# Stormshield Data Security

## for Google Workspace

## Version 4.1.2

# CSPN Security Target

**Document version:** 1.3

**Reference:** KAPUA/ST

**Date:** 24/09/2024

# Contents

# List of figures



# List of tables

# 1. INTRODUCTION

## 1.1 DOCUMENT PURPOSE

This document is produced as part of the evaluation of the «Stormshield Data Security for Google Workspace» product, developed by the **Stormshield** Company under the CSPN scheme (promoted by the ANSSI).

The considered TOE is Stormshield Data Security for Google Workspace in version “OnPremise”, i.e., hosted and maintained by the organization or company using it.

## 1.2 PRODUCT IDENTIFICATION

| | |
|---|---|
| **Developer** | Stormshield<br>2-10 Rue Marceau à Issy-les-Moulineaux<br>92130 Issy-les-Moulineaux |
| **Developer’s website** | www.stormshield.com |
| **Commercial name** | Stormshield Data Security for Google Workspace |
| **Evaluated version** | 4.1.2 |

*Table 1 – Product Identification*

## 1.3 REFERENCES

For the writing of this security target, the following documents were used:

- SDS-FR-Google-Workspace-Datasheet.pdf
- SDS-FR-Data-Security-Range-Brochure.pdf
- list-of-dependencies.html
- Cryptography.pdf
- sds-fr-sds_for_gw-guide_d_administration-v4.pdf

## 1.4 GLOSSARY

| Acronym | Definition |
|---|---|
| ANSSI | *Agence Nationale de la Sécurité des Systèmes d’Information* |
| COTS | Commercial Off-The-Shelf |
| CSE | Client Side Encryption |
| CSPN | *Certification de Sécurité de Premier Niveau* |

| Acronym | Definition |
|---|---|
| DEK | Data Encryption Key |
| KACLS | Key Access Control List Service |
| KEK | Key Encryption Key |
| KMIP | Key Management Interoperability Protocol |
| KMS | Key Management Service |
| SaaS | Software as a Service |
| SDS | Stormshield Data Security |
| TOE | Target Of Evaluation |

*Table 2 - Glossary*

# 2. PRODUCT DESCRIPTION

## 2.1 GENERAL DESCRIPTION

The Google Workspace environment offers the Client-Side Encryption (CSE) technology which allows companies to use their own encryption keys to protect document stored in Google environments, Google Slides presentation and Google Sheets spreadsheets stored in Google Drive, as well as Google Meet video and Google Calendar appointments.

The Stormshield Data Security solution is transparent and integrated into your usual Google workspace, enabling your business teams to create secure collaboration environments, regardless of the media, devices and applications involved.

The Stormshield Data Security solution offers you the guarantee of secure communications with all users in your environment. This full integration ensures that all your employees enjoy the same user experience. One click is all it takes to activate data protection

Cloud data is stored on servers beyond the scope of the company. There must, therefore, be a guarantee that the administrators of these platforms cannot consult sensitive data. In addition to file access controls, the data is also protected by a key for authorised users.

As part of this CSE infrastructure, **Stormshield Data Security (SDS) for Google Workspace** ensures the protection of encryption keys for sensitive data.

More specifically, SDS offers the following features:

- **Access control** to the encryption keys of sensitive data via authorization and authentication tokens ,
- **Protection** of the encryption key of sensitive data,
- **Secure communication** with CSE infrastructure components,
- **Logging** (encryption/decryption operations, access control results, etc.).

The possible logs are “operations logs” and “usage logs”.

The activation of the encryption feature is done on the Google Workspace admin console. The following elements must be done:

- Configure the key encryption service;
- Configure the IDP part;
- Enable the encryption function:
    - By group ;
    - By Google component ;
- Display encryption logs;
- Creation of encryption log reports.

