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 **Approving Authority**: Identyum CEO **Public Repository**: https://identyum.com/terms-policies/	**Service Provider**: Identity Consortium d.o.o. **Registered Address**: Trogirska ulica 2, 42000 Varaždin, Croatia **Company Registration Number**: 070166678 **Personal Identification Number (OIB)**: 44867795324 **General Contact**: info@identyum.com **User Support**: support@identyum.com

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	Clean replacement reflecting the modular Wallet, PID, authentication and connected trust-service model; alignment with and the current production scope.

Version 2.0 is issued as a complete replacement version. Therefore, changes are not individually highlighted YELLOW as usual.

SADRŽAJ

1. General Information

1.1. Purpose of the Document

This Identyum ID Wallet Practice Statement, hereinafter referred to as the Practice Statement, describes the practices implemented by Identity Consortium d.o.o., hereinafter referred to as Identyum, for the provision, operation, security and lifecycle management of the Identyum ID Wallet service.

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

In particular, this Practice Statement describes:

a) creation and use of an ID Wallet without stored identity data;
b) optional identity proofing, issuance of an Identyum PID and the separate User choice whether to store it in the Wallet;
c) establishment and management of Wallet authentication factors;
d) authentication and authorisation through the Wallet, including pseudonymous authentication without a civil-identity assertion;
e) controlled presentation of PID attributes to Relying Parties;
f) the interfaces between the Wallet and Identyum Identify and trust services;
g) the separate lifecycles of 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 Identyum CEO and is binding on Identyum to the extent that it describes practices which Identyum undertakes to implement.

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

Unless expressly stated otherwise, publication of this Practice Statement does not constitute a claim that the ID Wallet is a European Digital Identity Wallet, is issued under a notified national electronic identification scheme, or meets the requirements for assurance level Low, Substantial or High.

1.3. Scope

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

The scope covers the Wallet account, its verified contact identifier, authentication factors, supported interfaces, Wallet content, User instructions, Relying-Party interactions, lifecycle events and the records necessary to operate and evidence those functions.

Where the Wallet is used to request, activate or authorise a connected trust service, this Practice Statement governs the Wallet-side interaction. The certificate, private key, remote QSCD and trust-service lifecycles remain governed by the applicable Certificate Policy, Trust Service Practice Statement, 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 Identyum Identify and a Business Client's final onboarding, KYC, AML or access decision;
j) detailed identity-proofing mechanisms, biometric thresholds and evidence 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 other than the Wallet-side User interaction;
n) qualified electronic timestamps;
o) legal-person electronic identification and the lifecycle of QLSeal certificates;
p) future COL-C, COL-D, Identyum SMS, WEB, MOBILE, NIAS or C2G capabilities that are not part of the current production scope; and
q) European Digital Identity Wallet functions not expressly declared as part of the Identyum service.

1.5. Intended 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 evaluators;
f) supervisory, regulatory and competent authorities;
g) Identyum personnel responsible for the governance, 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-facing instructions, accessibility guidance, contextual notices, consent screens or customer-support materials.

1.6. Documentation Hierarchy and Precedence

This Practice Statement forms part of the Identyum controlled-documentation framework. Applicable legislation prevails over all Identyum documents. The Wallet Terms and Conditions govern the contractual Wallet relationship; the Wallet Privacy Policy governs the description of personal-data processing; and this Practice Statement governs the operational practices of the Wallet service.

For connected trust services, the applicable Certificate Policy, Trust Service Practice Statement, service profile, disclosure statement and trust-service Terms and Conditions prevail for certificate, key, signature and trust-service matters. A more specific applicable document prevails over a more general document for the matter it regulates.

This hierarchy is not a substitute for consistency. Identyum maintains the relevant documents so that known material contradictions are removed and the applicable requirements can be reconstructed from the published and controlled documentation set.

1.7. Applicable Legislation, Standards and Guidance

1.7.1. European Union and Croatian Legislation

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

Commission Implementing Regulation (EU) 2015/1502 is used as the primary assurance-structure reference for 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-claim design guidance where Identyum expressly adopts a compatible principle.

1.7.2. Standards and Technical Specifications

ETSI TS 119 461 applies to identity-proofing processes used for an Identyum PID in the scope stated by the TSPS. ETSI EN 319 401 and the applicable ETSI EN 319 411 standards apply to connected trust services in accordance with the relevant Certificate Policy and TSPS. ISO/IEC 27001, ISO/IEC 27002, relevant biometric standards and EN 301 549 are applied in the scope established by Identyum's management system, technical design and regulatory commitments.

A reference to a standard does not mean that every provision of that standard applies to every Wallet function. Exact applicability, versioning, evidence and exclusions are managed in the controlled compliance matrix and the governing service documentation.

1.7.3. Public and Internal Identyum Documents

Publicly applicable documents include the Wallet Terms and Conditions, Wallet Privacy Policy, this Practice Statement, the Identyum Trust Service Practice Statement, the Policies and Profiles of Identyum Trust Services and applicable service-specific disclosure statements.

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

1.8. Terms, Definitions and Abbreviations

Terms defined by applicable legislation and standards have the meaning given in those sources. The following product-specific distinctions are particularly important:

Term	Meaning in this Practice Statement
ID Wallet or Wallet	The Identyum service account, authentication context and protected data-management environment provided to a User.
Empty Wallet	An active Wallet with established authentication factors but without an Identyum PID or verified civil-identity assertion.
Identyum PID	Identyum's product-specific set of verified identity attributes, provenance and LoIP information resulting from an approved identity-proofing process. It is not represented as EUDI Wallet person identification data issued under Union or national law.
PID LoIP	The level of identity proofing assigned to an Identyum PID under the applicable Identyum identity-proofing rules. It is distinct from an eIDAS LoA.
Wallet authentication regime	The factor combination and transaction controls achieved for a Wallet operation. It is not, by itself, an eIDAS LoA.
Relying Party	A party that receives and relies on a Wallet authentication result, authorised PID attributes or another permitted Wallet output.
Business Client	An organisation contractually integrated with Identyum Identify, Wallet or connected services.
Connected 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 abbreviations AUTH-A through AUTH-E identify the authentication mechanisms defined in the controlled Wallet authentication documentation. ANSign, NAuth and QNSign identify separate certificate profiles defined by the applicable Certificate Policy and TSPS.

1.9. Document Administration, Approval and Change Management

The document owner coordinates periodic review, consistency with connected documentation, version control, approval and publication. Review is performed at least annually and following a material service, legal, security, architectural or scope change.

Each approved version identifies its version, effective date, owner, approving authority, public repository and change description. Superseded public versions are retained in the documentation archive in accordance with Identyum's controlled-documentation rules.

2. Identyum Wallet Service Model and Boundaries

2.1. Description of the ID Wallet Service

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

The Wallet is modular. Creation of a Wallet, issuance of a PID, storage of a PID, request for a certificate package, issuance of a certificate and activation of a certificate are separate events. Completion of one event does not imply that the User selected or completed another event unless the relevant User action and result were separately recorded.

2.2. Canonical Objects and Their Separation

Object	Primary function	Independent status or lifecycle
Wallet	Authentication, authorisation and protected data access	Active, suspended or permanently closed/revoked
Authentication factor	Verification of knowledge, possession, account control or inherence	Established, available, blocked, replaced or removed
Identyum PID	Verified identity attributes, provenance and LoIP	Issued, current, stale, updated, removed from Wallet or no longer available for reuse
Identity-proofing evidence	Proof of the procedure and result supporting PID or certificate issuance	Retained separately under applicable evidence rules
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 under the applicable key lifecycle

Logical or technical linkage between objects does not merge their legal or operational lifecycles. For example, removal of a PID from Wallet content does not delete the separately retained evidence for an existing certificate and does not, by itself, change that certificate's status.

2.3. Wallet Functional Modes

2.3.1. Empty or Authentication-Only Wallet

An empty Wallet contains no Identyum PID and makes no verified civil-identity claim. It may establish that the same Wallet authentication context is under the control of the person completing the required factors and may return an RP-specific pseudonymous identifier, transaction binding and achieved Wallet authentication regime.

An authentication-only result is not electronic identification within the meaning claimed for a notified eID scheme, does not carry an eIDAS LoA and must not be interpreted as confirmation of a civil name, national identifier, PID LoIP or other identity attribute.

2.3.2. Wallet with Stored Identyum PID

Where the User has successfully completed an approved identity-proofing process 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 Connected Certificate

A Wallet may authenticate and authorise use of a separately issued ANSign, NAuth or QNSign certificate even if the supporting PID is not stored as active Wallet content. Eligibility depends on the active Wallet, qualifying identity-proofing evidence, certificate status, key availability and the applicable profile requirements.

2.3.4. Future Electronic-Identification Credentials

Future eID credentials or integrations may be enabled only after the applicable technical, legal, assurance and documentation requirements have been implemented and approved. They are not part of the current production scope merely because they are technically contemplated or named in an internal roadmap.

2.4. Participants and Roles

The principal participants are the User, Identyum, Business Clients, Relying Parties, providers of connected trust services, external suppliers and the competent audit or supervisory bodies. One entity may perform more than one role, but responsibilities are determined separately for each function.

