GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

ARCHITECTURE AND SECURITY GUIDE

Version 11.0

Document last updated: November 2, 2023

Reference: sds-en-sdse-architecture_security_guide-v11.0

Table of contents

In the documentation, Stormshield Data Security Enterprise is referred to in its short form: SDS Enterprise and Stormshield Data Management Center in its short form: SDMC.

1. Getting started

The SDS Enterprise administration interface (SDMC) and the SDS Encryption Portal are offered in SaaS mode and managed by Stormshield's Cloud Service team.

This document provides technical information regarding the confidentiality, integrity and availability of our users' data.

2. Types of information stored

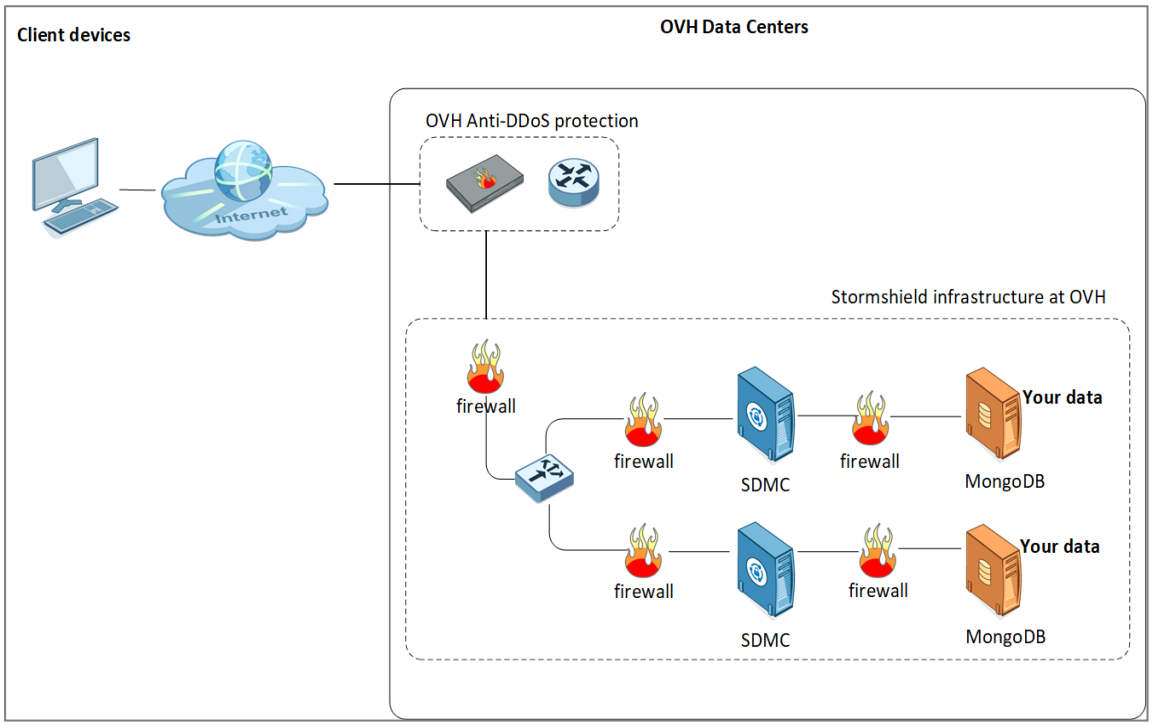
The table below describes the types of information that SDMC stores and how long such information is retained:

Data	Type	Location and retention duration
User data for access management	• First name, last name and e-mail address, • Device location (country).	• Operating system logs: 1 year • Daily backups of databases: 7 days • SDMC user logs: 30 days
Event logs for audit and monitoring	• User actions, date and time, • E-mail addresses (senders and recipients), • File name (no content), • Device: operating system, model, name and IP address.	• Operating system logs: 1 year • Daily backups of databases: 7 days • SDMC user logs: 30 days
System administration logs	• Software patches and updates • Account creation and deletion, • Operating system management operations, • Backup and restoration operations, • Server operations and maintenance.	• Operating system logs: 1 year • Daily backups of databases: 7 days • SDMC user logs: 30 days
End user keys Only for SDS Encryption Portal	End user keystore	As long as the user exists in SDS Encryption Portal
External user keys Only for SDS Encryption Portal	End user keys	As long as the user exists in SDS Encryption Portal

