STORMSHIELD

STORMSHIELD KEY MANAGEMENT AS A SERVICE

RELEASE NOTES

Version 4.6.0

Document last updated: April 02, 2026

Reference: sds-en-sds-kmaas-release_notes-v4.6

Table of contents

Version number

The business name of the Stormshield KMaaS 4.6.0 corresponds to version number 4.6.0.309.

Stormshield KMaaS 4.6.0 new features and enhancements

Support for Google features

Google data loss prevention (DLP)

The KACLS module now supports the *systemwrap* API to enable the "Apply Client-side Encryption" action in the Google Drive DLP feature.

Find out more

Microsoft Double Key Encryption

The Stormshield KMaaS now supports the Microsoft Double Key Encryption feature (DKE) securing the Microsoft Office environment.

You can write ABAC rules with a remote Policy Decision Point on the DKE module in order to manage access to encrypted data more finely.

Find out more

Stormshield KMaaS database

A PostgreSQL database is now available to the Stormshield KMaaS for KEK storage. The KEKs are wrapped with an MKEK before they are inserted in the database.

KEKs are loaded on demand rather than at Stormshield KMaaS startup to optimize performance.

mTLS authentication to the database is supported.

Find out more

Administration module

A new Administration module (Admin) is available to perform operations on KEKs for different Stormshield KMaaS modules, and to configure authentication and policy enforcement for the modules. The database mode is required to use the Admin module. The following operations are available through administration APIs:

- Creating symmetric and asymmetric KEKs,
- Retrieving non-sensitive information about the KEKs stored in the database,
- Revoking KEKs. A revoked key cannot be reactivated.

You can write ABAC rules with a local or remote Policy Decision Point on the Admin module in order to manage access to encrypted data more finely.

Find out more

Installation

The docker artifact is now compatible with NodeJS version 24 for enhanced security.

The Software Bill of Materials is now delivered as an artifact in the *cycloneDX* format.

Find out more

Key Access Management

The Key Access Management module can now use symmetric KEKs imported from a KMS using the KMIP protocol.
The */rewrap* route is not available in KMS mode.

Customized access rules (OPA)

The *kacls_owner_domain* parameter in authorization tokens can now be used when writing OPA rules if it is provided by Google.

Stormshield KMaaS 4.6.0 fixes

PKI module

The version of the certificates generated by the PKI module is now correct. It is now x509 v3 instead of x509 v1.

The PKI module now supports the *keyIdentifier* field of the *AuthorityKeyIdentifier* extension in the CA certificate.

The PKI module now correctly checks the values associated to the *SubjectAlternativeName* field of a certificate. They must be either DNS names or IP addresses.

Key Access Management and Crypto API

The *verify* log related to policy verification is no longer issued if this verification is disabled.

In the Key Access Management and Crypto API modules, if the *encrypted_data* field of the */decrypt* route is empty, the correct log is now issued.

OPA rules

The *containerType* OPA input for the *wrapprivatekey* route has been replaced by *contentType*. Make sure to modify your OPA rules accordingly if they include the *containerType* input.

Known issues

The up-to-date list of the known issues related to this version of the Stormshield KMaaS is available on the Stormshield Knowledge Base. To connect to the Knowledge base, use the same identifiers as for MyStormshield.

Previous versions of Stormshield KMaaS

In this section, you will find the new features from previous versions of Stormshield Key Management as a service.

4.5	Features		Bug fixes
4.4	Features		Bug fixes
4.3.2		Resolved vulnerabilities	
4.3.1			Bug fixes
4.3	Features	Resolved vulnerabilities	Bug fixes
4.2.4			Bug fixes
4.2.3			Bug fixes
4.2.2			Bug fixes
4.2.1	Features		Bug fixes
4.2	Features		
4.1.1	Features		
4.1	Features		Bug fixes
4.0	Features		
3.0	Features		

Stormshield KMaaS 4.5.0 new features and enhancements

Support for Google features

Send Gmail encrypted emails to anyone

KACLS now supports the Send to Anyone Gmail feature. It allows users to send end-to-end encrypted emails to anyone, even if the recipient uses a different email provider, without having to deploy a complex PKI.

For more information, refer to the Google documentation.

Full support for Google Meet hardware

It is now possible to join an encrypted Google Meet conference from a room with Meet hardware.

Key Access Management

The new Key Access Management feature is dedicated to the Stormshield SDK. It enables:

- Symmetric encryption and decryption,
- Asymmetric rewrap to allow Stormshield SDK to retrieve or re-encrypt keys needed to decrypt protected data.

