ericsson.com/
5g-security-for-hybrid-cloud

5G security for public and hybrid cloud deployments

September 2022

Introduction

Traditionally, mobile networks have been considered secure because they are integrated systems at the mobile network operator's site and run on their own infrastructure.

Contents

Authors:
Scott Poretsky
Peter Linder
Haseeb Akhtar

Acknowledgements:
The authors would like to thank and acknowledge the contributions from their colleagues: Danielle Francis from North America Marketing, Ari Pietikäinen from Security Technologies, Gordon Rawling from Cloud Product Marketing, Patrik Birgersson from Intelligent Automation Platform, Joakim Jardal from Cloud RAN Product, Gagan Shori from Customer Security and Ravi Vaidyanathan from Global Customer Unit HCPs.

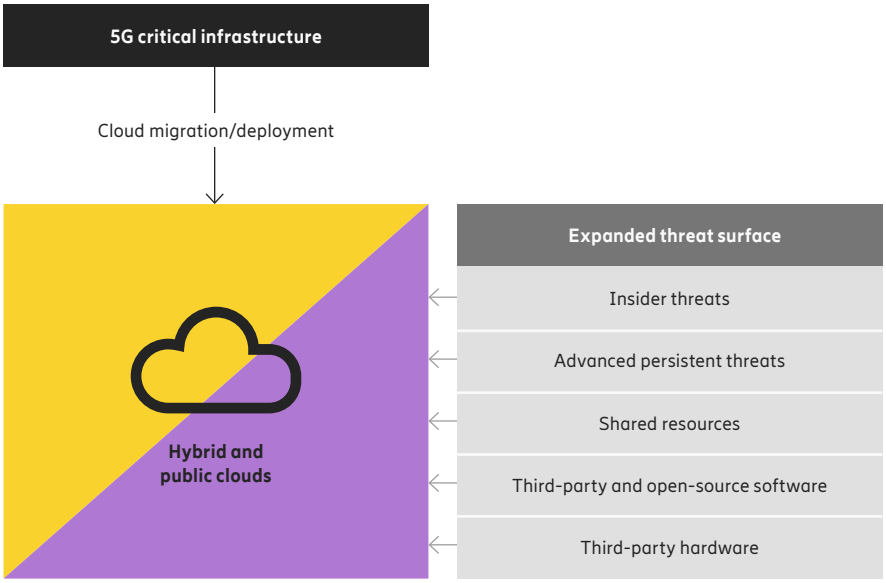
Network outages and privacy compromises are stark reminders that mobile networks are a critical infrastructure, providing the foundations for commerce, manufacturing, education, emergency services, utilities and mission-critical networks.

As we evolve from traditional on-premise 5G networks, to 5G networks running in public or hybrid cloud deployments, we see the 5G attack surface expanding. This is due to the inherent cloud characteristics of third-party infrastructure in a multi-tenant environment managed by another third-party. The cloud opens up the possibility for greater threats of lateral movement, reconnaissance and advanced persistent threats from nation-state, criminal and internal threat actors.[1]

Cloud security must therefore evolve to combat the realities of today's threat landscape and the reduced risk tolerance due to the impact of an exploit or attack. A new approach to securing mobile networks is also required. Protection must be provided from internal and external threats, and it must have a zero-trust architecture, where security micro-perimeters are established to protect network functions, applications and sensitive data.

Cloud security is a key consideration for mobile network operators (MNOs) when deploying cloud-native 5G network functions in public and hybrid clouds. Ericsson helps MNOs to manage their four main cloud security responsibilities: select, purchase, configure, and maintain. These are defined by nine regulatory bodies and standards and specifications bodies shaping cloud security, and the cloud infrastructure providers' own security offerings.

Figure 1: 5G critical infrastructure has expanded the threat surface in the cloud



[1] OpenRAN – 5G hacking just got a lot more interesting – MCH2022, July 24 2022

Risks and challenges of cloud migration

Hyperscale Cloud Providers (HCPs) have expertise in providing cloud services to enterprises and government agencies. However, 5G critical infrastructure requires a higher security baseline, which is achieved through due diligence and cyber hygiene.

