



**Core Network and Interoperability Testing (INT);
Artificial Intelligence (AI);
End-to-End Autonomic Security Management and Control in
Multi-Domain 5G Networks**

get full document from standards.iteh.ai

Reference

DTR/INT-00900

Keywords

5G, autonomic networking, cyber security, security,
security by default, self-management

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

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.

By way of exception and when the document is a normative deliverable (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)), ETSI authorizes to reproduce and incorporate into products, services and technical documentation only those extracts (e.g. templates) that are strictly necessary for the technical implementation of the normative deliverable, to ensure compliance with the latter. Nothing in this notice shall be construed as limiting any mandatory exceptions to copyright provided by applicable law.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	4
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	10
3.1 Terms.....	10
3.2 Symbols.....	11
3.3 Abbreviations	11
4 GANA 5G self-adaptive security management and control.....	13
4.1 Autonomic Security Management and Control (ASMC)	13
4.2 Security Requirements for GANA AMC	19
4.3 Security Testing of Components for GANA AMC and their Services.....	19
4.4 Drivers of ASMC for SECurity as a Service (SECaaS) in 5G	20
4.4.1 Overview	20
4.4.2 Drivers for Differentiated Security: SECaaS by Default for 5G Telcos	20
4.4.3 Autonomic SECaaS Assurance for Differentiated Security SLAs for 5G Slices.....	22
4.4.4 Summary of Core Principles, Design, and Commonalities towards Standardization and Harmonization	22
4.5 Multi-Domain Federated GANA KPs for E2E ASMC for 5G Slices	23
4.5.1 Overview	23
4.5.2 Security Challenge of 5G slice for ASMC	24
4.5.3 Integration of the GANA KP Platform for 5G Core Network with MDAS and NWDAF	28
4.5.4 Real-Time Security federated Threats Repository	29
4.5.5 E2E ASMC across Multiple Domains	31
4.5.6 ASMC.....	32
4.6 Security-DEs Orchestrations	34
4.7 Programmability of security attacks detection and threats/risks predictions.....	37
4.8 "Self-Protection" and "Self-Defending " 5G E2E ASMC	40
4.9 Summary	41
4.10 Other Autonomics Use Cases.....	43
5 Zero Trust Principles and Smart Contracts to GANA KPs Platforms Federations.....	47
6 Quantum Cybersecurity use cases in 5G and Verticals.....	48
7 Telco Data space in ASMC Applications.....	49
8 ASMC in Open RAN	50
9 NGMN ODiN Requirements call for Security Frameworks and Solutions suitable for ASMC Assurance in E2E Disaggregated Networks.....	52
10 GANA in ETSI 5G PoC Implementations executed by the Industry	53
11 Conclusion and Further Work	55
Annex A: Bibliography	56
Annex B: Change history	57
History	58

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) 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 IPR online database](#).

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™**, **LTE™** and **5G™** logo 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 Technical Report (TR) has been produced by ETSI Technical Committee Core Network and Interoperability Testing (INT).

Modal verbs terminology

In the present document "**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.

Introduction

The present document introduces a Generic Autonomic Network Architecture (GANA) framework for achieving End-to-End Artificial Intelligence (AI)-powered Autonomic Security Management and Control (ASMC) across multi-domain 5G networks. It explains the role of AI models in the management and control operations of 5G networks, particularly in the context of Autonomic Management and Control (AMC) systems.

The present document presents an instantiation of the GANA reference model (framework), i.e. the application of the generic model (GANA) onto an implementation-oriented architecture and its use of AI algorithms to drive self-security operations in networks. It also highlights the need for E2E Autonomic (closed-loop) Service and Security Assurance through the federation of GANA Knowledge Plane (KP) platforms.

The present document references ETSI specifications and ongoing Proof-of-Concept (PoC) programs on "5G network slices creation, AMC and E2E Orchestration, with Closed-Loop (Autonomic)". It emphasizes the importance of a standardized GANA Framework for implementing AMC systems in the industry. The present document further elaborates on the capabilities and aspects covered in the 5G PoC White Paper No.6, including the use of AI models for AMC, security analytics, security functions placement/orchestration, and programmability requirements for self security management DE.

It encourages readers to refer to the complementary White Papers of the ETSI 5G PoC for more information and invites interested parties to join the PoC Consortium.

