Ericsson White Paper
1/284 23-FGB 101 0781 Uen
February 2024

ERICSSON

Zero Trust Architecture for advancing mobile network security operations

Content

Executive Summary

Perimeter security alone is no longer sufficient for securing critical infrastructure due to evolving threats, including advanced persistent threats (APTs) from sophisticated adversaries. Once inside the network, the adversary could exploit vulnerabilities to move laterally undetected and perform reconnaissance or disrupt the network, if a monitoring system were not in place. The best way to prepare for evolving threats is to have a system aligned with a zero trust architecture (ZTA) that secures micro-perimeters across the entire mobile network and provides the ability to identify, protect, detect, respond, and recover from evolving attacks. Industry standards define technical capabilities that support a ZTA, but these capabilities need to be complemented with automated security operations to continuously achieve the desired security posture. This whitepaper describes a security management function that automates and orchestrates network security operations to help mobile network operators (MNOs) achieve a ZTA aligned with the US National Institute of Standards and Technology (NIST) Zero Trust Architecture [1] and US Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model (ZTMM). It also provides guidance for MNOs to implement the cross-cutting functions highlighted in the CISA ZTMM: visibility and analytics, automation and orchestration, and governance. The approach outlined is applicable to all MNOs that are integrating ZTA cyber hygiene capabilities and practices, particularly in the context of compliance with the NIS 2 directive in the European Union (EU), reference [2]. We delineate the relevance of ZTA in the context of mobile networks; emphasize the criticality of 3GPP security functions, and highlight the necessity for a dedicated security management function in the implementation of ZTA within mobile networks. Lastly, the whitepaper also offers a comprehensive guidance, presenting a systematic approach that progresses from existing operational conditions to an ideal state that harnesses the power of AI for network-wide visibility and rapid response capabilities.

Introduction

In recent years, a comprehensive transformation in computing infrastructure, threat landscape, and cybersecurity regulations have reshaped telecom networks. Regulators have heightened their focus on cybersecurity, particularly for critical infrastructure, where telecom networks play a vital role. To enhance cyber resiliency, regulatory bodies around the globe now advocate for ZTA to complement traditional perimeter-based defenses. ZTA was introduced and defined in the US NIST 800-207 Zero Trust Architecture [1] and its implementation is guided by CISA ZTMM [3]. ZTA operates on the principle of continuous verification and monitoring, assuming external and internal threats exist to the network. Its significance is further highlighted as it emerges in regulations, such as NIS2 [2].

For the telecom industry, security has been a top priority in the development of 3rd Generation Partnership Project (3GPP) 5G specifications from the start. Recently, the need for ZTA in telecom networks has been recognized in the 3GPP examination of zero trust principles in mobile networks [4], Alliance for Telecommunications Industry Solutions (ATIS) Enhanced Zero Trust and 5G paper [5], and US DHS CISA, Security Guidance for 5G Cloud Infrastructures [6].

Threats are constantly evolving and now leveraging artificial intelligence (AI) to conduct more sophisticated attacks. MNOs and governments are motivated to achieve a ZTA in critical infrastructure, including mobile networks. This, however, is not achieved through applying industry standards alone. While 3GPP standards provide foundational capabilities for zero trust in network functions (NFs) and interfaces, operational security is typically not in the scope of standardization. Correct implementation and configuration tailored to match each MNO's network context, are crucial at network deployment and during network operations. Ericsson products provide necessary capabilities to deploy a ZTA and are on the ZTA journey along with MNOs and industry bodies, including O-RAN Alliance, 3GPP, and ATIS. Achieving a ZTA that complies with all the NIST seven tenets of zero trust and CISA ZTMM requires a high level of automation and visibility in mobile network security operations. Ericsson also provides a security management solution to help automate and orchestrate security operations toward achieving a ZTA that protects mobile networks from external and internal threats.

This whitepaper provides guidance for MNOs to implement key ZTA functions highlighted in the CISA ZTMM [3]: visibility and analytics, automation and orchestration, and governance - across the entire mobile network in operations. This whitepaper concludes that a tailored security operation and management approach designed for the telecom sector is required to address the complex nature of telco. Such a security management approach enforces continuous micro-perimeter protection of all network assets and diverse infrastructure, covering security posture management, threat detection, and anomaly detection with telco-specific threat intelligence, vulnerability management, and enhanced visibility through integration with the MNO's existing security processes and systems such as SOAR and SIEM.