3. Protecting the infrastructure

3.1 Where your information is stored

All information regarding SDMC is stored in secure OVH datacenters in France. OVH deploys an anti-DDoS solution that protects the Stormshield infrastructure from denial of service attacks. In addition, all servers and databases that host your data are protected by several levels of Iptables firewalls.



3.2 How components communicate

All data flows between the various SDMC components go through the HTTPS protocol and port 443. The TLS version used is v1.2.

Service	Source	Destination	Description
Authentication with SDS Encryption Portal	User devices	https://sds.stormshieldcs.eu/portal	URL to access SDS Encryption Portal - and - Management of Helpdesk and Recovery users
Stormshield server (SDMC)	User devices	https://sds.stormshieldcs.eu	URL to access the Stormshield server (SDMC)
Stormshield API	User devices	https://sds.stormshieldcs.eu/api	URL to access information about users and logs, and to retrieve logs

Mailjet API	Stormshield server (SDMC)	Mailjet server	Used by Stormshield (SDMC) to send e-mails from the address *noreply@stormshieldcs.eu*

3.3 Vulnerability management

Stormshield's Cloud Services and Research & Development teams implement a vulnerability management policy during every publication without disrupting service. Stormshield's security officer monitors the results of automatic analyses of sensitive data.

4. Encryption algorithms

Passwords, password and file keys remain on users' devices and are never transferred anywhere or to anyone. User keys, group keys and your company's keys are stored encrypted on the SDMC server. All encryption operations take place on your device, never on Stormshield servers. Neither Stormshield nor the service host can access the private keys of your solution's internal users.

The following table lists the cryptographic algorithms used in SDMC.

Process	Algorithm	Details
Asymmetric key encryption	RSA PKCS 1.5 and RSA OAEP	2048 & 4096 bits
Symmetric key encryption	AES Key Wrap	256 bits
Symmetric data encryption	AES CBC Padding PKCS#7	256 bits
HMAC	HMAC SHA-256	256 bits
Password protection of keystore	PBKDF2	10,000 rounds and 32-bit salt
Password derivation	SHA-256 and Argon2d	Parallelism factor: 2 Memory cost: 8192 Iterations: 33 Salt: 128 bits

5. Protecting user accounts

This section deals only with SDS Encryption Portal.

There are several types of users in SDS Encryption Portal:

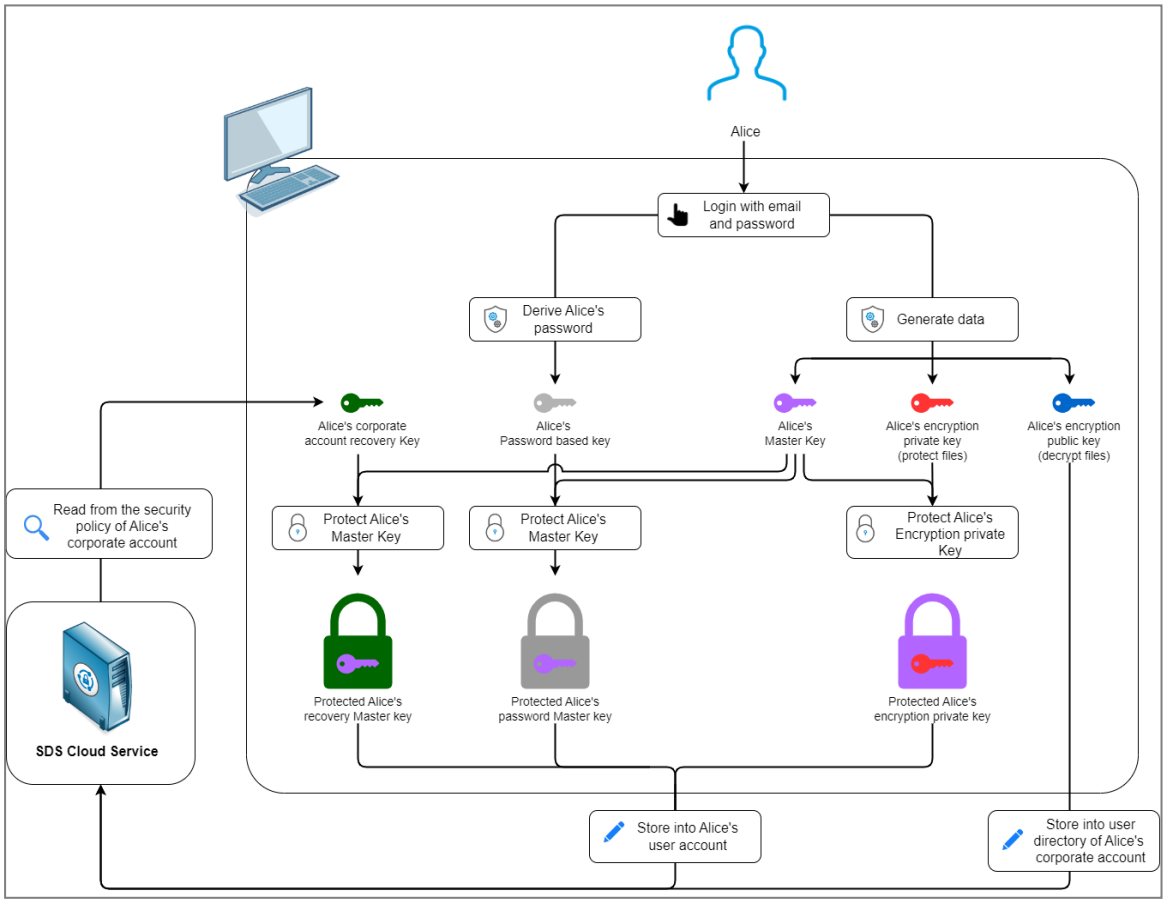
- Internal users who have paid a subscription fee through their company,
- External users who do not have user accounts.

Their data is protected differently, as they use different authentication methods.

5.1 Main principles for internal users

When a user creates an account in built-in key management mode, SDS Encryption Portal generates the following keys:

- The user's master key (purple key in the diagram),
- The user's private key (red key in the diagram),
- The user's public key (blue key in the diagram),
- The password key derived from a password hash (gray key in the diagram).



5.1.1 Public key

An SDS Encryption Portal user (Alice in the diagram) has a public key stored in the SDS cloud service, which all users of the corporate account can access. The public key makes it possible for these users to protect files for Alice. This is the only key saved in plaintext because it does not contain any sensitive information and is therefore not confidential.

5.1.2 Private key and master key

Alice needs her private key to read files that were protected for her. This key is wrapped with an intermediate asymmetric key, which is itself wrapped with the master key. As for the master key, it is wrapped in two ways:

- With Alice's password key, which only she knows (gray padlock in the diagram),
- With the public recovery key (green key in the diagram). The private recovery key is stored in the account of the recovery user and is protected with this account's master key, which is itself protected with a password.

As a result, Stormshield can never read your data, and no sensitive information is stored in the SDS cloud service.

5.1.3 Password key

The password key is derived from the user's password and never leaves the user's device. It is used to wrap the master key of the user's account. This master key will then be sent to the SDS cloud service database; the password itself is never stored. With this double level of protection, potential attacks are minimized.

The user's password key is the starting point in the process of decrypting a file – with it, the master key can be located, which itself makes it possible to locate the private keys needed to decrypt data.

SDS Encryption Portal never uses the password itself, only derivatives, i.e., the password key and/or this same key wrapped with the master key.