Find out more

Customized access rules (OPA)

Attribute Based Access Control (ABAC)

You can now write OPA rules using Attribute Based Access Control (ABAC) for Crypto API and Key Access Management. This allows for a better implementation of Data Centric Security and Zero Trust concepts.

Find out more

Centralized authorization server

You can enhance security by centralizing authorization through an OPA server for KACLS and Crypto API. You can still use the local *policy.wasm* and *policy.data.json* files if you do not have an OPA server.

Find out more

OPA enforcement

You can now configure OPA enforcement for each tenant and feature:

- For the KACLS, the configuration files are *policy.wasm* and *policy.data.json,*
- For Crypto API, the configuration files are *policy-crypto-api.wasm* and *policy-crypto-api.data.json*.

- For the Key Access Management, the configuration files are *policy-kas.wasm* and *policy-kas.data.json*.

If a feature is enabled, you must set its *policy_enforcement* parameter to specify whether the OPA rules must be used or not.

Find out more

KACLS

In the *config.json* file, you can now specify the KMS domain for Thales Ciphertrust API REST use. The domain is common to all tenants, and contains KEKs and Gmail private keys.

Find out more

Crypto API

API key authentication

Crypto API now supports API key authentication.

Find out more

KEK for data encryption

When encrypting data with Crypto API, you can now specify the key encryption key (KEK) to be used to encrypt the data encryption key (DEK).

Public API

The following fields have been renamed for more consistency:

- The "encryptedData" response field for the *crypto_api/encrypt* route has been renamed "encrypted_data",
- The "encryptedData" input parameter for the *crypto_api/decrypt* route has been renamed "encrypted_data".

Find out more

PKI

The new PKI feature allows issuing certificates for mTLS authentication from a Certificate Signing Request (CSR).

Find out more

Logs

Log format

In the *config.json* file, you can now specify the format of the logs to be generated, in order to prepare for migration to the new log format.

Find out more

Stormshield KMaaS 4.5.0 fixes

The KMS model must now be set to *ciphertrust* in the *config.json file*. You must change this value accordingly in your configuration if using Thales Ciphertrust KMS.

The *vendor_id* log field of the *status* route now displays "Stormshield" instead of the product name.

Error handling when verifying the configured proxy URL has been improved.

The management of the configured proxy URL validation has been improved.

The *operations_supported* log field of the *status* route now returns the *certs* route.

The decryption of an empty string via Crypto API no longer raises an error.

Stormshield KMaaS 4.4.0 new features and enhancements

For information about the Google services supported by the Stormshield KMaaS (client-side encryption), refer to the section *Which services CSE supports* of Google documentation About client-side encryption.

Environment

Deployment via a Docker image

In addition to the traditional RPM-based installation it is now possible to install using a Docker image.

New requirements for installation in RPM mode

The Stormshield KMaaS now requires RedHat Enterprise 8.10 or 9 to be installed.

Gmail message encryption

The Stormshield KMaaS now supports the *SHA512withRSA* algorithm for key encryption for Gmail.

Support for Google features

Google Drive and external users

The Stormshield KMaaS is now compatible with the Google Guest access feature. This enables users outside your company to access your encrypted content on Google Drive. To do this, you must configure a dedicated identity provider for Google Drive Guest users and add them to the list of authorized providers in the *config.json* file, section **tenants > user_authentication > idps**.

For more information, refer to the Google documentation.

Mass import of files to Google Drive

The Stormshield KMaaS now supports the mass importing of sensitive data into Google Drive. Data imported from third-party storage are encrypted by the Stormshield KMaaS in Google Drive. See an example on Github googleworkspace.

This Beta feature is currently under development at Google.

For more information, refer to the Google documentation and contact Google Support.

SDS CryptoAPI

The new SDS CryptoAPI feature provides two API routes, *crypto/encrypt* and *crypto/decrypt*, which enable data to be encrypted and decrypted, completely independently of Google.

You can write OPA rules for the CryptoAPI in dedicated files.

SDS CryptoAPI is currently in its alpha version. Stormshield does not guarantee that it will be possible to decrypt data encrypted with this version with a later version of the feature.

Support for Google Meet hardware

The new delegation feature enables a user to delegate their authentication to join an encrypted Google Meet conference from a room with Meet hardware. This feature is in *alpha* version.

Logs

Business operations logs (kind:domain)

- Generation of authentication tokens for delegation (*cse* category - *delegate* action)
- Key management as a service *(kmaas* category)
- Queries concerning KEK keys (kek *category*)
- Validation of authorization tokens (*authorization* category)
- Validation of authentication tokens (*authentication* category)

Logs of operations related to the environment (kind:system)

- Web server related operations(*server* category)
- Key Management System operations *(kms* category)

Stormshield KMaaS 4.4.0 fixes

The Stormshield KMaaS now displays an error at startup if the private key format entered in the *migration* section of the configuration file is not in base 64 format. This check prevents migration operations from failing afterwards.

