Identyum ID Wallet Practice Statement

OID: 1.3.6.1.4.1.65996.4.2.1.1

Effective Date: 24.08.2026 **Document Owner**: Identyum **Approved by**: Director of Identyum **Public Repository**: https://identyum.com/terms-policies/	**Service Provider**: Identity Consortium d.o.o. **Registered Office**: Trogirska ulica 2, 42000 Varaždin, Croatia **Court Register Number (MBS)**: 070166678 **Personal Identification Number (OIB)**: 44867795324 **General Contact**: info@identyum.com **Customer Support**: support@identyum.com

ROBERT ILIJAŠ

Digitally signed by ROBERT ILIJAŠ
Date: 2026.08.25 23:15:36 +02'00'

CHANGE HISTORY

VERSION	DATE OF CHANGE	AUTHOR	DESCRIPTION OF CHANGES
1.0	17.07.2025.	R. Ilijaš	Initial version
2.0	24.08.2026.	R. Ilijaš	Complete version aligned with the Identyum canonical model for the separation of the Wallet, the Identify service, Identyum PID, authentication and related trust services.

Version 2.0 is issued as a complete replacement version. Consequently, amendments are not individually highlighted in YELLOW as usual.

TABLE OF CONTENTS

1. General Information

1.1. Purpose of the Document

This Identyum ID Wallet Practice Statement (hereinafter: the Practice Statement) describes the practices applied by Identity Consortium d.o.o. (hereinafter: Identyum) in providing, operating, protecting and managing the lifecycle of the Identyum ID Wallet service.

Its purpose is to provide Users, Relying Parties, Business Clients, auditors, assessors and competent authorities with a transparent and verifiable description of the Wallet service, without equating the Wallet with identity proofing, person identification data, electronic identification means, certificates or remote signing services.

In particular, this Practice Statement describes:

a) the creation and use of an ID Wallet without stored identification data;
b) the optional initiation or continuation of the Identify service from the Wallet, and the receipt, linking, storage and presentation of the Identyum PID issued by Identify;
c) the establishment and management of Wallet authentication factors;
d) authentication and authorisation through the Wallet, including pseudonymous authentication without an assertion of the person's verified identity;
e) the controlled presentation of PID attributes to Relying Parties;
f) interfaces between the Wallet, the Identyum Identify service and trust services;
g) separate lifecycles for the Wallet, PID, authentication factors, certificates and cryptographic keys; and
h) security, evidence, governance, privacy and user-information practices applicable to the Wallet service.

1.2. Normative Status

This Practice Statement is Identyum's public statement of the operational, organisational, security and lifecycle practices applicable to the ID Wallet. It is approved by the Director of Identyum and is binding on Identyum insofar as it describes practices that Identyum undertakes to implement.

The document is structured with regard to the four areas set out in Commission Implementing Regulation (EU) 2015/1502 for the assurance of electronic identification: enrolment, electronic identification means management, authentication, and management and organisation. Such structural alignment does not in itself constitute a claim that the ID Wallet or any related credential has been notified, certified or formally assigned an eIDAS assurance level.

Unless expressly stated otherwise, publication of this Practice Statement does not constitute a claim that the ID Wallet is a European Digital Identity Wallet, that it has been issued under a

notified national electronic identification scheme, or that it meets the requirements of the Low, Substantial or High assurance level. The canonical and authoritative version of this Practice Statement is the Croatian-language version. Any translation into English or another language is for information purposes only; in the event of any discrepancy, the Croatian text shall prevail.

1.3. Scope

This Practice Statement applies to the ID Wallet service provided directly by Identyum to natural persons. A Wallet may be created and remain active without an Identyum PID or other verified person-identity data. Such a Wallet provides an authentication and authorisation context, but its mere existence does not constitute an electronic identification means or establish the verified identity of a person.

The scope covers the Wallet account, its verified contact identifier, authentication factors, supported interfaces, Wallet content, User instructions, interactions with Relying Parties, lifecycle events and records required for the operation and evidencing of those functions.

Where the Wallet is used to submit a request for, activate or authorise a related trust service, this Practice Statement governs the interaction on the Wallet side. The lifecycles of the certificate, private key, remote QSCD and trust service remain governed by the applicable CP, TSPS, Disclosure Statement and Terms and Conditions.

1.4. Matters Outside the Scope

The following matters are outside the primary scope of this Practice Statement:

i) the complete operation of the Identyum Identify service and the Business Client's final decision on onboarding, KYC, AML or granting access;
j) detailed identity-proofing mechanisms, biometric thresholds and evidentiary controls governed by the TSPS and controlled internal documentation;
k) certificate policies, certificate profiles, policy OIDs and complete certificate lifecycles;
l) the management and certified configuration of remote QSCD or QSealCD services;
m) the creation and validation of electronic signatures or seals, except for User interaction on the Wallet side;
n) qualified electronic time stamps;
o) electronic identification of legal persons and the lifecycle of QLSeal certificates;
p) the definition and operation of the COL-C and COL-D Identify mechanisms and the definition of separate Identyum SMS, WEB, MOBILE, NIAS or C2G credentials, except for their expressly described interface with the Wallet; and
q) European Digital Identity Wallet functions that are not expressly identified as part of Identyum's service.

1.5. Target Audience

This Practice Statement is intended for:

a) natural persons who use or intend to use the Identyum ID Wallet;
b) Relying Parties that accept authentication, PID or other data presented through the ID Wallet;
c) Business Clients that integrate the ID Wallet as an authentication or identity-reuse option within the Identyum Identify service;
d) trust service providers and other service providers that use the ID Wallet in connection with their services;
e) auditors, conformity assessment bodies and independent assessors;
f) supervisory, regulatory and other competent authorities;
g) Identyum personnel responsible for the management, security, operation and support of the ID Wallet service; and
h) external suppliers whose services materially support the ID Wallet.

The Practice Statement is a technical and normative service document. It is not intended to replace user instructions, accessibility guidance, contextual notices, consent screens or customer-support materials.

1.6. Documentation Framework and Resolution of Inconsistencies

The documentation through which Identyum governs the Wallet and related services consists of interconnected public and internal documents. Each document applies primarily to the matters assigned to it according to its purpose and scope; no single linear hierarchy is established for matters governed by different documents at different levels.

The documentation framework comprises: (1) Identyum Trust Services Policies and Profiles (CP), which define policies, profiles, OIDs, permitted uses and the meaning of profiles; (2) the Identyum Trust Services Practice Statement (TSPS), which governs the organisational, procedural, security and technical practices of trust services and constitutes the CPS in its Chapter 11; (3) this Wallet Practice Statement, as the primary document governing the creation, use and lifecycle of the Wallet, authentication and authorisation through the Wallet, and the storage, linking, display, presentation and removal of PID on the Wallet side; (4) the Terms and Conditions and Disclosure Statements, which govern contractual relationships, rights, obligations, use restrictions, liability and complaints; and (5) controlled internal documentation detailing implementation procedures, architecture, configurations and evidence.

For identity proofing, PID issuance, determination of LoIP and identity-proofing use cases, the TSPS shall prevail where Identify is used in the context of a trust service, and the relevant

controlled Identify documentation shall prevail in other contexts. For certificates, keys, signatures, seals and the remote QSCD, the CP, TSPS/CPS, applicable profile, Disclosure Statement and terms of the service concerned shall prevail. This Practice Statement remains authoritative for actions and effects on the Wallet side. If an inconsistency is identified, applicable legislation and binding regulatory requirements shall take precedence; the inconsistency shall be assessed according to the subject matter and functional scope of each document; pending alignment, no interpretation shall be applied that would reduce the required security, assurance level, qualified status or user rights; and the documentation shall be aligned through the controlled change-management process.

1.7. Applicable Legislation, Standards and Guidelines

1.7.1. European Union and Croatian Legislation

The principal regulatory framework comprises Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, Regulation (EU) 2016/679, applicable cybersecurity legislation and Croatian legislation implementing or supplementing those acts.

Commission Implementing Regulation (EU) 2015/1502 is used as the primary reference for the assurance structure of enrolment, electronic identification means management, authentication, and management and organisation. Requirements specific to European Digital Identity Wallets, including Commission Implementing Regulation (EU) 2024/2979, are used only as non-status-conferring design guidance where Identyum expressly adopts an aligned principle.

1.7.2. Standards and Technical Specifications

ETSI TS 119 461 applies to Identify identity-proofing procedures within the scope and use cases identified in the applicable TSPS where Identyum, as a TSP, performs such proofing itself; it does not apply to the creation of an empty Wallet as such. ETSI EN 319 401 and ETSI EN 319 411-1/-2 apply to related trust services in accordance with the CP and TSPS. ETSI TS 119 431-1 applies to the policy and security requirements of remote signing/SSAS, including SAD and evidence of sole control, and not to general Wallet authentication. ETSI TS 119 472-2 and ETSI TR 119 462 are relevant to the EUDI/EAA context and do not turn Identyum's product-specific PID into an EUDI PID. ISO/IEC 27001, ISO/IEC 27002, relevant biometric standards and EN 301 549 apply within the scope established by the management system, technical design and regulatory obligations.

A reference to a standard does not mean that every provision applies to every Wallet function. The applicable document, precise scope, version, evidence and any reasoned exception are maintained in the controlled compliance matrix. Access to Identify is also available without the

prior creation of a Wallet, so the Wallet biometric factor is not the only route to an identity-proofing procedure.

1.7.3. Public and Internal Identyum Documents

Publicly applicable documents include the Wallet Terms and Conditions, the Wallet Privacy Policy, this Practice Statement, the Identyum Trust Services Practice Statement (TSPS), the Identyum Trust Services Policies and Profiles document (CP), and applicable Disclosure Statements for individual services.

Internal supporting documents include the ID Wallet Authentication Rulebook, the Identification Mechanisms Rulebook, identity-management procedures, information-security and risk-management policies, incident- and continuity-management procedures, technical specifications and evidence records.

1.8. Terms, Definitions and Abbreviations

Terms defined in applicable legislation and standards have the meanings assigned to them in those sources. The following product-specific distinctions are particularly important:

Term	Meaning in this Practice Statement
ID Wallet or Wallet	Identyum's separate account, authentication and authorisation context, and protected data-management environment service. The Wallet does not perform identity proofing and does not issue PID.
Empty Wallet	An active Wallet with established authentication factors, but without an Identyum PID or an assertion of the person's verified identity.
Identyum PID	A product-specific structured result issued by the Identify service after successful completion of an applicable identity-proofing procedure. It contains verified identification attributes and metadata, including the relevant LoIP. It may exist and be used without a Wallet and is not an EUDI Wallet PID issued under Union or national law.
PID LoIP	The assurance level of an identity-proofing result assigned by Identify in accordance with the applicable rules. The Wallet neither calculates nor changes it. It differs from the Wallet authentication mode and from an eIDAS LoA.
Wallet Authentication Mode	The combination of factors and transaction controls achieved for a particular Wallet operation. It is not in itself an eIDAS LoA.
Relying Party	A party that receives and relies on a Wallet authentication result, approved PID attributes or another permitted Wallet output.
Business Client	An organisation contractually integrated with the Identyum Identify service, the Wallet or related services.

Term	Meaning in this Practice Statement
Related Trust Service	A trust service whose request or operation may be initiated or authorised through the Wallet, but which has a separate policy and lifecycle.

The designations AUTH-A to AUTH-E denote authentication mechanisms defined in the controlled Wallet-authentication documentation. ANSign, NAuth and QNSign denote separate certificate profiles defined in the applicable CP and TSPS.

1.9. Document Governance, Approval and Change Management

The Document Owner coordinates periodic review, alignment with related documentation, version control, approval and publication. A review is performed at least annually and following any material change to the service, legal framework, security, architecture or scope.

Each approved version states the version number, effective date, owner, approving person or body, public repository and description of changes. Superseded public versions are retained in the documentation archive in accordance with Identyum's controlled-documentation management rules.

2. Identyum Wallet Service Model and Boundaries

2.1. Description of the ID Wallet Service

The ID Wallet is a server-side service managed by Identyum and available through supported web and mobile interfaces. It enables the User to establish Wallet authentication factors, authenticate and authorise permitted operations, manage supported data and, where the User so chooses, store and present the Identyum PID.

The Wallet is modular. Wallet creation, PID issuance by the Identify service, storage of or linking the PID to the Wallet, requesting a related trust service, certificate issuance and making the certificate available are separate events with separate evidence and lifecycles. Completion of one event does not constitute selection or completion of another.

2.2. Canonical Objects and Their Separation

Object	Primary function	Independent status or lifecycle
Wallet	Authentication, authorisation and access to protected data	Active, suspended or permanently closed/revoked
Authentication factor	Verification of knowledge, possession, account control or a biometric characteristic	Established, available, blocked, replaced or removed
Identyum PID	Structured Identify service result: verified identification attributes, provenance and LoIP	Issued and updated by Identify; it may exist without a Wallet, be used for a transaction, or be stored in/linked to the Wallet at the User's choice
Identity-proofing evidence	Evidence of an Identify procedure or trust-service procedure; it is not active Wallet content	Retained separately under the applicable Identify or TSPS rules, independently of storage or removal of PID from the Wallet
Certificate	Profile-specific authentication or signing function	Pending, active, expired or revoked; certificate suspension is not supported
Private key	Profile-specific cryptographic operation	Protected, usable, blocked or destroyed in accordance with the applicable key lifecycle

Logical or technical linking of objects does not merge their legal or operational lifecycles. For example, removing PID from Wallet content does not delete separately retained evidence for an existing certificate or, by itself, change the status of that certificate.

2.3. Functional Wallet Modes

2.3.1. Empty Wallet or Authentication-Only Wallet

An empty Wallet does not contain an Identyum PID and does not provide an assertion of the person's verified identity. It may establish that the same Wallet authentication context is controlled by a person who has satisfied the required factors, and may return a Relying-Party-specific pseudonymous identifier, a transaction link and the achieved Wallet authentication mode.

An authentication-only result is not electronic identification in the sense applicable to a notified eID scheme, has no eIDAS LoA and must not be interpreted as confirmation of a personal name, national identifier, PID LoIP or other identification attribute.

