TRUST SERVICE POLICY
FOR THE NON-QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES ISSUANCE SERVICE
PROVIDED BY AUTHOLOGIC SP. Z O.O.

Policy owner	Authologic sp. z o.o.
Document identifier/OID	1.3.6.1.4.1.NNN.1
Effective date	13.07.2026
Version:	1.0
Related document:	TERMS AND CONDITIONS FOR THE PROVISION OF THE SERVICE OF ISSUING ELECTRONIC ATTESTATIONS OF ATTRIBUTES

Authologic

Document history

Version	Effective date	Description
1.0	13.07.2026	Trust Service Policy introduction

Authologic

Table of Contents

1 Introduction

1.1 Scope

Authologic Sp. z o.o. is a Polish company providing a non-qualified Trust Service following the eIDAS Regulation. This Trust Service Policy ("**Policy**") defines the rules applicable to the provision by Authologic Sp. z o.o. of a non-qualified Trust Service of issuance of Electronic Attestations of Attributes (EAA).

This Policy describes also how Authologic has implemented operational, organizational, and technical measures required from the Trust Service Provider.

This Policy establishes the general framework for the provision of the non-qualified EAA Service and refers to internal procedures, controls, risk assessments and operational processes implemented by the TSP to support compliance with Article 19a of the eIDAS Regulation and Commission Implementing Regulation (EU) 2025/2160. The practical implementation of these measures is performed through internal procedures and operational processes. In addition, the publication of this Policy supports ETSI EN 319 401 requirements concerning the specification and publication of policies and practices applicable to trust services, which is referenced in the Annex of CIR 2025/2160.

1.2 Definitions and Service Participants

For the purpose of this Policy, the following terms and abbreviations apply:

- **Attribute:** characteristic, quality, right or permission of a natural or legal person or of an object
- **Attribute(s) Subject:** a natural person, legal person or entity the attribute(s) is(are) referring to. The EAA Subject and Attribute Subject may be the same or different entities, where allowed by the applicable EAAP.
- **Authentic Source:** a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides Attributes about an Attribute subject and is considered to be a primary source of that information or recognised as authentic in accordance with European Union or national law, including administrative practice
- **Authoritative Source:** Any source, irrespective of its form, that can be relied upon to provide accurate data, information and/or evidence that can be used to validate attributes. For the purposes of this Policy, the term Authoritative Sources shall include Authentic sources, authoritative sources, and other sources accepted for the issuance of EAAs.
- **Authologic (or Trust Service Provider or TSP):** Authologic sp. z o.o. with its registered office in Warsaw, Poland, EUID: PLKRS.0000851095, entered into the register *[to be provided]* with id [*to be provided]*
- **CIR :** Commission Implementing Regulation
- **EAA Subject:** A natural or legal person to whom an EAA has been issued and who holds the EAA in the Wallet or as a file.
- **EAA Subscriber:** The Subscriber is the person or entity bound by the agreement with the TSP for requesting or using the service.
- **Electronic Attestation of Attributes (EAA):** an attestation in electronic form that allows Attributes to be authenticated and verified in accordance with the eIDAS Regulation
- **European Digital Identity Wallet (EUDIW):** electronic identification means, which allows the user to securely store, manage and validate identity data and Electronic Attestations of Attributes, to provide them to relying parties and to other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals
- **European Telecommunication Standards Institute (ETSI):** As a European Union recognised European Standardisation Organisation (ESO), ETSI provides an open, inclusive and collaborative environment for the development and testing of globally applicable standards for ICT-enabled systems, services and applications

- **Relying Party**: a natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a Trust Service
- **Registration Service -** is a service encompassing:
    - enrollment, identification and authentication of EAA Subjects and EAA Subscribers,
    - validation of completeness of EAA application before EAA issuance,
    - evidence collection.

