EXTERNAL FAQ

KEYSECURE PORTFOLIO

END OF LIFE PROCESS

VERSION 2.0 APRIL 16, 2020

THALES GROUP

Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 • Telephone: 512-257-3900

Contents

REVISION HISTORY

Date	Version	Description
April 2020	1.0	Overview of KS Physical Appliance End of Life Announcement
April 2021	2.0	Updated to include KS Connector Announcement

1. KeySecure End-of-Sale and End-of-Life Summary

1.1 Why is KeySecure being End-of-Sale / End-of-Life?

Vormetric's Data Security Manager (DSM) and Gemalto's KeySecure product portfolios have been in market for over a decade. As such, they have each developed a loyal customer following for their abilities surrounding key management and data encryption.

However, both product teams realized to evolve forward to meet customer requirements for hybrid operating environments and cloud solutions, changes were needed to meet these technology advancements.

Therefore, a decision was taken to combine the legacy SafeNet and Vormetric product lines to generate a "best of breed" solutions among the product lines. For the core of the CipherTrust Manager Data Security Platform (CDSP), CipherTrust Manager (CM) represents that combined "best of both" solution while also laying the foundation to provide superior hybrid key management and data encryption support.

Existing customers are prioritized as part of this effort to ensure existing use cases are migrated to CM and CDSP. Customers are provided a 3 year window to budget, plan and migrate from their existing DSM deployment to CDSP.

1.2 What KeySecure products are affected by the latest End-of-Life Announcement?

The following SafeNet/Gemalto KeySecure Connectors are impacted by this latest EOL announcement.

- ProtectFile
- ProtectDB
- ProtectApp
- Tokenization
- Transform Utility
- Database Native TDE
- Linux Native Encryption (LUKS)
- KMIP Connectors and bundles

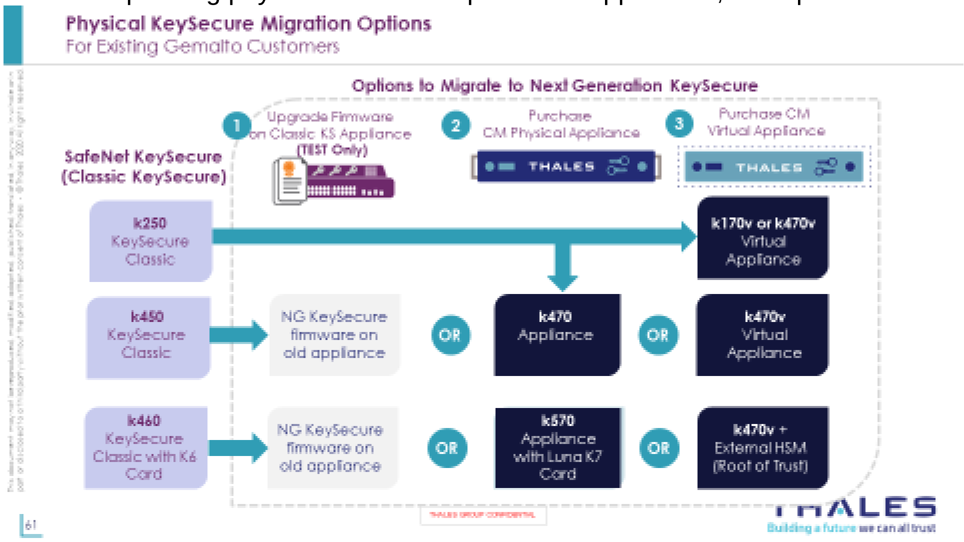
1.3 What are the time frames for End-of-Sale and End-of-Support?

Product	Milestones	Date	Description
KeySecure Physical Appliances • **k250** • **k450** • **k460**	External End of Sales/ End of Support Announcement to Customers	22-Apr-2020	Date when customers will be informed about End-of-Life
	End of Sales of KeySecure Physical Appliances	30-Jun-2020	Affected product Part Numbers removed from the Sales Catalog and cannot be sold after this date.
	End of Support Of KeySecure Physical Appliances	31-Dec-2023	Customers need to be migrated to CipherTrust Manager. KeySecure

			firmware and appliances no longer supported
KeySecure Connectors • **ProtectFile** • **ProtectDB** • **ProtectApp** • **Tokenization** • **Transform Utility** • **Database Native TDE** • **Linux Native Encryption (LUKS)** • **KMIP Connectors and bundles** **KeySecure Virtual Appliances** **Virtual KeySecure (k150v, k450v)**	External EOS/EOL Announcement to Customers	19-Apr-2020	Date when customers will be informed about End-of-Life
	End of Sales of KeySecure Connectors and Virtual KeySecure	31-Dec-2022	Affected product Part Numbers removed from the Sales Catalog and cannot be sold after this date.
	End of Support of KeySecure Connectors and Virtual KeySecure	31-Dec-2023	Customers need to be migrated to CipherTrust Manager. KeySecure firmware and appliances no longer supported

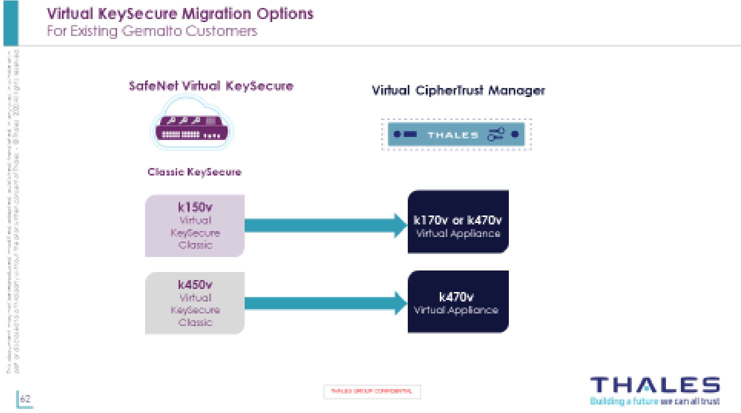
1.4 What are my migration options to CipherTrust Platform?

Customers have the following options to migrate their physical KeySecure appliance to the corresponding physical or virtual CipherTrust appliances, as depicted in the diagram below.