Sample Document

get full document from standards.iteh.ai

1 Scope

The present document provides a Framework that serves as an Implementation Guide for interoperable solutions that are aimed at addressing 5G security challenges. This is in reference to security challenges that should be addressed through the use of the following methods:

- 1) automated orchestration of security mechanisms and services that can be used for 5G network slices, network segments and services delivered by the End-to-End (E2E) network;
- 2) automated security policy computation and dynamic security policy enforcement in various points in the network infrastructure using GANA autonomics (closed control-loops) in response to new 5G slice and service instantiations, new intents and security SLAs supplied as inputs by the human network operator and/or in response to detected and predicted security attacks, threats and risks.

The Framework enables to implement solutions for "self-protection" and "self-defence" autonomic behaviours by 5G networks and their associated management and control systems without need for human operator involvement in the decisions and actions against detected and predicted security attacks, threats and risks - even across multiple 5G network operators by use of cross domain federated GANA KP platforms.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

- [i.1] [ETSI White Paper No.16 GANA](#): "Generic Autonomic Networking Architecture Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services".
- [i.2] [ETSI TS 103 195-2 \(V1.1.1\)](#): "Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management".
- [i.3] [White Paper No.1 of the ETSI 5G PoC](#): "C-SON Evolution for 5G, Hybrid SON Mappings to the ETSI GANA Model, and achieving E2E Autonomic (Closed-Loop) Service Assurance for 5G Network Slices by Cross-Domain Federated GANA Knowledge Planes".
- [i.4] [ETSI TR 103 473 \(V1.1.2\)](#): "Evolution of management towards Autonomic Future Internet (AFI); Autonomicity and Self-Management in the Broadband Forum (BBF) Architectures".
- [i.5] ETSI TR 103 404: "Network Technologies (NTECH); Autonomic network engineering for the self-managing Future Internet (AFI); Autonomicity and Self-Management in the Backhaul and Core network parts of the 3GPP Architecture".

- [i.6] [White Paper No.3 of the ETSI 5G PoC](#): "Programmable Traffic Monitoring Fabrics that enable On-Demand Monitoring and Feeding of Knowledge into the ETSI GANA Knowledge Plane for Autonomic Service Assurance of 5G Network Slices; and Orchestrated Service Monitoring in NFV/Clouds".
- [i.7] [White Paper No.2 of the ETSI 5G PoC](#): "ONAP Mappings to the ETSI GANA Model; Using ONAP Components to Implement GANA Knowledge Planes and Advancing ONAP for Implementing ETSI GANA Standard's Requirements; and C-SON - ONAP Architecture".
- [i.8] ETSI TC INT AFI WG 5G POC: "[Report on Specifications of Integration APIs for the ETSI GANA Knowledge Plane Platform with Other Types of Management and Control Systems, and with Info/Data/Event Sources in general](#)".
- [i.9] ETSI TS 128 533 (V15.0.0): "5G; Management and orchestration; Architecture framework (3GPP TS 28.533 version 15.0.0 Release 15)".
- [i.10] NGMN: "[5G End-to-End Architecture Framework v3.0.8](#)".
- [i.11] [White Paper No.4 of the ETSI 5G PoC](#): "ETSI GANA as Multi-Layer Artificial Intelligence (AI) Framework for Implementing AI Models for Autonomic Management and Control (AMC) of Networks and Services; and Intent-Based Networking (IBN) via GANA Knowledge Planes (KPs)".
- [i.12] [White Paper No.6 of the ETSI 5G PoC](#): "Generic Framework for Multi-Domain Federated ETSI GANA Knowledge Planes (KPs) for End-to-End Autonomic (Closed-Loop) Security Management and Control for 5G Slices, Networks/Services".
- [i.13] 5G security recommendations: "Package #2: Network Slicing", by NGMN Alliance, 27 April 2016.
- [i.14] ODA TM Forum's Open Digital Architecture (ODA): "IG1167 ODA Functional Architecture Vision R18.0.0 (Intelligence Management Function Block)".
- [i.15] 5G security - Package 3: "Mobile Edge Computing / Low Latency / Consistent User Experience", NGMN Alliance: 20 February 2018, by NGMN 5G security group.
- [i.16] ODA TM Forum's Open Digital Architecture (ODA): "IG1177 ODA Intelligence Management Implementation Guide R18.5.0", IG1177 Release 18.5, December 2018.
- [i.17] James Crawshaw: "Network Automation Roadmap: Where to Start and What to Aim for, A Heavy Reading white paper produced for Juniper Networks Inc".
- [i.18] Cabaj K., Szczypiorski K., Becker S. (2010): "Towards Self-defending Mechanisms Using Data Mining in the EFIPSANS Framework", In: Nguyen N.T., Zgrzywa A., Czyżewski A. (eds) Advances in Multimedia and Network Information System Technologies. Advances in Intelligent and Soft Computing, vol 80. Springer, Berlin, Heidelberg: DOI: 10.1007/978-3-642-14989-4_14.
- [i.19] Alberto Huertas, Manuel Gil Pérez, Félix J. García Clemente, Gregorio Martinez Perez: "Towards the autonomous provision of self-protection capabilities in 5G networks", December 2019, Journal of Ambient Intelligence and Humanized Computing 10(12):4707-4720; DOI: 10.1007/s12652-018-0848-6.
- [i.20] Manuel Gil Perez, et al: "Self-Organizing Capabilities in 5G Networks: NFV and SDN Coordination in a Complex Use Case", EuCNC 2018-3rd Network Management Workshop for 5G Networks, June 2018.
- [i.21] Ashutosh Dutta, Ph.D.: "Conference Slides: Security in SDN/NFV and 5G Networks Opportunities and Challenges", Chair, IEEE™ Future Network Initiative, 05/06/2019.
- [i.22] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov: "5G Security: Analysis of Threats and Solutions", In 2017 IEEE™ Conference on Standards for Communications and Networking (CSCN): DOI: 10.1109/CSCN.2017.8088621.
- [i.23] Palo Alto Networks White Paper: "5G SECURITY: Establishing a Holistic Approach to Paving the 5G Evolution", 2018.