  Trust Service Provider may outsource the Registration Service.
- **Status list:** A mechanism provided by the TSP for communicating the status of EAAs by publishing status information whether an EAA is valid or invalid
- **Trust Service Policy (or Policy):** this Trust Service Policy for the Non-Qualified Electronic Attestation of Attributes Issuance Service provided by Authologic Sp. z o.o., defining rules and measures applicable to the Trust Service
- **Trust Service (or EAA Service):** a non-qualified Trust Service provided by Authologic consisting of the issuance of Electronic Attestations of Attributes
- **EAA Policy (EAAP):** a policy defining rules applicable to a specific attestation issuance schema or rulebook. References in this document to an "EAA policy" shall be understood as implementation of the applicable rulebook and/or the attestation issuance schema, including technical, operational, and organizational provisions adopted to meet the requirements defined therein. The EAAP may include, where applicable, an issuance schema, technical profile, attribute definitions, issuance and validation rules, and other provisions relevant to the specific EAA
- **User:** an entity acting in one or more of the following roles:r EEA Subject, EEA Subscriber and Relying Party
- **Wallet Unit:** means a unique configuration of a Wallet solution that includes Wallet instances, Wallet secure cryptographic applications and Wallet secure cryptographic devices provided by a Wallet provider to an individual Wallet user
- **Wallet Unit Attestation (WUA):** A data object that describes the components of the Wallet Unit or allows authentication and validation of those components;
- **Wallet**: means a combination of software, hardware, services, settings, and configurations enabling storage, manage identity data and electronic attestations of attributes to provide them to relying parties

For an extensive description of the terms above, please refer to ETSI EN 319 401 and ETSI TS 119 471 referenced by this Policy.

1.3 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 and repealing Directive 1999/93/EC, amended by Regulation (EU) 2024/1183 (OJ 28.08.2014, L 257/79) **(eIDAS Regulation)**
- 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 (OJ L 119 4.5.2016, p. 1) **(GDPR)**
- COMMISSION IMPLEMENTING REGULATION (EU) 2025/2160 of 27 October 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards, specifications and procedures for the management of risks to the provision of non-qualified trust services (OJ L, 2025/2160, 28.10.2025,) **(CIR 2025/2160)**
- Act on trust services and electronic identification (PL: Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, Dz.U. z 2016 poz. 1579, z późn. zm.) (**Polish Trust Services Act**)
- Act of 5 July 2018 on the National Cybersecurity System, Dz. U. 2018 poz. 1560, z późn. zm) **(Polish Cyber Security Act)**
- COMMISSION IMPLEMENTING REGULATION (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and

methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (OJ L 2690 z 18.10.2024) **(CIR NIS2)**

- COMMISSION IMPLEMENTING REGULATION (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets (OJ L 2024/2979, 4.12.2024) **(CIR 2024/2979)**
- COMMISSION IMPLEMENTING REGULATION (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets (OJ L, 2024/2977, 4.12.2024) **(CIR 2024/2977)**
- COMMISSION IMPLEMENTING REGULATION (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties (**CIR 2025/848**)
- Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards protocols and interfaces to be supported by the European Digital Identity Framework (OJ L, 2024/2982, 4.12.2024) **(CIR 2024/2982)**
- ETSI EN 319 401 v.3.1.1 Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers **(ETSI EN 319 401)**
- ETSI TS 119 471 v1.1.1 Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services **(ETSI TS 119 471)**
- ETSI TS 119 472-1 Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 1: General requirements **(ETSI TS 119 472-1)**
- ETSI TS 119 412-6 Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers **(ETSI TS 119 412-6)**

Together as defined **“Applicable Regulations”.**

1.4 Overview of the Trust Service

The issuance of Electronic Attestations of Attributes is related to natural persons, legal persons and objects. The Trust Service covers all required components described in the present document for issuance, provisioning, and life-cycle management of EAAs.

The Trust Service Provider remains responsible for the Trust Service's conformity with this Policy, including when parts of the process are performed by subcontractors.

The Trust Service is provided through specified issuance models, including direct issuance to the EAA Subject and issuance requested by a EAA Subscriber on the EAA Subject's behalf.

This Trust Service supports issuance and handover EAA to European Digital Identity Wallets (when supported), other digital identity wallets, standalone files or other accepted transferable formats.