Delegation of security responsibilities can be complicated in hybrid clouds, such as multi-access edge compute, and multi-cloud deployment architectures.

While the Cloud Shared Responsibility Model provides guidance for security responsibility, a lack of a common security framework for cloud deployments of 5G critical infrastructure puts further responsibilities on the MNO.

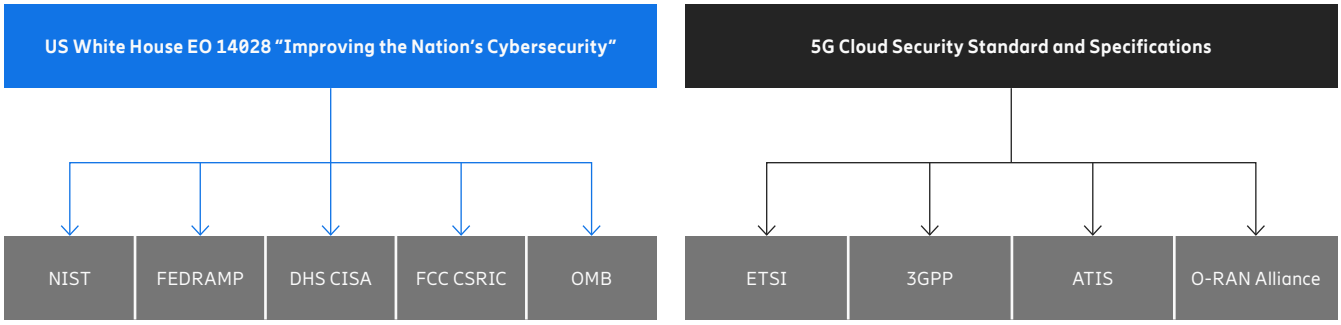
> "For hybrid clouds, special attention needs to be paid to areas such as compliance and data security, which are of concern due to the interconnection between the public and private clouds."
>
> **Cloud Security Alliance**[2]

Supporting businesses and mission-critical services requires a cellular infrastructure that is more resilient toward threats to confidentiality, integrity and availability. Migrating to a cloud infrastructure allows telco workloads with low tolerance for outage to be available when properly designed to take advantage of inherent redundancy of the cloud.

The importance of security considerations for mobile networks deployed on cloud infrastructure is expected to grow as 5G use cases take on more significance in society. A key concern when moving network functions to the cloud is the introduction of new risks and system vulnerabilities that can be exploited by a malicious external or internal threat actor. MNOs will need to mitigate these risks when migrating to the cloud without having full control of infrastructure.

Network infrastructure is an important part of national security agendas and needs to be protected against criminal actors and adversarial nation states. Future networks will rely on trusted vendors that are vetted by MNOs and governments. MNOs will need to implement a zero-trust architecture for cloud deployments designed to protect against external and internal threats.

Figure 2: US Government guidance for standardization of 5G cloud security



[2]Hybrid Cloud Security – Cloud Security Alliance, September 26 2022

5G: Raising the cloud security bar

Nine organizations influence global and local security specifications and solutions considered for deployment in North America.

Nine organizations provide global and local security specifications and solutions considered for deployment in North America. They provide global and national guidance for 5G security with increasing emphasis on cloud security and zero-trust architecture.

National Institute of Science and Technology[3] **(NIST)** evaluates and improves cybersecurity.

Federal Risk Authorization Management Program[4] **(FedRAMP)** enables the adoption of secure cloud services for the federal government and promotes security for all government cloud services.

Cyber Security and Infrastructure Security Agency[5] **(CISA)** works to reduce risk for cyber and physical infrastructure. It has also developed guidelines for 16 critical categories over generic cloud infrastructure security.

Communications Security, Reliability and Interoperability Council[6] **(CSRIC)** improves recommendations to FCC on how communications systems can be made more secure, reliable, and interoperable.

