SOLUTIONS BRIEF

Enterprise Migration Path for RSA DPM and RCM Users

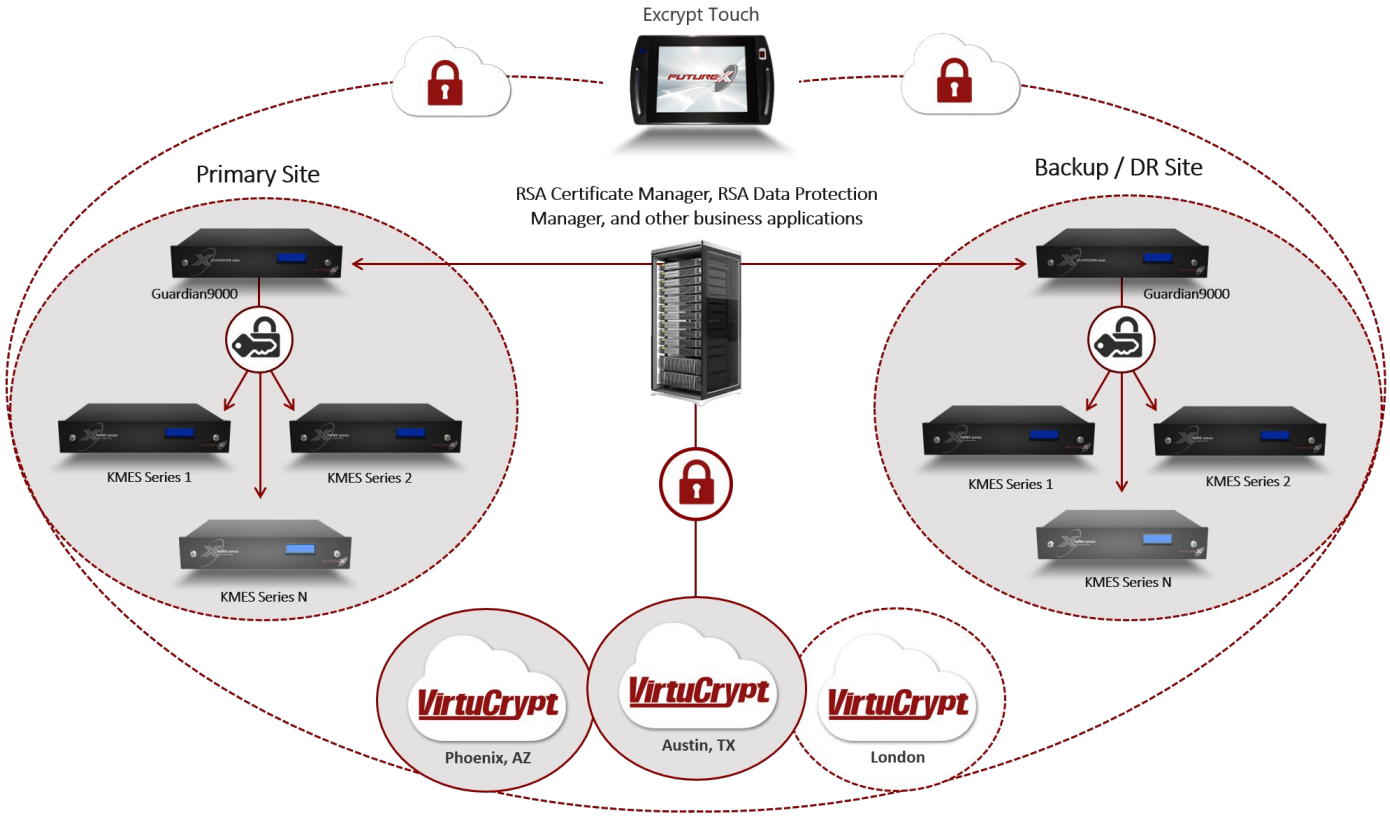
RSA_Migration.9/19/19.14:28

RSA DPM & RCM AND THE FUTUREX HARDENED ENTERPRISE SECURITY PLATFORM

RSA will soon discontinue support for its RSA Data Protection Manager (DPM) product line, which includes solutions for three encryption tasks: tokenization, application encryption, and key management. Similarly, RSA has announced end of product support for its RSA Certificate Manager (RCM) line, which includes the RSA Registration Manager and the RSA Validation Manager. Futurex offers a complete replacement to these products, adding both value and advanced functionality to current infrastructure. The Hardened Enterprise Security Platform performs tokenization, application encryption, symmetric key management, and asymmetric key management among many other encryption tasks.

