ETSI TS 104 102 V1.1.1 (2025-09)

TECHNICAL SPECIFICATION

Cyber Security (CYBER);
Encrypted Traffic Integration (ETI);
ZT-Kipling methodology

Reference

DTS/CYBER-00139

Keywords

Cyber Security

ETSI

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

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

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

Important notice

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

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 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 Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

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 defines a set of methods and the overall methodology for incorporating Zero Trust approaches as defined in NIST SP 800-207 [2] into an organization, product or service for the purpose of maximizing the transparency and explicability of the attack surface and to optimize the application of cybersecurity resources to minimize the attack surface.

The present document specifies the ZT-Kipling methodology applied to the requirements set out in ETSI TS 104 103 [1] and which addresses the countermeasure framework described in ETSI TS 104 101 [i.8].

NOTE: Whilst the ZT-Kipling methodology and its associated methods can be automated the present document does not directly address how it can be automated and this aspect may be addressed in future standardization

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 in the ETSI docbox.

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 TS 104 103: "Cyber Security (CYBER); Encrypted Traffic Integration (ETI); Problem Statement review and requirements definition".

[2] NIST SP 800-207: "Zero Trust Architecture".

[3] ETSI TS 102 165-1 (V5.3.1): "Cyber Security (CYBER); Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

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 TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.2] Rudyard Kipling's Just So Stories: "The Elephant's child", published in 1902.

[i.3] John Kindervag: "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security".

[i.4] GSMA™: "FS.37, GTP-U Security".

[i.5] GSMA™: "FS.40, 5G Security Guide", Version 3.0.

[i.6] E.M. Hutchins et al.:"Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains".

[i.7] Recommendation ITU-T X.200: "Information technology - Open Systems Interconnection - Basic Reference Model: The basic model".

[i.8] ETSI TS 104 101: "Cyber Security (CYBER); Encrypted Traffic Integration (ETI) Techniques to allow authorized users to identify and access encrypted traffic".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

least persistence: means of granting access to an asset for only sufficient time to perform the requested action

least privilege: means of granting access to a system asset only to those entities who have a legitimate purpose for access

NOTE 1: Thus access to a protected asset is granted to only allow those rights or privileges that are essential to perform the required task.

NOTE 2: As defined in NIST SP 800-207 [2].

3.2 Symbols

Void.

3.3 Abbreviations

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

5G NSA	5G Non-Stand Alone
5G SA	5G Stand Alone
AV	Attack Vector
C&C	Command and Control
CI/CD	Continuous Integration/Continuous Delivery
CKC	Cyber Kill Chain
CSC	Critical Security Control
DoS	Denial of Service
ETI	Encrypted Traffic Integration
H-MNO	Home Mobile Network Operator
IMEI	International Mobile Subscriber Identity
IMSI	International Mobile Equipment Identity
IoT	Internet of Things
IT	Information Technology
MitM	Man in the Middle
MNO	Mobile Network Operator
OSI	Open Systems Interconnection
PEI	Permanent Equipment Identifier
PoP	Point of Presence
RAN	Radio Access Network
RCE	Remote Code Execution
SBA	Service Based Architecture
SUPI	Subscription Permanent Identifier
TA	Threat Agent

TV	Threat Vector
UE	User Edge
UPF	User Plane Function
V-MNO	Visitor Mobile Network Operator
ZT	Zero Trust
ZTA	Zero Trust Architecture
ZT-Kipling	Zero Trust Kipling

4 Zero Trust security design principles

4.1 Introduction

Modern network design, supporting high speed, always-on connectivity with near 100 % availability, has led to a number of paradigms and initiatives that attempt to give assurance of security. These include "secure by design", "secure by default", and, as a stepping stone to Zero Trust (ZT), the principles of "least privilege" and "least persistence". "Never trust, always verify", as originally outlined by John Kindervag [i.3] is the main design principle of ZT, and has been formalized in NIST SP 800-207 [2].

ZT and the Kipling criteria, specified in this document, combine across the entire organization giving transparency and explicability of the security features and making all aspects of the network operation transparent and explicable. That, therefore, reinforces the application of best engineering practice in system provision. Without such attention to detail, the boundary of the system is unknown to its stakeholders and this uncertainty is an opening to the system being attacked. An open, attackable system costs more to maintain, and may lead to over-provisioning that, in turn, further exposes the system to attack. The approach to ZT and the application of the Kipling criteria applies to all aspects of a system, including planning, provisioning, operations, maintenance and security, where security is not optional and is embedded throughout.

The Kipling Criteria require that the analyst and designer ask the following questions of each and every system element for each context it is used: What?, Why?, When?, How?, Where?, and Who?

NOTE: The Kipling Criteria are so named as they come from a short story by Kipling [i.2] from which the following quote is taken "*I Keep six honest serving-men: (They taught me all I knew) Their names are What and Where and When And How and Why and Who*". In the context of the present document these 6 questions when asked appropriately of every element, and of how each element is associated to any other element, give a complete picture of the role and purpose of the element. Thus this allows the designer or analyst to be able to demonstrate the validity of the element in the system.

In giving an assurance of the security of a network the application of the ZT and the use of the ZT-Kipling methodology ensures that the following principles shall be strictly enforced at every stage of a cyber attack lifecycle:

- Minimize the attack surface
- Impose a principle of least privilege to allow the use of any asset
- Impose a principle of least persistence for the use of any asset

The ETI problem statement, in ETSI TS 104 103 [1] suggests that the following steps are taken to address the problem of pervasive encryption thus is consistent with the mandating of the principles above:

- transparency and explicability of all elements in the network;
- least persistence and least privilege to deploy, access and make use of any element in the network; and
- Application of the ZT Kipling methodology as defined in the present document.