The reception log for an HTTP request is now displayed, even if the body format of the request is incorrect. This correction only concerns the log in the new V2 format.

The Stormshield KMaaS now displays an error at startup when the *authorization* section of the configuration file is empty.

The following deprecated cryptographic suites are no longer supported to connect to the KMS via KMIP.

- TLS_RSA_WITH_AES_256_CBC_SHA256(0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA(0x0035)
- TLS_RSA_WITH_AES_256_GCM_SHA384(0x009d)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(0xc02c)
- TLS_RSA_WITH_AES_128_CBC_SHA256(0x003c)

Resolved vulnerability in Stormshield KMaaS 4.3.2

A medium severity vulnerability was fixed.

Details on this vulnerability can be found on our website:

- https://advisories.stormshield.eu/2024-033/

Stormshield KMaaS 4.3.1 fix

An issue when validating authentication on privileged routes caused the Stormshield KMaaS to stop unexpectedly if a KACLS was configured as a backup KACLS. This issue has been fixed.

Stormshield KMaaS 4.3 new features and enhancements

For information about the Google services supported by the Stormshield KMaaS (client-side encryption), refer to the section *Which services CSE supports* of Google documentation About client-side encryption.

New version numbering

Version numbers for the Stormshield KMaaS Saas and On Premises have been harmonized. They now use the following numbering pattern:

<major>.<minor>.<corrective>.<build>

The table below indicates the version number which corresponds to a business name:

Version name	Version number
4.3	4.3.0.158
4.3 beta 1	4.3.0.145

Environment

New installation requirements

Stormshield KMaaS now requires NodeJS 20, OpenSSL 3.0 and RedHat Enterprise 8.8 or 9 to benefit from the latest security updates.

Start-up time of the Stormshield KMaaS

The start-up time of the Stormshield KMaaS has been optimized.

TLS algorithms

The number of TLS algorithms used by default have been restricted to improve the security of incoming and outgoing communications.

Connections to the Key management System (KMS)

Connections to the KMS are no longer closed after each operation, but now remain open. When a connection problem occurs, the Stormshield KMaaS tries to reconnect, and logs are issued to inform the administrator.

Support for Google features

Support for Gmail on mobile

With the Stormshield KMaaS, users can now encrypt their emails in Gmail on iOS and Android mobile devices.

Edit encrypted Excel files with Google Sheets

Users can now view and edit encrypted Excel files directly with Google Sheets.

For more information, refer to the Google documentation.

Encrypted import of Excel files into Google Sheets

Users can now import and encrypt Microsoft Excel files into Google Sheets.

For more information, refer to the Google documentation.

Manage comments and action items on Google Docs

The Stormshield KMaaS is now compatible with comment and action item management on Google Docs.

For more information, refer to the Google documentation.

Co-host management in Google Meet

The Stormshield KMaaS is now compatible with the Google Meet co-host feature.

For more information, refer to the Google documentation.

External Google Meet invitations

The Stormshield KMaaS now supports Google's Beta feature for inviting external participants to Google Meet conferences. To do this, you must configure two dedicated identity providers and add them to the list of authorized providers in the *config.json* file, section **tenants > user_authentication > idps**.

This Beta feature is currently under development at Google. Contact Google Support for more information on implementation and limitations.

Encryption and signature keys

It is now possible to use different keys to decrypt and sign Gmail messages.

Gmail messages signing

PKCS1.5 signing using the KMIP protocol is now supported when the Stormshield KMaaS is configured to store the keys in the KMS to secure Gmail.

Administration route authentication

Authentication of privileged administration routes and authentication of the route used to initialize Google users for Gmail message encryption are now different to enhance security.

Algorithms for checking JWT tokens

It is now possible to configure the list of algorithms used to check the validity of authorization and authentication tokens (JWT).

Bulk file import

The Stormshield KMaaS now supports bulk import of encrypted files into Google Drive using a compatible third-party software. A new API route, `/privilegedwrap`, has been added for this purpose. It can only be used with administration rights.

For more information, refer to the Google documentation.

Resolved vulnerability in Stormshield KMaaS 4.3

Two medium severity vulnerabilities were fixed.