WHAT IS THE HARDENED ENTERPRISE SECURITY PLATFORM?

The Hardened Enterprise Security Platform is a collection of interoperable solutions that form an entire cryptographic infrastructure unique to the individual customer environment. It's a powerful platform capable of replacing either RSA DPM or RCM. The solutions can act both independently and interdependently, building off of each other to add industry-leading speeds, advanced functionality, and an easy experience. Supported by the Base Architecture Model (BAM) and a common interface and feature set across all solutions, the Hardened Enterprise Security Platform is built with zero reliance on third-party software or hardware. The diagram below shows a simple example of the Hardened Enterprise Security Platform.



The environment exemplified above has a primary site and a backup site, which mirrors the primary site. The KMES Series Key Management Enterprise Server provides symmetric and asymmetric key and certificate management. Meanwhile, the Guardian9000 provides centralized management, redundancy, load balancing, and monitoring.

Should there ever be an unexpected disaster, natural or man-made, the backup site will automatically take over all cryptographic tasks with zero downtime. The VirtuCrypt cloud offers additional scalability, testing environments, and add-on services through a compliant, cloud-based infrastructure. The redundancy, power, and functionality of this example captures the essence of the platform, but it only scratches the surface. The platform scales virtually limitlessly, and takes on the shape of the infrastructure it supports—including those infrastructures currently using RSA DPM or RSA RCM.

HOW DOES THE HARDENED ENTERPRISE SECURITY PLATFORM COMPARE?

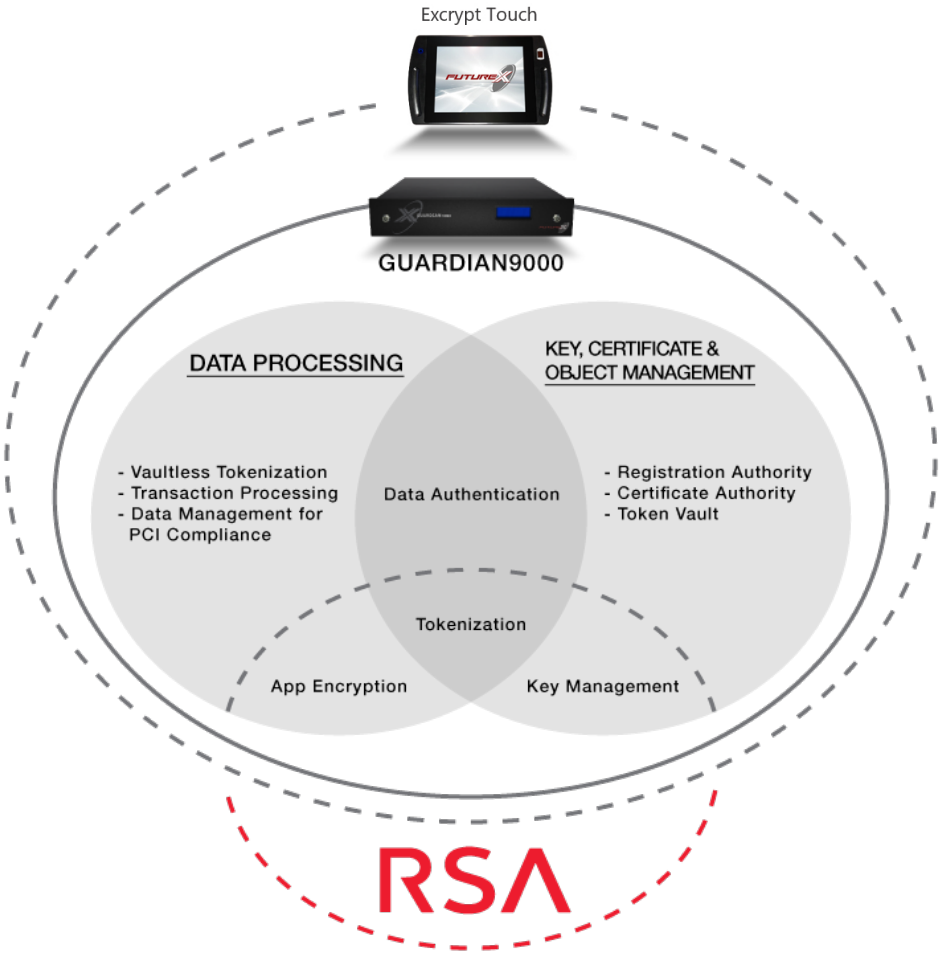
There are three products in the RSA DPM solution suite that will soon reach their end of life: the RSA Data Protection Manager Appliance, RSA Data Protection Key Client, and the RSA Data Token Client. All three can roughly be mapped to two categories of Futurex solutions: hardware security modules, such as the Vectera Plus, or key management servers, such as the Key Management Enterprise Server (KMES) Series. The same can be said of the RSA Certificate Manager product suite, including the RSA Registration Manager and the RSA Validation Manager. This means the tasks of six different RSA software-based solutions, and more, can be accomplished using only two Futurex devices.