Physical KeySecure Migration Options
For Existing Gemalto Customers
Options to Migrate to Next Generation KeySecure
1 Upgrade Firmware on Classic KS Appliance (TEST Only)
2 Purchase CM Physical Appliance
3 Purchase CM Virtual Appliance
THALES
THALES
SafeNet KeySecure (Classic KeySecure)
k250 KeySecure Classic
k450 KeySecure Classic
k460 KeySecure Classic with K6 Card
NG KeySecure firmware on old appliance
NG KeySecure firmware on old appliance
OR
OR
OR
OR
k170v or k470v Virtual Appliance
k470 Appliance
k470v Virtual Appliance
k570 Appliance with Luna K7 Card
k470v + External HSM (Root of Trust)
61
THALES GROUP CONFIDENTIAL
THALES
Building a future we can all trust

- k250 customers will migrate to k170v or k470 physical appliance. They may consider upgrading to a k470v.
- k450 and k460 customers have the following options. All update options have a cost associated wth them.
  - Apply a firmware upgrade that will allow them to run CipherTrust Manager on their existing KeySecure appliance. This will allow customers to validate the new product without the expense of purchasing new hardware. The upgrader will be made available to those with active support contracts until Q2 21. **Please note that the firmware upgrader is for validation purposes and not intended for long term production requirements**
  - Evaluate / purchase the k470 (for k450 customers) or k570 (for k460 customers).
  - Evaluate / purchase the k470v (with the option to configure an HSM Root of Trust)

Customers have the following options to migrate their virtual KeySecure appliance to the corresponding virtual CipherTrust appliance, as depicted in the diagram below.



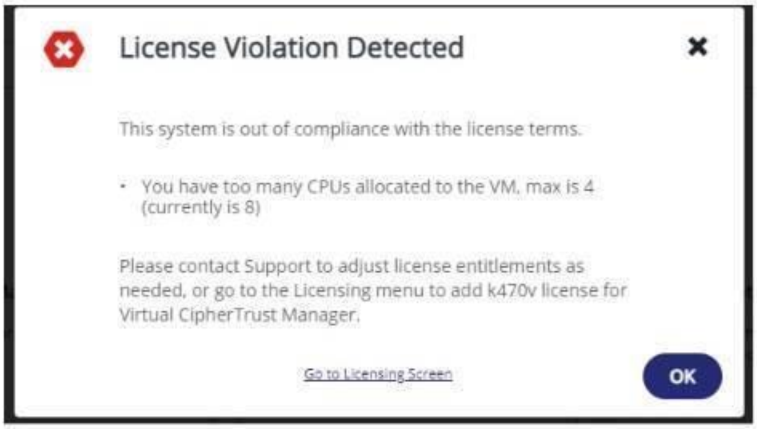
Virtual KeySecure Migration Options

For Existing Gemalto Customers

SafeNet Virtual KeySecure
Virtual CipherTrust Manager
THALES
Classic KeySecure
k150v Virtual KeySecure Classic
k170v or k470v Virtual Appliance
k450v Virtual KeySecure Classic
k470v Virtual Appliance
62
THALES GROUP CONFIDENTIAL
THALES
Building a future we can all trust

1.5 What is the difference between k170v and k470v?

K170v is intended for simplified and centralized key management. For example, k170v is suited to lab environments, low transaction encryption use cases, and storage encryption key management with KMIP (Key Management Interoperability Protocol). K170v allows for the usage of four CPUs or fewer. K170v is applied as a license.



License Violation Detected

This system is out of compliance with the license terms.

- You have too many CPUs allocated to the VM, max is 4 (currently is 8)

Please contact Support to adjust license entitlements as needed, or go to the Licensing menu to add k470v license for Virtual CipherTrust Manager.

k470v is intended to support high transaction-per-second encryption operations as is typically required from the CipherTrust Data Security Portfolio suite. k470v allows for the usage of more than four CPUs. k470v is applied as a license.

Note that in terms of feature/functionality or 3rd party integration, all CipherTrust Manager platforms (physical and virtual) are equal in function and capability.

2. Migration Plan

2.1 What is the migration strategy for KeySecure Connectors?

- Customers with existing SafeNet KeySecure Connector licenses under a valid maintenance and support contract will not be charged to migrate to equivalent CipherTrust Connectors.
- The responsible Thales Sales Team will need to submit a License Migration form to track the license migration and issue licenses for the corresponding CipherTrust Connectors.
- thalesdocs.com offers instructions to help SafeNet KeySecure customers to migrate to the CipherTrust Data Security platform.
- Thales also offers Professional Services packages to assist in the migration. Please contact your account representative for further details.

2.2 What products from the KeySecure portfolio are compatible with the CipherTrust platform?

Here is the current list of KeySecure Connectors compatible with the CipherTrust platform.

SafeNet / Gemalto Product	CipherTrust Product Connector	Notes
KeySecure	CipherTrust Manager (CM) CipherTrust Cloud Key Manager (CCKM Embedded)	Offers centralized key lifecycle management and access control to encryption keys
KMIP Connector	CipherTrust Flexibility Bundle	Provides external key management for storage solutions (SAN and NAS storage arrays), self-encrypting drives and hyper-converged infrastructure
ProtectFIle	CipherTrust Transparent Encryption (CTE)	Provides transparent encryption and access control for files/folders CTE provides additional support for additional environments like Teradata, SAP, Pure Storage and others
ProtectDB	CipherTrust Database Protection (CDP)	Protects transparent column-level encryption in databases
ProtectApp	CipherTrust Application Data Protection (CADP)	Offers DevSecOps friendly tools for key management and encryption operations
Tokenization	CipherTrust Vaulted Tokenization (CT-V) CipherTrust Vaultless Tokenization (CT-VL)	Offers non-disruptive format preserving tokenization with a wide range of options Provides dynamic data masking of sensitive data through APIs
N/A	CipherTrust Protection for Teradata Database (CPTD)	Protects transparent encryption of database columns in Teradata.
	CipherTrust Bulk Data Transformation (CBDT)	Provides static data masking of vast quantities of data quickly.
TDE/EKM Connector	CipherTrust TDE Key Management	Provides Transparent Database Encryption (TDE) for Oracle DB and Microsoft SQL servers.

2.3 Is CipherTrust fully compatible with KeySecure and KeySecure connectors?

NOTE: Older versions of most SafeNet Client Platforms (versions earlier than the minimum versions listed below) may have incompatible TLS clients. Gemalto recommends testing older versions of client platforms in a non-production environment to ensure proper functionality.

For the purpose of transitioning from KeySecure, you can temporarily connect to NextGen KeySecure with TLS/SSL disabled on CipherTrust Manager's NAE interface; however, this is recommended only in a non-production environment.