Details on these vulnerabilities can be found on our website:

- https://advisories.stormshield.eu/2024-009/
- https://advisories.stormshield.eu/2024-010/
- https://advisories.stormshield.eu/2024-012/
- https://advisories.stormshield.eu/2024-013/

Stormshield KMaaS 4.3 fixes

The type returned in the logs related to the identity provider configuration retrieval is now correct.

---

431 errors are now handled correctly when the requests received have too long headers.

Error messages issued when a proxy is unreachable have been improved.

The reading of environment variables when starting the Stormshield KMaaS has been optimized.

The management and display of network errors in logs have been improved.

A log is now issued for each outgoing connection made by the Stormshield KMaaS.

Stormshield KMaaS 4.2.4 fix

An issue when validating authentication on privileged routes caused the Stormshield KMaaS to stop unexpectedly if a KACLS was configured as a backup KACLS. This issue has been fixed.

Stormshield KMaaS 4.2.3 fix

An issue occurring when calculating the *key_hash* resource during migration between a third-party external key service (KACLS) and the Stormshield KMaaS has been fixed.

Stormshield KMaaS 4.2.2 fix

Some issues relating to the migration system between a third-party external key service (KACLS) and the Stormshield KMaaS have been fixed.

Stormshield KMaaS 4.2.1 new features and enhancements

For information about the Google services supported by the Stormshield KMaaS (client-side encryption), refer to the section *Which services CSE supports* of Google documentation **About client-side encryption**.

Support for Google Meet on mobile devices

With the Stormshield KMaaS, users can now encrypt confidential video conferences and calls in Google Meet. In addition to the Google Workspace Web Client, this feature is now available on iOS and Android mobile devices.

Stormshield KMaaS 4.2.1 fixes

When performing a migration between two KACLSs or using a backup KACLS, a migration token is generated by the Stormshield KMaaS. It was generated with the wrong time unit for the iat (issued at) and exp (expiration date) fields, which could make it impossible to migrate.

The Stormshield KMaaS no longer stops unexpectedly if a request parameter has the wrong type when calling the REST API. This error could have been exploited to execute a Denial of Service (DDOS) attack.

Stormshield KMaaS 4.2 new features and enhancements

For information about the Google services supported by the Stormshield KMaaS (client-side encryption), refer to the section *Which services CSE supports* of Google documentation About client-side encryption.

Google Meet in-meeting chat

The content of Google Meet chat messages can now be secured with the Stormshield KMaaS.

Periodic refresh of KEKs

If you are using a Key Management System (KMS), you can now set the refresh frequency for KEKs.

One-off refresh of KEKs

KEK retrieval has been optimized. A one-off KEK refresh is now performed if the KEK ID cannot be found in the host local cache. This may occur if you have several instances of the Stormshield KMaaS.

Thales Ciphertrust Manager Key management system

It is now possible to use the private keys for Gmail S/MIME in the Thales Ciphertrust Manager via REST API. The list of algorithms supported in this mode is limited. For more information, refer to the *Administration guide* of the Stormshield KMaaS.

Customized access rules (OPA)

Custom claims provided by the identity provider can now be used to create OPA rules.

HTTP proxy

You can now exclude certain endpoints from the HTTP proxy.

Stormshield KMaaS 4.1.1 new features and enhancements

For information about the Google services supported by the Stormshield KMaaS (client-side encryption), refer to the section *Which services CSE supports* of Google documentation About client-side encryption.

Compatibility with RedHat 9.0.

Support for chat messages in Google Meet
The content of Google Meet chat messages can now be secured with the Stormshield KMaaS.

Stormshield KMaaS 4.1 new features and enhancements

For information about the Google services supported by the Stormshield KMaaS (client-side encryption), refer to the section *Supported services and data types* of Google documentation About client-side encryption.

Support for Google Drive

With the Stormshield KMaaS, users can now encrypt confidential files in Google Drive and read them. This feature is available on Windows and macOS workstations, and on mobile iOS and Android devices.

Support for Gmail

Gmail messages and attachments can now be secured with the Stormshield KMaaS.

Support for Google Calendar

Google Calendar data can now be secured with the Stormshield KMaaS.

Support of customized access rules

The Stormshield KMaaS now supports the Open Policy Agent (OPA) technology, allowing administrators to create their own customized access rules to the Stormshield KMaaS.

Migration of the KACLS

The Stormshield KMaaS is compatible with Google's new specifications regarding the migration of an encryption service (KACLS) to another, allowing in particular a massive migration in a single operation.

Identity provider

The local *config.json* configuration file now makes it possible to add several clientIDs for the user connection. Google applications configured locally will therefore be supported.

It is now possible to use OpenID JWKS (JSON Webkey Set) configurations to configure user identity providers.