- [i.24] Falko Dressler, Gerhard Münz, Georg Carle: "Attack detection using cooperating autonomous detection systems (CATS)", Proceedings of 1st IFIP International Workshop on Autonomic Communication, Poster Session, Berlin, Germany, October 2004.
- [i.25] Anastasios Zafeiropoulos, Athanassios Liakopoulos, Alan Davy, Ranganai Chaparadza: "Monitoring within an Autonomic Network: A GANA Based Network Monitoring Framework: Conference: Service-Oriented Computing", ICSOC/ServiceWave 2009 Workshops - International Workshops, ICSOC/ServiceWave 2009, Stockholm, Sweden, November 23-27, 2009, Revised Selected Papers: DOI: 10.1007/978-3-642-16132-2_29.
- [i.26] [On Using sFlow for Security Attacks detection.](#)
- [i.27] Flowmon® White Paper: "Whitepaper - Flow for Security: IP flow based detection of cyber threats", and online article: ["Network Anomaly Detection and Network Behavior Analysis"](#).
- [i.28] Anna Sperotto: "PhD Thesis: Flow-Based Intrusion Detection", 2010.
- [i.29] Anna Sperotto, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras and Burkhard Stiller: "An Overview of IP Flow-Based Intrusion Detection", IEEE™ Communications Surveys and Tutorials, Vol. 12, No. 3, Third Quarter 2010.
- [i.30] Jordan Lam, Robert Abbas: ["Machine Learning based Anomaly Detection for 5G Networks"](#), March 2020.
- [i.31] Jiaqi Li, Zhao Zhifeng, Rongpeng Li: "A Machine Learning Based Intrusion Detection System for Software Defined 5G Network", DOI: 10.1049/iet-net.2017.0212.
- [i.32] European Union Agency for Network and Information Security (ENISA): "ENISA Threat Landscape for 5G Networks: Threat assessment for the fifth generation of mobile telecommunications networks (5G)", November 2019.
- [i.33] White Paper by Huawei: ["Partnering with the Industry for 5G Security Assurance"](#).
- [i.34] GSMA™: ["AI in Network Use Cases in China"](#), October 2019.
- [i.35] Andrea Peiro, CUJO AI: "Securing 5G Networks With Deep Learning-Based Threat Detection Systems", by Blogs and Opinions 6/10/2019.
- [i.36] ETSI TS 129 520 (V15.0.0): "5G; 5G System; Network Data Analytics Services; Stage 3 (3GPP TS 29.520 version 15.0.0 Release 15)".
- [i.37] White Paper by Huawei: "AI Security White Paper", 2018.
- [i.38] Kelsey Ziser, Jim Hodges, Gordon Mansfield, Christina Ashraf: "5G Exchange", eBook: Innovation at the Speed of 5G.
- [i.39] Jim Hodges: "Implementing 5G Security: Priorities and Preferences: A Heavy Reading white paper produced for F5 Networks", Heavy Reading White Paper, 2019, Fortinet, NetNumber, and Palo Alto Networks.
- [i.40] Verizon White Paper: "Network Threat Advanced Analytics", 2016.
- [i.41] ETSI TS 123 288: "5G; Architecture enhancements for 5G System (5GS) to support network data analytics services (3GPP TS 23.288 version 19.6.0 Release 19)".
- [i.42] RCR Wireless News: "How to develop 5G security standards at a global scale", online article.
- [i.43] Emmanouil Pateromichelakis, et al: "End-to-End Data Analytics Framework for 5G Architecture", In IEEE™ Access Online Special Section on Roadmap to 5G: Rising to the Challenge, Volume 7, 2019.
- [i.44] [White Paper No.5 of the ETSI 5G PoC](#): "Artificial Intelligence (AI) in Test Systems, Testing AI Models and ETSI GANA Model's Cognitive Decision Elements (DEs) via a Generic Test Framework for Testing GANA Multi-Layer Autonomics and their AI Algorithms for Closed-Loop Network Automation".

