Data Security

Micro Focus® 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-premises, and in mobile environments with continuous protection. And, it provides safe, secure migration for RSA customers with end-of-life products.

Quick View

- Safeguards data throughout its entire lifecycle
- Provides safe, secure migration for RSA customers with end-of-life products
- RSA customers can continue securing their PCI data by safely and securely by migrating to SecureData with Hyper SST, which can reduce PCI compliance costs significantly
- RSA customers can migrate safely and securely to ESKM, which can replace either DPM or RKM for symmetric key management

On September 30, 2017, RSA reached end-of-life (EOL) for its tokenization and key management and encryption product, RSA Data Protection Manager (DPM). This also affected any existing RSA Key Manager (RKM) customers or ex-RKM customers who upgraded to DPM when RKM was EOL in June 2014.

The EOL status of RSA DPM means RSA customers with DPM will no longer be supported with bug fixes or software updates. This also applies to RKM. 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 Micro Focus Voltage SecureData with Voltage Hyper Secure Stateless Tokenization (SST) or Micro Focus Atalla Enterprise Secure Key Manager (ESKM) with symmetric key management.

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

![Figure 1. Product mapping for RSA customers to migrate to security solutions](image-url)
platform with ease of implementation. The advantages of Hyper SST include random tokens with no databases, no data synchronization, no collisions, and high performance. Hyper SST is part of the SecureData platform, which unites marketleading encryption, tokenization, data masking, and key management to protect sensitive information in a single comprehensive solution.

Atalla Enterprise Secure Key Manager
Atalla 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 Micro Focus 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 Migrate Now?

- Now that RSA DPM is in EOL, its lack of support increases your security vulnerability.
- 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 secure a new tokenization solution, such as SecureData, which safely and securely migrates tokenization services.
- For key management, RKM is fully EOL. Customers need to take steps now to secure a new solution. ESKM is a great option to secure server, storage, and cloud against losses, mishandling, and administrative and operational attacks.

Why Micro Focus?

- 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 Voltage SecureData platform, which can deliver both Hyper SST and Formatpreserving Encryption (FPE)

Benefits of Micro Focus Security Solutions
RSA customers can continue securing their PCI data safely and securely by migrating to SecureData with Hyper SST, which can reduce PCI compliance costs significantly. RSA customers can migrate safely and securely to ESKM, which can replace either DPM or RKM for symmetric key management. DPM is a superset of the legacy RKM. Even as ESKM addresses RKM specifically, it can also address the key management within DPM, where many RSA customers might have migrated.

SecureData with Hyper SST provides these 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

ESKM provides these 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 two to eight 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 because RKM has 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 SecureData Migration Path?
In broad terms, the migration process consists of the following steps:

- Designing and implementing the 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 SecureData system. Micro Focus will help you design and implement the SecureData system in your pre-production and production environments.
- There is modest application modification. Applications that are currently making calls to the RSA system will need to be modified to go to the Micro Focus system instead. Since all applications using the RSA system are already making a request for tokenization or de-tokenization operation, this is generally a minor change, rather than a major re-engineering effort.
- Re-tokenization of existing data. You will de-tokenize the existing tokenized data using the RSA system and re-tokenize the data using SecureData.
- Retiring the RSA system after the SecureData system is running.

Project coordination is key. Micro Focus 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.

Training sessions for your staff will include an introduction to SecureData, system administrator training, programmer training, and code review sessions.

Learn More At www.microfocus.com/data-security-encryption