DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

QUALIFIED ELECTRONIC ATTRIBUTE ATTESTATION SERVICE POLICY AND PRACTICE STATEMENTS

VERSION 1.0 – 01/06/2026

[LANGUAGE: ENGLISH]

VERSION HISTORY

Date	Edition	Content
01/06/2026	1.0	Initial draft

RELATED DOCUMENTS

Document Details	Author(s)
Certification Practice Statement	DigitalSign

AUTHORIZATIONS

Created by	Approved by
	

LEGAL NOTICE

Any question or request for information regarding the content of this document should be directed to qeaas@digitalsign.pt.

CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

The present document is entitled "Qualified Electronic Attribute Attestation Service Policy and Practice Statement". The purpose of this Service Policy is to meet the general requirements in order to provide trust and confidence in electronic transactions, and to define the practices and procedures used to support the issuance, management, and revocation of Qualified Electronic Attribute Attestations (QEAAs) by DigitalSign – Certificadora Digital, S.A., acting as a Qualified Electronic Attestation of Attributes Service Provider (QEAASP) in conformity with Regulation (EU) No 910/2014, European Standards - ETSI, and the legal acts of Portugal.
This Service Policy guarantees that the QEAA service:

- Applies operational and security management procedures that exclude any possibility of manipulation of the attested attributes or of the validity status of the QEAAs;
- Issues QEAAs in accordance with Article 45a of Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183/EU, so that each QEAA constitutes a qualified electronic attestation of attributes under the Regulation;
- Verifies the identity of the attribute subject in accordance with Article 24(1a) of Regulation (EU) No 910/2014 and ETSI TS 119 461 V2.1.1 (2025-02);
- Verifies the attested attributes against authentic sources or designated intermediaries, in accordance with Article 24(1b) and Article 45e of Regulation (EU) No 910/2014 and Article 9 of Commission Implementing Regulation (EU) 2025/1569;
- Manages the validity status and revocation of QEAAs in accordance with Article 4 of Commission Implementing Regulation (EU) 2025/1569, applying privacy-preserving revocation techniques that prevent linkability and traceability;
- Bears the qualified electronic seal of DigitalSign on each issued QEAA;
- Is provided as a qualified trust service listed on the Portuguese Trusted List, supervised by the Gabinete Nacional de Segurança (GNS), Portugal's National Supervisory Body.

Furthermore, the present document has been prepared in accordance with current Portuguese legislation, European Union legislation, and the applicable ETSI standards for the provision of qualified trust services, in particular ETSI TS 119 471 V1.1.1 (2025-05).
DigitalSign issues three categories of QEAAs under this Service Policy, distinguished primarily by their validity period and the resulting revocation regime:

- Short-lived QEAAs, with a maximum validity period of 23 hours, 59 minutes, and 59 seconds (section 4.1). As their validity does not exceed 24 hours, no revocation service is provided, in accordance with Article 4(3) of Commission Implementing Regulation (EU) 2025/1569;
- Long-lived QEAAs, whose validity period is indexed to the validity of the qualified certificate of the subject (section 4.2). As their validity exceeds 24 hours, they are subject to a privacy-preserving revocation regime in accordance with Article 4 of Commission Implementing Regulation (EU) 2025/1569;

- EUDIW QEAAs, designed for issuance to, and presentation through, a European Digital Identity Wallet (EUDIW) in accordance with Regulation (EU) 2024/1183/EU (eIDAS 2.0) and the applicable implementing acts (section 4.3).

1.1.1. NORMATIVE REFERENCES

- **Regulation (EU) No 910/2014** of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), as amended by Regulation (EU) 2024/1183/EU;
- **Commission Implementing Regulation (EU) 2025/1569** of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 as regards qualified electronic attestations of attributes and electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source;
- **Commission Implementing Regulation (EU) 2025/1566** of 29 July 2025 laying down rules as regards reference standards for the verification of the identity and attributes of the person to whom the qualified certificate or qualified electronic attestation of attributes is to be issued;
- **Commission Implementing Regulation (EU) 2024/2977** of 28 November 2024 laying down rules as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets;
- **Commission Implementing Regulation (EU) 2024/2979** of 28 November 2024 laying down rules as regards the integrity and core functionalities of European Digital Identity Wallets;
- **ETSI EN 319 401** Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- **ETSI TS 119 471** Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services;
- **ETSI TS 119 472-1 V1.1.1** Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 1: General requirements;
- **ETSI TS 119 461 V2.1.1 (2025-02)** Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- **ETSI TS 119 312** Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;
- **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- **IETF RFC 3647** "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

1.1.2. USERS AND FIELDS OF APPLICATION OF THE QEAA SERVICE

The QEAA service enables the issuance of qualified electronic attestations of attributes for natural persons and legal entities. Attributes are characteristics, qualities, rights, or permissions of a natural or legal person, verified against authentic sources at the time of issuance. The users of the QEAA service provided by DigitalSign may be legal or natural persons, and the service may be used when a user wishes to attest one or more of their attributes in electronic form to relying parties. The service is available to:

- Natural persons holding a valid qualified certificate issued by DigitalSign, for use in the context of qualified electronic signatures or other electronic transactions;
- Legal entities whose attributes are verifiable in official registers, acting through duly authorised natural persons;
- Holders of a European Digital Identity Wallet (EUDIW) requesting QEAAs for storage and selective disclosure within the wallet environment.

.

1.1.3. QTSP IDENTIFICATION

DigitalSign – Certificadora Digital, S.A.
Largo Pe. Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira, Guimarães
Portugal
E-mail: geral@digitalsign.pt
Support Phone: +351 253 560 650

1.1.4. SUPPORTED NAME AND IDENTIFIER OF THE DOCUMENT

This Service Policy is identified with a registered formal object identifier (OID) 1.3.6.1.4.1.25596.8.1.1.

1.2. DEFINITIONS AND ABBREVIATIONS

For the purposes of this document, the terms defined in ETSI EN 319 401, ETSI TS 119 471 V1.1.1, and the eIDAS Regulation apply. In addition, the following definitions are used:

1.2.1. DEFINITIONS

Attribute: A characteristic, quality, right or permission of a natural or legal person or of an object.

Electronic Attestation of Attributes (EAA): An attestation in electronic form that allows the authentication of attributes.

Qualified Electronic Attribute Attestation (QEAA): A qualified attestation of attributes as defined in Article 45a of the eIDAS Regulation, issued by a qualified trust service provider listed in a Member State Trusted List.

Short-lived QEAA: A QEAA with a validity period not exceeding 23 hours, 59 minutes, and 59 seconds (section 4.1), for which no revocation service is provided in accordance with Article 4(3) of Commission Implementing Regulation (EU) 2025/1569.

Long-lived QEAA: A QEAA whose validity period is indexed to the validity of the underlying qualified certificate of the subject and which, exceeding 24 hours, is subject to a revocation regime (section 4.2).

EUDIW QEAA: A QEAA issued to, and presented through, a European Digital Identity Wallet (section 4.3).

Attribute Subject: The natural or legal person, or object, to which the attested attributes belong.

QEAA Subscriber: A natural or legal person bound by agreement with DigitalSign as QEAASP.
Relying Party: A natural or legal person that relies upon an electronic identification or a trust service.

Authentic Source: A repository or system held under the responsibility of a public sector body or private entity that contains and provides attributes about a natural or legal person and is considered a primary source of that information or recognised as authentic in accordance with Union or national law.

EUDIW: European Digital Identity Wallet – a wallet unit issued under the responsibility of a Member State, enabling users to store and present QEAAs and other identity data.

Verifiable Credential (VC): A tamper-evident credential used as the technical format for QEAAs issued by DigitalSign.