The White House Office of Management and Budget (OMB) has developed guidelines for federal agencies deploying cloud services to ensure zero trust is supported based upon risk analysis.

European Telecommunications Standards Institute (ETSI) Technical Committee Cybersecurity[7] **(TC Cyber)** offers "market-driven cybersecurity standardization solutions, along with advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators."

Third Generation Partnership Project[8] **(3GPP)** is an umbrella organization bringing together contributions from seven organizations into holistic reports and specifications. 3GPP TR 33.848 has identified 30 key areas for security impacts of virtualization.

Alliance for Telecommunications Industry Solutions[9] **(ATIS)** is forming a working group for 5G security specifications.

O-RAN Alliance is developing specifications for open, disaggregated, intelligent, virtualized, and fully inter-operable Radio Access Network (RAN).

Ericsson's strategy is to support MNO's and cloud providers by leveraging the US DHS CISA security framework for 5G cloud deployments. Ericsson will continuously offer guidance through contributions and collaborations to integrate additional parts into a holistic security solution framework for 5G and beyond to ensure that 5G critical infrastructure is secure in the cloud.

[3] National Institute of Science and Technology, U.S. Department of Commerce, September 26 2022
[4] The Federal Risk Authorization Management Program, Joint Authorization Board (DoD, DoHS, GSA), September 26 2022
[5] Cyber Security and Infrastructure Security Agency, September 26 2022
[6] Communications Security, Reliability, and Interoperability Council, FCC, September 26 2022
[7] Technical Committee Cyber, ETSI, September 26 2022
[8] Third Generation Partnership Project, September 26 2022
[9] Alliance for Telecommunications Industry Solutions, September 26 2022

MNOs, their offering, and their security

MNOs have four main responsibilities when it comes to deploying 5G security for the public/hybrid cloud, which revolve around selection, purchasing, configuration and maintenance.

While preparation is usually regarded as being key for success, the reality is that often MNOs learn about the implications of 5G security realities in their first public cloud infrastructure.

Selecting cloud security
The choices an MNO needs to make after establishing a cloud security posture suitable for critical infrastructure are:

1. Choose the required security capabilities with the help of a risk-based analysis. A Risk-based analysis for selection of security controls will also consider the cost of the control weighed against the risk level.
2. Next, choose the service provider that best aligns with the security posture, wanted security controls, and deployment cost.
3. The MNO fills in the gaps by bringing its own security controls, which is also part of the cost consideration during the risk analysis.

The Cloud Service Agreement must explicitly state the security controls to be provided by the HCP. The MNO must periodically repeat the risk analysis to address evolving threats and security controls.

Cloud security procurement
The security considerations vary with deployment strategies:

- A single public cloud deployment requires security controls for protection from other tenants sharing the same resources and workloads designed for failover to achieve resiliency.
- Multi-cloud deployments require a higher level of due diligence to ensure the deployment has consistent security controls across all cloud service providers, so that the deployment has one security posture. Mobile users should have a seamless user experience, including security.
- Hybrid clouds add an additional level of complexity where the private and public cloud security offerings need alignment.