A CSE infrastructure consists of the following components:

| Components | Roles |
|---|---|
| Google Workspace | It has a dual role. Firstly, it identifies the user and manages its authorizations. Secondly, it allows the storage of data encrypted by the user. In the context of the CSE, Google Workspace does not hold either clear data (encryption key, data) or the possibility of decrypting the encrypted data transmitted to it. |
| Identity Provider (IdP) | It identifies the user in the client’s infrastructure. Authentication through the identity provider ensures that the user belongs to the client’s infrastructure and has the necessary rights to access the resources. |
| Key Management System (KMS) and HSM | It is a secure environment that generates, persists and delivers KEKs to KACLS.<br>It centralizes and secures the KEKs. KEKs being a sensitive data, their transfer to the KACLS is done with the KIMP protocol on TLS. |
| SDS for Google Workspace (KACLS) | Its role is to:<br>• encrypt and decrypt the DEK with a KEK at the user’s request.<br>• Check a series of rules essentially to authenticate the user performing the request and its permission.<br>The KEK is stored only in RAM. There is no persistence of the KEK on the KACLS server. |
| User (browser) | Its role is to allow the user to benefit from the Google Workspace suite on its workstation (Drive, Meet, Calendar) and to allow it to encrypt them. It is the actor generating and using the DEK. |

*Table 3 - CSE Components*

SDS encryption services for Google Workspace can be managed manually via the config.json file.

## 2.2 PRINCIPE OF OPERATION

When the user wants to activate Google Documents encryption, he must be identified using IdP service. The user enables encryption by checking a box in the interface.

This figure illustrates encryption process:

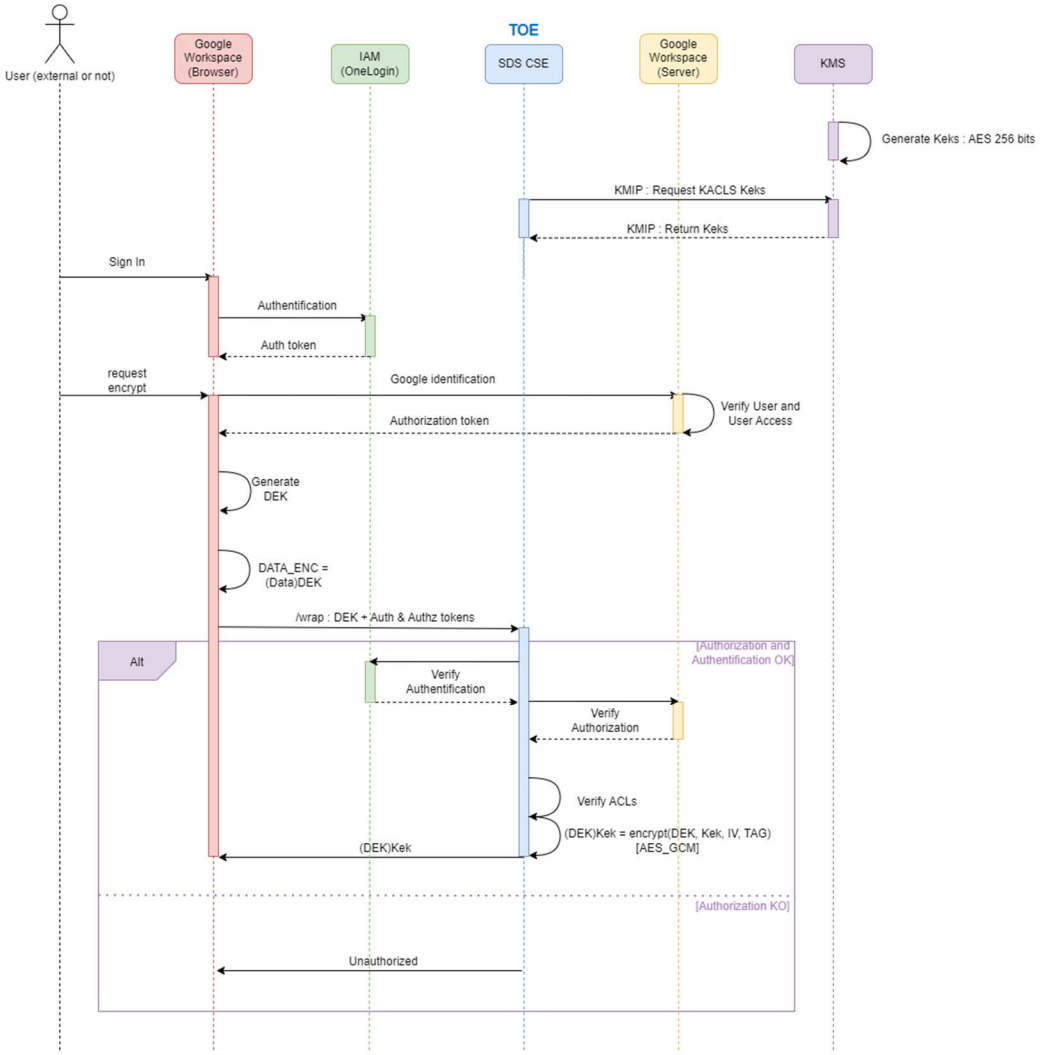


*Figure 1- Data Encryption operations*

The administrator administers using the configuration file.

## 2.3 DEPENDENCIES

Before installing the SDS encryption service for Google Workspace, it is necessary to install NodeJS 20 and OpenSSL 3 (delivered by default with OS RedHat Enterprise Linux 9.x).

## 2.4 INTEGRATED COTS

The third-party components integrated (COTS) into the product and used by the TOE are presented in the following table

For the COTS mentioned “Out of TOE”, It is the responsibility of the solution administrator to install andupdate those COTS.

| COTS | Used version | Last version | Patch or modification applied | Up to date | Always maintained | Usage | In or Out TOE |
|---|---|---|---|---|---|---|---|
| **OpenSSL** | 3.0.8 | 3.0.12 10/2023 | No | Yes | Yes | Secure communication | Out TOE |
| **Ajv** | 8.12.0 | 8.12.0 30/05/2023 | No | Yes | Yes | Data validation by scheme | In TOE |
| **cborg** | 2.0.5 | 4.0.8 **15/01/2024** | No | No | Yes | Encodes and decodes in cbor format | In TOE |
| **cors** | 2.8.5 | 2.8.5 04/11/2018 | No | Yes | Yes | Validation of request cors | In TOE |
| **Express** | 4.18.2 | 4.18.2 08/10/2022 | No | Yes | Yes | Framework web for nodejs | In TOE |
| **Node-fetch** | 2.7.0 | 3.3.2 23/08/2023 | No | Yes (Critical bugfix will still be publish on V2) | Yes | Making requests to other resources | In TOE |
| **Node-forge** | 1.3.1 | 1.3.1 30/03/2022 | No | Yes | Yes | Cryptographic operation | In TOE |
| **Node.js** | 20 | 20 18/04/2023 | No | Yes | Yes | Interface | Out TOE |
| **Reflect-metadata** | 0.2.1 | 0.2.1 2018 | No | Yes | No | Dependence injection | In TOE |
| **Tsyringe** | 4.8.0 | 4.8.0 | No | Yes | Yes | Dependence injection | In TOE |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 20/06/2023 | | | | | |
| **Winston** | 3.11.0 | 3.11.0<br>07/10/2023 | No | Yes | Yes | Formatting logs | In TOE |
| **Cryptsoft** | 2.1.1n | 2.1.1n | No | Yes | Yes | KMIP protocol implementation | In TOE |
| **@Open-policy-agent/opa-wasm** | 1.8.1 | 1.8.1<br>12/01/2024 | No | Yes | Yes | Open policy agent support | In TOE |
| **sanitize-html** | 2.11.0 | 2.11.0<br>21/06/2023 | No | Yes | Yes | Data sanitize | In TOE |
| **prom-client** | 15.1.0 | 15.1.0<br>15/12/2023 | No | Yes | Yes | Promotheus client for metric | In TOE |
| **lru-cache** | 10.1.0 | 10.1.0<br>22/11/2023 | No | Yes | Yes | Lru cache for fetcher | In TOE |
| **Jose** | 5.2.0 | 5.2.0<br>24/12/2023 | No | Yes | Yes | Json web token validation | In TOE |
| **https-proxy-agent** | 7.0.2 | 7.0.2<br>04/09/2023 | No | Yes | Yes | Allow Proxy usage | In TOE |