The evolution of Zero Trust Architecture

Traditional cybersecurity architecture has been perimeter-based, which relies on controls for external subjects accessing internal resources. However, the adoption of cloud computing and continuous integration, development, and deployment pipelines in critical infrastructure introduces new security challenges. Perimeter-based security is no longer sufficient because the network requires protection from both external and internal threats, including APTs from sophisticated adversaries.

This is where ZTA principles come in. ZTA is a comprehensive approach to network and data security that covers operations, endpoints, network functions, hosting environments, interfaces, and interconnected infrastructure, protecting assets as micro-perimeters across the entire network. Zero trust is an architectural approach that protects data in transit, at rest, and in use.

ZTA has become central to securing critical infrastructure, including mobile networks. A mobile network with a ZTA provides protection from external and internal threats with the assumption that a threat actor has established a foothold inside the network. There is no implicit trust granted to any asset based on ownership, physical location, or network location. ZTA controls include identity and access management, the principle of least privilege, multi-factor authentication, mutual authentication, network segmentation, micro-perimeters, and continuous monitoring and logging capable of detecting and defending against a range of external and internal threats.

The telecom industry has begun to move from centralized and tightly coupled hardware and software architectures towards more open and distributed systems. A key move in this direction has been the migration to cloud-native network functions in 5G Standalone (SA) core and Open RAN. Vendors and MNOs have also moved to higher velocity continuous

integration and deployment processes. These introduce internal threats that need ZTA to complement perimeter-based security.

Importantly, ZTA is not only about the threats of today, but it is also about protecting against the threats of tomorrow. The relentless improvement of computing power and breakthroughs in the field of artificial intelligence (AI) could lead to the creation of threats and scale of attacks that do not exist today. The best way to prepare for that future is to put in place a system that assumes that such attacks will be realized and provides the ability to identify, protect, detect, respond, and recover from these evolving attacks.

Guidance for implementing a ZTA

MNOs need to implement effective cybersecurity and resiliency practices for zero trust to be effective. When complemented with existing risk-based cybersecurity policies and guidance, ZTA can strengthen the mobile network's security posture.

A good starting point for an MNO to implement ZTA is by referring to the seven tenets published by NIST and as shown in Figure 1.

T1. All data sources and computing services are considered resources
T2. All communication is secured reagrdless of network location
T3. Access to individual resources is granted on a per-session basis
T4. Access to resources is determined by dynamic policy
T5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets
T6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed
T7. The enterprise collects information about the current state of assets, network infrastructure and communications and uses it to improve its security posture

Figure 1: NIST's seven tenets of zero trust [1]

NIST's seven tenets of zero trust can be summarized for mobile networks with the following four principles of ZTA

- Network functions and architectural elements are resources secured as micro-perimeters.
- Trust is not assumed for any subject, whether human user or network asset, attempting to access a resource. Authentication and authorization are enforced on a per-session basis for external and internal subjects.
- Confidentiality and Integrity protection is provided for data in transit on external and internal interfaces, data at rest, and data in use.
- Continuous monitoring, logging, and alerting are implemented to detect security events and enforce dynamic security policies.

Achieving a ZTA is an incremental process and should be viewed as a journey implemented in stages. CISA ZTMM [3] is published to complement ZTA by offering a roadmap for organizations to assess their current maturity level and provide guidance on steps to incrementally progress to higher maturity stages: Traditional, Initial, Advanced, and Optimal. These stages, as shown in Figure 2, are achieved for each of the five pillars – Identity, device, networks, applications and workloads, and data – and three cross-cutting functions – Visibility and analytics, automation and orchestration, and governance. These cross-cutting functions align with NIST tenets 4, 5, and 7 mentioned above.