- [i.45] [3GPP SA3 - Security](#).
- [i.46] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification".
- [i.47] ETSI GS NFV-REL 004: "Network Functions Virtualisation (NFV); Assurance; Report on Active Monitoring and Failure Detection".
- [i.48] ETSI TC INT / AFI WG 5G PoC BrightTalk Webinar: "[End-to-End Autonomic Closed-Loop Security Management and Control for 5G Networks](#)".
- [i.49] NGMN: "[ODiN -Operating Disaggregated Networks](#)", Project V 2.0, 20.09.2022.
- [i.50] TM Forum Telco Data Space Initiative: "[Promoting a trusted telco data space to drive new opportunities](#)", supported by Catalysts Projects.
- [i.51] Gaia-X European Association for Data and Cloud: "[Gaia-X Architecture Document](#)".
- [i.52] IEEE™ Industry Newsletter: "The Road to European Digital Sovereignty with GAIA-X and IDSA", Arnaud Braud, Gaël Fromentoux, Benoit Radier and Olivier Le Grand, Orange Labs, France - March issue.
- [i.53] Fraunhofer: "[Reference architecture model for the Industrial Data Space](#)". IDSA International Data Spaces Association.
- [i.54] IDSA: "Reference Architecture Model", Version 3.0, April 2019.
- [i.55] ENISA Threat Landscape for 5G Networks: "Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)", December 2020.
- [i.56] Allan Edgard Silva Freitas: "[On Design Autonomic Behavior for Blockchain platforms](#)", LADC '23, Proceedings of the 12th Latin-American Symposium on Dependable and Secure Computing, October 2023, pp. 166-167.
- [i.57] Fariba Ghaffari, Komal Gilani, Emmanuel Bertin, Noel Crespi: "Identity and access management using distributed ledger technology: a survey", International Journal of Network Management, 2022, 32(2), pp.e 2180. DOI: 10.1002/nem.2180.hal-03315497.
- [i.58] NIS Cooperation Group: "Report on the cybersecurity of Open RAN", 11 May 2022, Report produced jointly by EU Member States, with the support of the European Commission and the EU Agency for Cybersecurity (ENISA) on a concerted approach to the cybersecurity of 5G networks.
- [i.59] National Telecommunications and Information Administration (NTIA): "[Open RAN Security Report](#)", Outcome from Quad Critical and Emerging Technology Working Group, May 2023.
- [i.60] Madhusanka Liyanage, An Braeken, Shahriar Shahabuddin, Pasika Ranaweera: "[Open RAN security: Challenges and opportunities](#)", Journal of Network and Computer Applications, Volume 214, 2023, 103621, ISSN 1084-8045.
- [i.61] R. B. Bohn et al.: "[NIST Multi-Domain Knowledge Planes for Service Federation for 5G & Beyond Public Working Group: Applications to Federated Autonomic/Autonomous Networking](#)", 2023 IEEE™ Future Networks World Forum (FNWF), Baltimore, MD, USA, 2023, pp. 1-6, doi: 10.1109/FNWF58287.2023.10520595.
- [i.62] Pastor-Galindo J., López-Millán G., Marín-López R., et al.: "[A Framework for Dynamic Configuration of TLS Connections Based on Standards](#)", J Netw Syst Manage 30, 24 (2022).
- [i.63] ENISA: "Security in 5G Specifications: Controls in 3GPP Security Specifications (5G SA)", February 2021.
- [i.64] [NIST Special Publication 800-207](#): "Zero Trust Architecture".
- [i.65] H. A. Kholidy et al.: "Toward Zero Trust Security in 5G Open Architecture Network Slices", MILCOM 2022 - 2022 IEEE™ Military Communications Conference (MILCOM), Rockville, MD, USA, 2022, pp. 577-582, doi: 10.1109/MILCOM55135.2022.10017474.