2.3.2. Wallet with Stored Identyum PID

If the User has successfully completed an approved identity-proofing procedure and chooses to store the issued Identyum PID in the Wallet, the Wallet may present selected verified attributes to an authorised Relying Party. Authentication and PID disclosure remain separate steps.

2.3.3. Wallet Used with a Related Certificate

The Wallet may be used to authenticate and authorise the use of a separately issued ANSign, NAuth or QNSign certificate even if the PID on which the certificate is based is not stored as active Wallet content. Eligibility depends on an active Wallet, appropriate identity-proofing evidence, certificate status, key availability and the requirements of the applicable profile.

2.3.4. Specific eID Credentials and External Regulatory Statuses

A specific eID credential or integration is governed by its own profile and documentation and is not derived from the mere existence of the Wallet, PID or number of authentication factors. A claim of a notified eID means, eIDAS LoA or EUDI Wallet status is permitted only after completion of all applicable external assessment, approval or notification procedures.

2.4. Participants and Roles

The principal participants are the User, Identyum, Business Clients, Relying Parties, providers of related trust services, external suppliers, and competent audit or supervisory authorities. One entity may perform several roles, but responsibilities are determined separately for each function.

The contractual relationship for the Wallet is concluded directly between Identyum and the User. A Business Client may enable or disable display of the Wallet offer within its integrated

Identify flow, but it may not create the Wallet or enter into the Wallet relationship on the User's behalf without the User's explicit choice.

2.5. Service and Technical Boundaries

The boundary under Identyum's control includes the Wallet back-end system, authentication-factor records, protected Wallet content, server-side biometric verification, Relying Party interfaces, status management, monitoring and audit evidence. The supported User device provides an interface and may contain device-bound authentication material, but does not contain the entire Wallet service.

The Wallet is not a QSCD. Qualified signing keys and signature-creation operations belong to the separately governed boundary of the remote QSCD and trust service. The Wallet provides the permitted authentication and transaction authorisation required to invoke that service.

2.6. Normative Wallet Functionalities (TO-BE)

The normative part of this Practice Statement describes the canonical target behaviour of the Wallet as the applicable practice: creation of an empty Wallet, authentication and authorisation through the Wallet, optional initiation or continuation of the Identify service, optional storage or linking and presentation of the Identyum PID, pseudonymous B2B login and defined interfaces with related services.

This TO-BE approach does not constitute a claim that conformity assessment has been completed, qualified status has been granted, Trusted List entry has been made, or an externally regulated profile has already entered qualified production operation. Such facts are established solely by the applicable documentation, decisions and records for the service concerned.

2.7. Functions Outside the Wallet Scope and External Conditions

COL-C and COL-D are Identify service modes, while Identyum SMS, WEB and MOBILE are separate credentials or profiles; their definition, evidence and status are not governed by this Practice Statement. The Wallet governs only the expressly defined interface to such a function where it is used through the Wallet.

An externally regulated status or qualified function may be claimed publicly only after the relevant conformity assessment, regulatory approval or other applicable external prerequisite. Until then, the document normatively describes the architecture and controls of the TO-BE system, but does not attribute an incomplete external status.

2.8. Permitted and Prohibited Uses

Subject to the User's eligibility and the applicable agreement with the Relying Party, the Wallet may be used to authenticate control of the Wallet, provide a Relying-Party-specific pseudonymous login, authorise a related operation, store and present selected PID attributes, and manage supported Wallet authentication factors and data.

The Wallet must not be used to impersonate another person, transfer control to an unauthorised person, bypass security controls, provide false data, reuse an assertion outside its intended audience or validity period, or present an authentication-only result as a person's verified identity or a formal eIDAS LoA.

2.9. Reliance Assumptions and Limitations

Users are expected to protect their devices and factors, verify the identity and request of the Relying Party, confirm only intended operations, and report loss, compromise or suspicious activity without undue delay.

Relying Parties remain responsible for validating the integrity, issuer, intended audience, transaction reference, validity and status of each result and for determining whether the disclosed attributes, PID LoIP, freshness and authentication context are sufficient for their purpose.

Identyum does not warrant that the Wallet will be accepted by every public or private service, that the Wallet replaces an identification document issued by a public authority, that it is a notified eID means, or that it is a European Digital Identity Wallet.

3. Application, Establishment of Authentication Factors and Wallet Creation

3.1. Direct Initiation and B2B Wallet Offer

The Wallet-creation flow may be initiated directly through an approved Identyum interface or displayed after a successful Identify flow performed for a Business Client. The Business Client may contractually determine whether the Wallet offer is displayed, but the offer remains separate from the Business Client's onboarding decision.

Display of the offer does not create a Wallet. Wallet creation begins only when the User expressly requests a Wallet and enters into a direct Wallet relationship with Identyum.

3.2. Voluntary User Choice

Creation and use of the Wallet are voluntary. A Business Client may determine the consequences of the User's choice within its own service, but must not present Wallet creation as an Identyum requirement where the User has not chosen to enter into the Wallet relationship.

Declining or abandoning the Wallet offer does not invalidate an otherwise completed Identify service result or prevent use of that result in the transaction for which it was obtained, subject to the applicable Business Client and identity-proofing rules.

3.3. Information, Wallet Terms and Conditions and Privacy Notice

Before the Wallet is created, the User is provided, in a readable form, with access to the applicable Wallet Terms and Conditions, Privacy Policy, principal service features, mandatory authentication factors, security recommendations and available support channels.

The User performs an explicit and recorded action accepting the Wallet Terms and Conditions. Acceptance of the Wallet relationship is separate from any subsequent Subscriber agreement or certificate-acceptance action for a related trust service.

3.4. Registration Data for an Empty Wallet

Creation of an empty Wallet requires the minimum account and communication data necessary to create, protect and operate the service. Before activation, Identyum verifies the mobile phone number or email address selected as the unique Wallet account identifier.

For the creation of an empty Wallet as such, Identyum does not require identification-document data, a personal name or an identity-proofing result. Data collected solely to establish the Wallet account must not be described as verified person-identity data.

3.5. Establishment of AUTH-A and AUTH-D

When creating a new Wallet, the User establishes the following mandatory primary authentication factors within a single linked establishment session:

a) AUTH-A — ID Wallet PIN, as a knowledge factor; and

b) AUTH-D — Identyum facial biometrics, as a biometric factor.

All factors comprising the establishment event must be completed within the maximum duration of the linked session defined in the controlled authentication rulebook. If both mandatory factors are not established, the Wallet cannot be activated.

Where available, supported additional factors may be established. Their addition does not replace the mandatory initial establishment of AUTH-A and AUTH-D and does not create a verified person identity.

3.6. Meaning of AUTH-D in an Empty Wallet

For an empty Wallet, AUTH-D consists of a liveness check and establishment of a protected biometric representation for subsequent Wallet authentication. It confirms continuity of the Wallet authentication context when a subsequent capture of a live person is successfully compared with that representation.

Establishment of AUTH-D for an empty Wallet does not include comparison with a photograph from an identification document, does not prove the User's identity, does not issue an Identyum PID and does not establish or increase PID LoIP.

3.7. Creation and Activation of an Empty Wallet

The Wallet is created and becomes active after the verified contact identifier has been linked to the account, the mandatory Wallet factors have been established and the Wallet Terms and Conditions have been accepted. No separate identity-proofing decision is required for that activation.

An active empty Wallet may be used only for functions that do not require PID attributes or another separately established identity assertion. It may authenticate control of the Wallet, enable a Relying-Party-specific pseudonymous login and authorise permitted related operations.

3.8. Wallet Identifier and Uniqueness Rule

Each Wallet has an internal non-descriptive identifier and one verified mobile phone number or email address used as the unique account identifier. Only one Wallet may be created at the same time for the same verified mobile phone number or verified email address.

The rule is based on the account identifier, not on the person. A natural person who controls more than one verified mobile phone number or email address may have more than one Wallet. Separate Wallets are not merged automatically or manually.

The internal Wallet identifier is not disclosed as a common identifier across clients. Where a stable identifier is required for private-sector login, pseudonymous identifiers specific to each Relying Party are used.

3.9. Linking Devices and Authenticators

The basic Wallet is not considered permanently bound to a single general-purpose device. The User may access it through a supported interface after completing the authentication required for the operation concerned.

If AUTH-E or another device-specific authenticator is registered, the associated cryptographic or authentication material is bound to that authenticator and managed as a separate factor. Registration of a new factor requires the authentication defined in the controlled ID Wallet Authentication Rulebook.

3.10. Establishment Evidence and Audit Trail

Identyum records sufficient evidence to reconstruct Wallet creation, including the verified account identifier, applicable document versions, acceptance action, types of factors established, relevant transaction and session identifiers, timestamps, outcomes and any exceptional handling.

The evidence confirms the creation and control of the Wallet account. It must not be designated as evidence of the person's identity proofing unless an approved identity-proofing procedure has been completed separately.

3.11. Failed, Interrupted and Repeated Establishment

The Wallet is not activated if the User abandons the process, fails verification of the selected account identifier, fails to establish a mandatory factor, or fails to complete the required acceptance action.

Retries, rate limits and temporary delay measures are applied in accordance with controlled authentication and fraud-prevention rules. Failed establishment of an empty Wallet must not create a PID or be presented as a failed identity-proofing decision where identity proofing was not attempted.

4. Wallet Interface to the Identify Service and Identyum PID

4.1. Initiating or Continuing the Identify Service from the Wallet

Within the Wallet, the User may separately choose to initiate or continue an Identify procedure to obtain or refresh an identity result. The Wallet remains usable without that choice, and initiating Identify neither changes its status nor gives an empty Wallet an assertion of civil identity.

The request is submitted to Identify with the data required to link the session and return the result. The Wallet does not perform identity proofing, decide whether it is successful or assign LoIP.

4.2. Functional and Documentation Boundary of Identify

Identify is a separate Identyum service that collects, validates, links and assesses evidence and, where the conditions are met, issues an Identyum PID. The authoritative rules governing procedures, use cases, evidence sources, decisions, LoIP and the evidence package are established by the TSPS where Identify is used in the context of a trust service, and by the relevant Identify documentation in other contexts.

The Wallet is only the initiation and return channel and, at the User's separate choice, an environment for storing or linking, displaying and presenting the result. The requirements of ETSI TS 119 461 relating to the identity-proofing service, its use cases, evidence and decisions are not fulfilled by this Wallet Practice Statement.

4.3. Identify Flows Independent of the Existence of a Wallet

Identify may be initiated directly, from a Business Client flow, from the Wallet or from another approved channel. The existence of a Wallet is not a prerequisite for performing Identify or issuing a PID.

An Identify result may be used only in the current transaction or, if the issued PID is intended for reuse, subsequently linked to the Wallet based on the User's separate choice. Successful Identify does not automatically create a Wallet.

4.4. Identify Result Available to the Wallet

The Wallet accepts only a structured result issued by Identify for a permitted context and only to the extent necessary for the selected Wallet function. The result may be a PID intended for reuse or a transactional result used without storage in the Wallet.

The Wallet verifies the technical authenticity, integrity, intended context and status of the received result. It does not reassess Identify's evidentiary decision, determine acceptable evidence sources or independently calculate LoIP from the received data.

4.5. Storage or Linking of the Result on the Wallet Side

If the User chooses to store or link the PID, the Wallet associates it with the appropriate authentication context and retains its content or a secure reference in accordance with the service architecture. That action does not change the PID or Identify's evidentiary decision.

Evidence collection, liveness checking, biometric comparison with the identification document, cross-checks and evidentiary thresholds belong to Identify. Wallet AUTH-D is a separate authentication factor; by itself it does not prove civil identity or transfer evidentiary value to the Identify result.

The Wallet records initiation, return, the choice to store or link, and the result of technical processing on the Wallet side. Attempt limits, thresholds and reasons for the identity-proofing decision are recorded by Identify in its evidence system.

4.6. LoIP as Metadata of the Identify Result

Identify determines the outcome of identity proofing and assigns LoIP in accordance with the applicable rules. The Wallet receives, retains and presents that designation with the PID, but does not calculate, increase or decrease it.

LoIP expresses the assurance of the identity-proofing result and is neither a Wallet authentication mode nor an eIDAS LoA. ETSI TS 119 461 defines Baseline and Extended LoIP; each Identyum internal sublevel within the Extended range must be defined and mapped in the applicable TSPS or Identify documentation, and not as a separate ETSI level in this Practice Statement.

4.7. PID Issuance Independent of the Wallet

Following a successful decision, Identify issues an Identyum PID containing verified attributes and the required provenance, time and LoIP metadata. A PID may exist and be used without a Wallet.

The Wallet does not issue, sign as issuer or alter PID content. The designation Identyum PID is a product label and does not constitute a claim that it is an EUDI Wallet PID or person-identification data issued under Union or national law.

4.8. Separation of PID Issuance from Its Availability in the Wallet

PID issuance in Identify and its storage in or linking to the Wallet are separate, independently recorded events. Following issuance, the relevant data are displayed to the User, who is separately asked to decide whether to make the PID available through the Wallet.

Declining storage or linking does not invalidate the PID or the Identify result. The result may be used in the permitted current transaction or as input to a separately governed trust-service procedure, while the evidence package is retained outside active Wallet content.

4.9. Independent Choices Concerning PID and Related Services

Following successful Identify, the User independently decides whether to store the PID in or link it to the Wallet and whether to request a related trust service separately. Neither decision is an automatic consequence of the other.

The interface clearly separates PID storage/linking, PID presentation, a trust-service request, the subscriber agreement and each authorisation to use a key. Applicable profiles and eligibility criteria are established by the CP and TSPS, and each action and its outcome are recorded separately.

4.10. PID Freshness and Referral to a New Identify Procedure

The Wallet may offer to re-present an available PID only if its source, LoIP, time, status and attribute metadata satisfy the requirements of the particular transaction and the User has separately authorised that transaction.

If the PID is insufficient, the Wallet stops presentation or directs the User to the appropriate Identify flow. Only Identify may perform additional verification and issue a new or updated result with a new decision and LoIP; the Wallet then updates its own copy or reference according to the User's choice.

4.11. Identify and Trust-Service Evidence Outside the Wallet

Identity-proofing evidence is retained by Identify or by the QTSP evidence system where the result is used for a trust service. Subscriber, certificate and signature evidence is retained in the trust-service systems. None of those categories is active Wallet content.