Product	Migration Path	How to Migrate
KeySecure	Supported KS version: 8.4.3 or higher (Physical or Virtual Appliance) Supported CM Version: 2.2 or higher	https://thalesdocs.com/ctp/cm/2.2/deployment/legacy-appliances/migrating-keysecure-classic/index.html
KMIP	Supported KS version: 8.4.3 or higher (Physical or Virtual Appliance) Supported CM Version: 2.2 or higher	https://thalesdocs.com/ctp/cm/latest/kmip-ref/index.html
SafeNet ProtectFile Linux	Supported release version: PF Windows v8.11.1 PF Linux v8.11.2	KB0019579 ProtectFile Migration from KeySecure Classic to KeySecure 170v
SafeNet ProtectFile Windows		
SafeNet ProtectV	Supported release version: minimum version 4.8.0	KB0019572 ProtectV Clients Migration from KeySecure Classic to KeySecure 170v
SafeNet ProtectDB Oracle	Supported release versions: > ProtectDB-Oracle: minimum version 8.8.0	PDBCTL Utility 1.5.0 Bundle KB0023665
SafeNet ProtectDB SQL Server	> ProtectDB-SQL: minimum version 8.9.0	
SafeNet ProtectDB DB2	> ProtectDB-DB2: minimum version 8.7.0	
SafeNet ProtectApp JCE	Supported release versions: > ProtectApp JCE: minimum version 8.6.1 > ProtectApp Oracle TDE: minimum version 8.3.0 > ProtectApp SQL EKM: minimum version 8.3.0	Available from thalesdocs.com in Q2 21
SafeNet ProtectApp .Net	> ProtectApp .NET: minimum version 8.9.0	Available from thalesdocs.com in Q2 21
SafeNet ProtectApp ICAPI	> ProtectApp ICAPI: minimum version 8.10.0	Available from thalesdocs.com in Q2 21
SafeNet Tokenization	Supported release versions: > Tokenization Manager: minimum version 8.7.1 > Vaultless Tokenization Manager: minimum version 8.8.0	Available from thalesdocs.com in Q2 21
SafeNet ProtectV	Supported release version: minimum version 4.8.0	KB0019572 ProtectV Clients Migration from KeySecure Classic to KeySecure 170v

2.4 What is the migration plan for ProtectV on the CipherTrust platform?

ProtectV Manager is merged into CipherTrust Manager from v4.7.5 onwards. Customers can work with client services to migrate their licenses for CipherTrust and follow the migration document (KB0019572) to upgrade their ProtectV clients and migrate ProtectV manager configuration into a CipherTrust.

2.5 What are the plans for FIPS Certification with the new platform?

FIPS certification is based on a number of factors – hardware, software and the features enabled for each. With SafeNet KeySecure 8.x, we have the following certifications:

Product	Compliance
K170v/k470v	Currently can support Physical or Virtual HSM as a Root of Trust Plan to submit CipherTrust Manager Core Security Module (CMCSM) to NIST for Implementation Under Test in Q2 21
K470	Currently can support Physical or Virtual HSM as a Root of Trust Will ship with CMCSM module upon ratification by NIST
K570	Level 3 Based on HSM Card (https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3519) Will ship with CMCSM module upon ratification by NIST

2.6 My current support contract extends past the stated End of Support date. What happens then?

Thales will honor existing support contracts for their duration, but will not alter / enhance products past the stated dates. As most customers will need some time to stage and roll out new platform, we encourage customers to start planning/budgeting as soon as possible to migrate to CipherTrust.

2.7 I am a DataSecure customer who has not migrated to KeySecure. How do I skip forward to start using the CipherTrust Platform?

For DataSecure customers to migrate, the existing DS appliance must

a) Be upgraded to run KeySecure 8.4.3 (available from the Support Portal (search for Download Link DOW4439)
b) Take a backup of the upgraded appliance (check Admin guide documentation for instructions)
c) Restore the backup to a Virtual or Physical Next Generation KeySecure appliance

In terms of appliance migration options, customers can select from

- Physical Appliance (k470 or k570)
- Virtual Appliance (k170v or k470v)

The appliance upgrader is not available for legacy DataSecure appliances (i150, i450 or i460). If your environment does not meet the aforementioned guidelines, please contact your Sales/Account team for further discussion. In some cases, Professional Services can assist in such scenarios.

3. CipherTrust Data Security Platform

3.1 What is the CipherTrust Data Security Platform, and how is it related to KeySecure?

The CipherTrust Data Security Platform (CDSP) brings together the best of KeySecure and Vormetric product lines. CDSP is built on CipherTrust Manager appliance. CDSP features a suite of data protection products that can be deployed individually or in combination to deliver advanced encryption, tokenization, and centralized key management across on-premises, public and hybrid cloud environments.

The CipherTrust Data Security Platform was launched in September 2020. Migrating to the CipherTrust platform now will allow you to carry forward your current investments to the CipherTrust platform, and enable you to protect data in emerging technologies in the future including quantum, IoT, Blockchain, 5G and more.

3.2 What are the competitive advantages of the CipherTrust Data Security Platform?

The CipherTrust platform is bring together the best of the KeySecure and Vormetric product lines. Here are the top 10 reasons to migrate to the CipherTrust platform.

- **New intuitive graphical user interface (GUI):** simplifies data protection through its entire security lifecycle starting from licensing (unifying management across all data protection products (agents/connectors) that run on the platform), key management, data encryption, and monitoring/reporting,.

- **New Data Discovery and Classification (DDC)**: new functionality that did not exist in either KeySecure or Vormetric platforms. DDC provide visibility into sensitive data across your enterprise and helps you decide what critical data do you need to protect using CipherTrust data protection solutions to reduce business risk.

- **Multi-cloud Key Management:** Enables centralized key management across multiple cloud service providers – AWS, Azure, Google Cloud and more - as well as offers CCKM to simplify bring your own key (BYOK) use-cases that leverage native data encryption provided by each CSP.

- **DevOps Friendly:** REST apis to automate key management and encryption capabilities using DevOps tools such as Ansible, Puppet and Chef. Combined with KMIP, PKCS11 and other APIs, it supports standards based integration with a diverse range of third-party products.

- **Unmatched Partner Ecosystem:** Utilizing CipherTrust Application Data Protection and standards such as KMIP, CipherTrust Manager has more documented integrations than any other vendor in market. This is important for customers responsible for growing, diverse IT landscapes. Oracle and IBM are well suited for their own products but are primarily intended to support their ecosystem, not others.

- **Improved Scalability:** In head to head evaluations, CipherTrust Manager has proven superiority for clustering of a virtual CipherTrust appliance with a physical appliance to support high-availability configurations that protects against cloud outages. CipherTrust Manager is used by leading PaaS/IaaS/SaaS providers to fortify their offerings. It also now offers multi-domain support, further extending its scale with operational excellence.

- **Use Case Support**: CipherTrust Manager satisfies a variety of data compliance requirements (such as FIPS, PCI-DSS, GDPR, FISMA, and others) to separate encryption keys from the encrypted data. When combined with the encryption connector family of products, customers can leverage the solution for a variety of different data encryption uses cases, spanning file, database, big data, application, tokenization and virtual machine images.
- **Flexibility**: CipherTrust Manager comes in a variety of physical and cloud appliance types to satisfy various business and budget requirements—all form factors have consistent capabilities, management and interoperability. The IBM Key Management offerings for Enterprise (SKLM) and cloud (KeyProtect) bear no resemblance to each other and vary greatly in functionality.
- **Micro-services Architecture**: Built on a micro-services architecture for agile development using modular design. Auto-scaling capabilities will be available in the future.
- **Physical Appliance Improvements:** Improved bandwidth with NIC Bonding, optional 2x1GB/2x10GB NIC Interfaces for more scalable deployments

3.3 Will Virtual CipherTrust Manager run in clouds like Azure, AWS, GCP and private cloud solutions?

Yes. The Virtual CipherTrust Manager (NGKS) currently supports AWS, Microsoft Azure, Google Cloud Enterprise, IBM Cloud, Oracle Cloud, VMware, Microsoft Hyper-V and Openstack. Other public clouds can be adopted and supported within 1 release cycle (typically development for a new release is 3-4 months in duration).

