35B users (Statista), 48% to 57% of the global digital economy, 7.7% of global GDP, or 3.6 x the $2.2T of total global defense spending (International Institute for Strategic Studies). The cybercrime estimate includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, fraud, and other costs.

Cybersecurity Ventures expects cybercrime to grow at nearly 5 x the rate of global GDP through 2025 based on historical growth trends, a dramatic increase in nation-state sponsored and organized crime activities, and an "order of magnitude' increase in the cyberattack surface caused by booming growth in mobile, cloud, IoT, and other digital services and technologies.

Examples of high profile cybersecurity breaches include:

Apr 2024. UnitedHealth Group – Company has provided $6B+ in advance funding and loans to support healthcare providers impacted by ransomware attack against its Change Healthcare clearinghouse platform.

Feb 2024. Volt Typhoon – living off the land pre-positioning on critical infrastructure, posing "a critical business risk for every organization in the United States and allied countries."

Dec 2023. Kyivstar – Russian hackers reportedly "completely destroyed the core" of Ukraine's largest mobile operator and left 24 million customers without services for several days.

2. How would you characterize the Cybersecurity market?

Gartner estimates global spending on information security and risk management was $188B in 2023, which equates to ~8.2% of IDC's estimate for total digital transformation spending or 2.4% of the cost of global cybercrime in the year. Gartner forecasts information-related security spending will increase 14% to $215B in 2024, with $90B from security services, $33.3B from infrastructure protection, $24.4B from network security equipment, $18.6B from identity access management, $7B from cloud security, and the remainder from other segments.

In October 2022, McKinsey argued that cybersecurity spending around this level is probably insufficient considering the forecasted $10.5T global cybercrime problem by 2025. Noting that “As the digital economy grows, digital crime grows with it,” McKinsey estimated the global cybersecurity total addressable market could reach $1.5T to $2T at some point in the future – eventually placing it in the range of 7 to 9 times current spending on information security.

3. How would you characterize the SD-WAN market?

The SD-WAN market is fast-growing with tens of billions of dollars in revenue at stake over the next 5 years. Multiple analyst firms expect security to be an increasingly important factor in SD-WAN sales.

SD-WAN Services

The global managed SD-WAN services market is expected to grow at a 38% CAGR from $2.85B in 2020 to $14.5B in 2025, according to Frost & Sullivan. This estimate includes both SD-WAN overlay and associated underlay connectivity services.

Appledore Research estimates the global SD-WAN services market – including both service provider managed and integrated services – will reach at least $22B in 2027. Vertical Systems Group estimates the U.S. carrier managed SD-WAN services market surpassed $1B in 2020. This number includes SD-WAN service features as well as WAN access connectivity.

SD-WAN Technology Vendors

IDC estimates the global SD-WAN infrastructure market will grow at a 19% CAGR from $3B in 2020 to $7B in 2025.

Dell’Oro estimates the SD-WAN technology market will grow from $1.5+B in 2020 to at least $4B in 2025. The firm says the market grew 39% year over year in 1H21, with vendors increasingly differentiating around security.

Appledore Research estimates the global SD-WAN software supplier market is poised to grow from $1.2B in 2020 to a minimum of $7B in 2027.

4. How would you characterize the SASE market?

Frost & Sullivan research illustrates that a large and growing number of organizations are strategically committed to converging networking and security to achieve more efficient, secure, and scalable networks better suited than legacy architectures to support digital transformation, cloud adoption, and hybrid work. A 2023 Frost & Sullivan ICT Network Services survey of 1,624 cybersecurity decisionmakers and influencers revealed that 60% expected their organizations to converge network and security in their network strategy during the next two years.

Frost & Sullivan’s *2023 Voice of Enterprise Security Customer Survey* – which incorporated feedback from 2,448 cybersecurity leaders based in seven large economies – found that 46%

of organizations are using SASE solutions and another 38% plan to adopt SASE by 2024. Only 13% were not considering SASE adoption.

Gartner's 2023 *Forecast Analysis: Secure Access Service Edge, Worldwide* report predicts the SASE market will grow at a 29% CAGR from ~$9B in 2023 to more than $25B in , with the shift to cloud computing and remote work driving demand for secure access from any device and anywhere. The firm expects that the largest SD-WAN and SSE vendors will offer completely converged single-vendor SASE solutions by 2027. An estimated 60% of new SD-WAN purchases will be part of a single-vendor SASE offering by 2026, compared to 15% in 2023, according to the firm's *Critical Capabilities of Single-Vendor SASE* (2023) report.

In 2023, Gartner surveyed 2,457 CIOs and other technology executives based in 84 countries who represented all major industry sectors, ~$12.5T in revenue/public-sector budgets, and $163B in IT spending. Thirty-nine percent of respondents said that their organization had deployed or plans to deploy SASE by mid-2025, according to firm's *2024 CIO and Technology Executive Survey*.

Dell'Oro estimates the SASE technology market will grow 26% from $8.4B in 2023 to $10.6B in 2024, with the increased necessity for secure cloud and remote work solutions fueling robust growth. The SD-WAN portion of the technology market climbed above $3B in 2023, while the SSE segment moved past $4B during the same year.

Longer term, Dell'Oro anticipates spending on SASE technology will surge past $16B by 2028, with a double-digit CAGR fueled by rising demand for integrated networking and security solutions tailored for the hybrid work environment. The company expects SD-WAN revenues to climb above $6B (~40% of the SASE market), while SSE revenues are poised to reach nearly $10B (~60% of the SASE market).

5. What is MEF's role in the Cybersecurity market?

The SASE market has suffered from problems like those in the early years of SD-WAN. MEF interviews with dozens of service provider professionals revealed the lack of industry alignment to a SASE standard caused confusion, increased inefficiency and operational costs, impeded integration and interoperability, and hindered adoption. As one SP expert explained, "We have to do SASE 101 each time we talk with a customer." Others noted, "Everyone is talking SASE, but there is a lot of confusion in the market," with "SASE vendors all over the place – defining SASE to emphasize their strengths." Many vendors were "jumping on to check the boxes for SASE," but they ran into problems supporting individual functions that should be part of a holistic solution.

SASE technology vendors and service providers within the MEF community who have contributed to development of SASE standards and/or are participating in the SASE certification program are doing their part to help increase industry efficiency, enable deployment of robust, validated cybersecurity solutions, and accelerate SASE adoption. Government and private sector leaders are now able to leverage their work to align stakeholders on standardized and scalable converged cybersecurity/networking solutions and strengthen critical infrastructure and other sectors.

MEF’s SASE standardization and certification programs are designed to help build a vibrant, efficient market by addressing customer education, migration, and other top challenges that have slowed adoption. Standardization and certification, among other things, help align stakeholders on SASE terminology and service attributes, support SASE education and training, make it easier to integrate elements supplied by different vendors into a single unified SASE solution, and validate the cyber defense effectiveness and application performance of SASE technologies and services.

MEF Cybersecurity Standards

6. Why is MEF working to standardize Cybersecurity?

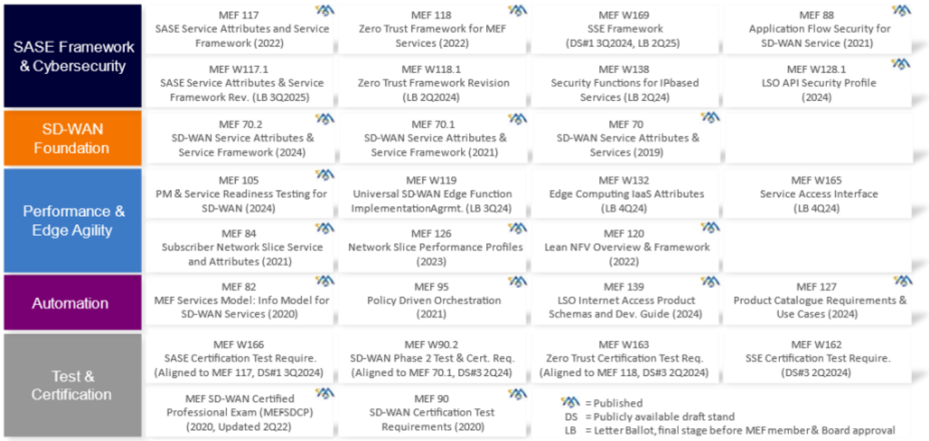
MEF is the world’s leading communications industry organization shaping SASE and SD-WAN markets through standardization and certification of services, technologies, and professionals. In 2019, MEF published the first global standard (*MEF 70*) defining an SD-WAN service and its attributes. And, in 2022, MEF introduced the industry-first *MEF 117 SASE Service Attributes and Service Framework* standard and closely tied *MEF 118 Zero Trust Framework* standard to address security needs associated with secure digital transformation.