The Wallet contractual relationship is concluded directly between Identyum and the User. A Business Client may enable or disable the presentation of a Wallet offer in its integrated Identify flow, but it cannot create a Wallet or conclude the Wallet relationship for the User without the User’s affirmative choice.

2.5. Service and Technical Boundaries

The Identyum-controlled boundary includes the Wallet backend, authentication-factor records, protected Wallet content, server-side biometric verification, Relying-Party interfaces, status handling, monitoring and audit evidence. A supported User device provides an interface and may hold device-bound authentication material, but it 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 remote QSCD and trust-service boundary. The Wallet supplies the permitted authentication and transaction authorisation required to invoke that service.

2.6. Current Production Capabilities

The normative body of this Practice Statement describes only capabilities that form part of the approved production scope. These include empty Wallet creation, Wallet authentication, optional Identify initiation, optional storage and presentation of an Identyum PID, pseudonymous B2B login, and approved Wallet interactions with connected Identyum trust services.

Identity-proofing routes, authentication mechanisms, certificate profiles and signature functions are available only where they are separately declared as production-ready in the governing documentation and supported by the required operational evidence.

2.7. Future or Conditional Capabilities

COL-C identity proofing through an existing eID means, COL-D identity proofing through an existing electronic signature, and Identyum SMS, WEB and MOBILE credentials are outside the initial production scope. References to those concepts in design documentation do not constitute an availability or assurance commitment.

A future capability enters the scope only after change approval, implementation, security and conformity assessment as applicable, documentation alignment and publication of the relevant effective version.

2.8. Permitted and Prohibited Uses

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

The Wallet must not be used to impersonate another person, transfer control to an unauthorised person, circumvent security controls, provide false data, reuse an assertion

outside its audience or validity period, or represent an authentication-only result as verified civil identity or a formal eIDAS LoA.

2.9. Reliance Assumptions and Limitations

Users are expected to protect their devices and factors, review 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, 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 is accepted by every public or private service, replaces a government-issued identity document, is a notified eID means or is a European Digital Identity Wallet.

3. Wallet Application, Authentication-Factor Enrolment and Creation

3.1. Direct Initiation and B2B Wallet Offer

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

Presentation of an offer does not create a Wallet. Wallet creation begins only when the User affirmatively requests the Wallet and enters the 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 a User's choice within its own service, but it must not represent Wallet creation as an Identyum requirement where the User has not chosen to enter the Wallet relationship.

A declined or abandoned Wallet offer does not invalidate an otherwise completed Identify result and does not prevent the result from being used in the transaction for which it was obtained, subject to the applicable Business Client and identity-proofing rules.

3.3. Information, Wallet Terms and Privacy Notice

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

The User performs an explicit and recorded action accepting the Wallet Terms and Conditions. Acceptance of the Wallet relationship is separate from any later subscriber agreement or certificate-acceptance action for a connected 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, secure and operate the service. Identyum verifies the mobile number or e-mail address selected as the Wallet's unique account identifier before activation.

Identyum does not require identity-document data, a civil name or an identity-proofing result merely to create an empty Wallet. Data collected only to establish the Wallet account must not be described as verified civil-identity data.

3.5. Establishment of AUTH-A and AUTH-D

During creation of a new Wallet, the User establishes the following mandatory primary authentication factors within one connected enrolment session:

a) AUTH-A — the ID Wallet PIN, as a knowledge factor; and
b) AUTH-D — Identyum face biometrics, as an inherence factor.

All factors forming the enrolment event must be completed within the maximum connected-session duration defined in the controlled authentication policy. Failure to establish both mandatory factors prevents activation of the Wallet.

Supported additional factors may be established where available. Their addition does not replace the mandatory initial AUTH-A and AUTH-D enrolment and does not create a verified civil identity.

3.6. Meaning of AUTH-D in an Empty Wallet

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

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

3.7. Creation and Activation of the Empty Wallet

The Wallet is created and becomes active after the verified contact identifier has been bound 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 this activation.

An active empty Wallet may be used only for functions that do not require PID attributes or another separately established identity claim. It may authenticate Wallet control, provide an RP-specific pseudonymous login and authorise permitted connected operations.

3.8. Wallet Identifier and Uniqueness Rule

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

The rule is account-identifier based and not person based. A natural person who controls more than one verified mobile number or e-mail address may hold more than one Wallet. Identyum does not currently offer automatic or manual merging of separate Wallets.

The internal Wallet identifier is not disclosed as a common cross-client identifier. Relying-Party-specific pseudonymous identifiers are used where a stable private-sector login identifier is required.

3.9. Device and Authenticator Binding

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

Where AUTH-E or another device-specific authenticator is registered, the corresponding 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 Wallet authentication policy.

3.10. Enrolment Evidence and Audit Trail

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

The evidence demonstrates creation and control of the Wallet account. It must not be labelled as civil-identity proofing evidence unless an approved identity-proofing process was separately completed.

3.11. Failed, Interrupted and Repeated Enrolment

A Wallet is not activated where the User abandons the procedure, fails verification of the selected account identifier, fails to establish a mandatory factor, or does not complete the required acceptance action.

Retries, rate limits and cooling-off measures are applied in accordance with the controlled authentication and fraud-prevention rules. A failed empty-Wallet enrolment must not create a PID or be represented as an unsuccessful identity-proofing decision where no identity proofing was attempted.

4. Optional Identity Proofing and Identyum PID

4.1. User Choice to Add Identity Data

A User may select the option to add identity data to the Wallet or may continue using an empty Wallet. The option is separate from Wallet creation and may be selected during the initial flow or later while the Wallet remains eligible.

Selection of the option initiates or continues an Identyum Identify process. It does not guarantee that identity proofing will succeed, that an Identyum PID will be issued or that the User will choose to store the resulting PID in the Wallet.

4.2. Relationship with Identyum Identify

Identyum Identify performs the approved collection, validation, binding and decision activities necessary to produce an identity-proofing result. The detailed mechanisms, thresholds, accepted evidence, LoIP rules and evidence controls are governed by the current TSPS and controlled identity-mechanism documentation.

The Wallet receives only the result and data necessary for the User-selected Wallet function.

A Business Client remains responsible for its final onboarding or regulated decision and for specifying its required data, minimum LoIP, freshness and additional checks.

4.3. Direct, B2B and Transaction-Specific Identify Flows

An Identyum PID may result from an Identify process initiated directly through a Wallet interface, from an Identify process embedded in a Business Client flow, or from another approved Identyum process.

A Business Client flow may produce a transaction-specific or one-shot PID that is used for the current transaction without being stored for future Wallet reuse. If the Business Client's configuration permits a Wallet offer, a User without a Wallet may separately choose to create one after the successful Identify process.

4.4. Accepted Identity-Proofing Results

An Identyum PID is issued only where the complete approved identity-proofing procedure has reached at least Identyum PID LoIP Baseline and all mandatory decision criteria for the selected route have been satisfied.

Current production routes are limited to mechanisms that are implemented, approved and supported by the required evidence. COL-C identity proofing through an existing eID means and COL-D identity proofing through an existing electronic signature are not part of the initial production scope.

4.5. Collection, Validation and Binding

Identity attributes and evidence are collected from approved sources using the mechanisms applicable to the selected route. Identyum validates the evidence and relevant attributes, binds the evidence to the person completing the procedure, performs required cross-checks and records the outcome.

Use of facial biometrics in identity proofing is distinct from AUTH-D enrolment for an empty Wallet. Identity proofing may include liveness and comparison with an identity-document photograph or another approved reference; empty-Wallet AUTH-D does not.

Remote face capture, liveness and face comparison are subject to the approved retry controls. The current maximum is five attempts followed by a one-hour cooling-off period, with all enforcement and outcomes recorded as evidence.

4.6. Identity-Proofing Decision and LoIP

Identyum determines the identity-proofing outcome and, where successful, assigns the applicable Identyum PID LoIP under the current decision rules. The available Identyum PID levels are Baseline, Extended High, Extended Very High and Extended Highest.

LoIP expresses confidence in the identity-proofing result and its underlying evidence. It is not an eIDAS LoA and does not, by itself, determine the security or assurance of an electronic identification means or authentication transaction.

4.7. Issuance of Identyum PID

Following a successful qualifying decision, Identyum issues an Identyum PID containing the verified attributes, provenance, relevant verification outcomes, issuance time and LoIP information required for its permitted use.

The term Identyum PID is an Identyum product designation. It is not a representation that the data constitute person identification data issued under Union or national law for a European Digital Identity Wallet or notified electronic identification scheme.

4.8. Separation of PID Issuance and Wallet Storage

PID issuance and PID storage are separate events. Following issuance, the User is shown the principal verified attributes and is asked whether the PID should be stored or associated as active Wallet content.

Declining Wallet storage does not invalidate the PID or the underlying identity-proofing result. The result may still be used for the current Business Client transaction or for an eligible certificate request, and the evidence may be retained separately where required.

4.9. Independent Post-Identify Choices

After a successful qualifying Identify result, the User may independently decide whether to store the PID in the Wallet and whether to request the applicable long-term Identyum certificate package. Neither choice is conditional on selecting the other.

