REPUBLIC OF ALBANIA

ASSEMBLY

LAW

No. 51/2026

ON ELECTRONIC IDENTIFICATION, TRUST SERVICES AND DIGITAL IDENTITY WALLET[1]

Pursuant to Articles 78, 81, point 1, and 83, point 1, of the Constitution, upon the proposal of the Council of Ministers,

ASSEMBLY

OF THE REPUBLIC OF ALBANIA

HEREBY DECIDED:

CHAPTER I

GENERAL PROVISIONS

Article 1

Purpose

The purpose of this Law is to ensure an adequate level of security of electronic identification means and trust services, enabling and facilitating the right of exercise by natural and legal persons to participate safely in the digital society, as well as to use public and private *online services*.

Article 2

Subject matter and scope

1. This law lays down the rules for:

a) conditions for the notification of electronic identification schemes and digital identity Wallet;

b) trust services, especially for electronic transactions;

c) electronic signature, electronic seals, electronic time stamps, electronic documents, electronic registered delivery service, website authentication, electronic archiving and electronic attestation of

[1] This law is fully aligned with:
- 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, as amended. CELEX number 32014R0910 , Official Journal of the European Union, Series L, No. 257, dated 28.08.2014, pages 73-114.

attributes, management of electronic signature creation devices, management of electronic seal creation devices and electronic ledgers.

2. This law also lays down the conditions for interoperability and cross-border recognition of electronic identification means of natural and legal persons, which are part of an electronic identification scheme.

3. This law shall apply to trust services, electronic identification schemes, electronic transactions, digital identity Wallets, as well as to trust service providers operating in the Republic of Albania.

4. This law shall not apply to the provision of trust services, used exclusively within closed systems, which derive from Albanian legislation or agreements between a certain group of participants, as well as in cases where the legislation in force provides otherwise.

5. This law shall not affect the validity of contracts in terms of their legal form and effects or other legal or procedural obligations related to sector-specific requirements.

6. This law shall be implemented without prejudice to the provisions of the applicable legislation on personal data protection.

Article 3

Definitions

For the purposes of this law, the following terms have the following meanings:

1. "Authority" means the authority responsible for regulating and supervising the field of electronic identification, trust services and digital identity Wallet, established by Law No. 25/2024 "On cyber security".

2. "Electronic archiving" means a service that ensures the receipt, storage, retrieval and deletion of electronic data and electronic documents, in order to ensure their stability and readability, as well as to maintain their integrity, confidentiality and authentication of origin throughout the storage period.

3. "Attribute" means a characteristic, quality, right or permission of a natural or legal person or of an object.

4. "Authentication" means an electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form.

5. "Strong user authentication" means an authentication based on the use of at least two authentication factors from different categories, such as knowledge, something that only the user knows, possession, something that only the user possesses, or being, something that the user is, which are independent of each other, such that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data .

6. "Authentic source" means a repository or system, maintained under the responsibility of a public sector body or private entity, that holds and provides attributes for a natural or legal person or object and that is considered to be the primary source of that information or recognized as authentic, in accordance with the provisions of the relevant applicable legislation or European Union legislation, including administrative practice.

7. "Certificate for website authentication" means an electronic certificate that enables the authentication of a website and links the website to the natural or legal person to whom this certificate was issued.

8. "Qualified certificate for website authentication" means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements set out in point 2 of Article 55 of this law.

9. "Certificate for electronic signature" means an electronic attestation that links electronic signature verification data to a natural person and confirms at least the name or pseudonym of that person.

10. “Qualified certificate for electronic signature” means a certificate for electronic signature, which is issued by a qualified trust service provider and meets the conditions set out in point 2 of Article 34 of this law.

11. “Certificate for electronic seal” means an electronic certificate that links data confirming the validity of the electronic seal to a legal entity and confirms the name of this person.

12. “Qualified certificate for electronic seal” means a certificate for electronic seal, which is issued by a qualified trust service provider and meets the requirements set out in point 2 of Article 46 of this law.

13. “Electronic document” means any content stored in electronic form, in particular in the form of text or sound, visual or audiovisual recording.

14. “European Digital Identity Group” means a body established by Regulation (EU) No. 2024/1183 of the European Parliament and of the Council of 11 April 2024, to support and facilitate cooperation and exchange of information on trust services, digital identity Wallets and electronic identification schemes between the Member States of the European Union.

15. “Electronic identification” means the process of using personal identification data, in electronic form, that uniquely represents a natural or legal person or a natural person representing another natural or legal person.

16. “Trust infrastructure” means the set of organizational mechanisms that assist create, maintain, monitor and improve the reliability and continuity of trust services, in accordance with the provisions of this law.

17. “Gatekeeper” means an enterprise that provides core platform services and meets the following criteria:

a) has a significant impact on the internal market;

b) provides a core platform service, which is an important gateway for business users to reach end users;

c) maintains an unchanging and stable position in its operations or it is foreseeable that it will maintain such a position in the near future.

18. “Creator of an electronic seal” means a legal person that creates an electronic seal.

19. “Digital Identity Wallet Trust Mark” means a verifiable, simple and recognizable indication which is communicated in a clear manner that a digital identity Wallet has been secured in accordance with the provisions of this law.

20. “Electronic identification means” means material or immaterial units, containing personal identification data or characteristics that together form identifiers, which enable authentication in an online or, where possible, offline service.

21. “Offline mode” means an interaction between a user and a third party in a physical location, using technologies that process in proximity, where the digital identity Wallet is not required to access remote systems via electronic communication networks, for the purposes of the interaction.

22. “Electronic signature” means all data in electronic form, which are logically linked to or associated with other electronic data, and which are used by the signatory to sign.

23. “Advanced electronic signatures” means electronic signatures that meet the conditions set out in Article 32 of this law.

24. “Qualified electronic signatures” are advanced electronic signatures, which are created by qualified electronic signature creation devices and which are based on a qualified certificate for electronic signatures.

25. “Signatory” means a natural person who creates an electronic signature.

26. “Trust service provider” means a natural or legal person, public or private, who provides one or more trust services, as a qualified trust service provider or as a non-qualified trust service provider.

27. “Qualified trust service provider” means a trust service provider, offering one or more qualified trust services, to which a qualified status has been granted by the Authority.

28. “Public body” means a state authority, at central, regional or local level, associations established by one or more of these authorities, as well as private entities authorized to provide an electronic public service within the meaning of this law.

29. “Bodies governed by public law” means bodies that meet the following characteristics:

a) are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character;

b) have legal personality;

c) are financed, for the most part, by the State, regional or local authorities or by other bodies governed by public law, or are subject to management supervision by such authorities or bodies, or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities or by other bodies governed by public law.

30. “Conformity assessment bodies” are competent bodies that carry out conformity assessment activities, including calibration, testing, certification and inspection, accredited under the applicable legislation on accreditation, which carry out conformity assessments of the activity of a qualified trust service provider or the trust services provided by it or the certification of the digital identity Wallet or electronic identification means.

31. “Product” means hardware or software or the relevant hardware or software components used for the provision of trust services and electronic identification.

32. “Electronic signature creation devices” are hardware and software products, configured for this purpose, to create an electronic signature.

33. “Qualified electronic signature creation device” means a device for creating an electronic signature that meets the requirements set out in points 2 and 3 of Article 35 of this law.

34. “Remote qualified electronic signature creation device” means a device for creating a qualified electronic signature, managed by a qualified trust service provider, in accordance with Article 36 of this law, on behalf of a signatory.

35. “Electronic seal creation device” means a software or hardware product, configured for this purpose, which is used to create an electronic seal.

36. “Qualified electronic seal creation device” means an electronic seal creation device that meets, to the extent possible, the requirements set out in points 2 and 3 of Article 35 of this law.

37. “Qualified remote electronic seal creation device” means an electronic seal creation device managed by a qualified trust service provider, in accordance with Article 48 of this Law, on behalf of a seal creator.

38. “Relying party” means a natural or legal person that relies on electronic identification, digital identity Wallets or other electronic identification means or on a trust service.

39. “User” means a natural or legal person or a natural person representing another natural or legal person who uses trust services or electronic identification means provided in accordance with this law.

40. “Business user” means any natural or legal person, acting in a commercial or professional capacity, using the services of the core platforms for the purpose of offering or in the course of offering goods and services to end users.

41. “Identity matching” means a process where a person's identification data or electronic means of identification are matched or linked to an existing account belonging to the same person.

42. “Digital Identity Wallet” (hereinafter “The Wallet”) is an electronic identification tool that allows the user to securely store, manage and authenticate personal identification data and electronic attestations of attributes, in order to provide them to the relying parties and other users of digital identity Wallets and to sign with qualified electronic signatures or seal with qualified electronic seals.

43. “Electronic ledger” means a sequence of electronic data records, which ensures the integrity and accuracy of the chronological order of these records.

44. “Qualified electronic ledger” means an electronic ledger provided by a qualified trust service provider that meets the requirements set out in Article 67 of this law.