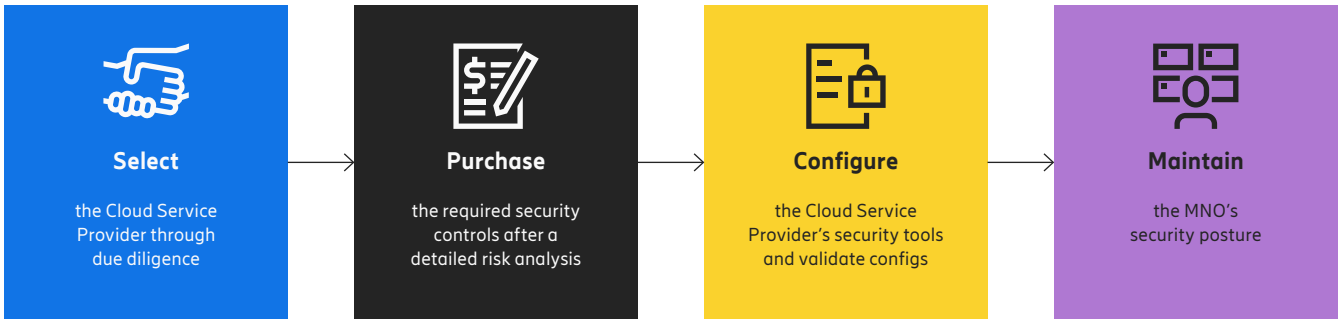
Public and hybrid cloud security offerings
A traditional MNO network is an integrated system with MNO-owned infrastructure and MNO-controlled access to facilities and networks. Public and hybrid cloud introduces new security risks as the infrastructure could be owned, operated and accessed by a third party in a facility controlled by a third party.

So, what are the main differences in security between public and hybrid clouds?

There are three options for deploying 5G network functions over private and public cloud infrastructure:

- In a private cloud, the MNO has full control of applications, network functions, and infrastructure.
- In the public cloud, 5G critical infrastructure runs on third-party infrastructure with shared resources managed by a third-party – this increases the threat of internal attacks.
- Hybrid cloud can make the Cloud Shared Responsibility Model less clear – this can add security complexity due to challenges in clarifying security responsibilities and ensuring a consistent security posture.

Figure 3: MNO's four security responsibilities



Understanding the key considerations for MNOs migrating to hybrid/public cloud will ensure critical requirements are in place, such as micro-segmentation and tenant isolation, configuring security controls, including Identity and Access Management (IAM) and firewalls, and continuous monitoring and logging.

Cloud security configuration
A key question is, who is responsible for configuring the procured cloud security solution? Even when an MNO procures security solutions from cloud service providers, they still retain responsibility for proper configuration of the security controls, including IAM and firewalls. The MNO is accountable for ensuring sensitive and private data is secure, including access and encryption.

Ongoing cloud security maintenance
MNOs are also responsible for maintaining the security solutions, including tasks such as periodically performing risk-based analysis to address evolving threats and security controls, configuration of security tools, and ensuring all software is upgraded to the most recent versions. In addition, MNOs are responsible for recognizing and patching critical vulnerabilities before they can be exploited. It's noteworthy that MNOs are still responsible for ensuring these tasks are completed, even when it comes to third-party software and applications provided by the cloud provider.

MNOs have three HCP security options: a Security Hub with Amazon Web Services (AWS) public clouds, a Security Center with Azure public clouds or a Security Command Center with Google Cloud Platform (GCP) public clouds.

Public clouds are in the introduction stage of carrying cloud-native network functions for mobile core and RAN. Private clouds are ahead of public clouds in supporting mobile network functions and meeting telco security requirements. Each public cloud provider tailors their security offering to their customer bases' unique needs.

It is crucial that MNOs push to raise the security bar for all HCPs to meet business and mission-critical needs.

Public cloud offerings

AWS' offering for cloud security on a cloud-native network functions

- AWS Security Hub
- An example is the DISH green field 5G network build, the first 5G network function reference[10]

Azure's offering for cloud security on a cloud-native network function

- Azure Security Center
- An example is the AT&T migration from private to public cloud, the first 5G network function reference[11]

GCP's offering for cloud security on a cloud-native network

- GCP Security Command Center
- An example is the Deutsche Telekom Standalone (SA) 5G Core, the first 5G network function reference[12]

[10] Telco meets AWS cloud: Deploying DISH's 5G network in AWS cloud, February 27, 2022
[11] AT&T moves 5G mobile network to Microsoft cloud, June 30, 2021
[12] Deutsche Telekom and Google Cloud Sign Partnership agreement focused on network transformation, July 12, 2022

Cloud security controls

Ericsson has identified 20 different security categories that are relevant for the deployment of cloud-based network functions for 5G networks. Together, they represent a comprehensive set of security categories that provide maximum protection in 5G networks.