1.5 EAA service general provisions

1. The EAA service is provided by the Trust Service Provider (TSP) as a non-qualified trust service within the meaning of applicable provisions of the eIDAS Regulation.
2. The TSP operates under the supervision of the Minister of Digital Affairs in Poland in accordance with the provisions of the Polish Trust Services Act.
3. The EAA service is delivered in accordance with this Policy and applicable terms and conditions (T&C), available on Trust Service Provider's official website: www.authologic.com.
4. Each issued EAA contains clear information identifying the issuing Trust Service Provider.
5. The TSP implements external rulebooks and schemes within the service as EAAPs.
6. The service may also define internal rulebooks and schemas as EAAPs.
7. The TSP confirms that all implemented EAAPs requirements are fulfilled by the provided Trust Service.
8. Each EAA is issued in accordance with an applicable EAAP and information about that policy is included in the issued EAA.
9. The structure and semantics of the data contained in an EAA are defined by the relevant EAAP, and interpretation of any EAA shall be performed in the context of that policy.
10. Where an EAA is issued to a European Digital Identity Wallet, the issuance process shall comply with the CIR 2024/2979 and CIR 2024/2977. Furthermore, when the TSP acts as a relying party to verify the identity of the user via the EUDIW during the enrolment process, it complies with the registration requirements laid down in CIR 2025/848.
11. The TSP keeps an internal list of recognized digital identity wallets to which EAAs may be issued. The issuance of EAAs in file-based format is governed by the applicable EAA policy, which defines the conditions, content, and format of such attestations.
12. Relying parties shall verify the integrity, authenticity, status, validity conditions, and any policy-specific limitations of an EAA before relying upon it.

1.6 Trust Service Policy administration

1.6.1 Organization responsible for the document

This Policy is administered by: Authologic sp. z o.o., Lumen Building, 6th floor, Złota 59, 00-120 Warsaw, Poland.

1.6.2 Contact

contact@authologic.com

1.6.3 Policy approval

This policy shall be reviewed at least annually by TSP Management Board and additionally whenever significant changes occur that may affect its validity, effectiveness or applicability. Any questions or comments regarding its content shall be submitted to the contact details provided in Section 1.7.2.

2 Publication and Repository Responsibilities

The TSP provides a public repository accessible through its official website at: https://authologic.com/ with which this Policy and other published information are made available. The repository is accessible on a 24/7 basis, subject to reasonable maintenance windows.

The TSP publishes:

- the current and historical version of Policy,
- terms&conditions
- EAA status lists,
- the list of supported EAAPs,
- certificates used for EAA issuance and sealing of status list.

Published information is updated without undue delay following approval of relevant changes.

3 Identification and Authentication

3.1 Naming

The Trust Service Provider applies names and identifiers to types of Attributes, EAA subjects, EAA subscribers and Authoritative Sources in a manner that supports the correct identification, interpretation and traceability of issued EAAs.
The applicable naming and identifier rules define the types of names and identifiers used, the conditions for their use and interpretation, any permitted use of pseudonyms, and the level of uniqueness required in the context of the applicable EAA Policy.
TSP may use identifiers defined in technical standards, including ETSI TS 119 472-1 or published rulebooks and schemas.

3.2 Identity validation

3.2.1 General provisions

The requirements for initial identity validation are determined by the relevant EAAP and may differ depending on the use case, as well as legal, regulatory, or business constraints. Each EAAP defines the specific identification requirements, along with the necessary verification procedures, proportionate to the intended purpose and risk context of the issued EAA and,where applicable, relationships between EAA Subject and EAA Subscriber.
The EAA request shall be submitted by a verified EAA Subscriber. Where identity verification is required, identity proofing of the EAA Subscriber shall be performed either for each EAA application or previously as part of the registered EAA Subscriber identity. The request may be submitted directly to the TSP or via an interface provided by the EAA Subscriber. Where required by the applicable EAAP, the process shall include identity proofing of the Attribute Subject or the EAA Subject.

3.2.2 Natural persons

The Registration Service performs identification of the natural person. The Policy defines the following methods for identifying natural persons:

- by means of the European Digital Identity Wallet (once available);
- by notified or other national electronic identification (eID) means at an assurance level of at least substantial,
- based on identity data where the identity has been previously verified in accordance with applicable AML/CFT regulations,
- by unattended remote identity proofing,
- by attended remote identity proofing,
- by use of an advanced or qualified electronic signature,
- by electronic attestation of attributes.

Identity validation may be performed either by the TSP or by an EAA Subscriber acting on behalf of TSP in accordance with the applicable agreement and the requirements of this Policy.

Where agreed, the TSP may also provide identification services directly to the EAA Subscriber.

3.2.3 Legal persons

The Registration Service performs identification of the legal person and its associated authorized representative(s), being a natural person(s). Verification of legal person includes:

- The full legal name of the legal person;
- The country of the registration or incorporation of the legal person;
- A unique official identifier and its type (such as a company registration number in the National Trade Register or any other relevant business, commercial or company register).

