ETSI GS ENI 002 V3.2.1 (2023-04)

Experiential Networked Intelligence (ENI); ENI requirements

Disclaimer

The present document has been produced and approved by the Experiential Networked Intelligence (ENI) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
RGS/ENI-002v321_Requirements

Keywords
artificial intelligence, management, network, requirements

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Experiential Networked Intelligence (ENI).

Modal verbs terminology

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

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

1 Scope

The present document specifies the requirements of how intelligence is applied to the network and applications in different scenarios to improve experience of service provision and network operation. Also, how intelligence enables dynamic autonomous behaviour and adaptive policy driven operation in a changing context. The ENI requirements are based on the ENI use case document and identified requirements from other SDOs. These requirements will form the base for the architecture design work.

In Release 3 the present document that is a specification will add:

- Requirements derived from API descriptions.
- Requirements derived from System Architecture.
- Requirements derived from new use cases.

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] ETSI GS ENI 001: "Experiential Networked Intelligence (ENI); ENI use cases".

[2] ETSI GS ENI 005: "Experiential Networked Intelligence (ENI); System Architecture".

[3] ETSI TS 102 165-1 (V5.2.5): "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[4] ETSI GS NFV 006 (V4.4.1): "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Architectural Framework Specification".

[5] ETSI TS 101 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

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 GR ENI 004: "Experiential Networked Intelligence (ENI); Terminology for Main Concepts in ENI".

[i.2] Service Operations Specification MEF 55: "Lifecycle Service Orchestration (LSO): Reference Architecture and Framework".

[i.3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR ENI 004 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

AI	Artificial Intelligence
API	Application Programming Interface
BP	Back Propagation
BSS	Business Support System
CAP	Context Aware related Policy
CAPEX	CAPital EXpenditure
DC	Data Collection

NOTE: Used in the context of servers.

DCA	Data Collection and Analysis
DSL	Domain-Specific Language
EMS	Element Management System
ENI	Experiential Networked Intelligence
GDPR	General Data Protection Regulation
GPM	General Policy Management
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
LI	Lawful Interception
LLC	Last Level Cache
LSO	Lifecycle Service Orchestration
LSO RA	Lifecycle Service Orchestration - Reference Architecture
MANO	MANagement and Orchestration
MEC	Multi-access Edge Computing
MEF	Metro Ethernet Forum
MOP	Mode Of Operations
NFV	Network Functions Virtualisation
NM	Network Model
NPD	Network Planning & Deployment
OPEX	OPerational EXpenditure
OR	Operational Requirements
OSS	Operational Support System
PINet	Polymorphic Network
PR	Performance Requirements
RA	Reference Architecture

RR	Resilience and Reliability
SDN	Software Defined Networking
SLA	Service Level Agreement
SOM	Service Orchestration and Management
SP	Security and Privacy
SP.2A	Security and Privacy 2A
SP.2B	Security and Privacy 2B
SVM	Support Vector Machine
TCO	Total Cost of Ownership
TVRA	Threat, Vulnerability and Risk Analysis
VNF	Virtualised Network Function

4 Introduction

4.1 Categorization of the requirements

The present document structure addresses the requirements in the following areas:

1) Service and network requirements:
   - General requirements
   - Service orchestration and management
   - Network planning and deployment
   - Network optimization
   - Resilience and reliability
   - Security and privacy
2) Functional requirements:
   - Data collection and analysis
   - Policy management
   - Data learning
   - Interworking with other systems
   - Mode of operations
   - Model training and iterative optimization
   - Mode of deployments
   - API requirements
3) Non-functional requirements:
   - Performance requirements
   - Operational requirements
   - Regulatory requirements

5 Service and network requirements

5.1 Overview

The requirements in this clause are addressed from service and network point of view and are derived directly from the related use cases.

5.2 General requirements

This clause captures the requirements that are general and independent from other requirements categorized in other specific clauses.

[GR.1] The ENI System shall use history data, context, and decisions taken to learn, process and provide responses to events, whether generated from devices or from management systems.

[GR.2] The ENI System shall use context information as part of the computations that result in recommendations, advisement, predictions, and decisions that are used to assist other network systems, e.g. orchestration and management systems.

NOTE: As an example, MANO (from ETSI GS NFV 006 [4]) or the LSO RA (from MEF [i.2]) are different types of orchestration and management systems.

[GR.3] The ENI architecture shall be flexible enough to support extensibility.

5.3 Service orchestration and management

This clause captures requirements related to the ENI System service provisioning, e.g. how to compile the service intent and orchestrate the service atoms and workflows, as well as automatic service on boarding.

[SOM.1] The ENI System shall invoke policies based on models that describe and/or define traffic behaviour, such as SLAs (e.g. past or current telemetry).

[SOM.2] The ENI System shall support the closed loop control model when different orchestration and management systems are used.

NOTE 1: As an example, MANO (from ETSI GS NFV 006 [4]) and LSO RA (from MEF [i.2]) are different types of orchestration and management systems.

[SOM.3] The ENI System should not directly manage, control or orchestrate physical or virtual entities, either at the infrastructure level or service level.

NOTE 2: ENI System may interact with the Orchestration system, EMS or OSS/BSS to influence the state of the resources or services.

5.4 Network planning and deployment

This clause captures requirements related to network planning and deployment, e.g. how to allocate network resources to VNFs, or automatic VNF on boarding.

NOTE 1: The network resources that can be managed are not limited to the requirements addressed in this clause.

[NPD.1] The ENI System shall recommend allocation or retrieval of network resources, e.g. virtual machines, bandwidth, IPv4 addresses and IPv6 prefixes to end users or service flows, in an intelligent way to improve the efficiency of resource utilization. This ENI System function may be implemented in a centralized and/or distributed manner, according to what is defined in ETSI GR ENI 004 [i.1] and according to ETSI GS ENI 005 [2].

