

G-02

System Certyfikacji PL Portfela EUDI

Słownik

WERSJA 1.01

2026.07.07

Oznaczenie dokumentu	G-02
Wersja	1.01
Status	Final
Data	07.07.2026
Rodzaj dokumentu	Słownik
Ramy nadrzędne	brak
Właściciel programu	Rzeczpospolita Polska / Minister Cyfryzacji
Przedmiot certyfikacji	System Certyfikacji Portfela EUDI
Odbiorcy pierwotni	Wszyscy interesariusze rozwiązania Portfela EUDI (aktorzy)
Odbiorcy wtórni	Jak wyżej
Poziom uzasadnienia zaufania <potwierdzanie tożsamości, CIR 2015/1502> lub <ocena, rozporządzenie (UE) 2019/881>	Oba
Dokumenty podrzędne	GP-01, GP-02, GP-03

Historia zmian

Nr.	Zmiana	Wersja	Data
1.	Tłumaczenie wersji angielskiej	1.0	2026-07-07
2.	Zmiany edycyjne	1.01	2026-07-07

Akronimy i skróty

Akronim	Pełny termin
CA	urząd certyfikacji (Certificate Authority)
CAB	jednostka oceniająca zgodność (Conformity Assessment Body)
CAB-CB	jednostka oceniająca zgodność — jednostka certyfikująca (Certification Body)
CAB-ITSEF	jednostka oceniająca zgodność — laboratorium badawcze (ITSEF)
CP	polityka certyfikacji (Certificate Policy)
EAA	elektroniczne poświadczenie atrybutów (Electronic attestation of attributes)
FAR	współczynnik błędnych akceptacji (False accept rate)
FRR	współczynnik błędnych odrzuceń (False reject rate)
HSM	sprzętowy moduł bezpieczeństwa (Hardware security module)
IDVP	dostawca weryfikacji tożsamości (Identity verification provider)
LoA	poziom uzasadnienia zaufania (Level of Assurance)
LoA „High”	poziom uzasadnienia zaufania „wysoki” (Level of Assurance „High”)
LoA „Substantial”	poziom uzasadnienia zaufania „średni” (Level of Assurance „Substantial”)
LoIP	poziom potwierdzania tożsamości (Level of identity proofing)
MCD	deskryptor możliwości aplikacji mdoc (mdoc App capability descriptor)
MSO	mobilny obiekt bezpieczeństwa (Mobile security object)
NAB	krajowa jednostka akredytująca (National Accreditation Body)
PID	dane identyfikujące osobę (Person Identification Data)
PKI	infrastruktura klucza publicznego (Public Key Infrastructure)
QEAA	kwalifikowane elektroniczne poświadczenie atrybutów (Qualified Electronic Attestation of Attributes)
QES	kwalifikowany podpis elektroniczny (Qualified Electronic Signature)
QSCD	kwalifikowane urządzenie do składania podpisu elektronicznego (Qualified Electronic Signature Creation Device)
QTSP	kwalifikowany dostawca usług zaufania (Qualified Trust Service Provider)
SAAO	obiekt poświadczenia obszaru bezpiecznego (Secure area attestation object)
SA-Application	aplikacja obszaru bezpiecznego (Secure area application)

TOE	przedmiot oceny (Target of Evaluation)
WSCA	bezpieczna aplikacja kryptograficzna portfela (Wallet Secure Cryptographic Application)
WSCD	bezpieczne urządzenie kryptograficzne portfela (Wallet Secure Cryptographic Device)
WUA	poświadczenie jednostki portfela (Wallet Unit Attestation)
WUTA	poświadczenie zaufania jednostki portfela (Wallet Unit Trust Attestation)
WUVA	poświadczenie ważności jednostki portfela (Wallet Unit Validity Attestation)
eID means	środek identyfikacji elektronicznej (Electronic identification means)

Terminy według kategorii

Aktor (Actor)

Podmioty uczestniczące w ekosystemie Portfela EUDI

dostawca poświadczeń (Attestation Provider);

źródło autentyczne (Authentic Source);

jednostka oceniająca zgodność (Conformity Assessment Body, CAB);

jednostka oceniająca zgodność — jednostka certyfikująca (Conformity Assessment Body – Certification Body, CAB-CB);

jednostka oceniająca zgodność — laboratorium badawcze (Conformity Assessment Body – Testing Laboratory (ITSEF) (CAB-ITSEF));

producent urządzenia (Device manufacturer);

posiadacz (Holder);

dostawca weryfikacji tożsamości (Identity verification provider, IDVP);

pośrednik (Intermediary);

krajowa jednostka akredytująca (National Accreditation Bodies, NAB);

wydawca certyfikatów rejestracji (Provider of registration certificates);

wydawca certyfikatów dostępu stron ufających portfela (Provider of wallet-relying party access certificates);

podmiot sektora publicznego (Public Sector Body);

dostawca zdalnego składania kwalifikowanego podpisu elektronicznego (Qualified Electronic Signature Remote Creation Provider);

kwalifikowany dostawca usług zaufania (Qualified Trust Service Provider, QTSP);

rejestrator (Registrar);

strona ufająca (Relying Party);

użytkownik (User);

weryfikator (Verifier);

dostawca portfela (Wallet Provider);

użytkownik portfela (Wallet User)

Komponent (Component)

Techniczne komponenty architektury Portfela EUDI

złożony przedmiot oceny (Composite TOE);

sprzętowy moduł bezpieczeństwa (Hardware security module, HSM);

jednostka portfela posiadacza (Holder Wallet Unit);

magazyn kluczy (Keystore);

aplikacja mdoc (mdoc App);

kwalifikowane urządzenie do składania podpisu (Qualified signature creation device, QSCD);

instancja strony ufającej (Relying Party Instance);

przedmiot oceny (Target of Evaluation (TOE));

jednostka portfela weryfikatora (Verifier Wallet Unit);

instancja portfela (Wallet Instance);

bezpieczna aplikacja kryptograficzna portfela (Wallet Secure Cryptographic Application, WSCA);

bezpieczne urządzenie kryptograficzne portfela (Wallet Secure Cryptographic Device, WSCD);

rozwiązanie portfela (Wallet Solution);

jednostka portfela (Wallet Unit)

Poświadczenie (Credential)

Rodzaje poświadczeń

czynnik uwierzytelniania do konta (Account authentication factor);

klucz akcji (Action key);

poświadczenie (Attestation);

atrybut (Attribute);

czynnik uwierzytelniania (Authentication factor);

elektroniczne poświadczenie atrybutów (Electronic attestation of attributes, EAA);

elektroniczne poświadczenie atrybutów wydawane przez podmiot sektora publicznego lub w jego imieniu (Electronic attestation of attributes issued by or on behalf of a public sector body, PuB-EAA);