The ZT-Kipling methodology and its supporting methods defined in the present document shall apply to all elements of a system, and by default, shall include the supply chain. As such, the present document is not a technology to be deployed, but rather a sound approach to the business of effective telecommunications.

Application of the ZT-Kipling methodology, and its associated methods, hereinafter simply referred to as ZT-Kipling, impacts how security technologies, elements, protocols are deployed. In the present document this is extended by application of the Kipling Criteria. ZT-Kipling enforces each stakeholder to answer a small set of questions that result in transparency and explicability of the purpose of the system and all of its functionality. This ensures that the minimum and most effective set of features, including security features, are included in the system, and by default unnecessary ones are removed.

4.2 Purpose of ZT in systems

As outlined in clause 4.1 above ZT is not a technology, rather it is an approach, formalized in the present document as the ZT-Kipling methodology and supporting methods, to look at systems in order to achieve transparency and explicability of the components or assets of a business system that when combined offer secure services to users. Zero Trust Architecture (ZTA) is based on the assumption that security breaches are inevitable with threat causes inside and outside of a perimeter of a concern, be it an organization, a Data Centre, a service provider infrastructure, or anything else.

The methods used to underpin ZT-Kipling are drawn from, and extend, the Critical Security Controls (CSCs) described by ETSI TR 103 305-1 [i.1]. The application of CSC is shown in more depth in clause 5 of the present document but the specific role played by CSC-7 and CSC-10, addressing continuous vulnerability management and malware defences respectively, is outlined below:

- CSC-7 (Continuous Vulnerability Management) is to "Develop a plan to continuously access and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information".

- CSC-10 (Malware Defences) is to "Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets".

4.3 ZT outline

All assets of the system are impacted by ZT-Kipling and are illustrated in Figure 1.

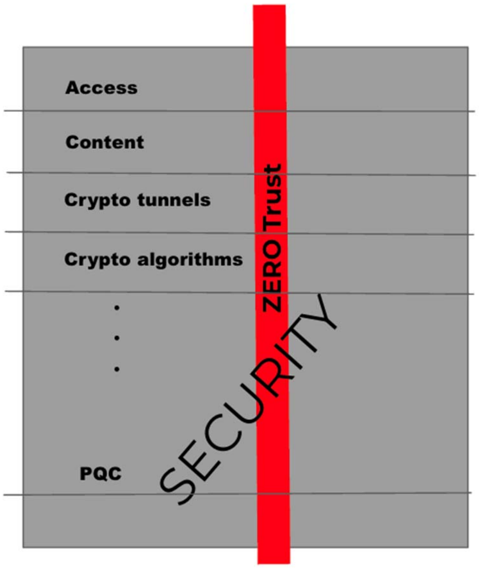

Figure 1: Perspective of Zero Trust in Security

To quote from ETSI TS 104 103 [1] "*Zero trust … provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.*". For the purposes of the present document the prior definition from ETSI TS 104 103 [1] is refined as follows, **ZT is a security strategy (or approach), which is based on no implicit trust (i.e. zero trust) in the digital world, and is designed to detect and prevent breaches, while consistently (or better continuously) verifying all users, all devices, all layers (e.g. OSI layered model Recommendation ITU-T X.200 [i.7]), all applications, across all locations in real time (run-time), and applying continuous integration and continuous delivery (CI/CD) pipeline security, resulting in preventative security from all attack vectors at all stages of the attacks: thus trust becomes explicit**.

ZT-Kipling consists of five (5) iterative (and recursive) steps in addition to asking the questions of the Kipling Criteria, as Figure 2 illustrates. The steps are repeated continuously for the lifetime of the protected surface. The steps are:

1) Define the protected surface - identify what needs to be protected.

2) Map the transaction flows - how does the traffic flow to, through, and from the protected surface.

3) Build a Zero Trust Architecture (ZTA) - based on the protected surface and the transaction flows, what should ZTA look like? What are its security components and mechanisms?

4) Create Zero Trust security policy - follow Kipling criteria to define the Zero Trust security policy, which adheres to the defined ZTA.

5) Monitor and maintain - maintain and monitor the protected surface.

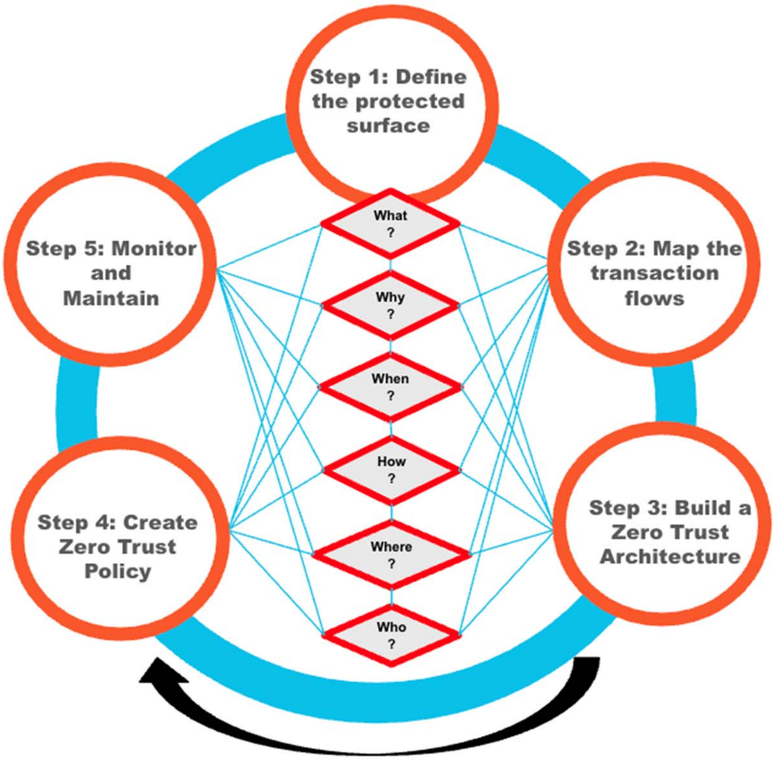
Step 1: Define the protected surface
Step 2: Map the transaction flows
Step 3: Build a Zero Trust Architecture
Step 4: Create Zero Trust Policy
Step 5: Monitor and Maintain
What ?
Why ?
When ?
How ?
Where ?
Who ?

