SLOVENSKI STANDARD
kSIST-TS FprCEN/TS 18297:2026

01-december-2026

Nadzor dostopa, delovanje in upravljanje sredstev v denarnici EUDI

EUDI Wallet Held Assets Access Control, Operation and Management

EUDI Wallet Held Assets Zugangskontrolle, Betrieb und Verwaltung

Sample Document

Ta slovenski standard je istoveten z: **FprCEN/TS 18297**

---

get full document from standards.iteh.ai

ICS:

33.040.01	Telekomunikacijski sistemi na splošno	Telecommunication systems in general

kSIST-TS FprCEN/TS 18297:2026 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

Sample Document

get full document from standards.iteh.ai

kSIST-TS FprCEN/TS 18297:2026

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

FINAL DRAFT
FprCEN/TS 18297

October 2026

ICS

English Version

EUDI Wallet Held Assets Access Control, Operation and Management

EUDI Wallet Held Assets Zugangskontrolle, Betrieb und Verwaltung

This draft Technical Specification is submitted to CEN members for Vote. It has been drawn up by the Technical Committee CEN/TC 224.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Sample Document

Warning : This document is not a Technical Specification. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a Technical Specification.

get full document from standards.iteh.ai



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

© 2026 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. FprCEN/TS 18297:2026 E

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

kSIST-TS FprCEN/TS 18297:2026

Contents

Page

European foreword 4
Introduction 5
1 Scope 6
2 Normative references 6
3 Terms and definitions 7
4 Conformance claim (Normative) 14
4.1 Applicability of this document 14
4.2 Items subject to conformance 14
4.3 Applicable requirements 14
5 Data Model 15
5.1 General 15
5.2 Wallet Held Access Control Metadata 16
5.2.1 Overview 16
5.2.2 Policies 16
5.2.3 Instructions 20
5.2.4 Data organization 21
5.2.5 Metadata mapping and reference to existing structures (informative) 21
5.3 Relying Party Request (RP Request) 22
5.3.1 Overview 22
5.3.2 Relying Party Authentication 22
5.3.3 Relying Party Authorizations (RP Authorizations) 23
5.3.4 Processing Information Notice 24
5.3.5 Wallet User Authentication 25
5.3.6 Relying Party Request data structures 25
5.3.7 Relying Party Request Content and Security Control 25
5.4 Aspects which are out of scope 26
5.5 Considerations relating to the various privacy approaches for presentation of Wallet Held Asset(s) 27
6 Access Control Model 27
6.1 General 27
6.2 Wallet Held Asset (WHA) 27
6.3 Access Control Model to WHAs 28
6.3.1 General 28
6.3.2 Relying Party access control over WHA 29
6.3.3 User access control over WHA 38
7 Wallet access control operational requirements 46
7.1 General 46
7.2 Metadata management 48
7.2.1 CTRL-MTDMG 48
7.3 RP operations access control 50
7.3.1 Wallet access control decision 50
7.3.2 Wallet user decision 65
7.3.3 Wallet response 72
7.4 User operations access control 76
7.4.1 General 76
7.4.2 User operations overview 76
7.4.3 Wallet Unit processing 78
7.4.4 Return the final decision 80
7.4.5 Execute user operation 80
7.5 Log Management and User Control 85
7.5.1 General 85
7.5.2 CTRL-ULOGD: Log deletion 86
7.5.3 CTRL-LOG: Log retention and audit 87

Sample Document
get full document from standards.iteh.ai

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

kSIST-TS FprCEN/TS 18297:2026

Annex A (informative) Mapping with the eIDAS regulation [1] 88

Annex B (informative) Risk Analysis Matrix 89

Annex C (informative) Embedded Disclosure Policy Implementation Example 91
C.1 General 91
C.2 Action Logic Scripts 91
C.3 Examples of coding 94
C.3.1 General 94
C.3.2 Example of WACE action logic in C language validating CBOR formatted request input 95
C.3.3 Rust Example of WACE action logic validating JSON formatted request input 97
C.3.4 Rust Example of WACE action logic validating CBOR formatted request input 100
C.3.5 Referencing WACE action logic bytecode from within credentials 103

