securosys

Securosys 365 - Double Key Encryption

Quick Start Guide

Securosys SA, Förrlibuckstrasse 70
CH-8005 Zürich, Switzerland
Tel. +41 44 552 31 00 • www.securosys.com
info@securosys.com

Document Information and Revision Control

Version	Date	Author	Description, Changes
1	12.12.2022	PM	Initial document

File: Securosys365-DKE_QuickStartGuide_AzureMarketplace_UG-E01.docx

Table of Contents

1 Glossar

Term	Description
CloudsHSM	CloudsHSM is a hardware security module (HSM) cloud service. It allows users to generate encryption keys, use them and store them securely without having to worry about time-consuming things like evaluation, setup, maintenance, and updating their HSM
DKE	**D**ouble **K**ey **E**ncryption uses two keys in Microsoft 365 desktop applications to protect access to files stored in the cloud and on premise
DKE - Key	The key which is used to Double Key encrypt Microsoft 365 applications
DKE – Web Service	Service which uses a DKE-Key to encrypt and decrypt Office documents with a second key. Securosys manages the DKE – Web Services – called "Apps" - within the Securosys 365 DKE – Cockpit.
DKE - Vault	User space /partition on an HSM cluster in the CloudsHSM service. The secure place where DKE – Keys are stored
HSM	Hardware Security Module
Microsoft Information Protection	Microsoft Information Protection (MIP) is a framework to provide lifecycle protection and data loss prevention
MIP label	Implementations of MIP solutions use sensitivity labels to control dataflow
Securosys 365 DKE - Cockpit	Web application to manage DKE-Web Services and DKE-Keys

2 Introduction

2.1 What is Double Key Encryption for Microsoft 365 (DKE)

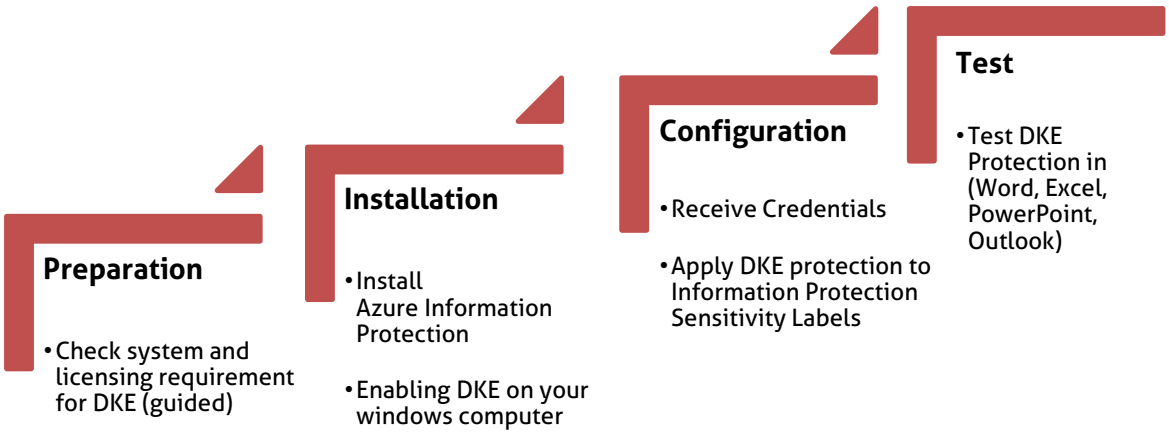
Microsoft 365 provides built-in data protection by encrypting customer data, both at rest and in transit. Customers can further protect their data based on content using *Microsoft Information Protection*'s classification and labeling capabilities. In addition, *Double Key Encryption* (DKE) enables them to protect their highly sensitive data while keeping full control of the encryption key. It uses two keys to protect the data—one key in customer's control, and a second key is stored securely in *Microsoft Azure*. Viewing and editing all Microsoft 365 Office documents (Word, Excel, PowerPoint, Outlook, PowerBI, ...) protected with DKE requires access to both keys. Since Microsoft can access only one of these keys, the customer's protected data remains inaccessible to Microsoft, ensuring that they have full control over their privacy and security.

2.2 What is Securosys 365 DKE

The service *Securosys 365 DKE* leverages Microsoft's Double Key Encryption offering: it securely stores the encryption key in a tamper-proof *Securosys CloudsHSM*. The CloudsHSM supports multiple tenants; As such, each customer will get their own isolated tenant space. It enables customers to deploy Double Key Encryption Services with **OneClick** according to security standards that follow international certification standards and are transposed by our security architects. If additional configurations required by customers he can do so, by requesting access to *Securosys 365 DKE Cockpit* cloud app to manage their keys (KMS), controlling the DKE web service(s) and *CloudsHSM* backed Vault configuration.

3 Installation (including one-month free trial)

3.1 Steps required to use DKE with Microsoft 365 Office Applications



3.2 Preparation

3.2.1 Check system and licensing requirements for DKE

- **Microsoft Office Apps for enterprise** version 2009 or later (Desktop versions of Word, Excel, PowerPoint and Outlook) on Windows.

  Double Key Encryption comes with Microsoft 365 E5. If you don't have a Microsoft 365 E5 license, you can sign up for a trial (one-month). For more information about how to setup your free-trial, see What Microsoft license do I need for DKE (double key encryption)

3.3 Installation

3.3.1 Install Azure Information Protection

- **Azure Information Protection**. DKE works with sensitivity labels and requires **Azure Information Protection Unified Labeling Client** versions 2.14.93.0 or later. Download and install the Unified Labeling client from the Microsoft download center.

  DKE sensitivity labels are made available to end users through the sensitivity button in the AIP Unified Labeling client in Office Desktop Apps. Install these prerequisites on each client computer where you want to protect and consume protected documents.

