Security view

2024-10-08

**Last modified** : 2024-10-08

**Last global review** :

**Document status** :

# Introduction

This is the security point of view. It describes all the measures implemented to prevent unauthorized use, misuse, illegitimate modification or misappropriation of application modules.

The other views of the document are accessible [from here](./README.adoc).

The project glossary is available [here](glossary.adoc). We will not redefine the functional or technical terms used here.

## Reference Documentation

Safety documentary references

| N ° | Version | Document title / URL | Detail |
| --- | --- | --- | --- |
|  |  |  |  |

# Not ruled

## Points subject to further study

Points subject to further study

| ID | Detail | Status | Subject holder | Deadline |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

## Assumptions

Assumptions

| ID | Detail |
| --- | --- |
|  |  |

# Constraints

# Requirements

## Integrity requirements

Integrity level required by data class

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data class | "Alterable" level (The data may be altered) | "Detectable" level (The data may be altered if the alteration is identified within a reasonable time) | "Controlled" level (The data may be altered, if the alteration is identified and the original data is recovered) | "Integral" level (The data must always be rigorously intact) |
|  |  |  |  |  |

## Confidentiality requirements

Level of confidentiality required by data class

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data class | “Public” level (Anyone can access the data) | Limited Level "(Data is only accessible to authorized persons) | "Reserved" level (Data can only be accessed by authorized internal staff) | Level "Private "(The data is visible only to the interested party) |
|  |  |  |  |  |

## Identification requirements

## Authentication requirements

Authentication requirement per use case

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Authentication case | Password respecting the company password policy | Known ssh public key | OTP by Token | Biometrics | Knowledge of business data | Activation email |
|  |  |  |  |  |  |  |

## Identity Federation Requirements

## SSO and SLO requirements

## Non-repudiation requirements

Non-repudiation requirements

| Signed data | Origin of the client certificate | Origin of the server certificate |
| --- | --- | --- |
|  |  |  |

## Anonymity and privacy requirements

## Authorizations requirements

## Traceability and auditability requirements

Data to be kept for proof

| Data | Objective | Retention period |
| --- | --- | --- |
|  |  |  |

# Security measures

## Integrity

Measures meeting the [Integrity requirements](#integrity-requirements) :

Measures to ensure the required level of integrity

| Data class | Required level | Measures |
| --- | --- | --- |
|  |  |  |

## Confidentiality

Measures meeting the [Confidentiality requirements](#confidentiality-requirements):

Measures to ensure the requested level of confidentiality

| Data class | Required level | Measures |
| --- | --- | --- |
|  |  |  |

## Identification

Measures meeting the [Identification requirements](#identification-requirements) :

## Authentication

Measures meeting the [Authentication requirements](#authentication-requirements):

## Identity federation

Measures meeting the [Identity Federation Requirements](#identity-federation-requirements):

## SSO, SLO

Measures meeting the [SSO and SLO requirements](#sso-requirements):

## Service accounts

Service accounts

| Account | Resource requiring authentication | How credentials are stored? |
| --- | --- | --- |
|  |  |  |

## Non-repudiation and timestamping

Measures meeting the [Non-repudiation requirements](#non-repudiation-requirements):

## Anonymity and privacy

Measures meeting the [Anonymity and privacy requirements](#privacy-requirements):

## Authorizations

Measures meeting the [Authorizations requirements](#authorization-requirements):

## Traceability, auditability

Measures meeting the [Traceability and auditability requirements](#traceability-requirements):

## Combatting Cyber Threats

### Prevention Solutions

### Detection Solutions

### Corrective Solutions

### Predictive Solutions

# RACI

* R: **Responsive** (person who will execute: she is responsible for it)
* A: **Accountable** (person who will approve the task: he is the authority)
* C: **Consulted** (person who will be consulted in the execution of the task)
* I: **Informed** (person who will be informed when the task is completed)

Management of …​

|  | Team A | Team B | Team C |
| --- | --- | --- | --- |
| …​ | R & A | C & I | A |

# Self-checks

## Self-check for vulnerabilities

Self-checking checklist to take into account common vulnerabilities

|  |  |  |
| --- | --- | --- |
| *Vulnerability* | *Taken into account?* | *Technical measures undertaken* |
|  |  |  |