Annex D (informative) Wallet User Notifications 105
D.1 General 105
D.2 Relationship to Clause 7 requirements 105
D.3 Notifications for RP operations over WHAs 105
D.4 Notifications for User Access Control operations 108
D.5 Language and localisation considerations 109
D.6 Domain-specific notification content 110
D.7 Presentation of detailed reasons for access not granted recommended 110
D.8 Reporting to supervisory authority 110
D.9 Withdrawal of consent 111
D.10 Transaction log recording of notification details 111

Bibliography 112

Sample Document

get full document from standards.iteh.ai

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

European foreword

This document (FprCEN/TS 18297:2026) has been prepared by Technical Committee CEN/TC 224, "Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment", the secretariat of which is held by AFNOR.

This document is currently submitted to the Vote on TS.

Sample Document

get full document from standards.iteh.ai

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

kSIST-TS FprCEN/TS 18297:2026

Introduction

The eIDAS regulation [1] as amended establishes a common framework for European Digital Identities. A central new feature is the European Digital Identity Wallet (EUDI Wallet or Wallet) which can be used to manage various wallet held asset(s) or WHA(s). These WHAs are personal data (as per [2]) relating to the Wallet User, which can be presented and managed by the Wallet User through the Wallet.

WHAs encompass(es) various types of data and includes (but is not limited to):

— attribute(s) relating to the Wallet User (e.g. PID;

— electronic attestation(s) of attributes of any type including with embedded disclosure policies: non qualified electronic attestation(s) of attributes, qualified electronic attestation(s) of attributes or EAAs issued by or on behalf of a public sector body responsible for an authentic source;

— attribute(s) or electronic attestation(s) of attributes relating to the wallet unit;

— transactions log keeping track of the access to the personal data stored in the wallet unit;

— public keys, associated certificates, and key attestations (e.g. proof of association) supporting cryptographic binding and trust establishment;

NOTE 1 Depending on implementation, Wallet Held Assets (WHAs) can be stored, processed, or accessed by the wallet unit from locations other than the user's local device. This includes scenarios where the wallet unit operates in a cloud-based environment on behalf of the Wallet User. This architectural flexibility allows for broader scalability, device independence, and policy enforcement, and it applies not only to transaction logs but to all types of WHAs.

Sample Document

Important aspects of the Wallet are privacy, transparency and security. Security and privacy imply that the Wallet implements access control before carrying out any operation on WHAs (presentation, view, update, deletion). For instance, privacy could be compromised by revealing WHAs to Relying Parties who are not allowed to handle them (e.g. under GDPR [2]). Transparency on the other hand implies that the Wallet User (1) is empowered with accepting or refusing the fulfilment of any operation on WHAs and (2) makes informed decision regarding the fulfilment of any operation on WHAs when such decision is deferred to them.

Access control for the various operations possible on WHAs is needed, namely:

— presentation of one or several WHAs under request of a relying party;

— management of one or several WHAs by the Wallet User through theirwallet unit (view, update, deletion, backup to and restoration from the wallet provider back end);

— access to one or several WHAs by a relying party (e.g. presentation, revocation).

This access control relies on a wallet access control decision engine (WACE) which is a dedicated sub component of a wallet unit verifying whether the access can be granted before the wallet unit can process the operation.

The WACE ensures the Wallet User (1) is empowered with accepting or refusing the fulfilment of the operation on WHAs and (2) makes wallet access control decision engine regarding the fulfilment of the operation on WHAs when such decision is deferred to them.

When the operation on WHAs involves a relying party (presentation or management of WHAs), the WACE also outputs a notification to the relying party containing the decision regarding the fulfilment of the operation on WHAs. That decision can be that the access is granted, refused, or granted provided the relying party meets some supplemental conditions;

NOTE 2 In addition to issuers and QTSP/TSP, other parties interacting with the wallet can deliver credentials or attestations that the user may want to host on their wallet. Access control is needed for the WACE to manage such operations when e.g. these assets are updated, deleted, etc.