MEF’s SASE standardization and certification programs are designed to help build a vibrant, efficient market by addressing customer education, migration, and other top challenges that have slowed adoption. Standardization and certification, among other things, help align stakeholders on SASE terminology and service attributes, support SASE education and training, make it easier to integrate elements supplied by different vendors into a single unified SASE solution, and validate the cyber defense effectiveness and application performance of SASE technologies and services.

7. What is the status of MEF’s Cybersecurity standardization work?

MEF thus far has initiated 28+ SASE-related standards initiatives within the context of the industry’s transformation toward NaaS across an automated ecosystem. Emerging NaaS solutions combine on-demand connectivity, application assurance, cybersecurity, and multi-cloud services into service bundles that can be ordered, delivered, and managed across horizontally integrated networks worldwide. Many organizations will evolve from SD-WAN to SASE and eventually NaaS with integrated SASE as they look to strengthen cyber defense and achieve other business objectives without having to build and maintain their own infrastructure.

MEF currently has 10+ active cybersecurity-related projects and incubation groups across five broad areas: SD-WAN foundation, automation, performance & edge agility, cybersecurity, and test & certification.



SASE Framework & Cybersecurity	MEF 117 ✓ SASE Service Attributes and Service Framework (2022)	MEF 118 ✓ Zero Trust Framework for MEF Services (2022)	MEF W169 SSE Framework (DS#1 3Q2024, LB 2Q25)	MEF 88 ✓ Application Flow Security for SD-WAN Service (2021)
	MEF W117.1 SASE Service Attributes & Service Framework Rev. (LB 3Q2025)	MEF W118.1 Zero Trust Framework Revision (LB 2Q2024)	MEF W138 Security Functions for IPbased Services (LB 2Q24)	MEF W128.1 ✓ LSO API Security Profile (2024)
SD-WAN Foundation	MEF 70.2 ✓ SD-WAN Service Attributes & Service Framework (2024)	MEF 70.1 ✓ SD-WAN Service Attributes & Service Framework (2021)	MEF 70 ✓ SD-WAN Service Attributes & Services (2019)	
Performance & Edge Agility	MEF 105 ✓ PM & Service Readiness Testing for SD-WAN (2024)	MEF W119 Universal SD-WAN Edge Function ImplementationAgrmt. (LB 3Q24)	MEF W132 Edge Computing IaaS Attributes (LB 4Q24)	MEF W165 Service Access Interface (LB 4Q24)
	MEF 84 ✓ Subscriber Network Slice Service and Attributes (2021)	MEF 126 ✓ Network Slice Performance Profiles (2023)	MEF 120 ✓ Lean NFV Overview & Framework (2022)	
Automation	MEF 82 ✓ MEF Services Model: Info Model for SD-WAN Services (2020)	MEF 95 ✓ Policy Driven Orchestration (2021)	MEF 139 ✓ LSO Internet Access Product Schemas and Dev. Guide (2024)	MEF 127 ✓ Product Catalogue Requirements & Use Cases (2024)
Test & Certification	MEF W166 SASE Certification Test Require. (Aligned to MEF 117, DS#1 3Q2024)	MEF W90.2 SD-WAN Phase 2 Test & Cert. Req. (Aligned to MEF 70.1, DS#3 2Q24)	MEF W163 Zero Trust Certification Test Req. (Aligned to MEF 118, DS#3 2Q2024)	MEF W162 SSE Certification Test Require. (DS#3 2Q2024)
	MEF SD-WAN Certified Professional Exam (MEFSDCP) (2020, Updated 2Q22) ✓	MEF 90 ✓ SD-WAN Certification Test Requirements (2020)	✓ = Published DS = Publicly available draft stand LB = Letter Ballot, final stage before MEF member & Board approval	

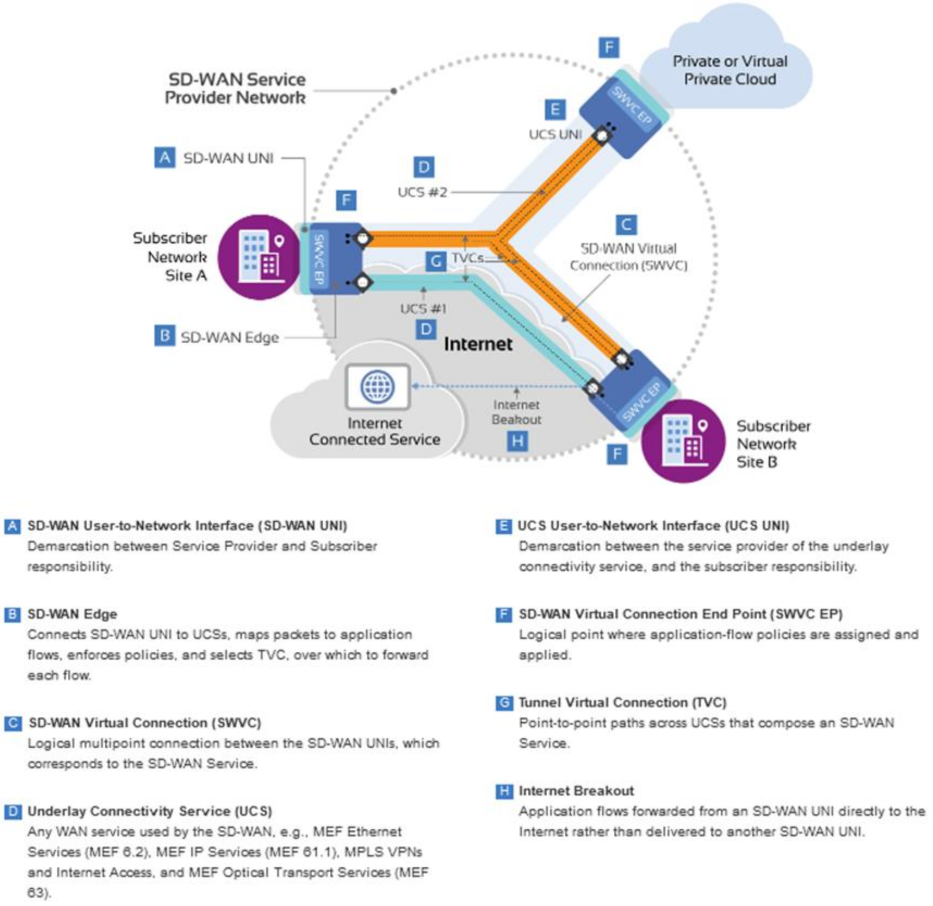
Figure 1 – MEF SD-WAN and SASE Standards Work

8. What is in the MEF 70.1 SD-WAN Service Attributes and Services Framework standard?

MEF 70.1 SD-WAN Service Attributes and Services Framework describes requirements for an application-aware, over-the-top WAN connectivity service that uses policies to determine how application flows are directed over multiple underlay networks irrespective of the underlay technologies or service providers who deliver them.

Building upon MEF 70, MEF 70.1 includes the following key elements:

- SD-WAN service concepts, service attributes for an SD-WAN virtual connection (SWVC), SWVC end point, and SD-WAN UNI, and new service attributes for an underlay connectivity service (UCS), UCS end point, and UCS
- SD-WAN service framework for defining instances of a service based on definitions, service elements, and service attributes.
- New measurable performance metrics for policy-defined application
- New support for virtual topologies that can be assigned by
- New support for partitioning subscribers IP hosts into zones and assigning zone-wide
- Provides the infrastructure to support application flow security defined in MEF


SD-WAN Service Provider Network
Private or Virtual Private Cloud
F
E
UCS UNI
SWVC EP
A SD-WAN UNI
D
UCS #2
F
C
SD-WAN Virtual Connection (SWVC)
Subscriber Network Site A
SWVC EP
G TVCs
UCS #1
D
B SD-WAN Edge
Internet
Internet Connected Service
Internet Breakout
H
SWVC EP
F
Subscriber Network Site B

A SD-WAN User-to-Network Interface (SD-WAN UNI)
Demarcation between Service Provider and Subscriber responsibility.

B SD-WAN Edge
Connects SD-WAN UNI to UCSs, maps packets to application flows, enforces policies, and selects TVC, over which to forward each flow.

C SD-WAN Virtual Connection (SWVC)
Logical multipoint connection between the SD-WAN UNIs, which corresponds to the SD-WAN Service.

D Underlay Connectivity Service (UCS)
Any WAN service used by the SD-WAN, e.g., MEF Ethernet Services (MEF 6.2), MEF IP Services (MEF 61.1), MPLS VPNs and Internet Access, and MEF Optical Transport Services (MEF 63).

E UCS User-to-Network Interface (UCS UNI)
Demarcation between the service provider of the underlay connectivity service, and the subscriber responsibility.

F SD-WAN Virtual Connection End Point (SWVC EP)
Logical point where application-flow policies are assigned and applied.