45. “Data record” means electronic data recorded together with the relevant metadata that supports data processing.

46. “Electronic identification scheme” means an electronic identification system under which electronic identification means are issued to natural or legal persons or natural persons representing other natural or legal persons.

47. “Qualified electronic archiving service” means an electronic archiving service, which is provided by a qualified trust service provider and which meets the requirements set out in Article 65 of this law.

48. “Trust service” means an electronic service provided for a fee, which consists of:

a) issuing certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;

b) validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;

c) creation of electronic signatures or electronic seals;

ç) validation of electronic signatures or electronic seals;

d) preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals;

dh) management of devices for creating remote electronic signatures or devices for creating remote electronic seals;

e) issuing electronic attestation of attributes;

ë) validation of the electronic attestation of attributes;

f) creation of electronic time stamps;

g) validation of electronic time stamps;

gj) provision of electronic registered delivery services;

h) validation of data transmitted through electronic registered delivery services and relevant evidence;

i) electronic archiving of electronic data and electronic documents;

j) recording of electronic data in an electronic ledger.

49. “Qualified trust service” means a trust service that meets the requirements set out in this law.

50. “Electronic registered delivery service” means a service that enables the transmission of data between third parties by electronic means and provides evidence regarding the handling of the transmitted data, including evidence of the sending and receiving of the data, and that protects the transmitted data against the risk of loss, theft, damage or any other unauthorized alteration.

51. “Qualified electronic registered delivery service” means an electronic registered delivery service, the provision of which meets the requirements provided for in Article 54 of this law.

52. “Core platform services” shall mean the following services:

a) online mediation;

b) internet search engines;

c) social networks on the internet;

ç) video sharing platforms;

d) interpersonal communications independent of number;

dh) operational;

e) web browsers;

ë) virtual assistants;

f) cloud computing;

g) online advertising, including any advertising network, advertising exchange or any other advertising intermediation service provided by an undertaking that provides any of the core platform services referred to in points (a) to (f) herein;

53. “Personal data” has the same meaning as the definition given in the applicable legislation on the personal data protection.

54. “Personal identification data” means a set of data that enables the identification of a natural person or a legal person, or a natural person who represents a legal person.

55. “Electronic signature creation data” means unique data used by the signatory to create an electronic signature.

56. “Electronic seal creation data” means unique data used by the electronic seal creator to create an electronic seal.

57. “Validation data” are data used to validate an electronic signature or an electronic seal.

58. “Electronic attestation of attributes” means an attestation in electronic form, which allows for the authentication of attributes.

59. “Electronic attestation of attributes, issued by or on behalf of a public body responsible for an authentic source” means an electronic attestation of attributes, issued by a public body responsible for an authentic source or by a public sector body designated as such to issue such attestations of attributes on behalf of public bodies responsible for authentic sources, in accordance with Article 60 and Article 61(1)(a) of this Law.

60. “Qualified electronic attestation of attributes” means an electronic certificate of attributes, which is issued by a qualified trust service provider and meets the requirements set out in Article 59(2) of this Law.

61. “Validation” means the process of verifying and confirming that data in electronic form is valid, in accordance with the provisions of this law.

62. “Electronic seal” means data in electronic form, which is attached or logically linked to other data in electronic form, to ensure the origin and integrity of the latter.

63. “Advanced electronic seal” means an electronic seal that meets the requirements set out in Article 44 of this law.

64. “Qualified electronic seal” means an advanced electronic seal, which is created by a qualified electronic seal creation device and is based on a qualified certificate for electronic seals.

65. “Electronic time stamp” means data in electronic form that links other data in electronic form to a particular time, proving that such data existed at that time.

66. “Qualified electronic time stamp” means an electronic time stamp that meets the requirements provided for in Article 52 of this law.

Article 4

Supervisory authority

The National Cybersecurity Authority is the authority responsible for regulating and supervising the field of electronic identification, trust services and digital identity Wallet in the Republic of Albania.

Article 5

Use of pseudonyms

The use of pseudonyms shall be permitted in electronic transactions, , except where the applicable legislation expressly requires the use of personal identity.

CHAPTER II

DIGITAL IDENTITY WALLET

Article 6

Digital identity Wallet

1. In order to ensure that all natural and legal persons have secure, trusted and seamless cross-border access to public and private services, while having full control over their data, at least one digital identity Wallet shall be established and operated in the Republic of Albania.

2. The source code of the software components of the Wallet application shall be provided as open source licensed. For duly justified reasons, the source code of specific components, other than those installed on the user's devices, shall not be disclosed.
3. The Wallet shall enable the user in a manner that is user-friendly, transparent, and traceable by the user, in order to:
a) securely request, obtain, select, combine, store, delete, share and present under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while ensuring that selective disclosure of data is possible;
b) generate pseudonyms and store them encrypted within the Wallet;
c) securely authenticate another person's Wallet and to receive and share the person's identification data and electronic attestations of attributes in a secured way between the Wallet of the Republic of Albania and the Wallets of the Member States of the European Union;
ç) have access to logs of all transactions carried out through the Wallet via a common dashboard, enabling the user to:
i. view an up-to-date list of relying parties with which the user has established a connection and, where applicable, all data exchanged;

ii. easily request the erasure of personal data by a relying party in accordance with applicable legislation on the protection of personal data;

iii. easily report a relying party to the Commissioner for the Right to Information and Personal Data Protection (hereinafter the Commissioner), where an allegedly unlawful or suspicious request for data is received;

d) sign by means of qualified electronic signatures or seal by means of qualified electronic seals;

dh) download, to the extent technically feasible, the user’s data, electronic attestation of attributes and configurations;

e) exercise the user's rights to data portability.

4. Wallet shall in particular:

a) support common protocols and interfaces for:

i. for issuance of person identification data, qualified and non-qualified electronic attestations of attributes or qualified and non-qualified certificates to the Wallet;

ii. for relying parties to request and validate person identification data and electronic attestations of attributes

iii. for the sharing and presentation to relying parties of person identification data, electronic attestation of attributes or of selectively disclosed related data online and, where appropriate, in offline mode;

iv. for the user to allow interaction with the Wallet and display a trust mark of this Wallet;

v. to securely onboard the user by using an electronic identification means in accordance with point 23 of this Article;

vi. for interaction between the Wallets of two persons, for the purpose of receiving, validating and sharing personal identification data and electronic attestations of attributes in a secure manner;

vii. for authenticating and identifying relying parties by implementing authentication mechanisms in accordance with Article 7 of this law;

viii. for relying parties to verify the authenticity and validity of the Wallets;

ix. or requesting a relying party the erasure of personal data pursuant to applicable legislation on the personal data protection;

x. for reporting a relying party to the Commissioner, where an allegedly unlawful or suspicious request for data is received;

xi. for the creation of qualified electronic signatures or electronic seals by means of devices for creating qualified electronic signatures or devices for creating electronic seals.

b) shall not provide any information to trust service providers of electronic attestation of attributes regarding the use of these electronic attestations;

c) ensure that the relying parties can be authenticated and identified, by implementing authentication mechanisms in accordance with Article 7 of this law;

ç) meet the requirements set out in Article 14 of this Law regarding a high level of assurance, particularly when applied to requirements for identity proofing and verification, electronic identification means management and authentication;

d) implement well-defined information disclosure policies and appropriate mechanisms to inform the user in the case of electronic attestation of attributes that the relying party or the Wallet user requesting the electronic attestation of attributes has the right to access these attestations;

dh) ensure that the person's identification data, which are available from the electronic identification scheme under which the Wallet is offered, uniquely represent the natural person, the legal person or the natural person representing the natural or legal person and is linked to the Wallet;

e) offer all natural persons the opportunity to sign using qualified electronic signatures free of charge;

ë) notwithstanding the provisions of point (e) herein, proportionate measures shall be determined by Decision of the Council of Ministers to ensure that the use of free of charge qualified electronic signatures by natural persons is limited to non-professional purposes.

5. The Wallet provider shall immediately inform users of any security breach that may have compromised their Wallet or its contents entirely or partially, in particular if their Wallet has been suspended or revoked, in accordance with Article 10 of this Law.

6. Without prejudice to Article 11 of this Law, additional functions of the Wallet, including interoperability with existing national electronic identification means, may be provided for by Decision of the Council of Ministers. Such additional functions shall be in accordance with this Article.

7. Free of charge validation mechanisms shall be determined in accordance with the provisions of point 22 of this Article in order to:

a) ensure that the authenticity and validity of the Wallet can be verified;

b) allow users to verify the authenticity and validity of the identity of registered third parties, in accordance with Article 7 of this law.

8. The validity of the Wallet is revoked in the following circumstances:

a) upon the explicit request of the user;

b) when the security of the Wallet has been compromised;

c) upon the death of the user or upon the cessation of the activity of the legal person.