A Futurex key and certificate management server such as the KMES Series and a hardware security module such as the Vectera Plus, as part of the Hardened Enterprise Security Platform, form the foundation of a replacement for RSA DPM and RCM.

RSA DPM AND THE HARDENED ENTERPRISE SECURITY PLATFORM

The RSA DPM product solutions accomplish approximately three different tasks. The first is application encryption, which includes the use of various standardized algorithms to encrypt data of varying types. The second is tokenization, which includes the ability to tokenize (replace with meaningless values) data. Finally, the RSA DPM product suite includes a solution for symmetric key management operations, including maintaining the lifecycle of keys and storing tokens alongside them in a vaulted database.

The Hardened Enterprise Security Platform covers all of these tasks and adds some value unavailable when using RSA DPM, as shown in the diagram on the following page.



In addition to performing the three tasks of the RSA DPM in more depth, the Hardened Enterprise Security Platform can provide secure, centralized and remote management platforms via the Guardian9000 and Excrypt Touch. In the graphic above, the Guardian9000 introduces centralized management, monitoring, log auditing, and alerting for the entire platform while the Excrypt Touch enables keying operations to be handled across multiple data sites from afar.

RSA RCM AND THE HARDENED ENTERPRISE SECURITY PLATFORM

Note that the above diagram provides an overview of the various tasks that the Hardened Enterprise Security Platform completes in relationship to RSA DPM, but the same devices which perform these tasks also perform the tasks of the RSA Registration Manager and the RSA Validation Manager. Certificate authority, as defined by Futurex devices, includes such tasks as certificate validation and certificate revocation (accomplished through both OCSP and CRLs). Furthermore, full certificate authority, registration authority, and key and object management lifecycles can be accomplished through the same platform.

IMPORTANT FEATURE SETS OF THE PLATFORM

The following is a feature to feature comparison of RSA and Futurex platforms.

Key, Certificate, and Object Management			
Feature	**Futurex**	**RSA**	**Notes**
Key Management Interoperability Protocol (KMIP)	Futurex Hardened Enterprise Security Platform	RSA DPM	Server-side KMIP support for KMIP client devices and a wide variety of applications.
OCSP	Futurex Hardened Enterprise Security Platform	RSA RCM	Use certificate revocation lists or online certificate status protocol.
Certificate authority	Futurex Hardened Enterprise Security Platform	RSA DPM and RCM	Futurex allows request, registration, generation, issuance, and revocation in one platform.
Secure key management	Futurex Hardened Enterprise Security Platform	RSA DPM	Hardware-based, access-controlled key/object storage and management enforcing physical and logical security.
Remote key management	Futurex Hardened Enterprise Security Platform		Manages keys from anywhere in the world with the hand-held Excrypt Touch tablet.
Registration authority	Futurex Hardened Enterprise Security Platform	RSA RCM	Web portal-based registration authority that can be white labeled to fit an organization's brand.
Certificate validation	Futurex Hardened Enterprise Security Platform	RSA RCM	Certificates are validated by a FIPS-140 2 Level 3 cryptographic device.
MS Active Directory Certificate Services integration	Futurex Hardened Enterprise Security Platform	RSA DPM	Enterprise-certificate authority server supporting AD CS and expedited signing and encryption activities.