*Table 4 - List of COTS used by the product*

## 2.5 TECHNICAL OPERATIONG ENVIRONMENT

### 2.5.1 Compatible or dedicated equipment

Not applicable. The TOE is a RedHat server.

### 2.5.2 Operating system selected

In the context of the evaluation, the product will be deployed on OnPremise with the RedHat 9 operating system with a Node.js 20 runtime environment.

## 2.6 EVALUATION SCOPE

### 2.6.1 Scope

The scope of the evaluation is composed of the SDS for Google Workspace and its communications with Google Workspace, the identified provider and the KMS.

The external storage of the keys in the KMS is considered out of scope, for the evaluation the KMS will be from Thales.

The configuration of the evaluated product is presented in the following table.

| Component of the overall system | | Included in the evaluation target (TOE) | Not evaluated (TOE environment) | |
|---|---|---|---|---|
| | | | Assumed to be trusted | Is a potential attacker |
| Component SDS Version 1 | Operating system : RedHat | | √ | |
| | Cryptographic functions : Open SSL | √ | | |
| Component KMS : | CypherTrust Manager version 2.8.0 | | √ | |
| **User workstation** | Operating system : Windows 11 22H2 | | √ | |
| | Google Workspace with Client-Side Encryption (CSE) activated | √ | | |
| **Identity provider** | Server OneLogin | | √ | |

*Table 5 - Evaluated product configuration*

### 2.6.2 Evaluation platform

The evaluation platform consists of the following components:

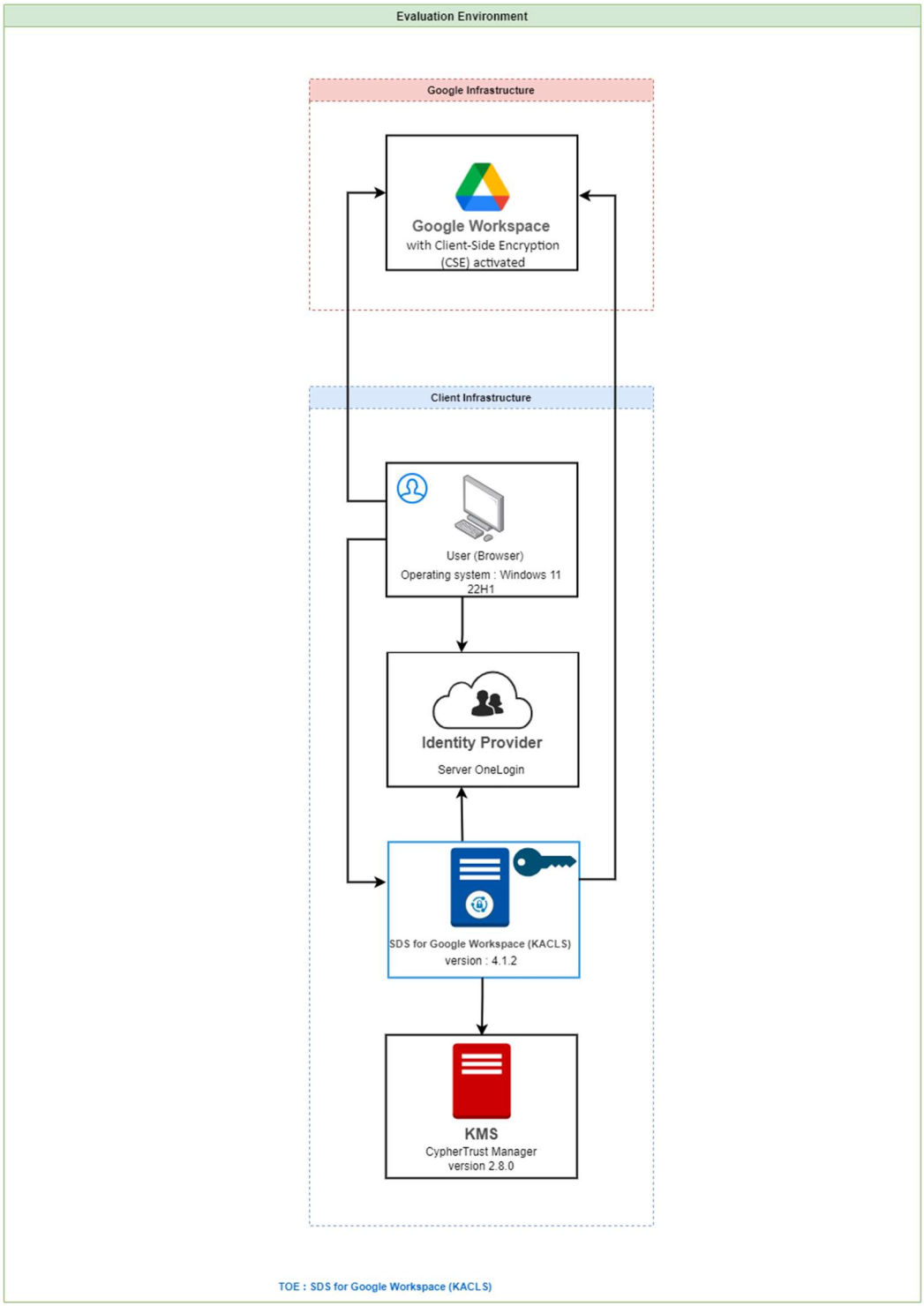


*Figure 2 - Evaluation Platform*

# 3. SECURITY PROBLEM

## 3.1 PRODUCT USERS

The users are the persons and applicative services that interact with the TOE. The following users are considered for this evaluation:

- **User**: TOE user, using the solution as a service to encrypt its data;
- **Administrator**: Administrator in charge of the administration of the TOE.

## 3.2 SENSITIVE ASSETS

An asset is a piece of data (or a function) assessed to be of value for the TOE. Its value is estimated according to safety criteria (also called security needs): availability, integrity, confidentiality, authenticity:

**Sensitive assets of end users:**

- **B1. User authentication token**

  The authentication token of users (including administrators), generated by the Identity Provider.

  Security needs: availability, integrity, confidentiality.

- **B2. User authorization token**

  The authorization token (JWT) ensures that the user is authorized to perform a request. It is generated by Google Workspace.

  Security needs: availability, integrity, confidentiality, authenticity.

**Sensitive assets of the TOE:**

- **B3. Configuration**

  The global configuration of the SDS encryption services for Google Workspace is managed via the config.json file. By default, this file is located in the folder: /etc/stormshield/cse. It defines the specifications for authentication and authorization, as well as the communication port, the service name and the service mode.

  Security needs: integrity.

- **B4. Network traffic**

  Network traffic between TOE and the client web browser must be protected.

  Security needs: availability, integrity, confidentiality and authenticity.

- **B5. Logs**

  The events logged by the TOE and available in JSON format must remain intact and available.

  Security needs: integrity, availability.

- **B6. Cryptographic material**

  The KEK used to protect the file encryption keys (DEK) must be protected.

  Security needs: availability, integrity and confidentiality.