środek identyfikacji elektronicznej (eID means);

token zewnętrzny (External token);

czynnik uwierzytelniania oparty na cechach (Inherent authentication factor);

czynnik uwierzytelniania oparty na wiedzy (Knowledge-based authentication factor);

mdoc;

dane identyfikujące osobę (Person Identification Data, PID);

klucz PID (PID key);

czynnik uwierzytelniania klucza PID (PID key authentication factor);

czynnik uwierzytelniania oparty na posiadaniu (Possession-based authentication factor);

kwifikowane elektroniczne poświadczenie atrybutów (Qualified Electronic Attestation of Attributes, QEAA);

konto użytkownika (user account);

poświadczenie jednostki portfela (Wallet Unit Attestation, WUA);

poświadczenie zaufania jednostki portfela (Wallet Unit Trust Attestation, WUTA);

poświadczenie ważności jednostki portfela (Wallet Unit Validity Attestation, WUVA)

Dane (Data)

dane biograficzne (Biographical data);

współczynnik błędnych akceptacji (False accept rate, FAR);

współczynnik błędnych odrzuceń (False reject rate, FRR);

deskryptor możliwości aplikacji mdoc (mdoc App capability descriptor, MCD);

przestrzeń nazw (Namespace);

pseudonim (Pseudonym);

obiekt poświadczenia obszaru bezpiecznego (Secure area attestation object, SAAO);

podmiot (Subject)

Inne (Other)

administracyjny okres ważności (Administrative validity period);

wymaganie wyspecyfikowane (Specified requirement);

nadzorowany (Supervised);

techniczny okres ważności (Technical validity period);

nienadzorowany (Unsupervised)

Proces (Process)

Procesy i operacje w cyklu życia portfela

uwierzytelnianie (Authentication);

powiązanie (Binding);

ocena zgodności (Conformity assessment);

powiązanie kryptograficzne (Cryptographic binding);

poświadczenie urządzenia (Device attestation);

powiązanie z urządzeniem (Device binding);

system identyfikacji elektronicznej (Electronic identification scheme);

wydanie (Issuance);

notyfikacja (Notification);

onboarding (On-boarding);

parowanie (Pairing);

wydanie PID (PID issuance);

dostarczanie (Provisioning);

selektywne ujawnianie (Selective Disclosure);
silne uwierzytelnianie użytkownika (strong User authentication);
powiązanie z użytkownikiem (user binding)

Bezpieczeństwo (Security)

Pojęcia i mechanizmy związane z bezpieczeństwem

kryptografia asymetryczna (Asymmetric cryptography);
polityka certyfikacji (Certificate Policy, CP);
aktywa krytyczne (critical assets);
klucz urządzenia (Device key);
wbudowana polityka ujawniania (Embedded disclosure policy);
kwalifikowany podpis elektroniczny (Qualified Electronic Signature, QES);
kwalifikowane urządzenie do składania podpisu elektronicznego (Qualified Electronic Signature Creation Device, QSCD);
rejestr ryzyka (risk register);
pieczęć (seal);
obszar bezpieczny (Secure area);
aplikacja obszaru bezpiecznego (SA-Application);
podpis (signature);
klucz portfela (Wallet Key)

Zaufanie (Trust)

Pojęcia ram zaufania i infrastruktury

certyfikat dostępu (access certificate);
uzasadnienie zaufania — ocena (assurance, evaluation);
uzasadnienie zaufania — potwierdzanie tożsamości (assurance, identity proofing);

lista unieważnień poświadczeń (Attestation Revocation List);
zbiór zasad poświadczenia (Attestation Rulebook);
lista statusów poświadczeń (Attestation Status List);
typ poświadczenia (Attestation type);
urząd certyfikacji (Certificate Authority, CA);
poziom uzasadnienia zaufania „wysoki” (Level of Assurance "High", LoA „High”);
poziom uzasadnienia zaufania „średni” (Level of Assurance "Substantial", LoA „Substantial”);
poziom uzasadnienia zaufania (Level of Assurance, LoA);
poziom potwierdzania tożsamości (Level of identity proofing, LoIP);
infrastruktura klucza publicznego (Public Key Infrastructure, PKI);
certyfikat rejestracji (registration certificate);
poświadczenie SUA (SUA attestation);
certyfikat najwyższego poziomu (Top-level certificate);
kotwica zaufania (Trust Anchor);
ramy zaufania (Trust Framework);
zaufana lista (Trusted List);
portfel (wallet)

Słownik alfabetyczny

A

certyifikat dostępu (access certificate)

Certyfikat pieczęci elektronicznej lub podpisu elektronicznego, uwierzytelniający i walidujący stronę ufającą (w odniesieniu do portfela), wydawany przez wydawcę certyfikatów dostępu stron ufających portfela.

Kategoria: Zaufanie

Źródło: CIR 2024/2977, art. 2 pkt 12

czynnik uwierzytelniania do konta (Account authentication factor)

Czynnik uwierzytelniania umożliwiający użytkownikom portfela uwierzytelnienie się wobec dostawcy portfela i uzyskanie dostępu do swojego konta użytkownika.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.17

klucz akcji (Action key)

Klucz używany przez aplikację mdoc do zatwierdzenia jednego z jej działań, na przykład weryfikacji posiadacza poświadczenia.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.1

administracyjny okres ważności (Administrative validity period)

Data (daty), od której lub do której atrybuty zawarte w poświadczeniu są ważne, reprezentowane jako atrybut(y) w poświadczeniu.

UWAGA: niektóre poświadczenia, na przykład dyplomy, nie mają administracyjnego okresu ważności.

Kategoria: Inne

Źródło: Architecture Reference Framework (ARF), pkt 2.3

uzasadnienie zaufania (ocena) (assurance, evaluation)

Podstawy zaufania, że przedmiot oceny (TOE) spełnia funkcjonalne wymagania bezpieczeństwa.

Kategoria: Zaufanie

Źródło: EN ISO/IEC 15408-1, 3.6

uzasadnienie zaufania (potwierdzanie tożsamości) (assurance, identity proofing)

Stopień zaufania do deklarowanej lub przypisywanej tożsamości osoby.

UWAGA 1 do hasła: definicja wywiedziona z rozporządzenia (UE) nr 910/2014, art. 8.

Kategoria: Zaufanie

Źródło: rozporządzenie (UE) nr 910/2014, art. 8

kryptografia asymetryczna (Asymmetric cryptography)

System kryptograficzny wykorzystujący pary kluczy: klucze publiczne, które mogą być szeroko rozpowszechniane, oraz klucze prywatne, znane wyłącznie właścicielowi.

Kategoria: Bezpieczeństwo

Źródło: ISO/IEC 18013-5, pkt 4.1

poświadczenie (Attestation)

Jeżeli nie doprecyzowano inaczej — zbiorcze określenie QEAA, PuB-EAA lub (niekwalifikowanego) EAA.

