Simplify Data Security by Automating Key Management for 5G Services

Run Thales CipherTrust on VMware Telco Cloud Platform™

AT A GLANCE

With Thales CipherTrust Data Security Platform solutions running on VMware Telco Cloud Platform™, it enables CSPs with VMware Telco Cloud Platform running on AWS to deploy client-side encryption, centralized key management and tokenization to simplify security operations such as data visibility, compliance auditing and policy execution and enforcement.

- Support multi-cloud environments.
- Support multiple deployment options.
- Simplifies data security, secure cloud migration.
- Accelerates Time to Compliance, Compliant with FIPS, GDPR, PCI-DSS, HIPPA.

The Thales CipherTrust Data Security Platform is an integrated suite of data-centric security products and solutions that unify data discovery, protection and control in one platform.

Thales CipherTrust Data Security

- Key Management System (KMS) – Securely store encryption keys for local storage, containers, vSAN, Virtual machines, cloud storage.
- Hardware Security Module (HSM) – Protect transactions, identities, and applications for both monolithic cloud-native.

Introduction

In the past, Communications Service Providers (CSPs) located their application software components in datacenter enclaves. Security was provided by strong perimeter defenses. With the advent of cloud, 5G, pandemic driven work from home, and edge computing technologies the service providing components are now being distributed throughout the CSP networks. Service-providing components are installed on standard computing platforms in most cases using virtualization in preference to the historical appliance form factor. With the new architecture, data can no longer be fully centralized, but instead must be distributed in whole or in part to insure service levels.

This new paradigm presents new challenges for insuring security. Encryption is required throughout the data lifecycle. This requires the distribution and secure storage of key data. In many cases, this requirement is not only good business practice but is imposed by regulatory requirements. Increasing the complexity is the potential for 1,000's or 10,000's of locations with multiple systems in each location.

Thales CipherTrust Data Security allows the secure distribution and storage of cipher keys. It insures that the key data is not stored with the data reducing the chances of a single system breech allowing unfetored access to sensitive data.

The Thales CipherTrust Data Security solution running on VMware Telco Cloud Platform™ is the robust solution to establish that data and keys are protected whether on physical disks, cloud storage or VMware vSAN.

The Opportunity

CSPs can gain competitive advantages in transitioning from purpose-built, appliance-based applications from single network equipment providers (NEPs) to a modern, open and disaggregated RAN architecture. This transition can enable CSPs to gain the flexibility to choose best-of-breed software components and deploy new services rapidly. New 5G services rely on CSPs to be able to host apps at the edge, close to end customers. A virtualized and open RAN allows CSPs to deliver these new edge services to customers directly from RAN sites. The distribution of modern applications poses new challenges in meeting business and regulatory requirements for security of customer information and data.

VMWARE TELCO CLOUD PLATFORM

The VMware Telco Cloud Platform enables CSPs to accelerate 5G rollouts from core to edge to the RAN for both containerized network functions (CNFs) and virtualized network functions (VNFs).

VMWARE TELCO CLOUD PLATFORM RAN

The VMware Telco Cloud Platform RAN is powered by field-proven virtualized compute coupled with VMware Telco Cloud Automation and VMware Tanzu for Telco RAN, a telco-grade Kubernetes distribution.

- Use the same common platform to virtualize the RAN now and migrate to O-RAN in the future.
- Run virtualized baseband functions, virtualized distributed units (vDUs), and virtualized central units (vCUs) in accordance with stringent RAN performance and latency requirements.
- Optimize the placement of DUs and CUs through programmable resource provisioning.
- Deploy and operate both RAN and non-RAN workloads on a horizontal platform.
- Transform the RAN into a 5G multi-services hub.
- Reduce time-to-deploy by automating the provisioning of RAN sites.
- Simplify the onboarding of vRAN functions with validated and standards-compliant packages.
- Automate lifecycle management of infrastructure, Kubernetes clusters, vRAN functions, and 5G services.
- Programmatically adjust the underpinning platform availability and resource configuration, based on the requirements of vRAN functions at the time of instantiation.
- Automatically discover, register and create Kubernetes clusters from a centralized location to manage thousands of distributed components with ease.

As CSPs continue building up their RAN and edge networks, disaggregating the RAN opens up numerous use cases. Disaggregation also enables CSPs to raise the value chain and offer a better and differentiated quality of experience to each customer, for both enterprise and consumer markets.

CSPs and their customers are launching new network-based services based on the increased bandwidth and decreased latency of 5G networks, such as emergency medical and public safety services, autonomous or driverless vehicles, and low-latency industrial and manufacturing applications. The thing that all these new services have in common is the need to manage data both locally and centralized. No matter where it is located, data must be stored in a secured fashion. The distribution of the data means that the historical solution of data-centers with perimeter defenses will no longer be adequate.