4. KMIP

4.1 What changes if any are there in CipherTrust support of the OASIS KMIP standard?

CipherTrust includes a new KMIP server tailored to our new micro-service based architecture. As a result, CipherTrust Manager offers KMIP 1.4 support. A number of integrations have already been completed. Aside from ensuring CM/CDSP maintain certifications with leading partners, functionality will be expanded to also support crypto operations (such as Encrypt/Decrypt).

Not every application or appliance supports KMIP – fortunately, CipherTrust support many other methods with CipherTrust Application Data Protection and its APIs for JCE, ICAPI, .NET (which is a competitive differentiator) as well as a new native REST interface. Additionally, support for SafeNet Network HSMs and Cloud HSMs as a root of trust provides customers with a superior, scalable, one-stop-shop compared to any other vendor on the market.

KMIP has currently released a 2.0 spec and is working on the 2.1 draft. At this point in time, we continue to monitor developments in the OASIS working group and within our ecosystem to determine when we shift our implementation to 2.x.

4.2 What integrations are currently support via KMIP on the CipherTrust platform?

NetApp: Cloud OnTap 9.6-9.8. others under development

Dell EMC: PowerEdge, Compellent, DataDomain, Unity, VxRail, VxRack (others in progress)

VMware: vSAN, VMCrypt, vTPM

Nutanix

Hitachi VSP (others in progress)

Cisco Hyperflex

Quantum

HPE:

3PAR, Primera, ESL/MSL Tape, StoreOnce (KMIP) (others under evaluation)

Proliant, StoreEasy iLO (thru proprietary XML interface)

IBM: DS8000, DB2, Spectrum Scale (others under evaluation)

Infinidat: Infinibox

Commvault: Hyperscale and Data Protection Advanced,

Bloombase

Cloudistics

CommVault

Huawei OceanStor

Infinidat

MarkLogic

MongoDB

MySQL

Overland Tandberg

Fujitsu

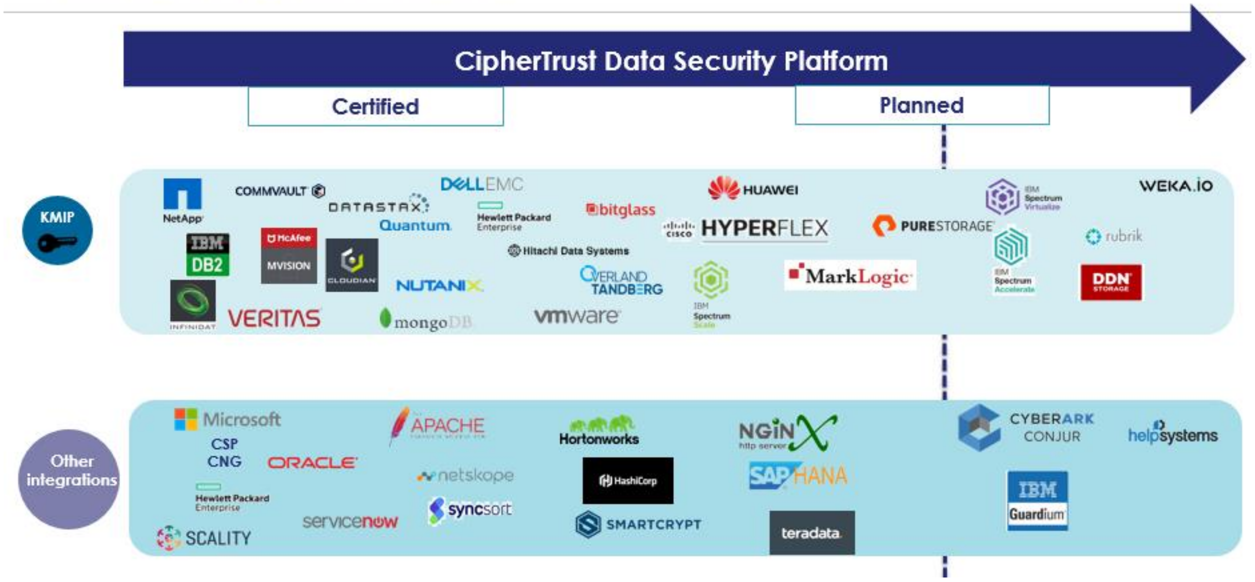
McAfee mVision (SkyHigh)

BitGlass

Datastax

There are a number of other integrations supported via NAE XML and REST, and the number of KMIP certifications will grow monthly. Please contact your SE or sales rep for further information.

Partner Ecosystem Overview



CipherTrust Data Security Platform

Certified

Planned

KMIP

Other integrations

5. Performance

5.1 What is the performance profile of CipherTrust Manager?

The virtual security appliances have similar profiles to their hardware counterparts. The appliance can support up to 1000 concurrent clients) and millions of keys. In the case of a virtual appliance, customers will need to tune their virtual machines to support key storage and performance requirements.

5.2 What do we mean by “software approaches” to key management?

Software approaches to key management require the customer to perform their own OS and VM hardening and secure configurations for database and key manager layers. This process is highly error prone and can introduce many vulnerabilities even when event performed by trained staff.

5.3 Are our virtual appliances a “soft approach” to key management?”

No. The CipherTrust Virtual appliances are dedicated and hardened virtual security appliances that remove software components of the OS not required to run the appliance or be used to circumvent security measures. The virtual machine is hardened according to the FIPS/NIST guidelines and the entire virtual machine is encrypted. Other security measures are built into the security appliance to mitigate attacks on encryption keys.