The password makes it possible to:

- Locate the master key to access sensitive data in the user account,
- Authenticate the user on SDS Encryption Portal.

5.1.4 Keystore

The user's keystore, which will be used to decrypt files, contains confidential data. It consists of the following keys:

- The master key wrapped in the password key,
- The master key wrapped in the public recovery key,
- The private key wrapped in an intermediate asymmetric key, which is itself wrapped in the master key.

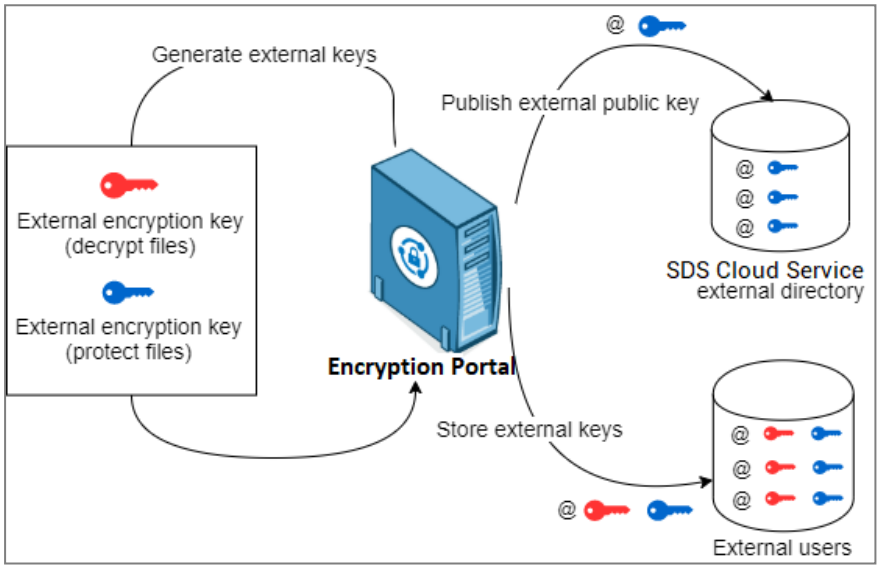
5.2 Main principles for external users

An external user (Bob) does not have a subscribed SDS Encryption Portal account. When another user wants to encrypt files for him, SDS Encryption Portal will generate the following keys:

- An external public key (blue key in the diagram). This key is published in the external directory in the SDS cloud service and can be accessed by all internal and external users. It allows these users to protect files for Bob.
- An external private key (red key in the diagram). It allows Bob to decrypt files that were protected for him. Unlike keys for internal users, the external private key is stored in the SDS cloud service.

Keys are associated with the user's e-mail address. They remain the same throughout the use of the SDS Encryption Portal.

The keystore of an external user, which will be used to decrypt files, contains only the external private key.