  Download and install the **AZInfoProtection_UL.exe**

After **restarting** all your Microsoft 365 applications, a new Section called '*Sensitivity*' shows up in the home view. (Most probably there is not entry like: Securosys365_HIGH....., that's okay you will configure your own labels later)

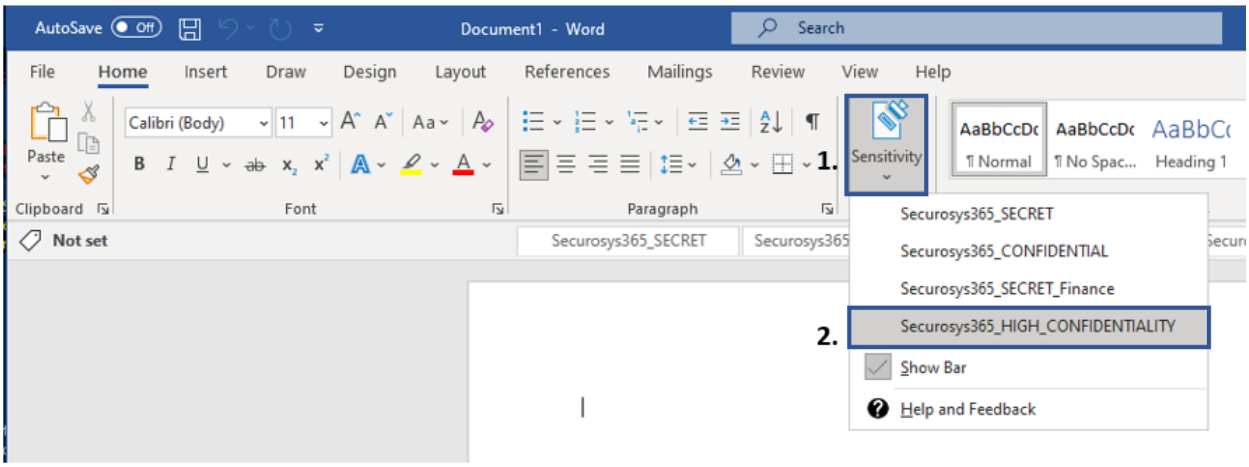


Figure 1: Check for Sensitivity AddOn

3.3.2 Enabling DKE on your windows computer

If you're an Office Insider, DKE is enabled for you. Otherwise, enable DKE for your client by adding the following registry keys. DKE must be enabled on all Client Computer (Windows computers) where DKE shall be consumed.

- Using Script (Download) https://support.securosys.com/external/knowledge-base/article/150

3.4 Configuration

3.4.1 Receive Credentials

After ordering, you will receive the credentials for logging in to the Securosys support portal, through which you will get your **DoubleKeyEncryption-URL** (*required for further proceeding*), Tenant name, Tenant Admin username, Tenant Admin password of the Securosys 365 DKE - Cockpit.

3.4.2 Create MIP label

The workflow presented below is an example of how to set up a Microsoft Information Protection label. The configurations listed here are only example configurations and must be set up on a company-specific basis.

IMPORTANT: You can skip this chapter if you are already familiar with creating MIP labels or your organization has created MIP policies and proceed with: Apply Double Key Encryption label

To create a new Information Protection label, you must have the correct permission (**Compliance Data Administrator**, **Compliance Administrator**, or **Security Administrator** role group) to access the Microsoft 365 Compliance Center https://compliance.microsoft.com/informationprotection?viewid=sensitivitylabels

Click on **Information Protection** (1) and then on **Create a label** (2).

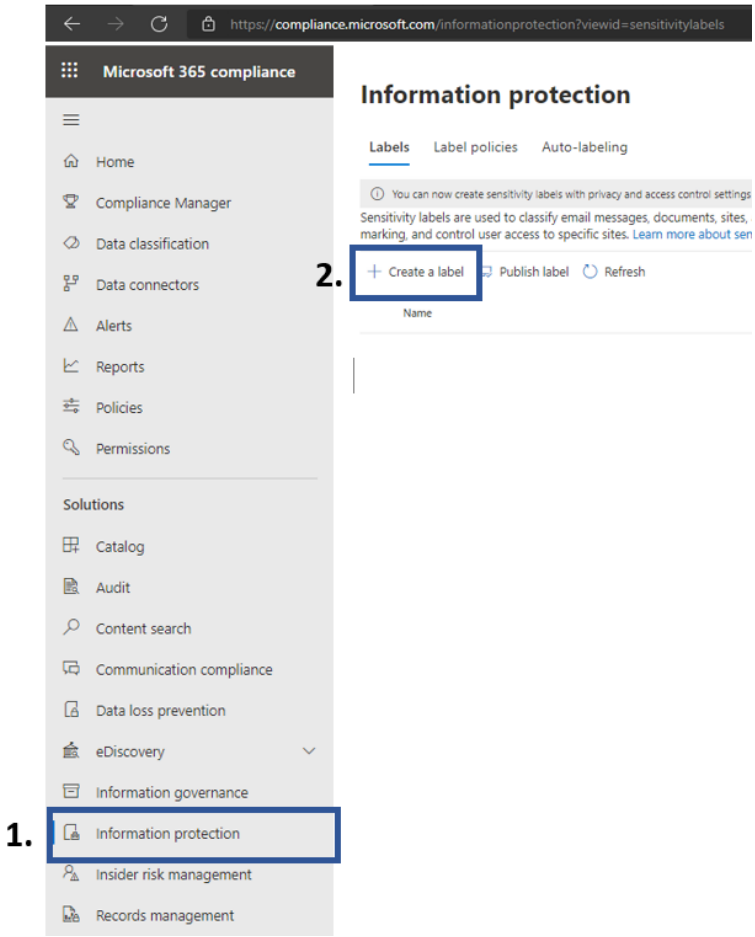


Figure 2: Create MIP label

In section *Name & description*, enter the following proposed values:

- (1) *OrganizationName*_DKE_SECRET
- (2) *OrganizationName*_DKE_SECRET
- (3) "A Label for high sensitivity data which uses double key encryption."
- (4) Press "Next".

