cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales 5G and UK Telecom Security Recommendations

Introduction

Thales has a long tradition of providing security products and services. The Thales cloud protection and licensing division has provided operators, network equipment providers and other partners with:

- HSMs used in secure element personalization, key diversification and local/remote key injection in manufacturing
- HSMs used on platforms for on boarding, remote provisioning and authentication verification on telecom networks
- HSEs used to secure latency sensitive connections between telecom datacentres
- Key Management platforms deploying a number of data at rest and application level encryption and tokenization for servers, storage and a number of enterprise software solutions
- Provider of secure elements and telecom modules to operators, such as UICC/eUICC SIM cards, secure elements for M2M use cases such as cars ECUs, tablets, wearable devices, etc.

The NCSC TSR

The National Cyber Security Centre is an organisation under the parent arm of the GCHQ and is responsible for providing advice and support to the public and private service in the UK involving:

- Avoiding security threats
- Respond to cyber emergencies (CERT)
- Protect the national infrastructure

Under these responsibilities and given the criticality of the 5G rollout, the NCSC is working on the creation of a document denominated Telecom Security Requirements (TSR). This document contains technical and non-technical recommendations for mobile telecom operators working on the 5G infrastructure in the UK. Such requirements have a profound impact on the whole telecom supply chain including equipment and service providers, data centre infrastructure, system integrators, etc.

TSR requisites are divided into specific requirement groups (and a few special interest subgroups):

- Protecting the Management Plane
- Protecting the Signalling plane
- Protecting virtualised and containerised environments
- Managing the supply chain
- Retaining national resilience and capability

Some of the topics are covered multiple times (transversal requirements), as they should, over the chapters. Some chapters are specialised, like the signalling (deals with the low level interconnectivity between telco operators) and NOFs (network oversight functions), dealing with accessory and support platforms present in telecom networks.

For each main area of security concern, the TSR makes recommendations tracked as principles (P), requirements (R) and section specific examples, highlights on critical points, implementation guides and other comments. For example there is a description on how a segregated management plane with multiple stakeholders should look like.

TSR highlights and solution mapping

Here we are highlighting a number of requisites from the TSR, that directly translate into a number of critical cybersecurity solutions strongly recommended as must haves for a 5G network deployment. Many of the items will be familiar to IT and cybersecurity practitioners, in the telco sector or not.

Thales solutions can be divided into 3 groups for this exercise that was based on TSR v0.92:

i) Direct use cases and deployment of cybersecurity products to achieve 5G use cases

ii) Direct application of products and services to enable technical controls

iii) Indirect application of products to enable other parts of the 5G infrastructure to achieve compliance

R:2.A.5 The central storage for any persistent credentials and secrets shall be protected within **hardware-protected** storage
R:4.A.7 All non-ephemeral secrets, passwords and keys shall be stored in hardware-backed secure storage.

Sect 5.4.3 As an initial position, the operator should not allow any data, either customer, system or corporate to **leave their control**.

P:4.A.5 **Sensitive data is protected** within the virtualised environment.
P:4.A.4 All host [virtual] infrastructure is a **trusted platform**.
P:4.C.6 Virtualisation control and orchestration functions are Network Oversight Functions and must reside in a **trusted** physical and logical location.

P:2.B.3 Multi-factor authentication **(MFA)** is used for all access to the management plane
R:2.B.3 Privileged access shall be via accounts secured with **MFA**. The second factor shall be locally generated, and not be transmitted.

P:1.C.1 Where feasible, operators **segregate** networks based on purpose
P:9.A.1 Network Oversight Functions are treated as the operator's '**crown jewels**' and have an enhanced level of protection against, potentially persistent, attack/exploitation.
R:9.A.1 Network Oversight Functions shall be robustly **locked down**

NOF's are auxiliary platforms that are not in any particular plane, or sometimes are multi-plane. It covers platforms such as user directories, jump gateways, VPNs, MFA providers, orchestrators, automation platforms, security gateways, etc.

Going through the requirements, it is easy to see that:

- There is a strong emphasis on deploying strong authentication / MFA especially in jump gateways, management consoles, privileged users logins and infra administrators accounts. This helps with segregation and maintaining a "least privilege" operation.

Here is a selection of TSR requirements that deals with a number of cybersecurity topics followed by a small comment on them.

- Software platforms such as secrets management, privileged access management and orchestrators must be backed by a hardware root of trust platform, typically an HSM (Hardware Security Module)
- In virtualized situations, protecting the data against the lower level infrastructure (that could easily be a third party, for example in a cloud provider scenario) means that encryption at the virtualisation level must be deployed, and application level encryption or tokenization for highly sensitive data

A note on vendor equipment and national resiliency premiums

The TSR has specific sections that emphasize the importance of using vendors with a track record of delivering and maintaining security in their solutions. There is also a concern that disruptions on the national relationship or technical issues with foreign actors should not impact the network (e.g. operations and critical platforms should be operated totally or mainly from the UK). It is encouraged that providers will receive more scrutiny of their products, development cycle and track record on responding to security incidents in the industry.

Thales recommendations

Deploy Thales Luna HSMs for:

- Code signing
- PKI/CA environments within the network
- Root of trust / security anchor of a number of other appliances
- 5G Authentication & Privacy
  - Privacy – SUPI/SUCI
  - Authentication vector Gen – as Milenage / Tuak / Comp 128
- Personalisation of secure elements
- Highly secure crypto environment, proprietary algorithm implementation (for example post quantum)

Deploy Thales High Speed Encryptors for:

- End-to-end network encryption to improve throughput and lower latency, enhance security, and ensure hyper connectivity
- Virtual and hardware platforms to optimize cloud connectivity, data center interconnects, and virtualized environments
- Secure layer 2, 3, and 4 networks concurrently to simplify next generation network connectivity
- Globally accredited by multiple certification bodies to ensure compliance for emerging threats and regulations

Deploy Thales STA (SafeNet Trusted Access) and SAS (SafeNet Authentication Service) for:

- Strong MFA integration based on industry standards (RADIUS, OIDC, SAML)
- Smart SSO to reduce the strain of using strong authentication to privileged users
- Deploy software (smartphone) and hardware tokens, such as TOTP/HOTP and PKI based ones (smartcards, USB smartcards, also for digital signature)
- Virtual smartcard solutions are available for specific/combined scenarios (for example, lost smartcard use case)

Deploy Thales CipherTrust Platform for key management based use cases such as:

- Data at rest encryption and external key management for storages, databases, noSQL databases, virtual volumes
- External key management for virtual systems such as VMware, openstack, docker, etc.
- Provide KMIP server functionality for a number of appliances (VDI consoles, applications requiring secure key storage, etc.)
- Full life cycle management of cloud encryption keys for AWS, Azure, Google, IBM and Salesforce

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations 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.

Decisive technology for decisive moments.

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