6. Specifications: Hardware and Software

6.1 CipherTrust Manager Hardware Specification

The following table helps to highlight the differences between physical appliance offerings:

Feature	K460 (Dell R330)	V6100 (SuperMicro)	K570 (AIC)
Chassis	1U with chassis intrusion detection	1U with chassis intrusion detection	1U with chassis intrusion detection
CPU	E3-1270v5 @3.6GHz		E3-1275v5 @3.6GHz
DRAM	8-16 GB DDR3/ECC (Recent upgrade)	16 GB	16GB DDR4/ECC
Disk	2 x 1TB SATA	1x 1TB	1 x 1TB SATA
RAID Controller	RAID 1	RAID1	RAID 1
Hot Swap HDD	Yes	No	No
Ethernet	2x1G or 4x1G	2x1GB	4 x 1G or 2 x 10G / 2x1G
Serial Port	1	1	1
PCIe Slot	1FH/1HH	??	2FH/1HH

6.2 CipherTrust Manager Safety Standard Specifications

Current Safety Standard Certifications	Countries/territory covered	Comment
CB Scheme	44 countries	Can be used to create country specific certificates
CSA-UL	Canada/US	
Current Emissions		
FCC Part 15, Subpart B, Class B	US	
EN55032:2010, EN55024:2010, EN61000-3-2:2006 +A1:2009 +A2:2009 EN61000-3-3:2008	EU	Used for CE mark
ICES-003 Issue 4 February 2004	Canada	

C-Tick AS/NZS CISPR 22:2009	Australia/NZ	
VCCI V-3/2009.04	Japan	
KN22, KN24, KC Mark	South Korea	
Optional (not done as part of our standard set today)		
NOM	Mexico	
BSMI	Taiwan	
BIS	India	

6.3 CipherTrust Platform Specifications

	K470	**K570**
Product Center	GA 15 Nov	GA 15 Nov
Keycard	N/A	K7
Hard Drive	1 X 2TB SATA SE (Spinning Disk)	1 X 2TB SATA SE (Spinning Disk)
Motherboard	AIC Antlia	AIC Antlia
CPU	E3-1275v6	E3-1275v6
Memory	16GB	16GB
NIC	4x1GB 2x10 GB / 2x 1GB	4x1GB 2x10 GB / 2x 1GB
Average Power (Watts)	0.7A @120V 84W	0.7A @120V 84W
Maximum Power (Watts)	100W	100W
Voltage	100-240V 50-60Hz	100-240V 50-60Hz
Power Cord	PSE Certified	PSE Certified
Dimensions	19.0"(W)21"(D)1.75"(H)	19.0"(W)21"(D)1.75"(H)
Weight	12.7 kg(28lbs)	12.7 kg(28lbs)
MTBF Telcordia	165279	153583
Operating temp	0~35	0~35
Storage temp	-20 - 60 °C	-20 - 60 °C
Relative Humidity	5% to 95% non-condensing	5% to 95% non-condensing
Airflow	Airflow is front to back and controlled within the appliance, no forced air is required by the installation	

Safety	Yes	Yes
Emissions	No KC Mark	Yes
Rails/Brackets	Non-sliding rail hardware and mounting brackets included. Sliding rails can be ordered.	Non-sliding rail hardware and mounting brackets included. Sliding rails can be ordered.

6.4 CipherTrust Platform Additional Specifications

	k570	k470	K470v	K170v
Max keys	1,000,000	1,000,000	Dependent on VM Configuration	Dependent on VM configuration
Max concurrent clients per cluster	1000	1000	1000	100
Redundant power supply	Yes	Yes	N/A	N/A
HSM Integration	Yes	Yes	Yes	Yes

6.5 HSM Compatibility

CipherTrust Platform will integrate with the following HSM platforms

- Gemalto Luna Hardware HSM v6 and v7
- Gemalto Data Protection on Demand (DPoD)
- AWS HSM
- Azure Dedicated HSM
- IBM Cloud HSM
- Thales TCT HSM for Government

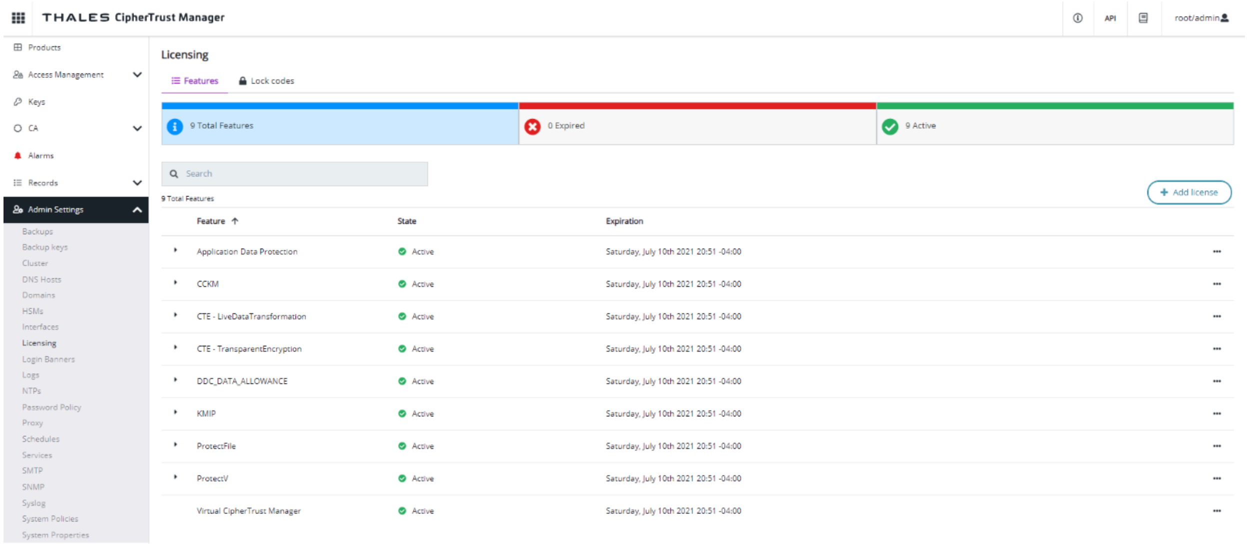
The k570 (which has a built in HSM card) will not support communications with an external HSM. It does offer the option ot PED or password based authentication. To learn more about authentication options, please review the following: https://thalesdocs.com/gphsm/luna/6.2/docs/pci/Content/overview/authentication/password-vs-ped_comparison.htm .
Both products contain the same FIPS140-2 L3 PCI-HSM card and will meet the same FIPS criteria as the KeySecure k460 or the Vormetric v6100 products.

Please note nShield HSMs are currently not supported with CipherTrust Manager.

7 Licensing and Migration

7.1 How does licensing work? Is it still based on an application/server connections to the appliance?

Yes. One of the new features with the platform is the ability for customers to be able to download and assign licenses within their organization thru access to our portal. The new Management Console allows admins the ability to define licenses as needed as well as have a readily available inventory thru a portal dedicated to the customer’s environment.



