

User Guide

FORTANIX DATA SECURITY MANAGER WITH AWS XKS - CONCEPTS

VERSION 1.0

1.0	INTRODUCTION	2
1.1	Terminologies	2
1.2	DSM With AWS XKS – Use Cases	3
1.3	DSM with AWS XKS - Advantages	3
2.0	DSM WITH AWS XKS WORKFLOW	4
3.0	DSM WITH AWS XKS - INTEGRATION	5
4.0	DOCUMENT INFORMATION	6
4.1	Document Location	6
4.2	Document Updates	6

1.0 INTRODUCTION

Welcome to the **Fortanix Data Security Manager (DSM)** with **Amazon Web Services (AWS) External Key Store (XKS)** documentation.

The Fortanix DSM integration with AWS XKS enables organizations to protect the data in AWS with keys stored in Fortanix DSM.

This document describes the following topics:

- DSM with AWS XKS use cases.
- Advantages of DSM with AWS XKS integration.
- DSM with AWS XKS workflow.
- DSM with AWS XKS integration.

1.1 TERMINOLOGIES

- **Fortanix Data Security Manager (DSM) –**

Fortanix DSM is the cloud solution secured with Intel® SGX. With Fortanix DSM, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data.

- **AWS KMS –**

AWS Key Management Service (AWS KMS) lets AWS users create and control cryptographic keys and their access policies for use by a large number of AWS Services.

- **AWS XKS –**

The External Key Store (XKS) feature allows AWS KMS users to establish an external Root of Trust for encryption keys managed by KMS. With XKS, AWS users can externally generate, host, and manage Root Keys to protect data encryption keys used by AWS Services and applications.

1.2 DSM WITH AWS XKS – USE CASES

The Fortanix DSM with AWS XKS integration provides Fortanix customers the ability to migrate privacy-sensitive workloads for highly regulated industries, such as financial services and healthcare, to the public cloud and comply with the highest data privacy regulations.

1.3 DSM WITH AWS XKS - ADVANTAGES

The following are the advantages of Fortanix DSM with AWS XKS integration:

- The users have complete custody of their keys and full control over the data encryption policies within AWS. This control helps them in specifying the location of the keys, and from where they may be accessed.
- Fortanix DSM offers comprehensive audit logs, so the users may demonstrate that their security controls adhere to regulations like the GDPR.
- AWS provides strong key protection, and Fortanix does not compete with these functions. Instead, Fortanix provides Segregation of Duties with external, granular access control.

2.0 DSM WITH AWS XKS WORKFLOW

XKS allows AWS KMS to use external, customer-managed root keys, giving the customer more control over key management and data security initiatives. Fortanix DSM is solely responsible for creating, safeguarding, and using the customer's root keys.

The figure below depicts how AWS XKS integration with Fortanix DSM works.