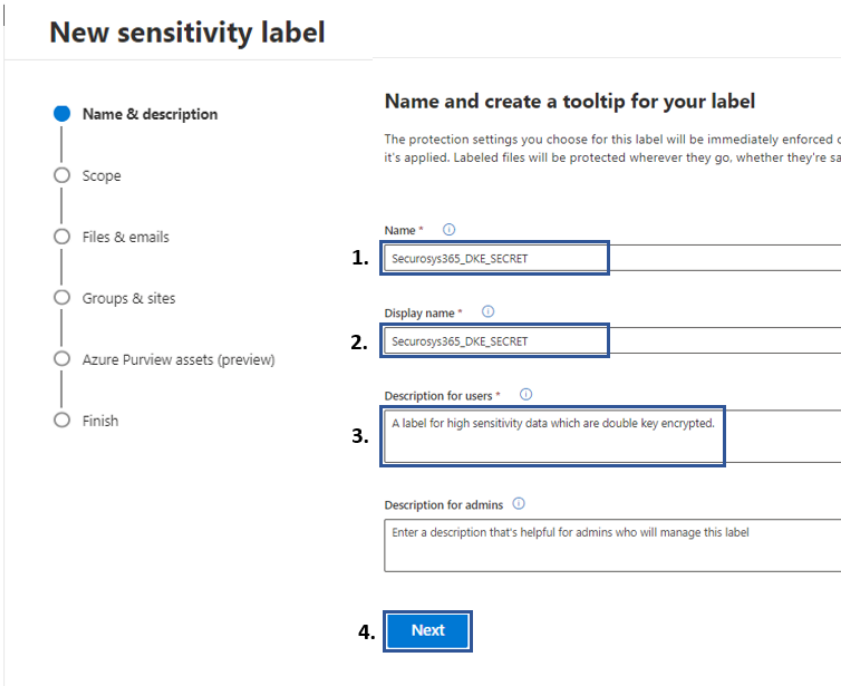


Figure 3: MIP Label configuration

In section *Scope*, select at least **Files & emails** then click the button "Next"

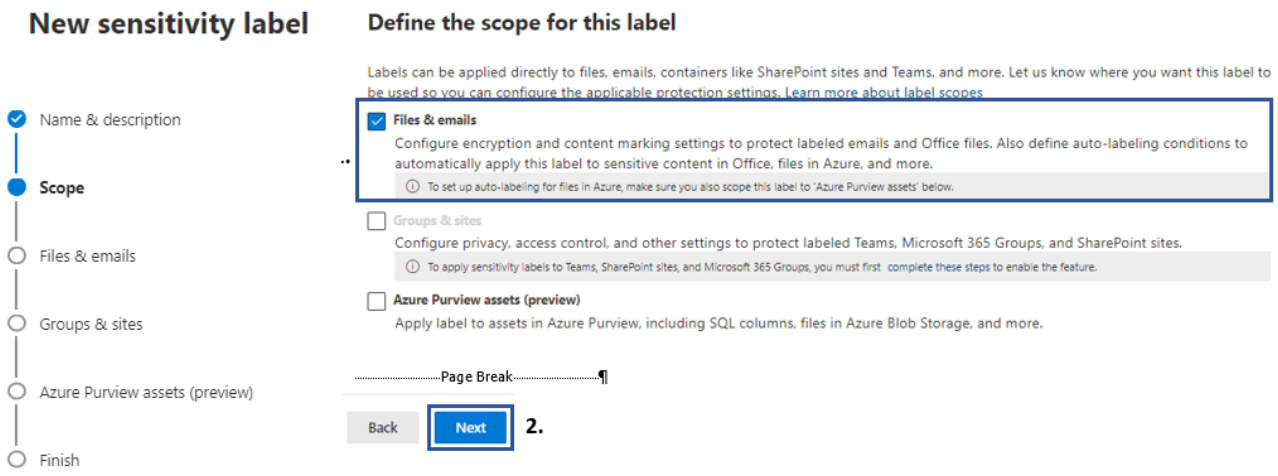


Figure 4: MIP Label (Scope)

In section *Files & emails*, select at least **Encrypt files and emails** then click the button "Next"

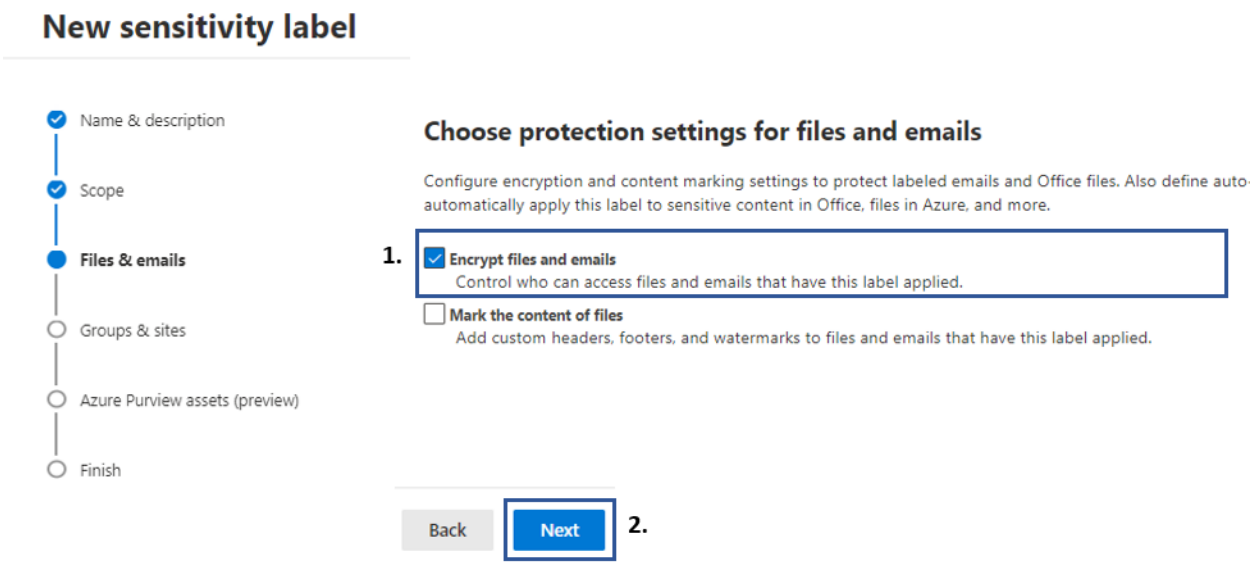


Figure 5: MIP Label (Encryption)