With increased risk of internal threats to critical infrastructure deployed in the cloud, it becomes necessary to secure the deployment with a zero-trust architecture providing protection from internal and external threats.

Ericsson consider these 10 cloud security categories to be a mandatory baseline for securing 5G network deployments with a zero-trust architecture on any cloud infrastructure:

- continuous monitoring, logging, and alerting
- micro-segmentation and micro-perimeters
- principle of least privilege
- automated Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- public key infrastructure (PKI) based mutual authentication
- sensitive data encryption
- Threat Detection and Response (TDR)
- SIEM/SOAR integration
- DevSecOps and Continuous Integration/Continuous Deployment (CI/CD)

For 5G network functions, four additional cloud security categories are recommended and they are available from public cloud providers. A risk analysis, including cost, will determine if these controls are provided by the MNO or service provider:

- key management and hardware-based key storage
- secure APIs and API gateway
- compliance audit to regulations and industry standards
- cloud security posture management

Figure 4: The 20 security capabilities for 5G in 3 tiers

The variation in support between cloud providers for these recommended controls is significantly different than for the 10 mandatory categories. Together with the 10 mandatory categories, the 14 in total represent the largest subset MNOs can expect for 5G network functions in a hybrid or public cloud infrastructure.

5G security standardization in six additional areas completes the list:

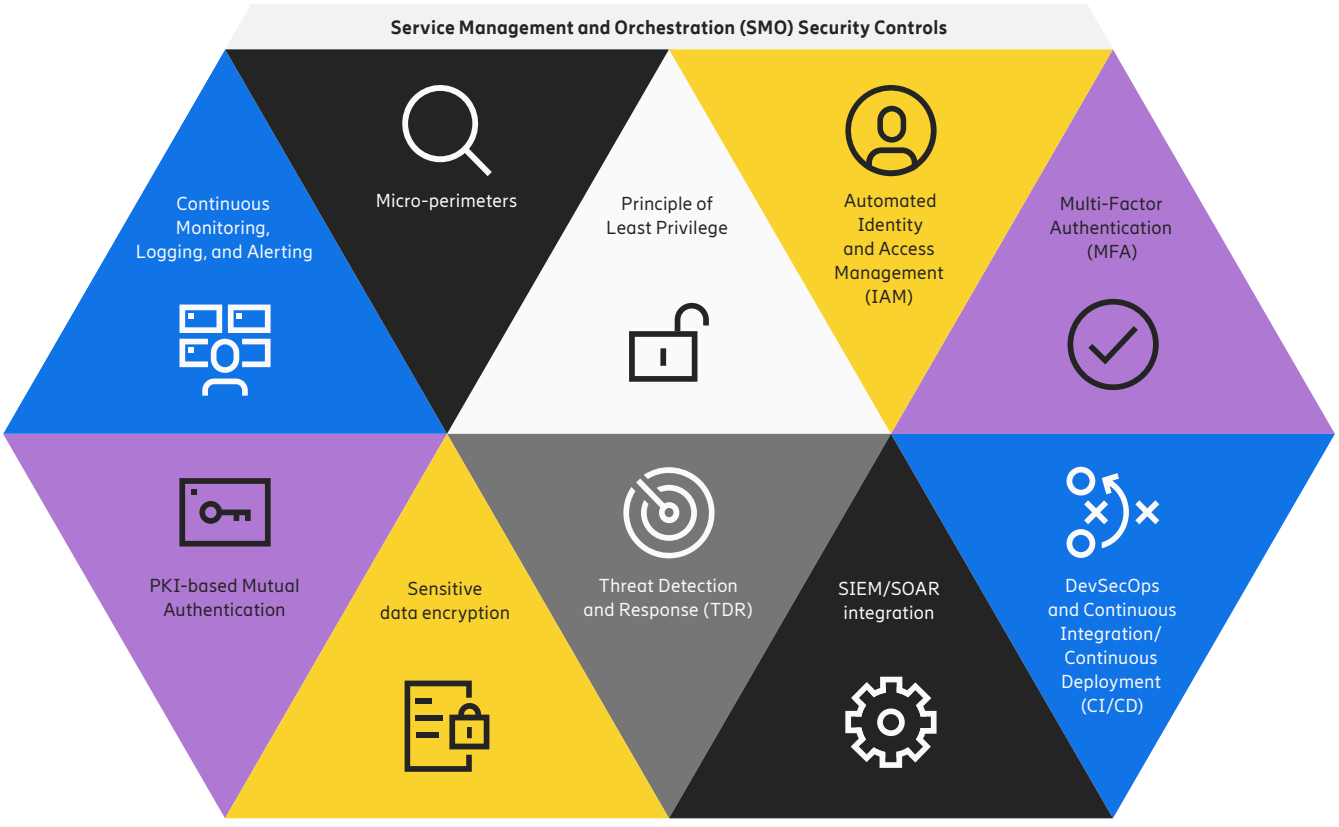
- security domains for RAN and Core
- confidentiality and integrity protection for control and user plane data in motion
- subscriber privacy using Subscription Concealed Identifier (SUCI)
- Service-Based Architecture (SBA) with PKI-based mutual authentication using Transport Layer Security (TLS) 1.3
- SBA with secure authorization using Open Authorization (OAuth) 2.0
- Service Management and Orchestration (SMO)