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

kSIST-TS FprCEN/TS 18297:2026

1 Scope

This document specifies the functionality of the wallet unit for Access Control to Wallet Held Assets (WHAs), i.e. personal data relating to the Wallet User and stored in the wallet unit. It defines the wallet access control decision engine (WACE) and the corresponding functional requirements, resulting in recommendations to the user on decision to be made.

This document aims at:

1) describing and specifying an access control model supporting access control to the various possible operations on WHAs;

2) providing the definitions and classification of the various types of data and metadata, and supporting access control to the various possible operations on WHAs;

3) describing and specifying a WACE controlling the access to the various possible operations on WHAs and the notification returned by the wallet access control decision engine to a wallet unit;

4) identifying requirements applicable to the wallet access control decision engine.

This document also:

— identifies technical specifications and standards that can be used to support the concepts described herein;

— specifies additional requirements for the use of the identified specifications to meet the above objectives;

— provides the missing technical specifications needed to meet the above objectives where needed;

— provides examples and use cases.

Sample Document
get full document from standards.iteh.ai

The access control model and wallet access control decision engine defined in this document aim to comply with the requirements regarding access control laid down in eIDAS [1]. Nevertheless, this document is applicable to any wallet unit , even those which do not claim compliance with eIDAS [1].

The following areas are out of the scope of this document:

5) content and encoding of the policies assigned for the disclosure of WHAs,

6) implementation choice and encoding of wallet held access control metadata;

7) encoding of electronic attestation(s) of attributes which are in the remit of ETSI/TC ESI.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ETSI TS 119 472-3, *Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 3: Profiles for issuance of EAA or PID*

ETSI TS 119 475 V1.2.1:2026, *Electronic Signatures and Trust Infrastructures (ESI); Relying party attributes supporting EUDI Wallet user's authorization decisions*

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

kSIST-TS FprCEN/TS 18297:2026

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at http://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

3.1
access control model
conceptual framework that defines the processes, roles, data structures, and decision logic governing how access to *wallet held asset* (3.25)(s) (*WHAs* (3.25)) is granted, denied, or made conditional within a *wallet unit* (3.32)

Note 1 to entry: An access control model describes the steps and components required to evaluate access requests to *WHAs* (3.25), including the role of the *wallet access control decision engine* (3.23) (WACE), relevant policies, *metadata* (3.8), *relying party* (3.16) requests, and user decisions.

Note 2 to entry: This document defines an access control model applicable to operations involving both relying parties and the Wallet User, covering actions such as presentation, update, deletion, and management of *WHAs* (3.25).

3.2
attribute
authorization, quality, right or permission of a natural or legal person or of an object

Sample Document

Note 1 to entry: This includes also attribute from the *PID* (3.10) set (each individual items from the *PID* (3.10)) as defined in eIDAS regulation [1].

Note 2 to entry: This definition is drawn from [1].

get full document from standards.iteh.ai

3.3
authentic source
repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognized as authentic in accordance with Union or national law, including administrative practice

Note 1 to entry: Authentic Sources are sources for attributes on, for instance, address, age, gender, civil status, family composition, nationality, education and training qualifications titles and licences, professional qualifications titles and licences, public permits and licences, or financial and company data. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/

3.4
credential
evidence or testimonials that support a claim of identity or assertion of an *attribute* (3.2) and usually are intended to be used more than once

[SOURCE: Committee on National Security Systems, CNSSI No. 400Ctrl9, Committee on National Security Systems (CNSS) Glossary, April 6, 2015. Unclassified.]

3.5
certificate policy
named set of rules that defines the applicability of a certificate to a particular community or class of applications with shared security requirements

Note 1 to entry: A certificate policy is used to indicate the level of assurance, scope of usage, and expected trustworthiness of a certificate issued within a specific trust framework.