Application Encryption			
Feature	**Futurex**	**RSA**	**Notes**
PKCS #11	Futurex Hardened Enterprise Security Platform	RSA DPM	Automation of cryptographic tasks using a standards-based library.
Data-agnostic format preserving encryption	Futurex Hardened Enterprise Security Platform	RSA DPM	Any data type supported; data can be obfuscated without losing referential integrity.
Transaction processing and validation	Futurex Hardened Enterprise Security Platform		Some of the fastest transaction processing speeds in the world.
Management of PCI compliance data	Futurex Hardened Enterprise Security Platform		Detailed reporting, monitoring, and logging as well as documentation services and audit preparation.

Tokenization			
Feature	**Futurex**	**RSA**	**Notes**
HMAC-based tokenization and hashing	Futurex Hardened Enterprise Security Platform	RSA DPM	Cannot be decrypted.
Tokenization using AES encryption	Futurex Hardened Enterprise Security Platform	RSA DPM	Hardware-based, cryptographically strong AES encryption of varying bit strengths. Tokens are reversible.
Vaulted tokenization	Futurex Hardened Enterprise Security Platform	RSA DPM	Tokens stored in a hardware-based secure vault located in an access-controlled environment.
Vaultless tokenization	Futurex Hardened Enterprise Security Platform		

THE ROLE OF VIRTUCRYPT

VirtuCrypt offers the functionality of the Hardened Enterprise Security Platform delivered via cloud service. The Hardened Enterprise Security Cloud combines the convenience of the cloud with the robust security only afforded by hardware-based security modules. The VirtuCrypt Hardened Enterprise Security Cloud offers three different options: VirtuCrypt Enterprise, VirtuCrypt Elements, and VirtuCrypt Plus. A combination of these solutions can allow organizations to build a solution that is fully or partially hosted by VirtuCrypt, meaning VirtuCrypt shoulders the costs of maintaining devices in an SSAE 16 (SOC 1, 2, and 3), PCI, TIA-942 Tier 4, and HIPAA-compliant datacenter. Alternately, organizations can add specific cryptographic functionalities using VirtuCrypt Elements. This means that organizations migrating from their end of life solutions, such as RSA DPM or RSA RCM, can move into a more flexible solution that accommodates their needs.

FUTUREX PROCEDURE FOR END OF LIFE PRODUCT MIGRATION

The amount of time it takes to migrate from a platform reaching end of life and end of product support depends on a number of factors, the most significant of which is the number of applications that will need to migrate over to the new system.

Some questions organizations should ask as they approach the decision to migrate:

- How many applications will migrate, and were they developed in-house or using third-party software?
- What functionalities are needed now and in the future?
- How many encryption keys will need to be moved or translated?
- What needs to be tokenized, retokenized, or detokenized, if possible?
- What bridges between application programming interfaces (APIs) will need to be built, if any?

While just a sample of a larger question base, these questions help gauge the overall scope of a migration project and time required. Futurex has established a migration pathway for end-of-life devices and application which takes into account organization responses to these questions as well as industry expertise from our team of CTGA-accredited Solutions Architects.

STEP 1: ANALYSIS AND DESIGN

To understand the unique needs of an organization, Futurex's team of CTGA-accredited Solutions Architects offer customized consulting—analyzing cryptographic infrastructures and helping to design a custom, turnkey solution based on the Hardened Enterprise Security Platform or Cloud.

STEP 2: TURNKEY DEPLOYMENT

Once the cryptographic environment has been analyzed and a solution designed, a turnkey deployment can take place. In the meantime, CTGA-accredited Solutions Architects help organizations develop documentation and train employees on the proper usage of the custom solution. The Solutions Architect team can also help organizations prepare for compliance audits.

