

WP-02-01

Decomposition - EUDI Wallet security  
requirements

**VERSION 1.01**

2026.06.12

/Cover page for the attached Excel spreadsheet  
WP-02-01\_Decomposition\_Sec\_req\_1.0.xlsx/

|                                                                       |                                                  |
|-----------------------------------------------------------------------|--------------------------------------------------|
| <b>Document reference</b>                                             | WP-02-01                                         |
| <b>Version</b>                                                        | 1.01                                             |
| <b>Status</b>                                                         | Final                                            |
| <b>Date</b>                                                           | 12.06.2026                                       |
| <b>Document type</b>                                                  | Product requirement security specification       |
| <b>Parent framework</b>                                               | GP-02                                            |
| <b>Scheme Owner</b>                                                   | Republic of Poland / Minister of Digital Affairs |
| <b>Certification target</b>                                           | EUDI Wallet Instance security functionality      |
| <b>Primary audience</b>                                               | EUDI Wallet Provider, PID Provider               |
| <b>Secondary audience</b>                                             | CAB-ITSEF, CAB-CB                                |
| <b>Assurance level &lt;evaluation<br/>REG (EU) 2019/881 - CSA&gt;</b> | High                                             |
| <b>Subsidiary Documents</b>                                           | WM-02-01, WM-02-02                               |

# 1 Introduction

- 1 The table presents a working summary of risks (Risks) and threats (Threats) arising from CIR 2024/2981, assigned to the decomposed Wallet Instance reference architecture at the functional module level. For each module, the corresponding security controls (Controls) according to NIST SP 800-53 Rev. 5 are indicated.
- 2 The mapping was performed based on currently available knowledge about the MVP solution and the adopted architectural decomposition. NIST SP 800-53 Rev. 5 controls were tailored to the analyzed solution by defining assignment and selection parameters. Their final completion requires additional information about the target architecture, operating environment, organizational roles, and implementation details.
- 3 It should be noted that NIST SP 800-53 Rev. 5 was developed for U.S. federal government systems and organizations. Consequently, references specific to the U.S. context are not appropriate. Government, such as organizational roles, authorization processes, the concept of an information system, or procedural requirements, should be interpreted as corresponding roles, processes, and components in the target organizational, legal, and technical model of the solution.
- 4 The table also indicates the expected coverage of individual security features by FITCEM PP requirements. This coverage is for analytical and supporting purposes. The attached spreadsheet contains a summary of the functional requirements and application notes assigned to the decomposed Wallet Instance reference architecture, at the level of functional modules and their corresponding functionalities.

## 2 Wprowadzenie

- 5 W tabeli przedstawiono zestawienie ryzyk (Risks) oraz zagrożeń (Threats) wynikających z CIR 2024/2981, przypisanych do zdekomponowanej architektury referencyjnej Wallet Instance na poziomie modułów funkcjonalnych. Dla każdego modułu wskazano odpowiadające zabezpieczenia (Controls) według NIST SP 800-53 Rev. 5.
- 6 Mapowanie zostało wykonane na podstawie aktualnie dostępnej wiedzy o rozwiązaniu MVP oraz przyjętej dekompozycji architektonicznej. Zabezpieczenia wg NIST SP 800-53 Rev. 5 zostały wstępnie dopasowane do analizowanego rozwiązania, poprzez określenie parametrów typu [assignment] oraz [selection]. Uzupełnienie można wykonać na podstawie dodatkowych informacji o docelowej architekturze, środowisku operacyjnym, rolach organizacyjnych i szczegółach wdrożenia.
- 7 Należy uwzględnić, że NIST SP 800-53 Rev. 5 został opracowany dla systemów i organizacji administracji federalnej USA. W konsekwencji, odniesienia właściwe dla kontekstu U.S. Government, takie jak role organizacyjne, procesy autoryzacyjne, pojęcie systemu informacyjnego lub wymagania proceduralne, należy interpretować jako odpowiednie role, procesy i komponenty w docelowym modelu organizacyjnym, prawnym i technicznym rozwiązania europejskiego portfela tożsamości cyfrowej.
- 8 Tabela zawiera również wskazanie przewidywanego pokrycia poszczególnych zabezpieczeń przez wymagania FITCEM PP. Pokrycie to ma charakter analityczny i uzupełniający.