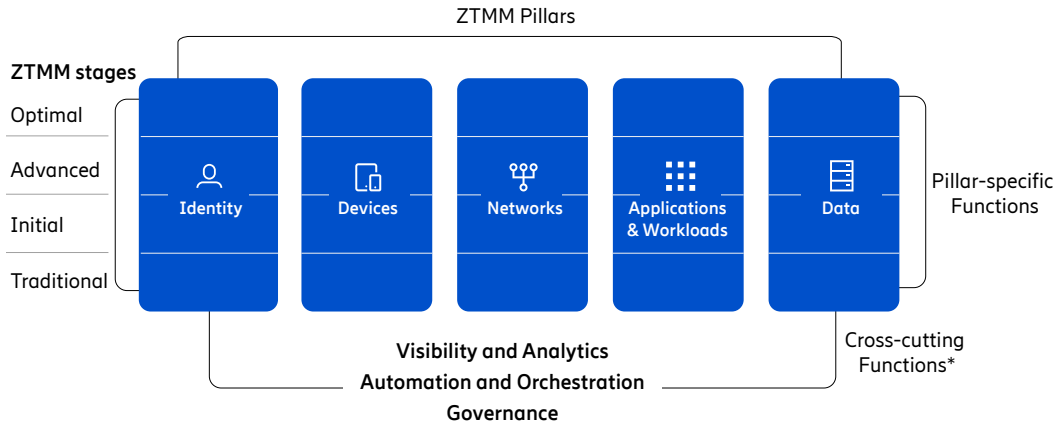


Figure 2: Summary of CISA ZTMM [adapted from 3]

ZTA implementation challenges for mobile networks

Mobile networks, being critical infrastructure, require a higher security posture than a typical enterprise network and the general guidance to achieve ZTA requires adaptation to the mobile network context. A difference between mobile networks versus enterprise networks is the presence of three planes in mobile networks – user, control, and management planes – and their specific context, standards, and protocols [7]. For example, while 3GPP specifications provide capabilities to address tenets 1, 2, 3, and 6, these are specified differently across the user data, control data, and management (OAM) data planes. A detailed analysis by ATIS [4] illustrates these telco-specific use cases, emphasizing confidentiality and integrity for the user and control planes, and availability for the management plane due to the large impacts of attacks.

Implementing standardized security controls across these planes while upholding mobile network service levels is complex and requires specialized knowledge and tools. To guide MNOs in implementing ZTA for improved cybersecurity and regulatory compliance, the process can be broken down into the four steps illustrated in Figure 3 - Secure approach, Secure products, Secure deployment, and Secure operations.

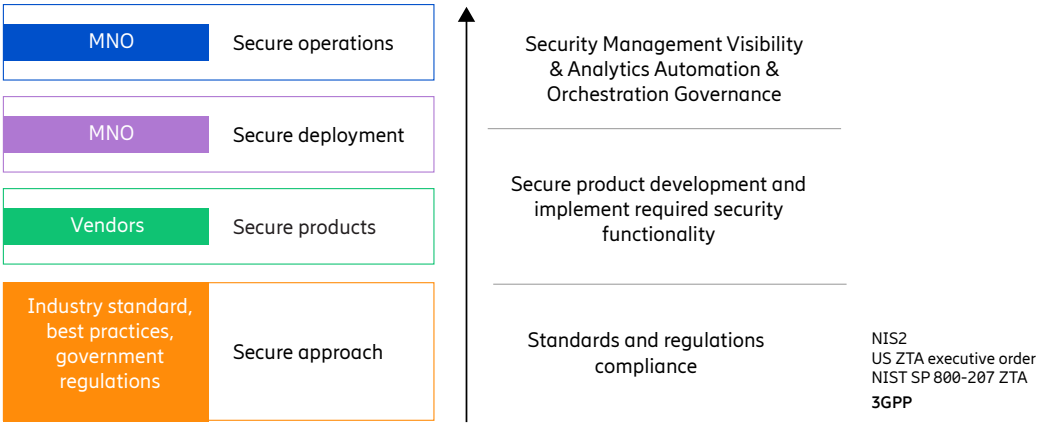


Figure 3: Building blocks for a secured mobile network

Secure Approach - The process begins with aligning with regulatory and standards guidelines, shaping a security strategy aimed at a ZTA security posture.

Secure Products - Vendor products are built according to industry standards, setting the stage for the implementation of security controls.