The primary source of data for legal person verification are relevant business, company or commercial registers, official documents from public administration or legal person identification data provided by the wallet.

Natural person's identity verification as the representative of legal persons is carried out in accordance with section 3.2.4.

Where the legal person acts as an EAA Subscriber:

a) if the TSP has a contractual relationship with the EAA Subscriber, identification and verification is performed in accordance with the applicable agreement;
b) if no such contractual relationship exists, identification and verification is performed in accordance with this section.

3.2.4 Natural persons representing legal persons

Verification of the authorized representative (natural person) includes identity verification as specified in section 3.2.2 and verification of that person's authority to represent the legal person.

The primary evidence for verifying representation may include:

- A valid power of attorney;
- Confirmation of the representation through government databases.

3.2.5 Method to prove possession or cryptographic control

If the EAA Provider issues EAA to the EUDIW, it verifies possession or cryptographic control of that specific wallet instance by authenticating and validating the Wallet Unit through its Wallet Unit Attestation and checking that the Wallet Unit has not been revoked.

For issuance to other Wallet, verification is performed in accordance with the applicable EAAP, including, where required, verification of proof of possession of the Wallet of the Wallet-related cryptographic keys.

3.2.6 Validation of EAA Subscriber

Where the Subscriber acts on behalf of the Subject, the TSP identifies EAA Subscriber as described 3.2.2 or 3.2.3.

3.3 Identification and authentication for revocation requests

An EAA Subscriber or EAA Subject may request a revocation of the EAA. The revocation request shall be submitted remotely by the EAA Subscriber or EAA Subject via email to contact@authologic.com

Upon requesting the revocation, the EAA Subscriber or EAA Subject will get an email receipt confirming the reception of the request. The revocation request form is available 24/7 per week.

TSP may accept automatic revocation requests from Authoritative Sources.

If the EAA is still valid, Authologic will authenticate the person submitting the revocation request using a Registration Service to ensure the person requesting the revocation is the EAA Subscriber or EAA Subject if necessary.

4 EAA Life-Cycle Operational Requirements

4.1 EAA application

The Trust Service Provider accepts applications for the issuance of EAAs from the EAA Subscriber or EAA Subject.

Each application includes at least email addresses of the EAA Subscriber and the EAA Subject.

Applications initiated by the EAA Subject may be submitted through:

a) an EAA Subscriber interface (webpage or mobile application);
b) a digital identity wallet capable of directly invoking issuance.

Applications initiated directly by the EAA Subscriber may be submitted through an established interface (i.e. like API) between the EAA Subscriber and the TSP.

4.2 EAA issuance application processing

The EAA application processing shall include:

- a formally registered request,
- verification of the applicant's entitlement to request and obtain the EAAs,
- confirmation if terms & conditions or relevant agreement were accepted/ concluded before EAA issuance,
- Attribute Subject or EAA Subject' consent for verification of data in accordance with applicable EAAP and,
- where applicable, confirmation of the identity verification of the EAA Subject or Attribute Subject or EAA Subscriber as specified in 3.2.

The EAA issuance may be carried out using different authorization models standards following OpenID for Verifiable Credential Issuance and complementary standards, such as ISO/IEC 18013-5 and ISO/IEC 18013-7). It includes:

- Authorization code flow
- Pre-authorized code flow
- Wallet-Initiated Issuance code flow

The TSP identifies and authenticates EAA Subject or EAA Subscriber following 3.2. If the EAA Subscriber has already been verified and a contractual relationship with TSP exists, the TSP relies on that verification and does not need to repeat it each time, unless re-verification is required due to changes in identification or attribute data, expiry or invalidity of previously verified information, security concerns, legal or regulatory requirements, or other circumstances affecting the reliability or validity of the verification data.

4.3 Attribute collection and validation requirements

The Trust Service Provider collects and validates attributes following the applicable EAAP.

The TSP may collect and validate attributes against the following Authoritative Sources:

- EUDIW
- Other digital Wallets supporting the storage, management, and presentation of Electronic Attestations of Attributes
- Public databases,

- Private databases,
- Electronically signed or sealed documents using at least an advanced electronic signature or advanced electronic seal

The Authoritative Sources used for obtaining or validating Attributes are defined by an internal agreed list of Authoritative Sources. The Trust Service Provider authenticates the source relied upon for Attribute validation. TSP establishes interfaces for Attribute validation.