Figure 2: ZT-Kipling methodology

The specific actions to be taken for each step are defined in more detail in clause 5. Annex A provides a normative use case of the application of ZT-Kipling.

In order to minimize the attack surface and to further develop knowledge of the attack surface the assets of the system or network the security controls defined in ETSI TR 103 305-1 [i.1], in particular CSC-1 and CSC-2, shall be applied.

As outlined in ETSI TR 103 305-1 [i.1] CSC-1 is intended to "Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise.

This will also support identifying unauthorized and unmanaged assets to remove or remediate", and CSC-2 does similarly for software assets as "Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution".

As Figure 2 illustrates, Kipling criteria is used in each of the 5 steps leading to the creation of Zero Trust security policies, following Least Privilege and Least Persistence principles.

4.4 ZT-Kipling application to achieve Least Privilege principle

In building an understanding of the application of ZT-Kipling to the least privilege paradigm the Kipling Criteria apply. In particular, when the use of an asset is determined by multiple criteria (e.g. attribute-based access control) the Kipling criteria provide deep knowledge of the role of an asset and its users, the reasons for the access, and the corresponding behaviours. Drilling into the meaning of each of the questions and what might represent its answer is use case dependent. Table 1 provides an example of how each question might be addressed within a Zero Trust security policy (Step 4) for asset access use case.

Table 1: Example of application of Kipling criteria for asset access in Step 4

Question	Example for asset access (Least Privilege principle)
What	What asset(s) are allowed to be accessed by the entity?
Why	Why is that entity accessing the asset?
When	When is the asset allowed to be accessed by the entity?
How	How does the asset know and verify that access is permitted?
Where	Where is the entity with relation to the asset?
Who	Who is the entity accessing the asset?

4.5 ZT-Kipling application to achieve Least Persistence principle

The security concern of persistent relationships (i.e. still in existence but idle) is that they act as uncontrolled attack surfaces. In maintaining the principle of always minimizing the attack surface, the aim of least persistence is to ensure that the protected surface is always maximized and controlled.

Application of the Kipling criteria to the least persistence principle is illustrated in Table 2.

Table 2: Example of application of Kipling criteria for asset existence

Question	Example for asset existence (Least persistence)	Comment
What	What is the asset	This is often the semantic or contextual element of an asset's identifier. E.g. border gateway.
Why	Why is that asset in the system	This extends the semantic identifier to address the context in which the asset exists.
When	When is the asset meant to be available (e.g. is it ephemeral or persistent, if ephemeral how is it invoked and so forth)?	The broad assumption should be to minimize the number of persistent elements.
How	How is the asset operated (e.g. what does it require in order to operate)?	
Where	Where is the asset (logically and geographically)?	
Who	Who owns the asset?	This should identify the liability chain including for reporting of any vulnerabilities.

5 Applying ZT-Kipling using Critical Security Controls

5.1 Considering Cyber Attack Lifecycle - Cyber Kill Chain

The cyber attack lifecycle - also known and referred to in the present document as Cyber Kill Chain (CKC) - is a framework that outlines the stages that a cyber attack typically follows, from initial reconnaissance stage to the final data exfiltration stage (Actions on Objectives). CKC consists of 7 stages, as illustrated in Figure 3 [i.6].

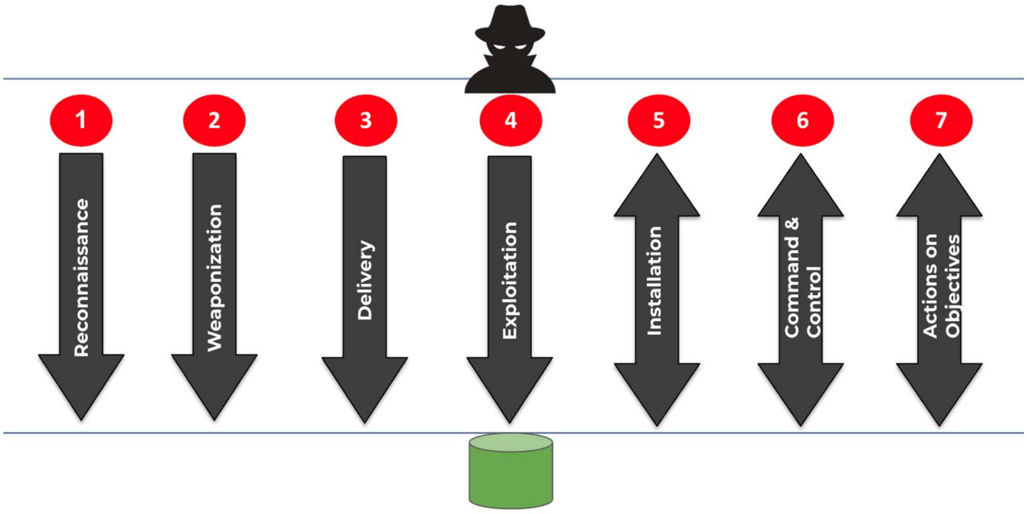

Figure 3: Cyber Kill Chain

Incorporating ZT-Kipling into networks' architectures from their inception delivers preventative security posture with the goal to provide proper security measurements as early as possible within the CKC, thereby diminishing the threat landscape. With that, no assumptions shall be made. ZT-Kipling applies for all CKC stages. Annex A provides illustrations of such ZT-Kipling implementations.