Revocation List (Token Status List): A signed, privacy-preserving status list (Token Status List) maintained by DigitalSign, through which the revocation status of QEAAs whose validity period exceeds 24 hours is published, in a manner that guarantees integrity and authenticity and that preserves the privacy of subjects.

Qualified Trust Service Provider (QTSP): An entity that provides one or more qualified trust services and is granted qualified status by the Supervisory Body.

Supervisory Body: The authority designated by a Member State to carry out supervisory activities over trust services and trust service providers under the eIDAS Regulation.

QSCD: Qualified Signature/Seal Creation Device – a device meeting the requirements of Annex II of the eIDAS Regulation.

1.2.2. ABBREVIATIONS

ARF EU Architectural Reference Framework
CA Certification Authority
CAB Conformity Assessment Body
CRL Certificate Revocation List
EAA Electronic Attestation of Attributes
EAAPS Electronic Attestation of Attributes Practice Statement
eIDAS Electronic Identification, Authentication and Signature (Regulation EU No 910/2014)
ETSI European Telecommunications Standards Institute
EUDIW European Digital Identity Wallet
GDPR General Data Protection Regulation (EU) 2016/679
GNS Gabinete Nacional de Segurança
HSM Hardware Security Module
JWT JSON Web Token
OCSP Online Certificate Status Protocol
OID Object Identifier
OID4VCI OpenID for Verifiable Credential Issuance
PID Person Identification Data
QEAA Qualified Electronic Attribute Attestation
QEAASP Qualified Electronic Attestation of Attributes Service Provider
QSCD Qualified Signature/Seal Creation Device
QTSP Qualified Trust Service Provider
SD-JWT Selective Disclosure JSON Web Token
VC Verifiable Credential

1.3. POLICIES AND PRACTICES

1.3.1. ORGANIZATION ADMINISTRATING THE QTSP DOCUMENTATION

DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal

1.3.2. CONTACT PERSON

Álvaro Matos
DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal
Email: svs@digitalsign.pt
Phone: +351 253560650
Fax: +351 253560639

1.3.3. QTSP (PUBLIC) DOCUMENTATION APPLICABILITY

DigitalSign's public documentation which is related to the provision of the QEAA service has been made available to all Users and is published on the internet on https://pki.digitalsign.pt/.

Present policy and practice statement

The management group of this policy evaluates the compliance and internal applicability of this Qualified Electronic Attribute Attestation Service Policy and Practice Statement, submitting it to the approval of DigitalSign's Administration, which is the competent body to determine its suitability to the applicable legislation.

The internal approval of this documentation and following fixes and/or updates are made by DigitalSign's Administration. After internal approval, should be assessed their compliance, as described in the previous paragraph. Corrections and/or updates shall be published in the form of new versions of the Qualified Electronic Attribute Attestation Service Policy and Practice Statement, replacing any previous version.

Policy OID is referred in section 1.1.4. of this document.

Terms and conditions

DigitalSign has its terms and conditions available on https://pki.digitalsign.pt/.

Risk assessment and Information security policy

DigitalSign has an information security management system based on the standard ISO/IEC 27001, ensuring that facilities, procedures, personnel, equipment and products comply with all regulatory and safety requirements applicable to the exercise of its activity.

DigitalSign performs and maintains a documented risk assessment for its qualified trust services in accordance with clause 5 of ETSI TS 119 471 and clause 6.1 of ETSI EN 319 401, as an integral part of its ISO/IEC 27001 Information Security Management System (ISMS).

DigitalSign's risk management methodology is defined in its internal procedure and is based on the guidance of the Portuguese National Cybersecurity Centre (CNCS), the ENISA *Risk assessment – Guidelines for trust service providers (Part 2)*, the ENISA *Interoperable EU Risk Management Toolbox* (February 2023), ISO/IEC 27001:2022 and ISO/IEC 27005:2022. The methodology assesses the infrastructure and processes essential to the delivery of DigitalSign's qualified services, rather than each service as an individual product. In accordance with ISO/IEC 27005, assets are classified as primary assets, the information assets (e.g., issuing keys and certificates, subjects' keys and certificates, log archives, audit records, revocation/status information) and the business processes (registration, key-pair generation, storage/backup/recovery, issuance, revocation and status validation), and supporting assets, such as software, hardware, networks, personnel and locations. For each asset, threats, vulnerabilities, existing controls, and the resulting risk level (likelihood × impact) are identified and evaluated, and risk treatment options are selected.

The QEAA service is delivered using the same infrastructure and the same primary processes already covered by DigitalSign's existing risk assessment: subject registration and identity proofing, key-pair generation and protection, issuance, revocation, and publication of validity status. The QEAASP sealing key belongs to the same asset class as DigitalSign's other issuing private keys, and the issued QEAAs and the Token Status List correspond to the same information-asset classes

as issued certificates and revocation/status information. Accordingly, the introduction of the QEAA service does not, in itself, require a new or separate risk analysis; it relies on assets, processes and supporting infrastructure already assessed. A revision of the risk assessment is warranted only where a service introduces a genuinely new asset, process or threat scenario not already reflected in the existing assessment. Based on the current design of the QEAA service, this is not the case.
Consistent with the above, DigitalSign has confirmed that the QEAA service introduces no new primary asset or process beyond those already assessed. The privacy risk of subject linkability and traceability, including the risk of the QEAASP colluding with relying parties to track subjects, and the correlation of attestation presentations across transactions, falls within the personal-data risk scenarios already addressed by the methodology and is treated by the design of the service itself: the privacy-preserving Token Status List (section 3.7.3), the absence of any information on QEAA usage at the time of a status check, and, for EUDIW QEAAs, the selective-disclosure and unlinkability measures (section 4.3.4). This satisfies the requirement of ETSI TS 119 471 that the QEAASP document how it addresses the risk of Attestation Provider linkability.
Risk treatment options are selected according to the assessed risk level and are formalised in risk treatment plans that assign a responsible owner and an implementation date to each action, in accordance with our internal documentation. The resulting level of residual risk is determined and is subject to acceptance by the risk owners and, above the defined acceptance threshold, by DigitalSign's top management, according to the risk acceptance criteria defined. The risk assessment, its treatment plans and its results are documented and retained as evidence, and are reviewed and, where necessary, revised at least once every twelve (12) months and whenever a significant change affects the qualified services, their assets or their threat landscape.

2. TRUST SERVICE MANAGEMENT AND OPERATION

2.1. INTERNAL ORGANIZATION AND ORGANIZATION RELIABILITY

DigitalSign conducts its operations as a Qualified Electronic Attestation of Attributes Service Provider in line with the adopted policies and practices. In order to achieve reliability and security in its operations, DigitalSign applies the requirements specified in ETSI EN 319 401 and ETSI TS 119 471, including:

- DigitalSign guarantees high level of security and reliability of its operations related to the QEAA service;
- DigitalSign offers its Qualified Trust Services under non-discriminatory practices;
- DigitalSign ensures that all requirements defined in ISO/IEC 27001 Statement of Applicability and this Practice Statement are implemented and remain applicable to the Qualified Trust Services provided;
- DigitalSign complies with all legal obligations applicable to the provisioning of its Qualified Trust Services;
- DigitalSign fulfils general security requirements set out in article 19 of the eIDAS Regulation as further developed in ETSI EN 319 401;
- The provision of the QEAA service is subject to an external audit performed at least every twelve (12) months by an accredited Conformity Assessment Body (CAB), in accordance with ETSI EN 319 403, and the qualified status is supervised by GNS;
- The provision of Qualified Trust Services is subject to an external audit performed at least every 12 months by a Conformity Assessment Body (CAB) and the qualified status is supervised by GNS (Gabinete Nacional de Segurança), the Portuguese National Supervisory Body;
- Records concerning the operation of the Qualified Trust Services are made available to affected parties upon legitimate request for the purposes of providing evidence of the correct operation of the Trust Services for the purposes of legal proceedings;
- DigitalSign has the necessary financial stability and resources for operation in accordance with this document;
- DigitalSign maintains insurance of its civil liability in accordance with the applicable legislation, to cover obligations arising from its operations and in line with Article 13 of eIDAS Regulation.