The Trust Service Provider binds collected Attributes with the relevant EAA Subject or Attribute Subjects.
The evidence supporting Attribute validation is retained and protected in line with chapter 5.11.

4.4 EAA issuance

The Trust Service Provider issues each EAA upon cumulative completion of both:

- application process as specified in 4.2, and
- validated Attributes as specified in 4.3.

Each EAA is issued in accordance with the specific EAA Policy.
The TSP generates and seals the EAA in accordance with the applicable EAAP. An electronic seal used for EAA issuance is an advanced electronic seal verified by a qualified certificate issued with compliance to ETSI TS 119 412-6.
Security controls applicable for cryptographic keys used for electronic sealing of EAAs are described in 5.6.

Each issued EAA is protected to ensure its integrity and authenticity..

An EAA will not be issued where the required evidence cannot be obtained, the attested Attributes cannot be verified with sufficient assurance, conflicting information is identified, or any other condition defined in the applicable EAAPis not satisfied.

4.5 EAA delivery (handover)

EAA delivery is issued to the User. EAAs may be delivered to supported target environments, including European Digital Identity Wallets, other digital identity wallets, repositories, or in file or hybrid formats, as defined in the applicable EAAP. TSP applies measures to ensure confidentiality and integrity of the EAA delivery process.

Where delivery is performed to a Wallet, the TSP may apply an appropriate binding mechanism as defined by the relevant EAAP and EAA format, ensuring that the EAA can only be used within the intended context. TSP, for the purpose of authentication to the EUDIW, uses an access certificate and a registration certificate with the entitlement Non_Q_EAA_Provider.

Where defined in EAAP, access to the EAA delivery may be protected using out-of-band mechanisms, such as one-time passwords.

The TSP maintains appropriate records of the handover process. In case of failed or incomplete delivery, appropriate measures such as retry, rejection, or escalation are applied in accordance with applicable procedures defined in the terms and conditions or the relevant agreement.

4.6 EAA Renewal

The Trust Service Provider renews an EAA in accordance with the applicable EAA Policy. Renewal requires verification of the relevant data against the authoritative sources.
Unless the applicable EAA Policy expressly requires otherwise, renewal does not include an additional identification of the EAA Subject. Where the EAA is issued to a wallet, renewal is performed only for the same wallet instance to which the EAA was previously issued.
Where the applicable requirements are not met, or where renewal or re-issuance cannot be supported based on validated data and applicable source checks, the Trust Service Provider requires a new application in line with 4.1.

4.7 EAA Revocation

The Trust Service Provider revokes an EAA where revocation is required under the applicable EAA Policy or where the EAA is no longer valid or reliable. The Trust Service Provider ensures that revocation is final and irreversible, and that a revoked EAA cannot subsequently return to a valid status.

Revocation requests may be submitted by authorized parties in accordance with 3.3.
The revocation status of an EAA is made available in accordance with 6.2.
The Trust Service Provider informs the EAA Subject or EAA Subscriber, when possible, about revoked EAAs.

4.8 Status services

The Trust Service Provider provides status information for issued EAAs in accordance with the applicable EAA Policy.
Status information reflects the current validity or revocation state of the EAA and is made available to relying parties and other authorized parties through the applicable status service mechanisms.
The status information conditions are described in 6.

5 Management, Operational, and Physical Controls

5.1 Risk management framework

The Trust Service Provider (TSP) implements a risk management framework in line with Commission Implementing Regulation (EU) 2025/2160, ensuring that risks related to the provision of non-qualified trust services are systematically identified, assessed, and managed.

TSP has implemented an information security management system certified against ISO/IEC 27001 and ISO/IEC 22301. Provisions of this trust service is covered by the management system.

The TSP establishes and maintains documented risk management policies and procedures, including continuous monitoring of risks, implementation of appropriate mitigation measures, and alignment with applicable legal and regulatory requirements.

As a provider of non-qualified trust services classified as an Important Entity under the Polish Cyber Security Act, TSP has designated contact point and is appointed for cooperation with the d relevant CSIRT.

The risk management process is regularly reviewed (at least annually) and updated to address evolving threats, technological developments, and changes in the legal and operational environment.

5.2 Internal organization

The Trust Service Provider maintains a documented internal organizational structure for the provision of the service. All roles, responsibilities and authorities are formally assigned and based on documented management decisions. The internal organization is based on formally established trusted roles. Persons assigned to such roles shall possess appropriate expertise and formally accept the obligations associated with their roles.