Removing or deleting PID from the Wallet does not delete separately retained evidence or, by itself, revoke a certificate. Conversely, retained evidence does not become available as active Wallet content and does not enable PID presentation after its removal.

4.12. Failed and Manually Processed Identify Procedures

If Identify returns a failure, interruption or a result not intended for storage or presentation, the Wallet does not create or modify a PID. It displays the permitted status and any next step to the User, while the detailed reason and evidence remain in the Identify system.

Manual review, an alternative procedure and the LoIP decision belong to Identify and are performed only under its applicable documentation. The Wallet does not permit that decision to be overridden manually.

5. Wallet Authentication Characteristics and Security Model

5.1. Empty Wallet as an Authentication Context

An empty Wallet is an authentication and authorisation context linked to a verified mobile phone number or email address, an internal Wallet identifier and Wallet authentication factors. It does not contain an Identyum PID or create a verified assertion of civil identity.

A person controlling an empty Wallet may authenticate to Identyum or a contractually connected private-sector Relying Party using a pseudonymous identifier specific to that Relying Party. The result confirms successful Wallet authentication for a particular transaction; it does not identify the person by civil identity.

5.2. Authentication Results without Identification

An authentication result without identification may contain Identyum as issuer, the intended Relying Party or audience, a Relying-Party-specific pseudonymous identifier, time and validity data, transaction binding and the achieved Wallet authentication mode.

It must not contain or imply a civil name, national identifier, Identyum PID, PID LoIP or eIDAS LoA unless those data or assertions have been separately established, requested and authorised under the applicable service profile.

5.3. Conditions for an Electronic Identification Means

The existence of a Wallet or successful Wallet authentication does not automatically create an electronic identification means. If Identyum subsequently issues or enables a specifically defined eID credential, the applicable system documentation must establish the complete means, its person-identification data, issuance and lifecycle rules, authentication mechanism, and any formally assessed assurance level.

NAuth is a certificate for certificate-based authentication. It is not automatically a notified electronic identification means and has no formal eIDAS LoA unless such status is expressly established by a separately approved eID scheme or integration.

5.4. Authentication Mode, PID LoIP and eIDAS LoA

Term	What it expresses	What it does not establish by itself
Wallet Authentication Mode	The factors and transaction controls successfully completed for a Wallet action	Civil identity, PID LoIP or eIDAS LoA
LoIP of the Identyum PID	Assurance of the identity-proofing result and evidence	Security of the authentication means or eIDAS LoA

Term	What it expresses	What it does not establish by itself
Certificate profile	The permitted purpose of the key and certificate and the policy requirements	Status of a notified eID means
eIDAS LoA	The overall assurance of an eID means with regard to enrolment, means management, authentication and organisation	A result derived solely from two-factor authentication or PID LoIP

Identyum does not automatically map PID LoIP levels or combinations of Wallet factors to the eIDAS Low, Substantial or High levels. Any formal mapping requires a complete assessment of all applicable assurance elements and an explicit controlled assertion in the applicable eID-scheme documentation.

5.5. Authentication Factors and Categories

Designation	Authentication factor	Operational Category
AUTH-A	ID Wallet PIN	Knowledge
AUTH-B	Verified mobile phone number and demonstrated control of the associated communication channel	Possession or control of the channel, depending on implementation of the action concerned
AUTH-C	Verified email address, Google account or Apple account	Control of an external account
AUTH-D	Identyum facial biometrics	Inherence
AUTH-E	Identyum mobile authenticator	Possession of the associated authenticator

AUTH-A and AUTH-D are mandatory upon initial Wallet creation. Additional factors may be established and used only for actions for which they are permitted by the controlled authentication policy.

5.6. Permitted Factor Combinations

The combination of factors is selected according to the requested action, the controlled Wallet authentication policy, the User's selected security setting, the Relying Party's requirements and the transaction risk. All factors comprising one authentication event must be completed during the same permitted linked session.

Action	Default Requirement
Creation of a new Wallet	AUTH-A + AUTH-D

Action	Default Requirement
Adding or changing identification data	AUTH-A + AUTH-D; additionally AUTH-E where a stricter mode applies
PID presentation or sharing identification data	AUTH-A + AUTH-D or AUTH-E, depending on the applicable policy and the User's setting
Pseudonymous Wallet login	AUTH-A + an approved second factor for that transaction
Higher-risk Wallet action	AUTH-A + AUTH-D + AUTH-E where required
Authorisation of a QNSign/QES transaction using AUTH-E	Online push challenge-response mechanism only

A stronger factor combination may be required, but successful completion of a stronger combination does not in itself increase PID LoIP or create a formal eIDAS LoA.

5.7. Wallet, Device and Server-Side Components

The Wallet operates through supported user interfaces and server-side components under Identyum's control. Protected Wallet content, authentication records, biometric comparison, status, Relying Party interactions and evidence are managed in the server environment.

A general-purpose User device remains outside Identyum's direct administrative control. Device-bound AUTH-E material is generated and protected for the registered authenticator and is not considered interchangeable with centrally protected certificate private keys.

5.8. Credential and Cryptographic-Key Boundaries

Authentication keys, certificate keys, Wallet data-protection keys and service keys have distinct purposes. A key used for one function must not be presented or reused as the key of another profile merely because those functions share technical infrastructure.

Generation, protection and use of subscriber private keys, including HSM/SAM, the remote QSCD, SAD and mechanisms evidencing sole control, are governed by the TSPS and the remote-signing service documentation. The Wallet may convey an authentication result and confirmation of a specific transaction, but is not itself a QSCD, nor is compliance with qualified-signature requirements derived from Wallet factors alone.

NAuth is an authentication certificate and is not used to create electronic signatures. ANSign and QNSign are signing profiles governed by their respective policies. Detailed information on key management and certified devices remains in the TSPS and controlled procedures.

5.9. Protection against Duplication, Unauthorised Modification and Replay

The Wallet authentication context is protected by a combination of server-side factor or credential control, multi-factor authentication, non-exportable private keys, transaction binding and status checking.

A copied user interface or knowledge of the Wallet identifier is insufficient to reproduce the Wallet authentication context. Use of the Wallet also requires successful verification of the applicable authentication factors and valid server-side factors or credentials.

Device-bound mobile-authenticator keys are generated separately for each registered device and retained in the device's protected cryptographic storage. Registration of a new authenticator requires authentication through the existing Wallet.

Short-lived session or challenge data are used in authentication transactions, and transactions are bound to the requesting service and intended action. A previously used one-time factor or credential, challenge or authorisation cannot be reused as valid approval of a new transaction.

Relying-Party-specific pseudonymous identifiers further reduce the risk of tracking or linking across different Business Clients.

Authentication requests and their results are integrity-protected, time-limited and bound to the intended Relying Party, audience and transaction. A copied interface, Wallet identifier or previous response is insufficient to reproduce valid new authentication.

5.10. User Control and Possession

The User demonstrates control of the Wallet using the combination of factors required for the action concerned. Approval is bound to the displayed recipient, purpose, transaction and data scope and must not be regarded as general permission for another action.

Control of the Wallet does not require direct possession of centrally protected certificate keys. Successful Wallet authentication and, where required, confirmation of a particular transaction authorise only the permitted action in the associated controlled service.

5.11. Protection of Stored Data and Data Protection by Design

Wallet content, authentication records and biometric representations are protected at rest and in transit. Data are exposed to the user interface or an authorised Relying Party only to the extent necessary for the requested and permitted action.

For authentication transactions without identification, Identyum uses Relying-Party-specific pseudonymous identifiers to reduce unnecessary data linkage across clients. Authentication does not disclose PID data, and PID disclosure does not include additional Wallet content beyond the authorised scope.

5.12. Regulatory Status and Disclaimer of Claims

The ID Wallet is not presented as a European Digital Identity Wallet, an identification document issued by a public authority, or a Wallet issued under a notified national electronic identification scheme. Application of selected security, privacy and interoperability principles to the Wallet does not change that status.

Identyum publishes a formal claim regarding an eID credential, LoA, notification or conformity only after the relevant scope, system and evidence have been established and the necessary external approvals completed. Such status must not be inferred from marketing terminology, the number of factors, PID LoIP or the availability of a related certificate.

6. Lifecycle Management of the Wallet and Wallet Content

6.1. Wallet Statuses and Separation of Related Objects

The Wallet, authentication factors, PID, certificates, private keys and related services have separate statuses and lifecycle events. Identyum maintains their technical links so that an event affecting one object produces only the effects defined for dependent functions.

A lifecycle event must be recorded with its time, initiator, reason, affected object and resulting status or restriction. A status term for one object must not be applied to another object unless the corresponding lifecycle action has actually been performed.

6.2. Normal Use

During normal use, the User may view and manage Wallet data, authenticate to supported services, authorise data sharing and use related eID and trust-service functions.

Each security-sensitive action requires the authentication combination defined for that action. All factors comprising one authentication event must be completed during the same linked session, which must not last longer than 15 minutes.

Authentication to the Wallet does not in itself disclose PID data. Disclosure requires a separate request identifying the Relying Party and requested data, followed by User authorisation.

Identyum may require stronger authentication where the action, Relying Party or applicable service policy requires a higher level of assurance.

An empty Wallet remains limited to authentication-without-identification and authorisation functions. PID management and presentation become available only once a PID has been separately issued and stored or otherwise made available for an authorised transaction.

6.3. Authentication-Factor Management

Authentication factors may be added or removed only after the User successfully authenticates using the factors prescribed for that change.

The following are required to add a mobile authenticator:

- ID Wallet PIN;
- facial biometrics; and
- verification of the registered mobile phone number.

The User may register more than one mobile authenticator.

Removal of a mobile authenticator requires the PIN and facial biometrics. The same two-factor combination is required to add or remove a verified mobile phone number or email address, Google account or Apple account used as a Wallet authentication factor.

The PIN cannot be removed while the Wallet is active. The mandatory PIN or facial-biometric factor may be changed only through a specifically supported secure procedure that preserves reliable linkage to the User.

Each change is recorded and immediately affects the permissibility and use of every function that depends on the changed factor.

Blocking or removing a Wallet factor affects actions that require that factor. It does not in itself suspend a certificate, because Identyum certificate profiles do not support certificate suspension.

6.4. Adding, Removing and Migrating Devices

The basic ID Wallet is not permanently bound to one device. The User may access it from another supported device after successful authentication to the Wallet.

A device becomes specifically bound to the Wallet when an Identyum mobile authenticator is registered on it. Registration creates a new device-specific authentication factor and does not copy an existing authenticator from another device.

The User may have more than one registered mobile authenticator. Each is managed independently and may be removed without removing the others.

Adding a new bound device requires the authentication specified in Section 6.3. Registration and removal events are recorded in the Wallet audit trail.

Because Wallet data are retained on the server side, migration to a new device does not require transfer of PID or other Wallet content between devices.

From a new device, the User accesses the existing Wallet and, if desired, registers a new mobile authenticator. Registration creates new device-specific cryptographic material that is linked to the existing Wallet.

After activation of the new authenticator, the previous authenticator may be retained or removed in accordance with Section 6.3.

If the previous device has been lost or may have been compromised, the User should first suspend the Wallet and remove the affected authenticator before returning the Wallet to normal use.

Migration or registration of a new authenticator does not merge separate Wallets. A Wallet associated with a different verified mobile phone number or email address remains a separate Wallet with its own lifecycle.

6.5. Changes to Contact Details and Account Identifier

A mobile phone number or email address may serve as contact data, an authentication channel and the unique Wallet account identifier. A change affecting the unique account identifier is

permitted only through a specifically supported procedure and following verification of the new identifier.

Identyum prevents two active Wallets from using the same verified mobile phone number or verified email address as their unique account identifier. Changing the account identifier does not merge the Wallet with another Wallet of the same person.

Changing contact details or the account identifier does not alter verified PID attributes. An attribute forming part of the PID is updated only in accordance with the applicable PID validation and update procedure.

6.6. Adding, Updating, Ageing and Removing PID

A PID may be added to the Wallet only following a successful corresponding identity-proofing result and the User's separate choice to store it. An update records the new source, checks, LoIP and time and does not overwrite the evidence record of the previous result.

Ageing or insufficiency for a particular use case may limit PID sharing or reuse, issuance of a new certificate, renewal, or a transaction requiring more recent evidence. This does not automatically revoke the Wallet or an existing certificate.

The User may remove PID from active Wallet content using the authentication required by the controlled policy. Removal does not revoke, suspend or block an existing ANSign, NAuth or QNSign certificate merely because PID is no longer stored in the Wallet.

6.7. Wallet Suspension

Suspension temporarily blocks normal Wallet authentication, PID presentation, data management and authorisation of related actions through the Wallet. It may be initiated by the User or Identyum where loss, compromise, suspicious activity, misuse, a legal requirement or another material risk is identified.

Wallet suspension prevents use of remote keys associated with the Wallet because the required authentication or authorisation cannot be performed. It neither suspends nor revokes the related certificate, and no suspended-certificate status is published through CRL or OCSP.

During a security or revocation investigation, Identyum may separately block use of a managed private key. Such a technical block is not certificate suspension and does not change the certificate's status until an applicable certificate-lifecycle decision is made.

6.8. Wallet Reactivation

A Wallet suspended by the User may be reactivated only after successful authentication using the combination of factors defined for reactivation and after any necessary replacement or removal of a compromised factor.

If suspension was initiated by Identyum, Identyum may require a security review, additional authentication, factor reset or renewed identity proofing before authorising reactivation. Reactivation restores only those Wallet functions whose dependencies remain valid.

Reactivation cannot restore an expired or revoked certificate or PID data previously removed by the User from active Wallet content.

6.9. Permanent Revocation or Closure of the Wallet

Permanent revocation or closure of the Wallet is final and cannot be reversed. It terminates active sessions, invalidates Wallet authentication-factor links and makes active Wallet content permanently unavailable in accordance with the deletion rules.

Permanent revocation, deletion or closure of the Wallet triggers revocation of all long-term ANSign, NAuth and QNSign certificates associated with that Wallet. Identyum records and performs the required certificate-revocation actions in accordance with the applicable Certificate Policy and TSPS.

