Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER – KEY OPERATIONS

VERSION 1.0

Fortanix Inc. | 800 West El Camino Real | Suite 180 | Mountain View, CA 94040 | United States of America | ☎ +1 (650) 943-2484 |
✉ info@fortanix.com | 🌐 www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

This document describes the various key operations supported by **Fortanix Data Security Manager** (DSM). These include Encrypt, Decrypt, WrapKey, UnwrapKey, DeriveKey, MacGenerate, MacVerify, Export, AppManageable, Sign, Verify, AgreeKey, and Export key operations.

2.0 DEFINITIONS

- **Fortanix Data Security Manager** -

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

- **Accounts** -

A Fortanix DSM account is the top-level container for security objects managed by the Fortanix DSM. An account is generally associated with an organization, rather than an individual. Security objects, groups, and applications belong to exactly one account. Different accounts are fully isolated from each other. *See support for more information.*

- **Users** -

Users are associated with an email address. A user can be a member of one or more accounts. Depending on permissions, users can:

- Perform management operations like adding or modifying users or groups
- Create security objects
- Change properties of security objects
- Review logs of Fortanix DSM activity

⚠ **Users cannot perform cryptographic operations. Only applications can perform cryptographic operations.**

- **Groups** -

A group is a collection of security objects created by and accessible by users and applications which belong to the group. The user who creates a group automatically gets assigned the role of the group administrator. You can add more users to the group in the role of administrators or auditors. You can also add applications to the group to enable the applications to create and use security objects in that group. *See support for more information.*

Access policies are set at the group level, so all security objects in a group share the same access policy. Any number of users and/or applications can be assigned to a group. *Some examples of usage of groups are given in the Authorization section*.

Quorum policies can also be set at the group level. A Quorum policy mandates that all security-sensitive operations in that group would require a quorum approval. Such operations include using a key for cryptographic operations or deleting or updating a group. *See Quorum Policy for more information.*

- **Applications** -

An application can use Fortanix DSM to generate, store, and use security objects, such as cryptographic keys, certificates, or an arbitrary secret. It can also be used to perform cryptographic operations, invoke plugins, and so on. Applications can authenticate to Fortanix DSM using an API key (a secret token), a TLS client certificate, and so on. An application can interact with Fortanix DSM using the REST APIs or using the PKCS#11, JCE, or CNG providers. *See support for more information.*

- **Fortanix Data Security Manager Security Objects** –

A security object is any datum stored in Fortanix DSM (for example, a key, a certificate, a password, or other security objects). Each security object is assigned to exactly one group. Users and applications assigned to the group have permission to see the security object and to perform operations on it. *See support for more information.*

3.0 KEY OPERATIONS

Key operations are cryptographic and management operations that can be performed on a security object.

Generally, key operations are defined at the time of creation of a security object. *For more information on key creation, refer to Creating-a-Security-Object*.

By default, all key operations except for 'Export' that are implemented for that type of key will be enabled. These may be overridden by requesting specific operations in the key creation request. Note that the key operations restricted for a security object on creation cannot be reenabled after creation. If none of the operations are selected all key operations will be disabled.

NOTE: Certain operations may be disabled due to cryptographic policy. *For more information on cryptographic policy, refer to User's Guide: Cryptographic Policy*.