Moving forward in the process, MNOs set security governance strategies tailored for their mobile network context to secure the network at deployment and during operations. The ZTMM cross-cutting functions are needed to maintain consistent and scalable operational security across the entire network.

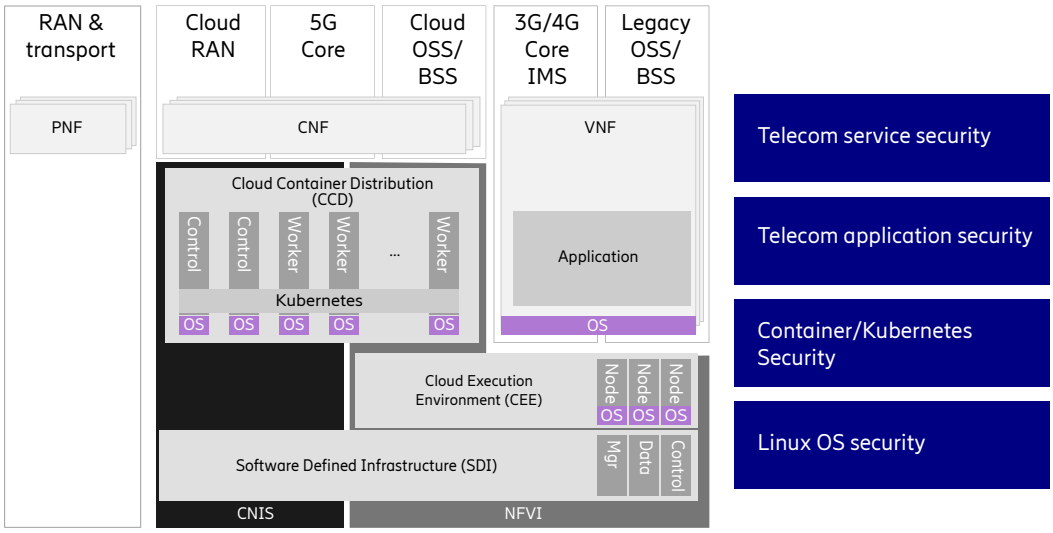
Secure Deployment - This step involves proper implementation and configuration of security controls where automation can enforce micro-perimeter security and improve the scalability and configuration accuracy across the network.

Secure Operations - During operations, MNOs ensure security visibility, monitoring, enforcement, and reporting aligned with NIST tenets 5 and 7:

- T5: The enterprise [service provider] monitors and measures the integrity and security posture of all owned and associated assets.
- T7: The enterprise [service provider] collects information about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

To achieve a ZTA, additional security management functionality is needed to complement existing mobile standards and meet the needs of security operations. Additionally, in the real world, the type and format of security-related data, such as security configuration and security event data, are not confined to the 5G System itself and are highly dependent on deployment specifics, such as the platforms and technologies in use. Addressing this challenge requires a dedicated security management function that bridges the security view across heterogeneous elements, such as the physical, virtualized, containerized NFs and radios running in a mobile network, as shown in Figure 4. Moreover, the various cloud deployment models - private, public, or hybrid - bring operational challenges to maintain

a high-security baseline across different cloud platforms [8]. The manual configuration of network assets and interfaces also poses practical challenges, which can be heightened by having diverse platforms, technologies, and vendors. This process is time-consuming and increases the risk of misconfigurations and policy conflicts, which is a significant threat highlighted in reports, including ENISA's threat landscape [9].



CNIS = Cloud Infrastructure Solution
NFVI = Network Function Virtualization Infrastructure

Figure 4: MNO technology stack

To address these issues, a security management function that bridges the security view across heterogeneous elements and automates the monitoring of robust security configuration plays a vital role in ensuring a solid security posture across the network, consistent with the ZTA principles. This security management function also serves to assess and monitor the implementation of a ZTA security posture compliance to regional security regulations such as NIS2.

Security Management to achieve ZTA maturity

In the landscape of mobile networks, ensuring a robust implementation of ZTA relies on effective security management to support secure deployment and operations. Building upon the challenges laid out in the previous chapter, this chapter illustrates the ideal controls required in a security management function. Furthermore, it provides insights into how an MNO can evaluate and enhance their current security management functions and governance to achieve ZTA maturity within their mobile network operation.