2.1.1. SEGREGATION OF DUTIES

DigitalSign has established and maintains a policy of strict control procedures to ensure segregation of duties, based on the responsibilities of each task, and ensuring that multiple Trusted Persons are required to perform sensitive tasks.

2.1.2. DIGITALSIGN'S LIABILITY

In accordance with Article 13 of the eIDAS Regulation, DigitalSign shall be liable for damages caused intentionally or negligently due to a failure to comply with its obligations under the eIDAS Regulation and this Service Policy. DigitalSign maintains professional liability insurance to cover claims arising from the QEAA service operations.
Any conflicting obligations and the scopes of responsibility shall be clearly delineated in order to minimise any possibility for unlawful or unintentional change or misuse of the QTSP's assets.

2.1.3. CONFIDENTIALITY

All subscriber and subject data processed in the context of the QEAA service is treated as confidential, except data included in issued QEAAs or otherwise publicly available. Confidential information may only be disclosed to law enforcement or national security agencies under applicable law, in legal proceedings, or upon the written request of the data subject.

2.2. HUMAN RESOURCES

In conformity with our global CPS (Certificate Practice Statement), DigitalSign ensures:

- All personnel involved in the provision of the QEAA service are either employees of DigitalSign or authorised and qualified personnel of sub-contracting entities;
- All members are subject to personnel and management practices that DigitalSign follows to provide reasonable assurance of the trustworthiness and competence of the staff members within the fields of electronic signature-related technologies and related services;
- DigitalSign requires that staff try to be a Trusted Person, must provide evidence of background, qualifications, experience and clearance necessary to perform their possible liability tasks, competently and satisfactorily.
- The senior executive, senior staff and staff in trusted roles concerned with QEAA issuance and revocation management are free from any commercial, financial or other pressure that might adversely influence trust in the services provided.
- DigitalSign acting as QTSP obtains a signed statement from each member of the staff on not having conflicting interests with the QTSP, on the preservation of confidentiality and the protection of personal data;
- DigitalSign ensures that all tasks, roles and responsibilities with respect to the DigitalSign trusted services are described in job descriptions and made available to the concerned personnel. These job descriptions are defined from the view point of segregation of duties and least privileges, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness;
- Personnel shall exercise administrative and management procedures and processes that are in line with the DigitalSign information security management procedures;

- Managerial personnel possess expertise in the field of electronic signature and related services, in risk assessment and information security as well as possess familiarity with security procedures for personnel with security responsibilities;
- Training and awareness-raising actions (internal and external);
- Periodic review of the Trusted Person Statute.

2.3. ASSET MANAGEMENT

DigitalSign ensures implementation and maintains appropriate level of protection to its assets and information systems. For this purpose, DigitalSign maintains an inventory of all information assets (both virtual and physical) and their owners, identifying their threats and assigning a classification for the protection requirements to those assets consistent with the risk analysis.

2.4. ACCESS CONTROL

In accordance with the information security policy, the DigitalSign's system access is limited to authorized individuals. In particular, DigitalSign ensures the following measures, among others:

- DigitalSign's personnel is identified and authenticated before using critical applications related to the service
- Use of firewalls to protect the internal network domains from unauthorized access including access by subscribers and third parties;
- Firewalls are configured to prevent all protocols and accesses not required for the operation of the QTSP;
- Constant monitoring of systems and recording of information security events;
- Existence of Antivirus protection – automated systems of virus detection and elimination;
- Separation of management flows for administrators and operators, according with the segregation of duties rule;
- Sensitive data are protected against being revealed through storage and restriction of access thereto for unauthorized Users.
- DigitalSign enforces multi-factor authentication for all accounts capable of directly causing the issuance of a QEAA, including the operator, supervisor and Wallet Service roles, through DigitalSign's Authentik system (which includes KeyPass, KeyOTP, and others) or through a username and password combined with an OTP code.

2.5. CRYPTOGRAPHIC CONTROLS

DigitalSign applies the requirements for cryptographic controls specified in clause 7.5 of ETSI EN 319 401 and clause 7.5 of ETSI TS 119 471. The key-management controls are established in DigitalSign's Certification Practice Statement (CPS), section 6 (Technical Security Controls).

The hardware security module used by DigitalSign to protect and operate its keys, and which acts as the Wallet Secure Cryptographic Device for the DigitalSign wallet, operates as a Qualified Signature/Seal Creation Device.
DigitalSign maintains controls to keep its access certificate and the associated private keys secure, in accordance with the key-management procedures set out in DigitalSign's Certification Practice Statement (CPS), section 6. Until the ecosystem access certificate can be obtained, the certificates used by the Wallet Service and their private keys are managed under those same qualified key-management procedures.
The cryptographic mechanisms used support the verification of combined presentations of attributes from multiple EAAs, including verification that they belong to the same user, through the holder key material referenced in the confirmation (cnf) claim and verified via the key-binding JWT (see section 4.3.6).

2.6. PHYSICAL AND ENVIRONMENTAL SECURITY

DigitalSign applies the requirements of clause 7.6 of ETSI EN 319 401 concerning the physical and environmental security. Physical access to DigitalSign offices & data centre facilities is appropriately restricted to authorized personnel, in conformity to our global CPS (Certification Practice Statement). Safeguard measures are in place to protect critical assets and ensure continuity.

- Elaboration and maintenance of a list of persons authorized to access the facilities where the servers and system equipment are located;
- Monitoring of entrances - all existing doors and installations have access control with an anti-passback system, not being allowed to leave a specific room without registration;
- Organization of the facilities structure in four security levels;
- Reinforcement of access control through the use of an identification proximity card and, in some cases, an additional need for biometric authentication (fingerprint reader) and application of the Two Men Rule. In particular, areas used to create and store cryptographic material enforce dual control, each through the use of two-factor authentication including biometrics;
- Existence of a CCTV system and armoured security doors;
- Existence of glass break detectors, movement and open/closed door sensors;
- Location of critic assets at level 4 of security equipment;
- Personnel without escort, including non-accredited staff or visitors are not allowed in such security areas;
- Realization of periodic inspections and updates.

2.7. OPERATION SECURITY

DigitalSign applies the requirements specified in clause 7.7 of ETSI EN 319 401 in order to ensure security of its operations, as per information security policy. DigitalSign uses trustworthy systems

and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

- DigitalSign employs a layered security approach for protection against malware;
- The integrity of the systems and information of DigitalSign are protected against viruses, malicious and unauthorised software;
- Backup copies are ensured for all DigitalSign online products and services provided for clients;
- Realization of event logging, protection of log information, administrator and operator logs, clock synchronization, as well as control of operational software, via the installation of software on operational systems;
- 24/7 monitoring on the infrastructure, network and security components;

Detailed descriptions of implemented operation security controls are available as internal document(s).

2.8. NETWORK SECURITY

DigitalSign ensures that network security controls (including but not limited to firewalls, network intrusion detection secure communication between PKI Participants ensuring confidentiality and mutual authentication, anti-virus protection, website security, databases and other resources protection from outside boundaries, etc.) are implemented in compliance with the standard ETSI EN 319 401, specifically with 7.8 clause.
Detailed descriptions of implemented network security controls are available as internal document(s).