The interface must not obscure the independence of the two choices or describe the certificate package as an automatic consequence of PID storage. Each choice, the information displayed and the resulting action are recorded separately.

4.10. PID Reuse, Freshness and Step-Up

A stored or otherwise available prior PID may be reused only where its source, LoIP, age, status and attributes satisfy the requirements of the new use case and the reuse is permitted by the applicable service profile.

Where the available result is incomplete, stale or below the required level, Identyum may revalidate selected attributes, obtain current data, perform additional mechanisms or require a new identity-proofing procedure. A successful step-up creates a new or updated identity-proofing result and, where applicable, an updated PID.

4.11. Identity and Certificate Evidence Retained Outside the Wallet

Identity-proofing and certificate evidence required for auditability, legal defence or regulatory retention is stored separately from active Wallet content and is accessible only to authorised roles for permitted purposes.

Removal or deletion of PID from the Wallet does not delete evidence which Identyum is required or entitled to retain. Conversely, retained evidence is not available to the User or a Relying Party as active Wallet content merely because it remains in the evidentiary repository.

4.12. Failed and Manually Handled Procedures

Where mandatory checks cannot be completed or the result does not meet the applicable decision rules, the identity-proofing procedure ends without issuance of a qualifying Identyum PID. Identyum records the result and reason to the extent required by the applicable evidence and security rules.

Manual review or fallback may be used only where it is defined, authorised and evidenced for the applicable mechanism. Manual handling must not silently override a mandatory technical failure or assign a higher LoIP than the completed evidence supports.

5. Wallet Characteristics and Electronic-Identification Assurance Model

5.1. Empty Wallet as an Authentication Context

An empty Wallet is an authentication and authorisation context associated with a verified mobile number or e-mail address, an internal Wallet identifier and the Wallet authentication factors. It contains no Identyum PID and makes no verified civil-identity assertion.

The person controlling an empty Wallet may authenticate to Identyum or a contracted private-sector Relying Party under an RP-specific pseudonymous identifier. The result confirms successful Wallet authentication for the specified transaction; it does not identify the person by civil identity.

5.2. Authentication-Only Results

An authentication-only result may contain Identyum as issuer, the intended Relying Party or audience, an RP-specific pseudonymous identifier, time and validity information, transaction binding and the achieved Wallet authentication regime.

It must not contain or imply a civil name, national identifier, Identyum PID, PID LoIP or eIDAS LoA unless those data or claims were separately established, requested and authorised under an 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. Where Identyum later issues or enables a specifically defined eID credential, the applicable scheme documentation shall identify 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 carries no formal eIDAS LoA unless a specific approved eID scheme or integration expressly establishes that status.

5.4. Authentication Regime, PID LoIP and eIDAS LoA

Concept	What it expresses	What it does not establish by itself
Wallet authentication regime	Factors and transaction controls successfully completed for a Wallet operation	Civil identity, PID LoIP or eIDAS LoA

Concept	What it expresses	What it does not establish by itself
Identyum PID LoIP	Confidence in the identity-proofing result and evidence	Security of the authentication means or eIDAS LoA
Certificate profile	Permitted key and certificate purpose and policy requirements	Notification as an eID means
eIDAS LoA	Holistic assurance of an eID means across enrolment, means management, authentication and organisation	A result inferred solely from two-factor authentication or PID LoIP

Identyum does not map PID LoIP levels or Wallet factor combinations automatically to eIDAS Low, Substantial or High. Any future mapping requires a complete assessment of all applicable assurance elements and an express, controlled claim.

5.5. Authentication Factors and Categories

Reference	Authentication factor	Operational category
AUTH-A	ID Wallet PIN	Knowledge
AUTH-B	Verified mobile number and demonstrated control of the associated communication channel	Possession or channel control, as implemented for the operation
AUTH-C	Verified e-mail, Google or Apple account	External-account control
AUTH-D	Identyum face biometrics	Inherence
AUTH-E	Identyum mobile authenticator	Possession of a bound authenticator

AUTH-A and AUTH-D are mandatory for initial Wallet creation. Additional factors may be established and used only for operations for which the controlled authentication policy permits them.

5.6. Permitted Factor Combinations

The factor combination is selected according to the requested operation, the controlled Wallet authentication policy, the User's selected security setting, Relying-Party requirements and transaction risk. All factors forming one authentication event must be completed within the same permitted connected session.

Operation	Default requirement
Creation of a new Wallet	AUTH-A + AUTH-D

Operation	Default requirement
Addition or modification of identity data	AUTH-A + AUTH-D; AUTH-E additionally where the stricter regime applies
PID presentation or identity-data sharing	AUTH-A + AUTH-D or AUTH-E, subject to the applicable policy and User setting
Pseudonymous Wallet login	AUTH-A + an approved second factor for that transaction
Higher-risk Wallet operation	AUTH-A + AUTH-D + AUTH-E where required
QNSign/QES transaction authorisation using AUTH-E	Online push challenge-response only

A stronger factor combination may be required, but successful completion of a stronger combination does not by 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 Identyum-controlled server-side components. The server-side environment manages protected Wallet content, authentication records, biometric comparison, status, Relying-Party interactions and evidence.

A general-purpose User device remains outside Identyum's direct administration. Device-bound AUTH-E material is generated and protected for the registered authenticator and is not treated as 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 are purpose-specific. A key used for one function must not be represented or reused as a key for another profile merely because the functions share technical infrastructure.

End-user certificate private keys are generated and used through the controlled SAM/HSM architecture. Protected or wrapped private-key objects may be stored in controlled databases and backups but are not usable without the SAM/HSM protection environment. The User does not receive plaintext private-key material through the Wallet interface.

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 key-management and certified-device information remains in the TSPS and controlled procedures.

5.9. Protection Against Duplication, Tampering and Replay

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

A copied User interface or knowledge of a Wallet identifier is not sufficient to reproduce the Wallet authentication context. Use of the Wallet also requires successful verification of the applicable authentication factors and valid server-side factor or credentials.

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

Authentication transactions use short-lived session or challenge data and are bound to the requesting service and intended operation. Previously used one-time factor or credentials, challenges or authorisations cannot be reused as valid approval for a new transaction.

Relying-Party-specific pseudonymous identifiers additionally reduce the risk of tracking or correlation between different Business Clients.

Authentication requests and 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 a valid new authentication.

5.10. User Control and Possession

The User demonstrates control of the Wallet through the factor combination required for the operation. Approval is bound to the displayed recipient, purpose, transaction and data scope and must not be treated as general permission for another operation.

Control of a Wallet does not require direct possession of centrally protected certificate keys. Successful Wallet authentication and, where required, transaction-specific confirmation authorise only the permitted operation within the connected controlled service.

5.11. Protection of Stored Data and Privacy by Design

Wallet content, authentication records and biometric representations are protected in storage 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 operation.

Identyum uses RP-specific pseudonymous identifiers for authentication-only transactions to reduce unnecessary cross-client correlation. Authentication does not disclose PID data, and PID disclosure does not include additional Wallet content outside the authorised scope.

5.12. Regulatory Status and Non-Claims

The ID Wallet is not presented as a European Digital Identity Wallet, a government-issued identity document or a Wallet issued under a notified national electronic identification scheme. The Wallet's use of selected security, privacy and interoperability principles does not alter that status.

Identyum will publish any future formal eID credential, LoA, notification or conformity claim only after the relevant scope, scheme, evidence and approval have been established. No such status may be inferred from marketing terminology, factor count, PID LoIP or availability of a connected certificate.

6. Wallet and Connected-Object Lifecycle Management

6.1. Separate Lifecycle Objects and Statuses

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

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

6.2. Normal Use

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

Each security-sensitive operation requires the authentication combination defined for that operation. All factors forming one authentication event must be completed within the same connected session, which may not exceed 15 minutes.

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

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

An empty Wallet remains limited to authentication-only and authorisation functions. PID management and presentation become available only where a PID has been separately issued and stored or otherwise made available for the authorised transaction.

6.3. Authentication-Factor Management

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

Adding a mobile authenticator requires:

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

The User may register more than one mobile authenticator.

Removing a mobile authenticator requires the PIN and face biometrics. The same two-factor combination is required to add or remove a verified mobile number or an e-mail, Google or Apple account used as a Wallet authentication factor.

The PIN cannot be removed while the Wallet remains active. Changes to the mandatory PIN or face-biometric factor may be performed only through a specifically supported security procedure that preserves reliable binding to the User.

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

Blocking or removal of a Wallet factor affects operations that require that factor. It does not, by itself, suspend a certificate, because Identyum certificate profiles do not support certificate suspension.

6.4. Device Addition, Removal and Migration

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

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

The User may maintain multiple registered mobile authenticators. Each is managed independently and may be removed without removing the others.

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

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

The User accesses the existing Wallet from the new device and, where desired, registers a new mobile authenticator. Registration creates new device-specific cryptographic material and binds it to the existing Wallet.

Once the new authenticator is active, an earlier authenticator may be retained or removed in accordance with section 6.3.

Where the previous device has been lost or may be 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 another verified mobile number or e-mail address remains a separate Wallet with its own lifecycle.