G Tunnel Virtual Connection (TVC)
Point-to-point paths across UCSs that compose an SD-WAN Service.

H Internet Breakout
Application flows forwarded from an SD-WAN UNI directly to the Internet rather than delivered to another SD-WAN UNI.

Figure 2 – SD-WAN Service Components

SD-WAN standardization offers numerous benefits that help accelerate SD-WAN market growth and improve customer experience. Key benefits include:

- Enables a wide range of ecosystem stakeholders to use the same terminology when developing, buying, selling, deploying, and delivering SD-WAN services.
- Makes it easier to interface policy with intelligent underlay connectivity services to provide a better end-to-end application experience with service resiliency.
- Facilitates inclusion of SD-WAN services in standardized LSO architectures, thereby advancing efforts to orchestrate SD-WAN services across automated networks.
- Facilitates creation of certified MEF 3.0 SD-WAN services, which give users confidence that a service meets a fundamental set of requirements.

9. What is in the MEF 117 SASE Service Attributes and Service Framework Standard?

MEF W117 SASE Service Attributes and Service Framework is the industry's first standard defining SASE services and attributes. SASE combines security functions and connectivity services with subscriber policies to address modern security concerns. A SASE service enables secure access and secure connectivity for subscriber users, devices, and applications to targeted resources (applications or devices). This access is independent of the location of users, devices, and applications and is authorized according to subscriber policies.

MEF 117 SASE Service Attributes and Services Framework describes requirements for an session-aware, over-the-top end-to-end secure connectivity service that uses policies to determine how:

- Sessions are encrypted and encapsulated
- Sessions have only actors that are authenticated and authorized
- Sessions meet the appropriate security posture
- Sessions are directed over multiple underlay networks irrespective of the underlay technologies or service providers who deliver them.
- Sessions are continuously monitored for compliance to policy

Key components of a SASE service are:

- Sessions
- SASE Edges
- Policy End Points
- Identity and Access Management
- Security Functions
- Advanced IP Packet Forwarding
- Continuous Monitoring
- SASE Policies

The SASE service secures the flow of IP packets between a subject actor and a target actor by recognizing a SASE session, authenticating the actors, implementing security functions, and determining forwarding behavior by applying and monitoring SASE policies to the session.

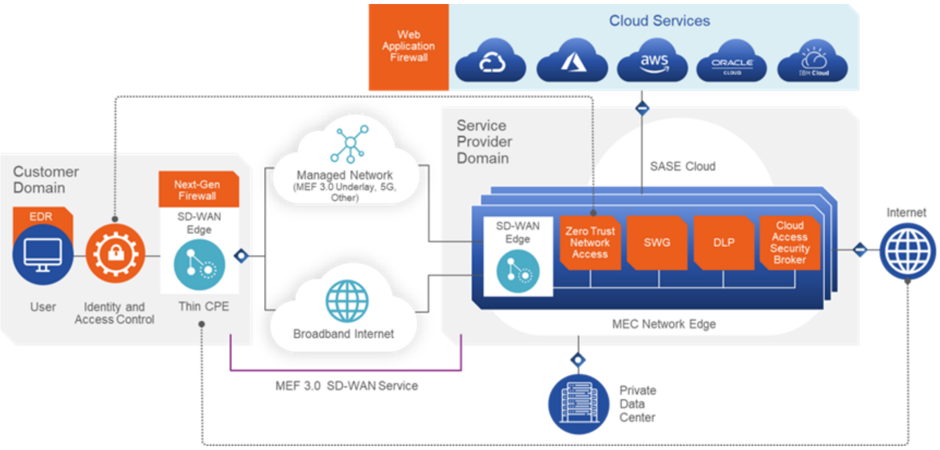


Figure 3 – Secure Access Service Edge

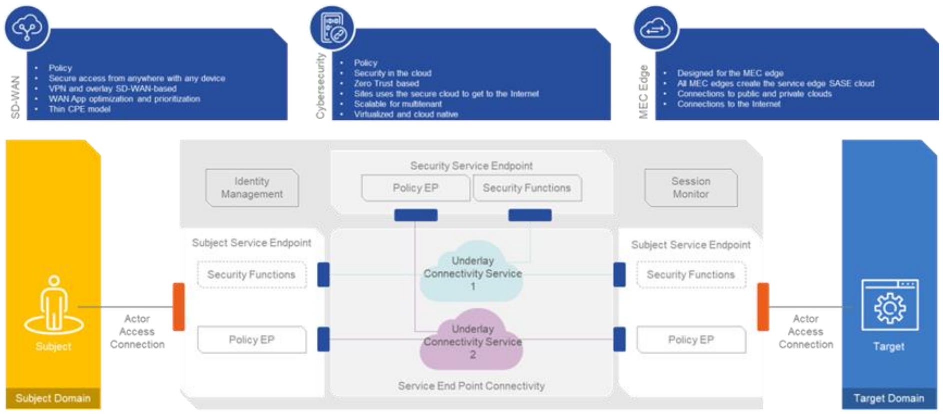

SD-WAN
Policy
Secure access from anywhere with any device
VPN and overlay SD-WAN-based
WAN App optimization and prioritization
Thin CPE model
Cybersecurity
Policy
Security in the cloud
Zero Trust based
Sites uses the secure cloud to get to the Internet
Scalable for multitenant
Virtualized and cloud native
MEC Edge
Designed for the MEC edge
All MEC edges create the service edge SASE cloud
Connections to public and private clouds
Connections to the Internet
Identity Management
Security Service Endpoint
Policy EP
Security Functions
Session Monitor
Subject Service Endpoint
Security Functions
Policy EP
Underlay Connectivity Service 1
Underlay Connectivity Service 2
Service End Point Connectivity
Subject Service Endpoint
Security Functions
Policy EP
Subject
Actor Access Connection
Subject Domain
Actor Access Connection
Target
Target Domain

Figure 4 – SASE Service Components

Important SASE standardization benefits include:

- Increases industry efficiency by aligning stakeholders on common terminology when developing, buying, selling, deploying, and delivering SASE services.
- Makes it easier to interface policy with security functions to provide consistent and uniform cybersecurity postures from anywhere.
- Facilitates inclusion of SASE services in standardized LSO architectures, thereby advancing efforts to orchestrate certified MEF 3.0 SASE services from enterprises and between cybersecurity ecosystem partners.
- Facilitates creation of certified MEF 3.0 SASE services, which will give users confidence that a service meets a fundamental set of cybersecurity requirements.

10. How does SASE compare to the traditional approach to network security?

The SASE concept adjusts for a fundamental change in how enterprise users access business systems and increased demand for lower-latency edge compute capabilities closer to the user. The well-defined and static network edge of the past is being replaced by more users working outside corporate walls and accessing business systems beyond corporate data centers. SASE shifts the focus from site-centric to user-centric security. The user can be anything and anywhere, and security and network functions can be distributed in cloud infrastructure, at high-performance edge locations, or in the enterprise data center to maximize the availability, reliability, and compliance to enterprise business requirements.

11. What is in the MEF 118 Zero Trust Framework standard?

MEF 118 Zero Trust Framework and Service Attributes defines a Zero Trust Framework (ZTF) and service attributes for dynamic policy-based actions applied to users, devices, and applications wanting to access networked resources. The ZTF consists of subject and target actors, identity management, access control, policy, policy end points, and continuous monitoring. While MEF 118 does not define a specific service, it does define ZTF service attributes that can be used by MEF-defined services, as shown in the SASE example below.