3.4.3 Apply Double Key Encryption label

In section *Encryption* of the label creation, use the following setting:

- (1) Select *Configure encryption settings*
- (2) Select *Assign permissions now*
- (3) configure your own needs
- (4) Select *Never*
- (5) Assign users inside your organization who are authorized to use the Double Key Encryption label
- (6) check *Double Key Encryption*
- 7) Enter the Double Key Encryption access URL that you obtained by Securosys Support

  Example DoubleKeyEncryption - URL: https://e556e4f2-6596-49c4-8b33-a09985805a69.securosys365.com/749cbb37-d559-4549-b89e-0ac30ddade2c

- Click the button "Next"

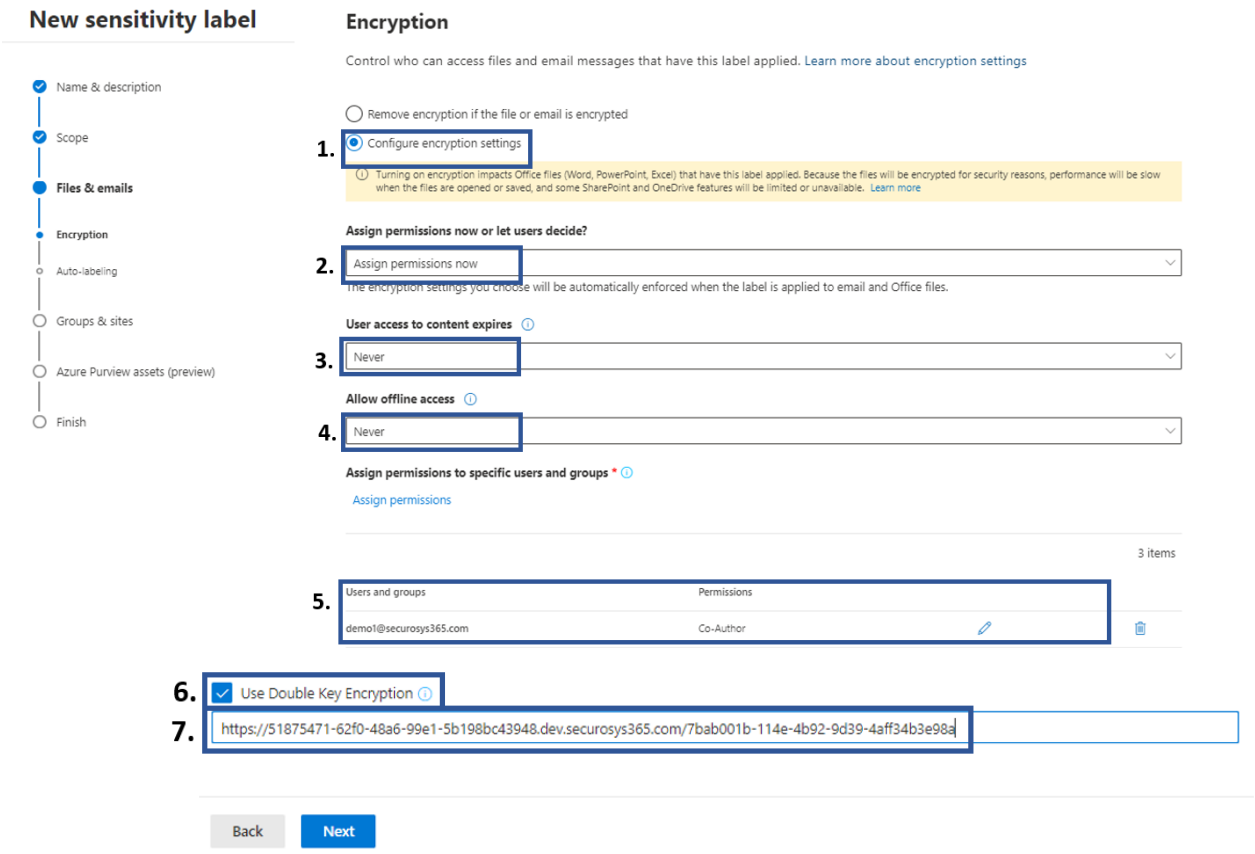


Figure 6: MIP Label (Enter DKE-URL)

Complete the label creation by completing the remaining sections *Auto-Labeling, Groups & sites, Azure Purview assets (preview)*, and *finally* click **Create Label**.

3.4.4 Publish label

The newly created label must be bound to a policy and published to display it to Microsoft 365 users. Select the **Publish Label** button.