6.5. Contact and Account-Identifier Changes

A mobile number or e-mail address may be contact data, an authentication channel and the unique identifier of the Wallet account. A change affecting the unique account identifier is

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

Identyum prevents two active Wallets from using the same verified mobile number or the same verified e-mail address as their unique account identifier. Changing an account identifier does not merge the Wallet with another Wallet held by the same person.

A change of contact or account identifier does not modify verified PID attributes. An attribute forming part of a PID is updated only through the applicable PID validation and update process.

6.6. PID Addition, Update, Staleness and Removal

A PID may be added to the Wallet only after a successful qualifying 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 evidentiary record of the earlier result.

Staleness or insufficiency for a use case may restrict PID sharing, reuse, new certificate issuance, renewal or a transaction requiring fresher evidence. It 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 the PID is no longer stored in the Wallet.

6.7. Wallet Suspension

Suspension temporarily blocks normal Wallet authentication, PID presentation, data management and Wallet-based authorisation of connected operations. 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 Wallet-bound remote keys because the required authentication or authorisation cannot be completed. It does not suspend or revoke the associated certificate and does not publish a suspended certificate status through CRL or OCSP.

Identyum may separately block use of a managed private key during a security or revocation investigation. Such a technical block is not certificate suspension and does not alter certificate status until the applicable certificate-lifecycle decision is made.

6.8. Wallet Reactivation

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

Where Identyum initiated suspension, Identyum may require a security review, additional authentication, factor reset or renewed identity proofing before authorising reactivation. Reactivation restores only the Wallet functions for which all dependencies remain valid.

Reactivation cannot restore a certificate that has expired or been revoked and cannot restore PID data which the User previously removed from active Wallet content.

6.9. Permanent Wallet Revocation or Closure

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

Permanent revocation, deletion or closure of a Wallet triggers revocation of all long-term ANSign, NAuth and QNSign certificates bound to that Wallet. Identyum records and processes the required certificate-revocation actions under the applicable Certificate Policy and TSPS.

This automatic consequence does not extend to QLSeal merely because an individual operator used a 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 renewed periodically as a single credential. Its account identifier, factors, PID, certificates and connected functions are reviewed or renewed under their respective rules.

A replacement Wallet is required where a previous Wallet has been permanently revoked or reliable continuity cannot be maintained. The new Wallet is created under the then-current requirements and is not automatically merged with or treated as a continuation of another Wallet associated with a different account identifier.

6.11. Recovery of Access

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 operation and preserves the required Wallet binding.

Where the User cannot satisfy an approved recovery procedure, Identyum does not restore access solely on the basis of an unverified 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 where a device, authentication factor or Wallet session is lost, stolen, exposed or suspected of compromise.

The appropriate immediate action is suspension or permanent revocation of the Wallet and notification to Identyum support.

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

Following suspension, the affected mobile authenticator, mobile number or external-account factor may be removed. Where the compromise concerns the PIN, face-biometric binding, PID or the User's identity itself, Identyum may require permanent revocation and new enrolment rather than 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 processed separately under the certificate-revocation and key-control procedures. Wallet support, key blocking and certificate revocation must remain distinguishable in the evidence and public status information.

6.13. Wallet Data Deletion and Retained Evidence

Following permanent Wallet closure, active Wallet content is deleted or rendered permanently inaccessible under the Wallet deletion procedure. Authentication bindings are invalidated and Wallet-specific cryptographic material that is no longer required is deactivated or destroyed according to the applicable rules.

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

6.14. Status Information and User Notifications

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

The User is notified of material Wallet lifecycle and security events through an available registered channel. Certificate issuance, acceptance, expiry and revocation notifications follow the separately applicable trust-service documentation.

7. Authentication and Authorisation Using the Wallet

7.1. Supported Use Cases

Use case	Permitted result
Pseudonymous B2B login	Confirmation of successful Wallet authentication with an RP-specific pseudonymous identifier; no civil identity or eIDAS LoA.
Authentication with PID presentation	Wallet authentication result plus the selected PID attributes separately requested and authorised by the User.
Connected-service authorisation	Confirmation that the User authorised a defined operation, including an eligible remote-signing operation.
Step-up authentication	Additional factor verification required by the transaction, User setting, Relying Party or connected-service policy.
NAuth certificate-based authentication	Proof of control of the NAuth key where the integration expressly requires or accepts the NAuth certificate; not automatically a notified eID transaction.

Identyum SMS, WEB and MOBILE eID credentials and their intended assurance levels are not part of the current production scope and are not selected in an ordinary Wallet authentication transaction.

7.2. Initiation by a Relying Party or Connected Service

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

The request identifies, as applicable:

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

The User may reach 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 the registered Relying Party and a specific transaction.

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

7.3. Relying-Party Identification

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

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

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

The User is shown a clear, human-readable identification of the Relying Party before confirming the transaction. Where the requesting party cannot be reliably identified, the transaction is not completed.

The Relying Party's contractual and technical registration is an Identyum control for the 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. Determination of the Required Authentication Regime

The required regime is determined from the operation, applicable Wallet authentication policy, Relying-Party request, User security setting, connected-service policy and assessed risk. Where requirements differ, the strongest applicable minimum is used.

The result identifies the achieved Wallet authentication regime or the particular credential used. It does not assign an eIDAS LoA merely because multiple factors were available or successfully completed.

7.5. Factor Selection and Step-Up

Unless a different approved regime applies, authentication or PID sharing requires:

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

A stricter transaction may require all three factors: PIN, face biometrics and mobile authenticator.

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

All factors forming one authentication event must be completed within the same connected session, which may not exceed 15 minutes.

Where the mobile authenticator is used for a high-risk or qualified trust-service operation, Identyum may require the online push-confirmation mode rather than an offline one-time password.

Step-up authentication may require an additional factor or a stronger permitted combination. Where a Relying Party also requires fresher identity data or higher PID LoIP, that requirement is handled through a separate identity-proofing or PID step-up and not merely by adding an authentication factor.

7.6. Dynamic Authentication

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

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

The User's confirmation authorises only the displayed transaction. It cannot be interpreted as approval of another transaction, a different Relying Party or a broader data disclosure.

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

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

7.7. Challenge, Nonce, Session and Audience Binding

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 period 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 regime;
- 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 a different transaction or session.

Authentication messages are protected during transmission 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 mobile authenticator's online mode uses a protected challenge-response process. The challenge is delivered to the registered authenticator and the response is created using device-bound cryptographic material. The resulting response is validated by Identyum before access is granted.

Authentication results are returned only to approved endpoints associated with the requesting Relying Party. 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, the required factors are available and valid for the operation, and the request is current and bound to the registered Relying Party or connected service.

Where a certificate or remote key is involved, certificate status, profile eligibility 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 by 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-only request clearly indicates that no PID attributes will be disclosed.

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

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

The User must perform an affirmative confirmation. Declining or abandoning the request terminates the transaction without producing a successful authentication or data-sharing result.

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

Data-protection consent is used only where consent is the applicable lawful basis. A security confirmation, contractual instruction or transaction authorisation must not be labelled as GDPR consent merely because the User clicks an approval control.

7.10. Authentication-Only Result

Where no PID attributes are requested, the Wallet may return an authentication-only result. The result identifies the intended Relying Party, contains an RP-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 process described in Chapter 8.

7.11. RP-Specific Pseudonymous Identifiers

Wallet authentication uses an RP-specific pseudonymous identifier contained in the authentication assertion or 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 enable cross-client correlation.

No separate anonymous certificate is issued. The controlled relationship between the User, Wallet and RP-specific identifiers is retained only within Identyum for lifecycle management, incident response and legally justified evidentiary purposes.

Civil identity data are disclosed to a 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 canonical Relying Party context, not the User's verified civil identity.

7.12. Authentication Assertion and Evidence

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

The result contains no PID attributes unless their disclosure formed part of the separately presented and authorised request. Identyum records sufficient evidence to reconstruct the request, Relying Party, factor categories performed, User action, result and any delivered data scope.

7.13. Failed Authentication and Misuse Detection

Authentication fails where a required factor is not completed successfully, the transaction has expired, the Wallet or credential is not valid, or the response cannot be bound to the requesting Relying Party and transaction.

The User may be permitted to repeat the authentication within controlled retry limits. A new transaction or challenge is required where the previous one has expired or can no longer be used safely.

Identyum may require step-up authentication where:

- the requested action is more sensitive than the current session;
- the Relying Party requests a stronger regime;
- the User's security settings require it;
- a separately applicable credential does not satisfy its stated assurance requirement; or
- the transaction presents an elevated risk.

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

Identyum monitors authentication activity for indications of misuse, fraud or unauthorised control of a Wallet.

Relevant events may include repeated failed attempts, unusual authentication patterns, invalid or repeated transaction responses, misuse of credentials, 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 managed-key use;
- notify the User;
- initiate an incident investigation; or
- require renewed identity verification.

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

Failure to complete a required stronger regime is not resolved by silently falling back to a weaker regime. The transaction is rejected or restarted under an explicitly permitted alternative flow.