The security requirements for each of the asses to be protected are summarized in the following table.

| Sensitive asset | Availability | Integrity | Confidentiality | Authenticity |
|---|---|---|---|---|
| B1. User authentication token | ● | ● | ● | |
| B2. User authorization token | ● | ● | ● | |
| B3. Configuration | ● | ● | | |
| B3. Network traffic | ● | ● | ● | ● |
| B4. Logs | ● | ● | | |
| B6. Cryptographic material | ● | ● | ● | |

*Table 6 - Sensitive assets*

## 3.3 ENVIRONMENTAL ASSUMPTIONS

An assumption is a statement on the context of use of the TOE or on the TOE environment. The assumptions about the TOE environment to be considered are as follows:

- **H1. Administrator**

  The TOE administrators are trained in good security practices and use of the TOE.

- **H2. Installation**

  The RedHat OS is, by assumption, up to date. Furthermore, during the installation, the ISO image is considered to be intact.

- **H3. Files encryption**

  The user always uses, by assumption, the encryption function proposed by Google Workspace to protect documents.

- **H4. KMS**

  The KMS used by the TOE is a reliable and integrated solution.

- **H5. IDP**

  The identity provider (IDP) used by the TOE is a trusted and integrated solution.

- **H6. Secure server environment**

  The TOE server is located in a secure physical environment with access control protocols.

## 3.4 THREATS

By definition, a threat is an action or event that may affect the security of the TOE. The threat agents to be considered for the evaluation are the following:

- Authorized entities :
  - A legitimate user (from Google Workspace) wanting to elevate its privileges on the Google file system.
- Unauthorized entities:
  - An entity that interacts with the TOE, but does not have legitimate access to it.

The administrator is considered trusted.

Consequently, the TOE must resist these threatening agents as well as the software and hardware means implemented by them. These means are the following:

| Means used by the threatening agents | Means applied | | TOE resistant to an attacker | |
|---|---|---|---|---|
| | Software | Hardware | Local | Distant |
| User session vulnerability | ● | | ● | ● |
| Network vulnerability | ● | | | ● |
| System vulnerability | ● | | | ● |

*Table 7 - Means deployed by threatening agents*

The threats to the sensitive assets of the TOE are the following:

- **T1. Session theft**

  An attacker manages to theft a legitimate user session in order to impersonate user identity.

- **T2. By passing access control**

  A legitimate user of the TOE manages to bypass access rights and thus elevate its privileges, or another beneficiary sharing the same base manages to access information from the TOE.

- **T3. Configuration corruption**

  An attacker manages to corrupt TOE configuration in order to downgrade its security.

- **T4. Tokens corruption**

  An attacker succeeds in altering the token of authorization of legitimate users of the TOE.

- **T5. Illegitimate access to the decryption key (in clear)**

  An attacker manages to access the decryption key of one or more files.

- **T6. Log data alteration**

  Logging data is corrupted or deleted (by an attacker to hide illegitimate actions).

- **T7. Cryptographic elements modification**

  An attacker manages to modify the cryptographic keys handled by the TOE.

- **T8. Denial of service**

  An attacker succeeds in making all or part of the TOE unavailable.

- **T9. Communication compromised**

  An attacker manages to modify or capture the content of communications between the TOE and other components.

## 3.5 SECURITY FUNCTIONS

### 3.5.1 Security functions

The security functions are the technical measures and the mechanisms enforced by the TOE to protect the sensitive assets from the threats. The security functions of the TOE are:

- **SF1. Identification, authentication and users access control**

  Before decrypting the files, the TOE performs a double check. The solution first verifies authentication, it checks the identity of the user thanks to OpenID. OpenID is used to identify and authenticate users. The solution then verifies the authorization, i.e., it checks the user's access rights to the files to be encrypted or decrypted.

- **SF2. Communications security**

  Communication between the user's web browser and the SDS server is done using the HTTPS protocol. Exchanges from SDS to KMS are done using the KMIP protocol, and exchange with the IDP implement the OpenID standard in HTTPS.