2.9. VULNERABILITIES AND INCIDENT MANAGEMENT

The management of security incidents and improvements is integrated within the overall operations model and the standard incident management procedures there. Incidents are logged into an internal tool and assigned based on their classification. Security and privacy incidents are also forwarded to the CISO or DPO respectively, to keep him/her informed, and take immediate appropriate action.
Detailed descriptions of implemented incident management controls are available as internal document(s).

2.10. COLLECTION OF EVIDENCE

DigitalSign applies the requirements specified in clause 7.10 of ETSI EN 319 401 with respect to collection of evidence.
In addition, the following particular requirements are applied:

- DigitalSign implements event logs, marked with the time of the event, to capture information needed for later proofs, including type of the event, the event success or failure and an identifier of the person and/or component at the origin for such an event;

- The archived data are stored for a period of 7 years after the QEAA expired. After expiration of this period the archived data are destroyed;

As above mentioned, DigitalSign maintains records concerning the operation of the services in scope for the purposes of providing evidence of the correct operation of these services. These records will only be disclosed to law enforcement authorities under court order and to persons with right to access to them upon legitimate request. Such information is managed in line with DigitalSign Personal Data Protection Policy.

2.11. BUSINESS CONTINUITY MANAGEMENT

DigitalSign applies the requirements specified in clause 7.11 of ETSI EN 319 401 with respect to business continuity management.
DigitalSign establishes the necessary measures to ensure full and highly automated recovery of the DigitalSign QEAA services in case of a disaster, corrupted servers, software or data.
A Business Continuity Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

2.12. QTSP TERMINATION AND TERMINATION PLANS

DigitalSign has up-to-date termination plan in accordance with clause 7.12 of ETSI EN 319 401.
DigitalSign has created a termination plan that deals with termination notification, subcontractor's management, information maintenance, private key destruction, termination phasing and updating of the termination plan procedure. DigitalSign has taken measure to ensure that the execution of the termination plan is executed in case of bankruptcy.

2.13. COMPLIANCE

DigitalSign applies the requirements specified in clause 7.13 of ETSI EN 319 401 in order to ensure compliance with the legal requirements.
In particular,

- DigitalSign guarantees that it operates in a legal and trustworthy manner and it provides evidence on how it meets the applicable legal requirements;
- The CPS and provision of DigitalSign PKI Services are compliant to relevant and applicable European and national laws;
- DigitalSign employs personnel with the required legal skills and has that fulfil the required roles in order to guard the correct implementation of legal requirements;
- DigitalSign ensures that appropriate technical and organisational measures are undertaken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to personal data, guaranteeing that personal data are processed in accordance with Regulation (EU) No. 2016/679 (commonly, GDPR).

- DigitalSign keeps the attributes and metadata relating to QEAA Subjects and Subscribers that are processed for the provision of the QEAA service logically separate from other data it holds.

2.14. SUPPLY CHAIN

DigitalSign applies the requirements for supply chain specified in clause 7.14 of ETSI EN 319 401.

3. QEAA SERVICE – COMMON PROVISIONS

3.1. QEAA CATEGORIES

DigitalSign issues three categories of QEAAs under this Service Policy, distinguished by their validity period, revocation regime, subject binding and delivery channel, as summarised in the table below. The provisions in this section are common to all categories; the provisions specific to each category are set out in section 4.

Category	Maximum validity	Revocation	Subject binding	Format
Short-lived (section 4.1)	23h 59m 59s	Not provided (Art. 4(3) CIR (EU) 2025/1569)	Subject's qualified certificate (x5t#S256)	W3C VC 2.0 (JOSE)
Long-lived (section 4.2)	Validity of the subject's qualified certificate	Token Status List (section 3.7)	Subject's qualified certificate (x5t#S256)	W3C VC 2.0 (JOSE)
EUDIW (section 4.3)	Defined per attestation profile	Token Status List (section 3.7)	EUDIW holder key material (device binding)	SD-JWT; ISO/IEC 18013-5 mdoc

3.2. QEAA TYPES

DigitalSign issues the following types of QEAAs:

- Identity Attribute QEAA: attests the identity attributes of the natural person subject, including name, date of birth, place of birth, and other identity-related information. This type enables the unambiguous identification of the subject in conjunction with their qualified electronic signature.
- Professional Attribute QEAA: attests attributes related to the professional roles, titles, or representative rights of the subject within a legal entity, including the subject's title or position, representative right scope, organisation name, and organisation identifier.
- Legal Person Attribute QEAA: attests attributes of a legal person subject, verified against official registers, including the legal name, registration number, legal form, registered office, legal status, and other attributes of the legal person recorded in the relevant authentic source. The legal person acts through duly authorised natural persons (see section 1.1.2).

The QEAA types described in this section are common to all QEAA categories (see section 3.1): the validity category determines the applicable validity period and revocation regime, and does not restrict the types of attributes that may be attested.

3.3. REQUESTING A QEAA

A QEAA may be requested by:

- A natural person holding a valid qualified electronic signature certificate issued by DigitalSign, used for identification at the time of the request, who has undergone prior identity verification by DigitalSign in accordance with section 3.4;

- A natural person acting as a representative of a legal entity, for attestation of organisational or professional attributes;
- A legal person whose attributes are verifiable in official registers, acting through a duly authorised natural person, for attestation of legal person attributes (see section 3.2).
- The holder of a European Digital Identity Wallet, for EUDIW QEAAs (see section 4.3).

Any QEAA category may attest the QEAA types described in section 3.2, including identity, professional and legal person attributes.
Issuance of a QEAA in any category may also be initiated by an authorised service acting on behalf of the subject, provided that the subject's identity has been verified (section 3.4), the requested attributes have been validated against authentic sources, and the subject's explicit consent to the issuance is obtained and recorded.
Requests shall be submitted through:

- The DigitalSign QEAA issuance interface, either as part of a qualified electronic signature workflow or as a standalone request via a DigitalSign front office.
- The DigitalSign subscriber portal; or
- The DigitalSign API for integrated service providers, in accordance with the applicable interface specification.
- For EUDIW QEAAs, the EUDIW itself, via the OpenID for Verifiable Credential Issuance (OID4VCI) protocol (see section 4.3).

The QEAA request shall specify the attributes to be included in the attestation. DigitalSign shall verify that the requested attributes are supported and that the subject has provided valid consent for their inclusion in the QEAA.
Where the QEAA is to be linked to a qualified certificate of the subject (long-lived QEAAs, see section 4.2), the request shall additionally identify that certificate.

3.4. IDENTITY VERIFICATION AND ATTRIBUTE VALIDATION

Identity verification for all QEAA categories shall be performed in accordance with Article 24(1a) of the eIDAS Regulation and ETSI TS 119 461 V2.1.1 (2025-02).
Attributes shall be verified against authentic sources, including official registers and databases recognised under Portuguese and European law. DigitalSign shall not include attributes in a QEAA unless they have been verified against an authentic source at the time of issuance. The verification date shall be recorded and taken into account in the validity period of the QEAA.
DigitalSign shall verify attributes at the time of issuance, as required by Article 45a(2)(a) of the eIDAS Regulation, and shall record the source, method, and date of verification in the QEAA metadata.
For attributes whose value may change over time (e.g., professional roles, representative rights), DigitalSign implements mechanisms to detect changes in the authentic source and to trigger revocation of the QEAA if the attribute is no longer valid (applicable to QEAA categories subject to revocation, see section 3.7).