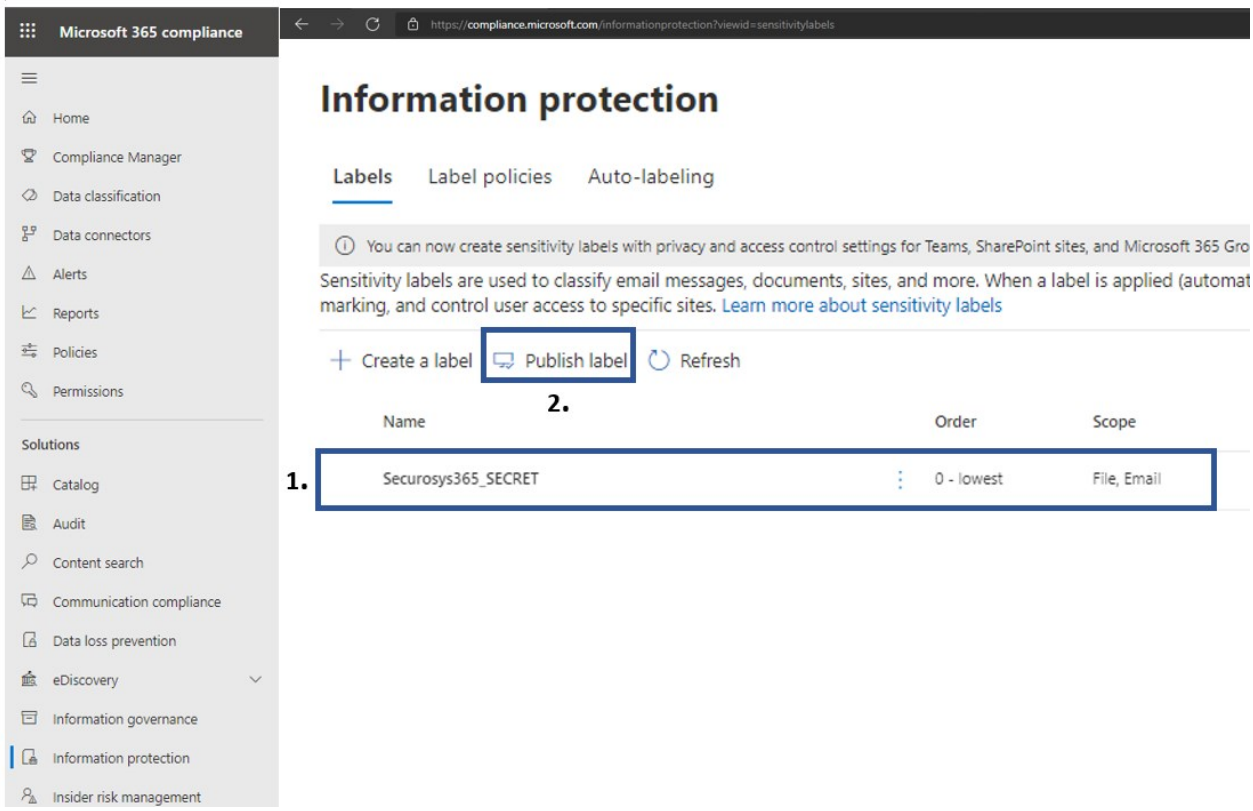


Figure 7: MIP Policy (Publish Label)

Click on the Link **Choose sensitivity label to publish** and select the newly created label *Securosys365_SECRET*

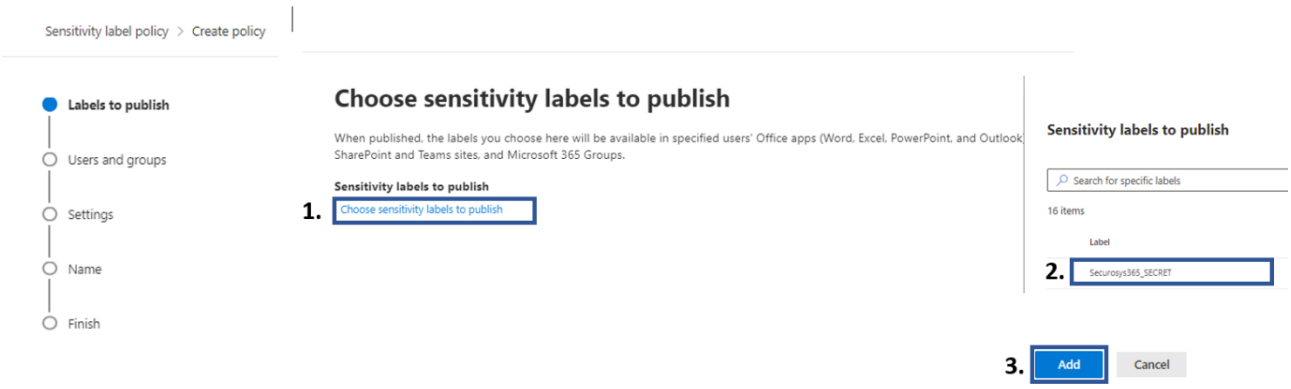


Figure 8: MIP Policy (selection label being published)

Continue with the remaining sections *Users&Groups*, *Settings*, *Name*, *Finish* and finally click the button **Submit**.

3.5 Test

3.5.1 Test DKE Protection

This chapter will test our newly created labels in Microsoft 365 applications. Please open Word, Excel, or PowerPoint.

3.5.2 Word, Excel, PowerPoint

- Create new file
- Select Sensitivity Label
- Save file to SharePoint or any other file location
- Close the file

