GUIDE

STORMSHIELD ENCRYPTION PLATFORM

DKE SAAS DEPLOYMENT GUIDE

Document last updated: June 27, 2026

Reference: sds-en-kmaas-dke_saas_deployment_guide

Table of contents

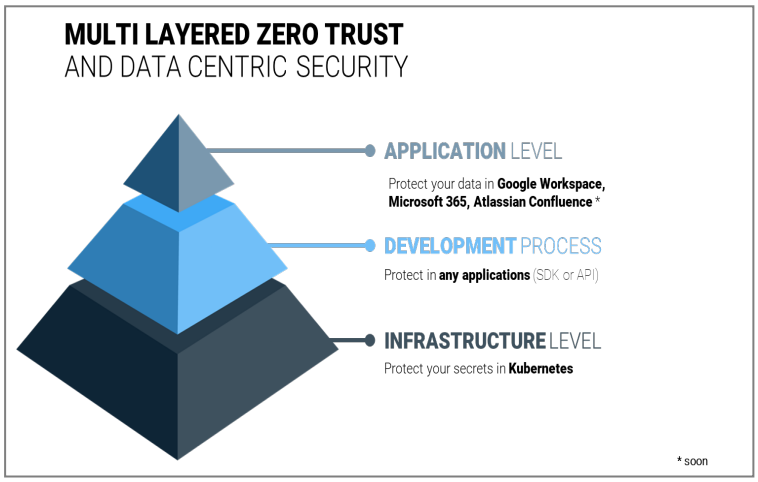
In the documentation, Stormshield Key Management as a service is referred to in its short form: Stormshield KMaaS.

This document is not exhaustive and minor changes may have been included in this version.

1. Getting started

The Stormshield Encryption Platform (SEP) solution helps implementing Data Centric Security and Zero Trust (ZT) in your environment at multiple levels:

- Application level: Integrate Zero Trust directly into your existing applications, or those currently under development (e.g., Google Workspace, Microsoft Office 365, healthcare applications, IoT, business),
- Development process: Secure your data and access to your data during your development processes. For instance by securing private HTTPS keys or API tokens for CI/CD, GitOps, etc.,
- Infrastructure level: Protect your secrets at the lowest level in your deployments, especially by securing Kubernetes.



Stormshield KMaaS is the backend component of this ecosystem and acts as a Policy Decision Point as defined in the Zero Trust architecture, securing and authorizing access to confidential data.

It includes the Double Key Encryption (DKE) module, which is dedicated to securing Microsoft Office files and emails in a Windows environment.

The DKE module allows you to configure your backend server to protect your data in a Microsoft environment. For more information, see the Microsoft documentation.

This module exposes:

- A public key retrieval endpoint used by Microsoft to get the keys used during local encryption of Data Encryption Keys (DEKs),
- A decryption endpoint used by Microsoft to request decryption of the previously encrypted DEKs.

All cryptographic material remains under the exclusive control of the Stormshield KMaaS.

NOTE
The use of the solution in any way other than as described in the documentation is not managed. Alternatively, get in touch with Stormshield Support for clarification.

This guide describes how to deploy the Stormshield KMaaS for DKE as an SaaS solution. To implement the solution on site, contact your Stormshield commercial referent at sales@stormshield.eu.

2. Understanding the requirements

To use the Stormshield KMaaS for DKE, your environment must comply with the following prerequisites:

- Microsoft License: A Microsoft 365 E5 subscription is required. Office 365 E5 is not sufficient for DKE. For more information, refer to the Microsoft documentation System and licensing requirements for DKE.
- Access rights: To configure the Stormshield KMaaS for DKE, you must be a Global Administrator or Compliance Administrator in your Azure/Microsoft 365 tenant.

3. Accepting the Stormshield application

First, you must allow the Stormshield platform to interact with your Microsoft 365 environment for encryption management.

1. Retrieve your Azure Tenant ID:
   a. Sign in to the Microsoft Entra ID portal.
   b. In the Overview section, copy the value from the Tenant ID field.
2. Generate your consent URL to authorize the Stormshield application: replace <YOUR_TENANT_ID> with your tenant ID in the following URL: https://login.microsoftonline.com/<YOUR_TENANT_ID>/adminconsent?client_id=8ec355aa-e580-4aa2-9430-f33ac946f87c
3. In your browser, paste the consent URL and press Enter.
4. Sign in with a Global Administrator or Compliance Administrator account.
5. Accept the Permissions requested for the Stormshield KMaaS for Microsoft 365 application.
6. Send your Microsoft 365 Tenant ID to your Stormshield contact to set up your dedicated service.
   Stormshield will provide you with the DKE service URL (i.e., the endpoint for your secondary key).
7. Create your Microsoft labels as described in Creating a sensitivity label. You will need the DKE service URL provided by Stormshield.

4. Creating a sensitivity label

After accepting the Stormshield application and receiving the DKE service URL from Stormshield, you must create the label that your users will apply to their sensitive documents. The following procedure describes the minimum steps to allow you to encrypt Microsoft Office with Stormshield KMaaS for DKE.

1. Go to the Microsoft Purview Center and sign in with one of these accounts:
   - Global Administrator,
   - Compliance Data Administrator,
   - Compliance Administrator account,
   - Security Administrator.
2. Click on **Information Protection**.
3. Go to **Sensitivity Labels** > **Create** > **Label**, and complete the fields in the following sections:
   - **Label Details**: Give your label a name and description (e.g., “Secret - DKE Stormshield”).
   - **Scope**: Select **Files & other data assets** and **Emails**.
   - **Items**: Select **Control access**. From the **Items** > **Access control** section:
     - In the **Assign permissions to specific users or groups section**, click on **Assign permissions** and choose who will be allowed to use this label.
     - Select the **Use Double Key Encryption** option and paste the DKE service URL provided by Stormshield.
   - **Finish**: Review the summary and click on **Create Label** to complete the configuration.

For more information, refer to Microsoft documents:

- Label and protect files in File Explorer in Windows
- PurviewInformationProtection Module

5. Publishing the label policy

For the label to be displayed in Word, Excel, or Outlook, you must publish it via a policy.

1. In **Sensitivity Labels**, click on **Publish labels** or go to **Label Policies > Publish label**.
2. Click on **Security labels to publish** and complete the fields in the following sections:
   - **Labels to publish**: Select the DKE label you have just created.
   - **Users and groups**: Choose the users or groups who will be able to see this label. By default: *All users and groups*.
   - **Policy settings**: Configure your business rules.
   - **Name**: Enter a name (e.g., *Stormshield DKE Policy*).
   - **Finish**: Review the summary and click on **Submit**.

   A new label policy may take up to 24 hours to propagate on workstations.
3. After a few hours, open Word or Outlook. Your new DKE label should display in your applications, under the **Sensitivity** menu.

STORMSHIELD