Solution Brief

GSMA 5G Security Guide

How Thales solutions help with 5G data security best practices as outlined by the GSMA

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

What is the GSMA 5G Security Guide?

The GSM Association (GSMA) is a non-profit organisation that represents mobile operators and their interests globally, and it plays a crucial role in fostering collaboration across the mobile ecosystem. One of its key goals is to enhance interoperability and make sure that various technologies can work together smoothly, which is especially important as the industry evolves with advancements like 5G.

The GSMA is active in defining security requirements and baseline security controls for 5G networks. This initiative seeks to guarantee that operators adopt these security measures effectively to safeguard their networks against emerging cybersecurity threats. As a part of this ongoing initiative, the GSMA published its "5G Security Guide" Version 3.0 which provides detailed guidance and recommendations for securing 5G networks, with a focus on key areas that Thales Solutions can help address such as authentication, subscriber privacy, network slicing, and interworking security.

What is a 'Secure-by-Design' Approach?

As outlined in section 1.1. of the GSMA 5G Security Guide, 5G introduces new security challenges due to the adoption of advanced technologies such as virtualization, containerization, and network slicing, which expand the potential attack surface and increase the complexity of managing security across diverse, multi-vendor environments. These innovations necessitate a more sophisticated and integrated approach to protecting network infrastructure and user data, particularly as the risk landscape evolves with the deployment of 5G networks. To meet those challenges, 5G networks should be designed with a 'secure-by-design' approach, which is based on three main foundational principles:

1. **Mutual authentication**
   Mutual authentication ensures that communication between parties is verified and trusted, preventing unauthorised access (Section 2.2).
2. **Zero-trust architecture**
   The zero-trust architecture operates on the principle that no entity, whether inside or outside the network, should be automatically trusted, requiring continuous validation of all interactions (Section 8.9.1).
3. **Mandatory encryption**
   This solution supports security across Kubernetes clusters and diverse infrastructures, bolstering data protection across both containers and underlying infrastructure. to unauthorised entities (Section 2.5).

Implementing security solutions that adhere to these secure-by-design principles make 5G more secure than previous generations, providing a robust defence against both emerging threats and legacy vulnerabilities.

GSMA 5G Security Guidelines and Recommended Thales Solutions

Thales helps by protecting:

- Data at rest, in use, and in motion
- Access to sensitive data, systems, and applications
- Cryptographic keys and implementing strong encryption and authentication
- Data across both public and private clouds, ensuring data sovereignty
- Against evolving threats with Quantum-ready, FIPS and CC certified solutions, as well as PQC Starter Kits (available for Thales HSE and/or Luna HSMs)

The table below is a summary of the key requirements and recommendations from the GSMA 5G Security Guide that Thales solutions can help address:

Section	GSMA Requirement	GSMA Recommendation	Thales Solutions
2.19	Cryptographic Enhancements	Various standards bodies are working on quantum-safe cryptographic algorithms, addressing the challenges of the quantum era.	Crypto-agile, quantum-safe Thales **High Speed Encryptors (HSE)** and **Luna Hardware Security Modules (HSMs)** provide future-proof Post-Quantum Crypto (PQC) protection today. Test your transition with the Thales HSE or HSM PQC Starter Kits.
3.4	AUSF: Authentication Server Function (in home network)	TS 33.501 [1] and FS.43 [90] define the requirements for storing the authentication credentials encrypted in a secure hardware component.	**Luna HSMs** protect subscriber privacy and authentication with a secure mechanism for the Authentication Server Function (AUSF) and ensure that encryption keys are always protected by a FIPS 140-3 Level 3 hardware environment. Luna HSMs have integrated 5G crypto mechanisms: Milenage, Tuak, COMP128.
8.9.1	Zero Trust Methodology	Protect and encrypt data at rest. For example, encryption of VNF volume/swap areas, as recommended by ENISA [129]. The best practice to secure the VNF volumes is by encrypting them and storing the cryptographic keys at safe locations.	**CipherTrust Data Security Platform** provides multiple capabilities for protecting data at rest in files, volumes, and databases. Among them: • **CipherTrust Transparent Encryption** delivers data-at-rest encryption with centralised key management and privileged user access control. This protects data wherever it resides, on-premises, across multiple clouds, and within big data and Kubernetes container environments. • **CipherTrust Tokenization permits** the pseudonymization of sensitive information in databases while maintaining the ability to analyse aggregate data, without exposing sensitive data during the analysis or in reports. • **Luna HSMs** can generate and protect the root master cryptographic key used to secure 5G VNFs in a secure, tamper-resistant hardware environment.
8.9.2	SBA API Security	The following recommendations apply: • Monitor SBA API data communications. • Validate API information.	**Imperva API Security** provides continuous protection of all APIs using deep discovery and classification of sensitive data.
13.2.2	Multi-Cloud Security Considerations	A single pane of glass to control and monitor data security, including key management and encryption based on ISO 19790 [146] or FIPS 140-2 Level 3 HSM is recommended.	**CipherTrust Manager** is FIPS 140-2 Level 3 validated, centralises and simplifies data security policies and key management with a single pane of glass. **Luna HSMs** provide FIPS 140-3 Level 3 and Common Criteria EAL 4+ protection of keys and encrypted data and establish a common root of trust across cloud applications and services.
13.2.3	Secure Public Clouds for Telcos	BYOK [Bring Your Own Key] and HYOK [Hold Your Own Key] enable operators to manage their encryption keys according to their policies, either by bringing them into the cloud environment or holding them in their own secure premises.	**CipherTrust Manager** provides centralised lifecycle management for BYOK, HYOK and cloud native encryption keys. **Luna HSMs** support BYOK and HYOK integrations, providing the flexibility to leverage cloud services, the ability to both own and control your encryption keys, and/or reduce the risk of unauthorised data access or data loss.
		BYOE [Bring Your Own Encryption] takes this a step further by allowing operators to use their own encryption algorithms and processes, ensuring that sensitive functions and data are handled in strict compliance with local laws and standards.	**CipherTrust Data Security Platform** provides advanced data at rest encryption, access control and data access audit logging.