Kategoria: Poświadczenie

Źródło: Architecture Reference Framework (ARF)

dostawca poświadczeń (Attestation Provider)

Jeżeli nie doprecyzowano inaczej — zbiorcze określenie dostawcy QEAA, dostawcy PuB-EAA lub dostawcy (niekwalifikowanych) EAA.

Kategoria: Aktor

Źródło: Architecture Reference Framework (ARF), pkt 3.6–3.8

lista unieważnień poświadczeń (Attestation Revocation List)

Mechanizm zapewniany przez dostawcę PID lub dostawcę poświadczeń (albo zaufaną stronę działającą w jego imieniu), służący do komunikowania statusu unieważnienia PID i poświadczeń poprzez publikację listy identyfikatorów unieważnionych PID lub poświadczeń.

Kategoria: Zaufanie

Źródło: Architecture Reference Framework (ARF)

zbiór zasad poświadczenia (Attestation Rulebook)

Dokument opisujący typ poświadczenia, przestrzeń (przestrzenie) nazw oraz inne cechy określonego typu poświadczenia.

Kategoria: Zaufanie

Źródło: Architecture Reference Framework (ARF)

lista statusów poświadczeń (Attestation Status List)

Mechanizm zapewniany przez dostawcę PID lub dostawcę poświadczeń (albo zaufaną stronę działającą w jego imieniu), służący do komunikowania statusu unieważnienia PID i poświadczeń poprzez publikację informacji o statusie (ważne albo nieważne) wszystkich właściwych PID lub poświadczeń.

Kategoria: Zaufanie

Źródło: Architecture Reference Framework (ARF)

typ poświadczenia (Attestation type)

Identyfikator typu poświadczenia, unikalny w kontekście ekosystemu Portfela EUDI.

Kategoria: Zaufanie

Źródło: Architecture Reference Framework (ARF)

atrybut (Attribute)

Cecha, właściwość, uprawnienie lub prawo osoby fizycznej lub prawnej albo przedmiotu.

Kategoria: Poświadczenie

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

źródło autentyczne (Authentic Source)

Repozytorium lub system, za które odpowiada podmiot sektora publicznego lub podmiot prywatny, zawierające i dostarczające atrybuty dotyczące osoby fizycznej lub prawnej albo przedmiotu, uznawane za podstawowe źródło tych informacji lub za autentyczne zgodnie z prawem Unii lub prawem krajowym, w tym z praktyką administracyjną.

Kategoria: Aktor

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

uwierzytelnianie (Authentication)

Proces elektroniczny, który umożliwia potwierdzenie identyfikacji elektronicznej osoby fizycznej lub prawnej albo potwierdzenie pochodzenia i integralności danych w postaci elektronicznej.

Kategoria: Proces

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

czynnik uwierzytelniania (Authentication factor)

Czynnik uwierzytelniania oparty na posiadaniu, czynnik uwierzytelniania oparty na wiedzy albo czynnik uwierzytelniania oparty na cechach.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.13

B

powiązanie (Binding)

Czynność lub proces zabezpieczania, przyłączania lub wiązania czegoś razem.

UWAGA 1 do hasła: może również opisywać stan bycia zobowiązanym.

UWAGA 2 do hasła: powiązanie to logiczne połączenie ustanowione między co najmniej dwoma elementami. Elementami tymi mogą być dane, osoba lub podmiot. Powiązanie może zachodzić na przykład między danymi a wydawcą, danymi a osobą, danymi a urządzeniem albo osobą a urządzeniem.

Kategoria: Proces

Źródło: CEN TS 18098, pkt 3.3

dane biograficzne (Biographical data)

Spersonalizowane dane posiadacza dokumentu, występujące jako tekst w strefie wizualnej i strefie odczytu maszynowego MRTD lub w chipie, jeżeli jest obecny.

Kategoria: Dane

Źródło: CEN TS 18098, pkt 3.4

C

urząd certyfikacji (Certificate Authority, CA)

Podmiot, któremu co najmniej jedna strona w ekosystemie Portfela EUDI ufa w zakresie tworzenia i pieczętowania certyfikatów.

Kategoria: Zaufanie

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0), pkt 3.18

polityka certyfikacji (Certificate Policy, CP)

Nazwany zbiór zasad wskazujący zastosowanie certyfikatu w określonej społeczności i/lub klasie zastosowań o wspólnych wymaganiach bezpieczeństwa.

Kategoria: Bezpieczeństwo

Źródło: Architecture Reference Framework (ARF), pkt 6

złożony przedmiot oceny (Composite TOE)

Część produktu złożonego podlegająca ocenie złożonego TOE.

UWAGA 1 do hasła: złożony TOE może zawierać części niezależne odpowiednio od komponentu bazowego lub bazowego TOE. Dla uproszczenia części takie uznaje się za należące do komponentu zależnego.

UWAGA 2 do hasła: ocenę złożonego TOE można stosować tyle razy, ile jest to konieczne, do produktu wielokomponentowego, w podejściu przyrostowym.

Kategoria: Komponent

Źródło: EN 17640:2022+A1:2026, 3.22

ocena zgodności (Conformity assessment)

Wykazanie, że wyspecyfikowane wymagania zostały spełnione.

Kategoria: Proces

Źródło: CEN TS 18098, pkt 3.5

jednostka oceniająca zgodność (Conformity Assessment Body, CAB)

Jednostka oceniająca zgodność w rozumieniu art. 2 pkt 13 rozporządzenia (WE) nr 765/2008, akredytowana zgodnie z tym rozporządzeniem jako właściwa do przeprowadzania oceny zgodności.

Kategoria: Aktor

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0), art. 2 pkt 13

Odesłania prawne: art. 2 rozporządzenia (WE) nr 765/2008

jednostka oceniająca zgodność — jednostka certyfikująca (Conformity Assessment Body – Certification Body (CAB-CB))

Zewnętrzna jednostka oceniająca zgodność wydająca oraz zarządzająca certyfikatami.

Kategoria: Aktor

Źródło: EN ISO/IEC 17065, 3.12

jednostka oceniająca zgodność — laboratorium badawcze (Conformity Assessment Body – Testing Laboratory (ITSEF) (CAB-ITSEF))

Jednostka oceniająca zgodność wykonująca działania badawcze lub oceny.

Kategoria: Aktor

Źródło: na podstawie PN-EN ISO/IEC 17025, 3.6

aktywa krytyczne (critical assets)

Aktywa w ramach jednostki portfela lub w odniesieniu do niej, o tak nadzwyczajnym znaczeniu, że naruszenie ich dostępności, poufności lub integralności miałyoby bardzo poważny, paraliżujący wpływ na możliwość polegania na jednostce portfela.