9 Total Features

Feature ↑	State	Expiration
Application Data Protection	Active	Saturday, July 10th 2021 20:51 -04:00
CCKM	Active	Saturday, July 10th 2021 20:51 -04:00
CTE - LiveDataTransformation	Active	Saturday, July 10th 2021 20:51 -04:00
CTE - TransparentEncryption	Active	Saturday, July 10th 2021 20:51 -04:00
DDC_DATA_ALLOWANCE	Active	Saturday, July 10th 2021 20:51 -04:00
KMIP	Active	Saturday, July 10th 2021 20:51 -04:00
ProtectFile	Active	Saturday, July 10th 2021 20:51 -04:00
ProtectV	Active	Saturday, July 10th 2021 20:51 -04:00
Virtual CipherTrust Manager	Active	Saturday, July 10th 2021 20:51 -04:00

7.2 How are CDSP Connectors licensed?

CipherTrust has introduced the concept of Flex Connector bundles. The bundles are groupings of CDSP products intended to allow customers to easily mix and match offerings. The bundle breakdowns are as follows:

Flex Connector-Basic	Flex Connector – Advanced	Flex Connector – Premium	Flex Utilities	Flex Ability	Other
• CTE (VTE replacement) • CTE User Space (NEW) • LUKS (KS Related) • CKM (TDE/SQL) • Integrations (based on KS NAE-XML and PKC#11 APIs	• CAPD (VAE replacement) • CTU (KS Related) • CT & CT-V (VTS)	• CTE SAP • CTE Teradata • CDP (KS related for db column level encryption) • CTP (VTPD) • CBDT (Batch Data Transformation)	• LDT • Efficient Storage • Container Security	• KMIP (VKMIP)	• DDC (based on amount of data) • CCKM (based on number of clouds)

Once purchased, customers are enrolled into the Thales EMS (Entitlement Management System). As licenses are purchased, customers are allocated license via EMS and provided the ability to assign these

Connector licenses to their CM deployment. For further information, login to the Thales Support Portal (https://supportportal.thalesgroup.com/) and search for KB0020558 (Thales CDSP Licensing).

7.3 So I am ready to migrate. What's the plan?

Customers need to complete the following steps to prepare and execute a migration strategy:

- Survey and document current use cases (appliances, cluster configuration, Connectors deployed, Production and Non-Production environments)
- Plan for Future Use Cases expected in the next 12- 24 months (Migration to Cloud, new data types subject to encryption, compliance standard changes, etc.)
- Prioritize and run Technical Proof of Concept for a subset of existing use cases. This will allow the customer to build familiarity with the new platform and connectors and ensure readiness to deploy CipherTrust Platform to production environments.
- Production Deployment Readiness: map required existing Connector licenses to new platform rollout
- Retire existing environment and commence using CipherTrust Platform into Production.

As always, engage our Sales and SE teams to assist in your analysis and proof of concept exercise to ensure as smooth a transition experience as possible

7.4 How much does it cost to migrate from KeySecure to CipherTrust Platform?

Current KeySecure customers have the following options to migrate to the CipherTrust Platform. Please fill-out the License Migration form on SFDC, to provide the customer's contact information and licensing details.

- **Physical Appliance**
  - In Place Upgrader (available for k450/k460 only): $10000 USD (on row 56 of the NG KS Price Intended for evaluation purposes and low volume transaction use cases.
  - Purchase New Physical Appliance: k470 or k570.
  - Purchase Virtual Appliance: (k170v or k470v), need to consider sizing of current physical environment to ensure virtual environment is equivalent or greater.

- **Virtual Appliance**

  The following scenarios are intended to provide guidance for owners of Perpetual and Term License scenarios:
  - Perpetual Scenario 1: Customer plans to migrate by expiration date of existing KS Maintenance Contract (within 1 year)
    - Customer will pay for maintenance on CipherTrust solution
    - Sales can defer maintenance until CM / CDSP is put into production
      - Support calls will be managed for both CipherTrust and KeySecure products during transition period.
  - Perpetual Scenario 2: Customer has more than 1 year maintenance (1+) remaining and may require more or less time to migrate (possibly until 12/31/2023)
    - Account team will work with customer to define new maintenance agreement (crediting existing maintenance contract) covering both KS and CM products (based on CM maintenance pricing)
    - Customer will be provided a pro-rated contract until such time as customer believes they will have "sufficiently" completed migration
  - Term Scenario 1: Customer plans to migrate by expiration date of existing KS Term License Bundle
    - Maintenance is automatically included in the new CM product sale.

- **Connectors**
  - All connectors from KS or DSM portfolios will migrate free of charge. Enhancements to functionality on CTE will be additional cost (e.g., Live Data Transformation, Efficient Storage, SAP, Teradata)
  - Account team must work to generate License Migration form to determine licenses to be migrated from KS to CM.
  - Further information on Connector licensing bundles can be found in our online documentation (https://thalesdocs.com/ctp/cm/latest/license/index.html)

7.5 How can I migrate Connector licenses from KeySecure to CipherTrust, especially when the licensing model for CipherTrust is completely different?

For KMIP and other connectors within the Encryption portfolio, the CipherTrust platform (CipherTrust Manager) provides improved license enforcement that will allow customers to manage their inventory of licenses through a secure licensing portal, and provide them an accurate display of deployed licenses (in use) and available licenses for KMIP or any other products within our portfolio.

As part of migration, KeySecure customers will be able to migrate existing KMIP licenses from current licensing mapped to new environment on a per cluster basis using the new licensing model. Customers are recommended to stage a parallel environment with the CipherTrust Manager before decommissioning of the existing KeySecure environment. Professional Service offerings will be available to assist in this effort.

Please work with your Thales Account team to complete the License Migration Form to generate your new CDSP Connector licenses.

7.6 What is process of swapping Virtual KeySecure/KS Connector with a Virtual CipherTrust Manager/CDSP Connector Deployment?

Your account representative will work with you to complete a license migration form. In preparation for this activity, please compile the following information for your Production and Test environments:

- **Current Appliance Type(s), Cluster ID(s) and Firmware Version:**
  This helps provide information on how current appliances are configured, and whether you plan to maintain a similar formation with CipherTrust or are looking to modify appliances in place
- **Current KS Connector(s) , Quantity Owned and Quantity to be Deployed, and Version(s)**
  This helps the Account team understand the current environment to be migrated. Please feel free to add additional/new requirements as necessary to provide full scope of effort for the CipherTrust deployment.

