THALES

www.thales-esecurity.com

MICROSOFT AND THALES DELIVER PERSISTENT INFORMATION PROTECTION WITH UNIQUE 'BYOK' OPTION THAT PUTS YOU IN CONTROL IN THE CLOUD

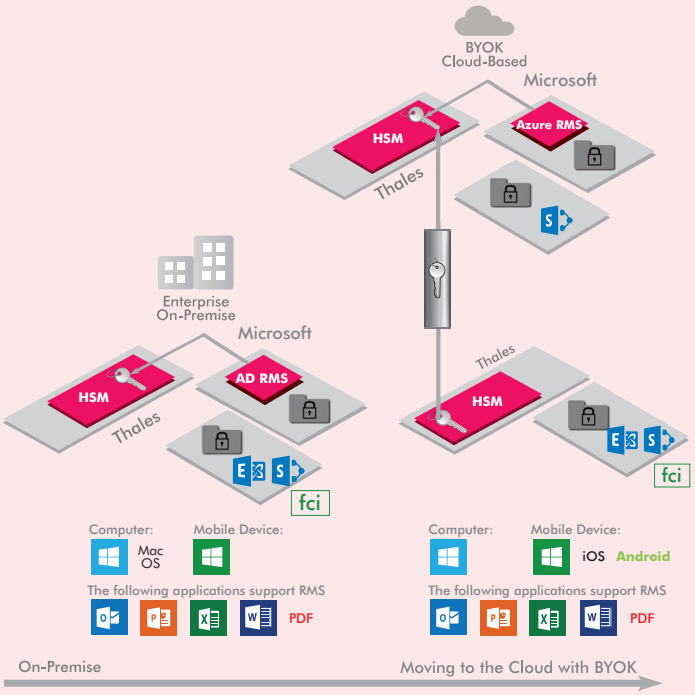
Solution Benefits

- Apply access and usage controls on the data you exchange across organizations
- Provide hardened key protection to RMS on-premise, cloud and hybrid solutions
- Deliver robust FIPS 140-2 certified key protection and lifecycle management
- Place you in control of keys that protect your sensitive data and intellectual property
- Ensure keys are never visible to Microsoft with the Bring Your Own Key (BYOK) option

Microsoft

Thales e-Security

Enhanced Security: Thales High Assurance for Microsoft RMS



Whether using RMS on-premise, in a hybrid configuration or completely in the cloud, Thales nShield HSMs deliver indispensable control over your critical keys.

Microsoft Rights Management Services (RMS) protects the data exchanged within your collaborative work environment by embedding enforceable security policies right on the data assets, no matter the data type. As a hosted subscription service, you can run applications on-demand without an IT infrastructure and ensure your information is protected across organizational boundaries.

The Problem: Collaborative Work Environments Require Persistent Information Protection

RMS employs cryptography to deliver controlled access and persistent protection to your data. The security of RMS depends on the level of protection given to the critical cryptographic keys. Exposure of keys compromises your sensitive data.

The Challenge: Maintaining Control of the Server Key that Secures your Sensitive Data

Deployment of on-premise AD RMS with a hardware security module (HSM) enables you to safeguard and manage the server key protecting your data. When using Microsoft Rights Management service (Windows Azure RMS), you don't have to give up control of the key securing your data in the cloud. Azure RMS uses Thales HSMs in such a way that you can ensure that your key is always under your control and never visible to Microsoft.

Enhanced Security: Thales High Assurance for Microsoft RMS

The Solution: Microsoft RMS with Enhanced Key Control from Thales

Thales nShield HSMs create tight controls around the management and use of the server key in Microsoft RMS deployments – on-premise and in the cloud.

If you use enterprise AD RMS: Thales nShield HSMs provide you a hardware solution to protect your critical server key. Thales nShield HSMs safeguard and manage the server key completely independent of the software environment.

If you subscribe to Azure RMS: Your server key becomes your tenant key. By default, Azure RMS generates and manages the lifecycle of your tenant key, but you can choose to protect your tenant key within a robust boundary using Thales HSMs. Thales HSMs generate, safeguard and manage the tenant key putting you, not Microsoft, in control.

If you adopt the BYOK option: Thales provides you the unique capability to generate your own tenant key on-premise per your IT policies and to transfer it securely to the cloud-based Thales nShield HSM hosted by Microsoft – effectively matching the security properties of an on-premise RMS deployment. While Azure RMS can use your tenant key and replicate it for disaster recovery, Microsoft cannot see or access your tenant key. BYOK ensures that your tenant key cannot be recovered from the HSMs in Microsoft's possession.

For additional security, near-real time usage logs allow you to see exactly how and when your key is used by Azure RMS. A future option will add capability to lend your key to the Microsoft-managed HSM for only short periods of time enabling you to further control its use and potential abuse.

Why use Thales HSMs with Microsoft RMS

If you use AD RMS on-premise now and want to leave your options open to move to Azure RMS, Thales nShield HSMs make it easy to securely migrate the on-premise AD RMS server key to the Azure RMS tenant key environment. Thales nShield HSMs:

- Transfer the tenant key securely from a Thales nShield HSM in your possession to a Thales nShield HSM in Microsoft possession without leaving the security boundary created by the HSMs
- Protect the tenant key while in Microsoft possession
- Secure the tenant key within a FIPS 140-2 certified cryptographic boundary that employs robust access control mechanisms with enforced separation of duties to ensure the key is only used for its authorized purpose
- Ensure tenant key availability using key management, storage and redundancy features

Thales nShield HSMs create a locked cage protecting your critical tenant key, neutralizing the perception that sensitive data maintained in the cloud is vulnerable because the cloud can only be a shared service with a shared security infrastructure.

Thales

Thales nShield HSMs maintain your key securely locked and usable only within the HSM. This enables you to maintain custody of your key and visibility over its use. Thales nShield HSMs:

- Protect keys in a hardened, tamper-resistant environment
- Enforce security policies, separating security functions from administrative tasks
- Comply with regulatory requirements for public sector, financial services and enterprises

Thales nShield HSMs are available to match specific performance and budgetary needs:

- For high-volume on-premise key generation and management (or as part of a hybrid deployment), **nShield Solo** embedded PCIe card and **nShield Connect** network-attached appliance provides high performance hardware security
- For low-volume on-premise key generation as part of the BYOK capability, **nShield Edge** provides convenient USB-attached hardware security

Microsoft

Microsoft has transformed the way businesses create and share content and build collaborative processes. Systems based on Microsoft RMS solutions maximize productivity. To protect data, Microsoft RMS uses cryptography to establish trustworthy business environments that:

- Manage identities across organizations
- Distribute certificates for authentication
- Control user access rights to data resources
- Provide total information protection

You can contact Thales at: msrms-hsm@thalesesec.com

For more information visit www.thales-esecurity.com/msrms or www.microsoft.com/rms

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Unit 4101, 41/F, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com