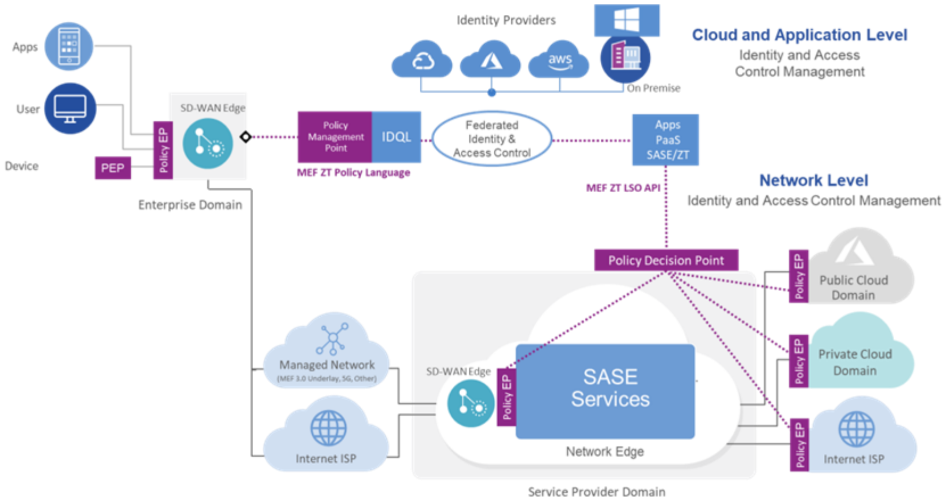
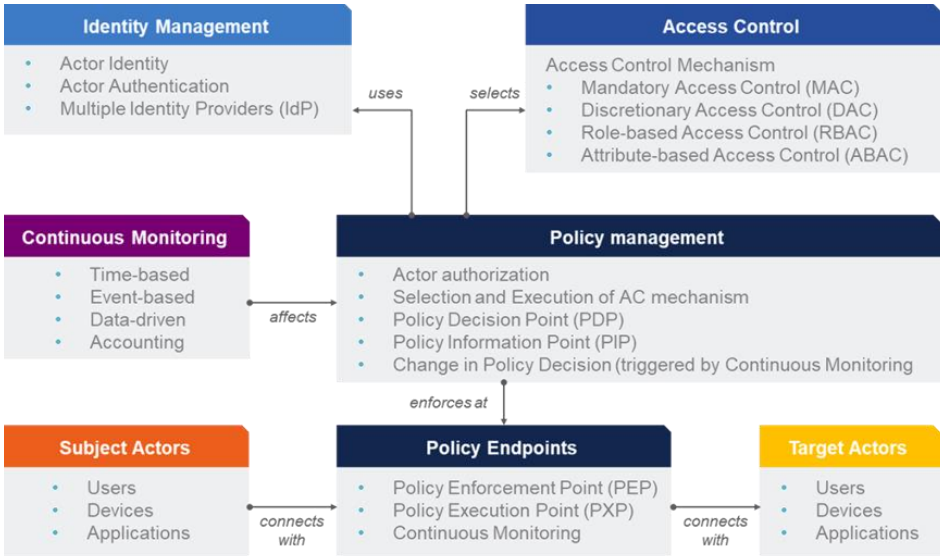


Figure 5 – Zero Trust Framework



Identity Management
Actor Identity
Actor Authentication
Multiple Identity Providers (IdP)
uses
selects
Access Control
Access Control Mechanism
Mandatory Access Control (MAC)
Discretionary Access Control (DAC)
Role-based Access Control (RBAC)
Attribute-based Access Control (ABAC)
Continuous Monitoring
Time-based
Event-based
Data-driven
Accounting
affects
Policy management
Actor authorization
Selection and Execution of AC mechanism
Policy Decision Point (PDP)
Policy Information Point (PIP)
Change in Policy Decision (triggered by Continuous Monitoring
enforces at
Subject Actors
Users
Devices
Applications
connects with
Policy Endpoints
Policy Enforcement Point (PEP)
Policy Execution Point (PXP)
Continuous Monitoring
connects with
Target Actors
Users
Devices
Applications

Figure 6 – SASE Service Incorporates Zero Trust

12. What is in the MEF 118.1 Zero Trust Framework Revision standard?

MEF 118.1 expands on the Zero Trust Framework definition by including the following:

- Introduction of multi-factor authentication (MFA) and introduces a requirement that MFA be supported for User Actor Authentication.
- Added requirements for logging successful and failed authentication requests that can assist in identifying the root cause of security breaches.
- Introduces Zero Trust requirements for non-programmatic, User-to-User interactions which occur when a Subject User Actor interacts with a Target User Actor, e.g., verbal communications directly between people or between a person and an AI-driven chatbot acting as a proxy for a person. Such interactions are common when using social engineering techniques where a User, impersonating a legitimate User, seeks to obtain access to legitimate User's information for malicious purposes.
- Introduces an Actor's Risk Score for Subject and Target Actors and a new Actor Risk Score Service Attribute
- New informative Appendix which introduces the term Trust Confidence Score which may be provided by a Risk Monitoring Service as opposed to a Risk Score. The section provides a mathematical model for how to convert a Trust Confidence Score to a Risk Score for use in the Risk Score Service Attribute
- New informative Appendix which provides examples of Event-based Continuous Monitoring for an IP Service that uses Security Functions specified in MEF 138 [32]
- New informative Appendix which provides example use cases for Continuous Monitoring of User, Device, and Application Actors
- New informative Appendix which provides example use cases for Authenticating and subsequently Allowing or Blocking User-to-User Actor interactions based on Security Policies

13. What is in the MEF 138 Security Functions for IP-based Services standard?

The MEF W138 Security Functions for IP-based Services standard specifies the requirements needed to add Security Functions to an IP Service.

MEF 138 defines the set of parameters that need to be agreed between the Subscriber and Service Provider for each Security Function. It also defines Security Functions that, when enabled, enforce the Policy on a per-Service Flow basis:

- IP, Port and Protocol Filtering Security Function,
- DNS Protocol Filtering Security Function,
- Domain Name Filtering Security Function,
- URL Filtering Security Function,
- Malware Detection and Removal Security Function,
- Data Loss Prevention Security Function,
- Protective DNS Security Function,
- Decryption and re-encryption by a Middlebox Security Function.

The capabilities required to support these Security Functions are also defined.

14. What is in the MEF 117.1 SASE Service Attributes and Service Framework Revision standard?

MEF 117.1 expands on the SASE Service definition by including the following:

- Adding the following Performance Metrics:
    - One-Way Mean Packet Delay
    - One-Way Mean Packet Delay
    - One-Way Packet Loss Ratio
- Adding the following Service Attributes:
    - List of SASE Rate Limiters Service Attribute
    - List of SASE Session Business Importance Levels Service Attribute
    - List of SA-IdAM Application Flow Specifications Service Attribute
    - List of Data Integrity Actions Service Attribute
    - SASE Performance Time Intervals Service Attribute
    - SASE Service Performance Objectives Reporting Periods Service Attribute
    - SASE UCS Service Attributes
    - UCS Identifier Service Attribute
    - UCS Type Service Attribute
    - UCS Billing Method Service Attribute
    - SASE UCS UNI Service Attributes
- Updating SASE Agent requirements to apply only if a SASE Service includes a SASE Agent.
- Enhancing Application Flow Specification Criteria
- Updating SASE Session Forwarding Policy to include the following Criterion:
    - Encryption
    - UCS type
    - UCS Billing Method
    - Session Business Importance
    - Session Performance
    - Bandwidth
- Adding the following Security Functions:
    - Supported Application Identity and Access Management (SA-IdAM)
    - Data Integrity
    - Proxy
    - Cloud Access Security Broker (CASB)
- Adding SD-WAN Policy considerations when SD-WAN utilized by a SASE Service
- Adding SASE Use Cases

15. What is in the MEF 119 Universal SD-WAN Edge standard?

MEF 119 defines the Universal SD-WAN Edge (USWE) and specifies the USWE implementation requirements. It also specifies the requirements on the vendor propriety SD-

WAN Edge and on SD-WAN vendor manager to support the interoperability between these entities and the USWE.

The Universal SD-WAN Edge included in this specification includes the following:

- Universal Management Plane
  - The set of functions that allows management of the USWE instance.
- Universal Control Plane
  - The set of functions that allows the USWE implementation to exchange routing information with the SD-WAN Vendor control plane.
- Universal Data Plane
  - The set of functions that allows the USWE implementation to exchange data traffic with other SD-WAN Edges within an SD-WAN Service

Some of these functions, as described, are required to be supported in both the Universal SD-WAN Edge and the interconnected or the SD-WAN Vendor Controller.

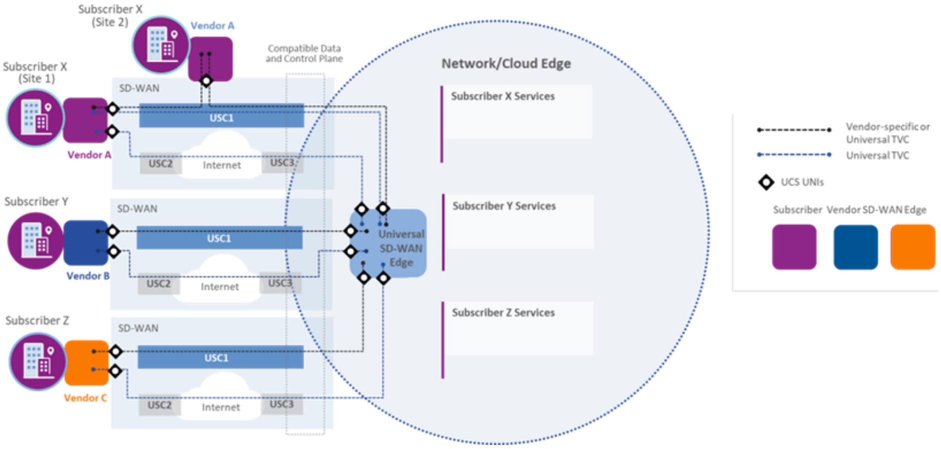


Figure 7 – Universal SD-WAN Edge

16. Can you describe the SD-WAN use case in the MEF 84 Network Slice standard?

Enterprise users are looking for a frictionless end-to-end experience with guaranteed performance and security from their devices to their applications/services, regardless of a user's location. The idea with network slicing is to carve out a subset of the end-to-end network infrastructure that could carry performance objectives and, in the future, security objectives. The end-to-end network slice needs to be orchestrated across all the individual networks involved in providing a subscriber's end-to-end experience, including the subscriber network, the service provider network(s), and the cloud provider network.