Security Controls for ZTA

Security management supports NIST's Cybersecurity Framework (CSF) with the Govern, Identify, Protect, Detect, Respond, and Recover functions. These six functions can be achieved by adopting the 12 ZTA critical control groups identified by ATIS in [5] and shown in Figure 5. These controls can be implemented through a combination of mobile industry standards and tailored operational security measures.

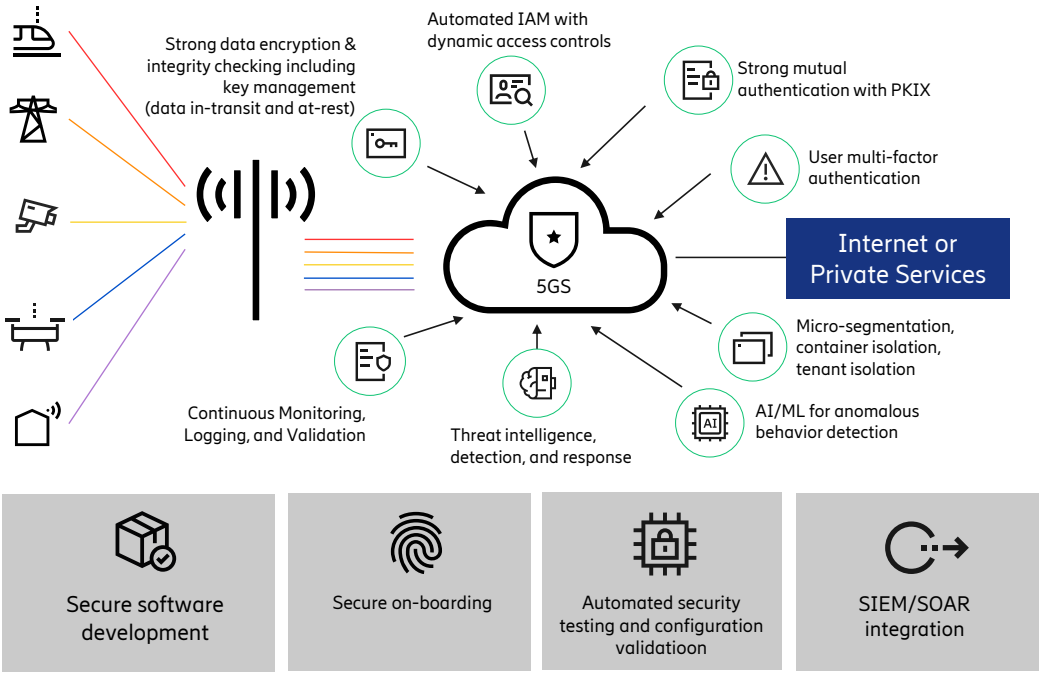


Figure 5: ZTA critical control groups [5]

The security management function enforces the security controls implemented across all mobile network domains (for example, RAN, Core, OSS, BSS, cloud infrastructure, and transport) to be in place and ties them into security operations workflows. The security management function also has its own security functions, such as posture management, continuous monitoring utilizing threat intelligence and AI/ML, and certificate automation and PKI.

Security management automates the process of onboarding network assets to the monitoring platform, orchestrates the protect and detect activities by including threat indicators based on multiple sources (for example, logs, cloud-native events, vulnerabilities, configuration status, and so on), and provides enriching context information to assist human and automated responses. MNOs can achieve round-the-clock visibility into the network security posture. This involves gathering and analyzing network-wide configuration status, logs, and events horizontally, while also comprehensively covering the entire MNO technology stack vertically. This approach supports the governance and monitoring objectives of ZTA.

Implementing ZTMM in mobile networks

The cross-cutting functions of the CISA Zero Trust Maturity Model (ZTMM) – Visibility and Analytics, Automation and Orchestration, and Governance – hold relevance for the telecommunications industry, especially concerning security management functions. The security management platform should meet the NIST tenets and CISA cross-cutting functions for the network to achieve a ZTA.