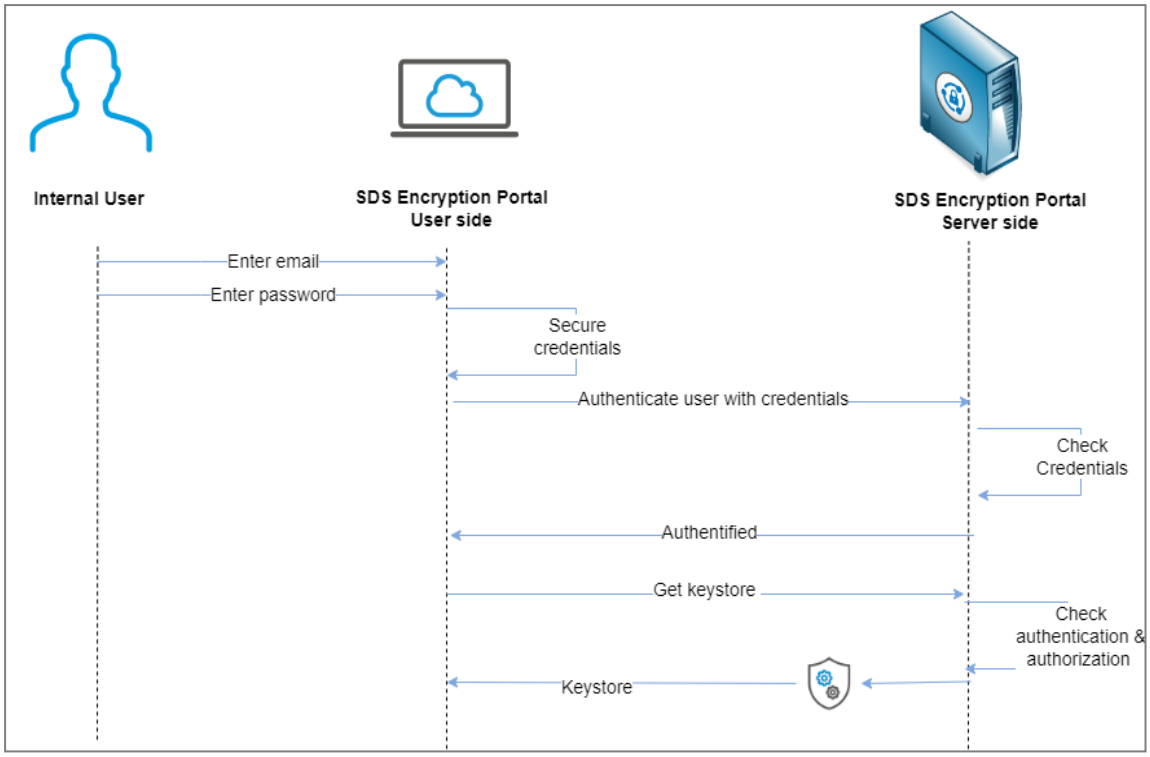


5.3 User authentication on SDS Encryption Portal

User authentication to log in to SDS Encryption Portal is different depending on whether the user is internal or external.

5.3.1 Connecting internal users on SDS Encryption Portal

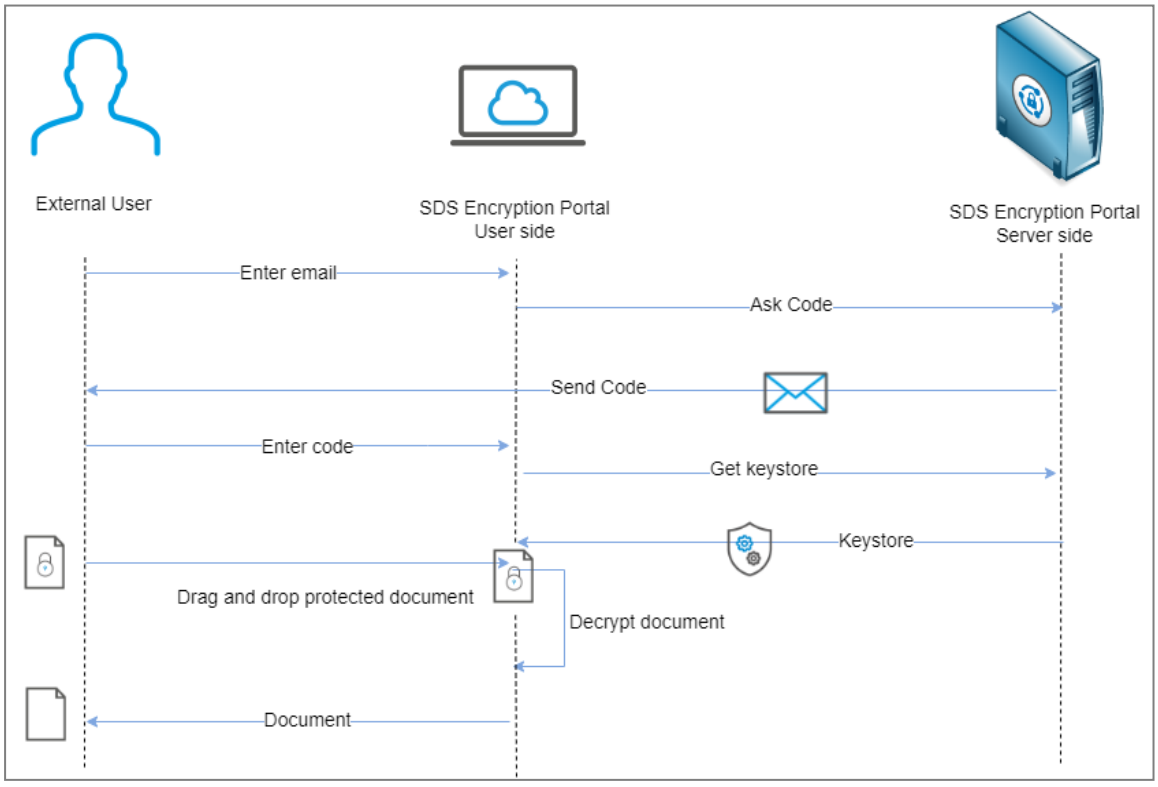
Internal users enter their e-mail addresses and passwords on SDS Encryption Portal, which sends them to the SDS cloud service. Passwords are sent via an SHA256 hash. The SDS cloud service checks the user's credentials, so the user can request the keystore. After verifying authorizations, the SDS cloud service makes the keystore available to the user. Once connected, the user can protect or decrypt files.