3.5. ISSUANCE AND MINIMUM CONTENT

Upon successful identity verification and attribute validation, DigitalSign issues the QEAA and delivers it through the channel applicable to its category. Where the subscriber is identified by their qualified electronic signature certificate, the subscriber may select the attributes to be included from the verified set, and the QEAA is issued automatically and immediately. Also, DigitalSign will request only the minimum data necessary for the issuance of the QEAA.
DigitalSign shall include in QEAAs only data that has been verified at issuance time against an authentic source. DigitalSign does not apply backdating; the validity start time of a QEAA shall not be earlier than the actual time of issuance.
Each QEAA shall contain, as a minimum:

- The identifier of the QEAASP (DigitalSign);
- A unique identifier for the QEAA;
- The validity start and end times (validFrom and validUntil), within the limits applicable to the category (see section 4);
- The identifier of the subject: for QEAAs linked to a qualified certificate of the subject, via the SHA-256 hash of that certificate (x5t#S256), encoded in accordance with RFC 7800; for EUDIW QEAAs, cryptographically bound to the EUDIW holder's key material (device binding, see section 4.3);
- The verified attributes selected by the subject, with provenance metadata indicating the authentic source and the verification date;
- A status reference (Token Status List URL and index, see section 3.7.3), for QEAAs subject to revocation;
- The electronic seal of DigitalSign as QEAASP.

3.6. ACCEPTANCE, USE AND OBLIGATIONS

3.6.1. QEAA ACCEPTANCE

The subject accepts the QEAA by explicit acceptance of the terms and conditions, which are available at: https://pki.digitalsign.pt/.

3.6.2. OBLIGATIONS OF THE SUBJECT AND SUBSCRIBER

By requesting a QEAA and by using it, the subject and, where different, the subscriber undertake to:

- Provide accurate and complete information to DigitalSign at the time of the request and throughout the validity of the QEAA;
- Use the QEAA only in accordance with this Service Policy and within the limitations notified to them, including any restrictions stated in the QEAA itself;
- Refrain from any unauthorised use of the QEAA, and cease using it if the attested attributes become inaccurate or invalid;
- Notify DigitalSign without undue delay of any change affecting the attested attributes, and request revocation where the QEAA is subject to revocation (see section 3.7).

3.6.3. USE BY RELYING PARTIES

When relying on attributes attested by a QEAA, relying parties are advised to exercise due care, in particular to:

- Verify the validity of the QEAA seal issued by DigitalSign as QEAASP;
- Where the QEAA is attached to a signed document or transaction, verify the electronic seal or signature on the base document;
- Verify that the QEAA was valid at the time of signing the base document or at the time of the transaction;
- Verify the QEAASP certificate chain up to the EU Trusted List entry for DigitalSign;
- For QEAAs subject to revocation, check the revocation status using the status reference embedded in the QEAA (see section 3.7.3);
- Take into account all restrictions appearing in the QEAA or in this Service Policy.

3.7. REVOCATION

DigitalSign will revoke any non-expired QEAA when: a) in case of any errors, fraud, or at the request of the QEAA Subscriber or QEAA Subject; b) the QEAA is no longer compliant with this practice statement; c) DigitalSign is aware of changes which impact the validity; d) DigitalSign is aware of a security incident that affects the QEAA.

Revocation is permanent and irreversible: once a QEAA has been revoked, it shall not be reinstated under any circumstances. Where continued attestation of the attributes is required following revocation, a new QEAA shall be issued through the issuance process applicable to its category (see section 3.5).

No revocation service is provided for short-lived QEAAs, whose validity does not exceed 24 hours, in accordance with Article 4(3) of Commission Implementing Regulation (EU) 2025/1569 (see section 4.1). QEAAs whose validity exceeds 24 hours (long-lived and EUDIW QEAAs) are subject to the privacy-preserving revocation regime described in this section.

DigitalSign maintains a publicly accessible revocation status service for QEAAs subject to revocation, based on a Token Status List (see section 3.7.3). Revocation status is provided through DigitalSign's Token Status List service. Each QEAA contains the exact URI and index of its status list entry. Relying parties shall consult this status service when verifying the validity of such QEAAs.

The revocation status service shall be available 24 hours a day, 7 days a week. In the event of a system failure or other circumstances beyond DigitalSign's control, DigitalSign shall make best endeavours to ensure that this status service is not unavailable for longer than the maximum recovery period defined in DigitalSign's business continuity plan.

3.7.1. REVOCATION GROUNDS

A QEAA subject to revocation shall be revoked in any of the following circumstances:

- The subject requests revocation of the QEAA;
- The subject's underlying qualified electronic signature certificate is revoked or has expired;
- The attested attribute is no longer valid (e.g., the subject's professional role has changed or ceased);

- A change in the authentic source invalidates the attested attribute;
- DigitalSign becomes aware that the QEAA was issued on the basis of false or inaccurate information;
- The subject's consent for the processing of the attested attributes is withdrawn;
- DigitalSign terminates the QEAA service.

For EUDIW QEAAs, additional revocation grounds apply (see section 4.3).

3.7.2. REVOCATION REQUEST PROCESS

Revocation of a QEAA may be initiated by:

- The subject (subscriber), via submission of a signed revocation request through e-mail.

All revocation requests shall be signed with either:

- A valid qualified electronic signature of the subscriber, using the subscriber's qualified electronic signature certificate; or
- A valid QEAA of the subscriber, as issued by DigitalSign under this Service Policy.

Unsigned or insufficiently authenticated revocation requests shall not be processed. DigitalSign shall verify the identity and authorisation of the requesting party before processing a revocation request.
DigitalSign shall process valid revocation requests and update the Token Status List within 24 hours of receiving a complete and authenticated revocation request.
DigitalSign may also initiate revocation without a subscriber request, upon detection of any of the revocation grounds listed in section 3.7.1. In such cases, DigitalSign shall notify the subject without undue delay.

3.7.3. REVOCATION STATUS LIST (TOKEN STATUS LIST)

DigitalSign publishes and maintains the revocation status of QEAAs subject to revocation by means of a Token Status List, in accordance with the IETF "Token Status List" specification.
Each such QEAA contains a status reference (status claim) indicating the URL of the Status List Token and the index assigned to that QEAA within the list. The Status List is a compressed bit array in which the value at the assigned index indicates the current status of the QEAA (valid or revoked). The Status List Token shall be signed with DigitalSign's electronic seal to ensure its integrity and authenticity, and shall be updated at least every twenty-four (24) hours, and upon any new revocation without undue delay.
This mechanism preserves the privacy of subjects: the Status List contains no personal data, no subject identifiers and no revocation reasons, and its aggregated nature prevents relying parties from deriving information about attestations other than the one being verified, in accordance with the privacy-preserving revocation requirements of Article 4 of Commission Implementing Regulation (EU) 2025/1569.
Relying parties are responsible for checking the revocation status of a QEAA, using the status reference embedded in the QEAA, at the time of reliance.

3.8. RENEWAL

QEAAs may be renewed upon request through DigitalSign's platform, subject to reverification of the attested attributes against the authentic source. Upon successful reverification, a new QEAA is issued through the issuance process applicable to its category (see section 3.5). In accordance with ETSI TS 119 471 V1.1.1, clause 4.2.4.2 (EUDIW specific), this renewal procedure applies also to EUDIW QEAAs.

Renewal shall not be granted if the authentic source indicates that the attested attribute is no longer valid. For EUDIW QEAAs, holder-initiated renewal through the wallet application, as well as automatic renewal subject to holder consent, are planned enhancements; this Service Policy will be updated once they become available.