7.14. Relying-Party Obligations

A Relying Party using the ID Wallet must:

- maintain its registration details, technical credentials and approved endpoints;
- identify itself accurately to both 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 that the achieved Wallet authentication regime, any expressly applicable credential assurance, PID LoIP and freshness satisfy its own requirements;
- comply with applicable contractual, privacy and data-protection obligations; and
- report suspected compromise, misuse or significant integration incidents to Identyum.

An authentication-only result must not be treated as evidence that civil identity data were disclosed or verified for the Relying Party.

Relying Parties shall not attempt to derive Identyum's internal Wallet identifier, correlate RP-specific pseudonyms belonging to different Relying Parties or reuse an RP-specific identifier outside the Relying Party context for which it was generated.

A Relying Party remains responsible for the decision to grant access, enter into a transaction or rely on presented PID data.

8. Management and Presentation of PID and Other Wallet Data

8.1. Categories of Wallet Data

Category	Examples and status
Wallet account data	Internal Wallet identifier, verified mobile number or e-mail account identifier, status and configuration.
Authentication data	Factor bindings, protected biometric representation, authenticator registration and security events.
Identyum PID	Verified identity attributes, provenance, verification result, LoIP and relevant timestamps, where the User chose storage.
Other verified data	Data validated through an approved source or provider and labelled with its provenance and status.
User-provided or custom data	Data not represented as verified unless a defined validation process was completed.
Activity information	User-visible records of supported authentication, disclosure and lifecycle events.

8.2. Identyum PID and Data Report

The Identyum PID is a logical set of identity attributes and related verification information within an Identyum Data Report. Where stored in the Wallet, the Data Report is protected using Wallet-controlled encryption and made available only for authorised Wallet operations.

The PID is not necessarily a physical file stored on the User's device. The interface presents the data managed by the Wallet service while the protected record remains within the Identyum-controlled environment.

8.3. Validated and Non-Validated Data

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

Validated data have passed the mechanisms required by the applicable Identyum policy. They are stored with their source, verification status and, where applicable, LoIP.

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

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

With the User's consent, a Business Client may write its own business data into 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 provided by the Client.

The Client is responsible for the lawfulness, accuracy, meaning and lifecycle of the custom business data. Unless separately stated, Identyum does not verify the data and makes no LoIP or authenticity claim regarding them.

The Client may permit another legal person to read the data by providing the necessary cryptographic access, but the User's consent remains required for their use or disclosure through the Wallet.

The interface and disclosures preserve the distinction between verified PID attributes, other validated data and data supplied without Identyum verification. Storage in the Wallet does not by itself make data verified.

8.4. Sources, Provenance, LoIP and Freshness

Identyum records the provenance of verified Wallet data.

Provenance may identify:

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

Where an attribute is obtained from more than one source, the PID may record the relevant sources and cross-validation result.

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 is assigned one of the LoIP levels defined in Chapter 4.

The PID also retains the results of the relevant collection, validation and binding mechanisms from which the LoIP was derived. These results allow Identyum to reconstruct and justify the assigned level.

Detailed internal scores, thresholds and fraud indicators are not part of the ordinary public Wallet display. They are maintained in controlled evidence records and may be made available to authorised auditors, competent authorities or other parties where legally justified.

When PID data are shared, Identyum provides the LoIP and only those supporting results or status indicators that are necessary for the relevant purpose.

The PID and its attributes include 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 an identity document or credential;
- the time elapsed since verification;
- a change notified by an authoritative source; and
- the freshness requirement of the Relying Party.

Data may remain visible in the Wallet after they have ceased to satisfy 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 a PID creates updated provenance, timestamps, verification results and LoIP. Earlier evidence may remain separately retained for audit and legal purposes.

LoIP belongs to the identity-proofing result and must not be combined with the achieved Wallet authentication regime into an unsupported single assurance claim.

8.5. Protected Storage

PID and other protected Wallet data are held in the Identyum backend within a User-specific security context and are made available through a supported interface only after the authentication required for the operation.

Protected Wallet content is encrypted at rest and in transit and is not maintained as an ordinary readable local copy on the User device. Where readable data are required temporarily for display, validation or sharing, processing occurs only within the 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 evidence copy required for an incident, legal claim or regulatory purpose is handled as separately retained evidence rather than active Wallet content.

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

8.6. User Access and Data Management

The User may access and review data stored in their ID Wallet after successful authentication.

The Wallet presents the data in a comprehensible form and, where relevant, also shows their verification status, source, LoIP, date of collection, 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 logs.
Where data were placed in the Wallet by a third party, the User's ability to interpret, modify or export those data 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 process; or
- a third party acting with the User's consent.

Adding or updating identity data requires the authentication specified in Chapters 4 and 5.
Verified identity data may be updated only through an approved source or verification process.
A refreshed result records its own provenance, verification time and LoIP rather than silently changing the evidentiary history of the previous result.
Self-declared or non-identity data may be edited through a supported Wallet function, but their status remains non-validated unless Identyum subsequently verifies them.

8.7. Selection and Data Minimisation

The Relying Party may request only the attributes needed for its stated purpose.
Identyum presents the requested data scope to the User and discloses no additional Wallet content merely because the User has authenticated.
Where the integration permits optional attributes, the User may exclude them from the disclosure. Attributes designated as mandatory for the requested service cannot be omitted if the User wishes to complete that transaction.
Where the Relying Party needs only a stable account identifier, authentication may be completed using an RP-specific pseudonym without disclosure of the User's name, national identifier or other civil identity data.
Authentication-only requests must not trigger PID disclosure. Where the Relying Party requires only an account-level pseudonym, no civil name, national identifier or other PID attribute is included.

8.8. PID Presentation and Attribute Sharing

PID presentation is performed through a protected transaction initiated by an authorised Relying Party and confirmed by the User.
The PID does not need to be disclosed as one complete data set. Identyum may provide only the selected attributes together with the metadata required to interpret and validate them.

Depending on the request, the disclosed result may include:

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

The data are transferred from the Identyum backend to the authorised Relying Party through the approved interface. Authorisation is limited to the specified recipient, transaction, data scope and, where applicable, access period.

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

Before confirmation, the User is shown the Relying Party, requested data and stated purpose.

The 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 required to interpret them.

Data prepared for the Relying Party are protected for that recipient and made available through a time-limited access mechanism. Unless another period is agreed and disclosed, 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. Recipient, Purpose and Transaction Binding

Before disclosure, the User is shown the human-readable identity of the Relying Party, the 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 treated as permission for a new recipient, purpose, 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 PID data are presented, Identyum determines whether the requested attributes are available and whether they satisfy the applicable status and validity requirements.

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

- where the data originated;
- how and when they were verified;
- the applicable PID LoIP;
- whether the underlying source or evidence remains valid; and

- whether the data satisfy the requested freshness requirement.

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

Where the available PID is too old, incomplete or below the requested LoIP, Identyum may require refreshed data, additional validation or a new identity-proofing process before completing the transaction.

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

8.11. Update, Removal and Reuse

The User may request an update of PID attributes through an approved validation or identity-proofing process. An update records the new source, checks, LoIP and time while preserving the evidence required to reconstruct the earlier result.

The User may remove individual PID attributes or the complete PID from active Wallet content after completing the authentication required for that operation. Removal ends future Wallet presentation of the removed data but does not withdraw data already lawfully delivered to a Relying Party and does not delete evidence that Identyum must retain separately.

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

An existing PID may be reused in a later Identify, onboarding or supported transaction only where it contains the required attributes and satisfies the applicable LoIP, validity and freshness requirements. Each reuse requires a new request and User authorisation; earlier sharing does not create unrestricted or permanent access.

Where an existing PID is insufficient, Identyum may collect additional attributes, revalidate existing data or require a new identity-proofing process. A material update may be notified to an authorised Business Client only while a valid access relationship exists and without automatically disclosing the changed value.

The User may receive Wallet notifications concerning material updates, removals, lifecycle events or security-sensitive changes. Permanent Wallet closure 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 material activities relating to their data, where supported by the relevant interface.

The overview may include:

- addition, update or deletion of Wallet data;
- data-sharing requests and 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 significant Wallet operations. Such records may contain timestamps, transaction references, Wallet or RP-specific identifiers, data categories involved and the outcome of the event.

Audit records do not provide ordinary access to the 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.

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

The export does not include:

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

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

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 current User functions and are subject to the Wallet deletion and privacy rules. Identity-proofing, subscriber, certificate, signature and security evidence retained for legal or regulatory purposes is held separately under controlled access.

Deleting or removing active Wallet content does not delete evidence subject to a longer applicable retention period. Retention of that evidence does not recreate the PID as active Wallet content or permit its further presentation to a Relying Party.

9. Integration with Identify and Trust Services

9.1. Relationship with Identyum Identify

Identyum Identify and the Wallet are separate but interoperating services. Identify performs identity proofing and produces the transaction result and, where the applicable decision is successful, an Identyum PID. The Wallet provides an optional environment for later storage, management, authentication and authorised presentation.

A User may complete Identify without creating a Wallet, may hold an empty Wallet without completing Identify, and may complete Identify without storing the resulting PID in the Wallet. The documentation and interface preserve each of those permitted outcomes.