3.1 KEY OPERATIONS DEFINITIONS

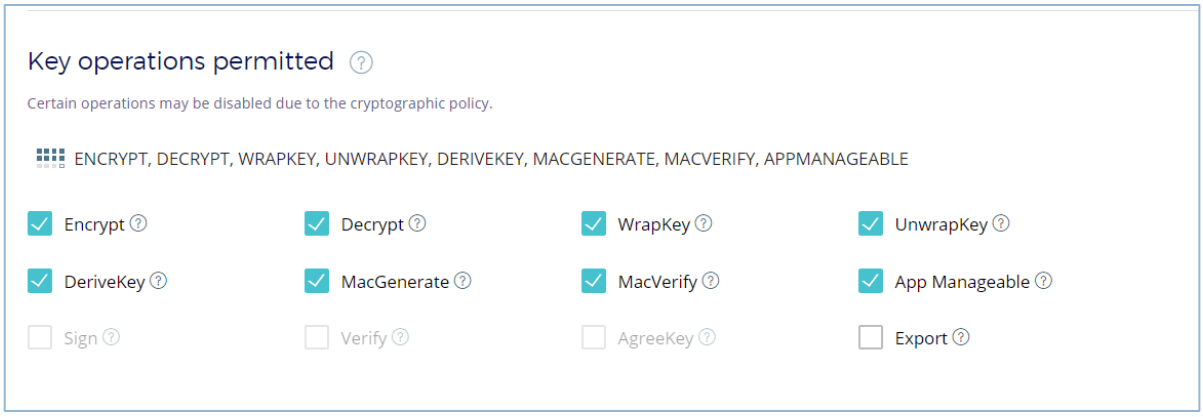

FIGURE 1: KEY OPERATIONS

- **Encrypt** – This operation allows the key to be used for encryption. Encryption involves the process of converting data in plain text format to an encoded format called ciphertext using a key generated by an algorithm. Both asymmetric and symmetric keys can be used to perform the 'Encrypt' operation.

- **Decrypt** - This operation allows the key to be used for decryption. Decryption involves the process of converting ciphertext into plain text using a key. Both asymmetric and symmetric keys can be used to perform the 'Decrypt' operation.

  NOTE: Security objects of type Opaque, EC, or HMAC may not be used for encryption or decryption.

- **WrapKey-** This operation allows a key to be wrapped (encrypted) by another key for export from Fortanix DSM, so they can be later imported into Fortanix DSM or another key management system. The key being wrapped must have the 'Export' operation enabled and the wrapping key must have the 'WrapKey' operation enabled.
  The following wrapping operations are supported:
  - Symmetric keys, HMAC keys, opaque objects, and secret objects may be wrapped with symmetric or asymmetric keys.
  - Asymmetric keys may be wrapped with symmetric keys. Wrapping an asymmetric key with an asymmetric key is not supported.

  For more information on the 'WrapKey' operation, refer to Wrapping a key.

- **UnwrapKey**- This operation allows the key to be used to unwrap (decrypt) a wrapped key. This allows securely importing security objects into Fortanix DSM, that were previously wrapped by Fortanix DSM, or another key management system. A new security object will be created in Fortanix DSM with the unwrapped data. The key used for unwrapping must have the 'UnwrapKey' operation enabled.
- **DeriveKey**- This operation allows the key to be used to derive another key. Fortanix DSM can generate new keys by deriving them from existing keys and some additional data. Currently, the only supported mechanism for deriving keys is by encrypting some data with a key. *For more information, refer to Deriving Security Object*.
- **MacGenerate and MacVerify** - These operations allow the key to be used to compute and verify Message Authentication Code (MAC) on a message using symmetric keys. The symmetric key must have the 'MacGenerate' operation enabled to generate a MAC and the 'MacVerify' operation enabled to verify a MAC. In addition, the key must be enabled.

- **AppManageable**- This operation enables applications (App) to perform management operations like `delete`, `destroy`, `rotate`, `activate`, `restore`, `revoke`, `revert`, `update`, `remove_private` (removes the private half of an asymmetric key), and so on, on the security object. A user with access or an admin app can still perform these operations. This option is only relevant for cryptographic applications. *For more information, refer to Security Controls for Applications*.
- **Sign**– This operation enables the key to be used for generating a digital signature. The signing key must be an asymmetric key such as RSA, DSA, or elliptical key, with the private part present. Symmetric keys may not be used to sign data. They can be used only with the 'MacGenerate' and 'MacVerify' operations.
- **Verify**- This operation enables the key to be used for verifying a signature. The verifying key must be an asymmetric key such as RSA, DSA, or elliptical curve key, with the 'Verify' operation enabled. Symmetric keys may not be used to verify data. They can be used only with the 'MacGenerate' and 'MacVerify' operations.
- **AgreeKey-** This operation enables the key to be used for key agreement. The cryptographic key agreement operation is between a public and private key.
  Both keys must have been generated from the same parameters (such as, the same elliptic curve) and must have enabled the 'AgreeKey' operation.
- **Export-** This operation enables the value of the key to be retrieved with an authenticated request. By default, the 'Export' 'operation is disabled for all key types. The operation should not be enabled unless required. It is more secure to keep the key's value inside Fortanix DSM only.
- **Highvolume-** This operation is enabled only when the audit logs for the key is disabled. It is used only for scenarios where a key is used for cryptographic operations with very high usage. *For more information on disabling audit logs*, *refer to User's Guide: Logging*.

  NOTE: Audit logs related to only cryptographic operations are disabled. Logs related to key management operations such as updating, rotating, activating/deactivating on the security object are still enabled.

4.0 DOCUMENT INFORMATION

4.1 DOCUMENT LOCATION

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

https://fortanix.zendesk.com/knowledge/articles/5335281255188/en-us?brand_id=360001216831

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