9. Wallet providers shall ensure that users can easily request technical support and report technical problems or any other incidents that have a negative impact on the use of Wallets.

10. Wallets are provided according to an electronic identification scheme, with an assurance level high.

11. Wallets ensure security by design.

12. The issuance, use and revocation of Wallets is free of charge for all natural persons.

13. Users shall have full control over the use of their Wallet data. The Wallet provider shall not collect information about the use of the Wallet that is not necessary for the provision of the Wallet services, nor shall it link personally identifiable information or any other personal data stored or related to the use of the Wallet with personal data from any other service provided by that provider or from third-party services that are not necessary for the provision of the Wallet services, unless the user has expressly requested otherwise. Personal data related to the provision of the Wallet shall be kept logically separate from any other data held by the Wallet provider. If the Wallet is provided by a private party, in accordance with the provisions of this Article, the provisions of point 3 of Article 63 of this Law shall apply *mutandis mutandis*.

14. The use of Wallets shall be voluntary. Access to public and private services in the labor market and the freedom to conduct business shall not be limited in any way or made disadvantageous for natural or legal persons who do not use Wallets. Access to public and private services will continue to be made through other existing means of identification and authentication.

15. The technical criteria of the Wallet shall:

a) not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the use;

b) enable privacy preserving techniques which ensure unlikeability, where the attestation of attributes does not require the identification of the user

16. Any processing of personal data, carried out by the Wallet provider or on their behalf by the bodies or parties responsible for providing the Wallet as a means of electronic identification, shall be carried out in accordance with the provisions of the applicable legislation on the personal data protection.

17. Upon accession to the European Union, the Republic of Albania shall notify the European Commission about:

a) the body responsible for establishing and maintaining the list of registered relying parties, that rely on the Wallet, in accordance with Article 7(5) of this Law, and the location of that list;

b) bodies responsible for providing the Wallet, in accordance with point 1 of this article;

c) the responsible bodies ensuring that the person's identification data are linked to the Wallet, in accordance with point 4(dh) of this Article;

ç) the mechanism allowing for the validation of the person's identification data, referred to in point 4(dh) of this Article, and of the identity of the relying parties;

d) the mechanism by which the authenticity and validity of the Wallet is verified.

18. The provisions of Article 11 of this Law shall apply *mutandis mutandis*, without conflicting with the provisions of point 22 of this Article.

19. The definitions in Article 30(5)(b)(ç)(d)(dh)(e)(ë)(f)(g) of this Law shall apply *mutandis mutandis* also to Wallet providers.

20. Wallets are made accessible for use by persons with disabilities on an equal basis with other users, in accordance with applicable legislation on the inclusion and accessibility of persons with disabilities.

21. The provisions made in Articles 13, 15, 16, 19 and 20 of this Law shall not apply to the provision of electronic Wallets and identification schemes.

22. The reference standards and, where necessary, the specifications and procedures to be used for the Wallet, as defined in points 3, 4, 7, 17 of this Article, shall be approved by Decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

23. By Council of Ministers' Decision, reference standards shall be approved and, where necessary, specifications and procedures are determined to facilitate the onboarding of users to the Wallet, either through electronic identification means, conforming to assurance level high or by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures that together meet the requirements of assurance level high.

24. The establishment of a digital identity Wallet, according to point 1 of this Article, in cases where it is offered as a service by a public authority, shall be determined by Council of Ministers' Decision.

Article 7
Relying party in Digital Identity Wallet

1. Where a relying party intends to rely upon the Wallet for the provision of public or private services by means of digital interaction, the relying party shall register at the Authority.

2. The registration process shall be cost-effective and proportionate-to-risk. The relying party shall ensure at least:

a) the information necessary to authenticate to the Wallet, which at a minimum includes:

i. the headquarters in which the party is established;

ii. the name and, where applicable, its registration number, as stated in an official record, together with the identifying data of that official record.

b) contact details of the relying party;

c) the use of Wallets, including an indication of the data that will be required by the party for the user.

3. The relying party shall not require users to provide any other data, other than those specified in point (c) of paragraph 2 of this Article.

4. The provisions made in paragraphs 1 and 2 of this Article shall also apply to the provision of specific services.

5. The Authority shall publish the information pursuant to paragraph 2 of this Article in an electronically signed or sealed form, suitable for automated processing.

6. The relying party registered in accordance with this Article shall inform the responsible authority of any change in the information provided, as defined in paragraph 2 of this Article.

7. The Authority shall provide a common mechanism to allow the identification and authentication of the parties involved, as referred to in point (c), paragraph 4, Article 6, of this Law.

8. When the relying party intends to be recognized in the wallet, it shall identify itself to the user.

9. The relying party shall be responsible for carrying out the procedure for authentication and verification of the validity of the person's identification data and electronic verification of the attributes required by the wallet. The relying party does not refuse the use of pseudonyms, when user identification is not required.

10. Authorized persons acting on behalf of the relying party shall be considered as involved parties and do not retain data on the content of the transaction.

11. By decision of the Council of Ministers, the technical specifications and procedures for the requirements set out in paragraphs 2, 5, 6 to 9 of this Article shall be approved in accordance with the acts set out in paragraph 23 of Article 6 of this Law and with the implementing acts of the European Commission.

Article 8

Certification of digital identity wallets

1. The conformity of the wallets and the electronic identification scheme shall be certified by the conformity assessment body according to the requirements set out in paragraphs 4, 5, 8, 14 of Article 6 of this Law and, where applicable, with the standards and technical specifications set out in paragraph 23 of Article 6 of this Law.

2. Certification of the conformity of wallets, in accordance with the requirements referred to in paragraph 1 of this Article, or parts thereof, that are important for cybersecurity, shall be carried out in accordance with the provisions made in the applicable legal framework for cybersecurity regarding cybersecurity certification schemes.

3. For the requirements referred to in paragraph 1 of this Article, whether or not related to cybersecurity, according to the cybersecurity certification scheme referred to in paragraph 2 of this Article, which does not cover or only partially covers these cybersecurity requirements, a national certification scheme shall be established for these requirements, implementing the requirements set out in paragraph 6 of this Article. Upon the accession of the Republic of Albania to the European Union, the Authority shall submit the draft national certification scheme to the European Digital Identity Cooperation Group.

4. The certification under paragraph 1 of this Article shall be valid for a period of up to five years, provided that a vulnerability assessment shall be carried out every two years. In the event that a vulnerability is identified and not corrected in a timely manner, the certification shall be revoked.

5. Compliance with the requirements set out in Article 6 of this Law regarding the processing of personal data shall be carried out in accordance with the legislation in force on the protection of personal data.

6. The reference standards, specifications and procedures for the certification of wallets, pursuant to paragraphs 1, 2 and 3 of this Article, shall be approved by decision of the Council of Ministers, in accordance with the implementing acts of the European Commission.

7. The Authority shall publish on its official website the names and addresses of the conformity assessment bodies referred to in paragraph 1 of this Article.

8. The specific criteria to be met by the conformity assessment bodies, referred to in paragraph 1 of this Article, shall be approved by decision of the Council of Ministers.

9. The wallet certification scheme is approved by decision of the Council of Ministers in accordance with the European digital identity wallet certification scheme.

Article 9

Publication of the list of certified digital identity wallets

1. Upon the accession of the Republic of Albania to the European Union, the Authority shall inform the European Commission and the European Digital Identity Cooperation Group, as defined in Article 73 of this Law, immediately of the wallets that have been provided in accordance with Article 6 of this Law and are certified by the conformity assessment bodies referred to in paragraph 1 of Article 8 of this Law, as well as the cases of revocation of a certification and the reasons for the revocation.

2. Except for the cases provided for in paragraph 17 of Article 6 of this Law, the information provided by the Authority, according to paragraph 1 of this Article, shall include at least:

a) the certificate and the wallet certification assessment report;

b) a description of the electronic identification scheme under which the wallet is offered;

c) the responsible institution and the applicable supervisory regime and information about the responsible regime in relation to the party providing the wallet;

ç) the authority or authorities responsible for the electronic identification scheme;

d) arrangements for the suspension or revocation of the electronic identification scheme or authentication or the compromised parts in question.

3. The Authority shall create and electronically maintain a list of certified wallets and publish them on its official website.

Article 10

Security breach of digital identity wallet

1. Where, for the wallets provided for in accordance with Article 6 of this Law, the validation mechanisms referred to in paragraph 7 of Article 6 or the electronic identification scheme under which they are provided have been breached or partially compromised in a way that affects their reliability or the reliability of other digital identity wallets, the Authority shall immediately suspend their provision and use. Depending on the degree of the security breach or compromise referred to in this paragraph, the Authority shall immediately withdraw the wallet. The Authority shall inform the affected users and the parties involved.

2. Where the security breach or compromise referred to in paragraph 1 of this Article is not remedied within three months of the suspension, the Authority shall withdraw the wallet and revoke its validity. The Authority shall inform the affected users and the parties involved.