MEF 84 Subscriber Network Slice Service and Attributes describes network slicing within the context of MEF LSO and MEF services. MEF 84 uses the term "Network Service" to define a network slice offered as a service to one or more subscribers. The idea is that service providers can structure and organize subsets of their infrastructure into network slices that can be managed, controlled, and orchestrated independently from other network slice subsets.

In an example SD-WAN use case, an enterprise could buy a set of several network slices (i.e., real-time, premium, or business) and overlay their SD-WAN performance objectives onto each of these slices. The end-to-end network slice could be based on networks involving both wireline and wireless resources, including 5G.

See the MEF CTO Chat: MEF End-to-End Slicing, SD-WAN, and 5G (September 2020) for a deeper discussion of this topic with illustrations.

17. What is NaaS?

Network-as-a-Service (NaaS) presents a new-paradigm solution by combining on-demand connectivity, application assurance, cybersecurity, and multi-cloud-based services delivered across a standards-based automated ecosystem of partners. MEF defines the building blocks for a NaaS industry model that enables rapid innovation. The baseline begins with the MEF3.0 Global Services Framework for LSO automation APIs, standardized services, testing, training & certification, and references work from other industry bodies.

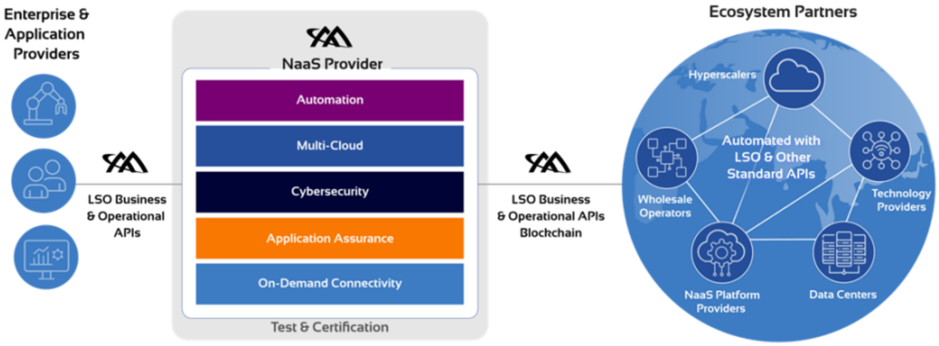


Figure 8 – Naas Framework

API Automation

18. What SD-WAN automation standards have been published thus far?

MEF thus far has published two SD-WAN automation-related standards: MEF 82 and MEF 95.

MEF 82 MEF Services Model: Information Model for SD-WAN Services describes MEF 70 in a programming object model representation that can be used to build LSO APIs to orchestrate SD-WAN services. This document defines the MEF Services Model (MSM) as well as the UML classes, data types, and enumerations for representing SD-WAN services.

MEF 95 Policy Driven Orchestration provides a unified policy framework for MEF 70.1 and other SD-WAN and SASE-related standards. MEF 95 specifies how policy-based management and modeling can be used to realize orchestration functionality defined in MEF 55.1 Lifecycle Service Orchestration: Reference Architecture and Framework. It includes an example Domain Specific Language (DSL) that provides an intent program to connect multiple SD-WAN users between multiple sites.

19. What additional SD-WAN automation-related standards are in development?

MEF has several active LSO-based automation initiatives designed to enable faster rollout of SD-WAN services:

- MEF Internet Access Payload Incubation Group – focused on driving standards alignment on an Internet Access product payload that can be included in the LSO Marketplace. Many service providers have called upon MEF to prioritize LSO Sonata support for automation of Internet Access services, with SD-WAN being a driving factor.
- MEF W100 LSO Legato Service Provisioning, SD-WAN Schema Guide – defines a JSON/YAML-based SD-WAN schema guide for LSO Legato service provisioning. This standard falls within the scope of the MEF Services Model project.

20. What standards has MEF created related to security of APIs?

MEF published MEF 128.1 LSO API Security Profile (April 2024) which defines the security profile, security approaches and security architecture for LSO API security using OAuth2 and OIDC within either a centralized or federated identity provider framework. This document applies to all current and future LSO APIs.

MEF 128.1 is not a general reference on API security, but an LSO API-specific standard.

MEF 128.1 first defines the LSO API security architecture and conformance requirements to that architecture. The standard then defines the following security components:

- JWT Best Practices for LSO API Security
- JWKS Endpoints for cryptographic signatures and their verifications
- Structure and conformance requirements for JWSs and JWEs
- LSO API Payload Authenticity

SASE Certification

21. How is MEF assuring that Services and technologies solve the Cybersecurity challenges?

To address cyber threats and enterprise demand, MEF has introduced the world's first standards-based certification program that validates the cyber defense effectiveness and application performance of SASE solutions. Specifically, MEF has led the industry in standardizing and now certifying SASE services and technologies, which incorporate software-defined wide area networking (SD-WAN), Secure Access Service Edge (SSE), and Zero Trust (ZT) Framework.

The SASE Certification program is the latest major development in the decade-plus networking transformation involving adoption, standardization, and certification of SD-WAN, SASE, ZT, SSE, and network-as-a-service (NaaS) solutions. This effort is designed to align stakeholders on common terminology, instill confidence in the services and technologies, validate integration of SD-WAN, ZT, and SSE solutions into unified SASE offerings, help the industry operate more efficiently, and accelerate SASE adoption and market growth.

22. How would you characterize the importance of MEF SASE service, technology, and professional certifications?

MEF received a mix of opinions when it comes to the challenge posed by a lack of test, certification, and other tools for SASE. While numerous service provider experts said they see high value in potential SASE and Zero Trust certification.

MEF believes that SASE certification is “critical” or “important” for accelerating SASE market growth.

“As digital architecture gets more flexible, diverse, and distributed – clouds, hardware components, IoT devices – customers need to know that every element is secure and protected: the whole and the parts….

We're proud to help spearhead a new initiative led by MEF to independently certify cybersecurity protections for networking services…These SASE networking products and services provided by program participants will be tested, evaluated, and rated against new and existing standards developed by MEF and the industry. This will be the gold standard for cybersecurity validation when it comes to next-gen network services."

- Mike Troiano, Senior Vice President, Business Products, AT&T Business

“Cybersecurity is a black box. SASE is a black box within a black box. Nobody knows if it's working. A robust testing and certification program is essential to provide customers with visibility into what they're buying.”

- Vikram Phatak, CEO, CyberRatings.org

23. What is the SASE Certification Program?

The Secure Access Service Edge (SASE) Certification Program provides the foundation for cybersecurity in delivering confidence to the market. The SASE Certification Program helps service providers validate that their SASE cloud services are secure and address the persistent and increasingly malicious cyberthreats that threaten the public and private landscape. The SASE Certification Program enables value to the enterprise by testing the following functionality:

- Application performance during simulated WAN Impairments
- Scale and performance of a SASE cloud service
- Correct classification of applications so that performance and/or security polices can be applied.
- Effective Threat Protection against current Threat Databases
- Effective Evasion Detection against current Evasions Databases
- TLS/SSL functionality to validate cryptographic suites, version functionality, etc.
- Zero Trust principles for authentication and authorization of applications, users and devices via policies at the network level
- Compliance to MEF standards to enable an industry wide vocabulary, language, constructs, and service definition.

24. What certifications are needed for a Technology Provider or Service Provider to become SASE Certified?

SASE Certification is comprised of three individual certification programs:

- Software-Defined Wide-Area Network (SD-WAN)
- Security Service Edge (SSE)
- Zero Trust

MEF SASE certification is comprised of three certification programs. SD-WAN, Security Service Edge (SSE) and Zero Trust are individual certifications. When all three individual certifications are achieved, a final SASE certification is issued to the technology provider. The SASE certification is rendered out with a scoring and rating that averages amongst all three individual certifications. The scoring and rating system is based on a rating, from D (lowest) to AAA (highest).

A technology provider can obtain individual certifications on SD-WAN, SSE and Zero Trust which will appear in the MEF certification registry, but to get to become SASE certified, all three certifications must be obtained.