5.2 Step 1 - Define the Protected Surface

The present document identifies means to implement ZT-Kipling using specific Critical Security Controls (CSCs) from ETSI TR 103 305-1 [i.1]. In this case where specific CSCs are identified the present document identifies how they shall be applied in order to satisfy the ZT-Kipling methodology. Step 1 of ZT-Kipling seeks to define or identify the protected surface by determining the attack surface that has to be protected. An analysis of the threats and vulnerabilities should also be carried out using the approach defined in ETSI TS 102 165-1 [3] with ZT-Kipling questions (What, Why, When, How, Where, Who), as illustrated in Figure 2.

An attack surface may consist of the following:

- Managed assets
- Unknown assets
- Assets controlled by or maintained by 3rd parties
- Ephemeral assets

The building of knowledge of the assets of the system and how they are connected or related shall be addressed by application of the following CSCs:

- CSC-1 (Inventory and Control of Enterprise Assets): "Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate".

- CSC-2 (Inventory and Control of Software Assets): "Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution".

- CSC-3 (Data Protection): "Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data".

- CSC-4 (Secure Configuration of Enterprise Assets and Software): "Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices, non-computing/IoT devices, and servers) and software (operating systems and applications)."

- CSC-5 (Account Management): "Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software".

- CSC-6 (Access Control Management): "Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software".

- CSC-7 (Continuous Vulnerability Management): "Develop a plan to continuously access and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information".

- CSC-9 (Email and Web Browser Protections): "Improve protections and detections of threat from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement".

- CSC-10 (Malware Defences): "Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets".

- CSC-12 (Network Infrastructure Management): "Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points".

- CSC-15 (Service Provider Management): "Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately".

- CSC-16 (Application Software Security): "Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise".

NOTE: Although the aforementioned CSCs refer to "enterprises", service providers' infrastructures are included into those definitions.

5.3 Step 2 - Map the Transaction Flows

Mapping the transaction flow step results in an intra-systems, inter-systems, or both flow, which could encompass any number of CSCs, ETSI TR 103 305-1 [i.1], depending on the type of transaction flow. The reflections of which CSCs matter for Step 2 are reflected in Step 1 (define the protected surface), Step 3 (build a Zero Trust Architecture (ZTA)), and Step 4 (create Zero Trust security policy). ZT-Kipling questions (Figure 2) shall be applied accordingly, which normative Annex A elaborates on further.

5.4 Step 3 - Build a Zero Trust Architecture

Once the protected surface is defined and transaction flows are mapped (Steps 1 and 2, as above) the architecture of the Zero-Trust implementation shall be developed. The CSCs [i.5], corresponding to the protected surface (Step 1) and, following the mapped transaction flows (Step 2), while applying ZT-Kipling questions (Figure 2), shall be used to build the resulting ZTA. Normative Annex A presents an example use case.

This step shall consider the protected surface (defined in Step 1), which is the attack surface that needs to be protected. Whilst the threat surface encompasses all the potential threats that can exploit vulnerabilities in the system, an attack surface is a sum of all possible points from which Threat Agents (TAs) can attack:

$$\textbf{Attack Surface} = \sum_{n=1}^{\infty} (\mathbf{TA}_n)$$

Those points may include various cloud environments, IoTs/OTs/UEs, Internet assets, IT infrastructures, and more.

Further, Step 3 shall consider Attack Vectors (AVs) and Threat Vectors (TVs). While the AVs are the methods through which TAs launch attacks, or the "how" of a cyber attack, the TVs include the potential sources and motivations behind them or the "who" and "why" of a cyber attack. ZT-Kipling shall apply for TAs, AVs and TVs identification for any given architecture considering all stages of CKCs.

5.5 Step 4 - Create Zero Trust Security Policy (policies)

Once ZTA is built (Step 3), ZT security policies shall be created. The CSCs [i.5] corresponding to the protected surface (Step 1), following the mapped transaction flows (Step 2), and resulting ZTA (Step 4), shall be reflected in the security policies. ZT-Kipling questions (Figure 2) shall apply to creation of ZT security policies. Normative Annex A presents an example use case.

5.6 Step 5 - Monitor & Maintain

Step 5 of ZT-Kipling focuses on monitoring and maintenance of the designed and implemented ZTA and ZT security policies. While addressing the ZT-Kipling questions (Figure 2), the following controls from ETSI TR 103 305-1 [i.1] shall apply:

- CSC-8 (Audit Log Management): "Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack".
- CSC-11 (Data Recovery): "Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-included and trusted state".
- CSC-12 (Network Infrastructure Management): "Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points."
- CSC-13 (Network Monitoring and Defence): "Operate processes and tooling to establish and maintain comprehensive network monitoring and defence against security threats across the enterprise's network infrastructure and uses base".
- CSC-14 (Security Awareness and Skills Training): "Establish and maintain a security awareness program to influence behaviour among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise".
- CSC-15 (Service Provider Management): "Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately."
- CSC-16 (Application Software Security): "Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise."

- CSC-17 (Incident Response Systems: "Establish a program to develop and maintain an incident response capability (e.g. policies, plans, procedures, defined roles, training and communications) to prepare, detect, and quickly respond to an attack".