APPENDIX A: Affected KeySecure Appliance

The following list provides customers with a reference of earlier appliance releases in order to determine the appliance vintage and ease of migration

Physical Appliances

Part Number	Description
947-000314-002-000	KeySecure k250, V8.9.0 FIPS L1, 25,000 Keys Capacity
947-000347-002-000	KeySecure k250, V8.9.0, with Crypto pack FIPS L1, 25,000 Keys Capacity
947-000314-403-000	KeySecure K250,V8.9.0,Non-Production
947-000347-402-000	KeySecure K250,V8.9.0,with Crypto pack,Non-Production, FIPS L1, 25,000 Keys Capacity
947-000475-001-000	KeySecure K450,10G NIC,V8.4
947-000475-402	KEYSECURE K450,10G NIC,V8.4,NON-PRODUCTION
947-000513-001	KEYSECURE K450,10G NIC,V8.4,WITH CRYPTO PACK
947-000513-401	KEYSECURE K450,10G NIC,V8.4,WITH CRYPTO PACK,NON-PRODUCTION
947-000500-002-000	KeySecure K450,1G NIC,V8.4 FIPS L1, 1 Million Keys Capacity
947-000500-404	KEYSECURE K450,1G NIC,V8.4,NON-PRODUCTION
947-000503-002-000	KeySecure K450,1G NIC,V8.4,with Crypto pack FIPS L1, 1 Million Keys Capacity
947-000503-403-000	KeySecure K450,1G NIC,V8.4,with Crypto pack,Non-Production, FIPS L1, 1 Million Keys Capacity
947-000500-001	KEYSECURE K450,DEC-01,V8.X
947-000503-001	KEYSECURE K450,V8.0.1,WITH CRYPTO PACK
947-000504-001	KEYSECURE K460,10G NIC,V8.4 (INCL K6 CARD,LOCAL PED,10 IKEYS)
947-000504-401	KEYSECURE K460,10G NIC,V8.4 (INCL K6 CARD,LOCAL PED,10 IKEYS),NON-PRODUCTION
947-000517-001	KEYSECURE K460,10G NIC,V8.4 (INCL K6 CARD,REMOTE PED,10 IKEYS)
947-000517-401	KEYSECURE K460,10G NIC,V8.4 (INCL K6 CARD,REMOTE PED,10 IKEYS),NON-PRODUCTION
947-000477-401	KEYSECURE K460,10G NIC,V8.4 (INCL K6 CARD;NO PED OR IKEYS SHIPPED WITH UNIT),NON-PRODUCTION
947-000477-401	KEYSECURE K460,10G NIC,V8.4 (INCL K6 CARD;NO PED OR IKEYS SHIPPED WITH UNIT),NON-PRODUCTION
947-000505-001	KEYSECURE K460,10G NIC,V8.4,WITH CRYPTO PACK (INCL K6 CARD,LOCAL PED,10 IKEYS)
947-000505-401	KEYSECURE K460,10G NIC,V8.4,WITH CRYPTO PACK (INCL K6 CARD,LOCAL PED,10 IKEYS),NON-PRODUCTION
947-000516-001	KEYSECURE K460,10G NIC,V8.4,WITH CRYPTO PACK (INCL K6 CARD,REMOTE PED,10 IKEYS)
947-000516-401	KEYSECURE K460,10G NIC,V8.4,WITH CRYPTO PACK (INCL K6 CARD,REMOTE PED,10 IKEYS),NON-PRODUCTION
947-000325-002-000	KeySecure K460,1G NIC,V8.4 (INCL K6 CARD,LOCAL PED,10 IKEYS) FIPS L3, 1 Million Keys Capacity
947-000325-403-000	KeySecure K460,1G NIC,V8.4 (INCL K6 CARD,LOCAL PED,10 IKEYS),Non-Production, FIPS L3, 1 Million Keys Capacity
947-000518-001	KEYSECURE K460,1G NIC,V8.4 (INCL K6 CARD,REMOTE PED,10 IKEYS)
947-000518-401	KEYSECURE K460,1G NIC,V8.4 (INCL K6 CARD,REMOTE PED,10 IKEYS),NON-PRODUCTION
947-000324-002-000	KeySecure K460,1G NIC,V8.4 (INCL K6 Card;No PED or IKEYS Shipped with unit)

947-000324-403	KEYSECURE K460,1G NIC,V8.4 (INCL K6 CARD;NO PED OR IKEYS SHIPPED WITH UNIT),NON-PRODUCTION
947-000340-002-000	KeySecure K460,1G NIC,V8.4,with Crypto pack (INCL K6 CARD,LOCAL PED,10 IKEYS)
947-000340-403-000	KeySecure K460,1G NIC,V8.4,with Crypto pack (INCL K6 CARD,LOCAL PED,10 IKEYS),Non-Production FIPS L3, 1 Million Keys Capacity
947-000519-001	KEYSECURE K460,1G NIC,V8.4,WITH CRYPTO PACK (INCL K6 CARD,REMOTE PED,10 IKEYS)
947-000519-401	KEYSECURE K460,1G NIC,V8.4,WITH CRYPTO PACK (INCL K6 CARD,REMOTE PED,10 IKEYS),NON-PRODUCTION
947-000325-001	KEYSECURE K460,V8.0.1 (INCLUDES K6 CARD,LOCAL PED,10 IKEYS)
947-000325-401	KEYSECURE K460,V8.0.1 (INCLUDES K6 CARD,LOCAL PED,10 IKEYS),NON-PRODUCTION
947-000324-001	KEYSECURE K460,V8.0.1 (INCLUDES K6 CARD;NO PED OR IKEYS SHIPPED WITH UNIT)

Virtual Appliances

Part Number	Description
947-000295-001-000	Virtual KeySecure, V8.x, with Crypto Pack, Term Limited, 1 Year, Standard Support
947-000295-401-000	Virtual KeySecure, V8.x, with Crypto Pack, Term Limited, 1 Year, Standard Support
947-000296-001-000	Virtual KeySecure, V8.x, with Crypto Pack, Term Limited, 2 Year, Standard Support
947-000296-401-000	Virtual KeySecure, V8.x, with Crypto Pack, Term Limited, 2 Year, Standard Support
947-000297-001-000	Virtual KeySecure, V8.x, with Crypto Pack, Term Limited, 3 Year, Standard Support
947-000297-401-000	Virtual KeySecure, V8.x, with Crypto Pack, Term Limited, 3 Year, Standard Support
947-000298-001-000	Virtual KeySecure, K150v, V8.x, with Crypto pack, Perpetual
947-000298-401-000	Virtual KeySecure, K150v, V8.x, with Crypto pack, Perpetual, Non-Production
947-000310-001-000	VIRTUAL KEYSECURE, V8.x, TERM LIMITED, 1 YEAR, Standard Support
947-000310-401-000	VIRTUAL KEYSECURE, V8.x, TERM LIMITED, 1 YEAR, Standard Support
947-000311-001-000	VIRTUAL KEYSECURE, V8.x, TERM LIMITED, 2 YEAR, Standard Support
947-000311-401-000	VIRTUAL KEYSECURE, V8.x, TERM LIMITED, 2 YEAR, Standard Support
947-000312-001-000	VIRTUAL KEYSECURE, V8.x, TERM LIMITED, 3 YEAR, Standard Support
947-000312-401-000	VIRTUAL KEYSECURE, V8.x, TERM LIMITED, 3 YEAR, Standard Support
947-000313-001-000	Virtual KeySecure, K150v, V8.x, Perpetual
947-000313-401-000	Virtual KeySecure, K150v, V8.x, Perpetual, Non-Production
947-000405-001-000	Bundle,SafeNet Virtual KeySecure for Nutanix storage
947-000406-001-000	Virtual KeySecure, K150v, V8.x, Term Limited, 1 year, Plus Support
947-000406-401-000	Virtual KeySecure, K150v, V8.x, Term Limited, 1 year, Plus Support, Non-Production
947-000409-001-000	Virtual KeySecure, K150v, V8.x, with Crypto pack, Term Limited, 1 Year, Plus Support
947-000409-401-000	Virtual KeySecure, K150v, V8.x, with Crypto pack, Term Limited, 1 Year, Plus Support, Non-Production
947-000411-001-000	Virtual KeySecure, K150v, V8.x, Term Limited, 2 year, Plus Support
947-000411-401-000	Virtual KeySecure, K150v, V8.x, Term Limited, 2 year, Plus Support, Non-Production
947-000414-001-000	Virtual KeySecure, K150v, V8.x, with Crypto pack, Term Limited, 2 Year, Plus Support
947-000414-401-000	Virtual KeySecure, K150v, V8.x, with Crypto pack, Term Limited, 2 Year, Plus Support, Non-Production