Kategoria: Bezpieczeństwo

Źródło: CIR 2024/2977, art. 2 pkt 10

powiązanie kryptograficzne (Cryptographic binding)

Powiązanie co najmniej dwóch powiązanych ze sobą elementów informacji z użyciem technik kryptograficznych.

Kategoria: Proces

Źródło: CEN TS 18098, pkt 3.8

D

poświadczenie urządzenia (Device attestation)

Dowód wykazujący, że producent urządzenia ręczy za bezpieczeństwo i wiarygodność urządzenia oraz dostarcza szczegóły techniczne o funkcjach urządzenia.

Kategoria: Proces

Źródło: CEN TS 18098, pkt 3.9

powiązanie z urządzeniem (Device binding)

Właściwość polegająca na tym, że poświadczenie jest powiązane z określonym urządzeniem (np. WSCD) i nie może być używane niezależnie od tego urządzenia.

UWAGA 1 do hasła: powiązanie z urządzeniem chroni poświadczenie przed kopiowaniem lub klonowaniem, co zwiększa jego bezpieczeństwo. Dostawca PID lub dostawca poświadczeń realizuje powiązanie z urządzeniem, umieszczając w poświadczeniu kryptograficzny klucz publiczny i podpisując je. Odpowiadający mu klucz prywatny jest chroniony przez certyfikowane WSCD używane przez jednostkę portfela.

UWAGA 2 do hasła: powiązanie z urządzeniem jest rodzajem powiązania kryptograficznego, w którym klucz tajny jest bezpiecznie przechowywany w urządzeniu.

Kategoria: Proces

Źródło: CEN TS 18098, pkt 3.10

klucz urządzenia (Device key)

Klucz uwierzytelniania mdoc.

Kategoria: Bezpieczeństwo
Źródło: CEN TS 18098, pkt 3.11

producent urządzenia (Device manufacturer)

Producent urządzenia, na którym zainstalowane jest rozwiązanie portfela.

UWAGA 1 do hasła: może to być producent urządzenia mobilnego, producent systemu operacyjnego (OS) lub sprzętu (OEM) albo producent komputera.

Kategoria: Aktor
Źródło: CEN TS 18098, pkt 3.12

E

elektroniczne poświadczenie atrybutów (Electronic attestation of attributes, EAA)

Poświadczenie w postaci elektronicznej, które umożliwia uwierzytelnienie atrybutów.

Kategoria: Poświadczenie
Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

elektroniczne poświadczenie atrybutów wydawane przez podmiot sektora publicznego lub w jego imieniu (Electronic attestation of attributes issued by or on behalf of a public sector body, PuB-EAA)

Elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne albo przez podmiot sektora publicznego wyznaczony przez państwo członkowskie do wydawania takich poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne, zgodnie z art. 45f i załącznikiem VII.

Kategoria: Poświadczenie
Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0), załącznik VII, art. 45f
Inaczej: PuB-EAA

środek identyfikacji elektronicznej (Electronic identification means, eID means)

Materialna lub niematerialna jednostka zawierająca dane identyfikujące osobę, używana do uwierzytelniania na potrzeby usługi online lub, w stosownych przypadkach, usługi offline.

UWAGA 1 do hasła: definicja zaczerpnięta z art. 3 eIDAS.

Kategoria: Poświadczenie
Źródło: CEN TS 18098, pkt 3.22

system identyfikacji elektronicznej (Electronic identification scheme)

System identyfikacji elektronicznej, w ramach którego środki identyfikacji elektronicznej wydaje się osobom fizycznym lub prawnym albo osobom fizycznym reprezentującym inne osoby fizyczne lub osoby prawne.

Kategoria: Proces
Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

wbudowana polityka ujawniania (Embedded disclosure policy)

Zbiór zasad, wbudowany w elektroniczne poświadczenie atrybutów przez jego dostawcę, wskazujący warunki, które strona ufająca portfela musi spełnić, aby uzyskać dostęp do tego elektronicznego poświadczenia atrybutów.

Kategoria: Bezpieczeństwo

Źródło: CIR 2024/2979, art. 2 pkt 9

token zewnętrzny (External token)

Nośnik danych identyfikujących osobę (PID) lub kluczy kryptograficznych, umożliwiający w niektórych scenariuszach proces onboarding z zapewnieniem poziomu bezpieczeństwa „wysoki” lub równoważnego.

UWAGA 1 do hasła: „równoważny” oznacza przypadki, w których rozwiązanie jest zapewniane na poziomie bezpieczeństwa eIDAS „wysoki” wraz z innymi środkami podnoszącymi je do poziomu równoważnego poziomowi bezpieczeństwa eIDAS „wysoki”.

UWAGA 2 do hasła: zgodnie z definicją podaną w Architecture and Reference Framework token zewnętrzny jest lokalnym zewnętrznym bezpiecznym urządzeniem kryptograficznym portfela (Local External WSCD).

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.23

F

współczynnik błędnych akceptacji (False accept rate, FAR)

Odsetek transakcji weryfikacji z fałszywymi deklaracjami biometrycznymi, które zostały błędnie zaakceptowane.

Kategoria: Dane

Źródło: CEN TS 18098, pkt 3.24

współczynnik błędnych odrzuceń (False reject rate, FRR)

Odsetek transakcji weryfikacji z prawdziwymi deklaracjami biometrycznymi, które zostały błędnie odrzucone.

Kategoria: Dane

Źródło: CEN TS 18098, pkt 3.25

H

sprzętowy moduł bezpieczeństwa (Hardware security module, HSM)

Fizyczne urządzenie obliczeniowe zapewniające odporne na manipulacje i włamania (z ewidencjonowaniem naruszeń) zabezpieczanie kluczy cyfrowych i innych sekretów oraz zarządzanie nimi, a także przetwarzanie kryptograficzne.

Kategoria: Komponent

Źródło: CEN TS 18098, pkt 3.26

posiadacz (Holder)

Użytkownik, który chce użyć swojej jednostki portfela do zaprezentowania atrybutów z PID lub poświadczenia użytkownikowi innej jednostki portfela.

Uwaga: patrz także: weryfikator.

Kategoria: Aktor

Źródło: Architecture Reference Framework (ARF)

jednostka portfela posiadacza (Holder Wallet Unit)

Jednostka portfela używana przez posiadacza.

Kategoria: Komponent

Źródło: Architecture Reference Framework (ARF), pkt 3.2

I

dostawca weryfikacji tożsamości (Identity verification provider, IDVP)

Podmiot przeprowadzający weryfikację tożsamości osoby (lub jej część) z użyciem dokumentu tożsamości.