- [i.66] H. A. Kholidy, A. Karam, J. L. Sidoran and M. A. Rahman: "5G Core Security in Edge Networks: A Vulnerability Assessment Approach", 2021 IEEE™ Symposium on Computers and Communications (ISCC), Athens, Greece, 2021, pp. 1-6, doi: 10.1109/ISCC53001.2021.9631531.
- [i.67] H. A. Kholidy and R. Kamaludeen: "An Innovative Hashgraph-based Federated Learning Approach for Multi Domain 5G Network Protection", 2022 IEEE™ Future Networks World Forum (FNWF), Montreal, QC, Canada, 2022, pp. 139-146, doi: 10.1109/FNWF55208.2022.00033.
- [i.68] H. A. Kholidy, A. Karam, J. H. Reed and Y. Elazzazi: "An Experimental 5G Testbed for Secure Network Slicing Evaluation", 2022 IEEE™ Future Networks World Forum (FNWF), Montreal, QC, Canada, 2022, pp. 131-138, doi: 10.1109/FNWF55208.2022.00032.
- [i.69] Suriya M.: "[Machine learning and quantum computing for 5G/6G communication networks - A survey](#)", International Journal of Intelligent Networks, Volume 3, 2022, pp. 197-203, ISSN 2666-6030, DOI: 10.1016/j.ijin.2022.11.004.
- [i.70] Draft new Recommendation ITU-T Y.3819: "Quantum key distribution network - Requirements and architectural model for autonomic management and control".
- [i.71] [ETSI TS 103 744 \(V1.2.1\)](#): "CYBER; Quantum-Safe Cryptography (QSC); Quantum-safe Hybrid Key Establishment".
- [i.72] ETSI TS 104 015 (V1.1.1): "Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies".
- [i.73] ETSI TR 103 616 (V1.1.1): "CYBER; Quantum-Safe Signatures".
- [i.74] ETSI TR 103 617 (V1.1.1): "Quantum-Safe Virtual Private Networks".
- [i.75] ETSI TR 103 618 (V1.1.1): "CYBER; Quantum-Safe Identity-Based Encryption".
- [i.76] ETSI TR 103 619 (V1.1.1): "CYBER; Migration strategies and recommendations to Quantum Safe schemes".
- [i.77] ETSI TR 103 692 (V1.1.1): "CYBER; State management for stateful authentication mechanisms".
- [i.78] ETSI TR 103 747 (V1.1.1): "Core Network and Interoperability Testing (INT/ WG AFI); Federated GANA Knowledge Planes (KPs) for Multi-Domain Autonomic Management and Control (AMC) of Slices in the NGMN(R) 5G End-to-End Architecture Framework".
- [i.79] ETSI TR 103 823: "CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation".
- [i.80] ETSI TR 103 949: "Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS migration study".
- [i.81] ETSI TR 103 966: "CYBER Security (CYBER); Quantum-Safe Cryptography (QSC); Deployment Considerations for Hybrid Schemes".
- [i.82] ETSI TR 103 965: "CYBER; Quantum-Safe Cryptography (QSC); Impact of Quantum Computing on Cryptographic Security Proofs".
- [i.83] ETSI TR 103 967: "Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Impact of Quantum Computing on Symmetric Cryptography".
- [i.84] ETSI TR 103 195-1: "Core Network and Interoperability Testing (INT/ WG AFI); Generic Autonomic Network Architecture; Part 1: Business drivers for autonomic networking".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP	3 rd Generation Partnership Project
6G	6 th Generation
AF	Application Function
AFI	Autonomic Future Internet
AI	Artificial Intelligence
AMC	Autonomic cognitive Management and Control
AMF	Access and Mobility Management Function
AN	Autonomous Network
API	Application Programming Interface
AS	Application Server
ASMC	Autonomic Security Management and Control
BB	Building Block
CEP	Complex Event Processing
C-SON	Centralized Self Organizing Network
CSP	Communications Service Provider
CUPS	Control and User Plane Separation
CYBER	Cyber Security
DC	Data Center
dDE	distributed DE
DDoS	Distributed Denial of Service
DE	Decision making Element
DL	Deep Learning
DoS	Denial of Service
D-SON	Distributed SON
DT	Domain Type
E2E	End-to-End
eMBB	enhanced Mobile Broadband
EMM	EPS Mobility Management
ENISA	European Union Agency for Network and Information Security
EPS	Edge Packet Service
ESM	EPS Session Management
FM	Fault-Management
F-MBTS	Federation - "Model Based Translation Service"
FW	Firewall
GAN	Generic Autonomic Network Architecture
gNB	next generation Node Base station
GS	Group Specification
H-SON	Hybrid SON
HSS	Home Subscriber Server
IAM	Identity and Access Management
IBN	Intent-Based Networking
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IDSA	International Data Spaces Association
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISG	Industry Specification Group
ISV	Independent Software Vendor
IT	Information Technology
ITS	Intelligent Transport Systems
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector

KP	Knowledge Plane
KP DE	Knowledge Plane Decision-making Element
KPI	Key Performance Indicator
LCM	Lifecycle Management
MANO	Management and Orchestration
MAPE-K	Monitor-Analyse-Plan-Execute over a shared Knowledge
MBTS	Model-Based Translation Service
MDAS	Management Data Analytics Service
MDKP	Multi-Domain Knowledge Plane
ME	Managed Entity
MEC	Mobile Edge Computing
ML	Machine Learning
MNO	Mobile Network Operator
NAS	Non Access Stratum
NE	Network Element
NEF	Network Exposure Function
NF	Network Function
NFV	Network Function Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
NFVO	NFV Orchestrator
NGMN	Next Generation Mobile Networks
NIST	National Institute of Standards and Technology (US)
NRF	Network Repository Function
NWDAF	Network Data Analytics Function
OBB	Out-Of-Band
O-CU	Open RAN-Centralized Unit
ODA	Open Digital Architecture
ODiN	Operating Disaggregated Networks
O-DU	Open RAN-Distributed Unit
ONAP	Open Network Automation Platform
ONIX	Overlay Network for Information eXchange
OoB	Out-Of-Band
O-RAN	Open Radio Access Network
O-RU	Open RAN-Radio Unit
OS	Operating System
OSS	Operations Support Systems
OTT	Over The Top
PCF	Policy Control Function
PM	Performance Management
PNF	Physical Network Function
PRINS	Protocol for (roaming security reference point) N32 Interconnect Security
PWG	Public Working Group
QF	QoS Function
QKD	Quantum Key Distribution
QoS	Quality of Service
QSC	Quantum Safe Cryptography
R&D	Research and development
RAN	Radio Access Network
REL	Reliability
RIC	RAN Intelligence Controller
SBA	Service Based Architecture
SDN	Software Defined Networks
SDO	Standards Development Organizations
SEC	Security
SECaaS	SECurity-as-a-Service
SF	Security Function
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SMF	Session Management Function
SON	Self Organizing Networks
SPAN	Switched Port Analyser
SSL	Secure Sockets Layer

TAP	Test Access Point
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TM	TeleManagement
TR	Technical Report
TS	Technical Specification
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function
VNF	Virtual Network Function
VPN	Virtual Private Network
WG	Working Group
ZTP	Zero Trust Principle

4 GANA 5G self-adaptive security management and control

4.1 Autonomic Security Management and Control (ASMC)

ETSI TS 103 195-2 [i.2], described the autonomics principles and enablers for Autonomic cognitive Management and Control (AMC) and Autonomous Networks (AN) paradigm instantiated in the 5G architectures in ETSI TR 103 747 [i.78]. AMC paradigm helps to achieve End-to-End (E2E) Closed-Loop (Autonomic) Security Management and Control (ASMC) in 5G E2E Architectures.

Generic Autonomic Network Architecture (GANA) Model defines an autonomic (closed-loop) manager for realizing security closed-loop that can be instrumented (implemented) as a software module. The autonomic manager component is referred to in the ETSI GANA Model as "**Security management Decision-making Element (DE)**".

In addition, such module could be powered by Artificial Intelligence (AI) such as Machine Learning (ML) or Deep Learning (DL) models that enable it to intelligently achieve security assurance targets at the level of its operations scope. A Cognitive Security-Management-DE is one that has a capability of learning and reasoning, and so it is considered as a deployable AI Model that needs to be tested before it is on boarded to run in a production environment.

A Security management-DE is responsible for autonomically managing any security issues. It does so by adaptively employing and managing "Managed Entities" (MEs) that pertain to the use of Certificates/Passwords Algorithms, Hash Algorithms, Encryption Algorithms, Access Control Mechanisms, Trust Mechanisms, Denial of Service (DoS) Detection/Prevention mechanisms, signature based intrusion detection mechanisms, and other security enforcement mechanisms.