9.2. Optional Wallet Offer Following Identify

A Business Client may configure whether a User who has successfully completed its integrated Identify flow is presented with an offer to create an Identyum Wallet. The offer is made only where the relevant Business Client agreement and Identyum flow permit it.

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

9.3. Independent PID-Storage and Certificate-Package Choices

Following a qualifying identity-proofing result, the User may independently choose whether to store the Identyum PID in the Wallet and whether to request the certificate package available for that PID LoIP. Declining one option does not disable the other.

The exact options and resulting profiles are displayed before the User acts. The interface must not use a generic label suggesting that every package is qualified or that all possible credentials are automatically included.

9.4. Trust-Service Boundary

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

Certificate issuance, subscriber registration, certificate acceptance, certificate status, key protection, signature creation and evidence follow the applicable Certificate Policy, TSPS, disclosure statement, Terms and Conditions and controlled procedures.

9.5. Certificate-Package Eligibility Matrix

Qualifying Identyum PID LoIP	Optional long-term package	Primary purpose
Baseline	ANSign	Non-qualified advanced electronic-signature profile under the applicable LCP policy.
Extended High	NAuth + QNSign	Certificate-based authentication where expressly required and qualified electronic signing.
Extended Very High	NAuth + QNSign	Certificate-based authentication where expressly required and qualified electronic signing.
Extended Highest	NAuth + QNSign	Certificate-based authentication where expressly required and qualified electronic signing.

ANSign is not automatically added to the NAuth + QNSign package. Identyum SMS, WEB and MOBILE are not included in either certificate package. Eligibility for a package does not itself issue a certificate; the User must separately request it and complete the applicable subscriber process.

9.6. Subscriber Request and Agreement

Before a certificate is issued, the User receives the applicable trust-service Terms and Conditions and other required information in readable form on a durable medium. The User then performs a deliberate and recorded action requesting the exact package and concluding the applicable subscriber agreement.

The agreement evidence identifies the package, certificate profiles, applicable document versions, User action, time and transaction. Acceptance of the subscriber agreement may incorporate the previously supplied Terms and Conditions; a separate checkbox for every referenced document is not required unless the applicable process expressly requires it.

9.7. Certificate Issuance, Display and Acceptance or Activation

Following successful issuance, the User is shown the principal content of each issued certificate and performs a separate recorded action equivalent to ‘Accept and activate’ before first use. This action is separate from the earlier request and subscriber agreement.

Identyum records the displayed certificate, its profile and serial number, the acceptance action, time and result. Where the User does not accept, the certificate is not made available for normal use and is handled under the applicable certificate policy.

9.8. Certificate Eligibility Without PID Stored in the Wallet

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

An empty Wallet does not itself establish certificate identity. It may nevertheless remain the valid authentication and authorisation environment for a certificate whose identity basis was separately established, linked and retained under the applicable trust-service rules.

9.9. Wallet Authentication for Remote-Key Use

Use of an Identyum-managed end-user private key requires the Wallet authentication and transaction authorisation prescribed for the profile and operation. Successful Wallet authentication authorises only the specified cryptographic operation and does not give the User direct access to the private key.

For QNSign and creation of a qualified electronic signature, AUTH-E is used only through the supported online push challenge-response flow where AUTH-E is part of the required authorisation. Offline TOTP or another unsupported mode must not be represented as an available QES activation method.

9.10. Effect of Wallet Events on Certificates and Keys

Wallet or PID event	**Effect on ANSign, NAuth and QNSign**
Wallet active	Certificate may be used if the certificate, key, required factors and connected service are separately valid.
Wallet suspended	Wallet-based key use is blocked; certificate status remains unchanged solely because of Wallet suspension.
Wallet reactivated	Use may resume only if the certificate and other dependencies remain valid.
PID stale or insufficient	Existing certificate status remains unchanged; new issuance, renewal or a specific transaction may require refreshed identity evidence.
PID removed from Wallet	Existing certificate status and key eligibility remain unchanged solely because of removal.
Wallet permanently revoked, deleted or closed	All long-term ANSign, NAuth and QNSign certificates bound to the Wallet are revoked.
Individual certificate expired or revoked	Only the affected certificate function ends; the Wallet may remain active.

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

9.11. Services Outside the Wallet Practice Statement Scope

Complete CA and RA operations, remote QSCD management, signature creation and validation, QLSeal operation, qualified timestamping, certificate status services and trust-service termination are governed outside this Practice Statement.

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

10. Security and Operational Management

10.1. Organisation and Responsibilities

Identyum operates the ID Wallet service through defined management, operational, security, technical, legal and support functions. The Director retains overall responsibility for service governance, allocation of resources, approval of policies and acceptance of material residual risks.

The principal responsibilities are allocated as follows:

Function	Principal responsibilities
Management	Service governance, policy approval, resources and acceptance of material risks
Risk and Compliance	Risk management, regulatory monitoring, compliance oversight and management reporting
Information Security	Security governance, monitoring, access oversight and incident management
Technology and Infrastructure	Development, infrastructure operation, deployment, availability and recovery
Identity Operations	Identity-proofing activities and manual decisions assigned to Registration Officers
Data Protection and Legal	Privacy governance, legal documentation and notification obligations
Customer Support	User enquiries, ticket management and escalation
Process and Asset Owners	Control of 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 process or technical matters are escalated to second-level support, while matters requiring software intervention or detailed system analysis are handled by authorised technical specialists. User communications and ticket status changes are retained within the support system.

Detailed role assignments, 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. Connected trust-service responsibilities are governed under the corresponding TSPS and service roles.

10.2. Risk and Information-Security Management

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

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

The assessment considers the 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 arrangement.

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 through annual and, where necessary, ad hoc reports. The risk-management framework itself is subject to periodic internal review.

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

The framework establishes controls intended to preserve:

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

Security and privacy requirements apply throughout service design, development, testing, production operation, support, incident handling and service termination.

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

Risk assessment distinguishes authentication-only Wallet functions, identity-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 separated to reduce the possibility that one person can independently introduce, approve and conceal an unauthorised action.

In particular:

- developers submit software changes for review;
- production deployment is restricted to authorised personnel;
- infrastructure changes require approval by the responsible technical function;
- identity-proofing decisions are performed by personnel assigned to that role;
- customer-support personnel do not receive unrestricted production-system access; and
- privileged access does not, by itself, authorise changes to identity, credential or Wallet records.

Where a strict organisational separation is not practical, Identyum applies compensating controls such as independent approval, peer review, recorded deployment, multi-person control or subsequent verification.

Access and role assignments are reviewed when responsibilities change and are removed promptly 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 informed of their confidentiality, information-security and data-protection obligations. Background or suitability checks are performed where lawful and proportionate to the role.

Personnel receive training appropriate to their responsibilities. This includes, where applicable:

- secure use and administration of information systems;
- handling of personal and biometric data;
- incident recognition and reporting;
- secure software and infrastructure change practices;
- customer-support escalation; and
- identity-document and biometric assessment for Registration Officers.

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

10.4. Supplier Management

Identyum may rely on external providers for 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 supplier failure could have on the ID Wallet service.

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

Access by a supplier to Identyum-controlled systems or equipment must be authorised, limited to the required purpose and recorded. Critical suppliers are included in applicable risk, incident, change and continuity processes.

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

A supplier's role, data access, service dependency, security obligations, incident duties, continuity arrangements and evidence are documented and reviewed. Outsourcing does not transfer Identyum's accountability for its Wallet commitments.

10.5. Access, Cryptographic and Data-Security Controls

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

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

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 hosted by an external data-centre provider, access to Identyum-owned equipment remains subject to Identyum approval and oversight. Physical areas containing critical equipment are monitored through appropriate security controls, including access logging and 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 these controls is intentionally limited. Detailed security zones, network addresses, monitoring configurations, access methods and system diagrams are maintained in confidential documentation. The current architecture separates production services into protected zones and provides redundant service components to support 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 operations are logged and 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, except where an emergency procedure is required to address an immediate security or availability risk.

Software changes follow a controlled path that includes source-code management, review by other team members, deployment to the development environment, functional testing, testing in the test environment and authorised production deployment. Builds and deployments are identifiable, and previous deployable versions are retained where required to support rollback.

Infrastructure changes are assessed for scope, risk, expected impact, possible downtime and rollback. Regular and emergency changes both require authorisation appropriate to their urgency and risk. Production changes are first tested in the test environment, and preferably also in development where applicable.

Before a production change, affected process owners and, where necessary, Business Clients are informed of expected downtime, temporary service limitations or required integration actions.

After deployment, Identyum verifies that the affected service operates correctly. Unsuccessful changes are reversed or corrected using the prepared rollback arrangement

A change that introduces a new identity-proofing route, authentication factor, eID credential, formal assurance claim, certificate package, signing flow or material privacy effect requires documented impact assessment and coordinated update of the affected public and internal documentation.

10.7. Logging, Evidence and Record Keeping

Identyum maintains records sufficient to demonstrate and reconstruct security-relevant and operationally significant ID Wallet events.