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

kSIST-TS FprCEN/TS 18297:2026

Note 2 to entry: Certificate policies are defined and maintained by certificate authorities and trust service providers. They can be referenced in certificate extensions and interpreted by relying parties to inform authorization decisions.

Note 3 to entry: Certificate policies are specified in ETSI EN 319 411-1 [3] and ETSI EN 319 411- 2 [4], which defines requirements for trust service providers issuing qualified and non-qualified certificates.

3.6
electronic attestation of attributess
EAA
EAAs
attestation in electronic form that allows the authentication of attributes

Note 1 to entry: This definition is drawn from [1] Article 3.

3.7
embedded disclosure policy
set of rules, embedded in an EAAs by its provider, that indicates the conditions that a Wallet *relying party* (3.16) has to meet to access the EAAs

Note 1 to entry: This definition is drawn from the draft implementing regulation taken for implementation of Article 5a(23) of eIDAS Regulation [1].

3.8
metadata
data that provides information about attributes, but not the content of the *attribute* (3.2)

[SOURCE: Wikipedia - https://en.wikipedia.org/wiki/Metadata#cite_note-1]

Sample Document

3.9
personal data
information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Note 1 to entry: In this document, personal data are typically represented as Wallet Held Assets (WHAs) managed by the Wallet User and may be subject to selective disclosure, access control, and transaction logging.

Note 2 to entry: In this document, PII is often represented as Wallet Held Assets (*WHAs* (3.25)) managed by the Wallet User, and may be subject to selective disclosure, access control, and transaction logging.

[SOURCE: Regulation (EU) 2016/679, Article 4(1) [5]]

3.10
person identification data
PID
credential (3.4), (1) containing the set of person identification data, (2) demonstrating that the *PID provider* (3.11) vouches for their integrity and authenticity and their binding with the *wallet unit* (3.32) and the User, and (3) that is verifiable

Note 1 to entry: This definition is drawn from the CIR (EU) 2024/2979 [6].

Note 2 to entry: Within this document, person identification data (PID) designates a *credential* (3.4) containing one or several data from the person identification data as described by eIDAS Article 3(3) and further refined by the implementing act . This definition differs from the meaning of person identification data (PID) as provided for in eIDAS Article 3(3) and further refined by the implementing act, which designates the set of data comprising person identification data.

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

kSIST-TS FprCEN/TS 18297:2026

Note 3 to entry: Person identification data (PID) is a technical representation of one or several data from the person identification data (PID) as defined by eIDAS Article 3(3) and further refined by the implementing act. PID can be of different formats (e.g. SD-JWT or MSO with mdoc as per ISO/IEC 18013-5:2021 [7]).

Note 4 to entry: Throughout this document there is not differentiation between the person identification data (PID) of a natural person or the one of a legal person.

3.11
PID provider
natural or legal person responsible for issuing and revoking the person identification data and ensuring that the person identification data of a user is cryptographically bound to a wallet unit

Note 1 to entry: This definition is drawn from the CIR (EU) 2024/2979 [6].

Note 2 to entry: The PID provider is the entity responsible for (1) ensuring *PID* (3.10) uniquely represents a person (natural or legal) and (2) issuing the *PID* (3.10) (s) into the *wallet unit* (3.32) of a Wallet User authorized to present the *PID* (3.10) of that person.

[SOURCE: CEN/TS 18098:2026 [8]]

3.12
processing information notice
data elements from the *RP Request* (3.20) that specifies purpose, retention period and other elements that assist the user to make an informed decision to grant access or deny access to the wallet held assets (*WHA* (3.25))

Note 1 to entry: Processing information notice may be encoded in natural language or machine readable language (ex ISO/IEC TS 27560:2023 [9]).

[SOURCE: ISO/IEC TS 27560:2023 [9]]

Sample Document
t full document from standards.iteh.ai

3.13
public issued EAA
EAAs (*EAAs* (3.6)) issued by a public sector body that is responsible for an *authentic source* (3.3) or by a public sector body that is designated by the Member State to issue such attestations of Attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45f and with Annex VII of [1]

Note 1 to entry: eIDAS Article 3(3) defines “person identification data” as “set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person”.