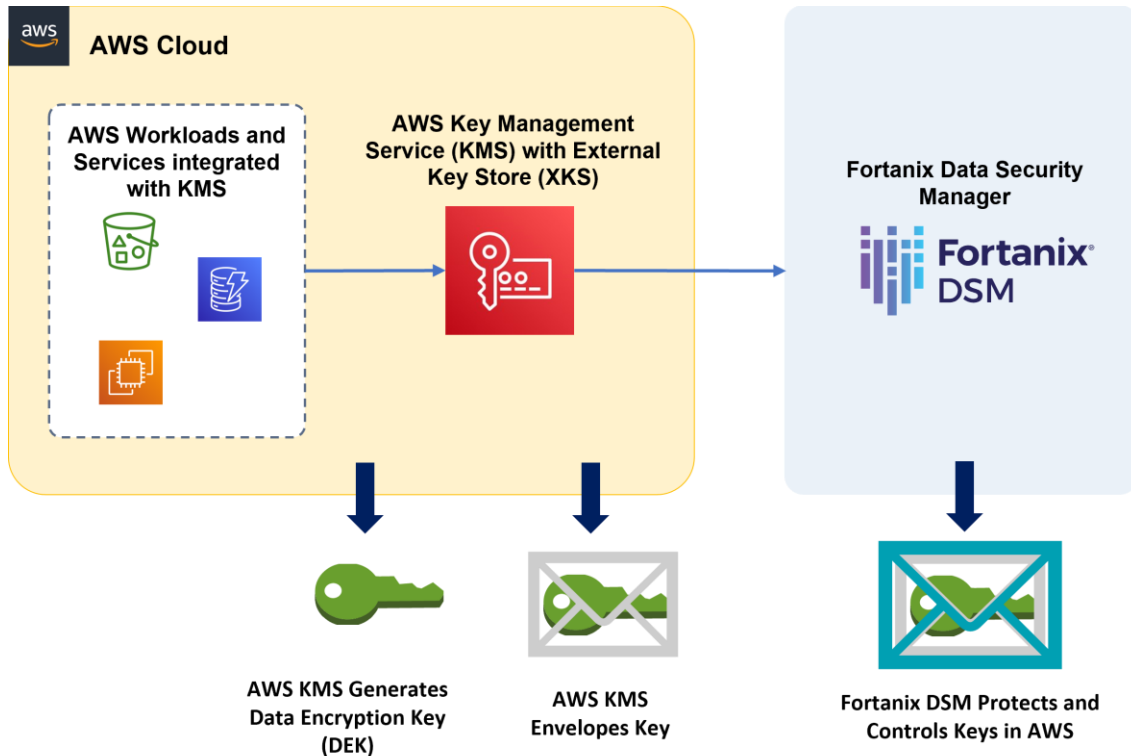


FIGURE 1: FORTANIX DSM WITH AWS XKS WORKFLOW

The workflow between the various services is as follows:

1. A supported AWS service calls KMS and asks for a new Data Encryption Key (DEK) in an XKS-backed Key Store. For instance, this could be S3 to encrypt an uploaded file for storing in a bucket.
2. KMS generates the DEK and envelopes (encrypts) it using a key store-specific Key Encryption Key (KEK)
3. KMS calls Fortanix DSM which, upon satisfying access controls and policies, envelopes the already enveloped key using a DSM-protected Root KEK.
4. DSM sends the double encrypted DEK back to KMS.

5. KMS stores the double enveloped DEK in its Key Store.
6. KMS then immediately retrieves the DEK, unseals the double envelope by sending it back to DSM and opening the inner envelope itself, and hands the DEK to the calling service for use. Every time the calling service needs the DEK (for instance, S3 to satisfy a download request of the encrypted file), the last step (*Step 6*) is repeated.

3.0 DSM WITH AWS XKS - INTEGRATION

With FIPS 140-2 Level 3 certified™ HSM protection, Fortanix DSM is available as an on-premises solution as well as a SaaS offering.

- In an AWS XKS with DSM SaaS integration, the AWS service reaches out to the Fortanix DSM service to access the user's Root Key.
- For on-premises Fortanix DSM clusters, the users need to allow network access from AWS.

For the Fortanix DSM with AWS XKS integration steps, click [here](#).

4.0 DOCUMENT INFORMATION

4.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

<https://support.fortanix.com/hc/en-us/articles/11201117419412-Fortanix-DSM-with-AWS-External-Key-Store-XKS-Concepts>

4.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com

© 2016 – 2022 Fortanix, Inc. All Rights Reserved.

Fortanix® and the Fortanix logo are registered trademarks or trade names of Fortanix, Inc.

All other trademarks are the property of their respective owners.

NOTICE: This document was produced by Fortanix, Inc. (Fortanix) and contains information which is proprietary and confidential to Fortanix. The document contains information that may be protected by patents, copyrights, and/or other IP laws. If you are not the intended recipient of this material, please destroy this document and inform info@fortanix.com immediately.