For the initial version of the SASE Certification Program, service providers will inherit the ratings of their technology providers in a particular service offering. A service provider can inherit individual certifications on SD-WAN, SSE and Zero Trust which will appear in the MEF certification registry. SASE certification will be provided if the service provider SASE solution contains a technology provider certification for each of the three categories (SD-WAN, Zero Trust, and SSE). It is possible that service providers can have multiple certification badges with each badge representing a specific service offering derived from different technology provider certifications for each certification category (ie: SD-WAN, SSE and Zero Trust). For a given service provider service offering, the technology provider certifications for each certification category will be averaged to provide a service provider SASE rating. The scoring and rating system is based on a rating, from D (lowest) to AAA (highest).

25. Who is the MEF accredited certification and testing partner?

CyberRatings is the MEF accredited certification and testing partner (MEF-ATCP). CyberRatings (CRO) launched in December 2020, CRO is a world-class lab dedicated to sharing knowledge of how to build, manage, and apply testing providing transparency and confidence in cybersecurity products and services.

CRO was founded by former executives of NSS Labs, an independent analysis and testing company recognized around the world for its fact-based cybersecurity guidance. Vikram Phatak, founder of CRO, was CEO of NSS Labs from 2007 – 2018.

CRO's proprietary ratings system (similar to Moody's) provides guidance on products and services capabilities in a language understood by all. This methodology is now an important component of MEF certifications.

26. What certification testing tools are used in the SASE Certifications?

The MEF SASE Certification is powered innovative solutions provided by Keysight and Spirent.

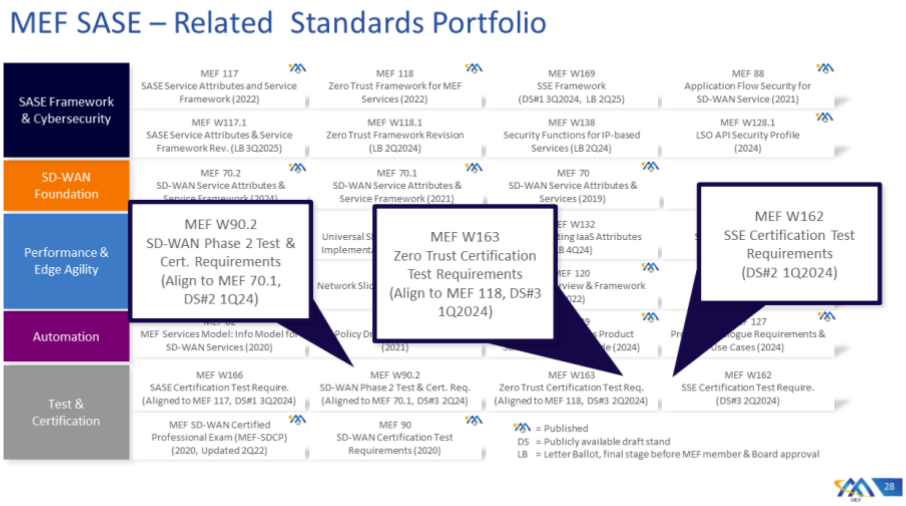
27. What certifications standards govern the SASE Certifications?

The SASE Certification for SD-WAN is governed by MEF W90.2 SD-WAN Phase 2 Test and Certification Requirements Draft (revision 1).

The SASE Certification for SSE is governed by MEF W162 SSE Certification Test Requirements Draft (revision 1).

The SASE Certification for Zero Trust is governed by MEF W163 Zero Trust Certification Test Requirements Draft (revision 1).

For information about all the MEF Test and Certification Standards which govern the SASE Certification Program, information can be found here.



MEF SASE – Related Standards Portfolio

SASE Framework & Cybersecurity

MEF 117
SASE Service Attributes and Service Framework (2022)

MEF 118
Zero Trust Framework for MEF Services (2022)

MEF W169
SSE Framework
(DS#1 3Q2024, LB 2Q25)

MEF 88
Application Flow Security for SD-WAN Service (2021)

MEF W117.1
SASE Service Attributes & Service Framework Rev. (LB 3Q2025)

MEF W118.1
Zero Trust Framework Revision (LB 2Q2024)

MEF W138
Security Functions for IP-based Services (LB 2Q24)

MEF W128.1
LSO API Security Profile (2024)

SD-WAN Foundation

MEF 70.2
SD-WAN Service Attributes & Service Framework (2024)

MEF 70.1
SD-WAN Service Attributes & Service Framework (2021)

MEF 70
SD-WAN Service Attributes & Services (2019)

Performance & Edge Agility

Universal S
Implement

EF W132
ting IaaS Attributes
B 4Q24)

Network Slic

EF 120
rview & Framework
022)

Automation

MEF Services Model: Info Model for SD-WAN Services (2020)

Policy Dr
(2021)

s Product
le (2024)

127
Pr logue Requirements & Use Cases (2024)

Test & Certification

MEF W166
SASE Certification Test Require.
(Aligned to MEF 117, DS#1 3Q2024)

MEF W90.2
SD-WAN Phase 2 Test & Cert. Req.
(Aligned to MEF 70.1, DS#3 2Q24)

MEF W163
Zero Trust Certification Test Req.
(Aligned to MEF 118, DS#3 2Q2024)

MEF W162
SSE Certification Test Require.
(DS#3 2Q2024)

MEF SD-WAN Certified Professional Exam (MEF-SDCP)
(2020, Updated 2Q22)

MEF 90
SD-WAN Certification Test Requirements (2020)

MEF W90.2
SD-WAN Phase 2 Test & Cert. Requirements
(Align to MEF 70.1, DS#2 1Q24)

MEF W163
Zero Trust Certification Test Requirements
(Align to MEF 118, DS#3 1Q2024)

MEF W162
SSE Certification Test Requirements
(DS#2 1Q2024)

= Published
DS = Publicly available draft stand
LB = Letter Ballot, final stage before MEF member & Board approval

28

Figure 9 – SASE Related Standards

28. How does the SASE Certification Program differ from the previous MEF SD-WAN Certification Program?

The SASE Certification Program (SD-WAN, SSE, Zero Trust, and SASE) is a subscription-based continuous integration/continuous test (CI/CT) model and process that allows service and technology providers repeated certification and the ability to get progressively better certification scores to deliver exceptionally great SD-WAN and cloud-based cybersecurity products to the market. The subscription period is 1 year for each certification from the initiation of the first tests. It should be noted that a yearly subscription must be maintained to keep any previous certifications and badges. For technology providers a single SASE Certification is a specific hardware family and a specific software revision. For service providers, a single SASE Certification applies to single service offering.

29. If a company has been previously MEF certified for SD-WAN, does that company need to achieve SASE Certification for SD-WAN?

Yes, the SASE Certification Program includes an improved SD-WAN certification based on MEF 70.1. The previous SD-WAN certification was based on MEF 70. Also, the SASE Certifications go beyond just conformance to MEF standards, but include performance metrics and ratings in specific categories.

30. Previously, MEF had advertised MEF 88 Application Security for SD-WAN, can a company still get certified in Secure SD-WAN and use that as part of the SASE Certification?

No, the SASE Certification Program includes SD-WAN, SSE, and Zero Trust. MEF W162 SSE Certification Test Requirements Draft (revision 1) document governs the testing methodologies and requirements for the MEF SASE Certification security component.   MEF W162 SSE Certification Test Requirements Draft (revision 1 relies on MEF 138 Security Functions for IP-based Services, which supersedes MEF 88 Application Security for SD-WAN.

31. Does a Technology Provider need to be a unified SASE vendor to achieve a SASE Certification?

No, a Technology Provider does not have to be a unified SASE vendor to achieve a SASE Certification. The SASE Certification Program allows for multiple products to be tested and achieve a SASE Certification. A Technology Provider only needs to certify the appropriate SASE components for SD-WAN, Zero Trust and SSE.

32. Does a Service Provider need to use a single unified SASE vendor in their service offering to achieve a SASE Certification?

No, a Service Provider does not have to use a single unified SASE Technology Provider to achieve a SASE Certification. The SASE Certification Program allows for multiple products to be tested and achieve a SASE Certification. A Service Provider only needs to present the appropriate SASE Technology Providers used in the service offering for SD-WAN, Zero Trust and SSE.

33. Can Service Provider achieve a SASE Certification without using SASE Certified Technology Providers in the service offering?

No, a Service Provider must use SASE Certified Technology Providers in the service offering to achieve a SASE Certification.

34. In order to inherit a certification from a Technology Provider, does a Service Provider need to run the same software version that a Technology Provider certified?

No, a Service Provider must use software versions within two major releases of the software certified by the Technology Providers in the service offering to achieve a SASE Certification.