3. When the security breach or compromise referred to in paragraph 1 of this Article is corrected, the Authority shall ensure the restoration and use of the wallet and immediately inform the affected users and the parties involved.

4. The Authority shall publish on its official website the updated list according to the provisions of Article 9 of this Law.

5. The list of reference standards and the procedures for the measures referred to in paragraphs 1, 2 and 3 of this Article shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

Article 11

Interoperability of digital identity wallets

1. To access an *online service* provided by a public sector body, when electronic identification and authentication are required to access this service, wallets provided in accordance with the provisions of this Law are also accepted.

2. Where private relying parties that provide services, with the exception of microenterprises and small enterprises, as defined in the legal framework in force for micro, small and medium-sized enterprises, are required by Law to use strong user authentication for online identification or where strong user authentication for online identification is required, arising from contractual obligations, including in the areas of transport, energy, banking, financial services, social security, healthcare, drinking water, postal services, digital infrastructure, education or telecommunications, these private relying parties shall, no later than 36 months from the date of entry into force of the acts referred to in Article 6 and paragraph 6 of Article 8 of this Law, and only upon voluntary request of the user, shall accept wallets offered in accordance with the provisions of this Law.

3. When providers of large online platforms require user authentication for access to online services, they shall also accept and facilitate the use of wallets that are offered in accordance with the provisions of this Law for user authentication, only upon voluntary request of the user and in relation to the minimum data necessary for the specific online service for which authentication is required.

4. The Authority, in cooperation with civil society and all stakeholders involved in the digital identity wallet, encourages wallet service providers to develop codes of conduct, with the aim of ensuring the widest possible availability and use of the digital identity wallet.

5. Within 24 months after the deployment of the wallets, the Authority shall assess the requirements, availability and use of the wallets, considering criteria such as: user acceptance, cross-border presence of the service provider, technological developments, evolution in usage patterns and consumer demand.

CHAPTER III

ELECTRONIC IDENTIFICATION

Article 12

Mutual recognition

1. Electronic identification schemes and trusted services shall be recognized and implemented in accordance with the agreements ratified by the Republic of Albania, for their acceptance and data exchange, in accordance with the legislation in force on the protection of personal data.

2. Identifications and trusted services issued by qualified trust service providers operating in the Member States of the European Union and having received the “qualified” status from the responsible authorities, as well as being part of the European Union trusted list, shall have the same legal validity and evidentiary power as those issued by a qualified trust service provider operating in the Republic of Albania.

3. For the purpose of paragraph 1 of this Article, mutual recognition shall meet the following conditions:

a) the electronic identification means is issued according to an electronic identification scheme, which is included in the list published by the relevant authorities of the states;

b) the security level of the electronic identification means corresponds to a security level equal to or higher than the security level required by the relevant public sector body to access that *online*

service in the other country, provided that the security level of that electronic identification means corresponds to a substantial or high level of security;

c) the relevant public sector body uses the level of security of substantial or high in relation to access to that *online service.*

4. An electronic identification means, issued under an electronic identification scheme, included in the list published by the responsible authorities or the European Commission and corresponding to the low security level, may be recognized by public sector bodies for the purposes of cross-border authentication for the *online* service provided by these bodies.

Article 13

Notification of electronic identification schemes

1. An electronic identification scheme is eligible for notification under paragraph 1 of Article 15 of this Law provided that the following requirements shall be met:

a) electronic means of identification, according to the electronic identification scheme, are issued by the Republic of Albania;

b) electronic identification means, under the electronic identification scheme, may be used to access at least one electronic service provided by a public sector body, which requires electronic identification;

c) the electronic identification scheme and the electronic identification means issued under this scheme must meet the requirements for at least one of the security levels, as defined in Article 14 of this Law;

ç) the published electronic identification scheme ensures that personal identification data uniquely represent a natural or legal person in accordance with the technical specifications, standards and procedures, according to the security level, set out in paragraph 3 of Article 14 of this Law, at the time of issuing the electronic identification means;

d) the party issuing the electronic identification means, according to this scheme, provides identification data within the electronic identification means, corresponding to the person to whom the means have been issued, in accordance with the technical specifications, standards and procedures for the relevant security level, set out in paragraph 3 of Article 14 of this Law;

dh) ensure the availability of authentication *online*, so that each relying party is able to confirm the person's identity data, obtained in electronic form;

e) the electronic identification scheme meets the requirements set out in paragraph 5 of Article 19 of this Law.

2. Access conditions for authentication shall be defined for parties involved, other than public sector bodies. Specific disproportionate technical requirements which prevent or significantly hinder the interoperability of electronic identification schemes shall not be imposed on such parties.

3. Cross-border authentication shall be provided free of charge when used for an electronic service provided by a public sector body.

Article 14

Security levels of electronic identification schemes

1. The electronic identification scheme, according to the definitions of paragraph 1 of Article 15 of this Law, shall ensure low, considerable and/or high levels of security for the electronic identification means issued under this scheme.

2. The low, considerable and high security levels shall meet the following criteria:

a) low level of security refers to an electronic identification means, issued under an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person and meets the technical specifications, standards and procedures related to them,

including technical controls, the purpose of which is to reduce the risk of misuse or alteration of the identity;

b) substantial level of security refers to an electronic identification means, issued under an electronic identification scheme, which provides a significant degree of confidence in the claimed or asserted identity of a person, and meets technical specifications, standards and procedures related to them, including technical controls, the purpose of which is to significantly reduce the risk of misuse or alteration of the identity;

c) high level of security refers to an electronic identification means issued under an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the significant level of security, and meets the technical specifications, standards and procedures related to them, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

3. By decision of the Council of Ministers, the minimum technical specifications, standards and procedures shall be approved, based on which the levels of security, low, considerable and high, for electronic means of electronic identification are specified, considering the following elements:

a) the procedure to confirm and verify the identity of natural or legal persons applying for the issuance of electronic identification means;

b) the procedure for issuing the requested electronic identification means;

c) the authentication mechanism through which a natural or legal person uses electronic identification means to confirm his identity to a relying party;

ç) the entity issuing the electronic identification means;

d) any other body involved in the application for the issuance of electronic identification means;

dh) technical and security specifications of the electronic identification means issued.

Article 15

Notification

1. The Authority shall immediately publish on its official website the electronic identification schemes and any subsequent changes thereto with the following information:

a) a description of the electronic identification scheme, including the security levels and the issuer of electronic identification means under the scheme;

b) the responsible institution and the applicable supervisory regime, as well as information regarding the area of responsibility as follows:

i. the party issuing the electronic identification means;

ii. the party operating the authentication procedure.

c) the entity or entities that manage the registration of the person's unique identification data;

ç) a description of the fulfillment of the requirements set out in paragraph 4 of Article 19 of this Law;

d) a description of the authentication, referred to in point (dh) of paragraph 1, paragraphs 2 and 3 of Article 13 of this Law;

dh) provisions for the suspension or revocation of the electronic identification or authentication scheme or of the compromised parts.

2. The Authority, immediately, in case of changes in electronic identification schemes or the information mentioned in paragraph 1 of this Article, shall make their update and shall publish them together with basic information on these schemes whenever necessary.

3. The Authority shall determine the format for publishing information on the electronic identification scheme pursuant to paragraph 1 of this Article.

Article 16

Security breaches in electronic identification schemes

1. When the electronic identification scheme, as defined in paragraph 1 of Article 15 of this Law, or the authentication referred to in point (dh) of paragraph 1 and paragraphs 2 and 3 of Article 13 of this Law, has been breached or partially compromised, in a way that affects the reliability of cross-border authentication of the scheme, the Authority shall suspend or revoke without delay that authentication or the compromised parts of the scheme, and shall inform the affected country.

2. When the breach or compromise referred to in paragraph 1 of this Article is corrected, the Authority shall restore the scheme and authentication according to that scheme, and shall inform the affected state.

3. If the breach or compromise referred to in paragraph 1 of this Article is not corrected within three months of the suspension or revocation, the Authority shall notify the withdrawal of the electronic identification scheme and inform the affected state.

4. A decision of the Council of Ministers shall determine the rules and criteria for the suspension and revocation of violated or partially compromised cross-border authentication and compromised parts of the electronic identification scheme.

Article 17

Liability

1. The Authority shall be liable for damage caused intentionally or negligently to any natural or legal person due to failure to fulfil obligations in a cross-border transaction, according to the points (ç) and (dh) of paragraph 1 and paragraphs 2 and 3 of Article 13 of this Law.

2. The entity issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to failure to fulfil the obligation referred to in point (d) of paragraph 1 of Article 13 of this Law.

3. The entity carrying out the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to failure to ensure the correct functioning of the authentication, referred to in point (dh) of paragraph 1 and in paragraphs 2 and 3 of Article 13 of this Law.

4. Paragraphs 1, 2 and 3 of this Article shall be applied in accordance with the legislation in force on liability for damage.