Note 2 to entry: With in this document, PID is a technical representation of one or several data from the person identification data (PID) as defined by eIDAS Article 3(3). Therefore, for the same set of person identification data as defined by eIDAS Article 3(3), there may be one or several PID(s), each being characterized for instance by (1) its format (e.g. MSO with mdoc as per ISO/IEC 18013-5:2021 [7]), (2) the number and combination of person identification data as defined by eIDAS Article 3(3) it contains, or (3) the granularity of the information (e.g. year of birth, month of birth, etc.). The set of person identification data as defined by eIDAS Article 3(3) may be contained in a single credential, or scattered across several credentials.

Note 3 to entry: Throughout this document there is not differentiation between the person identification data (PID) of a natural person or the one of a legal person.

3.14
qualified certificate
qualified certificate for electronic signature, qualified certificate for electronic seal or qualified certificate for website authentication (QWAC).

Note 1 to entry: These types of certificates are defined in eIDAS Regulation [1].

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

kSIST-TS FprCEN/TS 18297:2026

3.15
qualified electronic attestation of attributes
QEAA
QEAAs
EAAs, which is issued by a qualified trust service provider and meets the requirements laid down in [1] Annex V

Note 1 to entry: This definition is drawn from [1] Article 3.

3.16
relying party
RP
RPs
external entity that interacts with the Wallet Unit to request and receive, or perform operations on Wallet Held Assets (WHAs), based on access control policies and metadata

Note 1 to entry: A Relying Party may act in different roles, including as a verifier, credential issuer, or a trusted service provider. Regardless of role, all such entities are subject to the same access control enforcement process defined in this specification.

Note 2 to entry: This definition is drawn from [1] Article 3.

Note 3 to entry: This definition expands on the narrower use of "Relying Party" in ETSI TS 119 475 V1.2.1:2026 [10], which assumes a verifying role. In the context of Wallet Access Control, issuers and service providers may also operate as Relying Parties when accessing WHAs or invoking Wallet-controlled operations.

3.17
relying party access to special WHAs category
situation in which a Relying Party requests access to Wallet Held Assets (WHAs) that include or relate to special categories of personal data (see 3.17), which may require enhanced protection measures according to applicable policy or regulation

Standards Document
get full document from standards.iteh.ai

Note 1 to entry: Such requests can require enhanced Wallet User authentication, selective disclosure, or issuer-enforced policies (e.g. Embedded Disclosure Policies) before access is granted.

Note 2 to entry: Examples of special category WHAs include health-related data, biometric identifiers, or personal information associated with increased privacy or security risk when not properly protected.

Note 3 to entry: The designation of special category WHAs is determined by the data issuer or attribute provider through Wallet Held Access Control Metadata or other configured policies. The Wallet does not inherently classify services as critical or sensitive.

3.18
relying party authentication
means by which a Relying Party proves its identity to the Wallet Unit using an **Access Certificate** as defined by applicable regulation (e.g. CIR (EU) 2024/2979 [6])

Note 1 to entry: The Wallet User retains the ability to control whether a Relying Party Request is accepted, depending on how the Wallet evaluates the authentication outcome.

Note 2 to entry: The Access Certificate enables the Wallet Unit to authenticate the origin of a Relying Party Request before allowing access to Wallet Held Assets (WHAs).

Note 3 to entry: The Access Certificate typically contains information such as the RP identifier, domain, and in some implementations, the session or specific request is cryptographically bound to the certificate authority chain.

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

kSIST-TS FprCEN/TS 18297:2026

3.19
relying party authorizations
RP Authorizations
attributes of a Relying Party which characterize the very nature of the Relying Party

Note 1 to entry: RP Authorizations encompass various information, such as its identification, its role, its entitlements, its sector, the identification of its certification authority, etc.