35. Does MEF plan to enhance the SASE Certification Program to test the Technology Provider?

Yes, MEF is currently working on the testing methodologies and procedures necessary to test the Technology Provider for a SASE integration Certification. This enhancement would certify that the three components of the SASE Certification Program (SD-WAN, SSE, and Zero Trust) integrate into a single solution (either by utilizing a unified SASE solution or a disaggregated SASE solution of multiple vendor components).

36. Does MEF plan to enhance the SASE Certification Program to test the Service Provider service offering?

Yes, MEF is currently working on the testing methodologies and procedures necessary to test Service Provider service offerings such that Service Providers will no longer be required to use SASE Certified Technology Providers in the service offering to achieve a SASE Certification.

37. Does a company need to be a MEF member in order to achieve a SASE Certification?

Yes, a company must be a MEF member in order to achieve a SASE Certification. It should be noted that a yearly subscription must be maintained to keep any previous certifications and badges on the MEF Certification Registries.

38. What is the status of MEF SASE Certification Program?

The SASE Certification Program launched the 29th of October 2024.

39. Why did MEF choose a subscription model for the SASE Certification Program?

The SASE Certification program (SD-WAN, SSE, Zero Trust, and SASE) is a subscription-based continuous integration/continuous test (CI/CT) model and process that allows technology and service providers the ability retest to get progressively better certification scores to deliver exceptionally great SD-WAN and cloud-based cybersecurity products to the market. This aligns with industry standards that requires cybersecurity solutions to be periodically tested for effectiveness. The SASE Certification Program not only provides for a conformance to MEF Standards, but also provides enterprise relevant performance metrics for each hardware model tested. This allows enterprises to more effectively determine which SASE service or technology is best suited for the enterprise requirements.

40. How many companies have been certified?

Currently, four technology providers have achieved SASE Certifications in different subcategories. Two technology providers, Fortinet and Versa Networks have achieved full SASE certification.

Based on the Fortinet and Versa SASE Certifications, eleven service providers have achieved SASE Certification.

For a complete listing of the SASE Certification Program certified companies can be found in the MEF Services Certification Registry and the MEF Technology Certification Registry.

Companies interested in participating in the MEF SASE Certification Program should contact MEF.

41. What is next for the SASE Certification Program?

The SASE Certification Program is expected to evolve and include the following:

- Technology provider SASE Integration Certification. This additional certification will demonstrate that the technology provider can properly integrate the SD-WAN, Zero Trust, and SSE components of a SASE solution.
- Service provider SASE Certification for SD-WAN, Zero Trust, SSE and SASE Integration. These certifications will allow the service provider solutions to be tested and demonstrate SASE Certifications based on the performance of the service provider's service offerings.

42. What is the status MEF SD-WAN professional certification?

Introduced in late 2019, MEF’s SD-WAN Certified Professional (MEF-SDCP) program is the industry’s only exam verifying knowledge, skills, and abilities in the domains of SD-WAN based on the MEF 70 standard as well as other fundamentals of SD-WAN solutions. This exam is designed for technically oriented SD-WAN professionals ranging from pre-sales to network/service engineering and operational personnel in the service provider, technology vendor, and enterprise communities.

As noted above, 720+ MEF SDCPs are employed by 121+ companies.

Click here to learn about and register for the MEF-SDCP exam. Visit the MEF Professional Registry to see a list of MEF-SDCP and other certified professionals.

Participate in MEF

43. How can service, technology, or enterprise professionals participate in or learn more about MEF's SD-WAN and SASE work?

MEF SD-WAN & SASE Initiatives provides summaries and links to various items of work and serves as a useful starting point and a helpful resource to share with colleagues.

There are evolving resources and information on the SD-WAN and SASE sections of the MEF website, and the MEF Infinite Edge Series on YouTube offers valuable perspectives from thought-leading service and technology providers on SD-WAN and SASE-related topics.

Contributions to the SD-WAN and SASE work are welcomed. Contact MEF to express your interest and to obtain details on how you can participate.

Industry Perspectives on MEF SD-WAN & SASE

44. What are leading industry professionals saying about MEF's SD-WAN & SASE standardization work and SASE certification?

Below are nearly examples of public comments from leading service, technology, and market research professionals on MEF's SD-WAN and SASE standardization work and SASE certification.

Service Provider Perspectives

Aamir Hussain, *Chief Product Officer and Senior VP, Verizon Business Group*

"MEF 3.0 standards help drive SD-WAN and Carrier Ethernet interoperability for enterprises, service providers, and technology developers. Additionally, they drive end-to-end automation resulting in an improved customer experience and lower TCO. As a MEF 3.0 certified service provider, Verizon leverages these standards and capabilities to help drive our own Network-as-a-Service strategy. We are long-time supporters and contributors of the MEF mission." (MEF PR, June 2021)

Will Eborall, *AVP, Product Marketing Management, AT&T Business*

"There is value in these certifications, as they align with the telecommunications industry to help deliver the highest quality in networking functions. As companies continue their digital transformation, these standards assist to demonstrate the managed service providers' compliance in critical service functions around performance, assurance, and agility. It's definitely accelerated many aspects of our business." (MEF PR, June 2021)

Rupesh Chokshi, *VP Cybersecurity, AT&T*

"I think bodies and organizations like MEF can play a very important role as they bring the ecosystem together….We are providing that very critical infrastructure. So, the more standardization, the more scale, the more interoperability and federation, the better off we're going to be in the long run." (MEF Infinite Edge – SASE, March 2021)

Bob Victor, *SVP Product Management, Comcast Business*

"Becoming one of the first service providers to achieve MEF 3.0 SD-WAN certification underscores our commitment to being a technology and standards leader to improve the quality, management and interoperability of Ethernet and IP services for our customers. We're proud to lead the industry as the combination of SD-WAN, Ethernet and broadband connectivity displaces legacy networking and transport technologies." (MEF PR, March 2020)

Shena Seneca Tharnish, *VP, Cybersecurity Product Management, Comcast Business*

"I believe that standardization of new technology like SD-WAN and new frameworks like SASE are beneficial to all – not just the end consumer, but also the technology providers and the service providers – all those that are involved in architecting these solutions for business consumption. Standardization also allows for more efficient integration among technology partners involved in increasing consumer confidence that they're going to select quality products or solutions that have been vetted as secure, safe, and reliable." (MEF Infinite Edge – SASE, March 2021)

Mirko Voltolini, *VP, Innovation, Colt Technology Services*

"The MEF 70 standard sets the foundation for the adoption of common SD-WAN service attributes between service providers. The definition of a common standard for SD-WAN services will allow the industry to coordinate and align on the technology development. It will enable us to build end to end services across disparate service providers' domains and serve our global customer needs." (MEF PR, May 2019)

Frederick Chui, *Chief Commercial Officer, PCCW Global*

"PCCW Global's managed SD-WAN service is available in 80 countries and provides our customers with intelligent path selection on a dynamic high-speed underlay of IP-MPLS, Global Internet Access (GIA) and broadband connections. We are proud to be among the first few service providers in the world to be certified for MEF 3.0 SD-WAN services and applaud MEF for their efforts in setting up the first industry-wide SD-WAN standard (MEF 70). Our enterprise and wholesale customers embarking on their digital transformation journey can therefore expect better interoperability and improved application performance across disparate service providers' domains." (MEF PR, March 2020)

Vassilis Sanidas, *VP, Security Solutions Management, Global Presales & Technology Engagement, PCCW Global*

"One of the biggest challenges facing SASE adopters is the lack of standardization, which can create significant confusion for an enterprise considering a transition to the new technology. Standardization is very, very important." (MEF Infinite Edge – SASE, March 2021)

Satya Parimi, *Group Vice President, Data Products, Spectrum Enterprise*

"We are proud that Spectrum Enterprise is one of the first MEF-certified SD-WAN service providers because it demonstrates our commitment to industry standards and innovation. As wide area networks evolve, enterprises can confidently partner with Spectrum Enterprise to guide them on their WAN journey and match the right SD-WAN design and access service to the client's specific network needs and at the client's preferred pace." (MEF PR, March 2020)

Tomi Airola, *Head of Business Networking, Telia Company*

“Telia is proud to be one of the first service providers to have successfully achieved the MEF 3.0 SD-WAN certification milestone. We view our MEF 3.0 certification as a key step in addressing the requirements of our enterprise customers. Certification is especially important for helping customers simplify the process of selecting a service provider that is committed to standardized global services. SD-WAN has become an essential part of Telia’s managed services portfolio to accelerate our customers’ digital transformation journey.” (MEF PR, March 2020)

Marten Scheffer, *Managing Executive for Enterprise Technology and FTTX, Vodacom Business*

“The MEF 3.0 certification underscores Vodacom Business’s commitment to being a technology and standards leader which improves the quality, management and interoperability of Ethernet and IP services for all our clients across the continent. The accolade highlights that indeed Vodacom Business offers best in class SD-WAN service offerings. (Vodacom Business PR, October 2020)