5. Paragraphs 1, 2 and 3 of this Article shall not affect the liability under the legislation in force in a transaction in which electronic identification means that fall under the electronic identification scheme notified under paragraph 1 of Article 15 of this Law are used.

Article 18

Cross-border identity matching

1. Where the relying party acts as a provider of cross-border services, it shall ensure a clear identity match for natural persons using notified electronic identification means or wallets.

2. The Authority, through the Commissioner, shall enable the determination of technical and organizational measures to ensure a high level of protection of personal data used for identity matching and to prevent user profiling.

3. The list of reference standards, specifications and procedures for the requirements referred to in paragraph 1 of this Article shall be approved by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

Article 19

Interoperability

1. In the case of mutual recognition, the national electronic identification scheme, notified under paragraph 1 of Article 15 of this Law, shall interact with other schemes.

2. For the purposes of paragraph 1 of this Article, an interaction framework shall be established.

3. The interoperability framework shall meet the following criteria:

a) aims to be neutral with regard to the technology used and does not differentiate between specific national technical solutions for electronic identification;

b) follows, as far as possible, European and international standards;

c) facilitates the implementation of privacy and security by design.

4. The interaction framework shall consist of:

a) a reference to the minimum technical requirements regarding security levels as defined in Article 14 of this Law;

b) a framework of national security levels of electronic identification schemes according to the definitions of Article 14 of this Law;

c) a reference to the minimum technical requirements for interoperability;

ç) a reference to a minimum set of personal identification data necessary to uniquely represent a natural or legal person or a natural person representing another natural or legal person, which are available through electronic identification schemes;

d) rules of procedure;

dh) mechanisms for resolving disputes;

e) common operational safety standards.

5. The interoperability framework, as defined in paragraph 4 of this Article, shall be approved by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

Article 20

Certification of electronic identification schemes

1. The conformity of electronic identification schemes, in accordance with the cybersecurity requirements set out in this Law, including the relevant cybersecurity requirements set out in paragraph 2 of Article 14 of this Law, regarding the security levels of electronic identification schemes, shall be certified by conformity assessment bodies accredited in the Republic of Albania or by the Member States of the European Union.

2. Certification under paragraph 1 of this Article shall be carried out on the basis of the national cybersecurity certification scheme, to the extent that the cybersecurity certificate or parts thereof cover these cybersecurity requirements.

3. The certification, based on paragraph 1 of this Article, shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. When a vulnerability is identified and not corrected within three months of such identification, the certification shall be revoked by the conformity assessment bodies.

4. Notwithstanding the provisions of paragraph 2 of this Article, upon the accession of the Republic of Albania to the European Union, the Authority shall request additional information on electronic identification schemes or on a certified part thereof from the responsible authority of the notifying Member State.

Article 21

Access to *hardware* and *software* features

1. In case the notified wallet providers and electronic identification means issuers use core platform services, as defined in paragraph 52 of Article 3 of this Law, for commercial or professional purposes, for the provision of wallet services to end-users, within the meaning of paragraph 40 of Article 3 of this Law, they shall have the right to access the same *hardware* or *software operating system of the* access controller (*gatekeepers*).

2. The access provided shall be effective and free of charge, regardless of whether the *hardware* or software features are part of the available operating system *or* are used by the access controller (*gatekeeper*) when providing such services. This Article shall not conflict with the provisions of paragraph 13 of Article 6 of this Law.

CHAPTER IV

TRUSTED SERVICES

SECTION 1

GENERAL PROVISIONS

Article 22

Liability and burden of proof

1. Notwithstanding the provisions of paragraph 2 of this Article and without prejudice to the provisions of the legislation in force on the protection of personal data, trusted service providers shall be liable for damage caused, intentionally or through negligence, to any natural or legal person, due to the failure to fulfil obligations, according to the provisions of this Law. Any natural or legal person who has suffered material or non-material damage, as a result of violations of the provisions made in this Law by the trusted service provider, shall have the right to claim compensation in accordance with the provisions of the legislation in force.

2. The burden of proving the intention or negligence for the damage caused by an unqualified trust service provider shall lie with the natural or legal person claiming the damage mentioned above.

3. The intent or negligence of a qualified trust service provider shall be presumed in all cases, except when that qualified trust service provider proves that the aforementioned damage occurred through no fault of his own.

4. Trust service providers shall inform their clients in advance of the limitations of the use of the services they provide, even if these limitations are also known to third parties. Trust service providers shall not be liable for damages resulting from the use of the services that exceed the limitations made known.

5. The provisions made in paragraphs 1, 2, 3 and 4 of this Article shall be applied in accordance with the provisions of the legislation in force regarding liability for damage.

Article 23

Accessibility for persons with disabilities and special needs

The use of electronic identification means, trusted services and end-user products used in the provision of these services shall be made possible in simple and understandable language, in accordance with the United Nations Convention on the Rights of Persons with Disabilities and applicable legislation on the inclusion and accessibility of persons with disabilities, including persons with special needs, such as the elderly and persons with limited access to digital technologies.

SECTION 2

UNQUALIFIED TRUSTED SERVICES

Article 24

Requirements to be met by trusted service providers

1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the security risks presented by the trust services they provide. These measures shall ensure that the level of security is proportionate to the degree of risk, considering the state of the art. In particular, trust service providers shall take measures to prevent and minimise the impact of security incidents and to inform interested parties of the effects caused by such incidents.

2. Immediately and in any case, within 24 hours of receiving knowledge, pursuant to paragraph 1 of this Article, qualified and non-qualified trust service providers shall notify the Authority and, where necessary, the Commissioner of any security breach or loss of integrity that has a significant impact on the trust service provided or on personal data.

3. When the security breach or loss of integrity has a negative impact on a natural or legal person to whom the trust service has been provided, the trust service provider shall immediately notify the latter of the security breach or loss of integrity.

4. If a security breach or loss of integrity concerns two or more countries, the Authority shall inform the supervisory authorities in the other relevant countries and the European Union Agency for Cybersecurity (hereinafter ENISA).

5. The Authority shall inform the public or require the trusted service provider to do so when it decides that the publication of information on the security breach or loss of integrity is in the public interest.

6. Upon the accession of the Republic of Albania to the European Union, the Authority shall annually send to ENISA a summary of notifications of security breaches and loss of integrity received from trusted service providers.

7. The measures, formats, procedures and deadlines, in accordance with paragraphs 1, 2, 3, 4, 5 of this Article, shall be approved by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

Article 25

Requirements for non-qualified trust service providers

1. A non-qualified trust service provider, which provides non-qualified trust services, shall:

have appropriate policies and take appropriate measures to manage legal, business, operational and other direct or indirect risks in the provision of non-qualified trust services, which, notwithstanding the provisions of Law no. 25/2024 “On cybersecurity” on risk management, include at least measures relating to:

i. procedures for accepting and registering a trust service;

ii . procedural or administrative controls necessary to provide trust services;

iii . management and implementation of trust services.

b) notify immediately and no later than 24 hours after becoming aware of any breach or interruption of security the Authority, the affected individuals, the public, if it is in the public interest, and other responsible authorities, of any breach of security or interruption in the provision of the service or the implementation of the measures referred to in subsections “i”, “ ii ” or “ iii ” of point “a” of this Article, which have a significant impact on the provision of the trust service or on personal data.

2. The reference list of standards, specifications and procedures, according to point 1(a) of this article, is approved by decision of the Council of Ministers, in accordance with the implementing acts of the European Commission.

SECTION 3

TRUST QUALIFIED SERVICES

Article 26

Supervision of qualified trust service providers

1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The audit shall be carried out to confirm that the qualified trust service providers and the qualified trust services provided by them comply with the requirements set out in this Law, as well as with the provisions relating to risk management, in accordance with the legislation in force on cybersecurity. Qualified trust service providers shall submit the conformity assessment report to the Authority within three working days of receipt by the conformity assessment body.

2. Qualified trust service providers shall inform the Authority no later than one month of any planned inspection, pursuant to point 1 of this Article, allowing the Authority to participate in observer status upon its request.

3. The Authority shall publish in its official website the list with the names, addresses and accreditation details of the conformity assessment bodies referred to in point 1 of this article, as well as any subsequent amendments thereto.

4. Notwithstanding the provisions of paragraph 1 of this Article, the Authority may at any time carry out an inspection or request a conformity assessment body to carry out a conformity assessment of qualified trust service providers, at the latter's expense, to confirm compliance with the requirements set out in this Law. When the Authority ascertains a violation of the rules on the protection of personal data, it shall notify the Commissioner of the results of its inspections.

5. When the Authority finds irregularities in the activity of a qualified trust service provider, it recommends their correction, within a certain time limit, in fulfilling the requirements of this law. When the provider fails to comply with the recommendations within the time limit set by the Authority, and taking into account the extent, duration and consequences of this failure, the latter shall decide to withdraw the “qualified” status for this provider or the services provided by it.