Note 2 to entry: RP Characteristics may according to ETSI TS 119 475 V1.2.1:2026 [10] be role or other attributes.

3.20
relying party request
RP Request
message sent from the Relying Party to the Wallet Unit which includes a request to access WHAs

3.21
sensitive personal data
special categories of personal data that require enhanced protection due to their sensitive nature, as defined in Article 9(1) of the GDPR

Note 1 to entry: These include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, or data concerning a natural person's sex life or sexual orientation.

Note 2 to entry: In this document, such data may be classified as Wallet Held Assets (WHAs) subject to stricter access control and disclosure limitations. Such classification is up to WHA's provider and depends on their policy and jurisdictional context. Accordingly, the designation of personal data as sensitive may be reflected in associated metadata or policy requiring enhanced protection measures.

[SOURCE: GDPR Article 9(1)]

Sample Document
get full document from standards.iteh.ai

3.22
critical service
service (aka critical) provided by a Relying Party of which the consequence incurred by the wallet user may be severe or harmful in case of impersonation attack, and thus requiring strong authentication and user binding of the presented credentials

Note 1 to entry: Metadata configured by their issuer(s) indicates that some assets are subject to highest care (security, privacy) before being disclosed. It depends on (1) the attribute, (2) the RP domain or authorizations or registration attestation, (3) the transaction purpose, (4) the risk incurred by the user in case of misuse of such data. A standard cannot define what "sensitive personal data" are but the issuer can do ; it is part of metadata configuration (see example given in Annex C).

3.23
wallet access control decision engine
WACE
component of the Wallet Unit in charge of processing the access control request to an operation on a WHA

Note 1 to entry: An access control decision engine ensures the Wallet User is empowered with accepting or refusing the fulfilment of the operation on WHAs and makes an informed decision regarding the fulfilment of the operation on WHAs when such a decision is deferred to them.

3.24
wallet held access control metadata
access control metadata that may be locally stored or dynamically retrieved and that features the policies fir access control to WHAs

Note 1 to entry: Wallet held access control metadata is also known as wallet held metadata in this document.

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

kSIST-TS FprCEN/TS 18297:2026

3.25
wallet held asset
WHA
WHAs
personal data relating to the Wallet User and stored in the Wallet Unit

Note 1 to entry: WHAs encompass(es) various types of data and includes but is not limited to:
— attribute(s) relating to the Wallet User (e.g. PID);
— electronic attestation(s) of attributes of any type including with embedded disclosure policies: Non-qualified electronic attestation(s) of attributes, qualified electronic attestation(s) of attributes or EAAs issued by or on behalf of a public sector body responsible for an authentic source;
— attribute(s) or electronic attestation(s) of attributes relating to the Wallet Unit;
— transactions log keeping track of the access to the personal data stored in the Wallet Unit;
--- pseudonym;
— keys and certificates.

Note 2 to entry: Pseudonyms can be generated/renewed with some randomization whereby they are dynamic assets that might not be part of WHAs as they are computed on-demand within the wallet.

3.26
wallet held asset policy manager
entity responsible for defining, managing, or updating access control–relevant policies and metadata associated with a WHA, including but not limited to embedded disclosure policies (EDP)

Note 1 to entry: Access control–relevant policies may include disclosure conditions, usage constraints, assurance requirements, pricing conditions, or other issuer-defined restrictions associated with a WHA.

3.27
wallet held metadata management interface
interface exposed by the Wallet Unit and/or the WACE through which authorized parties (WHA Providers, Wallet Provider, authenticated Wallet User) may perform lifecycle operations on wallet held access control metadata, namely provisioning, updating, deleting and reading

Sample Document
get full document from standards.iteh.ai

3.28
wallet unit attestation
WUA
WUAs
data object that describes the components of the wallet unit or allows authentication and validation of those components

Note 1 to entry: This definition is drawn from the CIR (EU) 2024/2979 [6].