Kategoria: Aktor

Źródło: CEN TS 18098, pkt 3.27

czynnik uwierzytelniania oparty na cechach (Inherent authentication factor)

Czynnik potwierdzony jako powiązany z osobą, oparty na fizycznej cesze osoby fizycznej w odniesieniu, do którego podmiot musi wykazać, że tę fizyczną cechę posiada.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.16

pośrednik (Intermediary)

Strona ufająca oferująca innym stronom ufającym usługi polegające na łączeniu się w ich imieniu z jednostkami portfela i żądaniu atrybutów użytkownika, których te inne strony ufające potrzebują.

Kategoria: Aktor

Źródło: Architecture Reference Framework (ARF)

wydanie (Issuance)

Proces wydania i ewentualnie dostarczania.

UWAGA 1 do hasła: termin odnosi się do poświadczenia i oznacza jego utworzenie przez organ oraz ewentualne dostarczenie. Obejmuje sformatowanie danych i ich podpisanie z użyciem mechanizmu kryptograficznego w celu uzyskania poświadczenia.

Kategoria: Proces

Źródło: CEN TS 18098, pkt 3.28

K

magazyn kluczy (Keystore)

Wspierane sprzętowo repozytorium i usługa, w których niekrytyczne aktywa kryptograficzne są generowane, przechowywane i używane wyłącznie wewnątrz dedykowanej sprzętowej granicy bezpieczeństwa.

Uwagi: przykłady obejmują Secure Element, TPM, TEE lub bezpieczną enklawę albo zdalny HSM. Krytyczne aktywa kryptograficzne są generowane, przechowywane i używane w WSCA/WSCD.

Kategoria: Komponent

Źródło: Architecture Reference Framework (ARF), pkt 4.3.2

czynnik uwierzytelniania oparty na wiedzy (Knowledge-based authentication factor)

Czynnik potwierdzony jako powiązany z osobą w odniesieniu, do którego podmiot musi wykazać jego znajomość.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.15

L

poziom uzasadnienia zaufania „wysoki” (Level of Assurance „High”, LoA „High”)

Poziom zapewniający wyższy stopień zaufania do deklarowanej lub przypisywanej tożsamości osoby niż środki identyfikacji elektronicznej o poziomie uzasadnienia zaufania „średni”, którego celem jest zapobieżenie nadużyciu tożsamości lub jej zmianie.

UWAGA 1 do hasła: definicja inspirowana art. 8 ust. 2 lit. c eIDAS.

Kategoria: Zaufanie

Źródło: CEN TS 18098, pkt 3.30

poziom uzasadnienia zaufania „średni” (Level of Assurance „Substantial”, LoA „Substantial”)

Poziom zapewniający średni stopień zaufania do deklarowanej lub przypisywanej tożsamości osoby, którego celem jest znaczne zmniejszenie ryzyka nadużycia tożsamości lub jej zmiany.

UWAGA 1 do hasła: definicja inspirowana art. 8 ust. 2 lit. b eIDAS.

Kategoria: Zaufanie

Źródło: CEN TS 18098, pkt 3.31

poziom bezpieczeństwa (Level of Assurance, LoA)

Poziom uzasadnienia zaufania dotyczący wiarygodności i jakości: (1) rejestracji, (2) zarządzania środkami identyfikacji elektronicznej, (3) uwierzytelniania, (4) zarządzania i organizacji.

UWAGA 1 do hasła: definicja zaczerpnięta z art. 8 eIDAS.

Kategoria: Zaufanie

Źródło: CEN TS 18098, pkt 3.29

poziom potwierdzania tożsamości (Level of identity proofing, LoIP)

Pewność osiągnięta w potwierdzaniu tożsamości.

Kategoria: Zaufanie

Źródło: CEN TS 18098, pkt 3.32

M

mdoc (mdoc)

Poświadczenie sformatowane zgodnie z ISO/IEC 18013-5:2021.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.33

aplikacja mdoc (mdoc App)

Aplikacja na urządzeniu mobilnym, która zarządza atrybutami i poświadczeniami użytkownika do celów identyfikacji elektronicznej oraz kontroluje dostęp do atrybutów i poświadczeń użytkownika, niezależnie od tego, czy atrybuty i poświadczenia użytkownika są przechowywane na urządzeniu mobilnym, na serwerze, czy na urządzeniu zewnętrznym.

UWAGA 1 do hasła: w kontekście niniejszego dokumentu aplikacja mdoc odpowiada instancji portfela (a nie jednostce portfela).

Kategoria: Komponent

Źródło: CEN TS 18098, pkt 3.34

deskryptor możliwości aplikacji mdoc (mdoc App capability descriptor, MCD)

Zbiór danych opisujący możliwości aplikacji mdoc, obejmujący co najmniej jeden obiekt poświadczenia obszaru bezpiecznego.

Kategoria: Dane

Źródło: CEN TS 18098, pkt 3.35

mobilny obiekt bezpieczeństwa (Mobile security object, MSO)

Obiekt w rozumieniu ISO/IEC 18013-5:2021, § 9.1.2.3.

Źródło: CEN TS 18098, pkt 3.36

N

przestrzeń nazw (Namespace)

Specyfikacja identyfikatora atrybutu oraz składni i semantyki atrybutów, które mogą być użyte w poświadczeniu, mająca identyfikator unikalny w kontekście ekosystemu Portfela EUDI.

Kategoria: Dane

Źródło: Architecture Reference Framework (ARF)

krajowa jednostka akredytująca (National Accreditation Body, NAB)

Jednostka wykonująca akredytację na mocy upoważnienia państwa członkowskiego na podstawie rozporządzenia (WE) nr 765/2008.

Kategoria: Aktor

Źródło: Architecture Reference Framework (ARF), pkt 3.16

Odesłania prawne: rozporządzenie (WE) nr 765/2008

notyfikacja (Notification)

Czynność przekazania informacji do Komisji Europejskiej.

Kategoria: Proces

Źródło: Architecture Reference Framework (ARF)

O

onboarding (On-boarding)

Proces, w którym pełny zbiór danych identyfikujących osobę (PID), wydanych zgodnie z prawem Unii lub prawem krajowym, jest przypisywany do jednostki portfela, która nie zawiera jeszcze PID albo zawiera PID nieważne (unieważnione lub wygasłe), w sposób zapewniający jego powiązanie (1) z użytkownikiem tej jednostki portfela oraz (2) z urządzeniem, na którym jednostka portfela została zainstalowana.

UWAGA 1 do hasła: W szczególności, onboarding obejmuje (1) instalację aplikacji klienckich i oprogramowania na urządzeniu użytkownika (zależnie od architektury może to być cała instancja portfela) oraz (2) aktywację portfela.

UWAGA 2 do hasła: dane identyfikujące osobę (PID) definiuje art. 3 pkt 3 eIDAS, doprecyzowany aktem wykonawczym.

Kategoria: Proces

Źródło: CEN TS 18098, pkt 3.37

P

parowanie (Pairing)

Proces ustanowienia początkowego połączenia między urządzeniami albo między urządzeniem a osobą fizyczną w celu umożliwienia interakcji między nimi.