In the current version, re-issuance of an attestation may be requested through the DigitalSign management platform: an approval record allows, through the API, the issuance of new QEAAs for the same subject without repeating the full verification process, thereby covering renewal on approaching expiry or on changes in the attribute value. Re-issuance initiated by the EUDIW instance itself, through a secured session established by the Wallet Unit using the OID4VCI protocol, is a planned enhancement; this Service Policy will be updated once it becomes available.

3.9. TECHNICAL FORMATS AND PROFILES

QEAAs are issued in the formats below, in accordance with ETSI TS 119 472-1 and, for EUDIW QEAAs, the applicable implementing acts. All formats bear the qualified electronic seal of DigitalSign and, where applicable, the status reference described in section 3.7.3.

Category	Format(s)	Status reference
Short-lived	W3C Verifiable Credentials Data Model 2.0, secured with JOSE (JWS)	No
Long-lived	W3C Verifiable Credentials Data Model 2.0, secured with JOSE (JWS)	Yes (Token Status List)
EUDIW	SD-JWT (primary format); ISO/IEC 18013-5 mdoc, as specified in ISO/IEC TS 23220-2	Yes (Token Status List)

EUDIW QEAA formats support selective disclosure of individual attributes and are compatible with the EUDIW technical interface specifications (see section 4.3).

3.10. VALIDATION AND STATUS SERVICES

In accordance with clause 4.3.1 of ETSI TS 119 471, DigitalSign provides the services described below to enable relying parties to establish the validity of QEAAs issued under this Service Policy. The EUDIW-specific additions are set out in section 4.3.6.

For QEAAs subject to revocation (long-lived and EUDIW QEAAs), DigitalSign provides revocation status information by means of the Token Status List described in section 3.7.3. This status information:

- is available 24 hours a day, 7 days a week; upon system failure or other circumstances beyond DigitalSign's control, DigitalSign makes best endeavours to ensure that it is not

unavailable for longer than the maximum recovery period defined in DigitalSign's business continuity plan;

- has its integrity and authenticity ensured through DigitalSign's qualified electronic seal on the Status List Token;
- remains available at least until the QEAA expires;
- is made publicly and internationally available; and
- is provided in a privacy-preserving manner: DigitalSign obtains no information on the usage of a QEAA when its validity status is checked.

Short-lived QEAAs are not subject to a status service, in accordance with Article 4(3) of Commission Implementing Regulation (EU) 2025/1569 (section 4.1); relying parties verify their validity period as part of their reliance checks.

DigitalSign provides an EAA validation service enabling relying parties to verify the QEAAs presented to them. For any QEAA category, this service:

- verifies the qualified electronic seal of DigitalSign on the QEAA;
- verifies the QEAASP certificate chain up to the EU Trusted List entry for DigitalSign;
- checks the revocation status of the QEAA, where the QEAA is subject to revocation; and
- provides a signed validation report of the outcome.

Relying parties may alternatively perform these checks themselves, as described in section 3.6.3.

4. CATEGORY-SPECIFIC PROVISIONS

4.1. SHORT-LIVED QEAAS

This section defines the policy for QEAAs with a maximum validity period of twenty-three (23) hours, fifty-nine (59) minutes, and fifty-nine (59) seconds (hereinafter: Short-lived QEAAs). Short-lived QEAAs are designed to be attached to qualified electronic signatures or qualified electronic seals, enabling the authentication of the subject's attributes at the time of signing. They are also suitable for use in online transactions requiring immediate, time-bounded attribute attestation.
The maximum validity period of a short-lived QEAA is twenty-three (23) hours, fifty-nine (59) minutes, and fifty-nine (59) seconds. The validity start time shall correspond to the time of issuance. DigitalSign does not issue short-lived QEAAs with a validity period exceeding this limit under any circumstances.
For professional attribute QEAAs related to official registers (e.g., commercial register entries), the validity period may additionally be constrained to expire at 23:59:59 on the day of issuance, in order to align with the daily update cycle of the relevant authentic source.
Due to the inherently short validity period of short-lived QEAAs (maximum 23 hours, 59 minutes, and 59 seconds), no revocation service (CRL or OCSP) is provided for this QEAA type. Revocation is not applicable to short-lived QEAAs. Relying parties shall verify the validity period of the QEAA as part of their reliance checks.

4.2. LONG-LIVED QEAAS

This section defines the policy for QEAAs whose validity period is indexed to the validity of the qualified electronic signature certificate of the subject (hereinafter: Long-lived QEAAs). Long-lived QEAAs are designed to provide persistent attribute attestation over time, suitable for use cases where the attribute is expected to remain valid for an extended period, such as professional roles, organisational memberships, or other attributes that do not change frequently.
Unlike short-lived QEAAs, long-lived QEAAs require an active revocation mechanism to allow their invalidation before natural expiry when the underlying attribute changes, the subject's relationship with the attesting organisation changes, or the qualified certificate to which they are linked is revoked or expires.
The validity period of a long-lived QEAA shall be set so that it does not exceed the remaining validity period of the subject's qualified electronic signature certificate to which it is linked. When the subject's qualified certificate expires or is revoked, all associated long-lived QEAAs shall be considered invalid, regardless of any stated validity period.
DigitalSign shall monitor the status of qualified certificates to which long-lived QEAAs are linked and shall ensure that relying parties can ascertain the current validity status of a long-lived QEAA through the revocation mechanisms described in section 3.7.
In addition to the minimum content set out in section 3.5, long-lived QEAAs include the following specifics:

- The validity end time (validUntil) shall be set to the expiry date of the subject's qualified certificate, or earlier if required by the nature of the attested attribute;

- The QEAA shall include a reference to the unique identifier of the subject's qualified certificate;
- The QEAA shall include a status reference (Token Status List URL and index, see section 3.7.3) through which its revocation status may be checked.

4.3. EUDIW QEAAs

This section defines the policy for QEAAs issued by DigitalSign for presentation within a European Digital Identity Wallet (EUDIW), as defined in Regulation (EU) 2024/1183/EU (eIDAS 2.0) and the applicable implementing acts, in particular Commission Implementing Regulation (EU) 2025/1566, Commission Implementing Regulation (EU) 2024/2977, ETSI TS 119 471 V1.1.1 (2025-05), ETSI TS 119 472-1 V1.1.1 (2025-12), and ETSI TS 119 461 V2.1.1 (2025-02) (hereinafter: EUDIW QEAAs).
EUDIW QEAAs enable the holder of a European Digital Identity Wallet to store, manage, and selectively disclose qualified attribute attestations within the EUDIW ecosystem. They are designed to support the privacy, portability, and interoperability requirements of the European Digital Identity Framework.

4.3.1. REGULATORY FRAMEWORK

EUDIW QEAAs issued under this Service Policy comply with the following requirements:

- Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183/EU, in particular Articles 45a to 45d on electronic attestations of attributes;
- Commission Implementing Regulation (EU) 2025/1569 on qualified electronic attestations of attributes;
- Commission Implementing Regulation (EU) 2025/1566 on the verification of the identity and attributes of the person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued;
- Commission Implementing Regulation (EU) 2024/2977 on person identification data and electronic attestations of attributes issued to EUDIW;
- ETSI TS 119 471 V1.1.1 (2025-05), in particular clauses 4.2 (EUDIW-specific), 4.3 (EUDIW-specific), 4.2.4 (EUDIW-specific), 4.2.5 (EUDIW-specific), 6.1.2, 7.5.5;
- ETSI TS 119 472-1 V1.1.1 (2025-12) on EAA building blocks and profiles;
- ETSI TS 119 461 V2.1.1 (2025-02) on identity proofing requirements;
- ISO/IEC TS 23220-2:2024 on data objects and encoding rules for generic eID systems.