Remote configuration file

Access to the remote configuration file *.well-known/cse-configuration* can now be disabled so that the local file can be used to validate user authentication.

Mass extraction and decryption of encrypted data

To ensure that data can be reversed, you can now extract all encrypted data and decrypt all of it in a single action using the Google tool (currently in beta version) and the Stormshield KMaaS. Stormshield must first provide you with a specific configuration. Please note that in the Beta version of the Google tool, only Gmail and Drive files can be used after decryption. Files from other Google Workspace applications are decrypted but not usable.

Compliance with RFC 7519

The Stormshield KMaaS is now compliant with RFC 7519 and supports multiple values for the "aud" field of the authentication token.

HTTP proxy

If there is an HTTP proxy in your network environment, it can now be used to manage the external requests of the Stormshield KMaaS.

Cache

The Stormshield KMaaS now includes a cache for external requests (e.g., openid connect, jwks), which optimizes response time.

Logs

Some logs are now issued for the */health* API route.

Stormshield KMaaS 4.1 fixes

The Stormshield KMaaS now lists the right options for the */status* API route.

The Stormshield KMaaS now checks the UUID-V4 format for the *tenant_id* provided by the Key management system (KMS).

Requests no longer fail if the value of the *kacls_url* parameter in the *config.json* file ends with the / character. Both URL formats - with or without / - are supported.

The configuration file cleanup and validation processes have been improved. These operations are no longer simultaneous, but executed consecutively.

Access privileges to configuration files have been restricted. The Stormshield KMaaS now requires configuration files to hold read and write access privileges for the current user and read-only privileges for the current group. Otherwise a warning will be raised.

Stormshield KMaaS 4.0 new features and enhancements

Support for Google Meet

Google Meet data can now be secured with the Stormshield KMaaS.

Using two KACLS

The Stormshield KMaaS is compatible with the new Google feature that allows two KACLS to coexist for the purpose of migrating from one service provider to another. For example, new files can be encrypted with the Stormshield KMaaS, while older files protected by another KACLS provider can be decrypted.

Operating system

The Stormshield KMaaS can now be installed on a server hardened with Security-Enhanced Linux (SElinux).

The Stormshield KMaaS is now compatible with RedHat Enterprise Linux 8.6 and only this version.

User authentication

User authentication can now be strengthened on privileged API routes by using a configured IdP.

Key management system (KMS)

In KMS mode, KEKs are no longer stored in the configuration file but in the KMS from now on.

KEKs are now automatically and transparently refreshed in KMS mode.

Stormshield KMaaS 3.0 new features and enhancements

Collaboration with external users

The users are now able to securely share Google Drive files (Docs, Sheets and Slides) with other users who work in different companies equipped with Google Client-Side Encryption.

There are two ways to configure this feature:

- Through the local configuration file, *config.json*, by specifying several identity providers in the *local_cse_configurations* section,
- Through a remote configuration file, */.well-known/cse-configuration*, located at the root of your domain.

Key management system (KMS)

It is now possible to add a key management system (KMS) to your Stormshield KMaaS infrastructure to secure key storage. In such a configuration, the key encryption keys (KEKs) are protected with a master key managed by the KMS. The KEKs in the keks.json file are thus encrypted.

New NodeJS 16 requirement

Stormshield KMaaS now requires NodeJS 16 to benefit from the latest security updates. It is available with RedHat Enterprise 8.

Summary of features in Stormshield KMaaS 1.2.1

With Stormshield KMaaS, you can guarantee the absolute confidentiality of your corporate data and benefit from Google Workspace collaboration tools at the same time, while complying with the regulatory restrictions of your sector.

Users can therefore protect their data before sending it to Google Workspace applications. Uncrypted data and encryption keys are never sent to Google.

The following are the features in Stormshield KMaaS 1.2.1:

Protection of files before sharing them	Users protect their files on their workstations via their browsers.
Sharing of files in shared spaces	Users share their protected files on Google Workspace.
Management of privileges on files	The operations that each user can perform depend on the privileges that the Google Workspace administrator has granted in the configuration. For example, the privilege of sharing files with external users who belong to specific domains.
Verification of authorized persons	During each operation in which a file is protected or modified, the solution will ensure that persons allowed to look up the file are trustworthy.

Contact

To contact our Stormshield Technical Assistance Center (TAC):

- https://mystormshield.eu/
  All requests to technical support must be submitted through the incident manager in the private-access area https://mystormshield.eu, under Technical support > Manage cases.
- +33 (0) 9 69 329 129
  In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on https://mystormshield.eu.

STORMSHIELD