The Challenge

When provisioning any new solution, the infrastructure must be ideal to establish operational readiness, security and accessibility. VMware Telco Cloud Platform provides the capability to select and provision the appropriate virtual infrastructure. Unlike the past, the distribution of modern applications poses new challenges. 1) Need for flexible but proven virtualized infrastructure that's easy to scale and manage and 2) Meeting business and various mandated data regulatory requirements for the security of customer information and data and centrally managing the encryption keys no matter where it is located from thousands and likely tens of thousands of systems and components. Failing to protect data can resut in costly fines and reputation damages. In addition, storing keys with encrypted data is an unacceptable solution. How can this be simplified and assured?

The Solution

To accomplish these goals in thousands of RAN and edge sites, the **VMware Telco Cloud Platform RAN** reduces the footprint and resources required at each edge and central locations. **VMware Telco Cloud Platform** supports both RAN and non-RAN workloads on the same platform. **VMware ESXi™** with **VMware Tanzu™ for Telco RAN** supports both virtualized compute resources and Kubernetes at the cell, aggregation and datacenter sites.
This innovative, common and horizontal design provides the flexibility and adaptability for CSPs that they need. CSPs can now build out the infrastructure to support thousands of RAN sites using a pay-as-you-grow approach, from virtualizing the RAN now, to migrating to O-RAN, then transforming into 5G multi-service hubs when ready.

VMware's experience and track record in virtualizing data-centers and networks combined with Thales leadership in data security and sovereignty at a global level make both natural and critical partners for 5G operators and enterprises. Combined they allow CSP's to monetize the 5G services they deliver across their network. See Fig 1 below.

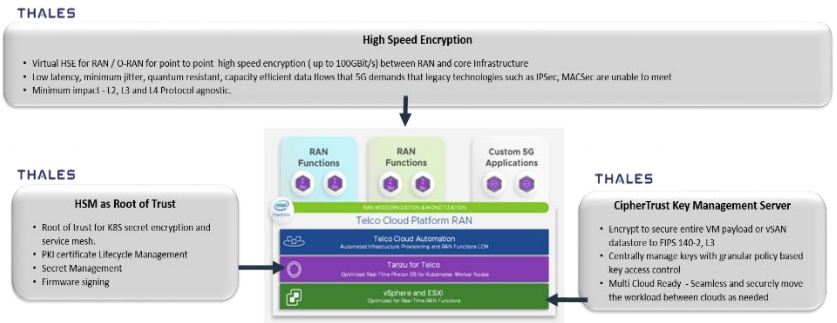


FIGURE 1: VMware Telco Cloud Platform and Thales

THALES CIPHERTRUST SECURITY PLATFORM

Thales CipherTrust Security Platform

Thales CipherTrust Platform addresses mandated Data Security and Data Sovereignty requirements.

Key Management System (KMS)

- Centrally manage a large number of encryption keys used to protect sensitive data used or within apps, (VNF, CNF), databases, files/folders, and storage whether they are physical or vSAN within NFV infrastructure and OSS/BSS systems.
- Multi-cloud ready. Manage your encryption keys from a single pane of glass, no matter where your data is: private, public, or hybrid cloud.
- Granular control over keys and key access policies to help with audit.
- Optional Data Discovery and Classification feature to assist SecOps to find and secure sensitive data in a system.

Hardware Security Module (HSM)

- High assurance FIPS 140-2, L3 certified protection for encryption keys and certificates used to protect application be VNF/CNF, signed firmware code, user and device ID's, K8S' secrets, etc.

High-Speed Encryption (HSE)

- Vendor agnostic, low latency, low overhead, high speed (up to 100GBit/s) point-to-point link encryption.
- Ideal for protecting network traffic between RAN and core or data centers to data centers from a man-in-the-middle attack.

Other solutions from Thales Group

- eSIM/SIM.
- AI/ML and Analytics tools (Guavas).
- IoT modules.

VMware Telco Cloud Platform allows CSPs to accelerate the disaggregation of their proprietary RAN and modernize their RAN and core so they can monetize the 5G services they deliver across their network. With Thales CipherTrust Security running on VMware Telco Cloud Platform, CSPs can establish secure, consistent and successful provisioning of new services and solutions.

As part of the VMware Telco Cloud Platform, **VMware Telco Cloud Automation** is a multi-cloud, multi-layer automation that can extend from the 5G core to the RAN, providing end-to-end operational consistency for CSPs to radically simplify how they provision and manage their 5G networks.

With VMware Telco Cloud Automation, CSPs can automatically provision, deploy and redeploy thousands of platform instances across distributed sites. By understanding the requirements of each vRAN or function as well as each non-RAN function including corresponding characteristics (such as latency and bandwidth) that is intended to be instantiated, the platform can select and automatically configure the underpinning resources to meet the service requirements in the SLAs and QoS. This intelligence enables CSPs to dynamically adjust where functions should be deployed with cloud-first lifecycle management, simplifying Day 0, Day 1 and Day 2 operations while providing the telco-grade resiliency and service availability needed for for both RAN and next-generation 5G service.