Kategoria: Proces

Źródło: CEN TS 18098, pkt 3.38

dane identyfikujące osobę (Person Identification Data, PID)

Zestaw danych wydawanych zgodnie z prawem Unii lub prawem krajowym, umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej albo osoby fizycznej reprezentującej inną osobę fizyczną lub osobę prawną.

Kategoria: Poświadczenie

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

wydanie PID (PID issuance)

Proces wydania danych identyfikujących osobę (PID) użytkownikowi jednostki portfela i zapisania tych danych w jednostce portfela.

UWAGA 1 do hasła: zbiór danych identyfikujących osobę w rozumieniu art. 3 pkt 3 eIDAS, doprecyzowany aktem wykonawczym, nie jest wydawany, ponieważ są to dane niezmiennie, przypisane osobie prawnej lub fizycznej zgodnie z prawem krajowym. Wydawane są efemeryczne reprezentacje tych danych, w postaci jednego lub kilku poświadczeń, które następnie są zapisywane w jednostce portfela. Te efemeryczne reprezentacje (poświadczenia) również są wydawane i zapisywane zgodnie z prawem krajowym.

Kategoria: Proces

Źródło: CEN TS 18098, pkt 3.40

klucz PID (PID key)

Klucz kryptograficzny umożliwiający portfelowi wykonywanie operacji bezpieczeństwa, poręczony przez dostawcę PID.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.41

czynnik uwierzytelniania klucza PID (PID key authentication factor)

Czynnik uwierzytelniania umożliwiający użytkownikowi portfela uwierzytelnienie się wobec jednostki portfela i uzyskanie dostępu do klucza PID.

UWAGA 1 do hasła: ten czynnik uwierzytelniania pozwala użytkownikowi portfela używać kluczy PID.

UWAGA 2 do hasła: czynnik uwierzytelniania klucza PID może być różny dla każdego klucza PID (jeżeli jest ich kilka) albo ten sam.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.19

czynnik uwierzytelniania oparty na posiadaniu (Possession-based authentication factor)

Czynnik potwierdzony jako powiązany z osobą w odniesieniu, do którego podmiot musi wykazać jego posiadanie.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.14

wydawca certyfikatów rejestracji (Provider of registration certificates)

Osoba fizyczna lub prawna upoważniona przez państwo członkowskie do wydawania certyfikatów rejestracji (stron ufających portfela) stronom ufającym (portfela) zarejestrowanym w tym państwie członkowskim.

Kategoria: Aktor

Źródło: CIR 2024/2982, art. 2 pkt 15

wydawca certyfikatów dostępu stron ufających portfela (Provider of wallet-relying party access certificates)

Osoba fizyczna lub prawna upoważniona przez państwo członkowskie do wydawania certyfikatów dostępu strony ufającej lub stronom ufającym (w odniesieniu do portfela), zarejestrowanym w tym państwie członkowskim.

Kategoria: Aktor

Źródło: CIR 2024/2982

Inaczej: Access CA, urząd certyfikacji dostępu (Access Certificate Authority)

dostarczanie (Provisioning)

Załadowanie i przechowanie.

UWAGA 1 do hasła: termin odnosi się do poświadczenia.

UWAGA 2 do hasła: dostarczenie poświadczenia nie obejmuje jego wydania.

Kategoria: Proces

Źródło: CEN TS 18098, pkt 3.43

pseudonim (Pseudonym)

Dane jednoznacznie reprezentujące użytkownika, które same w sobie nie pozwalają wywnioskować atrybutów użytkownika ani danych identyfikujących osobę bez użycia dodatkowych informacji, przechowywanych oddzielnie przez wydawcę danych, jednoznacznie reprezentujących użytkownika.

Kategoria: Dane

Źródło: Architecture Reference Framework (ARF)

infrastruktura klucza publicznego (Public Key Infrastructure, PKI)

Systemy, oprogramowanie i protokoły komunikacyjne używane przez komponenty ekosystemu Portfela EUDI do dystrybucji kluczy publicznych, zarządzania nimi i ich sterowania. PKI publikuje klucze publiczne i ustanawia zaufanie w środowisku poprzez walidację i weryfikację przyporządkowania kluczy publicznych do podmiotów.

Kategoria: Zaufanie

Źródło: Architecture Reference Framework (ARF), pkt 6

podmiot sektora publicznego (Public Sector Body)

Organ państwowy, regionalny lub lokalny, podmiot prawa publicznego lub stowarzyszenie utworzone przez co najmniej jeden taki organ lub co najmniej jeden taki podmiot prawa publicznego, lub podmiot prywatny upoważniony przez co najmniej jeden z tych organów, podmiotów lub stowarzyszeń do świadczenia usług publicznych, działający na podstawie takiego upoważnienia.

Kategoria: Aktor

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

Q

kwalikowane elektroniczne poświadczenie atrybutów (Qualified Electronic Attestation of Attributes, QEAA)

Elektroniczne poświadczenie atrybutów wydawane przez kwalifikowanego dostawcę usług zaufania i spełniające wymagania określone w załączniku V rozporządzenie eIDAS 2.0

Kategoria: Poświadczenie

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0), załącznik V

kwalikowany podpis elektroniczny (Qualified Electronic Signature, QES)

Zaawansowany podpis elektroniczny składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego, weryfikowany za pomocą kwalifikowanego certyfikatu podpisu elektronicznego.

Kategoria: Bezpieczeństwo

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

kwalikowane urządzenie do składania podpisu elektronicznego (Qualified Electronic Signature Creation Device, QSCD)

Skonfigurowane oprogramowanie lub skonfigurowany sprzęt używane do składania podpisu elektronicznego, spełniające wymagania określone w załączniku II rozporządzenia eIDAS 2.0.

Kategoria: Bezpieczeństwo

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0), załącznik II

Terminy powiązane: kwalifikowany podpis elektroniczny

dostawca usługi zdalnego składania kwalifikowanego podpisu elektronicznego (Qualified Electronic Signature Remote Creation Provider)

Osoba fizyczna lub prawna oferująca usługi związane ze zdalnym składaniem, walidacją i zarządzaniem kwalifikowanymi podpisami elektronicznymi, spełniające wymogi prawne i standardy określone w rozporządzeniu eIDAS 2.0, tak aby były uznawane za prawnie równoważne podpisom własnoręcznym.

Kategoria: Aktor

Źródło: Architecture Reference Framework (ARF), pkt 3.9

kwalikowane urządzenie do składania podpisu (Qualified signature creation device, QSCD)

Urządzenie do składania podpisu elektronicznego, które składa podpis kwalifikowany.

UWAGA 1 do hasła: mające zastosowanie wymagania określa załącznik II eIDAS.

UWAGA 2 do hasła: definicja zaczerpnięta z art. 3 eIDAS.