5.3.2 Connecting external users on SDS Encryption Portal

Every time external users log in to SDS Encryption Portal with their e-mail addresses, they receive a unique access code that remains valid for two hours and is deleted after use. This code allows users to authenticate and retrieve the keystore they need to decrypt the file.

External users who have never been invited cannot log in to SDS Encryption Portal.



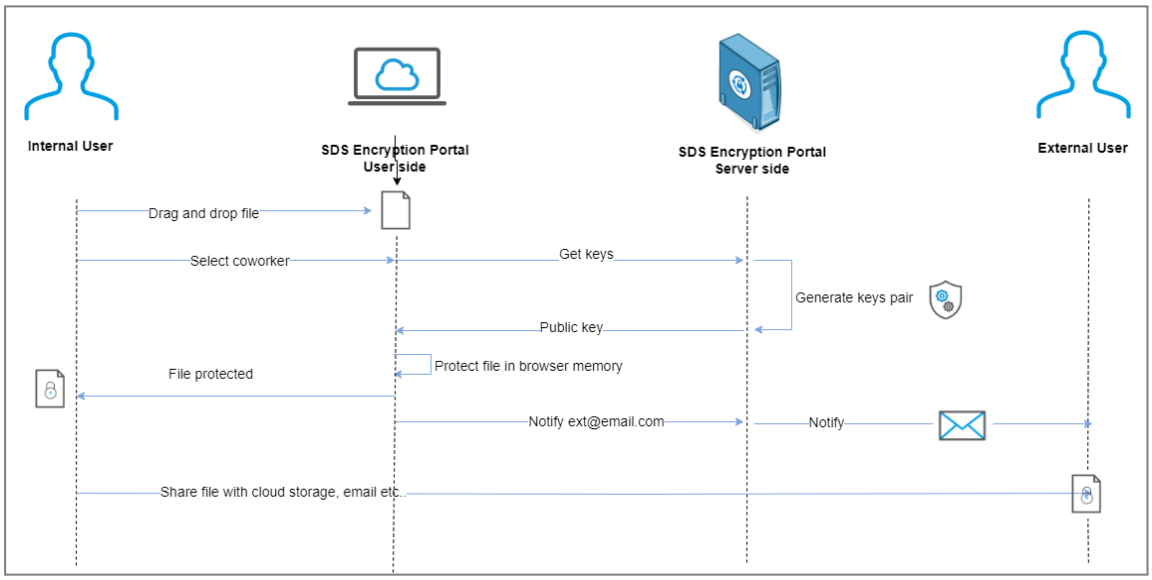
6. Protecting files in SDS Encryption Portal

SDS Encryption Portal combines asymmetric encryption with RSA, and symmetric encryption with AES. Every file has its own random key, which is generated when the file is created and every time content is changed. The file key is used to protect the file's contents and to decrypt it. For more information, refer to the section **Encryption algorithms**.