- CSC-18 (Penetration Testing): "Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker".

Annex A (normative): 5G roaming use case for application of ZT-Kipling

A.1 Overview

Figure A.1 illustrates a use case, which is used to explain the application of ZT-Kipling steps. A high level schema of 5G Non-Stand Alone (NSA) and 5G Stand Alone (SA) infrastructures are depicted, where a roaming 5G SA User Edge (UE), attached to the 5G NSA - Roaming UE, is required to connect to its Destination.

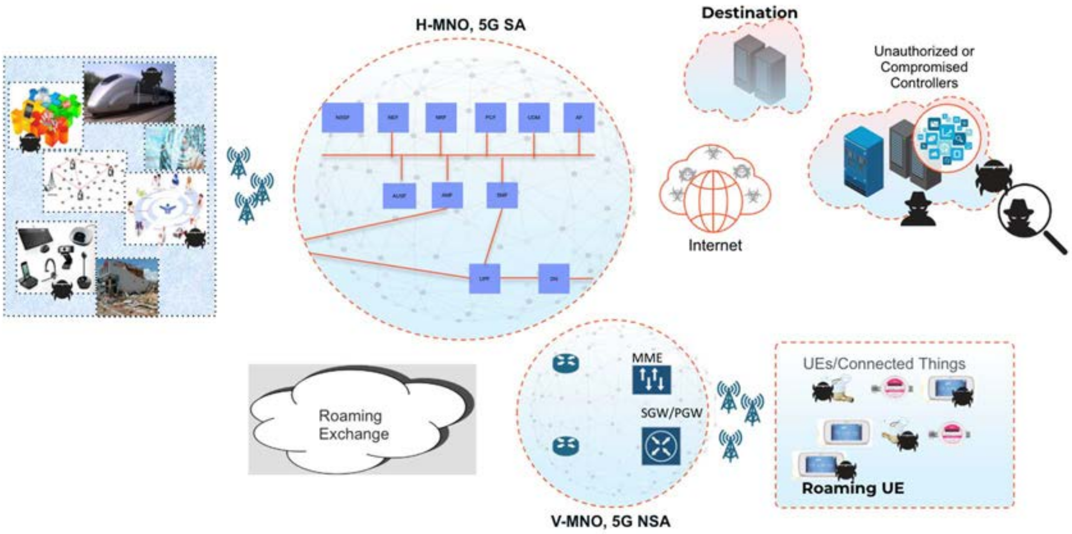

Figure A.1: Use Case - 5G SA and 5G NSA Infrastructures with Roaming UEs

In relation of ZT-Kipling to 5G roaming use case, ZT is a cybersecurity paradigm focused on:

- real time continuous monitoring /visibility for cyber risks, threats and vulnerabilities;
- least privileged security policies enforcement to protect from cyber risks, threats, and vulnerabilities;
- 5G User-ID (SUPI) and 5G Equipment/Device-ID (PEI) security policies granularity for both monitoring and enforcement;
- security across all layers of mobile networks: Application, Signalling, Data, and Management;
- security across all exposed locations: Roaming, RAN, Open-RAN, N6/SGi, APIs;
- security against all attack vectors: C&C, RCE, botnets, malware, MitM, fraudulent IDs, identity, Ransomware, DoS; and
- security across all software lifecycle stages: runtime, CI/CD (shift left), DevOps.

NOTE: The aforementioned list applies to all use cases of 5G networks.

A.2 Step 1 - Define the Protected Surface

Using Table A.1, ZT-Kipling questions apply to define the protected surface.

Table A.1: ZT-Kipling Questions Applied to Step 1 - Define the Protected Surface

What	What assets [applications, devices, etc.] can the Roaming UE access?
Why	Why is that roaming UE accessing those assets (Destination)?
When	When can the roaming UE access Destination?
How	How does the Destination know and verify that Roaming UE access is permitted?
Where	Where is the Roaming UE in relation to the Destination?
Who	Who [what is its IMEI, IMSI, user] is the Roaming UE accessing the Destination?

The protected surface for the UE (depicted in Figures A.1) that is roaming through the visitor's 5G NSA network, roaming exchange, its home 5G SA network, and continuing to transit through Internet to Destination, is the sum of the following elements:

1) roaming UE;

2) UE - V-MNO (5G NSA) transit;

3) V-MNO (5G NSA) Core;

4) V-MNO (5G NSA) Core - Roaming Exchange - H-MNO (5G SA) Core transit;

5) H-MNO (5G SA), including Service Based Architecture (SBA) and User Plane Function (UPF), Core;

6) H-MNO 5G SA Core - Internet - Destination transit; and

7) destination.

Table A.2 summarizes the applicability of CSCs from ETSI TR 103 305-1 [i.1] for each identified protected surface element.

Table A.2: Step 1 - Define the Protected Surface & CSCs

Protected Surface Element	CSC-#
1. Roaming UE	1, 2, 3, 4, 5, 6, 9, 10,16
2. UE - V-MNO (5G NSA) transit	1, 2, 3, 4, 5, 6, 7, 10, 12
3. V-MNO (5G NSA) Core	1, 2, 3, 4, 5, 6, 7, 10, 12, 15, 16
4. V-MNO (5G NSA) Core - Roaming Exchange - H-MNO (5G SA) Core transit	1, 2, 3, 4, 5, 6, 7, 10, 12
5. H-MNO (5G SA) Core	1, 2, 3, 4, 5, 6, 7, 10, 12, 15, 16
6. H-MNO (5G SA) Core - Internet - Destination transit	1, 2, 3, 4, 5, 6, 7, 10, 12
7. Destination	1, 2, 3, 4, 5, 6, 9, 10, 16

A.3 Step 2 - Map the Transaction Flows

Figure A.2 illustrates the transaction flow from the Roaming UE to Destination. Although the figure illustrates one-directional flow, in most cases, the flows are bi-directional, depending on the application used.