4.3.2. EUDIW QEAA ISSUANCE: INITIATION

The EUDIW QEAA issuance process may be initiated:

- By the EUDIW holder, via the wallet application, by requesting the issuance of a specific QEAA from DigitalSign as the designated QEAASP;
- By an authorised service that presents a valid request on behalf of the EUDIW holder, with explicit holder consent.

The initiation protocol shall comply with the applicable EUDIW technical specifications, including the OpenID for Verifiable Credential Issuance (OID4VCI) protocol as referenced in the EU

Architectural Reference Framework (ARF). DigitalSign shall verify the authenticity and integrity of the EUDIW before issuing a QEAA to it, in accordance with the requirements of the EUDIW certification scheme.
In accordance with ETSI TS 119 471 V1.1.1, clause 4.2.1.2 (EUDIW specific), DigitalSign shall verify the EUDIW instance's conformity certification (wallet unit attestation) before proceeding with issuance, once the certification mechanism for EUDIW providers and the corresponding trusted list of certified wallet providers, established under Regulation (EU) 2024/1183/EU, are operational. Until such certification mechanism and trusted list become available, DigitalSign issues EUDIW QEAAs only to wallet solutions previously assessed and approved by DigitalSign, and verifies the authenticity and integrity of the wallet instance at the time of issuance.

Wallet Unit authentication and provenance:

- Before issuing a EUDIW QEAA, DigitalSign authenticates the Wallet Unit and verifies that it originates from a trusted Wallet Provider by validating the Wallet Unit Attestation (WUA). DigitalSign verifies the signature over the WUA, accepts only the trust anchors registered for the supported Wallet Solutions, verifies that the EUDIW Provider is present in a Wallet Provider Trusted List, authenticates and validates the WUA using the registered trust anchor(s), and verifies that the WUA is not revoked. Until the certification mechanism for EUDIW providers and the Wallet Provider Trusted List established under Regulation (EU) 2024/1183/EU are operational, DigitalSign issues EUDIW QEAAs only to Wallet Solutions previously assessed and approved by DigitalSign; DigitalSign will validate the WUA against the Trusted List as soon as it is published.

Wallet Secure Cryptographic Device (WSCD) validation:

- Before issuance, DigitalSign validates that the Wallet Unit's Wallet Secure Cryptographic Device (WSCD) meets the required security level, on the basis of the certification information made available by the Wallet Provider. In the current architecture the WSCD is the remote hardware security module operated by DigitalSign, whose assurance level is therefore controlled directly by DigitalSign as QTSP (see section 2.5).

Verification of person identification data:

- Before issuing a EUDIW QEAA, DigitalSign verifies and validates the person identification data (PID) received from the Wallet Unit. Until the official PID is available, the Wallet Unit holds a DigitalSign identity attestation (DSID) whose data are validated by DigitalSign at onboarding and against the relevant authentic source (see section 3.4); at issuance the Wallet Service verifies and validates the DSID received from the Wallet Unit. DigitalSign will migrate to the official PID/LPID once it is made available by the competent authority.

Mutual authentication and access certificate:

- DigitalSign authenticates to the EUDIW instance through mutual authentication between the Wallet Service and the Wallet Unit, using a certificate issued by DigitalSign's qualified certification authority, thereby meeting the requirement for an access certificate issued by

a qualified certification authority. When using the OpenID for Verifiable Credential Issuance (OID4VCI) protocol, DigitalSign includes its access certificate in its client metadata. DigitalSign will align with the EUDIW ecosystem access-certificate scheme once the registration of issuers and access certification authorities becomes operational.

EUDIW instance status:

- Before issuance, DigitalSign validates the status of the EUDIW instance and does not issue to an instance that is revoked or suspended. As the DigitalSign wallet is operated by DigitalSign, the status of each instance (active, suspended or revoked) is managed internally and checked by the Wallet Service at issuance; DigitalSign will adopt the ecosystem verification mechanism once the Wallet Provider Trusted List is published.

4.3.3. ISSUANCE AND DEVICE BINDING

In addition to the minimum content set out in section 3.5, the issuer identifier of a EUDIW QEAA may be expressed as a DigitalSign DID, and each EUDIW QEAA shall include a cryptographic binding to the EUDIW holder's key material (device binding).
DigitalSign shall not issue EUDIW QEAAs without a valid device binding to the EUDIW holder's key material, ensuring that the QEAA can only be presented by the legitimate holder of the wallet.

Proof of possession:

- When a EUDIW QEAA is issued with wallet binding, DigitalSign verifies, as part of Wallet Unit Attestation validation at issuance, that the WSCD described in the WUA has proven possession of the private key corresponding to the public key contained in the WUA, and that the WSCD has proven possession of the attestation private key.

Batch issuance:

- DigitalSign will support batch issuance when requested by the Wallet Unit, allowing multiple cryptographically independent attestations with the same content to be issued for privacy-preserving (one-time-use) presentations. In the current version the DigitalSign wallet does not request batch issuance, and privacy is mitigated through the short validity period of EUDIW QEAAs and selective disclosure (see section 4.3.4); batch issuance with cryptographically independent attestations will be implemented together with per-attestation key generation in the hardware security module.

4.3.4. PRIVACY AND SELECTIVE DISCLOSURE

EUDIW QEAAs are designed to support selective disclosure, enabling the EUDIW holder to present only the minimum set of attributes required for a given transaction, in accordance with the data minimisation principle of the GDPR and the eIDAS 2.0 framework. DigitalSign shall implement privacy-preserving techniques, including:

- Selective disclosure mechanisms, such as SD-JWT or equivalent, allowing individual attributes to be disclosed independently;

- Unlinkability measures, where technically feasible, to prevent relying parties from correlating QEAA presentations to the same holder across different transactions, in accordance with ETSI TS 119 471 clause 4.2.3.2;
- No logging of the content of QEAA presentations by DigitalSign.

Attestation Provider (issuer) linkability:

- DigitalSign, acting as Attestation Provider, addresses the risk of Attestation Provider linkability as follows: it does not enter into any arrangement with relying parties to track users, and it has no technical means to learn when or where an issued QEAA is used. Revocation status is published through the privacy-preserving Token Status List (see section 3.7.3), which relying parties retrieve without DigitalSign obtaining any information on the QEAA being checked; DigitalSign does not log the content of QEAA presentations; and no unique trackable identifiers beyond those strictly necessary are included in the QEAA.

4.3.5. REVOCATION SPECIFICS FOR EUDIW QEAAS

EUDIW QEAAs shall be revoked on the same grounds as long-lived QEAAs (see section 3.7.1), and additionally:

- The EUDIW is revoked, suspended, or otherwise becomes invalid;
- The device binding is compromised or the EUDIW holder loses control of the wallet;
- A change in the applicable regulatory framework requires revocation.

Revocation of EUDIW QEAAs may be initiated in accordance with the same process as for long-lived QEAAs (see section 3.7.2), using either a qualified electronic signature or a valid QEAA of the subscriber. Revocation requests may be submitted:

- By email to, signed with a qualified electronic signature or a valid QEAA of the subscriber;

DigitalSign shall process valid revocation requests and update the relevant revocation status in accordance with the EUDIW revocation protocol (as specified in Commission Implementing Regulation (EU) 2024/2977 and ETSI TS 119 471 V1.1.1, clause 4.2.5.2).
DigitalSign provides a revocation status service for EUDIW QEAAs, based on the Token Status List mechanism described in section 3.7.3, compliant with the EUDIW revocation protocol. EUDIW-compatible clients and relying parties may query the revocation status of a EUDIW QEAA using the status reference embedded in the QEAA. The revocation status service is available continuously (24/7).