6. The Authority, as the body responsible for cybersecurity, when it finds that the qualified trust service provider does not meet the requirements set out in the risk management measures, according to the legislation in force on cybersecurity, when the extent, duration and consequences of that damage are justified, shall remove the “qualified” status from the trust service provider or the trust service provided by it.

7. When the Authority is informed by the Commissioner that the qualified trust service provider has not met the requirements set out in the legislation in force for the protection of personal data,

when the extent, duration and consequences of the damage caused are justified, the Authority shall withdraw the "qualified" status from the provider or the trust service provided by it.

8. The Authority shall inform the qualified trusted service provider of the removal of the "qualified" status or of the "qualified" status of the service provided by it, and shall update the trusted list.

9. By decision of the Council of Ministers, the specifications and procedures are determined in accordance with the implementing acts of the European Commission as follows:

a) accreditation of conformity assessment bodies and for the conformity assessment report, referred to in point 1 of this article;

b) control requirements for conformity assessment bodies to carry out conformity assessment, including the comprehensive assessment of qualified trust service providers, pursuant to point 1 of this article;

c) conformity assessment schemes for carrying out conformity assessment of qualified trust service providers by conformity assessment bodies and for issuing the report, according to point 1 of this article.

Article 27

Initiation of the activity of a qualified trust service provider

1. Trust service providers who have not obtained the "qualified" status and intend to provide qualified trust services shall submit to the Authority a request accompanied by the relevant documentation, including the conformity assessment report issued by a conformity assessment body, which confirms the fulfillment of the requirements set out in this law and the requirements related to risk management, according to the legislation in force on cybersecurity.

2. The Authority shall verify whether the trust service provider and the trust services provided by it meet the requirements set out in this law and in particular the requirements for qualified trust service providers and for the qualified trust services they provide.

3. Notwithstanding the conformity assessment report required under point 1 of this Article, the Authority, as the body responsible for cybersecurity, shall verify the fulfillment of the requirements of the trusted service provider regarding risk management measures, as defined in the applicable cybersecurity legislation, and shall draft a report with the results within two months of the submission of the request. This deadline may be extended by the Authority for justified reasons.

4. If the Authority finds that the trust service provider and the trust services provided by it meet the requirements set out in this Law, no later than three months from the receipt of the request from the trust service provider, the Authority shall grant the "qualified" status to the trust service provider and the trust services provided by it, and shall update the trusted list. If the verification by the Authority has not been completed within three months from the receipt of the request from the trust service provider, the Authority shall inform the trust service provider of the reasons for the delay and the period within which the verification must be completed, which shall not exceed six months.

5. Qualified trust service providers begin to provide qualified trust services after obtaining the "qualified" status, as well as after publication in the trusted list.

6. The notification and verification formats and procedures regarding the documentation of trusted service providers for obtaining qualified status are approved by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

7. The registration fee for qualified trust service providers is approved by decision of the Council of Ministers and is paid 100% into the state budget.

Article 28

Trusted lists

1. The Authority shall create, maintain and publish the trusted list, which includes information regarding qualified trust service providers, as well as information on the qualified trust services provided by them, operating in the Republic of Albania.

2. The Authority shall create, store, and publish in a secure manner the electronically signed or sealed trusted list and publishes it on its official website in accordance with the provisions of European Union standards.

3. Upon accession of the Republic of Albania to the European Union, the Authority shall notify the Commission of the information on the authority responsible for creating, maintaining and publishing national trusted lists and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.

4. The Authority shall make available to the public, through a secure channel, the information referred to in point 3 of this article, in electronically signed or sealed form, suitable for automated processing.

5. The technical specifications and formats for the applicable trusted lists, for the purposes of points 1 to 4 of this Article, shall be approved by decision of the Council of Ministers, in accordance with the technical specifications and formats approved by the European Commission.

Article 29

European Union trust mark for qualified trust services

1. After obtaining the "qualified" status referred to in points 2, 3 and 4 of Article 27 of this Law, as well as after publication in the trusted list referred to in point 1 of Article 28 of this Law, qualified trust service providers may use the European Union trust mark to indicate in a simple, recognizable and clear manner the qualified trust services they provide.

2. When using the trust mark for qualified trust services, referred to in point 1 of this Article, qualified trust service providers must ensure that a link to the relevant trusted list is available on their official website.

Article 30

Requirements for qualified trust service providers

1. A qualified trust service provider, which issues a qualified certificate or a qualified electronic attestation of attributes, verifies the identity and, where applicable, any specific attributes of the natural or legal person to whom the qualified certificate or qualified electronic attestation of attributes are issued.

2. Identity verification under point 1 of this article shall be carried out by appropriate means by the qualified trust service provider, directly or by a third party, based on one of the following methods or, where necessary, in a combination thereof according to the definitions of point 4 of this article, as follows:

a) by means of a wallet or an electronic identification means notified in accordance with the requirements set out in Article 14 of this law regarding the level of assurance "high";

b) by means of certificate of a qualified electronic signature or qualified electronic seal, issued in accordance with (a), (c) or (ç) in this point;

c) using other identification methods that ensure the identification of the person with the highest level of assurance, whose conformity is confirmed by a conformity assessment body;

ç) through the physical presence of the natural person or of an authorized representative of the legal person through authorization and appropriate procedures in accordance with the legislation in force.

3. The verification of the attributes referred to in point 1 of this article shall be carried out by appropriate means by the qualified trust service provider, directly or through a third party, based on one of the following methods or, where necessary, a combination thereof, in accordance with the definitions of point 4 of this article as follows:

a) by means of a wallet or a notified electronic identification means, in accordance with the requirements set out in Article 14 of this law regarding the high level of assurance;

b) by means of a certificate of a qualified electronic signature or qualified electronic seal, issued in accordance with (a), (c) or (ç) in this point;

c) by means of a qualified electronic attestation of attributes;

ç) using other methods that ensure the verification of attributes with a high level of confidence, the conformity of which is confirmed by a conformity assessment body;

d) through the physical presence of the natural person or an authorized representative of the legal person, through authorization and appropriate procedures, in accordance with the legislation in force.

4. The reference list of standards and, where necessary, the specifications and procedures for verifying identity and attributes, in accordance with points 1, 2 and 3 of this article, shall be approved by decision of the Council of Ministers, in accordance with the provisions of the implementing acts of the European Commission.

5. The qualified trust service provider must:

a) inform the Authority at least one month before the implementation of any change in the provision of qualified trust services or at least three months in advance in the event of cessation of activity;

b) employ personnel and, where applicable, subcontractors, who possess the necessary expertise, reliability, experience and qualifications and have received appropriate training on security and personal data protection issues, as well as implement administrative and management procedures that correspond to European and international standards;

c) possess the necessary financial resources for possible compensation, according to Article 22 of this law;

ç) inform, before entering into a contractual relationship, in a clear, comprehensive and easily accessible manner, in a publicly and individually accessible space, any person seeking to use the qualified trust service of the terms and conditions of use, as well as any restrictions on the use of this service;

d) use reliable systems and products that are protected against modification and that guarantee the technical security and reliability of the processes supported by them, including the use of appropriate cryptographic techniques;

dh) use reliable systems to store the data provided to them in a verifiable form, so that:

i. they may be made available to the public only with the consent of the person to whom these data belong;

ii. changes or entries in this data may only be made by authorized persons;

iii. the data can be checked for its authenticity.

e) regardless of risk management measures, according to the legislation in force on cybersecurity, qualified trusted service providers must have appropriate policies and take appropriate measures to manage legal, business, operational and other direct or indirect risks to the provision of qualified trust services, including at least the following measures:

i. procedures for registration and admission to a service;

ii. procedural or administrative controls;

iii. management and implementation of services.

ë) in the event of an incident, immediately and in any case within 24 hours from the moment of its identification, notify the Authority, the affected individuals, other relevant competent bodies and the public, when it is in the public interest, as well as for any security breach or interruption in the provision of the service or the implementation of the measures referred to in subsections “e(i)”, “e(ii)” or “e(iii)” of this article, which have a significant impact on the provision of the trust service or on personal data;

f) take appropriate measures against falsification, theft, misuse, deletion, alteration or making data inaccessible;

g) record and keep accessible, for as long as necessary after the cessation of activity, all relevant information on data issued and received by the qualified trust service provider, for the purpose of their use in legal proceedings, as well as to ensure the continuity of the service. Such records shall be kept electronically;

gj) have an updated plan to ensure continuity of service in accordance with the provisions of point 3(gj) of Article 70 of this law;

h) create and maintain an updated database of qualified certificates issued.

The Authority shall request additional information in addition to the information notified under point (a) of this point or the outcome of the conformity assessment report, and may make the issuance of the permit conditional on the implementation of the changes envisaged for qualified trust services. If the verification has not been completed within three months of receipt of the request, the Authority shall inform the trust service provider of the reasons for the delay and the period within which the verification must be completed.

6. If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall record this revocation in the certificate database and publish the revocation status of the certificate in any case within 24 hours of receiving the holder's request. The revocation shall take effect immediately after its publication.