947-000415-001-000	Virtual KeySecure, K150v, V8.x, Term Limited, 3 year, Plus Support
947-000415-401-000	Virtual KeySecure, K150v, V8.x, Term Limited, 3 year, Plus Support, Non-Production
947-000419-001-000	Virtual KeySecure, K150v, V8.x, with Crypto pack, Term Limited, 3 Year, Plus Support
947-000419-401-000	Virtual KeySecure, K150v, V8.x, with Crypto pack, Term Limited, 3 Year, Plus Support, Non-Production
947-000531-001-000	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Perpetual
947-000531-401	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Perpetual,Non Production
947-000531-401-000	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Perpetual,Non Production
947-000532-001-000	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,1 year,Plus Support
947-000532-401	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,1 year,Plus Support,Non Production
947-000532-401-000	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,1 year,Plus Support,Non Production
947-000533-001	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,2 year,Plus Support
947-000533-401	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,2 year,Plus Support,Non Production
947-000533-401-000	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,2 year,Plus Support,Non Production
947-000534-001-000	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,3 year,Plus Support
947-000534-401	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,3 year,Plus Support,Non Production
947-000534-401-000	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,3 year,Plus Support,Non Production
947-000535-001-000	Virtual KeySecure,K450v,V8.X,Perpetual License
947-000535-401	Virtual KeySecure,K450v,V8.X,Perpetual License,Non Production
947-000535-401-000	Virtual KeySecure,K450v,V8.X,Perpetual License,Non Production
947-000536-001-000	Virtual KeySecure,K450v,V8.X,Term Limited,1 year,Plus Support
947-000536-401	Virtual KeySecure,K450v,V8.X,Term Limited,1 year,Plus Support,Non Production
947-000536-401-000	Virtual KeySecure,K450v,V8.X,Term Limited,1 year,Plus Support,Non Production
947-000537-001-000	Virtual KeySecure,K450v,V8.X,Term Limited,2 year,Plus Support
947-000537-401	Virtual KeySecure,K450v,V8.X,Term Limited,2 year,Plus Support,Non Production
947-000537-401-000	Virtual KeySecure,K450v,V8.X,Term Limited,2 year,Plus Support,Non Production
947-000538-001-000	Virtual KeySecure,K450v,V8.X,Term Limited,3 year,Plus Support
947-000538-401	Virtual KeySecure,K450v,V8.X,Term Limited,3 year,Plus Support,Non Production
947-000538-401-000	Virtual KeySecure,K450v,V8.X,Term Limited,3 year,Plus Support,Non Production
947-000539-001	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,1 year,Standard Support
947-000539-401	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,1 year,Standard Support,Non Production
947-000540-001	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,2 year,Standard Support
947-000540-401	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,2 year,Standard Support,Non Production
947-000541-001	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,3 year,Standard Support

947-000541-401	Virtual KeySecure,K450v,V8.X,with Crypto Pack,Term Limited,3 year,Standard Support,Non Production
947-000542-001	Virtual KeySecure,K450v,V8.X,Term Limited,1 year,Standard Support
947-000542-401	Virtual KeySecure,K450v,V8.X,Term Limited,1 year,Standard Support,Non Production
947-000543-001	Virtual KeySecure,K450v,V8.X,Term Limited,2 year,Standard Support
947-000543-401	Virtual KeySecure,K450v,V8.X,Term Limited,2 year,Standard Support,Non Production
947-000544-001	Virtual KeySecure,K450v,V8.X,Term Limited,3 year,Standard Support
947-000544-401	Virtual KeySecure,K450v,V8.X,Term Limited,3 year,Standard Support,Non Production
947-000587-001-000	Virtual,Keysecure AWS,Term Limited,1 Year Plus Support

APPENDIX B: Product Mapping Guide

Vormetric Product	SafeNet / Gemalto Product	CipherTrust Connector	Notes
Vormetric Data Security Manager	KeySecure	CipherTrust Manager (CM) CipherTrust Cloud Key Manager (CCKM Embedded) CipherTrust Manager (KMIP Server is built into server)	Offers centralized key lifecycle management and access control to encryption keys
CipherTrust Cloud Key Manager (CCKM Appliance)			Supports cloud provider key management APIs for BYOK, HYOK and native cloud key life cycle management, logging and reporting.
Vormetric KMIP Server	KMIP Connector		Provides external key management for storage solutions (SAN and NAS storage arrays), self-encrypting drives and hyper-converged infrastructure.
Vormetric Transparent Encryption	ProtectFIle	CipherTrust Transparent Encryption (CTE)	Provides transparent encryption and access control for files/folders
	ProtectDB	CipherTrust Database Protection (CDP)	Protects transparent column-level encryption in databases
Vormetric Application Encryption	ProtectApp	CipherTrust Application Data Protection (CADP)	Offers DevSecOps friendly tools for key management and encryption operations
Vormetric Tokenization w/ Dynamic Data Masking	N/A	CipherTrust Vaultless Tokenization (CT-VL)	Provides dynamic data masking of sensitive data through APIs
N/A	Tokenization	CipherTrust Vaulted Tokenization (CT-V)	Offers non-disruptive format preserving tokenization with a wide range of options
Vormetric Protection for Teradata Database	N/A	CipherTrust Protection for Teradata Database (CPTD)	Protects transparent encryption of database columns in Teradata.
Vormetric Batch Data Transformation		CipherTrust Bulk Data Transformation (CBDT)	Provides static data masking of vast quantities of data quickly.
Vormetric TDE Key Agent (VKM)	TDE/EKM Connector	CipherTrust TDE Key Management	Provides Transparent Database Encryption (TDE) for Oracle DB and Microsoft SQL servers.