STEP 3: FUTURE EXPANSION

As a business grows, so too does its cryptographic needs. Expansion can take many forms, including increasing cryptographic throughput, adding additional functionalities, or requesting custom development initiatives.

THE RIGHT QUESTIONS TO ASK

Poising the right questions during the migration process can have a direct impact on the success of the project. Arriving at the unique answers to important questions will streamline the project and help identify goals, needs, and potential pitfalls. As a matter of perspective, when a product such as RSA DPM reaches end of product support, treat the resulting change as an opportunity to review and expand your organization's current infrastructure.

We've separated the questions out based on the perspectives of three key parties: executives, system administrators, and developers.

FOR EXECUTIVES

- What is our current infrastructure costing us?
- What will it cost us to maintain an unsupported product?
- How can we better support projected growth?
- How large is the organization currently, and how will that impact the migration process?
- What is the long-term return on investment for a new solution?

FOR SYSTEM ADMINISTRATORS

- How will the end of support for our existing product impact our infrastructure security?
- What can be done do fortify that security?
- How do we currently manage user roles and permissions, and how can that be made better?
- What works and what doesn't within the existing infrastructure?
- How do we handle monitoring and alerting? Can this be improved?
- How many encryption keys and of what kind will need to migrate?
- Have we suffered from issues related to ease of use and user friendliness?
- What additional functionality do we need either now or in the future?

FOR DEVELOPERS

- How many in-house applications need migrating?
    - Do we have the source code for these applications?
- What throughput ratings will we need now and in the future?
- How many databases need to be tokenized, or, if applicable, retokenized? Detokenized?
- What has worked with our current API command protocols? What hasn't?

THE BENEFIT OF THE HARDENED ENTERPRISE SECURITY PLATFORM

The Hardened Enterprise Security Platform can help organizations both ask the right questions and provide answers. Futurex devices have numerous benefits outside of their ability to perform all of the functions of RSA DPM and RCM. Those benefits cascade down from executives down to the developer.

FOR EXECUTIVES

A migration to the Hardened Enterprise Security Platform benefits executives primarily in three arenas.

- Single-vendor, turnkey solution with 24x7x365 support
- FIPS 140-2 level 3-validated cryptographic hardware hosted by you or through the VirtuCrypt cloud
- Customized, lean solutions based on cryptographic need to control costs, scaling to the n^{th} degree as necessary

FOR SYSTEMS ADMINISTRATORS

The Hardened Enterprise Security Platform makes life far easier for system administrators.

- Centralized device management with central audit logging and reporting based on user-defined parameters via the Guardian9000
- Full key and certificate lifecycle management
- Remote keying operations via the Excrypt Touch
- Easy to use application interface, with common functionality across all Futurex devices
- Redundantly designed hardware with disaster recovery and backup
- Device interoperability that allows for globally scalable operations

FOR DEVELOPERS

Finally, developers likewise benefit from the Hardened Enterprise Security Platform, particularly when using the Excrypt API.

- Developer-centric design supports reuse of functionality across multiple applications and growth in use of cryptographic technology over time
- RESTful API for custom HTTP requests to managed devices using the Guardian9000
- Diverse, extensible API with intuitive command syntax using field identifiers to parse data

OTHER REASONS TO MIGRATE TO FUTUREX

With RSA DPM and RCM, organizations must rely on third-party vendors for the hardened security component of the applications. This is not the case with the Futurex Hardened Enterprise Security Platform or the VirtuCrypt Hardened Enterprise Security Cloud. Futurex manufacturers and supports its own hardware, and its turnkey solutions are built such that organizations can base their entire cryptographic infrastructure on a single source.

Furthermore, because the Hardened Enterprise Security Platform relies on a Base Architecture Model, devices are updated swiftly and propagated to the entire platform easily. Similarly, the platform maintains a consistent, easy-to-use, and aesthetically pleasing graphical user interface across all devices—making use and training convenient and cost effective. The Hardened Enterprise Security Platform not only provides a replacement for end of life RSA products, but also for an organization's entire core cryptographic infrastructure.

For more information, visit the Futurex website, and contact us to schedule a custom webinar and discover how your organization can benefit by switching to the Hardened Enterprise Security Platform.

FUTUREX ENGINEERING CAMPUS
OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163