EOL or accelerate next?

By September 2017, RSA will reach end-of-life (EOL) for its tokenization and key management and encryption product, RSA Data Protection Manager (DPM). This will also affect any existing RSA Key Manager (RKM) customer or ex-RKM customer who upgraded to DPM when RKM was EOL in June 2014.

When RSA DPM is deemed EOL, this means RSA customers with DPM will no longer be supported with bug fixes and software updates. This applies for RKM too. Hence, DPM and RKM will increasingly become vulnerable to cyber-attacks and valuable sensitive data will be targeted by data thieves.

RSA customers can avoid this major security gap by migrating safely and securely to HPE SecureData with Hyper Secure Stateless Tokenization (SST) or HPE Enterprise Secure Key Manager (ESKM) with symmetric key management.

This document helps you understand the business interruptions that you may face, and offers a safe and secure migration path to HPE SecureData with Hyper SST or HPE ESKM to avoid these problems.

See figure 1 for a product mapping showing how RSA customers can migrate to HPE solutions.
HPE Enterprise Secure Key Manager

HPE ESKM is a complete key management solution to secure server, storage, and cloud against losses, mishandling, and administrative and operational attacks, with Key Management Interoperability Protocol (KMIP)-standardized interoperability and HPE Secure Encryption. It enables you to protect and ensure continuous access to business-critical, sensitive, data-at-rest encryption keys, both locally and remotely.

Why HPE?

• Safe and secure migration path—experts in this process
• Customer references—good track record across industries
• Hyper SST (no token database) and ESKM—innovative, powerful, highly scalable
• End-to-end payments protection—ability to protect transactions from card swipe or from browser to backend
• Multi-platform—supported from mainframe to open systems, Hadoop, and Big Data platforms
• Extends protection for Personally Identifiable Information (PII) and Protected Health Information (PHI) with the HPE SecureData platform, which can deliver both Hyper SST and Format-preserving Encryption (FPE)

Why migrate now?

• With an imminent RSA DPM EOL in a little over a year, support will be minimal, which adds security vulnerability. If you are considering moving from RKM to the latest release of DPM, this is a costly RSA Professional Services engagement as the move is to a platform, which is also on EOL list.
• Time is of the essence. Consider the potential brand damage of a data breach—the "front page" story of "major data breach, at Company X with legacy security product, EOL by their provider".
• To guarantee no disruption to tokenization and maintain the security of existing tokens, RSA customers need to take steps now to secure a new tokenization solution, such as HPE SecureData, which safely and securely migrates tokenization services.

Benefits of HPE Security solutions

RSA customers can continue securing their PCI data by safely and securely migrating to HPE SecureData with Hyper SST, which can reduce PCI compliance costs significantly.

RSA customers can migrate safely and securely to HPE ESKM, which can replace either DPM or RKM for symmetric key management. DPM is a superset of the legacy RKM. Even as HPE ESKM addresses RKM specifically, it can also address the key management within DPM, where many RSA customers may have migrated.

HPE SecureData with Hyper SST provides the following benefits:

• Secures sensitive PAN data via stateless tokenization
• Protects credit card and PAN data from breach by rendering it valueless to data thieves
• Safeguards brand reputation by neutralizing data breach
• Enables enterprises and merchants to remove stored credit card data from their environments completely
• Helps pass PCI audits and significantly reduces compliance audit scope and costs
• Enables business processes and analytics to be run on de-identified data

Figure 1: Product mapping for RSA customers to migrate to HPE Security solutions

HPE SecureData with Hyper SST

or

HPE Enterprise Secure Key Manager

For key management, RKM is fully EOL and RSA customers need to take steps now to secure a new solution. HPE ESKM is a great option to secure server, storage, and cloud against losses, mishandling, and administrative and operational attacks.
HPE ESKM provides the following benefits:

- Protects and preserves access to business-critical, sensitive, data-at-rest encryption keys, either locally or remotely
- Offers robust scalability with FIPS 140-2 level 2 validated for strong security standards; it is the industry’s first certified OASIS KMIP server product—no other competitor is certified today
- Scales easily to support thousands of clients, millions of keys, and multisite distributed clusters from 2–8 nodes
- Is a hardened, redundant appliance with millions of unit hours and zero loss of customer keys or data

What versions of RSA DPM and RKM products are facing EOL?

The RSA DPM product was available from 2012 through 2015 with three major versions:

- 3.1 or 3.2: End of Primary Support (EOPS) 30 June 2015; extended support through 30 June 2016
- 3.5.x: EOPS 30 September 2017; extended support through 30 September 2019

Even RSA customers on DPM 3.5.2 (the most up-to-date) should be aware that the product is EOL, and are receiving minimal support today.

RKM was widely sold and used for a variety of use cases—typically related to PCI compliance, from 2007 to 2012.

- Many RSA customers upgraded to DPM since RKM had been EOL since June 2014
- RSA encryption and key management on RKM are fully EOL—any RSA customer that is on RKM 2.x, DPM 3.1, or 3.2 is unsupported and must go to DPM 3.5.2

What is the migration path?

HPE SecureData migration basics

In broad terms, the migration process consists of the following steps:

- Designing and implementing the HPE SecureData system. The tokens that have been produced by the RSA system are not usable by other systems. They must be converted in order to use them with the HPE SecureData system.
- Re-tokenization of existing data. With Hewlett Packard Enterprise, you will de-tokenize the existing tokenized data using the RSA system and re-tokenize the data using HPE SecureData.
- Retiring the RSA system once the HPE SecureData system is running.
- Project coordination is important, as Hewlett Packard Enterprise will work with your team to make sure the project proceeds smoothly. A solutions delivery manager will set up clear and open lines of communication with your project manager.

HPE ESKM migration basics

- In qualified environments, enables migration of RSA keys to ESKM key management by acting as a proxy between RSA clients and legacy RSA servers to retrieve, vault and distribute keys using native RSA protocols.
- This incremental approach minimizes disruption by avoiding bulk decryption and re-encryption with a transition to standards-based key management (KMIP) that avoids vendor lock-in.

About HPE Security — Data Security

HPE Security — Data Security is a leader in data-centric security. It safeguards data throughout its entire lifecycle—at rest, in motion, in use—across the cloud, on-premise, and in mobile environments with continuous protection.

About HPE Security

Hewlett Packard Enterprise is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HPE Security ArcSight, HPE Security Fortify, and HPE Security — Data Security, the HPE Security Intelligence Platform uniquely delivers the advanced correlation and analytics, application protection, and data security to protect today’s hybrid IT infrastructure from sophisticated cyber threats.

Learn more at voltage.com
hpe.com/software/datasecurity