Figure 1 illustrates the two levels at which "Security management DEs" can be designed to operate. The higher "Network-level Security management-DE" in the KP is responsible for controlling the lower "Node-level Security Management DEs" in Networks Elements (NEs) with Networks Functions (NFs) belonging to the network segment. The Security management DEs is a sub-part of the what is called the "Node-main-DE" in a GANA Node, along with other sub-DEs of the Node-main-DE such as Autoconfiguration and discovery management DE, resilience management DE, and Fault Management DE.

NOTE 1: Some MEs of an NE, such as Protocols of the Stack, may have own intelligence for security enforcement or may intrinsically embed security features. However, the MEs communications with the outside world may need to be constrained or policy-controlled by the global security enforcement policies of the Security Management-DE. And so the two GANA levels-DE to give particular in designing and implementing ASMC are the Node level-DE (GANA Level 3) and Network Level-DE (GANA Level 4).

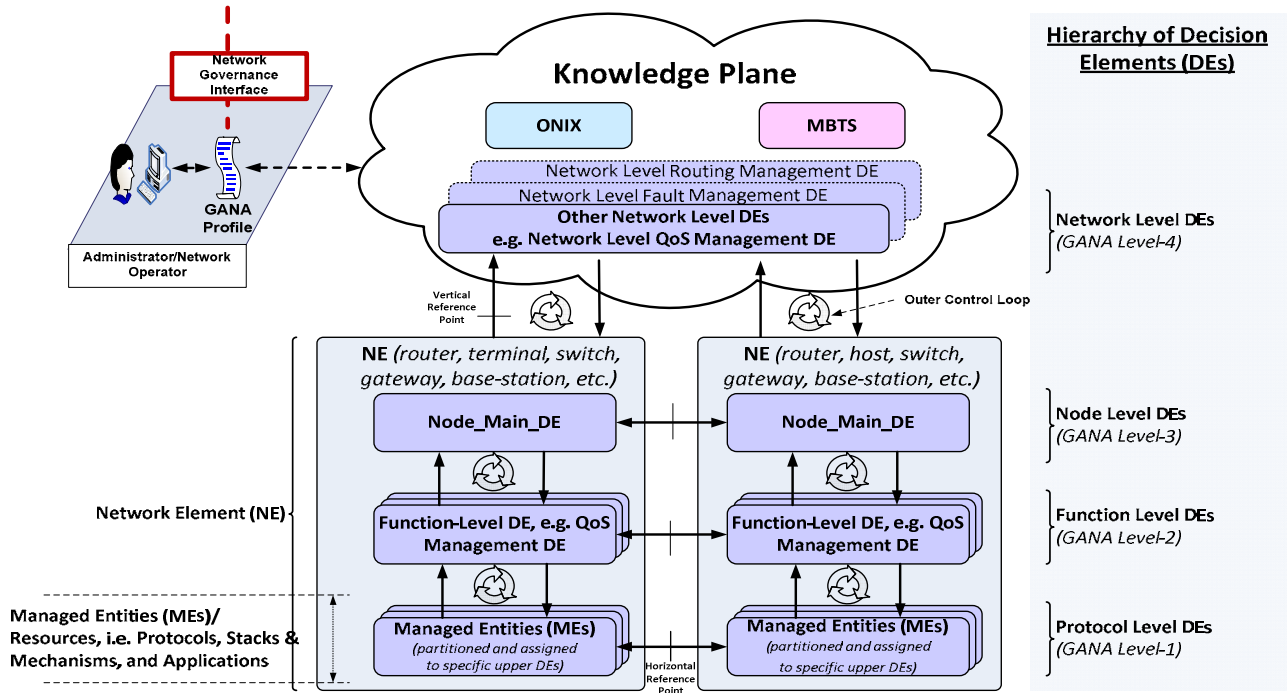


Figure 1: GANA Framework

The two layers (abstraction levels) of Security-management DEs that should be of focus in introducing Autonomic (Closed-Loop) are the Security DE in Network Level DEs for slow control loops and the Security DE in Node Level DEs for Fast control loops

The Security-Management-DEs are expected to implement **Self-Protection** and **Self-Defending** Policies and Operations for specific Network Segments/Domains as driven by whole GANA KP Platforms.

