Product Specification

MULTI-FACTOR AUTHENTICATION (MFA)

Current Version	1.0
File Name	Multi-factor authentication (MFA)
Requirement unique ID	Sec_Req 1
Responsible / Approver	Richard Ben Aleya
Classification	Public

Vauban project

Document Control

Version	Description	Date	Editor
1.0	Initial Version	24/07/2024	Richard Ben Aleya

Table of contents

1. Introduction 3

1.1. Introduction 3

2. Authentication methods properties 3

2.1. Authenticator Apps (OATH) 3

2.2. SMS 3

1. Introduction

1.1. Introduction

The Vauban project wants the product to implement multi-factor authentication (MFA).

2. Authentication methods properties

Hereby are the details on the MFA methods that will be supported by the product:

2.1. Authenticator Apps (OATH)

- **Description:** OATH (Initiative for Open Authentication) is a set of standards for strong authentication. Authenticator apps like Google Authenticator, Microsoft Authenticator, and Authy implement OATH standards to generate OTPs.
- **How It Works:**
  - OATH apps can generate TOTP or HOTP (HMAC-based One-Time Password) codes.
  - The user scans a QR code or enters a code provided by the service to link the app to their account.
  - After setup, the app generates temporary codes that the user must enter to log in.
- **Usage:** Used as a secondary authentication method (2FA) by many online services.
- **Advantages:**
  - Works without a network connection after initial setup.
  - More secure than SMS since codes are generated locally on the user's device.
- **Disadvantages:**
  - The user must have a smartphone or compatible device.
  - Loss or replacement of the device requires reconfiguration.
- **Security:** Authenticator apps based on OATH are considered very secure, especially when using TOTP, as they are not vulnerable to network interceptions.

2.2. SMS

- **Description:** An authentication code is sent via SMS to the user's phone number. The user must enter this code to complete the authentication process.
- **Usage:** Often used as a second factor of authentication (2FA) in addition to a password.
- **Advantages:**
  - Easy to use and deploy.
  - Any mobile phone can receive SMS, eliminating the need for additional installations.
- **Disadvantages:**
  - Vulnerable to interception attacks (such as SIM swap attacks).
  - Dependent on network coverage and mobile service providers.
- **Security:** Although convenient, SMS is considered less secure compared to other methods due to the vulnerabilities mentioned.

Vauban project