Implementing ZTA is a journey that runs through the stages of 'Traditional,' 'Initial,' 'Advanced,' and 'Optimal'. It evolves from static policies and manual controls with limited visibility to dynamic policies with automated controls that leverage AI and continuous monitoring to gain network-wide visibility and faster response. Table 1 provides CISA ZTMM definitions for these three cross-cutting functions, with recommended tailoring for mobile networks.

Cross-cutting capabilities	Traditional	Initial	Advanced	Optimal
Visibility & Analytics	• Manually collect limited logs across network with low fidelity and minimal analysis	• **Automate the collection and analysis of logs and events** for mission critical functions • Regularly assess processes for gaps in visibility • **Continuous monitoring of security configurations**	• Expand the automated collection of logs and events **network-wide (including virtual environments)** for centralized analysis **that correlates across multiple sources** • **Telecom specific threat detection** • **Attack surface assessment**	• Maintain comprehensive visibility network-wide via centralized dynamic monitoring and advanced analysis of logs and events • **Risk profiles for network functions**
Automation & Orchestration	• Rely on static and manual processes to orchestrate operations and response activities with limited automation	• Automate orchestration and response activities in support of critical mission functions • **Automate selected manual tasks** • **Managing backhaul IPsec certificates**	• Automate orchestration and response activities network-wide, leveraging contextual information from multiple sources to inform decisions • **Automate selected processes** • **Certificate automation for mTLS**	• Orchestration and response activities dynamically respond to network-wide changing requirements and environmental changes • **Automated and streamlined processes**
Governance	• Implement policies in an ad hoc manner across the network • Policies enforced via manual processes or static technical mechanisms	• Define and implement policies for telco network-wide enforcement with minimal automation and manual updates • **Select 3GPP security controls for implementation**	• Implement tiered, tailored policies **network-wide and leverages automation** where possible to support enforcement • Access policy decisions incorporate contextual information from multiple sources	• Implements and **fully automates** network-wide policies that enable tailored local controls with **continuous enforcement and dynamic updates**

Regular text = adopted from ZTMM
Bold text = addition of cross-cutting functions for mobile network context
Bold underlined = highlight of end-to-end security management and automation required in ZTMM

Table 1. Cross-cutting ZTA maturity for the mobile network (adapted from ZTMM [3])

The Traditional stage is the perimeter-based security and the Initial stage is the first step on the ZTA journey. The following points provide recommendations to step through the stages of the ZTMM:

- **To reach the Initial stage** – Conduct a comprehensive risk assessment and define a targeted security posture accordingly. Implement continuous monitoring to compare the current security posture with the intended target. Emphasize the automation of log collection and analysis for NFs and the underlying cloud infrastructure.
- **To reach the Advanced stage** – Automate asset discovery for NFs, for example in the 5G Core and Radio Access Network (RAN). Enhance threat detection capabilities by deploying comprehensive methods, encompassing both agent-based and log-based detection, ensuring complete coverage. Implement mechanisms to identify rogue assets within the network that could potentially impact service availability. For effective network function identity management, establish a system that oversees the distribution, enrollment, and enforcement of public key infrastructure (PKI) certificates, while facilitating secure communication between NFs.
- **To reach the Optimal stage** – Establish comprehensive centralized security visibility and control across all telco nodes. Implement dynamic monitoring, enforcement, and policy updates with the help of AI/ML in response to threats or regulatory changes.

Security management should facilitate the MNO's progression through this maturity journey, adapting to evolving technology and shifts in the threat landscape. For instance, while a patch for a vulnerability might require time to be disseminated across all software, the security management tool can promptly adjust and enforce the acceptable baseline security configuration to mitigate the potential risk posed by the potentially unpatched vulnerability.

Ericsson's journey toward ZTA

Ericsson embraces ZTA to bolster telecom security, providing support for MNOs striving to achieve their targeted security postures while addressing ZTA guidance from regulatory agencies. Ericsson has set out a program to facilitate the realization of zero trust in the telecom network, addressing individual product levels, refining processes, and complementing 3GPP standards with dedicated products essential for establishing a robust ZTA in 5G. Ericsson is also leading industry standards bodies to establish requirements for a ZTA in 5G and 6G networks.