The following trusted roles are assigned by Authologic:

- Security Officer
- System Administrator
- System Operator
- System Auditor

5.3 Human resources

Trust Service Provider applies personnel policies and procedures supporting the secure and reliable provision of the service. Before employment or assignment to a trust service role, appropriate verification of the person's competence and trustworthiness is performed. Personnel assigned to trusted roles are suitably qualified, bound by formal obligations, and adequately trained.

5.4 Asset management

TSP has implemented and maintains an asset management process ensuring that all assets are accurately inventoried and classified based on risk and business value, with classifications reflecting confidentiality, integrity, authenticity, and availability requirements.

Asset availability is aligned with business continuity and disaster recovery objectives, and classification levels are regularly reviewed.

Rules for acceptable use and handling of information and assets are defined and enforced, and procedures are in place for personnel changes, including the return of assigned assets.

Storage media are managed throughout their lifecycle, from acquisition to disposal and are protected against damage, theft, unauthorized access, and obsolescence, with measures ensuring data remains accessible and preserved for the required retention period in line with chapter 5.11.

The Trust Service Provider monitors current and projected capacity demands to ensure that adequate resources are available to operate the EAA Service.

5.5 Access control

TSP has implemented and maintains access control measures ensuring that system access is limited to authorized individuals and aligned with defined policies.
Access rights are assigned based on the principle of least privilege, with dedicated accounts for administrative activities and strict controls over the use of privileged accounts.
Strong identification and authentication mechanisms are applied, and access rights are regularly reviewed and updated in line with organizational changes, including termination or role changes.
Access to systems and information is restricted according to information security policy, with enforced separation of duties and controlled use of system utilities.
Personnel are uniquely identified, authenticated before accessing critical systems, and held accountable for their actions.

5.6 Cryptographic controls

Trust Service Provider applies cryptographic controls supporting the protection of the EAA service and issued EAAs. All cryptographic data used for the provision of the EAA service are generated in a controlled manner within an environment that protects them against disclosure and unauthorised use.
All keys used to provide the EAA service are registered and subject to lifecycle management, including their generation, activation, storage, use, renewal, revocation, and destruction.

5.7 Physical and environmental security

The Trust Service Provider uses two independent data centers to ensure high availability and resilience of the service.
The primary data center is provided through colocation service by a third-party data center operator and maintains certifications in accordance with recognized standards, including ISO/IEC 27001, ISO 22301, and EN 50600.
Secondary data center is ensured by certified cloud service provider.

5.8 Operation security

Trust Service Provider implements operational security measures to ensure the secure and reliable operation of the service, based on defined policies, procedures, and formally assigned roles. These measures include controlled change management processes covering the planning, approval, testing, and deployment of changes, as well as secure software development lifecycle (SSDLC) practices

ensuring that systems are designed, developed, tested, and maintained in a secure manner throughout their lifecycle.

5.9 Network security

The Trust Service Provider applies network security measures protecting communications, interfaces and service environments relevant to the service. Documentation relating to the network architecture and configuration is formally approved, maintained, and updated in accordance with the applicable internal procedures. Significant changes to the network infrastructure are documented and managed through the change management process.

The Trust Service Provider performs regular penetration testing of the network infrastructure to assess the effectiveness of the implemented network security measures.

5.10 Vulnerabilities and incident management

The Trust Service Provider applies procedures for the identification, handling, and remediation of vulnerabilities, incidents, and security events affecting the service. Mechanisms are implemented to detect potential security incidents, including continuous monitoring and logging of activities across network and information systems.

Where an incident is identified and meets the applicable reporting criteria, it will be reported and handled in accordance with the TSP's internal incident management procedure, including notification to the competent supervisory authorities and other designated bodies within 24 hours of its classification as a significant incident.

5.11 Collection of evidence

The Trust Service Provider stores the following evidence for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. In particular, TSP collects:

- validation evidence linked to the corresponding EAA issuance or renewal record,
- identification data of the EAA Subject, EAA Subscriber, and Attribute Subject,
- EAA application processing data,
- EAA lifecycle events,
- agreements with EAA Subscriber,
- activities performed by trusted roles.

Data maintained for archival purposes are retained in accordance with the internal retention policy, taking into account legal requirements and the principle of data minimization, for the validity period of Attribute but not exceeding 6 years from the end of the calendar year following the expiry or termination of the Attribute's validity.