That automatic consequence does not apply to QLSeal merely because an individual operator used the Wallet. A QLSeal certificate belongs to the legal person and follows its own certificate and authorisation lifecycle.

6.10. Renewal and Replacement

The Wallet is not periodically renewed as a single credential. Its account identifier, factors, PID, certificates and related functions are reviewed or renewed under their respective rules.

A replacement Wallet is required if the previous Wallet has been permanently revoked or reliable continuity cannot be maintained. The new Wallet is created under the then-current requirements and is neither automatically merged with nor treated as a continuation of another Wallet associated with a different account identifier.

6.11. Access Recovery

Identyum does not disclose or retrieve the User's existing PIN. Recovery is permitted only through a specifically approved procedure that provides sufficient assurance for the affected action and preserves the required linkage between the Wallet and the User.

If the User cannot meet the requirements of the approved recovery procedure, Identyum does not restore access solely on the basis of an unverified customer-support request. The Wallet is permanently terminated and a new Wallet is created if the User wishes to continue using the service.

6.12. Loss, Theft and Compromise

The User must act without undue delay if a device, authentication factor or Wallet session is lost, stolen, exposed or suspected of compromise.

The appropriate immediate action is to suspend or permanently revoke the Wallet and notify Identyum customer support.

Identyum may independently suspend the Wallet if it detects suspicious activity or receives a credible report of compromise.

Following suspension, the affected mobile authenticator, mobile phone number or external-account factor may be removed. If the compromise concerns the PIN, facial-biometric link, PID or the User's identity itself, Identyum may require permanent revocation and new enrolment instead of reactivation.

The User remains responsible for protecting devices and factors until the affected access has been disabled.

A report affecting a certificate or managed private key is handled separately under the certificate-revocation and key-control procedures. Wallet support, key blocking and certificate revocation must remain clearly distinguishable in evidence and public status information.

6.13. Deletion of Wallet Data and Retained Evidence

Following permanent closure of the Wallet, active Wallet content is deleted or made permanently unavailable under the Wallet-deletion procedure. Authentication links become invalid, and Wallet-specific cryptographic material that is no longer required is deactivated or destroyed under the applicable rules.

Deletion of active Wallet content does not require deletion of identity-proofing, subscriber-agreement, certificate, authentication, security or lifecycle evidence that Identyum must retain separately. Such evidence is protected, purpose-limited and removed after expiry of the applicable retention period.

6.14. Status Information and User Notifications

Wallet Status	Meaning
Active	The Wallet may be used for functions whose separate dependencies and statuses are valid.
Suspended	Normal Wallet use is temporarily blocked; certificate status remains unchanged solely on the basis of Wallet suspension.
Permanently revoked or closed	The Wallet cannot be reactivated; long-term ANSign, NAuth and QNSign certificates associated with it are revoked.

The User is notified through an available registered channel of significant Wallet lifecycle and security events. Notifications concerning certificate issuance, acceptance, expiry and revocation are governed separately by the applicable trust-service documentation.

7. Authentication and Authorisation Using the Wallet

7.1. Types of Wallet Authentication and Authorisation Transactions

Wallet Transaction Type	Permitted Result
Pseudonymous B2B login	Confirmation of successful Wallet authentication with a Relying-Party-specific pseudonymous identifier; without civil identity or eIDAS LoA.
Authentication with PID presentation	Wallet authentication result together with selected PID attributes separately requested and authorised by the User.
Authorisation of a related service	Confirmation that the User authorised a defined action, including an eligible remote-signing action.
Step-up authentication	Verification of an additional factor required by the transaction, the User's setting, the Relying Party or the policy of the related service.
Authentication based on an NAuth certificate	Evidence of control of the NAuth key where the integration expressly requires or accepts an NAuth certificate; it does not automatically constitute a transaction using a notified eID means.

Identyum SMS, WEB and MOBILE, where defined and enabled in the applicable profiles, remain separate eID credentials. They do not become Wallet authentication modes, nor does this Practice Statement assign them an eIDAS LoA.

7.2. Initiation by a Relying Party or Related Service

Authentication through an approved Identyum interface is initiated by a registered Relying Party or an Identyum service acting for a defined transaction.

Depending on applicability, the request contains:

- the Relying Party;
- the transaction or session;
- the requested Wallet authentication mode or, where applicable, a separately defined credential requirement;
- the action to be authorised;
- any requested PID attributes;
- the purpose of the request; and
- the registered response destination to which the result is to be returned.

The User may access the authentication flow through a browser redirect, application link, QR code or another supported channel. Regardless of the channel, the request must be traceable to a registered Relying Party and a specific transaction.

Requests that are incomplete, expired, altered or received from an unregistered integration are rejected.

7.3. Identification of the Relying Party

Before processing an authentication request, Identyum verifies that the Relying Party is registered and authorised to use the requested service.

Verification is based on the Relying Party's registered technical credentials, approved interfaces and endpoints, contractual status and canonical Relying Party identity.

The canonical Relying Party identity represents the actual service or organisation for which authentication is performed. It is managed independently of changes to domains, technical clients, redirect addresses or other implementation details.

Before confirming the transaction, the User is shown a clear and readable identification of the Relying Party. If the requesting party cannot be reliably identified, the transaction is not completed.

Contractual and technical registration of the Relying Party is an Identyum control for this service. It must not be described as EUDI Wallet Relying Party registration or an EUDI Wallet Relying Party access certificate unless that separate regulated framework is actually implemented.

7.4. Determining the Required Authentication Mode

The required mode is determined according to the action, applicable Wallet authentication policy, Relying Party request, User security setting, related-service policy and assessed risk. Where requirements differ, the strictest applicable minimum applies.

The result states the achieved Wallet authentication mode or the particular credential used. An eIDAS LoA is not assigned to the result merely because several factors were available or successfully used.

7.5. Factor Selection and Step-Up Authentication

Unless another approved mode applies, the following are required for authentication or PID sharing:

1. ID Wallet PIN; and
2. Identyum facial biometrics or the Identyum mobile authenticator.

For a stricter transaction, all three factors may be required: PIN, facial biometrics and mobile authenticator.

For an approved lower-risk transaction, the Relying Party may permit a PIN together with a verified mobile phone number or external-account factor. Such a lighter combination cannot be used if the User selected a stricter mode or the applicable service requires stronger authentication.

All factors comprising one authentication event must be completed during the same linked session, which must not last longer than 15 minutes.

If the mobile authenticator is used for a high-risk action or a qualified trust-service action, Identyum may require online push confirmation instead of an offline one-time password.

Step-up authentication may require an additional factor or a stronger permitted combination. If the Relying Party also requires more recent identification data or a higher PID LoIP, that requirement is handled through separate enhanced identity or PID verification and not merely by adding an authentication factor.

7.6. Dynamic Authentication

Where required by the risk or legal nature of the action, authentication is dynamically linked to a specific transaction.

The information displayed to the User identifies the action being approved and, as applicable, the Relying Party, requested data, transaction reference and relevant document or service.

By confirming, the User authorises only the displayed transaction. It cannot be interpreted as approval of another transaction, another Relying Party or broader data disclosure.

The mobile authenticator may perform dynamic authentication through an online challenge-response procedure. The request is displayed on the registered device and approved by a cryptographic response generated on that device.

Static or offline one-time-password authentication may be used only where permitted by the applicable authentication mode.

7.7. Binding of Challenge, One-Time Value, Session and Audience

Each authentication transaction is assigned a unique transaction context.

Where a challenge-based protocol is used, Identyum generates a fresh and unpredictable challenge that is valid only for a limited time and for one authentication attempt.

The authentication request and response are bound to the relevant:

- User session;
- Relying Party or audience;
- transaction identifier;
- requested authentication mode;
- requested PID scope, where applicable; and
- approved response destination.

A response intended for one Relying Party cannot be accepted by another Relying Party. Likewise, an authentication result from one transaction cannot be transferred to another transaction or session.

Authentication messages are protected in transit and checked for integrity, origin, validity period and transaction context.

Identyum prevents reuse of expired or previously accepted challenges, authentication responses and one-time passwords.

The online mobile-authenticator mode uses a protected challenge-response procedure. The challenge is delivered to the registered authenticator, and the response is generated using device-bound cryptographic material. Identyum validates the response before granting access.

Authentication results are returned only to approved endpoints associated with the Relying Party that requested them. Requests whose transaction identifiers, audience, redirect destination or other protected parameters do not match are rejected.

7.8. Wallet and Credential Status Checks

Before completing a Wallet authentication transaction, Identyum verifies that the Wallet is active, that the required factors are available and valid for the action, and that the request is valid and bound to a registered Relying Party or related service.

If the transaction involves a certificate or remote key, certificate status, profile permissibility and key availability are checked separately. Wallet suspension blocks Wallet-based use but does not change certificate status. A revoked or expired certificate cannot be restored through Wallet reactivation.

7.9. User Confirmation and Transaction Authorisation

Before confirmation, the User is shown the identity of the Relying Party and the nature of the requested action.

An authentication request without identification clearly states that no PID attributes will be disclosed.

If data sharing is requested, the User is also shown:

- the requested attributes;
- the stated purpose;
- relevant validity or access information; and
- any additional information necessary to make an informed decision.

The User must give explicit confirmation. Declining or abandoning the request terminates the transaction without a successful authentication or data-sharing result being created.

Consent for one transaction does not constitute continuing permission for unrelated future transactions.

Consent to personal-data processing is used only where consent is the applicable legal basis. A security confirmation, contractual instruction or transaction authorisation must not be designated as consent under the GDPR merely because the User clicks an approval control.

7.10. Authentication Result without Identification

If no PID attributes have been requested, the Wallet may return an authentication result without identification. The result identifies the intended Relying Party, contains a Relying-Party-specific pseudonymous identifier and records the authentication context and transaction outcome.

The Relying Party must not use that result as evidence that Identyum verified or disclosed the User's civil identity. If civil identity is required, the Relying Party must request and receive the necessary PID attributes through the separate procedure described in Chapter 8.

7.11. Relying-Party-Specific Pseudonymous Identifiers

Wallet authentication uses a Relying-Party-specific pseudonymous identifier contained in the authentication assertion or an equivalent authentication result.

The identifier is stable for the same User and the same canonical Relying Party, but differs between Relying Parties. It does not disclose the internal Wallet identifier, national identifier or another common value intended to link data across clients.

No separate anonymous certificate is issued. Identyum retains the controlled relationship between the User, Wallet and Relying-Party-specific identifiers solely for lifecycle management, incident response and legally justified evidentiary purposes.

Civil-identity data are disclosed to the Relying Party only through a separate PID-sharing transaction authorised by the User.

The identifier may be issued for an empty Wallet. In that case it identifies the same Wallet relationship within the context of the canonical Relying Party, and not the User's verified civil identity.

7.12. Authentication Assertion and Evidence

Following successful authentication, Identyum returns an integrity-protected result through an approved interface. Depending on the use case, the result identifies Identyum, the intended audience, a Relying-Party-specific identifier, authentication context, transaction reference, issuance time, validity period and outcome.

The result does not contain PID attributes unless their disclosure formed part of a separately displayed and authorised request. Identyum records sufficient evidence to reconstruct the request, the Relying Party, factor categories completed, the User's action, the result and the scope of any data provided.

7.13. Failed Authentication and Detection of Misuse

Authentication is unsuccessful if a required factor is not completed successfully, the transaction has expired, the Wallet or credential is invalid, or the response cannot be bound to the requesting Relying Party and the transaction concerned.

The User may be permitted to repeat authentication within controlled attempt limits. If the previous transaction or challenge has expired or can no longer be used securely, a new transaction or challenge is required.

Identyum may require step-up authentication if:

- the requested action is more sensitive than the current session;
- the Relying Party requested a stronger mode;
- it is required by the User's security settings;
- a separately applicable credential does not meet the stated assurance-level requirement; or
- the transaction is associated with increased risk.

A lighter authentication mode is not used as a substitute where a stronger mode was required but could not be completed.

Identyum monitors authentication activity to detect indications of misuse, fraud or unauthorised control of the Wallet.

Relevant events may include repeated failed attempts, unusual authentication patterns, invalid or replayed transaction responses, credential misuse, inconsistent session information, or activity associated with a reported loss or compromise.

Depending on the assessed risk, Identyum may:

- reject the transaction;
- require stronger authentication;
- temporarily block an authentication factor;
- suspend the Wallet or block the affected factor or use of a managed key;
- notify the User;
- initiate an incident investigation; or
- require renewed identity proofing.

Detailed detection rules and thresholds are confidential and are not published in this Practice Statement.

Inability to complete the required stronger mode is not resolved by silently falling back to a weaker mode. The transaction is rejected or restarted within an expressly permitted alternative flow.

7.14. Relying Party Obligations

A Relying Party using the ID Wallet must:

- keep its registration data, technical credentials and approved endpoints up to date;
- accurately identify itself to Identyum and the User;
- request only the authentication level and data necessary for the stated purpose;

- protect authentication results and PID data against unauthorised access or reuse;
- validate the integrity, issuer, audience, validity period and transaction binding of each result;
- verify whether the achieved Wallet authentication mode, any expressly applicable credential assurance level, PID LoIP and freshness meet its requirements;
- comply with applicable contractual, privacy and personal-data-protection obligations; and
- report to Identyum any suspected compromise or misuse and any material incidents associated with the integration.

An authentication result without identification must not be regarded as evidence that civil-identity data were disclosed to or verified for the Relying Party.

Relying Parties must not attempt to derive Identyum's internal Wallet identifier, link pseudonyms specific to different Relying Parties, or reuse a Relying-Party-specific identifier outside the context of the Relying Party for which it was generated.

The Relying Party remains responsible for deciding whether to grant access, conclude a transaction or rely on the presented PID data.

8. Data in the Wallet and Presentation of the Identyum PID

8.1. Wallet Data Categories

Category	Examples and Status
Wallet account data	Internal Wallet identifier, verified mobile phone number or email address as the account identifier, status and configuration.
Authentication data	Factor links, protected biometric representation, authenticator registration and security events.
Identyum PID	A copy of or secure reference to a PID issued by Identify, together with verified attributes and provenance, LoIP and time metadata, where the User has chosen to make the PID available through the Wallet.
Other verified data	Data validated through an approved source or provider and labelled with their provenance and status.
User-provided or customised data	Data that are not presented as verified unless a defined validation procedure has been performed.
Activity information	User-visible records of supported authentication, disclosure and lifecycle events.