Product Security

The Security Reliability Model (SRM) [10] is Ericsson's comprehensive framework for developing products and solutions. It encompasses specific requirements and procedures for security functions and controls, along with guidelines for security assurance activities and the provision of security services. The security functions include requirements for the baseline security level and architecture rules and guidelines and many of them can be mapped directly to the NIST zero trust tenets. The SRM requirements align with 3GPP SCAS requirements, such as TS 33.117, establishing a solid foundation for product and network security.

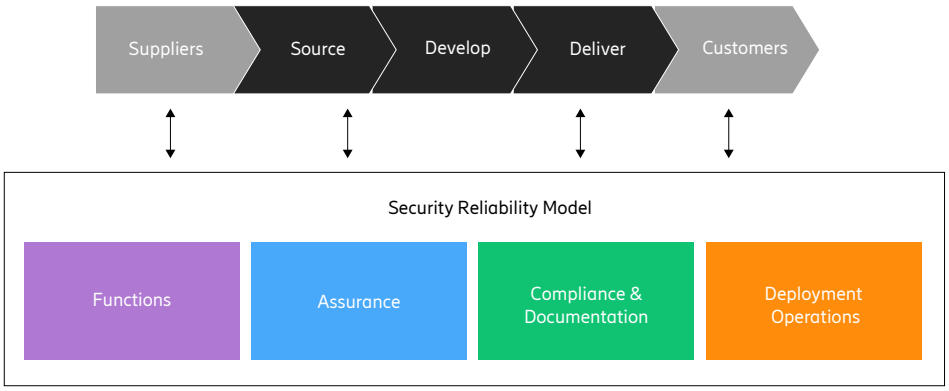


Figure 6: The Ericsson Security Reliability Model

Deployment security practices

The SRM mainly covers product security. To deploy secure products in a network targeting a ZTA, each NF and its interfaces must be implemented with the right security controls and security configuration to establish it as a micro-perimeter. Each NF can be deployed with secure by default settings automatically verified by Ericsson Security Manager (ESM) to identify and correct any configuration drift. Additional and contextualized controls ensure proper confidentiality and integrity protection along with adequate access controls and authentication mechanisms for external and internal interfaces. Manual security checklists can be replaced by automation tools for configuring the baseline at deployment.

Security Management of network in operation

While mobile industry standards specify security architecture and security controls for individual network functions and interfaces, their scope does not cover the essential end-to-end aspects of network operations at runtime, including automation, continuous monitoring and reporting, dynamic policy orchestration, and vulnerability assessment and management, which are part of a ZTA. These have been pointed out by ATIS as the recommended capabilities that mobile networks need to implement to comply with a ZTA.

Ericsson Security Manager (ESM) is a cybersecurity platform tailored for mobile networks to achieve a ZTA with these recommended capabilities. Its capabilities integrate with multi-vendor products, addressing operational security and simplifying the implementation of ZTA across different technologies and vendors. ESM acts as the foundation to elevate zero trust maturity by providing ZTMM cross-cutting functions - visibility and analytics, automation and orchestration, and governance - currently not covered by industry standards. Integrating ESM in an MNO's network ensures that security functionality included in industry standards and regulatory guidance is correctly implemented.

Conclusion

Regulators, MNOs, NF vendors, and industry standards bodies are pursuing a ZTA for mobile networks, which are considered critical infrastructure by many governments since they serve as the backbone of other digital services. NIST SP 800-207 and CISA ZTMM offer guidance that goes beyond the conventional focus on perimeter-based defense to achieve a ZTA with micro-perimeters that protect against emerging external and internal threats.

The CISA ZTMM cross-functional capabilities - visibility and analytics, automation and orchestration, and governance - are vital for achieving higher maturity in ZTA. These cross-functional capabilities and operational security are not covered in mobile industry standards but can be gained by deploying a dedicated security management tool or capability. This whitepaper provides guidance to implement security management to achieve a ZTA tailored to the unique context of mobile networks.

To successfully achieve ZTA in mobile networks, all industry stakeholders should collaborate on cybersecurity implementation, with consideration of network performance and availability. In North America, ATIS has embraced ZTA for mobile networks by consolidating 12 security controls and providing a set of recommendations for the industry to achieve a ZTA in 5G networks [5].