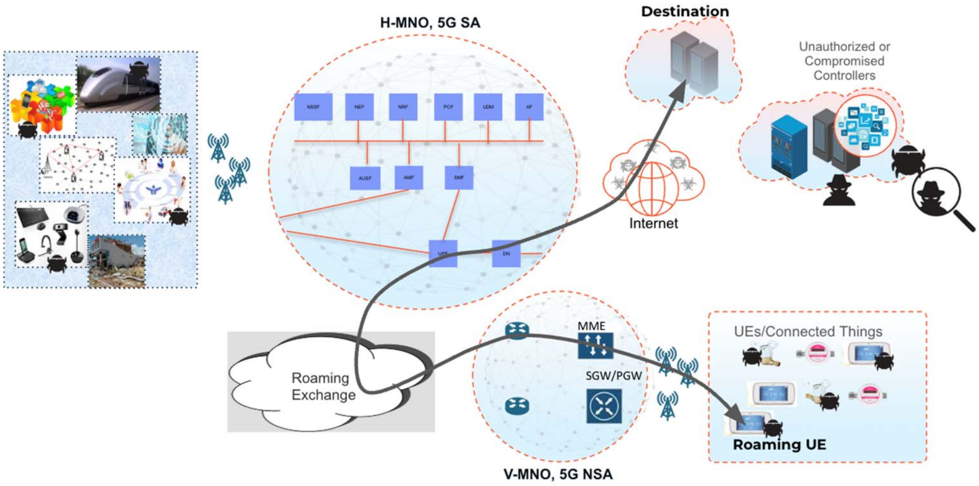

Figure A.2: 5G Roaming Use Case. Step 2 - Map the Transaction Flows

Although the illustration of the transaction flow in the present document is a high-level view, a deeper perspective is highly recommended. It is like peeling an onion - starting with a high-level architecture and then, digging down to the next level, all the way to physical interfaces and ports, mapping the flows from one element to another one. Therefore, responses to the ZT-Kipling questions might be slightly different, based on the level of the transaction flow considered. For example, Table A.3 illustrates the responses to the ZT-Kipling questions for a high level of transaction flow, while Table A.4 illustrates the responses to the questions for a lower level of the transaction flow details. The aforementioned tables provide a good illustration of how the responses to ZT-Kipling questions might differ.

Table A.3: ZT-Kipling Questions Applied to Step 2 - Map the Transaction Flows, high level

What	What service providers will the Roaming UE use to reach the Destination?
Why	Why will the Roaming UE use those service providers?
When	When can the Roaming UE use those service providers ?
How	How will the transiting traffic traverse through all service providers?
Where	Where from the Roaming UE can connect to the Destination?
Who	Who [what is its IMEI, IMSI, user] is the Roaming UE accessing the Destination?

Table A.4: ZT-Kipling Questions Applied to Step 2 - Map the Transaction Flows, lower level

What	What Point of Presence (PoP) of the V-MNO will be used to attach to the network?
Why	Why will the Roaming UE use that service provider (V-MNO)?
When	When can the Roaming UE use the V-MNO?
How	How will the V-MNO and H-MNO verify the Roaming UE?
Where	Where can the Roaming UE access the V-MNO from?
Who	Who [what is its IMEI, IMSI, user] is the Roaming UE accessing the Destination?

A.4 Step 3 - Build a Zero Trust Architecture

Once the protected surface is defined and transaction flows are mapped (Steps 1 and 2, respectively, are completed), ZTA (Step 3) can be built. Before any security architecture can be considered, it is important to understand AVs, TVs and TAs related to all the elements are within the defined protected surface and the mapped transaction flows are valid [2]. Application of ZT-Kipling identifies AVs, TVs, and TAs for all stages of CKCs within the architecture, as illustrated in Table A.5. Further, the CSCs identified in TR 103 305-1 [i.1], in Steps 1 and 2, shall apply by applying the ZT-Kipling method as defined in the present document.

Table A.5: ZT-Kipling Questions Applied to Step 3

		Comment
What	What are the TAs for the defined protected surface?	Identify AVs & TVs
Why	Why could the TAs attack the defined protected surface?	Identify TVs
When	When could the TAs attack the defined protected surface?	Identify TVs
How	How could identified TAs launch attacks on the defined protected surface	Identify AVs & TVs
Where	Where from TAs could attack the defined protected surface?	Identify AVs & TVs
Who	Who are the possible TAs?	Identify AVs & TVs

Depending on the CKC stage, the TAs could camouflage, using the penetrated elements, which need to be protected in the first place, as extensions of themselves, resulting in the increase of TA attack surface and its impact.

Figure A.3 illustrates the seven (7) TAs and AVs for the Roaming UE use case discussed in the present document. Considering all stages of CKC, the TAs and the AVs for the use case are:

- TA1 & AV1 - Roaming UE;
- TA1 & AV2 - RAN;
- TA3 & AV3 - V-MNO, 5G NSA Infrastructure;
- TA4 & AV4 - Roaming Exchange;
- TA5 & AV5 - H-MNO, 5G SA Infrastructure;
- TA6 & AV6 - Internet; and
- TA7 & AV7 - Destination.