7. In accordance with the provisions of point 6 of this Article, qualified trust service providers shall provide the relying party with any information on the validity or revocation status of qualified certificates issued by them. This information shall be available at any time, even beyond the validity period of the certificates, in an automated manner that is reliable, free of charge and effective.

8. The provisions in points 6 and 7 of this article shall apply in accordance with the revocation of qualified electronic attestation of attributes.

9. The list of reference standards, specifications and procedures for the requirements referred to in point 5 of this Article shall be adopted by decision of the Council of Ministers, in accordance with the provisions of the implementing acts of the European Commission. Compliance with the requirements set out in this point shall be deemed to have been achieved when these standards, specifications and procedures have been met.

SECTION 4

ELECTRONIC SIGNATURES

Article 31

Legal effects of electronic signature

1. An electronic signature has legal effect and is admissible as evidence in legal proceedings even if it is in electronic form or does not meet the requirements for qualified electronic signatures.

2. A qualified electronic signature has the same legal effect as a handwritten signature.

Article 32

Requirements for advanced electronic signatures

1. The advanced electronic signature meets the following requirements:

a) is uniquely linked to the signatory;

b) enables the identification of the signatory;

c) it is created using data for creating an electronic signature, with a high level of confidence, belonging exclusively to the signatory;

ç) is linked to the signed data in such a way as to enable easy detection of any subsequent changes to these data.

2. The reference standards and, where necessary, the specifications and procedures for advanced electronic signatures shall be adopted by decision of the Council of Ministers, in accordance with the provisions of the implementing acts of the European Commission. Compliance with the requirements for advanced electronic signatures shall be presumed where an advanced electronic signature complies with the standards, specifications and procedures.

Article 33

Electronic signatures in public services

1. If an advanced electronic signature is required for use in an online service provided by or on behalf of a public sector body, the public sector body shall recognize advanced electronic signatures based on a qualified certificate for electronic signatures and qualified electronic signatures in at least one of the specified formats or methods, as defined in point 4 of this Article.

2. If the use of an advanced electronic signature based on a qualified certificate is required in public electronic services provided by a public sector body to use an *online service* provided by or on behalf of a public sector body, the public sector body shall recognize advanced electronic signatures based on a qualified certificate and qualified electronic signatures in at least one of the specified formats or methods as defined in point 4 of this article.

3. In a cross-border *online service* provided by a public sector body, the security level of the electronic signature cannot be higher than that of a qualified electronic signature.

4. Reference formats for advanced electronic signatures and reference methods, when alternative formats are used, shall be approved by decision of the Council of Ministers, in accordance with the implementing acts of the European Commission.

Article 34

Certificate for qualified electronic signature

1. Certificates for qualified electronic signatures shall meet the requirements set out in point 2 of this article.

2. Qualified certificates for electronic signatures shall contain:

a) an indication, at least in a format suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;

b) a set of data, clearly representing the qualified trust service provider issuing qualified certificates, including at least the country in which this provider is established and:

i. for a legal entity: the name and registration number (NUIS), which appears in the official records;

ii . for a natural person: the name of the person.

c) at least the name of the signatory or a pseudonym. If a pseudonym is used, it must be clearly indicated;

ç) the data on the validity of the electronic signature, which corresponds to the data on the creation of the electronic signature;

d) details of the start and end of the certificate's validity period;

dh) the certificate identification code, which must be unique for the qualified trust service provider;

e) advanced electronic signature or advanced electronic seal, issued by a qualified trust service provider;

ë) the location of the relevant certificate of the advanced electronic signature or advanced electronic seal, referred to in (e) in this point, which is provided free of charge;

f) information or location of services that can be used to identify the validity status of the qualified certificate;

g) where applicable, an appropriate indicator enabling automatic processing, indicating that the data for the creation of an electronic signature are linked to the data for its validity and are placed on the device for the creation of a qualified electronic signature.

3. Certificates for qualified electronic signatures are not subject to any mandatory requirements that exceed the requirements set out in point 2 of this article.

4. Certificates for qualified electronic signatures may include additional non-mandatory specific attributes, which do not affect the interoperability and recognition of qualified electronic signatures.

5. If a certificate for qualified electronic signatures is revoked after initial activation, it shall lose its validity from the moment of revocation and its status shall not be reverted under any circumstances.

6. By decision of the Council of Ministers, rules shall be established for the temporary suspension of a qualified electronic signature certificate in the following cases:

a) if a certificate for qualified electronic signature is temporarily suspended, that certificate loses its validity for the period of suspension;

b) the period of suspension is clearly indicated in the certificate database and the suspension status must be visible during the suspension period from the service providing information on the status of the certificate.

7. The reference standards and, when necessary, the specifications and procedures for qualified electronic signatures shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission. Compliance with the requirements set out in point 2 of this Article shall be presumed where a certificate for qualified electronic signature complies with the standards, specifications and procedures.

Article 35

Requirements for devices for creating qualified electronic signatures

1. Devices for creating qualified electronic signatures must meet the requirements set out in point 2 of this article.

2. Devices for creating qualified electronic signatures, by means of appropriate technical and procedural means, shall ensure at least that:

a) the confidentiality of the electronic signature creation data used for this electronic signature is secure;

b) the data used to create the electronic signature may only be used once;

c) the data for creating a high-security electronic signature cannot be extracted outside the electronic signature creation device, and are reliably protected against forgery, using available technology;

ç) the data for creating an electronic signature are securely protected by the legitimate signatory against unauthorized use.

3. Devices for creating a qualified electronic signature do not alter the signed data or prevent the signature creator from accessing the data before creating the signature.

4. The generation or management of data for creating the electronic signature or the duplication of data for the creation of signature for *backup purposes* shall be carried out only on behalf of the signatory, at the request of the signatory and by a qualified trust service provider, which offers a qualified trust service for the management of a qualified remote electronic signature creation device.

5. The reference numbers of the standards for qualified electronic signature creation devices shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission. Compliance with the requirements set out in point 2 of this Article shall be presumed when a qualified electronic signature creation device complies with these standards.

Article 36

Requirements for the qualified service for the management of qualified remote electronic signature creation devices

1. The management of qualified remote electronic signature creation devices, as a qualified service, shall be performed only by a qualified trust service provider, who:

a) generates or manages the electronic signature creation data on behalf of the signatory;

b) notwithstanding the provisions of point 2(b) of Article 35 of this law, duplicates the data for creating the electronic signature only for *backup purposes*, provided that the following requirements are met:

i. security of duplicated data must be at the same level of security as the original data;

ii . the number of duplicated data should not exceed the minimum necessary to ensure continuity of service.

c) it complies with any requirements identified in the certification report of the specific qualified remote electronic signature creation device, issued under Article 37 of this Law.

2. The reference standards and, where necessary, the specifications and procedures, for the purposes of point 1 of this Article, shall be adopted by decision of the Council of Ministers, in accordance with the implementing acts of the European Commission.

Article 37

Certification of qualified electronic signatures creation devices

1. The conformity of devices for creating qualified electronic signatures with the requirements set out in point 2 of Article 35 of this law shall be certified by conformity assessment bodies from the list published by the Authority or the European Commission.

2. The Authority shall publish the names and addresses of conformity assessment bodies, as defined in point 1 of this Article, on its official website.

3. The certification referred to in point 1 of this article is based on the following processes:

a) in a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products, included in the list established in accordance with point 2 of this article; or

b) in a process other than the process referred to in (a) of this point, provided that it uses comparable levels of security and provided that the conformity assessment bodies referred to in point 1 of this Article notify the Authority of the process.

This process may only be used in the absence of standards referred to in (a) of this point, or when a security assessment process referred to in (a) of this point is ongoing.

4. The validity of the certification referred to in point 1 of this Article shall not exceed five years, provided that vulnerability assessments are carried out every two years. When vulnerabilities are identified and not corrected, the certification shall be cancelled.

5. The list of standards for the assessment of the security of information technology products, referred to in point 3(a) of this article, shall be approved by decision of the Council of Ministers, in accordance with the implementing acts of the European Commission.

6. Criteria that conformity assessment bodies must meet, according to point 1 of this article, are approved by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

Article 38

Publication of the list of certified devices for creating qualified electronic signatures

1. Conformity assessment bodies in the Republic of Albania shall, within 30 days from the completion of the certification process of devices for the creation of qualified electronic signatures, submit to the Authority the information on the certified devices. The Authority shall recognize the list of certified devices published by the European Commission. Conformity assessment bodies shall be obliged to notify the Authority of the revocation of the certification of devices within 30 days from the revocation.

2. The Authority creates, publishes and maintains the list of certified devices for the creation of qualified electronic signatures.