8.2. PID Stored in or Linked to the Wallet

The Identyum PID is issued by Identify as a structured identity result. At the User's choice, the Wallet retains a protected copy of the PID or a secure reference enabling its retrieval and presentation; in doing so, it does not become the PID issuer or assume responsibility for its LoIP decision.

The PID need not be a physical file on the User's device or a permanently stored copy in the Wallet. The interface may display data from a protected copy or retrieve them through a secure reference while preserving the issuer, integrity, status and metadata of the Identify result.

8.3. Validated and Non-Validated Data

Data stored in the Wallet are classified according to whether their source and content have been verified.

Data labelled as validated carry an assertion and metadata from the source that performed the applicable validation procedure. The Wallet retains and displays the source label, verification status and, for a PID, the LoIP assigned by Identify; storage alone does not make data validated.

Non-validated data may be stored for specific use cases, but must be clearly distinguished from verified data. They do not form part of the Identyum PID and must not support an eID credential, certificate issuance or another regulated function unless subsequently verified.

When data are presented to a Relying Party, the result states whether the data are verified, self-declared or otherwise unsupported by an Identyum assurance assertion.

With the User's consent, a Business Client may write its own business data to the User's Wallet.

Such data may include information arising from the relationship between that Client and the User. The data are encrypted under the Client's control, and Identyum cannot read them without access enabled by the Client.

The Client is responsible for the lawfulness, accuracy, meaning and lifecycle of customised business data. Unless otherwise stated separately, Identyum does not verify those data and makes no LoIP or authenticity assertion concerning them.

The Client may allow another legal person to read the data by enabling the necessary cryptographic access, but their use or disclosure through the Wallet still requires the User's consent.

The interface and disclosure process preserve the distinction between verified PID attributes, other validated data and data supplied without Identyum verification. Data do not become verified merely by being stored in the Wallet.

8.4. Sources, Provenance, LoIP and Freshness

Identyum records the provenance of verified Wallet data.

Provenance may identify:

- the identification document, register, eID, certificate, bank or other source from which the data originate;
- the data-collection method;
- whether the source was primary or used for additional validation;
- the time of retrieval or presentation; and
- the relevant verification status.

Where an attribute has been obtained from several sources, the relevant sources and cross-validation result may be recorded in the PID.

Provenance remains associated with the attribute when it is stored, refreshed or shared, to the extent necessary for the User and Relying Party to assess the reliability of the data.

Each PID available through the Wallet carries the LoIP assigned to it by Identify under the applicable Identify documentation or the TSPS.

The Wallet retains only the provenance and status data that form part of the issued PID or are necessary for its permitted use. The complete evidentiary results from which LoIP was derived remain in the Identify or QTSP evidence system, outside active Wallet content.

Detailed scores, thresholds, identity-proofing mechanisms and fraud indicators do not form part of Wallet content. They are maintained in the applicable controlled evidence records of Identify or the trust service and are available only to authorised parties for a permitted purpose. When the Wallet presents a PID, it conveys the LoIP and only such source, status and freshness metadata as were issued or confirmed by Identify and are necessary for the specific authorised purpose.

The PID and its attributes contain timestamps showing when the data were obtained or verified. The continued usability of an attribute may depend on:

- the validity of its original source;
- expiry, suspension or revocation of the identification document or credential;
- the time elapsed since verification;
- a change communicated by an authoritative source; and
- the Relying Party's freshness requirement.

Data may remain visible in the Wallet after they cease to meet a particular freshness requirement. In that case, they cannot be presented as current for that use case without additional validation or a refreshed PID.

Refreshing the PID creates updated provenance data, timestamps, verification results and LoIP. Earlier evidence may continue to be retained separately for audit and legal purposes.

LoIP belongs to the identity-proofing result and must not be combined with the achieved Wallet authentication mode into a single unsupported assurance assertion.

8.5. Protected Storage

PID and other protected Wallet data are retained in Identyum's back-end system within a User-specific security context and are made available through a supported interface only after the authentication required for the action.

Protected Wallet content is encrypted at rest and in transit and is not retained on the User's device as an ordinary readable local copy. Where readable data are temporarily required for display, validation or sharing, processing is performed only in a controlled environment and temporary material is removed in accordance with the applicable security procedure.

Administrative and support access is restricted by role, purpose, approval and logging. Support activity does not create an unrestricted secondary copy of Wallet content. Any exceptional evidentiary copy required for an incident, legal request or regulatory purpose is handled as separately retained evidence and not as active Wallet content.

Separately retained identity-proofing and trust-service evidence is not ordinary active Wallet content and is subject to the access and retention controls described in Sections 8.13 and 10.8.

8.6. User Access and Data Management

Following successful authentication, the User may access and review data stored in their ID Wallet.

The Wallet displays data in an intelligible form and, where relevant, their verification status, source, LoIP, collection date, validity or freshness.

User access does not necessarily include confidential security information such as internal fraud indicators, detailed technical scores, cryptographic secrets or system audit records.

Where data have been stored in the Wallet by a third party, the User's ability to interpret, modify or export them may also depend on the applicable format, encryption and rights of that third party.

Data may be added to the Wallet by:

- the User;
- Identyum following an approved collection or verification procedure; or
- a third party acting with the User's consent.

A request to add or update a PID in the Wallet requires Wallet authentication, but the collection, validation and issuance of the updated PID itself are performed in Identify.

Verified identification data may be updated only through an approved source or verification procedure. The refreshed result records its provenance, verification time and LoIP instead of silently altering the evidentiary history of the previous result.

Self-declared or non-identification data may be edited through a supported Wallet function, but their status remains non-validated unless subsequently verified by Identyum.

8.7. Data Selection and Minimisation

A Relying Party may request only the attributes necessary for the stated purpose.

Identyum displays the scope of the requested data to the User and does not disclose any additional Wallet content merely because the User authenticated.

Where the integration permits optional attributes, the User may exclude them from disclosure. Attributes designated as mandatory for the requested service cannot be omitted if the User wishes to complete that transaction.

If the Relying Party requires only a stable account identifier, authentication may be completed using a Relying-Party-specific pseudonym without disclosing the User's name, national identifier or other civil-identity data.

Authentication requests without identification must not trigger PID disclosure. Where the Relying Party requires only an account-level pseudonym, the civil name, national identifier and other PID attributes are not included.

8.8. PID Presentation and Attribute Sharing

A PID is presented in a protected transaction initiated by an authorised Relying Party and confirmed by the User.

The PID need not be disclosed as one complete data set. Identyum may provide only selected attributes together with the metadata necessary for their interpretation and validation.

Depending on the request, the disclosed result may include:

- verified identification attributes;
- their source or provenance;
- the applicable LoIP;
- the time when the data were obtained or verified;
- validity or freshness information; and
- the status of the PID or relevant attribute.

Data are transferred from Identyum's back-end system to the authorised Relying Party through an approved interface. Authorisation is limited to the particular recipient, transaction, data scope and, where applicable, access period.

Wallet data are shared only in a transaction authorised by the User.

Before confirmation, the User is shown the Relying Party, requested data and stated purpose. Disclosure is limited to the selected recipient, attributes and transaction.

The shared result may include the requested data together with source, LoIP, freshness and validity information necessary for their interpretation.

Data prepared for a Relying Party are protected for that recipient and made available through a time-limited access mechanism. Unless another period has been agreed and published, the default availability period is five days. After expiry or retrieval, temporary delivery copies are deleted in accordance with the applicable storage policy.

Authentication-factor data are not shared with the Relying Party.

8.9. Binding to Recipient, Purpose and Transaction

Before disclosure, the User is shown the readable identity of the Relying Party, requested attributes, stated purpose and transaction context. Authorisation is limited to that recipient, scope and transaction or permitted access period.

A previous authentication or disclosure approval cannot be regarded as permission for a new recipient, new purpose, different data scope or unrelated transaction. Requests that cannot be reliably bound to a registered Relying Party are rejected.

8.10. PID Status and Freshness Verification

Before presenting PID data, Identyum determines whether the requested attributes are available and meet the applicable status and validity requirements.

The result provides the Relying Party with sufficient information to assess:

- where the data originate;
- how and when they were verified;
- the applicable PID LoIP;
- whether the source or evidence on which the data are based remains valid; and
- whether the data meet the requested freshness requirement.

The Relying Party remains responsible for determining whether the PID and LoIP are sufficient for its legal or business purpose.

If the available PID is too old, incomplete or below the requested LoIP, the Wallet does not change its status or LoIP, but stops presentation or directs the User to Identify for a new or refreshed result.

If the PID does not meet the requested requirements, the transaction may continue only after an approved revalidation, refresh or enhanced-verification procedure. The Relying Party remains responsible for deciding whether the resulting PID is sufficient for its legal or business purpose.

8.11. Updating, Removal and Reuse

The User may request initiation of a PID-update procedure from the Wallet, but the new source, checks, decision, LoIP and time are determined by Identify. Following a successful outcome, the Wallet replaces or links the new copy/reference while preserving separate evidence records.

The User may remove individual PID attributes or the entire PID from active Wallet content after completing the authentication required for that action. Removal prevents future presentation of the removed data through the Wallet, but does not retract data already lawfully provided to a Relying Party or delete evidence that Identyum must retain separately.

Removing PID from Wallet content does not change the status of an existing ANSign, NAuth or QNSign certificate or, by itself, block the corresponding private key. Removal may prevent future PID sharing or require new evidence for issuance, renewal, re-keying or another regulated action.

An existing PID may be reused in a subsequent Identify procedure, user-onboarding process or another supported transaction only if it contains the required attributes and meets the applicable LoIP, validity and freshness requirements. Each reuse requires a new request and User authorisation; previous sharing does not create unlimited or permanent access.

If the existing PID is insufficient, Identify may collect additional attributes, revalidate data or perform a new procedure. The Wallet notifies an authorised Relying Party only within a valid request and without automatically disclosing the changed value.

The User may receive Wallet notifications of significant updates, removals, lifecycle events or security-sensitive changes. Permanent closure of the Wallet and final handling of Wallet data are governed by Chapter 6.

8.12. Activity History, Export and Portability

The Wallet provides the User with an overview of significant activities associated with their data where supported by the relevant interface.

The overview may include:

- adding, updating or deleting Wallet data;
- data-sharing requests and their outcomes;
- the Relying Party involved;
- authentication and credential events;
- changes to authentication factors; and
- Wallet suspension, reactivation or revocation.

Identyum separately maintains audit records sufficient to reconstruct material Wallet actions. Such records may contain timestamps, transaction references, Wallet identifiers or Relying-Party-specific identifiers, data categories involved and event outcomes.

Audit records do not provide routine access to complete Wallet content and may be retained longer than the corresponding active data where required for legal, security or evidentiary purposes.

Where supported, the User may export selected data from the ID Wallet in a commonly used machine-readable or human-readable format.

The export may include selected Wallet data and relevant metadata, such as their source, verification status, LoIP and collection date.

The export does not include:

- Identyum's internal security rules or fraud indicators;
- cryptographic private keys protected in central or remote environments;
- confidential encryption keys of another party;
- internal system and audit records; or
- data whose export would infringe third-party rights or applicable law.

An exported data file is not in itself an active Identyum PID, eID credential or authentication result. Its subsequent acceptance and evidentiary value depend on the format, integrity protection and requirements of the receiving party.

The export or activity-history functionality does not include private keys, authentication secrets, protected biometric templates, security-sensitive internal evidence or records whose disclosure is restricted by law or security requirements.

8.13. Separation from Retained Regulatory Evidence

Active Wallet data are managed for the functions used by the User and are subject to the Wallet deletion and privacy rules. Identify, subscriber, certificate, signature and security evidence retained for legal or regulatory purposes is kept separately with controlled access.

Deletion or removal of active Wallet content does not delete evidence subject to a longer applicable retention period. Retention of that evidence does not make the PID active Wallet content again or permit its further presentation to a Relying Party.

9. Wallet Interfaces with the Identify Service and Related Trust Services

9.1. Relationship with the Identyum Identify Service

Identyum Identify and the Wallet are separate services that interact with each other. Identify performs identity proofing and creates a transaction result and, where the applicable decision is successful, an Identyum PID. The Wallet provides an optional environment for subsequent storage, management, authentication and authorised presentation.

The User may complete Identify without creating a Wallet, may have an empty Wallet without completing Identify, and may complete Identify without storing the resulting PID in the Wallet. The documentation and interface preserve all these permitted options.

9.2. Optional Wallet Offer Following an Identify Procedure

A Business Client may configure whether a User who has successfully completed its integrated Identify flow is offered creation of an Identyum Wallet. The offer is made only where permitted by the relevant Business Client agreement and Identyum flow.

The User's explicit choice is required. A Business Client cannot make the Wallet relationship mandatory on Identyum's behalf or create a Wallet without the User's direct acceptance of the applicable Wallet Terms and Conditions.

9.3. Independent Choices Concerning PID and a Related Trust Service

Following an appropriate Identify result, the User independently chooses whether to store the PID in or link it to the Wallet and whether to request a particular trust service separately. Declining one option does not in itself prevent the other where the criteria of the applicable CP and TSPS are met.

Before the action, the Wallet displays the exact service and profile to which the request relates and refers to the applicable terms. A generic designation must not suggest that every profile is qualified, that qualified status has already been obtained, or that the certificate and PID are automatically included in the Wallet.

9.4. Trust-Service Boundary

The Wallet may be used to request, access or authorise a related Identyum trust service. The Wallet itself is not a certification authority, remote QSCD or signature-creation service, and storage of ordinary Wallet content does not include a usable certificate private key.

Certificate issuance, Subscriber registration, certificate acceptance, certificate status, key protection, signature creation and evidence are governed by the applicable Certificate Policy, TSPS, Disclosure Statement, Terms and Conditions and controlled procedures.