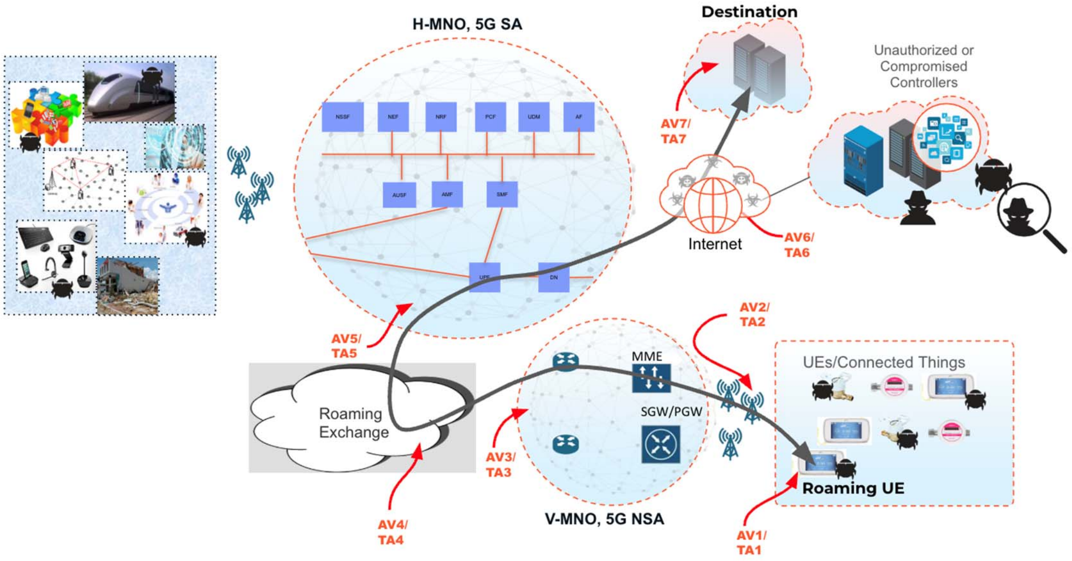

Figure A.3: 5G Roaming Use Case, TAs and AVs

The aim of ZTA is to deliver the architecture, which provides defences from any TA and AV at any CKC stage. To achieve this, ZTA includes the following methodologies and technologies:

- Identity and Access Management;
- Devices;
- Networks;
- Micro-segmentation;

- Encryption;
- Applications and Workloads Validation;
- Data; and
- Visibility and Analytics.

ZTA has three (3) main elements:

- Users;
- Applications; and
- Infrastructure.

Applying the aforementioned ZTA methodologies and technologies to those main three elements, while addressing ZT-Kipling, results in a ZTA. Table A.6 provides a cross-reference between the TAs and AVs for the corresponding Protected Surface Elements, the corresponding ZTA Elements, and ZTA methodologies and technologies, which shall be included into ZTA for the discussed Roaming UE use case. Further, applicable CSCs [i.1], as identified in clause 5.2 of the present document, are depicted in Table A.6.

Table A.6: Step 3 - ZTA Methodologies & Technologies to be Applied Against Identified TAs

TA & AV	CSC-#	Protected Surface Element	ZTA Element	ZTA Methodologies & Technologies to be Included
1, 2, 3, 4, 5, 6, 7	1, 2, 3, 4, 5, 6, 9, 10, 16	1. Roaming UE	Users Applications	Apply principles of least privilege access and identity. Verify the Roaming UE integrity, including IMSI/SUPI, IMEI/PEI validation. Validate the UE data integrity through visibility and analytics [i.4].
1, 2, 3	1, 2, 3, 4, 5, 6, 7, 10, 12	2. UE - V-MNO (5G NSA) transit	Infrastructure	Micro-segment networks and possible workloads Devices' management [includes RAN elements, routers, switches, mobile core elements facing RAN, UE] Encrypt traffic transiting through air or in RAN sharing use cases.
1, 2, 3, 4, 5, 6, 7	1, 2, 3, 4, 5, 6, 7, 10, 12, 15, 16	3. V-MNO (5G NSA) Core	Infrastructure Applications (related to the core)	Micro-segment networks and possibly workloads Devices' management [includes routers, switches, mobile core elements and functions, Operations Support Systems (OSS)/Business Support Systems (BSS) systems, UE] Validate core elements' workloads continuously (CI/CD) Validate UE device integrity, including IMSI/SUPI, IMEI/PEI Visibility and analytics of data integrity [i.4].
3, 4, 5	1, 2, 3, 4, 5, 6, 7, 10, 12	4. V-MNO (5G NSA) Core - Roaming Exchange - H-MNO (5G SA) Core transit	Infrastructure	Micro-segment networks and possibly workloads Devices' management [includes routers, switches, mobile core elements and functions] Encrypt traffic transiting through untrusted roaming exchanges.
1, 2, 3, 4, 5, 6, 7	1, 2, 3, 4, 5, 6, 7, 10, 12, 15, 16	5. H-MNO (5G SA) Core	Infrastructure Applications (related to core)	Micro-segment networks and possibly workloads Devices' management [includes routers, switches, mobile core elements and functions, Operations Support Systems (OSS)/Business Support Systems (BSS) systems, UE] Validate core elements' workloads continuously Validate UE device integrity, including IMSI/SUPI, IMEI/PEI Visibility and analytics of data integrity [i.4].

TA & AV	CSC-#	Protected Surface Element	ZTA Element	ZTA Methodologies & Technologies to be Included
1, 5, 6, 7	1, 2, 3, 4, 5, 6, 7, 10, 12	6. H-MNO (5G SA) Core - Internet - Destination transit	Infrastructure	Micro-segment networks and possibly workloads Devices' management [includes routers, switches, mobile core elements and functions] Validate the Destination integrity Encrypt traffic transiting through untrusted domains.
1, 6, 7	1, 2, 3, 4, 5, 6, 9, 10, 16	7. Destination	Users Applications	Apply principles of least privilege access and identity Verify Destination integrity Validate the device integrity, including IMSI/SUPI, IMEI/PEI Validate data integrity through visibility and analytics [i.4].