- **SF3. Cryptographic functions and random number generation**

  The user's files are encrypted using a DEK key from the user's computer (out of scope). This DEK key is itself protected by the TOE with a KEK key. The KEK key is generated and stored in the KMS (outside the TOE). The configuration is protected by access rights.

  The TOE generates the 96-bit initialization vector used to protect/encrypt the DEK key.

- **SF4. Logging**

  All operations performed by the TOE are logged in JSON format. There are two types of logs:

  - Operation logs: TOE start-up, KEK request to KMS, etc.
  - Usage logs: encryption request, decryption request, etc.

### 3.5.2 Disabled functions

Deactivated functions are function considered to be outside the scope of the evaluation (outside the TOE) and not accessible to an attacker. These functions will not be considered during the evaluation. The disabled function of the TOE are the following:

- **DF1.Autonomous mode**

  The device supports autonomous mode for KEK storage. This is not considered for evaluation.

- **DF2. GMAIL encryption**

  The device supports Gmail encryption. This is not considered for evaluation.

- **DF3. KACLS migration**

The solution enables migration from one KACLS to another. This is not considered for evaluation.

- **DF4. Metrics**

  The solution enables the usage of metrics for a promotheus monitoring. This is not considered for evaluation.

- **DF5. Proxy**

  The solution enables the usage of a proxy. This is not considered for evaluation.

- **DF6. OPA**

  The solution enables the support of open policy agent. This is not considered for evaluation.

## 3.6 TRACING

### 3.6.1 Threats and sensitive assets

The following table traces back the sensitive assets to the threats (letters “V”, “I”, “C”, “A” meaning respectively Availability, Integrity, Confidentiality, Authenticity):

| | B1. User authentication token | B2. . User authorization token | B3. Configuration | B4. Network traffic | B5. Logs | B6. Cryptographic material |
|---|---|---|---|---|---|---|
| T1. Session theft | IC | | | | | |
| T2. By passing access control | | IC | | | | |
| T3. Configuration corruption | | | IC | | | |
| T4. Tokens corruption | I | IA | | | | |
| T5. Illegitimate access to the decryption key | | | | | | C |
| T6. Log data alteration | | | | | I | |
| T7. Cryptographic elements modification | | | | | | I |
| T8. Denial of service | V | | V | V | V | V |
| T9. Communication compromised | | | | ICA | | |

*Table 8 - Covering of the sensitive assets by the threats*

### 3.6.2 Threats and means exploited by threatening agents

The following table presents the coverage of the means exploited in relation to the identified threats.

| | User session vulnerability | Network vulnerability | System vulnerability |
|---|---|---|---|
| T1. Session theft | √ | | |
| T2. By passing access control | √ | | |
| T3. Configuration corruption | √ | | √ |
| T4. Tokens corruption | | | √ |
| T5. Illegitimate access to the decryption key | | | √ |
| T6. Log data alteration | | √ | √ |
| T7. Cryptographic elements modification | | | √ |
| T8. Denial of service | | √ | √ |
| T9. Communication compromised | | √ | |

*Table 9 - Coverage of the means exploited in regard to the threats*

### 3.6.3 Threats and security functions

The following table back the security functions to the threats:

| | F1. Identification, authentication and users access control | F2. Communications security | F3. Cryptographic functions and random generation | F4. Logging |
|---|---|---|---|---|
| T1. Session theft | √ | √ | | |
| T2. By passing access control | √ | | | |
| T3. Configuration corruption | √ | √ | | |
| T4. Tokens corruption | √ | √ | | |
| T5. Illegitimate access to the decryption key | | | √ | |
| T6. Log data alteration | | √ | | √ |
| T7. Cryptographic elements modification | | | √ | |
| T8. Denial of service | √ | √ | √ | √ |
| T9. Communication compromised | | √ | | |

*Table 10 - Covering of the threats by the security functions*

End of document