Note 2 to entry: A Wallet Unit Attestation is a credential identifying a Wallet Unit, demonstrating that the Wallet Provider vouches for the (1) security, (2) trustworthiness of that Wallet Unit and (3) the binding between that Wallet Unit and the User, and that is verifiable.

Note 3 to entry: ETSI TS 119 476-3 [11] further specifies the Wallet Unit Attestation as comprising one Wallet Instance Attestation (WIA), attesting the integrity and authenticity of the wallet instance, and one or more Wallet Key Attestations (WKA), attesting properties of cryptographic keys stored in the Wallet Unit's key storage. The Wallet Unit Attestation is a device-and-key security attestation, not a user identity credential."

3.29
wallet provider
natural or legal person who provides wallet solutions

Note 1 to entry: This definition is drawn from the CIR (EU) 2024/2979 [6].

Note 2 to entry: The wallet provider is the entity that is responsible for provisioning and managing one or more Wallet Solution and Wallet..

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026

kSIST-TS FprCEN/TS 18297:2026

3.30
wallet solution
combination of software, hardware, services, settings, and configurations, including wallet instances, one or more wallet secure cryptographic applications (WSCA) and one or more wallet secure cryptographic devices (WSCD)

Note 1 to entry: This definition is drawn from the CIR (EU) 2024/2979 [6].

3.31
wallet unit trust attestation
WUTA
credential (1) describing the properties - including the security properties - of the Wallet Solution, the Wallet Instance, the device on which it is installed and the WSCD, (2) containing the information allowing to cryptographically bind PID and attestation of any kind to the Wallet Unit, (3) for which the Wallet Provider vouches and (4) which is verifiable

Note 1 to entry: A Wallet Unit Trust Attestation (WUTA) is a Credential.

Note 2 to entry: The Wallet Unit Trust Attestation (WUTA) is a part of the Wallet Unit Attestation (WUA).

Note 3 to entry: The WUTA forms part of the WIA component of the WUA as decomposed in ETSI TS 119 476-3 [11](subject to confirmation once ETSI TS 119 476-3 [11] is stable).

[SOURCE: CEN/TS 18098:2026 [8]]

3.32
wallet unit
unique configuration of a wallet solution that includes wallet instances, wallet secure cryptographic applications and wallet secure cryptographic devices provided by a wallet provider to an individual wallet user

Sample Document

Note 1 to entry: This definition is drawn from the CIR (EU) 2024/2979 [6].

Get full document from standards.iteh.ai

Note 2 to entry: A Wallet Unit includes any installed software which is part of an EUDI Wallet Solution, whether it is installed on the User's device or on a server.

Note 3 to entry: In the case part of the Wallet Solution is installed on a server, despite there will be a single installation on the server, each User will be associated to a unique configuration (containing its credentials, keys, etc.) which then consists as the corresponding part of the Wallet Unit.

3.33
(wallet) user
natural person who is in control of the wallet unit

Note 1 to entry: In the context of this document, the User is the User of the Wallet Unit and is only one allowed to use the PID(s) contained in the Wallet Unit. It may [RA1] not necessarily be the PID's Subject.

Note 2 to entry: The User is the one allowed to use the PID(s) contained in the Wallet Unit. It is not necessarily the PID's Subject.

[SOURCE: CEN/TS 18098:2026 [8]]

3.34
wallet user authentication
process by which the Wallet User proves their identity to the Wallet Unit, using one or more authentication factors (e.g. PIN, biometrics, possession of device), in order to authorize access to Wallet Held Assets (WHAs)

Note 1 to entry: This process supports user approval, prevents impersonation, and can include generation of cryptographic proof for binding the user to the WHAs.

Note 2 to entry: The Wallet Unit can enforce different assurance levels depending on the nature of the requested WHAs, the Relying Party request, or policies defined in Wallet Held Metadata.

kSIST-TS FprCEN/TS 18297:2026 • https://standards.iteh.ai/catalog/standards/sist/545f0fa3-105c-4bc9-b51a-d1166e8c7794/ksist-ts-fprcen-ts-18297-2026