Records include, as applicable:

Area	Examples
Enrolment and PID	Sources, validation and binding results, manual decisions, PID issuance and LoIP
Wallet lifecycle	Creation, activation, suspension, reactivation, revocation and closure

Area	Examples
Authentication factors	Addition, replacement and removal of 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, 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 applied at the time.

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

The evidence model distinguishes Wallet account creation, identity proofing, PID storage choice, certificate-package request, subscriber agreement, certificate acceptance, authentication, PID disclosure and lifecycle actions as separate events.

10.8. Retention and Secure Disposal

Retention is assigned by record category, legal purpose and governing service. Ordinary Wallet content and general Wallet logs are not automatically subject to the retention period applicable to QTSP evidence.

Record category	Working retention model
QTSP identity, subscriber, certificate and signature evidence	Ten years under the applicable TSPS and controlled retention schedule.
Generic operational and security logs not promoted to QTSP evidence	Three years unless a different legal, incident or evidentiary requirement applies.
Active Wallet content	For the duration needed for the Wallet function and according to the Wallet Privacy Policy and deletion rules.
Security incident or legal-hold records	For the applicable incident, limitation, regulatory or legal-hold period.

After the applicable period, records are securely deleted, anonymised or rendered permanently inaccessible unless a lawful hold or another documented ground requires continued retention.

10.9. Monitoring and Incident Management

Identyum monitors relevant application, infrastructure, network, authentication and privileged-access events to detect failures, unauthorised activity, fraud indicators and security incidents. Monitoring includes review of logs and automated detection through security controls deployed within the relevant system zones.

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

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

The detailed detection rules, alert thresholds and monitoring architecture are confidential.

Any employee or other authorised information-system user must report a suspected incident. Users and Business Clients may report suspected problems 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 where the wider 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 may increase harm. Recovery includes verification and testing before the affected component is returned to production.

Where 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 legal or contractual deadlines.

Each material incident is documented. Post-incident review identifies the cause, effectiveness of the response and any corrective or preventive controls required to reduce the risk of recurrence.

Incident actions distinguish 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 arrangements for services and components whose unavailability could materially affect ID Wallet functions.

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

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

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

Restoration does not reinstate a Wallet or credential that had been validly revoked, expired or terminated before the disruption.

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

10.11. Service Termination

Identyum maintains arrangements for the orderly termination of the ID Wallet or an associated eID function.

The termination process addresses:

- cessation of new Wallet or credential issuance;
- notification of Users, Business Clients and competent authorities;
- treatment of active Wallets, Wallet functions and connected 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 required to interpret earlier transactions.

For a planned termination, Users are informed sufficiently in advance where reasonably possible and are provided with instructions regarding available data-export or replacement options.

Termination of connected certificates, trust services or remote signature functions is additionally governed by the applicable Certificate Policy and Trust Service Practice Statement.

Termination planning includes the consequences for active Wallets, User notification, access to or export of eligible data, deletion of active content, protection and retention of evidence, and revocation of bound long-term ANSign, NAuth and QNSign certificates where the 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 performed at least annually, with additional assessments after 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 and continuity processes; 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 shall publish a LoA, certification or regulatory conformity claim only for the scope and production configuration that have been formally assessed and approved.

Audit against a trust-service scope does not automatically certify the Wallet as an electronic identification means or European Digital Identity Wallet. Any such claim requires the 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:

- the identity and contact details of Identyum;
- the main functions of the ID Wallet;
- the conditions for Wallet creation and use;
- the mandatory authentication factors;
- the relationship between the Wallet, PID, eID credentials and connected trust services;
- applicable fees;
- principal security precautions;
- the procedure for suspension, revocation and termination;
- privacy information and User rights; and
- available support and complaint channels.

The information is provided through this Practice Statement, the Terms and Conditions, Privacy Policy, service interfaces and other applicable disclosure documents.

User-facing information is written in a form intended to be understandable without requiring access to Identyum's confidential technical or security documentation.

Where a connected service is provided under separate terms, the User is informed of that fact before requesting or using the service.

The published definition distinguishes current production capabilities from future or conditional capabilities and distinguishes authentication-only Wallet use from PID presentation and electronic identification.

11.2. Terms and Conditions

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

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

The basic Wallet agreement becomes effective only when the User has:

1. accepted the Terms and Conditions and 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 by itself create an active ID Wallet.

The optional electronic-identification and qualified-signing package is subject to separate, explicit acceptance of the relevant certificate, trust-service and remote-signing terms. Its acceptance is recorded independently of the acceptance required for the basic Wallet.

Where the Terms and Conditions, Privacy Policy or another service-specific document govern a matter more specifically than this Practice Statement, the document hierarchy described in section 1.6 applies.

Wallet Terms and Conditions are separate from trust-service subscriber agreements. Where the Wallet is used to request a certificate package, the trust-service information, subscriber agreement and later certificate acceptance are handled as the separate stages described in Chapter 9.

11.3. Security Recommendations

Identyum provides Users with information necessary for the safe 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 requested data and transaction details before confirmation;
- suspend or revoke the Wallet without undue delay after 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 in connection with the ID Wallet.

It identifies, as applicable:

- the categories of personal data processed;

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

Privacy information is provided before the User creates the 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 the detailed description of personal-data processing.

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

Its role may differ for a connected service.

Processing context	**Typical role**
Provision and management of the ID Wallet	Identyum as controller
Identyum's own eID or trust-service functions	Identyum as controller, subject to the applicable service documentation
Identify process configured for a Business Client	Roles allocated according to the specific processing purpose and Client agreement
Delivery of User-authorised data to a Relying Party	The Relying Party generally becomes responsible for its subsequent processing after receipt
External supplier supporting Identyum	Supplier acting under the applicable controller–processor or other contractual arrangement

A Business Client does not become the provider or controller of the Wallet merely because Wallet creation was offered within its integrated process.

The same data may be processed by different parties for separate purposes and under separate legal roles. Those roles are determined by the actual processing activity rather than by the technical fact that the parties use the same Identyum platform.
The current Privacy Policy already distinguishes Identyum's controller role for the Wallet from its possible processor role in a Business Client or connected certificate context.
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 controller activities from processing performed for a Business Client.

11.5. User Control, Authorisation and Rights

The User controls whether the ID Wallet is created and, except where a Client process lawfully requires Wallet creation as part of its service, whether data are subsequently shared through it.
Each data-sharing transaction identifies the Relying Party and 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:

- biometric-data processing;
- optional electronic-identification and qualified-signing functions;
- disclosure of Wallet data to a Relying Party;
- marketing or other optional communications; and
- another processing activity for which consent or other applicable User authorisation is the applicable legal basis.

Where processing is based on consent or other applicable User authorisation, the User may withdraw that consent or other applicable User authorisation in accordance with the Privacy Policy. Withdrawal does not affect the lawfulness of processing performed before withdrawal.
A function that technically or legally depends on the withdrawn consent or other applicable User authorisation may become unavailable. In particular, the Wallet cannot remain active without the mandatory face-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 relating to personal data processed by Identyum, including the right to:

- obtain information and access to personal data;

- request correction of inaccurate or incomplete data;
- request erasure where continued processing is not justified;
- request restriction of processing;
- object to processing based on legitimate interests or direct marketing;
- withdraw consent or other 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 the User to authenticate through the Wallet, particularly where disclosure, modification or deletion could affect identity, security or connected credentials.

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

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

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

Exercise of a data-protection right does not require deletion of records which must be retained under an applicable legal obligation or which are necessary for the establishment, exercise or defence of legal claims. Any restriction is explained under 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 public service model.

A connected trust service, transaction, Business-Client service or future optional function may be subject to a separate fee under its applicable terms. A fee payable by the User is disclosed clearly before the User requests the charged service and is not inferred merely from the availability of the Wallet.

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

11.7. User Responsibilities

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

The User is responsible for:

1. using the Wallet only personally and for lawful purposes;
2. protecting authentication factors and registered devices;
3. reviewing requests before confirming authentication or disclosure;
4. maintaining User-controlled contact data and factors where required;
5. correcting or refreshing outdated data through the supported process;
6. reporting suspected unauthorised use without undue delay; and
7. complying with security instructions and lifecycle procedures.

The User shall 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 may result in rejection of a transaction, suspension or revocation of the Wallet, termination of a credential or termination of the agreement.

The current Terms and Conditions similarly require personal use, accurate information, protection of authentication factors and immediate reporting of suspected compromise.

A User must not present an empty-Wallet authentication result as verified civil identity or transfer Wallet control, 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 arrangement.

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 result’s validity and status;
- the Wallet authentication regime and any separately applicable credential assurance;
- the PID LoIP;
- data provenance and freshness; and
- any limitations stated in the result.

The Relying Party is responsible for the lawful processing and protection of data after receipt.

It must not reuse data or authentication results outside the authorised purpose unless another legal basis permits such processing.

An RP-specific pseudonym shall be used only within the domain for which it was issued. Relying Parties shall not attempt to correlate their identifiers with those 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 presented identity data.

A Relying Party receiving a pseudonymous authentication-only result must not infer civil identity, PID LoIP or a 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 may 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 regime or a separately expressed assurance level; or
- the Wallet as sufficient for a specific 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 a government-issued identity document, a notified national eID means or a European Digital Identity Wallet.