4.3.6. EAA VALIDATION SERVICE FOR EUDIW QEAAS

In accordance with clause 4.3.2 of ETSI TS 119 471, and in addition to the general validation and status services set out in section 3.10, the validation service for EUDIW QEAAs is made compatible with the European Digital Identity Wallet ecosystem. It is accessible to EUDIW-compatible clients and relying parties through the applicable EUDIW relying-party interface and revocation/validation protocol, and the signed validation report conforms to the format required for the EUDIW context.

Validation across presentation flows:

- The validation service supports the validation of EUDIW QEAAs presented in remote flows (same-device and cross-device) through OpenID4VP and, as a planned enhancement, in proximity flows (supervised and unsupervised) using the ISO/IEC 18013-5 (mdoc) format.

Combined presentations and same-holder verification:

- Where multiple QEAAs are presented together, DigitalSign's validation mechanisms support cryptographic verification that the presented QEAAs belong to the same user: QEAAs issued to the same wallet share the holder's key material referenced in the confirmation (cnf) claim, which is verified through the key-binding JWT (KB-JWT) at presentation. Support for combined presentations of multiple attestation types will accompany the expansion of the attribute catalogue.

Level of assurance of the WSCD signature:

- DigitalSign's validation mechanisms verify that the WSCD signs at the required level of assurance. As the WSCD is the remote hardware security module operated by DigitalSign, the assurance level of the key and of the signature is controlled directly by DigitalSign as QTSP; the certification of that module is set out in section 2.5.

4.3.7. EUDIW QEAA PRESENTATION

This section addresses the presentation of EUDIW QEAAs by the holder, complementing the general provisions on use by relying parties set out in section 3.6.3.
DigitalSign ensures that the EUDIW QEAAs it issues can be presented by the holder in the presentation flows defined for the European Digital Identity Framework, according to user needs and relying party requirements, namely:

- in remote flows, both same-device and cross-device, through the OpenID for Verifiable Presentations (OpenID4VP) protocol; and
- in proximity flows, both supervised and unsupervised, using the ISO/IEC 18013-5 (mdoc) format.

EUDIW QEAAs intended for wallet presentation currently support the remote same-device and cross-device flows through OpenID4VP, which cover the relying-party needs of the present use case. Proximity presentation using the ISO/IEC 18013-5 (mdoc) format is a planned enhancement, building on a capability already present in the DigitalSign wallet; this Service Policy will be updated once it becomes available.
At the time of presentation, the holder exercises selective disclosure, presenting only the minimum set of attributes required for the transaction (see section 4.3.4). QEAAs intended for embedding in PAdES-signed documents are not presented through the wallet and are validated in the context of the electronic signature.

5. QEAAS FOR WALLETS IN CLOSED ECOSYSTEMS

5.1. PURPOSE AND SCOPE

This section defines the policy for QEAAs issued by DigitalSign to wallets operated within a closed (managed) ecosystem, in particular the DigitalSign wallet, as distinct from the European Digital Identity Wallets (EUDIW) addressed in section 4.3. QEAAs issued under this section are qualified electronic attestations of attributes within the meaning of Article 45d of Regulation (EU) No 910/2014 and meet the same qualified requirements as the other QEAAs issued under this Service Policy. They differ only in the delivery environment and in the wallet ecosystem mechanisms that are applicable.

5.2. REGULATORY CONTEXT

The issuance of QEAAs to wallets in closed ecosystems is provided in anticipation of the Proposal for a Regulation of the European Parliament and of the Council on the establishment of European Business Wallets (COM(2025) 838 final, 2025/0358(COD), of 19 November 2025), whose Article 6 provides that European Business Wallet providers shall support common protocols and interfaces, inter alia, for the issuance of qualified and non-qualified electronic attestations of attributes to European Business Wallets. That proposal has not yet been adopted and is subject to the ordinary legislative procedure, so this section is forward looking. The qualified status of the QEAAs issued under this section derives solely from Article 45d of Regulation (EU) No 910/2014 and does not depend on the European Business Wallet framework. DigitalSign does not represent the wallet referred to in this section as a European Digital Identity Wallet or as a European Business Wallet.

5.3. APPLICABLE REQUIREMENTS

QEAAs issued under this section are subject to all the common provisions of section 3 (categories, types, request, identity verification and attribute validation, issuance and minimum content, acceptance and obligations, revocation, renewal and technical formats) and to the validation and status services of section 3.10. The device binding, privacy, selective disclosure, revocation and validation provisions established for EUDIW QEAAs in section 4.3 apply equally, save for the requirements that presuppose the European Digital Identity Wallet ecosystem, which are addressed in the following subsection.

5.4. PROVISIONS SPECIFIC TO CLOSED ECOSYSTEMS

Certain requirements applicable to EUDIW QEAAs presuppose components of the European Digital Identity Wallet ecosystem that, by definition, exist only for EUDIWs, namely person identification data (PID) issued under a Member State scheme, the Wallet Provider Trusted List, the Wallet Unit Attestation (WUA) signed by a certified EUDIW provider, and the ecosystem access-certificate scheme. As those components are not present in a closed ecosystem, the corresponding EUDIW-specific requirements do not apply to QEAAs issued under this section.

DigitalSign instead applies the following equivalent controls, appropriate to an ecosystem that it operates end to end:
Identity of the wallet owner: The identity of the subject is established by DigitalSign through its own identity proofing at onboarding, in accordance with Article 24(1a) and (1b) of Regulation (EU) No 910/2014 and ETSI TS 119 461 V2.1.1 (2025-02), and is represented by a DigitalSign identity attestation (DSID) whose data are validated against the relevant authentic source (see section 3.4). At issuance, the Wallet Service verifies and validates the DSID held by the wallet instance.
Wallet authenticity and provenance (in lieu of the Wallet Provider Trusted List and WUA): As DigitalSign is both the provider and the operator of the wallet in this closed ecosystem, the authenticity and integrity of each wallet instance are verified directly by DigitalSign against its own internal wallet registry, rather than against an external Wallet Provider Trusted List or a WUA signed by a third-party wallet provider. Only wallet instances provisioned and managed by DigitalSign are eligible to receive QEAAs under this section.
Authentication of the issuer (in lieu of the ecosystem access certificate): Mutual authentication between the Wallet Service and the wallet instance uses certificates issued by DigitalSign's qualified certification authority.

5.5. RETAINED CONTROLS

All other controls applicable to EUDIW QEAAs apply, without change, to QEAAs issued under this section, in particular: (a) the cryptographic binding of the QEAA to key material held under the holder's control in the wallet's secure cryptographic device (device binding), with verification of proof of possession at issuance (see section 4.3.3); (b) verification of the attested attributes against authentic sources, with provenance metadata (see section 3.4); (c) the qualified electronic seal of DigitalSign and the minimum content set out in section 3.5; (d) revocation and validity status through the privacy-preserving Token Status List (see sections 3.7 and 3.10); (e) selective disclosure and the measures against Attestation Provider linkability (see section 4.3.4); and (f) the validation service (see sections 3.10 and 4.3.6).

5.6. FORWARD ALIGNMENT

Once the Regulation on European Business Wallets is adopted and the corresponding certification scheme, trusted lists and common protocols and interfaces (including those referred to in its Article 6) become operational, DigitalSign will align the issuance of QEAAs under this section with that framework, adopting the ecosystem mechanisms in place of the equivalent controls described in this section where applicable.
Where the adoption of the Regulation on European Business Wallets, or of its implementing acts, introduces new requirements, assets, processes or threat scenarios relevant to the issuance of QEAAs under this section, DigitalSign will carry out a new risk assessment covering that scope, in accordance with its risk management methodology (see section 1.3), before adopting the corresponding ecosystem mechanisms.