This section describes how files are protected and decrypted in SDS Encryption Portal.

6.1 Protecting files

1. When Alice, regardless of whether she is an internal or external user, uploads a file on SDS Encryption Portal, she must specify the e-mail address of the external user (Bob) for whom she is protecting the file.
2. If Bob does not yet have an external public key, **a pair of external keys will be generated** for him.
3. SDS Encryption Portal uses Bob's external public key to protect the file for him.
4. Alice makes the protected file available to SDMC, through SDS Encryption Portal Server side.



6.2 Decrypting protected files

1. After logging in to the SDS Encryption Portal external user Bob uploads a protected file.
2. The file is decrypted directly on the portal using the user's external private key.
3. The file is then downloaded and saved on the user's workstation.

7. The corporate account

The corporate account contains all the information relating to your company: It is created at the beginning, when your company is registered on the SDMC solution.

The corporate account is dedicated to a single company and is never shared with other companies.

7.1 Information stored in the corporate account

The corporate account contains the following information:

Type of information	Description
Administrators	Information on administrators.
Users (In SDS Encryption Portal only)	• Operations performed by users, • User characteristics, including helpdesk and recovery roles dedicated to the corporate account, • Information on the user account and public keys (in built-in key management mode only).
Policies	Information on workstation policies.
License	Information on the license that defines components and the number of users allowed to use the service.
Settings	Information about your company, domains associated with your corporate account and collaboration with external companies.

7.2 Link between the company and the corporate account

When you create your corporate account, you must use an e-mail address attributed to your company. The domain name that it contains will automatically be considered the default domain – only users who have e-mail addresses with this domain name will be allowed to create a corporate account in SDS Encryption Portal.

You can then add one or several domains to your corporate account so that users belonging to these domains can also create an account in SDS Encryption Portal. This will make it possible to include users from subdomains or branches of your company.

8. Helpdesk and recovery

The use of SDS Encryption Portal requires setting up a recovery system that makes it possible to retrieve encryption data within legal requirements.

In SDS Encryption Portal, the first user account that is created becomes the recovery account, and its owner is the security administrator. This account is needed to run the solution and will never be deleted.

The roles of the security administrator are the following:

Helpdesk: assigns a new password to users who have forgotten their passwords or if password confidentiality has been compromised,

Recovery: grants access to all the protected files of one user to another user, for example if the former user has left the company.

Since external users do not have paid SDS Encryption Portal accounts, they do not need a helpdesk or recovery system. They also do not have passwords and authenticate with a unique temporary code. To retrieve their protected files, they only need to provide their e-mail addresses.

8.1 Generating recovery keys

When the first user creates an account, SDS Encryption Portal generates recovery keys on the same basis that it generates encryption keys for standard users.

All user accounts created after this will be protected with both the key from the user password and the public key of the recovery account.

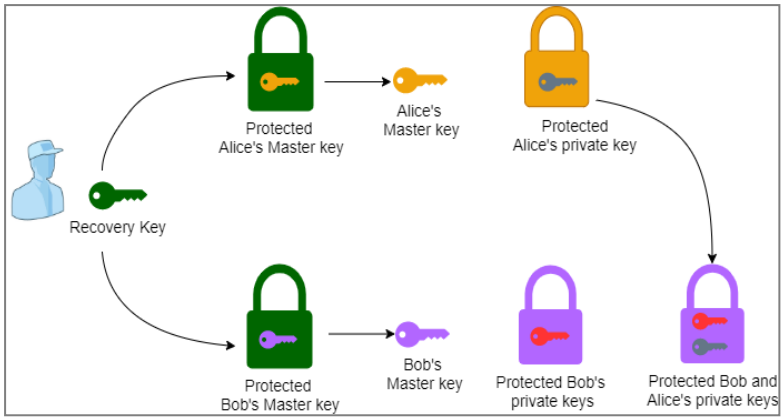
For more information, refer to the diagram in the section Main principles for internal users.