9.5. Applicable Documents for Related Trust Services

Matter	Applicable Document	Role of the Wallet
Supported profile and eligibility criteria	CP and corresponding TSPS/CPS	The Wallet displays the available separate service; it does not determine the profile or eligibility.
Request and subscriber agreement	TSPS, Terms and Conditions and Disclosure Statement	The Wallet may display information and record the User's explicit action.
Certificate issuance, status and lifecycle	CP and TSPS/CPS	They are separate from PID storage and the Wallet lifecycle, except for expressly defined effects.
Remote signing and key use	TSPS and SSAS documentation, including ETSI TS 119 431-1	The Wallet is a user interface for authentication and transaction confirmation; it does not itself evidence sole control or QSCD status.

This Practice Statement does not prescribe mapping of LoIP to certificate profiles or package content. Such rules, including permitted profile combinations and any qualified assertions, are established by the CP and TSPS and become operationally applicable only after the required external conditions have been met.

9.6. Wallet-Side Request and Acceptance of Related-Service Terms

Where a request for a related trust service is initiated from the Wallet, the Wallet displays the exact service/profile to the User before the action and provides access to the applicable terms and information on a durable medium. The User then submits the request or accepts the agreement through a separate intentional action in accordance with the procedure governed by the TSPS.

The Wallet records the information displayed, versions of the referenced documents, User action, time and transaction reference and provides that evidence to the applicable trust-service system. The legal validity of the request and content of the subscriber relationship are determined outside this Practice Statement.

9.7. Display of Related-Service Result and Status in the Wallet

If the applicable trust-service procedure requires display, acceptance or activation of an issued certificate, or another action before use, the Wallet may provide that user interface. Each such

action remains separate from the earlier request and agreement and is performed in accordance with the CP and TSPS.

The Wallet records the User display and action and exchanges status with the applicable trust-service system. Certificate issuance, activation, rejection, status and subsequent handling are determined exclusively under the CP and TSPS.

9.8. Certificate Eligibility without PID Stored in the Wallet

Long-term ANSign, NAuth and QNSign require an active Wallet and an appropriate identity-proofing result and evidence package linked to the subject and certificate request. PID need not remain stored as active Wallet content.

An empty Wallet does not by itself establish identity for a certificate. Nevertheless, it may remain a valid authentication and authorisation environment for a certificate whose identity basis has been separately established, linked and retained in accordance with the applicable trust-service rules.

9.9. Wallet Authentication for Remote-Key Use

Use of an End User's private key managed by Identyum requires the Wallet authentication and transaction authorisation prescribed for the profile and action concerned. Successful Wallet authentication authorises only the particular cryptographic action and does not give the User direct access to the private key.

Where AUTH-E forms part of the remote-signing authorisation procedure, it is used through a transaction-bound online challenge-response flow that displays the data necessary for informed confirmation to the User. Compliance with the requirements for SAD, sole control and a qualified electronic signature is evidenced by the complete SSAS/QSCD procedure under the TSPS and ETSI TS 119 431-1, and not by the mere existence of AUTH-E or the Wallet.

9.10. Effect of Wallet Events on Certificates and Keys

Wallet or PID Event	Effect on ANSign, NAuth and QNSign
Wallet is active	The certificate may be used if the certificate, key, required factors and related service are separately valid.
Wallet is suspended	Wallet-based key use is blocked; certificate status remains unchanged solely because of Wallet suspension.
Wallet is reactivated	Use may continue only if the certificate and other dependencies remain valid.
PID is stale or insufficient	The status of an existing certificate remains unchanged; refreshed identity evidence may be required for new issuance, renewal or a particular transaction.

Wallet or PID Event	Effect on ANSign, NAuth and QNSign
PID is removed from the Wallet	The status of an existing certificate and key eligibility remain unchanged solely because of the removal.
Wallet is permanently revoked, deleted or closed	Under the canonical closure rule and applicable CP/TSPS, long-term ANSign, NAuth and QNSign certificates associated with the Wallet are revoked; performance and evidence of revocation belong to the trust service.
An individual certificate has expired or been revoked	Only the function of the affected certificate ceases; the Wallet may remain active.

Identyum does not support temporary certificate suspension. Where immediate risk mitigation is required during an investigation, Identyum may block use of a managed private key while leaving certificate status unchanged until the reason for revocation has been sufficiently confirmed.

9.11. Services Outside the Scope of the Wallet Practice Statement

The complete activities of the CA and RA, remote QSCD management, signature creation and validation, QLSeal operation, qualified time stamping, certificate-status services and trust-service termination are governed outside this Practice Statement.

Availability of a related function through the Wallet interface does not make that function part of the Wallet service or make Identyum the provider of a third-party service. The applicable service provider and governing documentation are identified for each integration.

10. Security and Operations Management

10.1. Organisation and Responsibilities

Identyum manages the ID Wallet service through defined management, operational, security, technical, legal and support functions. The Director retains overall responsibility for service governance, resource allocation, policy approval and acceptance of significant residual risks. Principal responsibilities are allocated as follows:

Function	Principal Responsibilities
Management Board	Service governance, policy approval, resources and acceptance of significant risks
Risk and compliance	Risk management, regulatory monitoring, compliance oversight and Management Board reporting
Information security	Security management, monitoring, access control and incident management
Technology and infrastructure	Development, infrastructure operation, deployment, availability and recovery
Identify service interface management	Integration rules, transfer of requests and results, and separation of authority; identity-proofing decisions remain with Identify
Data protection and legal affairs	Privacy governance, legal documentation and notification obligations
Customer Support	User enquiries, support-request management and escalation
Process and asset owners	Control over assigned processes, systems, information and other assets

Customer support is organised in three levels. First-level support receives, records and initially analyses enquiries. More complex procedural or technical matters are escalated to second-level support, while matters requiring software intervention or detailed system analysis are handled by authorised technical specialists. Communications with Users and changes in request status are retained in the support system.

Detailed role allocation, deputies and internal reporting lines are maintained in Identyum's controlled organisational documentation.

Responsibility for the Wallet service remains with Identyum even where a supplier performs a supporting activity. Responsibilities for related trust services are governed by the corresponding TSPS and service roles.

10.2. Risk and Information-Security Management

The ID Wallet service is included within Identyum's organisation-wide business and information-system risk-management framework.

Risks are identified and assessed at least annually and additionally following material changes, including the introduction of new services or technologies, material architectural changes, significant incidents or changes affecting critical processes.

The assessment considers relevant assets, threats, vulnerabilities, existing controls, likelihood and potential impact. Risks are classified as low, medium or high and recorded in the confidential Business Risk Register.

Depending on the assessment, Identyum may:

- accept the risk;
- reduce it through additional controls; or
- transfer part of the risk through a supplier, contract or insurance.

Where mitigation is selected, the Risk Register identifies the control, responsible person, implementation deadline and expected residual risk. Residual risk is reassessed after implementation and accepted by the authorised management function.

Risk results are reviewed in annual and, where necessary, ad hoc reports. The risk-management framework itself is subject to periodic internal review.

The ID Wallet operates within Identyum's information-security and privacy-management framework.

The framework establishes controls intended to preserve:

- the confidentiality of identification, biometric and authentication data;
- the integrity and authenticity of PID, credentials and transaction evidence;
- the availability of the Wallet and supporting services; and
- accountability for security-sensitive actions.

Security and privacy requirements apply during the design, development, testing and production operation of the service, provision of support, incident handling and service termination.

Identyum maintains approved policies and procedures covering access control, asset, change and incident management, data retention, physical security, supplier management and business continuity. Detailed technical configurations and detection rules remain confidential.

Risk assessment distinguishes between Wallet authentication-without-identification functions, identification-data functions and trust-service dependencies. Controls and acceptance criteria are proportionate to the actual function and do not assume a higher assurance classification than has been formally established.

10.3. Roles, Competence and Segregation of Duties

Security-sensitive responsibilities are segregated to reduce the possibility that one person could independently introduce, approve and conceal an unauthorised action.

In particular:

- software developers submit software changes for review;
- production deployment is restricted to authorised personnel;
- infrastructure changes require approval by the responsible technical function;
- decisions in the Identify procedure are made only by personnel assigned that role under the applicable Identify documentation; Wallet roles do not override such a decision;
- customer-support personnel do not have unrestricted access to production systems; and
- privileged access does not in itself authorise changes to identity, credential or Wallet records.

Where strict organisational segregation is impracticable, Identyum applies compensating controls such as independent approval, peer review, recorded deployment, dual control or subsequent verification.

Access and role assignments are reviewed when responsibilities change and are removed without delay when no longer required.

Personnel are assigned to ID Wallet-related roles according to their competence, responsibilities and need for access.

Before access is granted, personnel are made aware of their confidentiality, information-security and personal-data-protection obligations. Background or suitability checks are performed where lawful and proportionate to the role.

Personnel receive training appropriate to their responsibilities. Depending on applicability, it includes:

- secure use and management of information systems;
- handling personal and biometric data;
- recognising and reporting incidents;
- secure software- and infrastructure-change practices;
- customer-support escalation; and
- delineation of authority and secure handling at the Wallet interface with the Identify service.

Training is repeated where material changes are introduced or where an incident, audit or risk assessment demonstrates a need for additional competence.

10.4. Supplier Management

Identyum may rely on external providers of infrastructure, hosting, communications, security components, identity sources or other supporting services.

The supplier-management process considers the importance of the supplied function, the sensitivity of the data involved, operational dependencies and the effect that a supplier's failure to perform could have on the ID Wallet service.

Relevant supplier agreements govern matters such as confidentiality, personal-data protection, access restrictions, security incidents, service availability, subcontracting, continuity, audit evidence and termination.

Supplier access to systems or equipment under Identyum's control must be authorised, limited to the necessary purpose and recorded. Critical suppliers are included in the applicable risk-, incident-, change- and continuity-management procedures.

Use of an external supplier does not remove Identyum's responsibility for functions stated to be within the scope of the ID Wallet service.

The supplier's role, data access, service dependency, security obligations, incident duties, continuity measures and evidence are documented and reviewed. Outsourcing does not transfer Identyum's responsibility for its Wallet-related obligations.

10.5. Access, Cryptographic and Data-Security Controls

Identyum records relevant tangible and intangible assets, information assets and human resources in the Asset Register. Each recorded asset is assigned an owner responsible for its identification, classification, use, protection and lifecycle management.

Assets are classified according to their importance to confidentiality, integrity, availability and personal-data protection. Assets supporting regulated or trust-service functions are additionally identified within the scope of the relevant service.

Physical access to critical server, network and cryptographic equipment is restricted to authorised persons. The identity, time and purpose of access are recorded. Where equipment is located at an external data-centre provider, access to Identyum-owned equipment remains subject to Identyum approval and oversight. Physical areas containing critical equipment are monitored by appropriate security controls, including access logging and video surveillance.

Technical controls include controlled administrative access, encrypted communications, network segmentation, firewalls, security monitoring and separation of critical cryptographic components from general application services.

The public description of those controls is intentionally limited. Detailed security zones, network addresses, monitoring configurations, access methods and system diagrams are maintained

in confidential documentation. The existing architecture separates production services into protected zones and provides redundant service components for availability and recovery.
Access to active Wallet content, authentication data, biometric representations and separately retained identity or trust-service evidence is restricted by role and purpose. Administrative access and sensitive actions are logged and are subject to the applicable segregation and review controls.

10.6. Change and Configuration Management

Software and infrastructure changes are governed by separate controlled procedures.
Identyum maintains independent development, test and production environments. A change is not introduced directly into production without prior testing and approval, unless an emergency procedure is required to address an immediate security or availability risk.
Software changes follow a controlled path that includes source-code management, peer review, deployment to the development environment, functional testing, testing in the test environment and authorised production deployment. Build and deployment versions can be identified, and deployable previous versions are retained where necessary for rollback.
Infrastructure changes are assessed for scope, risk, expected effect, possible downtime and rollback. Regular and emergency changes require authorisation appropriate to their urgency and risk. Production changes are first tested in the test environment and, where possible and applicable, also in the development environment.
Before a production change, affected process owners and, where necessary, Business Clients are notified of expected downtime, temporary service restrictions or required integration actions.
Following deployment, Identyum verifies that the affected service operates correctly. Failed changes are reversed or corrected using the prepared rollback mechanism.
A Wallet change that modifies the interface to Identify, introduces an authentication factor, changes the data model or PID presentation, introduces a new related service or external status assertion, changes the signing-authorisation flow or materially affects privacy requires a documented impact assessment and coordinated update of the affected documentation.

10.7. Logging, Evidence and Record Keeping

Identyum maintains records sufficient to evidence and reconstruct security-relevant and operationally significant ID Wallet events.
Depending on applicability, the records include:

Area	Examples
Wallet creation and PID link	Account identifier, establishment of factors, Identify transaction reference, receipt of the result and storage/linking choice; excluding identity-proofing evidence and decision
Wallet lifecycle	Creation, activation, suspension, reactivation, revocation and closure
Authentication factors	Adding, replacing and removing factors and devices
Authentication and sharing	Relying Party, transaction, credential, User decision and disclosed scope
Credential lifecycle	Issuance, status changes, expiry and revocation
Administration	Privileged access and configuration and deployment events
Support and incidents	User reports, communication, escalation, investigation and resolution

Records identify the relevant time, action, object, initiator or automated process and result. Where necessary, they also identify the policy, software version or configuration in effect at that time.

Audit and evidence records are protected against unauthorised access, modification and deletion. Access is restricted to personnel with a justified operational, security, legal or audit need.

The Wallet evidence model distinguishes account creation, establishment of factors, initiation of Identify, receipt of a result, the choice to store/link PID, authentication, PID presentation, authorisation of a related service and lifecycle events. Identity-proofing, subscriber, certificate, signature and certificate-status evidence is maintained separately in the applicable systems and documentation.

10.8. Retention and Secure Disposal

The retention period is determined according to the record category, legal purpose and applicable service. The retention period applicable to QTSP evidence does not automatically apply to ordinary Wallet content and general Wallet records.

Record Category	Working Retention Model
QTSP evidence concerning identity, the Subscriber, certificates and signatures	Ten years under the applicable TSPS and controlled retention schedule.
General operational and security records not included in QTSP evidence	Three years, unless another legal, incident-related or evidentiary requirement applies.