These combined control categories represent the ideal target security baseline for MNOs to implement for their cloud deployments. While all public cloud providers support certain cloud security controls, there is a difference in their offerings. 5G requirements will dictate customization of security controls that are unique to support critical infrastructure in the cloud. It is important for the MNO to align its security requirements with the HCP security offerings. There will be a difference in needs that require customization or integration of 5G network functions. The scope for cloud security is a moving target, evolving over time with an increasing threat surface.

Ericsson RAN Security Automation Solution

Ericsson is investing in service management and orchestration for RAN automation, which also facilitates a secure migration to public and hybrid clouds. Ericsson Intelligent Automation Platform (EIAP) implements SMO for Open RAN, and extends it to take openness and automation forward with multi-vendor and multi-technology RAN support. The platform is not a security tool itself, but is designed for the efficient management of many security tools. The security capabilities offered in the platform can be a mix of Ericsson and third-party Non-Real-Time RAN Intelligent Controller Application (rApps), to continuously evolve towards new security threats. Ericsson Cloud RAN applications will support automation through the Ericsson Security Manager (ESM) as well as the EIAP. Both can be integrated with security information and event management (SIEM) and security orchestration automation and response (SOAR) in the security operations center (SOC) for end-to-end threat detection. The platform is capable of supporting the required security controls to achieve a zero-trust architecture.

Figure 5: SMO security controls for a zero-trust architecture in 5G cloud



The way forward for MNOs

The MNO is accountable for the security posture of the deployment, regardless of the delegation of responsibility to the cloud provider.

We invite MNOs to engage with Ericsson to set a clear and executable strategy for secure mobile networks deployed in public and/or hybrid clouds. Ericsson can facilitate three party conversations with cloud providers to achieve the desired outcomes. As 5G critical infrastructure migrates to hybrid and public cloud deployments, it is necessary to build-in a zero trust architecture to protect the expanded attack surface from internal threats.

The MNO should perform a risk-based analysis that considers the cost of security controls and customize the 5G cloud deployment to the security requirements. This will assist the MNO in the selection of the preferred cloud provider partner and identify the controls the MNO must provide to fill any security requirements gaps.

We also want them to engage in three-party conversations with the cloud provider and Ericsson to set a clear and executable security strategy for mobile network functions in public/hybrid cloud.

About Ericsson

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans Networks, Digital Services, Managed Services, and Emerging Business and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. The Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.
www.ericsson.com

Ericsson
SE-164 80 Stockholm, Sweden
Telephone +46 10 719 0000
www.ericsson.com

MANA-22:003631 Uen