5.12 Business continuity management

The Trust Service Provider applies business continuity and recovery measures supporting the continued provision or orderly restoration of the service.

The primary business continuity mechanism is maintaining the service infrastructure in two independent data centers, enabling high availability and resilience of the trust service.

5.13 Termination plan

The Trust Service Provider maintains arrangements for the orderly termination of the service, where applicable.
Prior to discontinuing an EAA Service, the TSP shall, if applicable:

- notify all EAA Subscribers, EAA Subjects, Attribute Subject and other parties with whom it maintains contractual relationships,
- revoke all still valid issued EAAs
- revoke all certificates associated with electronic seals;

- securely delete all private keys (including backups and decommissioned keys) in a manner that prevents their recovery,
- revoke the authorization of all subcontractors to perform any activities related to EAA issuance.

5.14 Compliance

The Trust Service Provider ensures compliance with applicable legal, regulatory, policy and internal requirements relevant to this EAA service.

5.15 Supply chain

The Trust Service Provider identifies and manages suppliers, subcontractors, and external service providers supporting the EAA service, including relevant ICT and infrastructure providers.

6 EAA Status information

6.1 Revocation checking requirement for relying parties

The relying party shall verify the integrity and authenticity of the EAA based on the issuer's electronic seal and trust chain, as well as its current validity status using status information provided by the TSP. For EAAs with a validity period of less than 24 hours, verification of the status is not required. Instead, the relying party shall confirm integrity, authenticity, and that the EAA is within its validity period at the time of use.

6.2 Status List Binding

If status information for a given EAA is managed through a Status List, the issued EAA contains a reference to the applicable Status List and the information necessary to locate the corresponding status entry for that EAA within the Status List. The Status List referenced by theEAA is made available until its defined expiration date.

The Status List is published over HTTPS at the URI embedded in each EAA and remains available until the expiration date defined for the corresponding Status List. The Status List is served as:

- a signed JWT (Token Status List) for SD-JWT VC profiles, with media type application/statuslist+jwt,
- a signed CWT for ISO/IEC mdoc profiles, with media type application/statuslist+cwt.

6.3 Status list availability

Revocation status information is available 24 hours per day, 7 days per week under its identifier specified in EAA. In the event of system failure, EAAS failure, or other factors beyond the Trust Service Provider's control, the Trust Service Provider ensures that the cumulative downtime does not exceed 8 hours in any rolling 30-day period.

7 Technical profiles

EAA service may issue EAAs in the following formats:

- SD-JWT VC
- ISO/IEC-mdoc
- JSON-LD W3C-VC
- X.509-AC

Specific data fields and profile semantics are defined in each EAAP.

8 Other Business and Legal Matters

This Policy defines the general principles applicable to the provision of the Trust Service and is addressed to EAA Subscribers, EAA Subjects, Relying Parties, and other participants interacting with the service, as applicable to the relevant business and operational model of a EAA service.

This Policy and Trust Service provided under it are governed by Polish law, subject to applicable European Union regulations.

Specific contractual rights, obligations, liability regimes, service limitations, and financial terms are defined in separate terms and conditions, relevant EAA Subscriber agreements, or other binding contractual arrangements applicable to the relevant service variant. In case of conflict, the terms and conditions of the specific service take precedence.

8.1 Obligations and guarantees

8.1.1 TSP's obligations

The Trust Service Provider ensures that the Trust Service is provided in accordance with this Policy and Applicable Regulations.

The Trust Service Provider applies appropriate technical and organisational measures to protect personal data in accordance with applicable data protection laws.

The Trust Service Provider identifies the Authoritative Source to a given type of Electronic Attestation of Attributes and applies appropriate organisational and technical measures to protect the authenticity, integrity and secure processing of data used for EAA issuance.

The Trust Service Provider maintains agreements with its subcontractors and service providers supporting the Trust Services, including ICT and data center providers. These agreements define relevant responsibilities and ensure compliance with applicable security and operational requirements.

8.1.2 Authoritative Source obligations

The Trust Service Provider establishes the obligations of the private Authoritative Source in contractual arrangements between the Trust Service Provider and the relevant Authoritative Source.

Where publicly available or third-party sources constituting Authoritative Source within the meaning of this Policy are used, the applicable obligations and conditions are defined in the respective terms and conditions or other governing documentation of such Authoritative Sources.