Key Use Cases

5G SECURITY

5 Key Components of a Trusted 5G Architecture are:

- Core Network
- Multi-Access Edge Compute (MEC)
- Backhaul/Fronthaul/Mid-haul
- Subscriber Authentication and Privacy
- Management Layer

DATA SECURITY & ENCRYPTION

With the Data Security Platform from Thales, IT organizations can address their security objectives and compliance mandates in a number of systems and environments. Whether we're looking to guard against abuse by privileged users, encrypt sensitive data in a database, or address compliance mandates in the cloud, Thales CipherTrust Transparent Encryption is of the great significance.

Data-at-rest Encryption

The Benefits are:

Operational Simplicity

Centralized policy and encryption key management establishes control of the data across every physical and virtual server on and off premises.

Minimize Risk

Meet compliance and best practice requirements for protecting data from external threats or malicious insiders with proven, high-performance and scalable data encryption.

Security Agility

Quickly address new data security requirements and compliance mandates by having a solution in place ready and able to protect all sensitive data.

Why Thales

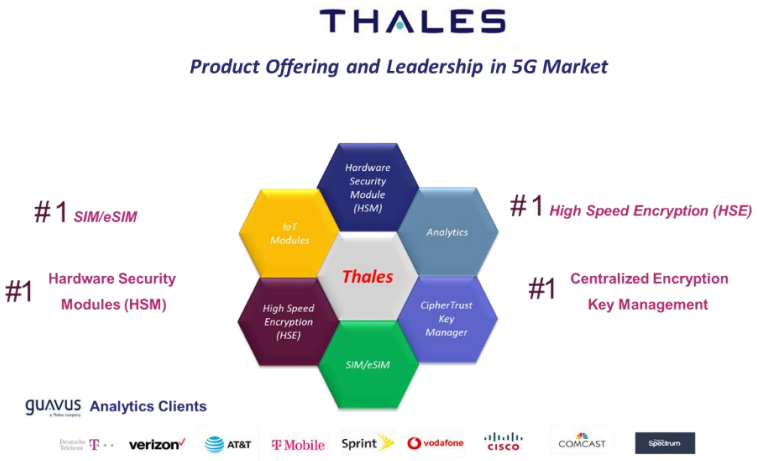


FIGURE 2: Thales CipherTrust Platform KMS and HSM

Data Security and Sovereignty

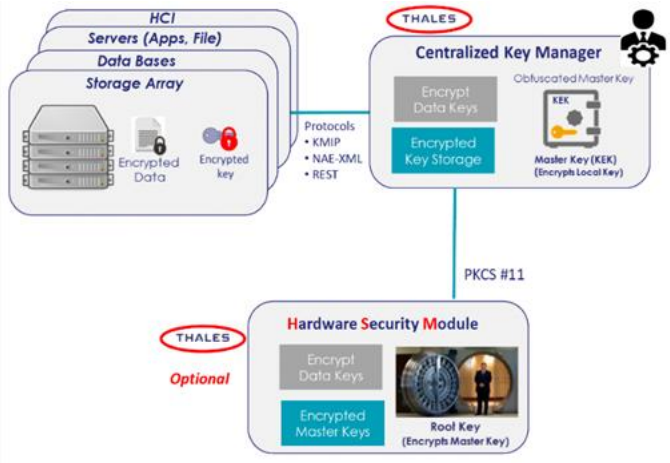
Data is the new gold. Securing data is not only a good business practice but is required to meet various mandatory compliance laws at the regional and/or global level. Failing to protect data and any subsequent data breach can result in not only large financial penalties but also unwanted negative publicity.

To protect valuable data, cryptographic tools are widely used to encrypt the data, rendering the stolen data useless. Encryption of data at the appliance level is increasingly common, however, in highly distributed systems, managing the encryption keys and key lifecycle for hundreds or thousands of appliances from multiple vendors, is a daunting task, to say the least.

Thales CipherTrust Data Security Platform and other cryptographic tools solutions addresses this issue. It takes the local encryption keys used to encrypt apps such as monolithic, virtual, or containerized, databases, files/folders, and data on HDD/SDD drives and re-encrypts them with master or root keys. The root keys are then securely stored away from encrypted data in tamper-proof FIPS-certified virtual or physical appliances. No matter where data resides; on-premises, edge, or cloud, the encryption keys, and key lifecycle are centrally managed. All from using a single pane of glass. Furthermore, access to keys is enforced with strong role-based access policies and logging to insure effective audit control.

The Thales CipherTrust Data Security Platform has been tested and validated by the largest ecosystem of partners at the global level, including VMware Telco Cloud Platform™, a must-

have in a highly distributed and multi-cloud system to establish that data, no matter where it resides, is secure and stays protected. Allowing end customers to move their workloads seamlessly & securely in a highly distributed and multi-cloud environment, without any concern or vendor lock-in.



Summary

The solution with Thales CipherTrust Security Platform running on the VMware Telco Cloud Platform is easily deployed and integrated into CSP's multi-cloud environment. It allows to provide a secure platform to meet the most stringent requirements. Whether requirement is for FIPS, GDPR or HIPPA compliance, the combination of VMware and Thales platforms yields a secure and auditable environment meeting the needs of the most complex multi-cloud architectures.

For more information on VMware Telco Cloud Platform, please visit *telco.vmware.com* or contact your VMware representative.