Section	GSMA Requirement	GSMA Recommendation	Thales Solutions
13.3	Impact of 5G Functions' Virtualisation on Security	Those security mechanisms should include and be not limited to containers' workloads security assurance, API security, deployed protocols' validation at Layer 7 of the OSI reference model, threat detection and mitigation between VNFs/CNFs, including protection of the interfaces external to SBA.	**Imperva API Security** offers continuous protection of all APIs using deep discovery and classification of sensitive data. **Luna HSMs** provide a secure root of trust for 5G VNFs, code signing and TLS / SSL applications by generating and storing private keys associated with certificates and performing digital signing operations within the secure environment of the HSM.
		Ensuring the security of data stored by telcos, whether in storages, databases, or file shares, demands meticulous attention. It is advised to employ robust encryption and key management solutions, consistently maintaining sensitive data in encrypted form.	**CipherTrust Data Security Platform** provides advanced data at rest encryption, access control and data access audit logging.
13.3.3	Security Guidelines for Storage of UICC Credentials	Use of a HSM is needed to ensure that the credentials are never exposed and potentially intercepted when stored in the memory of functional elements like the UDM.	**Luna HSMs** ensure network credentials are never exposed in the memory of functional elements such as UDM/HLR/HSS. They protect subscriber privacy and authentication by offering a secure mechanism for the UDM to ensure that the encryption keys are always protected.
16.4	O-RAN Security Specifications	Specific requirements include resilience against volumetric Distributed Denial of Service (DDoS) attacks, secure handling of internal and external communications with confidentiality, integrity, replay protection, and mutual authentication.	**Imperva DDoS Protection** Secure all assets at the edge for uninterrupted operation. **High Speed Encryptors (HSE)** provide a multi-point solution and support a wide range of RAN/O-RAN network requirements such as network slicing and are equipped with Transport Independent Mode (TIM), for concurrent encryption over network Layers 2, 3 and 4.

Thales CPL 5G Security Solutions Summary

Thales can support your 5G security strategy, including integration, deployment, and addressing compliance needs.

Luna HSMs

Protect Operator and Authentication Keys, PKI, Subscriber Identity and Privacy with a Hardware Root of Trust

- Protect network keys, subscriber credentials and authentication algorithms.
- Secure subscriber digital identity and privacy.
- FIPS 140-3 Level 3 and Common Criteria EAL 4+ hardware root of trust for your entire network, PKI, and critical infrastructure.

High Speed Encryptors (HSE)

Protect Data in Motion with High-Speed Encryption

- When security, high bandwidth and low latency are required.
- Secure data in motion from the RAN to the edge, from the edge to the core network guaranteeing the confidentiality and integrity of your data transmissions.

CipherTrust Data Security Platform

A Comprehensive Data Security Platform that Provides Robust Key Management, Encryption, and Tokenization Solutions

- Protect data-at-rest across public, private, and hybrid cloud environments safeguarding it from unauthorized access.
- Implement digital sovereignty controls and meet compliance requirements with encryption and key management solutions that align with industry standards.
- Discover sensitive data and secrets, allowing them to be secured and managed.

Imperva API Security and DDoS Protection

Protect APIs and Against DDoS Attacks

- Continuous protection of all APIs using deep discovery and classification of sensitive data.
- Secure your assets at the edge for uninterrupted operation.
- Ensure business continuity with guaranteed uptime.

About Thales

Thales is a global leader in data security, trusted by governments and the most recognised companies around the world to help them protect their most sensitive data. The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organisations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us