Kategoria: Komponent

Źródło: CEN TS 18098, pkt 3.45

kwalfikowany dostawca usług zaufania (Qualified Trust Service Provider, QTSP)

Dostawca usług zaufania, który świadczy co najmniej jedną kwalifikowaną usługę zaufania i któremu organ nadzoru nadał status kwalifikowanego.

Kategoria: Aktor

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

R

rejestrator (Registrar)

Organ wyznaczony przez państwo członkowskie, odpowiedzialny za ustanowienie i prowadzenie wykazu zarejestrowanych stron ufających portfela, mających siedzibę na terytorium państwa członkowskiego.

Kategoria: Aktor

Źródło: CIR 2024/2982, art. 2 pkt 16

certyfikat rejestracji (registration certificate)

Obiekt danych wskazujący atrybuty, w odniesieniu do których strona ufająca zarejestrowała zamiar występowania do użytkowników.

Kategoria: Zaufanie

Źródło: CIR 2024/2982, art. 2 pkt 14

strona ufająca (Relying Party)

Strona ufająca, która zamierza polegać na jednostkach portfela przy świadczeniu usług publicznych lub prywatnych w drodze interakcji cyfrowej.

Kategoria: Aktor

Źródło: CIR 2024/2977, art. 2 pkt 11

instancja strony ufającej (Relying Party Instance)

Moduł programowy i/lub sprzętowy zdolny do interakcji z jednostką portfela i wykonywania uwierzytelnienia strony ufającej, kontrolowany przez stronę ufającą.

Kategoria: Komponent

Źródło: Architecture Reference Framework (ARF), pkt 3.11.2

rejestr ryzyka (risk register)

Zapis informacji o zidentyfikowanych ryzykach, istotnych dla procesu certyfikacji.

Kategoria: Bezpieczeństwo

Źródło: rozporządzenie wykonawcze Komisji (UE) 2024/2981, art. 2 pkt 7

S

pieczęć (seal)

Dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, tak aby zapewnić ich pochodzenie i integralność.

Kategoria: Bezpieczeństwo

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

obszar bezpieczny (Secure area)

Wyodrębniony wewnętrzny lub dołączony obszar urządzenia mobilnego, zapewniający bezpieczne przetwarzanie i przechowywanie danych nawet w przypadku naruszenia głównego systemu operacyjnego (OS).

Kategoria: Bezpieczeństwo

Źródło: CEN TS 18098, pkt 3.47

aplikacja obszaru bezpiecznego (Secure area application, SA-Application)

Aplikacja obszaru bezpiecznego, która zarządza poświadczeniami i może zarządzać atrybutami użytkownika do celów identyfikacji użytkownika oraz może kontrolować dostęp do atrybutów użytkownika.

Kategoria: Bezpieczeństwo

Źródło: CEN TS 18098, pkt 3.48

obiekt poświadczenia obszaru bezpiecznego (Secure area attestation object, SAAO)

Zbiór danych opisujący możliwości aplikacji obszaru bezpiecznego (SA-Application).

Kategoria: Dane

Źródło: CEN TS 18098, pkt 3.49

selektywne ujawnianie (Selective Disclosure)

Zdolność umożliwiająca użytkownikowi zaprezentowanie podzbioru atrybutów zawartych w PID lub poświadczeniu.

Kategoria: Proces

Źródło: Architecture Reference Framework (ARF), pkt 2.3

podpis (signature)

Dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, których podpisujący używa do podpisania.

Kategoria: Bezpieczeństwo

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

wymaganie wyspecyfikowane (Specified requirement)

Potrzeba lub oczekiwanie, które zostało określone.

Kategoria: Inne

Źródło: CEN TS 18098, pkt 3.51

silne uwierzytelnianie użytkownika (strong User authentication)

Uwierzytelnianie oparte na wykorzystaniu co najmniej dwóch czynników uwierzytelniania z różnych kategorii: wiedzy (coś, co wie wyłącznie użytkownik), posiadania (coś, co posiada wyłącznie użytkownik) lub cech (coś, czym jest użytkownik), które są od siebie niezależne w tym sensie, że naruszenie jednego z nich nie podważa

wiarygodności pozostałych, i które jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających.

Kategoria: Proces

Źródło: rozporządzenie w sprawie europejskiej tożsamości cyfrowej (eIDAS 2.0)

poświadczenie SUA (SUA attestation)

Poświadczenie używane do silnego uwierzytelniania użytkownika w kontekście płatności elektronicznych, takie że gdy strona ufająca wysyła do jednostki portfela żądanie prezentacji tego poświadczenia, to zawiera w żądaniu dane transakcyjne.

Kategoria: Zaufanie

Źródło: Architecture Reference Framework (ARF)

podmiot (Subject)

Podmiot, z którym powiązane są dane identyfikujące osobę (PID).

UWAGA 1 do hasła: podmiot obejmuje osobę fizyczną, osobę prawną albo osobę fizyczną reprezentującą osobę fizyczną lub prawną zgodnie z eIDAS. Na przykład rodzic („użytkownik”) może posiadać PID swojego dziecka („podmiotu”).

Kategoria: Dane

Źródło: CEN TS 18098, pkt 3.52

nadzorowany (Supervised)

Obserwowany i/lub kierowany przez człowieka, który ma odpowiednie umiejętności i został przeszkolony w celu wyeliminowania ryzyka oszustw.

Kategoria: Inne

Źródło: CEN TS 18098, pkt 3.53

T

przedmiot oceny (Target of Evaluation, TOE)

Zestaw oprogramowania, oprogramowania układowego (firmware), sprzętu lub ich kombinacji, ewentualnie wraz z dokumentacją użytkową (guidance), będący przedmiotem oceny.

Kategoria: Komponent

Źródło: EN ISO/IEC 15408-1, 3.93

techniczny okres ważności (Technical validity period)

Daty (i ewentualnie godziny), od której i do której poświadczenie jest ważne, reprezentowane jako metadane poświadczenia.

UWAGA: wszystkie PID i poświadczenia mają techniczny okres ważności, który jest zwykle znacznie krótszy niż administracyjny okres ważności (jeżeli taki istnieje). Techniczny okres ważności dobiera się na podstawie analizy ryzyka, np. ze względu na prywatność użytkownika.

Kategoria: Inne

Źródło: Architecture Reference Framework (ARF), pkt 2.3

certyfi­kat naj­wyż­szego po­zio­mu (Top-level certificate)

Deklaracja zgodności składana do Komisji Europejskiej i EUDICG zgodnie z art. 5d ust. 1 rozporządzenia (UE) 910/2014, oparta na zbiorze certyfi­katów wynikających z realizacji wszystkich właściwych programów certyfikacji w ramach Systemu Certyfikacji PL Portfela EUDI.