Ericsson Security Manager is built as a security management function to meet this challenge, automating continuous enforcement of micro-perimeter protection from network deployment to operations and, thereby, facilitating the realization of a robust ZTA framework in mobile networks. Ericsson enables MNOs to achieve ZTA through three axes:

- securing products through the SRM,
- implementing security measures throughout delivery and deployment, and
- simplifying network security operations using the ESM, the single management point from which to implement, monitor, and report on ZTA across the end-to-end 5G network.

Implementing ZTA in mobile networks requires cybersecurity knowledge and deep domain expertise to meet regulatory guidance. With Ericsson's robust product development and deployment practices, alongside utilizing tools like ESM as a telco zero trust keystone, MNOs can attain both cyber resilience and regulatory compliance within a ZTA.

References

1. Zero Trust Architecture (ZTA), NIST SP 800-207, US DoC NIST, September 2020
2. NIS2 Directive, Digital Strategy, European Commission, 2023 https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.
3. Zero Trust Maturity Model (ZTMM), version 2.0, US DHS CISA, April 2023
4. "Technical Report 33.894: Study on applicability of the zero trust security principles in mobile networks (Release 18)", 3rd Generation Partnership Project (3GPP), July 2023
5. Enhanced Zero Trust and 5G, Alliance for Telecommunications Industry Solutions (ATIS), July 2023, https://www.atis.org/resources/enhanced-zero-trust-and-5g/
6. Security Guidance for 5G Cloud Infrastructures, Cybersecurity and Infrastructure Security Agency (CISA), October-November 2021, https://www.cisa.gov/resources-tools/resources/security-guidance-5g-cloud-infrastructures
7. Security in 5G RAN and Core Deployments, Ericsson, 2020, https://www.ericsson.com/en/reports-and-papers/white-papers/security-in-5g-ran-and-core-deployments
8. 5G security for public and hybrid cloud deployments. Ericsson, 2022. https://www.ericsson.com/en/reports-and-papers/further-insights/5g-security-for-hybrid-cloud
9. European Union Agency for Cybersecurity. "Threat Landscape for 5G Networks." ENISA, 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks
10. The Ericsson Security Reliability Model - SRM

Authors

Hans Byström is Technology Director at Ericsson Security Solutions. He has more than 20 years of experience in telecommunications system architecture, product development, and strategy. In his current role, he leads the development of technology strategies and system evolution plans for security management functions in the mobile network. Hans has four patents in the areas of mobile network service management and media transport. He holds an MSc in electrical engineering from the Royal Institute of Technology (KTH), Stockholm, Sweden.

Hsin-Yi Chen is a Security Solution Manager at Ericsson. In her current role, she consults security operational challenges with customers across the globe, advocating secure network deployment and operations through security automation and risk mitigation with Ericsson's security solution. Hsin-Yi holds a joint master's degree in Security & Cloud Computing from Aalto University and the Norwegian University of Science and Technology, specializing in wireless communication security. She has published several peer-reviewed papers on mobile network security in international conferences and journals.

Scott Poretsky is Ericsson North America's Director for Security, Network Product Solutions. He has over 30 years of industry experience in a variety of networking and security technologies. Scott is currently working in the areas of 5G security, Open RAN security, cloud security, and zero trust architectures. Scott serves as Co-Chair of O-RAN Alliance's Security Working Group (WG11) and on the Advisory Board for the IEEE ComSoc technical committee for Communications Quality and Reliability (CQR). He also recently completed a term as Co-Chair of the ATIS 5G Zero Trust study group. Scott has represented Ericsson in government-industry collaboratives on Open RAN security at FCC CSRIC VIII and the NSA/CISA sponsored Enduring Security Framework (ESF) and served on the NSTAC subcommittee for Communications Resiliency. Scott has one patent, numerous published papers, and numerous invited talks. Scott is a Certified Information Systems Security Professional (CISSP) and Certified Cloud Security Professional (CCSP). He earned an MSEE from the Worcester Polytechnic Institute (WPI) and a BSEE from the University of Vermont.