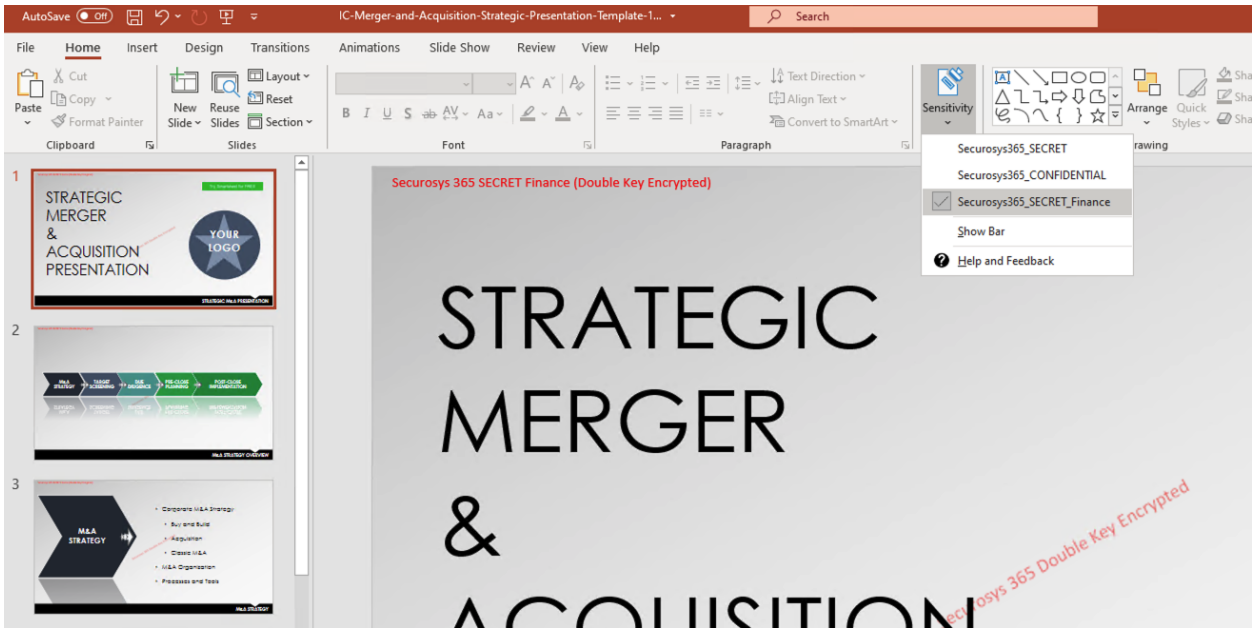


Figure 9: Applying Label to PowerPoint, Word, Excel

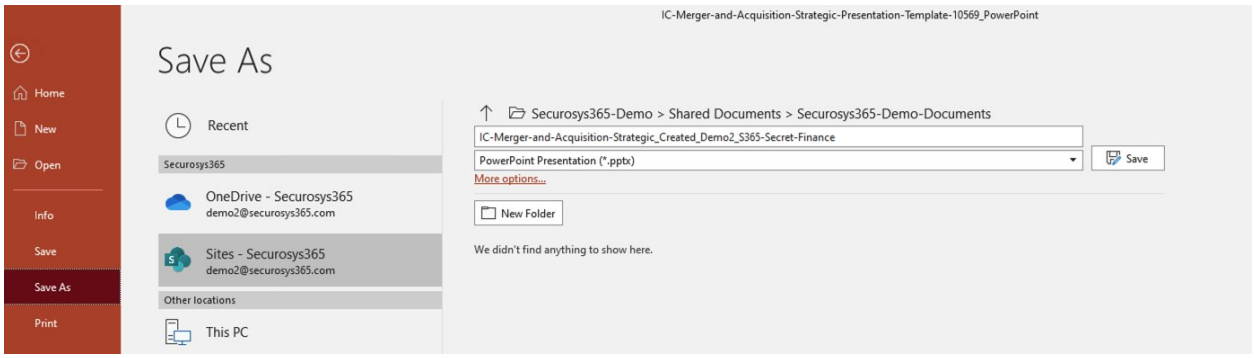


Figure 10: Saving Microsoft 365 Office Document

3.5.3 Outlook

- Create new E-Mail
- Send to a user with permission to the sensitivity label
- Attach a File (as attachment)
- Send

Note: Only file attachments with Microsoft Information Protection will automatically be protected.