Figure A.4 illustrates the resulting ZTA for the discussed Roaming UE use case, identifying the positioning of security elements following the ZT principle of securing across all layers of mobile networks (Application, Signalling, Data, and Management), exposed locations (Roaming, RAN, Open-RAN, N6/SGi, APIs), and securing against all TAs and AVs, as identified in Figure A.3 and Table A.6. ZTA includes security control checks along the transaction flow path through the identified protected surface elements. The protection mechanisms and technologies include strict security policies, which Step 4 of ZT-Kipling addresses.

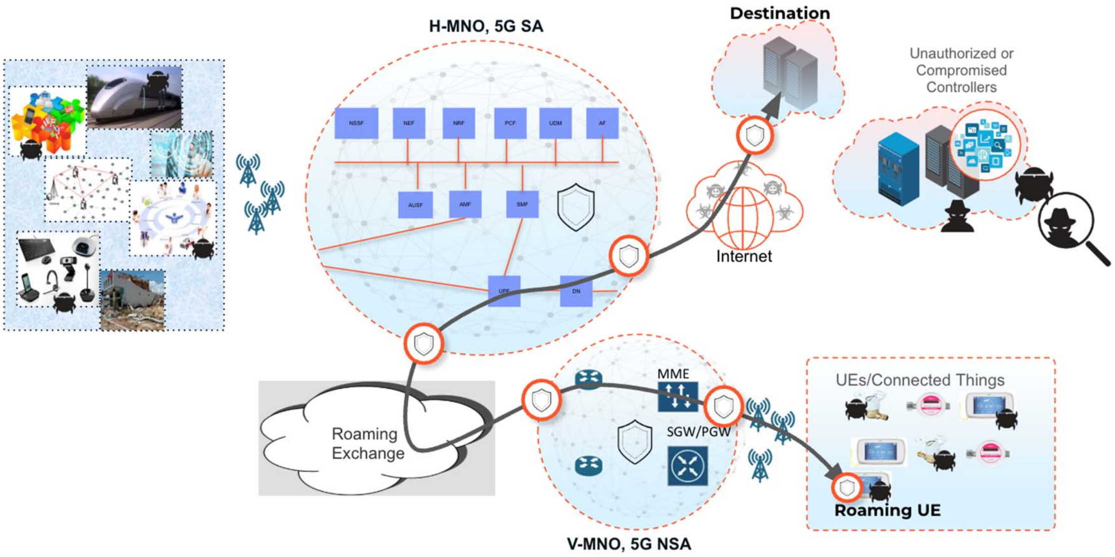

Figure A.4: Use Case. Step 3 - Build ZTA

A.5 Step 4 - Create Zero Trust Security Policy (policies)

Once the protected surface (Step 1) is defined, roaming transaction flow (Step 2) is mapped, and ZTA is built (Step 3), ZT security policies are created using ZT-Kipling.

Table A.7 provides the applicable ZT-Kipling questions to be used for roaming ZT security policies use case.

Table A.7: ZT-Kipling questions applies to Step 4 - Create ZT Security Policy

What	What applications are being used to traverse the networks? Identify and validate signalling and user plane applications.
Why	Why is the packet accessing a resource? Identify legitimate flows for signalling & user planes.
When	When is the resource being accessed? Predictable signalling/user planes traffic behaviours.
How	How does the packet access the protected surface throughout the communications? Visibility into signalling and user planes.
Where	Where is the packet source and destination? Specify the source/destination.
Who	Who should be connected to this flow? Validate unique mobile user IDs - IMSIs/SUPIs, IMEIs/PEIs.

As ZT security policies apply to every security element along the transaction flow, the responses to ZT-Kipling questions might vary, depending on the security element's position within ZTA. Further, every security element along the transaction flow path shall address the CSCs corresponding to the protected surface element, which was identified in Step 1 of ZT-Kipling (clause 5.2 of the present document) and reflected in Tables A.2 and A.6.

A.6 Step 5 - Monitor & Maintain

During this step, roaming network monitoring and maintenance shall take place contiguously. CSCs applicable to this step are: 8, 11, 12, 13, 16, 17, and 18, as identified in clause 5.6 of the present document.

Table A.8 provides the applicable questions for this ZT-Kipling step 5 for the Roaming use case.

Table A.8: ZT-Kipling Questions Applied to Step 5 - Monitor & Maintain

What	What applications are traversing the networks? Identify and validate all transiting applications without relying on port numbers, as those may be spoofed. Any changes?
Why	Why is specific traffic transiting? Is it legitimate?
When	When is the resource being accessed? Does it follow the pattern? What are the differences? Any changes?
How	How does the packet access the protected surface throughout the communications? Any changes?
Where	Where is the packet sourced from? Was it validated? Any changes?
Who	Who is accessing the assets? Are the unique mobile user IDs - IMSIs/SUPIs, IMEIs/PEIs - validated?

Depending on the monitored roaming traffic, customers' coverage, involved MNOs' and roaming partners changes, Step 5 shall lead to step 1 recursively, as illustrated in Figure 2.

Annex B (informative): Bibliography

- GSA ZTA 3.1: "Zero Trust Architecture (ZTA) Buyer's Guide", Version 3.1.
- CISA ZTMM 2.0: "Zero Trust Maturity Model", Version 2.
- ETSI TR 103 644 (V1.2.1): "Cyber; Observations from the SUCCESS project regarding smart meter security".

History

Document history		
V1.1.1	September 2025	Publication