The User must not represent the Wallet, PID or credential as having a status, assurance level or legal effect greater than the one 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 that every external system, device, network or Relying Party will operate without error.

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

The responsibility of Identyum may be limited for loss resulting from matters outside its 1reasonable 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 of a Relying Party or third-party service;
- telecommunications or internet disruption; and
- force-majeure events.

No limitation excludes liability where exclusion is prohibited by applicable law. Mandatory consumer rights and liability arising from intentional misconduct, gross negligence or another legally non-excludable basis remain unaffected.

The detailed contractual limitations are stated in the applicable Terms and Conditions.

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

11.10. Support and Security Reporting

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

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

11.11. Complaints and Dispute Resolution

Complaints are handled through the applicable published complaint procedure and Terms and Conditions. Identyum records the complaint, acknowledges it through an available contact channel and provides a reasoned response within the applicable timeframe.

Nothing in the complaint process limits mandatory consumer, data-protection, regulatory or judicial remedies. A complaint concerning a connected third-party service may be forwarded 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 that apply to the User regardless of the contractual choice of law.

The parties shall seek to resolve disputes through support, complaint or other appropriate amicable procedures before initiating court proceedings.

Where a dispute cannot be resolved amicably, jurisdiction is determined by the applicable law and the provisions of the Terms and Conditions.
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 current Terms and Conditions specify Croatian law and provide for prior amicable resolution of disputes.

11.13. Notification of Changes

Identyum may update the ID Wallet service, this Practice Statement, the Terms and Conditions, Privacy Policy or another applicable document.
A change is assessed according to its effect on:

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

The current version and effective date of each public document are published through the applicable Identyum channel.
Users are informed of material changes through the registered e-mail address, the ID Wallet notification channel or another appropriate electronic method. The notice describes the nature of the change and, where applicable, the 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 provides the required confirmation. Where a mandatory service change cannot be accepted, the User may terminate or revoke the Wallet subject to the applicable lifecycle and retention rules.
Emergency security changes may take effect before ordinary notice where delay would expose Users, Relying Parties or the service to material risk. The User is informed as soon as reasonably possible afterward.
The currently published Terms and Conditions already require electronic notice of significant service or rule changes and provide for publication of revised contractual documents.

A material change that affects Wallet creation, authentication-only outputs, PID use, lifecycle consequences or connected trust-service choices is reflected in the applicable public

documents before or when the changed practice becomes effective, subject to urgent security measures.

Annexes

Annex A — Current Capability and Assurance Matrix

Component or capability	Current status	Assurance or regulatory statement
Empty Wallet	Production scope	Authentication and authorisation context only; no PID, civil identity, eID means claim or eIDAS LoA.
Pseudonymous B2B login	Production scope for contracted integrations	RP-specific Wallet identifier and authentication context; not electronic identification of civil identity.
Identyum PID	Production scope for approved Identify routes	Product-specific verified identity dataset with Identyum PID LoIP; not EUDI Wallet PID.
PID presentation	Production scope where supported	Selected attributes, provenance, LoIP and freshness information disclosed after separate User authorisation.
ANSign	Connected trust-service profile	Optional package for PID LoIP Baseline; no eIDAS LoA.
NAuth	Connected trust-service profile	Optional with QNSign from PID LoIP Extended High; X.509 authentication certificate, not automatically a notified eID means.
QNSign	Connected qualified trust-service profile	Optional with NAuth from PID LoIP Extended High; qualified-signature certificate profile, not an eID LoA.
COL-C / COL-D	Outside initial production scope	No current availability or assurance claim.
Identyum SMS / WEB / MOBILE	Outside initial production scope	No current LoA or availability claim.
European Digital Identity Wallet	Outside scope	Identyum does not claim EUDI Wallet status.

Annex B — Authentication Requirements by Operation

Operation	Default Wallet authentication	Important limitation
New Wallet creation	AUTH-A + AUTH-D in one valid enrolment session	AUTH-D does not prove civil identity or issue PID.
Pseudonymous B2B login	AUTH-A + approved second factor	No PID or eIDAS LoA unless separately established and disclosed.
Add or modify PID data	AUTH-A + AUTH-D; stricter regime may add AUTH-E	Identity proofing or validation is separate from Wallet authentication.
Present PID attributes	AUTH-A + AUTH-D or AUTH-E as permitted	Separate data request and User authorisation are required.
Change factors	As defined by the controlled authentication policy	Unavailable factors may require suspension, recovery or replacement.
Suspend Wallet	Approved suspension authentication or Identyum risk action	Certificate status is unchanged solely by Wallet suspension.
Reactivate Wallet	Approved reactivation combination and any required review	Does not restore an expired or revoked certificate.
Permanently close Wallet	Approved permanent-termination procedure	Bound long-term ANSign, NAuth and QNSign are revoked.
QNSign/QES authorisation with AUTH-E	Online push challenge-response	Offline TOTP is not an available QES activation method.

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

Event	Wallet/PID effect	Certificate/key effect
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	Wallet remains empty; PID may be used for the current transaction	Eligible certificate may still be requested using separately retained evidence.
PID stored	PID becomes active Wallet content	No automatic certificate issuance.
PID becomes stale	Reuse or disclosure may require refresh or step-up	Existing certificate status unchanged; new issuance or a transaction may require fresh evidence.
PID removed	PID no longer available as Wallet content	Existing ANSign, NAuth and QNSign status unchanged solely by removal.
Wallet suspended	Wallet operations blocked temporarily	Wallet-based key use blocked; certificate status unchanged.
Wallet reactivated	Eligible Wallet operations resume	Use resumes only if certificate/key and all other dependencies remain valid.
Wallet permanently closed	Wallet cannot be reactivated	Bound long-term ANSign, NAuth and QNSign revoked; QLSeal unaffected solely by this event.
Certificate expires or is revoked	Wallet and PID may remain active	Affected certificate and its permitted key use end.
Managed-key use blocked during investigation	Wallet may be separately suspended where appropriate	Key operation blocked; certificate status remains unchanged until a revocation decision.

Annex D — Authentication-Only and PID-Disclosure Output Matrix

Output element	Authentication-only	Authentication with PID disclosure
Identyum issuer identity	Included	Included
Intended audience / Relying Party	Included	Included
Transaction and time binding	Included	Included
RP-specific pseudonymous identifier	Included where required	May be included where required
Wallet authentication regime	Included or referenced	Included or referenced
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 a separate applicable eID credential expressly provides it
Other Wallet content	Not included	Not included outside the authorised data scope

Annex E — Evidence and Retention Matrix

Event or record	Minimum evidence purpose	Applicable retention category
Wallet creation	Account identifier, T&C acceptance, factor establishment and activation	Wallet contractual/security record under the applicable retention schedule
Identity proofing and PID issuance	Sources, checks, binding, decision, LoIP and issued data	Identity-proofing or QTSP evidence category as applicable
PID storage choice	Data displayed and User's store/skip action	Wallet evidence; linked to identity evidence where applicable
Certificate-package request	Exact profiles, durable-medium documents, subscriber agreement and User action	QTSP subscriber/certificate evidence — ten years
Certificate acceptance or activation	Certificate content, serial/profile, acceptance action, time and result	QTSP certificate evidence — ten years
Wallet authentication	RP, transaction, factor categories, outcome and assertion metadata	Generic log or promoted evidence according to purpose
PID presentation	Recipient, purpose, scope, authorisation and delivered attributes	Wallet/privacy evidence or regulated transaction evidence as applicable
Wallet suspension, reactivation or closure	Initiator, authentication, reason, decision, notification and result	Wallet lifecycle/security evidence
Certificate revocation	Request/report, verification, decision, status publication and notification	QTSP certificate evidence — ten years

Where the same record supports more than one category, the longest applicable lawful retention period and the strictest applicable access control are applied without extending active Wallet availability.

Annex F — Regulatory Traceability Matrix

Reference area	Practice Statement coverage	Claim boundary
CIR (EU) 2015/1502 section 2.1 — Enrolment	Chapters 3 and 4	Used as assurance-structure guidance; no notified-scheme claim.
CIR (EU) 2015/1502 section 2.2 — eID means management	Chapters 5 and 6	Empty Wallet is not represented as an eID means.
CIR (EU) 2015/1502 section 2.3 — Authentication	Chapter 7	Wallet authentication regime is not an eIDAS LoA.
CIR (EU) 2015/1502 section 2.4 — Management and organisation	Chapters 10 and 11	Controls apply in the declared Wallet scope.
ETSI TS 119 461	Chapter 4 and the TSPS identity-proofing provisions	Applies to the approved identity-proofing scope, not empty-Wallet creation.
ETSI EN 319 401 / 319 411	Chapter 9 and the applicable CP/TSPS	Applies to connected trust services, not all Wallet functions.
eIDAS Article 5a and CIR (EU) 2024/2979	Selected privacy, RP-identification, logging and User-control principles	Non-claim design guidance only; Identyum is not represented as an EUDI Wallet provider.
GDPR	Chapters 8, 10 and 11 and the Wallet Privacy Policy	Roles and lawful bases depend on the concrete processing context.