The definitions of **Self-Protection** and **Self-Defense** behaviours that help implementers of Security-Management-DEs in implementing the DEs at the two GANA levels and make them to interwork:

- Self-Protection** involves the capability by which individual NEs/NFs of the network (thanks to embedding Security Management-DEs) automatically apply security policies and software patch updates that help protect the NE/NF and services using it from being compromised by security attacks (including intrusions, violations, etc.) and vulnerabilities/risks/threats (both, known and unknown attacks and vulnerabilities). This low-level security enforcement on NE/NF level should be complemented (enhanced and controlled) by a security enforcement capability that operates on the level of management and control systems of the network (thanks to Network-Level Security Management-DEs). The complementary capability at the network level dynamically computes and applies security policies for the whole network (e.g. a specific network segment) and services using any knowledge of known attacks that may occur to NEs/NFs and network services, and applying software patches as may be necessary to protect the network resources from being compromised by attacks and any vulnerabilities.

- **Self-Defense** involves the capability by which individual NEs/NFs of the network (thanks to embedding Security Management-DEs) automatically exercise the ability to detect security attacks (including intrusions, violations, etc.) and vulnerabilities(risks/threats) and apply security policies or software patch updates in reaction (defense) to any detected attacks or vulnerabilities/risks, and if the capability is more intelligent, then exercise the ability to predict security attacks and vulnerabilities and apply appropriate defense techniques. The effect of the self-defense actions is to minimize impacts of the detected or predicted attacks or vulnerabilities/risks/threats on services that depend on the NE/NF. As in the case of Self-Protection, the low-level security enforcement and security hardening on NE/NF level should be complemented (enhanced and controlled) by a capability that operates on the level of management and control systems of the network (thanks to Network-Level Security Management-DEs). The complementary capability at network level dynamically computes and applies security policies for the whole network (e.g. a specific network segment) and services using the knowledge of attacks or risks detected or predicted by a NE(s)/NF(s). In addition, applies software patches to defend and protect the network resources from being compromised by detected or predicted attacks or vulnerabilities/risks such that their impacts on network services is none or minimal. Self-Defense is closely related to the concept of **Resilience** (reactive and proactive resilience).

NOTE 2: The term security "**attack**" is generalized in the present document, to include all forms of security attacks or violations, including Denial of Service (DoS) Attacks for example, intrusions, and other forms of violations of the security of a system, service or network. There are various sources in literature that provide taxonomy on network, services and systems related security matters, e.g. [i.24].

A Security-Management-DE can be configured to operate in "Open-Loop Mode" or "Closed-Loop Mode". In Open-Loop Mode (allows human in the loop operation) the DE produces recommendations on actions the human operator can take to meet certain security enforcement or assurance objectives. ETSI GANA describes in much more detail these two modes of configuring a DE. The following aspects relate to how the ASMC part of the broader AMC is supposed to be realized by the interworking of the Security-Management-Des hierarchically (at the two levels) and horizontally (for certain ASMC strategies and algorithms that may be implemented in a distributed fashion within and across NEs/NFs of network):

- a) **Node Level Security-Management-DE.** The autonomies (closed-loop(s)) of this DE includes orchestration of security mechanisms/techniques within a Network Element (NE) / Network Function (NF) in order to achieve self-protection and self-defence against security threats and attacks detected or predicted. Also the DE is responsible for planning and executing strategies for dynamically enforcing secure communications between the NE and the outside world, e.g. firewalling of traffic, tunnelling of traffic (including dynamic Virtual Private Networks (VPNs) provisioning to meet certain security objectives), encryption, use of trust models, etc.
- b) **GANa KP Level Security-Management-DE.** The autonomies of this DE includes Dynamic Security Policies computation and their enforcement by the KP Level Security Management DE onto the lower Node level Security-Management-DE. In addition, the DE's autonomies include dynamic programming of security-policy-enforcement such as SDN controllers and specialized security functions of the network such as Firewalls, Security Gateways, Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs). This is because the KP Level Security Management-DE is the DE responsible for the security assurance and self-protection and self-defence of the whole domain (network segment) against security attacks and threats. The KP Level Security-Management-DE should also exhibit intelligence (thanks to autonomies algorithms for achieving **self-protection, self-healing, and self-defence** for the network and its services) that causes the DE to dynamically orchestrate or (re)-configure security functions wherever they may be needed on demand in response to security threats detection and prediction. Such dynamic configurations by the KP level Security Management DE apply to physical security functions as well.
- c) **Specialized Security Functions** such as firewalls, IPSs, and IDSs, as NEs may need to embed the Node-level Security-Management-DE, like in the case of certain NEs such as routers and switches. In this way the DE can also serve as an embedded agent that should be policy controlled by the one at the KP level.