Jeremy Wubs, *SVP for Product, Marketing, and Professional Services, Bell Business Markets, Bell Canada*

“MEF’s done a fantastic job. It’s kind of why I was excited to join around the journey to SD-WAN – to help set and guide those standards….If you’re in the domain of setting and guiding the standards around SD-WAN, you have a responsibility, an obligation to make sure SD-WAN has a security posture and framework around it. You can’t go and drive the industry standards around SD-WAN and say, hey, good luck to everybody on security.” (MEF Infinite Edge Series – SASE, March 2021)

Jeremiah Ginn, *Software Defined Evangelist – Global Business – RMI, AT&T Business*

”Creating standardized abstract definitions for SASE-managed services offers an excellent opportunity for industry leaders to join this MEF effort, thereby growing the market, reducing market fragmentation, and enabling different stakeholders to maximize innovation in their respective areas of strength.” (MEF Guest Blog, June 2021)

Laurent Perrin, *Director, Application Driven Networks, Orange Business Services*

“Orange Business Services is very pleased to support the first MEF SD-WAN standard. Our customers are expecting agile and application driven network services and we believe that this new standard will facilitate the adoption and deployment of SD-WAN and meet their expectations. We look forward to working with MEF on ongoing initiatives to develop the interoperability of SD-WAN solutions and to define standardized APIs that will allow to integrate SD-WAN in a simplified and fully secured end-to-end orchestration model, from the end user to the applications.” (MEF PR, October 2018)

Michael Strople, *President & CEO, Allstream*

“Customers are embracing SD-WAN to improve network performance, obtain affordable and reliable connectivity to cloud applications, and gain greater visibility and control over network services. MEF’s SD-WAN service standardization will benefit all industry stakeholders by eliminating confusion regarding SD-WAN service components, core capabilities, and concepts. Standardization also will enable service and technology providers to focus on providing a core set of common capabilities and then building on that for differentiated offerings, helping ensure maximum flexibility for customers." (MEF PR, May 2019)

Technology Expert Perspectives

Nan Chen, *President, MEF*

"MEF has a proven track record of standardizing abstract constructs, attributes, and architectures for network services such as SD-WAN, Carrier Ethernet, Optical Transport, and IP. By achieving consensus on what a converged networking and security framework and associated SASE services should look like, MEF can empower technology and service providers to focus on providing a core set of common capabilities and then building their own innovative, differentiated offerings beyond those core features." (MEF PR, August 2020)

Pascal Menezes, *CTO, MEF*

"The SASE concept adjusts for a fundamental change in how enterprise users access business systems and the associated increased demand for lower-latency edge compute capabilities closer to the user. The well-defined and static network edge of the past is being replaced by more users working outside corporate walls and accessing business systems beyond corporate data centers. SASE shifts the focus from site-centric to user-centric security. The user can be anything (human, IoT, etc.) and anywhere, and security and network functions can be distributed away from the enterprise data center to maximize the availability of high performance edges (e.g. PoPs) and security clouds." (MEF PR, August 2020)

JL Valente*, VP, Product Management, Enterprise Routing and SD-WAN, Cisco*

"As businesses accelerate their digital initiatives and adoption of hybrid, multicloud network environments, SD-WAN continues to be the preferred choice for secure access and delivers the best user experience when connecting to cloud applications. To help fuel the growth of SD-WAN services, Cisco is supporting standards and certifications including MEF 3.0 to provide exceptional SD-WAN service capabilities, simplified integration, and peace of mind for optimized application experiences with guaranteed resiliency." (MEF PR, June 2021)

Sunil Khandekar, *Head of Nuage Networks from Nokia*

"Demand for SD-WAN is growing rapidly in all market segments and geographies, and there is strong momentum for it to be delivered as a managed service. The availability of the MEF 3.0 SD-WAN technology vendor certification is an important step in providing enterprises an industry benchmark for vendor selection and Nuage Networks from Nokia is proud to demonstrate its SD-WAN market leadership as a member of the first group to achieve this certification milestone." (MEF PR, January 2020)

Kumar Mehta, *Co-founder and CDO, Versa Networks*

"SD-WAN has become a key part of the managed services portfolio of service providers globally in order to accelerate their enterprise customers' digital transformation journey. With more than 60 percent of enterprises projected to deploy SD-WAN over the next two to four years, service providers needed to come together and establish standards, to help enterprises understand what they are buying and evaluate different solutions to accelerate services across automated networks. We congratulate MEF in taking a leadership role and are pleased to demonstrate our commitment to the standards by achieving MEF 3.0 SD-WAN certification." (MEF PR, January 2020)

Apurva Mehta, *Co-Founder and Chief Technology Officer, Versa Networks*

"MEF and its members continue to be at the forefront of driving industry standardization, collaboration, and innovation across leading technologies. Versa is excited to be participating in the MEF SASE initiative and sharing our expertise based on Versa SASE enabling businesses and organizations to deliver, enforce, and monitor networking and security in the cloud and on-premises for comprehensive security, application performance, multi-cloud connectivity, and consistent policy." (MEF PR, August 2020)

Jonathan Nguyen-Duy, *VP, Field CISO, Fortinet*

"Standards are fabulous because it allows consumers and enterprises to understand what is being offered and to judge and see what's best for them. I applaud the MEF efforts around that." (MEF Infinite Edge – SASE, March 2021)

Charles Eckel, *Principal Engineer, Global Technology Standards, Cisco; Co-Chair of MEF Test & Certification Committee*

"Standardization is really key to growing the market and accelerating the deployment of SASE services. (MEF Infinite Edge – SASE, March 2021)

Marc Cohn, *Head of Virtualization, Spirent*

"Spirent joins MEF in congratulating Comcast Business, PCCW Global, Spectrum Enterprise, and Telia Company in attaining the first MEF SD-WAN service certifications. By participating in the pilot, the four leading SD-WAN MSPs validated and enhanced the industry's first SD-WAN Certification Program, building upon the three initial pilot SD-WAN product certifications announced in January. We are proud to contribute as the neutral SD-WAN testing/validation/assurance authority." (MEF PR, March 2020)

Industry Analyst Perspectives

Rosemary Cochran, *Principal & Co-Founder, Vertical Systems Group*

"MEF 3.0 certifications are having a significant impact on the networking industry worldwide. Our research over many years has tracked the strong correlation between Carrier Ethernet market share leadership and compliance with MEF specifications. Now this trend is developing for Managed SD-WAN as market leading service providers and platform suppliers attain MEF 3.0 certification. Ultimately the advantages gained are competitive differentiation, services assurance for customers, and streamlined collaboration among industry players." (MEF PR, June 2021)

Mauricio Sanchez, *Research Director, Network Security and Data Center, Dell'Oro*

"While SASE is in its early days, I applaud the SASE standardization efforts that MEF has undertaken. In the near term, they are contributing vocabulary and aligning conceptual frameworks that are vital to getting the industry to rally behind common implementation approaches. In the long term, let us hope that the resulting standards help make multi-vendor SASE a reality and accelerate adoption.” (MEF Guest Blog, April 2021)

Ron Westfall, *Research Director and Senior Analyst, Futurum Research*

“Enterprises are swiftly expanding their digital workforces, increasing the number of users, devices, and services touching their network. As a result, the attack surfaces of their networks are enlarged, increasing exposure to malicious attacks across cloud and on-prem environments. Service providers’ ability to offer secure enterprise connectivity services is essential to boosting the value of their evolving cloud-based offerings. There are many SASE attributes that, once standardized on the basis of MEF SASE Services, will create a strong foundation to deliver innovative security services and solutions that enterprises will value in meeting their unified network and security business objectives.” (MEF PR, August 2020)

Jennifer Clark, *Principal Analyst, Heavy Reading*

“The momentum of SD-WAN adoption, along with the large and ever-growing community of players in the SD-WAN ecosystem – vendors, service providers and enterprises – has created an information vacuum in terms of how we deploy SD-WAN over multiple underlay connectivity services and across multiple service provider networks. The MEF SD-WAN standard is the first step to addressing this vacuum with a common language by which we can define SD-WAN services and service attributes. This and the MEF follow-on SD-WAN standards are the building blocks leading to a MEF SD-WAN certification process, which enterprise SD-WAN customers will need as they evaluate and deploy SD-WAN services.” (MEF PR, August 2019)

Greg Bryan, *Senior Manager, Enterprise Research, TeleGeography*

"Our WAN Manager Survey indicates that in 2018 fewer than 1/5th of enterprises had already installed SD-WAN and 1/3 were still researching their SD-WAN options. With dozens of potential suppliers to choose from – from technology start-ups to large SD-WAN managed service providers – WAN managers will benefit from the standards MEF has worked to create in this space." (MEF PR, May 2019)

MEF

MEF SASE Certification
March 2025, FAQ v1