8.1.3 EAA Subscriber' and EAA Subject's obligations

The EAA Subscriber and the EAA Subject are responsible for providing accurate and complete information and for promptly informing the Trust Service Provider of any error, defect, or change affecting the EAA or the underlying data.

The EAA Subscriber and the EAA Subject shall promptly notify the Trust Service Provider of any known changes, inaccuracies, defects, or outdated information relating to the data used for EAA issuance or the issued EAA itself.

8.1.4 Relying Party obligations

Relying Parties shall verify the integrity, authenticity, status, validity conditions, and any Policy-specific limitations of an EAA before relying upon it.

8.1.5 User obligations

The User is strictly prohibited from providing, uploading, or transmitting any content of an unlawful nature through the Trust Service.

8.2 Liability

The Trust Service Provider does not assume responsibility for the substantive accuracy, completeness, or currentness of data maintained by the Authoritative Source itself towards any of the Users or third parties. To the maximum extent permitted by applicable law, any and all liability of the Trust Service Provider is strictly excluded, except solely for liability directly resulting from a proven, non-compliant failure to fulfill its explicit obligations under the eIDAS Regulation. Its operational duties are strictly limited to the correct authentication of the Authoritative Source, the secure collection of data, and the correct processing of the data as received.

The Trust Service Provider is not liable for defects in Authoritative Source data, including outdated or incorrect information, where such defects originate in the Authoritative Source and are not caused by the Trust Service Provider.

Unless expressly stated otherwise, an issued EAA reflects the information available at the time of issuance. The Trust Service Provider is not liable for a failure to reflect later changes where the Authoritative Source does not communicate them in time.

TSP shall not be liable for any damages resulting from the use of its services in excess of the declared limitations specified in issued EAA or referenced EAAP. The limitations of liability set forth herein shall not exclude liability for intentional wrongdoing or negligence.

The Trust Service Provider is not liable for how an issued EAA is used, presented, relied upon, interpreted, or acted upon by the EAA Subscriber, the EAA Subject, a Relying Party, or any other third party, except where damage results directly from an intentional failure or negligence of the Trust Service Provider to provide the Trust Service in accordance with this Policy or applicable law.

TSP shall not be liable for the Trust Service's fitness for a particular purpose, including any business purposes.

8.3 Privacy of Personal Information

The Trust Service Provider applies privacy-preserving measures in the provision of the EAAS and ensures the confidentiality and integrity of personal data and registration data. Each EAA Policy is designed in accordance with data minimisation principles so that only Attributes necessary for the relevant type of EAA are included. The Trust Service Provider does not, after issuance, track, link, correlate, or otherwise obtain knowledge of EAA Subject transactions or behaviour, and does not export personal data to other services, unless explicitly authorised by the EAA Subject and/or EAA Subscriber. Attributes, metadata, and logs relating to the provision of the EAAS are kept logically separate and limited to the minimum necessary for security, management, legal compliance, auditability, and transparency purposes.

For additional information regarding the processing of personal data, including applicable retention periods, data subject rights, and data protection measures, please refer to the Authologic Privacy Policy available at https://authologic.com/privacy-policy.

8.4 Dispute resolution procedures

Dispute resolution procedures, including the submission and handling of claims and complaints, are specified in the applicable terms and conditions.

8.5 Amendments

This Policy shall remain in force for an indefinite period.

Authologic reserves the right to introduce changes to the Policy at any time.

The TSP reserves the right to amend the Policy for good cause which shall include:

a) The need to align the Trust Services or accompanying documentation with changes in applicable laws, including but not limited to regulations on trust services, electronic identification or electronic services, and data protection, as well as with evolving standards, frameworks, and requirements in Information and Communication Technologies (ICT),

b) Changes in technical standards, ETSI/ISO norms, or guidelines issued by supervisory authorities or auditors that affect the provision of the Trust Services,
c) The implementation of new security measures, verification tools, or technologies aimed at enhancing or modifying service infrastructure or preventing fraudulent activities,
d) Expanding, restricting, or modifying the functionalities of the Trust Services provided, including the introduction of new or modifying Attribute verification methods by Authologic.

The Trust Service Provider shall notify the User via email of any amendments to the Policy, providing the updated text. The User has the right to terminate the Agreement with immediate effect within 14 calendar days from the date on which they became aware of the amendment.