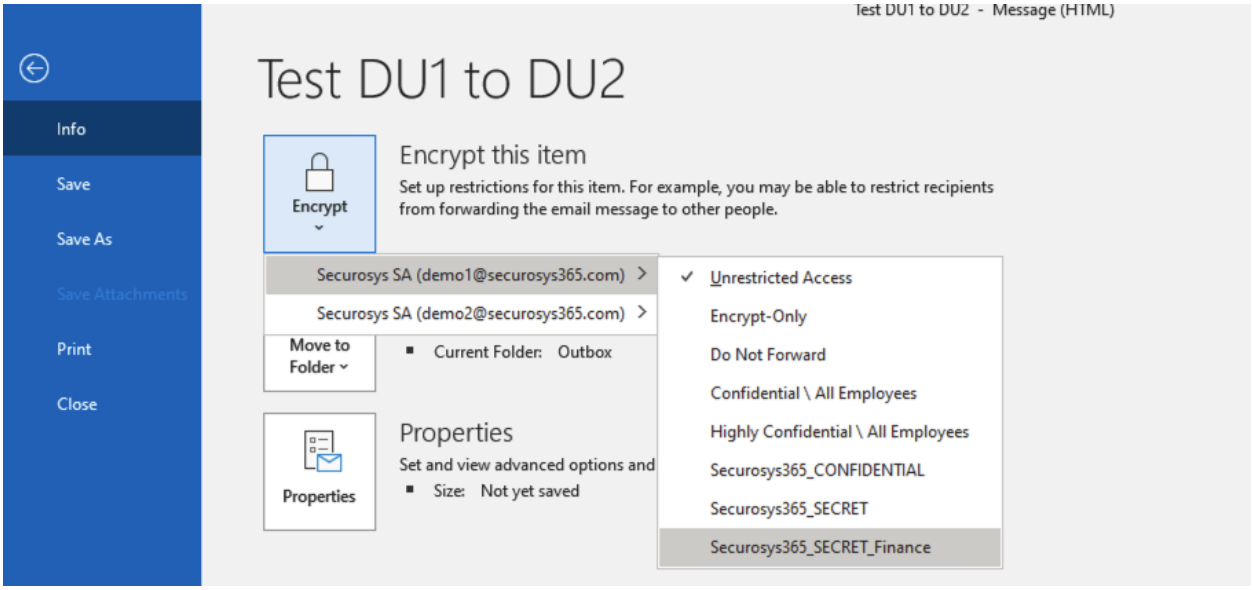


Figure 11: Sending DKE protected E-Mail

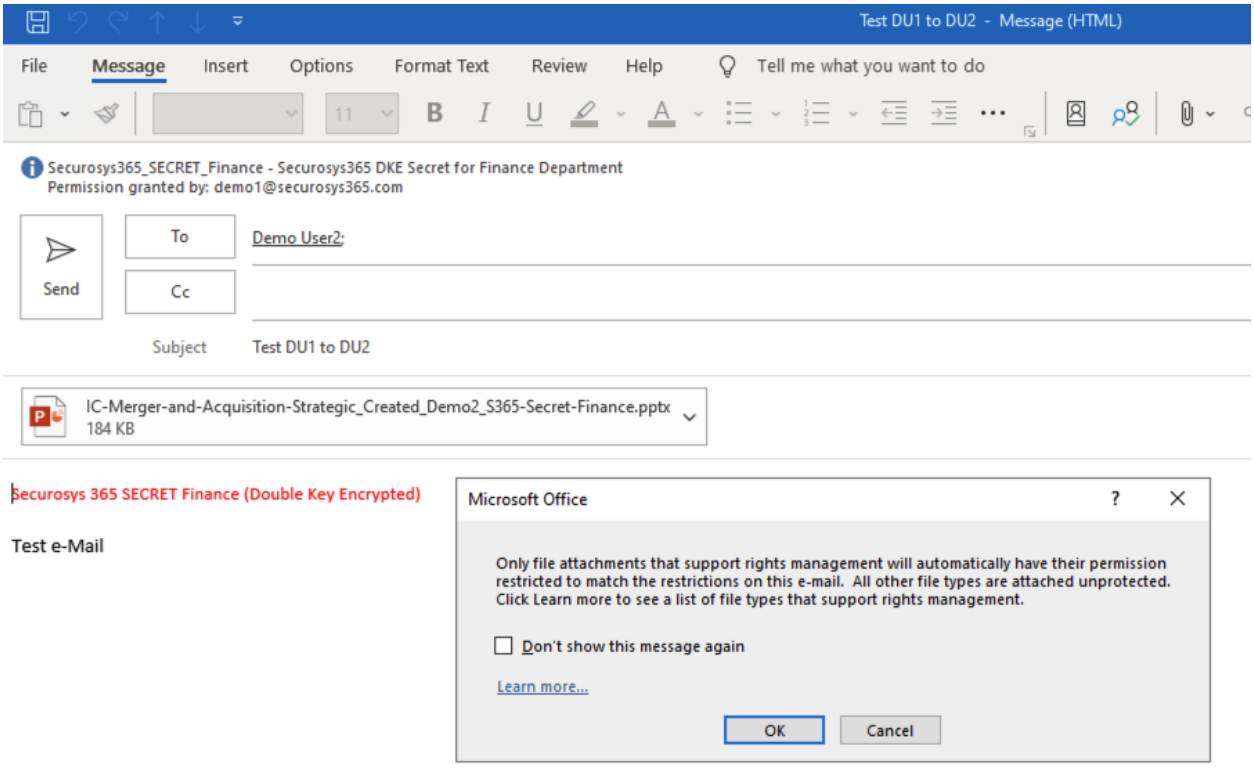


Figure 12: DKE protected E-Mail attachement

DISCLAIMER: The first time your organization uses Double Key Encryption in any Microsoft 365 application, a pop-up window will appear asking for your permission. To use Securosys 365 DKE, you must grant consent on behalf of your organization. Therefore, a user with permission level **Application Administrator**, must approve the permission request. Therefor the first Double Key Encryption process must be performed by an Application Administrator.

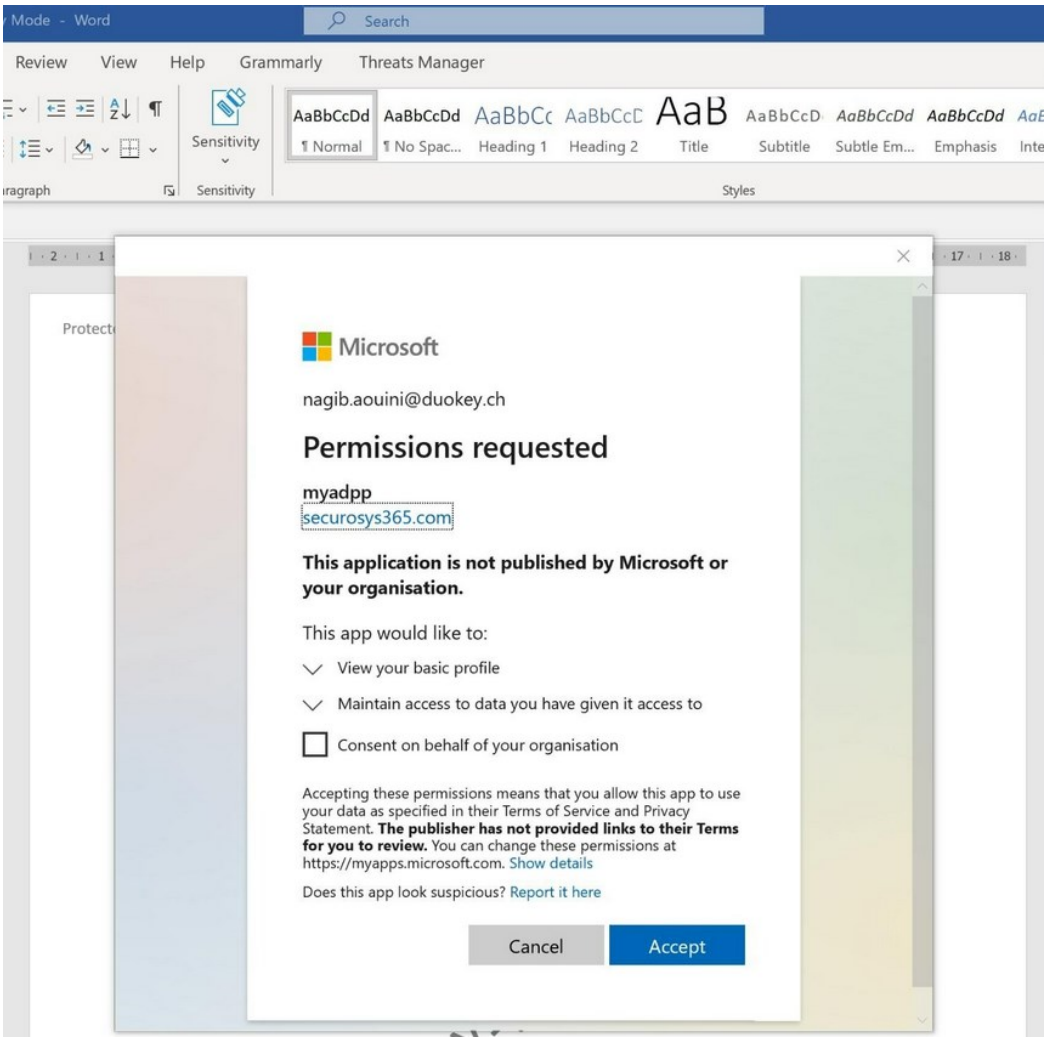


Figure 11: IMPORTANT (Applying consent of using Securosys DKE solution)