Record Category	Working Retention Model
Active Wallet content	For the period necessary for the Wallet function and in accordance with the Wallet Privacy Policy and deletion rules.
Security-incident records or records subject to a legal hold	For the applicable period connected with the incident, limitation period, regulatory requirement or legal hold.

After expiry of the applicable period, records are securely deleted, anonymised or rendered permanently inaccessible, unless continued retention is required by a lawful hold or another documented basis.

10.9. Monitoring and Incident Management

Identyum monitors relevant events in the application, infrastructure, network, authentication and privileged access to detect failures, unauthorised activities, fraud indicators and security incidents.

Monitoring includes log review and automated detection through security controls implemented in the relevant system zones.

Events are assessed according to their potential impact on confidentiality, integrity, availability, authenticity, Users, Business Clients and regulated services.

Monitoring also supports vulnerability management. Identified vulnerabilities are assessed according to severity and affected systems and are remediated, mitigated or formally managed according to risk.

Detailed detection rules, alert thresholds and monitoring architecture are confidential.

Every employee or other authorised user of the information system must report a suspected incident. Users and Business Clients may report a suspected problem through the established customer-support channels, from which potentially serious matters are escalated to the responsible security or technical function.

Incidents are classified as low, medium or high according to their operational and security impact. Incidents affecting critical identity, Wallet authentication, credential-status, cryptographic or evidence functions may be classified as high even if the broader platform remains available.

The incident-management lifecycle comprises:

1. preparation;
2. identification and classification;
3. containment;
4. eradication;
5. recovery; and

6. reporting and lessons learned.

Containment takes priority where continued operation could increase harm. Recovery includes verification and testing before the affected component is returned to production.

If an incident affects personal data, service integrity or regulated functions, Identyum assesses the need to notify affected Users, Business Clients and competent authorities within the applicable statutory or contractual time limits.

Every significant incident is documented. The post-incident review identifies the cause, the effectiveness of the response and any corrective or preventive controls required to reduce the risk of recurrence.

Incident-response actions distinguish between Wallet suspension, factor blocking, key-use blocking and certificate revocation. Certificate suspension is not used as an incident-response status.

10.10. Business Continuity and Disaster Recovery

Identyum maintains continuity and recovery measures for services and components whose unavailability could materially affect ID Wallet functions.

Continuity measures include protected backups, redundant or recoverable infrastructure, restoration procedures, alternative means of communication and defined recovery responsibilities.

Critical application and security components operate with primary and secondary service capabilities. Relevant data and service components are synchronised or replicated to support continued operation or recovery after failure of the primary environment.

Following an incident or disaster, systems are restored from approved sources or backups, necessary updates and security patches are applied, and the resulting configuration is tested before production use resumes.

Restoration does not reinstate a Wallet or credential that was validly revoked, expired or terminated before the interruption.

Recovery priorities take account of the integrity and status of Wallet authentication, Relying Party transactions, protected Wallet content and dependencies on related trust services. A recovered component is returned to service only after its security and data consistency have been verified.

10.11. Service Termination

Identyum maintains measures for the orderly termination of the ID Wallet or a related eID function.

The termination procedure covers:

- cessation of the issuance of new Wallets or credentials;

- notification of Users, Business Clients and competent authorities;
- handling of active Wallets, Wallet functions and related credentials and sessions;
- preservation of legally required evidence;
- export, return or deletion of supported User data;
- termination of supplier and administrator access; and
- continued availability of information necessary to interpret previous transactions.

In the event of planned termination, Users are, where reasonably possible, notified sufficiently in advance and given instructions on available data-export or replacement options.

Termination of related certificates, trust services or remote-signing functions is further governed by the applicable Certificate Policy and Trust Services Practice Statement.

Termination planning includes consequences for active Wallets, notification of Users, access to or export of data eligible for export, deletion of active content, protection and retention of evidence, and revocation of linked long-term ANSign, NAuth and QNSign certificates when Wallets are permanently closed.

10.12. Audit and Conformity Assessment

Identyum reviews the operation of the ID Wallet through management oversight, risk reporting, internal controls and audits.

Risk-management activities are carried out at least annually, with additional assessments following significant changes. The overall business-risk-management framework is independently reviewed at planned intervals.

Audits may examine, among other matters:

- compliance with this Practice Statement;
- implementation of security and privacy controls;
- access and segregation of duties;
- asset and supplier management;
- software and infrastructure changes;
- incident-management and continuity procedures; and
- completeness and protection of evidence.

Findings are assigned to responsible persons and tracked until corrective action has been completed and verified.

Independent conformity assessments or certification audits are performed where required by the legal framework, an applicable standard or a specific assurance claim made by Identyum. Identyum publishes a claim concerning an LoA, certification or regulatory conformity only for a scope and production configuration that have been formally assessed and approved.

An audit within the scope of a trust service does not automatically certify the Wallet as an electronic identification means or a European Digital Identity Wallet. Any such claim requires a separately applicable assessment and approval.

11. User Information, Privacy and Legal Matters

11.1. Published Service Definition

Identyum publishes sufficient information to enable a prospective User to understand the principal characteristics of the ID Wallet before entering into the service relationship.

The published information includes, as applicable:

- Identyum's identity and contact details;
- the main ID Wallet functions;
- the conditions for creating and using a Wallet;
- mandatory authentication factors;
- the relationship between the Wallet, PID, eID credentials and related trust services;
- applicable fees;
- principal security precautions;
- the suspension, revocation and termination procedure;
- information on privacy and User rights; and
- available support and complaint channels.

Information is provided through this Practice Statement, the Terms of Use, the Privacy Policy, the service interface and other applicable disclosure documents.

Information intended for Users is written in a form that should be understandable without access to Identyum's confidential technical or security documentation.

Where a related service is provided under separate terms, the User is informed accordingly before requesting or using that service.

The published definition normatively describes the canonical TO-BE Wallet functions, clearly distinguishes authentication without identification from PID presentation, and separately identifies any status dependent on external conformity assessment, qualification, notification or regulatory approval.

11.2. Terms of Use

The contractual relationship for the ID Wallet is governed by the applicable Terms of Use together with the Privacy Policy and any additional terms accepted for optional or related services.

The User must be enabled to read and retain the applicable documents before accepting them. Acceptance is performed electronically and recorded together with the document versions and the time of acceptance.

The basic Wallet agreement takes effect only when the User has:

1. accepted the Terms of Use and the Privacy Policy;

2. successfully established the mandatory Wallet authentication factors; and
3. completed Wallet issuance.

Acceptance of a document without completion of Wallet issuance does not in itself create an active ID Wallet.

Each related eID function or trust service is subject to its own terms, profile and, where applicable, subscriber agreement and remote-signing rules. Acceptance and the request are recorded separately from the agreement for the basic Wallet.

Where the Terms of Use, Privacy Policy or another service-specific document regulates a matter in greater detail than this Practice Statement, the document hierarchy described in Section 1.6 applies.

The Wallet Terms of Use are separate from subscriber agreements for trust services. Where the Wallet is used to request a certificate package, the trust-service information, subscriber agreement and subsequent certificate acceptance are treated as separate stages described in Chapter 9.

11.3. Security Recommendations

Identyum provides Users with the information necessary for secure use of the ID Wallet.

The User is informed that authentication factors are personal and must not be transferred or made available to another person. Particular care must be taken to protect the Wallet PIN, registered devices, communication accounts and mobile authenticators.

Users are instructed to:

- keep devices and supported software reasonably secure and up to date;
- prevent unauthorised access to active Wallet sessions;
- verify the identity of the requesting Relying Party;
- review the requested data and transaction details before confirmation;
- suspend or revoke the Wallet without undue delay following suspected loss or compromise; and
- report suspected misuse or security incidents to Identyum.

Identyum may issue additional warnings or instructions where a particular threat, service change or incident creates an increased risk.

Security information published to Users does not disclose confidential monitoring logic, fraud thresholds, network configurations or other details that could weaken the service.

11.4. Privacy Notice and Data-Protection Roles

The Privacy Policy explains how Identyum collects and processes personal data connected with the ID Wallet.

It specifies, as applicable:

- the categories of personal data processed;
- the purposes and legal bases of processing;
- processing of authentication and biometric data;
- recipients and categories of recipients;
- international data transfers;
- retention principles;
- security measures;
- User rights; and
- the available privacy contact and complaint channels.

Privacy information is provided before the User creates a Wallet and remains publicly available throughout the service relationship.

Where a new function introduces a materially different processing purpose, data category, recipient or legal basis, the User receives the relevant information before that function is enabled.

The Privacy Policy forms part of the contractual documentation but remains the authoritative document for a detailed description of personal-data processing.

Identyum acts as controller for processing necessary to provide and manage the ID Wallet service, including Wallet enrolment, authentication-factor management, security, support and Wallet lifecycle actions.

Its role may differ for a related service.

Processing context	**Usual role**
Provision and management of the ID Wallet service	Identyum as controller
Identyum's own eID or trust-service functions	Identyum as controller, in accordance with the applicable service documentation
Identify process configured for a Business Client	Roles allocated according to the specific processing purpose and the agreement with the Client
Delivery of data to a Relying Party authorised by the User	The Relying Party generally becomes responsible for their subsequent processing upon receipt
External supplier supporting Identyum	The supplier acts under the applicable controller-processor relationship or another contractual relationship

A Business Client does not become the Wallet provider or controller for the Wallet merely because Wallet creation is offered within its integrated flow.

The same data may be processed by different parties for separate purposes and in separate legal roles. Those roles are determined by the actual processing activity, not by the technical fact that the parties use the same Identyum platform.

The Privacy Policy distinguishes Identyum's role as controller for the Wallet from its role, which may differ, in the context of a Business Client, Identify or a related trust service.

The Privacy Policy distinguishes AUTH-D biometric enrolment for an empty Wallet from biometric identity proofing, active Wallet content from separately retained evidence, and Identyum's own activities as controller from processing performed for a Business Client.

11.5. User Control, Authorisation and Rights

The User always decides directly whether to establish an ID Wallet relationship and accept its terms. A Business Client may define the terms of its own service or offer the Wallet in its flow, but may not create a Wallet, accept the terms or manage Wallet content on the User's behalf.

Each sharing of data through the Wallet requires a separate permitted action by the User.

Each data-sharing transaction identifies the Relying Party and the requested data. The User's approval is limited to that recipient, scope and transaction and does not constitute general access to the Wallet.

Separate consent or other applicable User authorisation or acceptance is obtained where required for:

- processing biometric data;
- a related eID function or trust service for which the governing document requires separate authorisation or acceptance;
- disclosure of Wallet data to a Relying Party;
- marketing or other optional communications; and
- another processing activity for which consent or another applicable User authorisation is the applicable legal basis.

Where processing is based on consent or another applicable User authorisation, the User may withdraw it in accordance with the Privacy Policy. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

A function that technically or legally depends on withdrawn consent or another applicable User authorisation may become unavailable. In particular, the Wallet cannot remain active without the mandatory facial-biometric factor required by this Practice Statement.

Consent is not used as a substitute for another legal basis where processing is necessary to perform the Wallet agreement, comply with a legal obligation, protect the service or maintain mandatory evidence.

Subject to the conditions and limitations of applicable law, the User may exercise rights concerning personal data processed by Identyum, including the right to:

- information and access to personal data;
- rectification of inaccurate or incomplete data;
- erasure where continued processing is not justified;
- restriction of processing;
- object to processing based on legitimate interests or direct marketing;
- withdraw consent or another applicable User authorisation;
- receive applicable data in a portable format; and
- lodge a complaint with the competent supervisory authority.

A request concerning data stored as active Wallet content may also require authentication of the User through the Wallet, particularly where disclosure, modification or deletion could affect identity, security or related credentials.

Verified PID attributes are not converted into self-declared data merely because the User requests rectification. Rectification must be supported by an approved source or verification procedure.

Erasure rights do not require Identyum to erase evidence that must be retained under a legal obligation, certificate policy, trust-service rule, requirement for the defence of legal claims or another lawful retention basis.

Requests are handled through the privacy and support contacts published by Identyum. The Privacy Policy describes access, rectification, erasure and related rights in greater detail.

Exercise of personal-data-protection rights does not require deletion of records that must be retained under an applicable legal obligation or that are necessary for the establishment, exercise or defence of legal claims. Any limitation is explained in accordance with the applicable Privacy Policy and law.

11.6. Fees

Creation, storage and ordinary use of the ID Wallet are provided to the User without a separate Wallet issuance or subscription fee under the current publicly disclosed service model.

A related trust service, transaction, Business Client service or other optional function may be subject to a separate fee under its applicable terms. A fee payable by the User is clearly disclosed before the User requests the chargeable service and does not arise merely from the availability of the Wallet.

Fees payable by a Business Client, Relying Party or another legal person are governed by the relevant commercial agreement and do not alter the Wallet fee information intended for the User.

11.7. User Responsibilities

The User provides accurate information and must not knowingly use false, altered or unlawfully obtained identity evidence.

The User is responsible for:

1. personal use of the Wallet solely for lawful purposes;
2. protecting authentication factors and registered devices;
3. reviewing requests before confirming authentication or disclosure;
4. maintaining contact details and factors under the User's control where required;
5. correcting or refreshing outdated data through a supported procedure;
6. reporting suspected unauthorised use without undue delay; and
7. complying with security instructions and lifecycle procedures.

The User must not circumvent service controls, interfere with Identyum systems, automate unauthorised access, introduce malicious code, reverse-engineer protected components or use the Wallet to impersonate another person.

Failure to comply with obligations may result in rejection of a transaction, suspension or revocation of the Wallet, termination of a credential or termination of the agreement.

The Terms of Use require personal use, accurate information, protection of authentication factors and reporting of suspected compromise without undue delay.

The User must not represent an empty-Wallet authentication result as a verified civil identity or transfer control of the Wallet, authentication factors or transaction approvals to another person.

11.8. Relying Party Responsibilities

A Relying Party may use the ID Wallet only under an applicable agreement or approved integration relationship.

It must identify itself accurately and request only the authentication level and data reasonably necessary for the stated purpose.