In SDS Encryption Portal, the recovery account is a user account, not an administrator account, because recovery operations require keys to be generated. Administrator accounts do not have keys.

8.2 How the Recovery role works

The Recovery role allows the security administrator to delegate the private key of User A (Alice) to User B (Bob) so that Bob can access all of Alice's protected files. To do so:

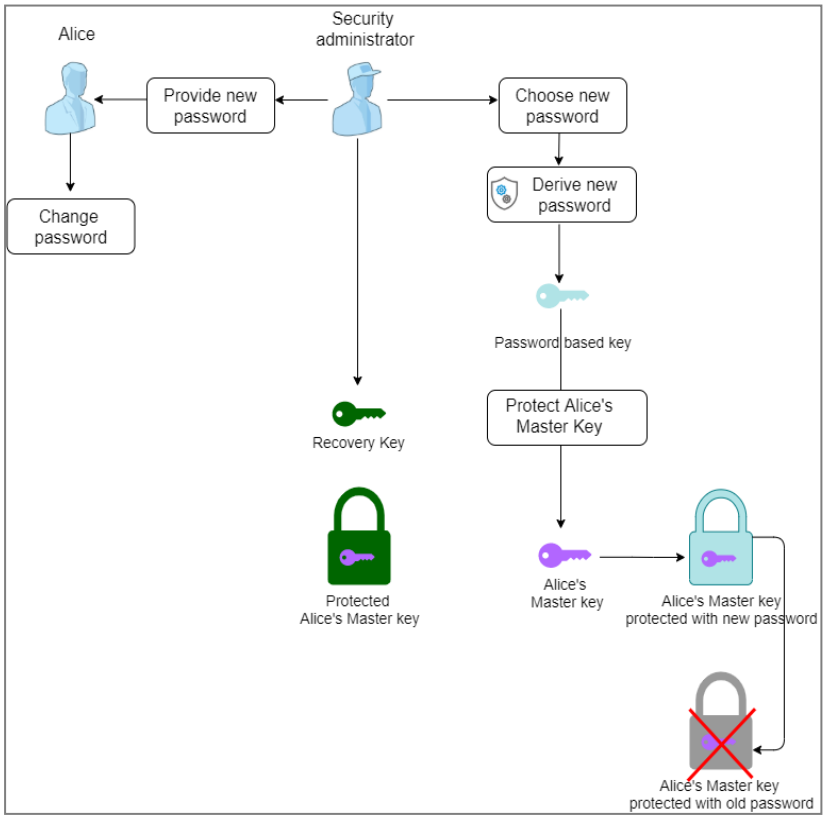
1. The security administrator retrieves Alice's master key using the private recovery key.
2. The master key decrypts Alice's key store.
3. Likewise, the security administrator retrieves Bob's master key.
4. Bob's master key is then used to wrap Alice's private key again, which will then be added to Bob's keystore. This key will only be used to decrypt files.



8.3 How the Helpdesk role works

The Helpdesk role allows the security administrator to change a user's (Alice) password if it is forgotten or needs to be more secure. To do so:

1. Alice informs the Helpdesk security administrator that she has lost her password.
2. The security administrator decrypts Alice's master key using the private recovery key.
3. The security administrator chooses a new password from which SDS Encryption Portal will generate a password key.
4. The master key is wrapped with the new password key.
5. The security administrator sends Alice the new password assigned to her.
6. Alice logs in to SDS Encryption Portal with this new password and she will be asked to replace it with a password of her choice. The security administrator will not know Alice's final password.



9. 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

documentation@stormshield.eu