Kategoria: Zaufanie

Źródło: rozporządzenie (UE) 910/2014, art. 5d ust. 1

ko­twi­ca zaufania (Trust Anchor)

Autorytatywny podmiot reprezentowany przez klucz publiczny i powiązane dane.

Uwaga: na podstawie RFC 5914.

Kategoria: Zaufanie

Źródło: Architecture Reference Framework (ARF), pkt 6

ra­my zaufania (Trust Framework)

Zbiór zasad, norm i wymogów prawnych określających, w jaki sposób tożsamości cyfrowe mogą być bezpiecznie tworzone, weryfikowane i udostępniane między różnymi interesariuszami ekosystemu Portfela EUDI.

Kategoria: Zaufanie

Źródło: Architecture Reference Framework (ARF)

zaufana lista (Trusted List)

Repozytorium informacji o autorytatywnych podmiotach w określonym kontekście prawnym lub umownym, dostarczające informacji o ich bieżącym i historycznym statusie.

Kategoria: Zaufanie

Źródło: Architecture Reference Framework (ARF), pkt 3.5

U

nienadzorowany (Unsupervised)

Niebędący nadzorowanym.

Kategoria: Inne

Źródło: CEN TS 18098, pkt 3.54

użytkownik (User)

Osoba fizyczna lub prawna albo osoba fizyczna reprezentująca inną osobę fizyczną lub osobę prawną, korzystająca z usług zaufania lub środków identyfikacji elektronicznej zapewnianych zgodnie z rozporządzeniem eIDAS 2.0.

Kategoria: Aktor

Źródło: Architecture Reference Framework (ARF)

konto użytkownika (user account)

Konto u dostawcy portfela umożliwiające użytkownikowi portfela zlecenie dostawcy portfela wykonywania w jego imieniu operacji zarządzania jego jednostką portfela, po pomyślnym uwierzytelnieniu z użyciem czynnika (czynników) uwierzytelniania do konta.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.55

powiązanie z użytkownikiem (user binding)

Właściwość polegająca na tym, że PID lub poświadczenia — to znaczy dane osoby fizycznej lub prawnej zawarte w PID lub poświadczeniu — pozostają pod kontrolą osoby, która prezentuje PID lub poświadczenie stronie ufającej.

Kategoria: Proces

Źródło: CEN TS 18098, pkt 3.56

V

weryfikator (Verifier)

Użytkownik, który chce użyć swojej jednostki portfela do zażądania atrybutów z PID lub poświadczenia od użytkownika innej jednostki portfela.

Kategoria: Aktor

Źródło: Architecture Reference Framework (ARF)

jednostka portfela weryfikatora (Verifier Wallet Unit)

Jednostka portfela używana przez weryfikatora.

Kategoria: Komponent

Źródło: Architecture Reference Framework (ARF), pkt 3.2

W

portfel (wallet)

Środek identyfikacji elektronicznej umożliwiający użytkownikowi bezpieczne przechowywanie danych identyfikujących osobę i elektronicznych poświadczeń atrybutów, zarządzanie nimi i ich walidację.

Kategoria: Zaufanie

Źródło: CEN TS 18098, pkt 3.57

Inaczej: portfel EUDI (EUDI wallet)

instancja portfela (Wallet Instance)

Aplikacja zainstalowana i skonfigurowana na urządzeniu lub w środowisku użytkownika portfela, stanowiąca część jednostki portfela, której użytkownik portfela używa do interakcji z jednostką portfela.

Kategoria: Komponent

Źródło: CIR 2024/2977, art. 2 pkt 6

klucz portfela (Wallet Key)

Klucz kryptograficzny umożliwiający jednostce portfela wykonywanie operacji bezpieczeństwa, poręczony przez dostawcę portfela.

Kategoria: Bezpieczeństwo

Źródło: CEN TS 18098, pkt 3.59

dostawca portfela (Wallet Provider)

Osoba fizyczna lub prawna, która dostarcza rozwiązania portfela.

Kategoria: Aktor

Źródło: CIR 2024/2979, art. 2 pkt 9

bezpieczna aplikacja kryptograficzna portfela (Wallet Secure Cryptographic Application, WSCA)

Aplikacja zarządzająca aktywami krytycznymi, powiązana z bezpiecznym urządzeniem kryptograficznym portfela i wykorzystująca zapewniane przez nie funkcje kryptograficzne i niekryptograficzne.

Kategoria: Komponent

Źródło: CIR 2024/2977, art. 2 pkt 7

bezpieczne urządzenie kryptograficzne portfela (Wallet Secure Cryptographic Device, WSCD)

Urządzenie odporne na manipulacje, zapewniające środowisko powiązane z bezpieczną aplikacją kryptograficzną portfela i przez nią wykorzystywane w celu ochrony aktywów krytycznych oraz zapewnienia funkcji kryptograficznych do bezpiecznego wykonywania operacji krytycznych.

Kategoria: Komponent

Źródło: CIR 2024/2977, art. 2 pkt 8

rozwiązanie portfela (Wallet Solution)

Kombinacja oprogramowania, sprzętu, usług, ustawień i konfiguracji, obejmująca instancje portfela, co najmniej jedną bezpieczną aplikację kryptograficzną portfela i co najmniej jedno bezpieczne urządzenie kryptograficzne portfela.

Kategoria: Komponent

Źródło: CIR 2024/2977

jednostka portfela (Wallet Unit)

Unikalna konfiguracja rozwiązania portfela, obejmująca instancje portfela, bezpieczne aplikacje kryptograficzne portfela i bezpieczne urządzenia kryptograficzne portfela, dostarczana przez dostawcę portfela indywidualnemu użytkownikowi portfela.

Kategoria: Komponent

Źródło: CIR 2024/2977, art. 2 pkt 2

poświadczenie jednostki portfela (Wallet Unit Attestation, WUA)

Obiekt danych opisujący komponenty jednostki portfela albo umożliwiający uwierzytelnienie i walidację tych komponentów.

Kategoria: Poświadczenie

Źródło: CIR 2024/2977, art. 2 pkt 5

poświadczenie zaufania jednostki portfela (Wallet Unit Trust Attestation, WUTA)

Poświadczenie opisujące właściwości rozwiązania portfela, instancji portfela, urządzenia, na którym jest ona zainstalowana, oraz WSCD.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.66

poświadczenie ważności jednostki portfela (Wallet Unit Validity Attestation, WUVA)

Poświadczenie identyfikujące instancję portfela, wykazujące, że dostawca portfela ręczy za jej bezpieczeństwo.

Kategoria: Poświadczenie

Źródło: CEN TS 18098, pkt 3.67

użytkownik portfela (Wallet User)

Osoba fizyczna sprawująca kontrolę nad jednostką portfela.

Kategoria: Aktor

Źródło: CEN TS 18098, pkt 3.68