Before relying on a result, the Relying Party must verify, as applicable:

- the issuer and integrity of the result;
- the intended audience and transaction binding;
- the validity and status of the result;
- the Wallet authentication mode and any separately applicable credential assurance level;
- the PID LoIP;
- the provenance and freshness of the data; and
- any limitations stated in the result.

The Relying Party is responsible for lawful processing and protection of the data after receipt. It must not reuse data or authentication results beyond the authorised purpose unless another legal basis permits such processing.

A Relying-Party-specific pseudonym may be used only within the domain for which it was issued. Relying Parties must not attempt to link their identifiers with identifiers issued to another party or derive Identyum's internal Wallet identifier.

The Relying Party remains responsible for its final decision to grant access, conclude a transaction or accept the presented identification data.

A Relying Party receiving a pseudonymous authentication result without identification must not infer a civil identity, PID LoIP or formal eIDAS LoA that is not expressly contained in the result.

11.9. Identyum Responsibilities and Limitations

The User receives a personal, non-transferable right to use the ID Wallet in accordance with the applicable documentation and law.

The Wallet may be used only by the natural person to whom it was issued. It must not be transferred, shared, sold or made available to another person.

The Wallet and its authentication results do not guarantee that every Relying Party will accept:

- a particular PID;
- the stated LoIP;
- a particular eID credential;
- the achieved Wallet authentication mode or separately expressed assurance level; or
- the Wallet as sufficient for a particular legal or business purpose.

The Relying Party remains responsible for determining its own evidentiary, regulatory and risk requirements.

Unless expressly stated otherwise, the ID Wallet is not an identity document issued by a public authority, a notified national eID means or a European Digital Identity Wallet.

The User must not represent the Wallet, PID or a credential as having a status, assurance level or legal effect greater than that expressly stated by Identyum.

Identyum is responsible for providing the ID Wallet in accordance with the applicable agreement, this Practice Statement and mandatory law.

Identyum applies reasonable technical and organisational measures to protect the service but does not guarantee uninterrupted availability or error-free operation of every external system, device, network or Relying Party.

Identyum is not responsible for decisions made independently by a Relying Party, including a refusal to accept a PID or authentication result, unless Identyum generated the relevant result incorrectly.

Identyum's liability may be limited for loss resulting from circumstances beyond its reasonable control, including:

- misuse or disclosure of authentication factors by the User;
- an insecure or compromised User device;
- inaccurate data provided by the User or an external source;
- failure by a Relying Party or third-party service to fulfil its obligations;
- telecommunications or internet interruption; and
- force majeure events.

No limitation excludes liability where exclusion is prohibited by applicable law. Mandatory consumer rights and liability arising from intent, gross negligence or another basis that cannot lawfully be excluded remain unaffected.

Detailed contractual limitations are set out in the applicable Terms of Use.

Any limitation or allocation of liability is subject to mandatory law and the applicable Terms of Use. This Practice Statement does not in itself create a financial guarantee, transaction-value recommendation or service-level commitment.

11.10. Support and Security-Event Reporting

General Wallet support is available through support@identyum.com and the support channels published for the Wallet service. Users may use those channels to report loss, access problems, suspicious activity or other Wallet incidents.

Certificate, revocation and other trust-service matters are reported through trust@identyum.com or the service-specific channel stated in the applicable trust-service documentation. Internal routing of messages from those addresses does not alter their public purpose.

11.11. Complaints and Dispute Resolution

Complaints are handled under the applicable published complaints procedure and the Terms of Use. Identyum records the complaint, acknowledges its receipt through an available contact channel and provides a reasoned response within the applicable period.

Nothing in the complaints procedure limits mandatory consumer, regulatory or judicial remedies or remedies relating to personal-data protection. A complaint concerning a related third-party service may be forwarded to or coordinated with the responsible provider where permitted and necessary.

11.12. Governing Law

The ID Wallet agreement and this Practice Statement are governed by the law of the Republic of Croatia, subject to any mandatory consumer-protection or other rules applicable to the User irrespective of the contractual choice of law.

Before commencing judicial proceedings, the parties will endeavour to resolve a dispute through support, a complaint or another appropriate amicable procedure.

If a dispute cannot be resolved amicably, jurisdiction is determined in accordance with applicable law and the provisions of the Terms of Use.

A contractual jurisdiction clause does not deprive a consumer of any mandatory right to bring proceedings before another competent court under applicable consumer law.

The Terms of Use specify Croatian law and provide for prior amicable dispute resolution.

11.13. Notification of Changes

Identyum may update the ID Wallet service, this Practice Statement, the Terms of Use, the Privacy Policy or another applicable document.

A change is assessed according to its impact on:

- User rights and obligations;
- data processing;
- security and authentication;
- supported credentials and assurance claims;
- service availability;
- fees; and
- functions of related trust services.

The current version and effective date of each public document are published through the applicable Identyum channel.

Users are notified of significant changes through the registered email address, the ID Wallet notification channel or another appropriate electronic method. The notice describes the nature of the change and, where applicable, its effective date and any action required from the User.

A change requiring new consent or acceptance does not take effect for the affected optional function until the User gives the required confirmation. If a mandatory service change cannot be accepted, the User may terminate or revoke the Wallet in accordance with the applicable lifecycle and retention rules.

Urgent security changes may take effect before regular notice if delay would expose Users, Relying Parties or the service to material risk. The User is notified subsequently as soon as reasonably possible.

The Terms of Use require electronic notification of material changes to the service or rules and provide for publication of amended contractual documents.

A material change affecting Wallet creation, authentication results without identification, use of PID, lifecycle consequences or choices concerning related trust services is reflected in the applicable public documents before or when the changed practice takes effect, subject to urgent security measures.

Annexes

Annex A — Canonical Functions and Regulatory-Status Boundaries Matrix

Component or capability	Canonical functional status	Assurance or regulatory-status claim
Empty Wallet	Basic Wallet function	Authentication and authorisation context only; no PID, civil identity, eID-means claim or eIDAS LoA.
Pseudonymous B2B login	Wallet function for contracted integrations	Relying-Party-specific Wallet identifier and authentication context; not electronic identification of a civil identity.
Identyum PID	Result of a separate Identify service; optionally available through the Wallet	Product-specific structured identity result with a LoIP assigned by Identify; not an EUDI Wallet PID.
PID presentation	Wallet function where PID is available through a copy or secure reference	Selected attributes, provenance, LoIP and freshness information are disclosed following separate User authorisation.
ANSign	Separate trust-service profile under the CP/TSPS	Availability and eligibility are determined by the CP/TSPS and external conditions; storage of a PID does not issue a certificate.
NAuth	Separate certificate profile under the CP/TSPS	An authentication certificate is not, by that fact alone, a notified eID means, nor does the Wallet assign it an LoA.
QNSign	Separate qualified profile, subject to completion of all external conditions	The Wallet may form part of the authentication/authorisation interface; qualified status and sole control are evidenced by the applicable TSPS/SSAS scope.
COL-C / COL-D	Identify service mechanisms; outside the normative scope of the Wallet PS	Their use cases, evidence and LoIP are governed by the Identify documentation/TSPS, not by this Practice Statement.
Identyum SMS / WEB / MOBILE	Separate eID credentials or profiles; outside the normative scope of the Wallet PS	Availability and any LoA are determined by their own profile and external approval, not by the Wallet.
European Digital Identity Wallet	External regulatory status not claimed by this document	Identyum does not claim EUDI Wallet status.

Annex B — Authentication Requirements by Action

Action	Default Wallet authentication	Important limitation
Creation of a new Wallet	AUTH-A + AUTH-D during a single valid enrolment session	AUTH-D does not prove civil identity or issue a PID.
Pseudonymous B2B login	AUTH-A + an approved second factor	No PID or eIDAS LoA unless separately established and disclosed.
Adding or modifying PID data	AUTH-A + AUTH-D; a stronger mode may add AUTH-E	Identity proofing or validation is separate from Wallet authentication.
Presentation of PID attributes	AUTH-A + AUTH-D or AUTH-E, as permitted	A separate data request and User authorisation are required.
Changing a factor	As defined by the controlled authentication policy	Unavailable factors may require suspension, recovery or replacement.
Wallet suspension	Approved authentication for suspension or a risk-based action by Identyum	Certificate status remains unchanged solely because of Wallet suspension.
Wallet reactivation	Approved combination for reactivation and any required review	Does not reinstate an expired or revoked certificate.
Permanent Wallet closure	Approved permanent-termination procedure	Linked long-term ANSign, NAuth and QNSign certificates are revoked.
QNSign/QES authorisation using AUTH-E	Online push challenge-response procedure	Offline TOTP is not an available QES activation method.

Annex C — Wallet, PID, Certificate and Key Lifecycle Matrix

Event	Effect on Wallet/PID	Effect on certificate/key
Wallet creation	Empty active Wallet; no PID unless separately issued and stored	No certificate unless separately requested, issued and accepted.
PID issued but storage declined	The Wallet remains empty; the PID may be used for the immediate transaction	An eligible certificate may still be requested using separately retained evidence.
PID stored	The PID becomes active Wallet content	No automatic certificate issuance.
PID is outdated	Reuse or disclosure may require refresh or enhanced verification	The status of an existing certificate remains unchanged; new evidence may be required for a new issuance or transaction.
PID removed	The PID is no longer available as Wallet content	The status of existing ANSign, NAuth and QNSign certificates remains unchanged solely because of the removal.
Wallet is suspended	Wallet actions are temporarily blocked	Wallet-based key use is blocked; certificate status remains unchanged.
Wallet is reactivated	Permitted Wallet actions resume	Use resumes only if the certificate/key and all other dependencies remain valid.
Wallet permanently closed	The Wallet cannot be reactivated	Linked long-term ANSign, NAuth and QNSign certificates are revoked; this event does not in itself affect QLSeal.
Certificate expired or revoked	The Wallet and PID may remain active	The affected certificate and its permitted key use cease.
Use of a managed key is blocked during an investigation	The Wallet may be suspended separately where appropriate	Key operation is blocked; certificate status remains unchanged until a revocation decision is made.

Annex D — Authentication-Without-Identification and PID-Disclosure Results Matrix

Result element	Authentication without identification	Authentication with PID disclosure
Identyum issuer identity	Included	Included
Intended audience / Relying Party	Included	Included
Transaction and time binding	Included	Included
Relying-Party-specific pseudonymous identifier	Included where required	May be included where required
Wallet Authentication Mode	Included or specified by reference	Included or specified by reference
Civil name or national identifier	Not included	Included only if requested, available and authorised
PID LoIP and provenance	Not included	Included to the extent necessary for interpretation and reliance
Formal eIDAS LoA	Not included	Not included unless expressly provided by a separate applicable eID credential
Other Wallet content	Not included	Not included outside the authorised data scope

Annex E — Evidence and Retention Matrix

Event or record	Minimum evidentiary purpose	Applicable retention category
Wallet creation	Account identifier, acceptance of the Terms of Use, factor establishment and activation	Wallet contractual/security record under the applicable retention schedule
Identify process and PID issuance	Sources, checks, binding, decision, LoIP and issued result; maintained by Identify or the QTSP evidence system, not the Wallet	Identify or QTSP evidence category under the governing TSPS; outside active Wallet content
PID storage choice	Displayed data and the User's “store/skip” action	Wallet evidence; linked to identity evidence where applicable
Request for a related trust service	Exact profile, referenced documents, User action and transaction reference; the full subscriber evidence is maintained by the trust service	QTSP Subscriber/certificate evidence — ten years
Certificate acceptance or activation	Certificate content, serial number/profile, acceptance action, time and result	QTSP certificate evidence — ten years
Wallet authentication	Relying Party, transaction, factor categories, outcome and assertion metadata	General record or higher-category evidence according to purpose
PID presentation	Recipient, purpose, scope, authorisation and attributes delivered	Wallet/privacy evidence or regulated-transaction evidence, as applicable
Wallet suspension, reactivation or closure	Initiator, authentication, reason, decision, notice and result	Wallet lifecycle/security evidence
Certificate revocation	Request/report, verification, decision, status publication and notice	QTSP certificate evidence — ten years

Where the same record supports multiple categories, the longest applicable lawful retention period and the strictest applicable access control apply, without extending the availability of the active Wallet.

Annex F — Regulatory Applicability and Governing Documents Matrix

Source of requirement	Primary area and governing document	Relationship to the Wallet PS
Commission Implementing Regulation (EU) 2015/1502	Notified electronic identification schemes and means; governing eID-scheme documentation	Selected principles inform the design; neither the Wallet nor an authentication mode has an LoA without a separate, formally assessed eID scheme.
ETSI TS 119 461	Identify/identity-proofing service; TSPS for use in trust services and Identify documentation for other contexts	OVR-6.1-02/-03 and COL-8.2.1-06X are satisfied by identifying the use cases, evidence sources and context in the governing Identify/TSP practice, not in the Wallet PS.
ETSI EN 319 401	General requirements for a TSP and its practices; TSPS and the TSP management system	Applies to the Wallet only as a component within the scope of a particular trust service; it does not apply to all Wallet functions.
ETSI EN 319 411-1 and ETSI EN 319 411-2	Certificate policies, registration, issuance and lifecycle; CP and TSPS/CPS	The Wallet governs the user interface and authentication/authorisation; it does not determine certificate profile, eligibility or status.
ETSI TS 119 431-1	SSAS, SAD, sole control and remote signing; TSPS and remote QSCD/SSAS documentation	The Wallet may convey an authentication result and transaction confirmation; it is not itself a QSCD and does not by itself evidence QES requirements.
ETSI TS 119 472-2 and ETSI TR 119 462	EUDI Wallet, EAA and EUDI PID/presentation context	Informative for interoperability where expressly applied; this does not make the product-specific Identyum PID an EUDI PID.
Article 5a of eIDAS and EUDI Wallet implementing acts, including (EU) 2024/2979	EUDI Wallet status, certification and Relying Party ecosystem	This Practice Statement does not claim EUDI Wallet status; such a claim is permitted only after all prescribed external procedures have been completed.

Source of requirement	Primary area and governing document	Relationship to the Wallet PS
Regulation (EU) 2016/679 (GDPR)	Processing of personal data; Privacy Policy and documentation of the specific processing	Roles and legal bases are determined according to the actual purpose and activity of the Wallet, Identify, the TSP and the Relying Party.