4 Additional Information

4.1 A Complete User Guide is available at (only accessible with SupportPortal Login)

https://support.securosys.com/external/knowledge-base/article/85

4.2 Securosys 365 DKE - Cockpit: Key and Service Management Web Application

Accessing the Key Management User Interface for more advances Double Key Encryption Configuration, please raise a ticket at

- https://support.securosys.com/external
- or contact us using https://www.securosys.com/contact

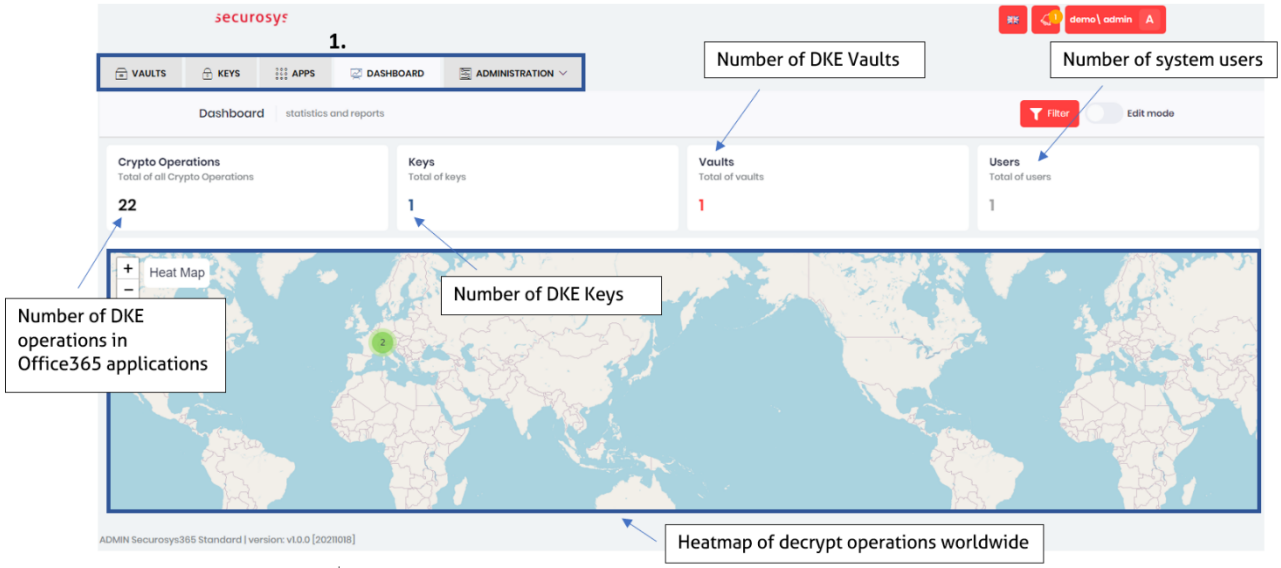


Figure 12: Securosys 365 - DKE: Cockpit (Key and DKE Service Management Web application)

4.3 Sample Architecture (best practice)

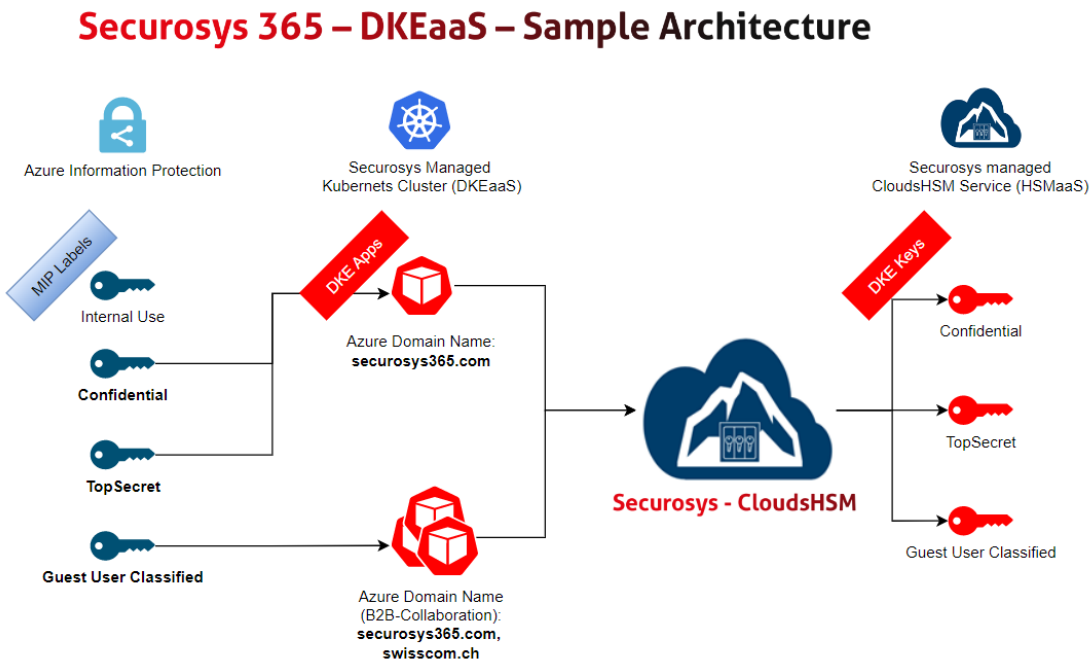


Figure 13: Double Key Encryption Sample Architecture

5 Table of Figures