[NPD.2] The ENI System shall assist the network equipment or network function to use the resource pools that are used for resource allocation (e.g. virtual machines, network bandwidth, IP addresses, CPU cores, CPU frequencies, memory, memory bandwidth), in an intelligent way in order to improve the efficiency of resource utilization and user experiences.

[NPD.3] The ENI System should dynamically and intelligently compute and recommend the required network resources, including both IPv4 and IPv6 resources as well as other resources.

[NPD.4] The ENI System shall compute the network resources required to dynamically and intelligently deploy a given network service efficiently.

[NPD.5] IT resources to enable network services shall be managed within the ENI System.

NOTE 2: Similar capabilities within the data centre are outside the network scope of this phase of ENI.

[NPD.6] The ENI System shall be capable of understanding the context that a set of devices is operating within.

[NPD.7] The ENI System shall be capable of performing the proper planning and deployment of resources to ensure that applicable deployed policies are not violated.

[NPD.8] The ENI System shall identify different types of rollouts for different types of resources that lead to the upgrade of virtualised software-based resources.

[NPD.9] The ENI System shall, in an efficient and dynamic manner, combine network slices, slice/service prioritization and resource allocation concepts, e.g. in order to resolve resource allocation conflicts between competing network slices deployed on top of a shared infrastructure.

[NPD.10] The ENI System shall support cross-domain and global resource management, e.g. cross-domain node content resource aggregation and integration, as well as cross-domain permissions management of unified user identity.

5.5 Network optimization

This clause captures requirements related to network optimization, e.g. how to adjust the network configurations to improve its efficiency and performance, as well as the user experience of the service.

[NO.1] The ENI System shall collect and process the necessary data according to specific algorithms in order to achieve network optimization.

NOTE 1: Data collection and processing algorithms for systems will be specified in the functional architecture.

[NO.2] The ENI System shall meet or exceed all performance requirements when improving the target performance.

[NO.3] The ENI System shall support central optimization, local optimization and distributed joint optimization, according to what is defined in ETSI GR ENI 004 [i.1].

[NO.4] The ENI System shall support an adaptive optimization process where changes in the environment are reflected in the results of the optimization.

[NO.5] The ENI System shall use prioritization and other scheduling and traffic shaping techniques to prevent SLA violations related with priority services.

[NO.6] The ENI System shall use AI (e.g. Machine Learning) to identify traffic type and support traffic handling and QoS assurance for specific type of traffic.

[NO.7] The ENI System shall support traffic type identification in different granularity levels, including application types, action types (e.g. sending pictures, voice calls, etc.).

[NO.8] The ENI System shall support dynamic policy adjustment, i.e. to select or re-select and enforce a policy dynamically, for a specific flow based on traffic identification results.

NOTE 2: Applying policies to specific flows may lead to hundreds of thousands of policies.

5.6 Resilience and reliability

This clause captures requirements related to resilience and reliability of the network, including fault diagnosis and prediction, high availability and back up, conflict detection, and rolling back to previous policies and status.

[RR.1] The ENI System shall intelligently recommend allocation or retrieval of IP addresses without causing route oscillation.

[RR.2] The ENI System shall intelligently recommend allocation or retrieval of IP addresses without causing any interruption in the offered services.

[RR.3] The ENI System shall support root cause analysis to diagnose existent faults and potential faults caused by new cases, according to what is defined in ETSI GS ENI 005 [2].

[RR.4] The ENI System shall support the use of one or more AI algorithms to perform network service fault prediction.

[RR.5] The ENI System shall learn and predict the pattern of resource requirements of services.

[RR.6] When optimization of energy consumption is required, which implies a switch of servers, the ENI System shall trigger the reallocation of services to appropriate resources in another server.

[RR.7] The ENI System shall wake up an appropriate number of servers in time to meet the growing resource needs required by services, after learning and predicting the pattern of resource requirement of those services.

[RR.8] The ENI System shall provide the operators with the ability to define services that are critical or prioritized.

[RR.9] The ENI System shall allow the on-going services in a server to be moved from this server to another without interruption, e.g. during reallocation for energy saving purposes.

[RR.10] The ENI System shall not interrupt the on-going services on the target servers, e.g. when reallocation of services from other servers takes place for energy saving purposes.

[RR.11] Energy saving need not be the only criterion for moving a service.

[RR.12] The ENI System shall calculate and propose proper backup actions to the operators in order to prevent or to mitigate a service degradation or disruption when a planned operation occurs.

[RR.13] The ENI System shall support the use of one or more intelligent methods to perform network anomaly (fault, error and unusual behaviour) prediction and prevention.

[RR.14] The ENI System shall be aware of the impact of adjustment on services and guarantee seamless adjustment of network slice and high valued services.

5.7 Security and privacy

This clause captures requirements related to security and privacy issues (e.g. it is recommended that data collection shall be captured in a secure way and not add more security risks). In addition, it is recommended that the collected data shall be accessible by authorized accounts, and that the privacy of both subscribers and operators are protected.

The requirements indicated in the present document have been derived from application of the ETSI TVRA method defined in ETSI TS 102 165-1 [3], the details of the analysis leading to the requirements have been examined with respect to the use cases defined in ETSI GS ENI 001 [1] and with respect to the terminology defined in ETSI GR ENI 004 [i.1].

[SP.1] The ENI System shall use AI (e.g. Machine Learning) to detect abnormal traffic patterns that can lead to service disruptions or security threats as well as to carry out the identification of abnormally operating devices.

[SP.2] The ENI System shall provide means to detect a corrupted device.

[SP.2A] The ENI System shall provide means to identify a corrupted device.