3. The format and applicable procedures, for the purposes of point 1 of this article, shall be approved by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

Article 39

Requirements for certifying the validity of qualified electronic signatures

1. The process for certifying the validity of a qualified electronic signature confirms the validity of a qualified electronic signature provided that:

a) the certificate supporting the signature at the time of signing was a certificate for qualified electronic signature, in accordance with the requirements of point 2 of Article 34 of this law;

b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

c) the signature validation data corresponds to the issued data of the relying parties;

ç) the unique set of data representing the signatory in the certificate has been correctly provided to the relying party;

d) the use of any pseudonym is clearly indicated to the relying party if the pseudonym was used at the time of signing;

dh) the electronic signature was created by a qualified electronic signature creation device;

e) the integrity of the signed data has not been compromised;

ë) the requirements provided for in Article 32 of this law have been met at the time of signing.

Compliance with the requirements set out in point 1 of this Article shall be taken into account when the validation of qualified electronic signatures complies with the standards, specifications and procedures referred to in point 3 of this Article.

2. The system used for validating the qualified electronic signature shall provide the relying parties the correct result of the validation process and allows the relying parties to identify any potential security issues.

3. The reference standards and, where necessary, the specifications and procedures for verifying the validity of qualified electronic signatures shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

Article 40

Requirements for the validation of advanced electronic signatures based on qualified certificates

1. The process for the validation of an advanced electronic signature, based on a qualified certificate, confirms the validity of an advanced electronic signature, based on a qualified certificate, by fulfilling the following conditions:

a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signatures, complying with the requirements laid down in Article 34(2) of this Law;

b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

c) the signature validation data correspond to the data provided to the relying party;

ç) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;

d) where a pseudonym is used at the time of signing, the use of the pseudonym is clearly indicated to the relying party;

dh) the electronic signature was created by a qualified electronic signature creation device;

e) the integrity of the signed data has not been compromised;

ë) the requirements laid down in Article 32 of this Law were fulfilled at the time of signing.

Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the validation of qualified electronic signatures complies with the standards, specifications and procedures referred to in paragraph 3 of this Article.

2. The system used for the validation of qualified electronic signatures shall provide the relying parties with the correct result of the validation process and shall enable the relying parties to detect any security-related issues.

3. The reference standards and, where necessary, the specifications and procedures for the validation of qualified electronic signatures shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

Article 40

Requirements for the validation of advanced electronic signatures based on qualified certificates

1. The validation process for an advanced electronic signature based on a qualified certificate shall confirm the validity of an advanced electronic signature based on a qualified certificate, provided that:

a) the certificate supporting the signature was, at the time of signing, a qualified certificate for electronic signatures complying with the requirements laid down in Article 34(2) of this Law;

b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

c) the signature validation data correspond to the data provided to the relying party;

ç) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;

d) where a pseudonym was used at the time of signing, the use of the pseudonym is clearly indicated to the relying party;

dh) the integrity of the signed data has not been compromised;

e) the requirements laid down in Article 32 of this Law were met at the time of signing.

2. The system used for validating an advanced electronic signature based on a qualified certificate shall provide the relying party with the correct result of the validation process and shall enable the relying party to detect any security-related issues.

3. The reference standards and, where necessary, the specifications and procedures for the validation of advanced electronic signatures based on qualified certificates shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission. Compliance with the requirements set out in paragraph 1 of this Article shall be presumed where the validation of the advanced electronic signature, based on qualified certificates, is carried out in accordance with these standards, specifications, and procedures.

Article 41

Qualified validation service for qualified electronic signatures

1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider that:

a) provides for the validation process in accordance with the requirements laid down in Article 39(1) of this Law;

b) enables relying parties to receive the result of the validation process in an automated manner that is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the qualified validation service provider.

2. The reference standards and, where necessary, the specifications and procedures for the qualified validation service referred to in paragraph 1 of this Article shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.
Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the qualified validation service for qualified electronic signatures complies with those standards, specifications and procedures.

Article 42

Qualified preservation service for qualified electronic signatures

1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

2. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures comply with the standards, specifications and procedures referred to in paragraph 3 of this Article.

3. The reference standards and, where necessary, the specifications and procedures for the qualified preservation service for qualified electronic signatures shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

SECTION 5

ELECTRONIC SEAL

Article 43

Legal effects of the electronic seal

1. An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.

2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

Article 44

Requirements for advanced electronic seals

1.An advanced electronic seal shall meet the following requirements:

(a) it is uniquely linked to the creator of the seal;

(b) it is capable of identifying the creator of the seal;

(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

(ç) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

2. The reference standards and, where necessary, the specifications and procedures for advanced electronic seals shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission. Compliance with the requirements for advanced electronic seals shall be presumed where an advanced electronic seal complies with those standards, specifications and procedures.

Article 45

Electronic seals in public services

1. If an advanced electronic seal is required to use an *online* service offered by, or on behalf of, a public sector body, that public sector body shall recognise advanced electronic seals based on qualified certificates for electronic seals and qualified electronic seals in at least the reference formats or by using the methods referred to in paragraph 4 of this Article.

2. If an advanced electronic seal based on a qualified certificate is required to use an *online* service offered by, or on behalf of, a public sector body, that public sector body shall recognise advanced electronic seals based on qualified certificates and qualified electronic seals in at least the reference formats or by using the methods referred to in paragraph 4 of this Article.

3. In a cross-border *online* service provided by a public sector body, the required level of security of the electronic seal shall not exceed the level of security of a qualified electronic seal.

4. The reference formats for advanced electronic seals and the reference methods where alternative formats are used shall be adopted by decision of the Council of Ministers in accordance with the acts adopted by the European Commission.

Article 46

Qualified certificates for electronic seals

1. Qualified certificates for electronic seals shall meet the requirements laid down in paragraph 2 of this Article.

2. Qualified certificates for electronic seals shall contain:

a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seals;

b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates, including at least the State in which that provider is established and:

i. for a legal person: the name and, where applicable, the registration number as stated in the official records;

ii. for a natural person: the person's name;

c) at least the name of the seal creator and, where applicable, the registration number as stated in the official records;

ç) electronic seal validation data corresponding to the electronic seal creation data;

d) the beginning and end of the period of validity of the certificate;

dh) the certificate identity code, which shall be unique for the qualified trust service provider;

e) the advanced electronic signature or advanced electronic seal of the qualified trust service provider issuing the qualified certificate;

ë) the location at which the advanced electronic signature or advanced electronic seal referred to in point (e) is available free of charge;
f) information on, or the location of, the services that may be used to verify the validity status of the qualified certificate;
g) if the electronic seal creation data related to the electronic seal validation data are located in a qualified electronic seal creation device, an appropriate indication thereof, at least in a form suitable for automated processing.
3. Qualified certificates for electronic seals shall not be subject to any mandatory requirements other than those laid down in paragraph 2 of this Article.
4. Qualified certificates for electronic seals may contain additional non-mandatory specific attributes. Such attributes shall not affect the interoperability and recognition of qualified electronic seals.
5. If a qualified certificate for an electronic seal has been revoked after its initial activation, it shall lose its validity from the moment of its revocation and its status shall not under any circumstances be reinstated.
6. The rules governing the temporary suspension of qualified certificates for electronic seals shall be determined by decision of the Council of Ministers under the following conditions:
a) if a qualified certificate for an electronic seal has been temporarily suspended, that certificate shall lose its validity for the duration of the suspension;
b) the suspension period shall be clearly indicated in the certificate database, and the suspension status shall be visible, for the duration of the suspension, through the service providing information on the certificate status.
7. The reference standards and, where necessary, the specifications and procedures for qualified certificates for electronic seals shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission. Compliance with the requirements laid down in paragraph 2 of this Article shall be presumed where a qualified certificate for an electronic seal complies with those standards, specifications and procedures.

Article 47

Equipment for creating qualified electronic seals

1. The requirements laid down in Article 35 of this Law shall apply, where appropriate, to qualified electronic seal creation devices.

2. The requirements laid down in Article 37 of this Law shall apply, where appropriate, to the certification of qualified electronic seal creation devices.

3. The requirements laid down in Article 38 of this Law shall apply, where appropriate, to the publication of a list of certified qualified electronic seal creation devices.

Article 48

Requirements for the qualified remote management service for qualified electronic seal creation devices

The provisions laid down in Article 36 of this Law shall apply, insofar as applicable, to the qualified remote management service for qualified electronic seal creation devices.

Article 49

Validation and preservation service for qualified electronic seals

The provisions laid down in Articles 39, 41 and 42 of this Law shall apply, insofar as applicable, to the validation and preservation of qualified electronic seals.

Article 50

Requirements for the validation of advanced electronic seals based on qualified certificates

The provisions laid down in Article 40 of this Law shall apply, insofar as applicable, to the validation of advanced electronic seals based on qualified certificates.

SECTION 6

ELECTRONIC TIME STAMPS

Article 51

Legal effects of the electronic time stamp

1. An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely because it is in electronic form or because it does not meet the requirements for qualified electronic time stamps.

2. A qualified electronic time stamp shall benefit from the presumption of the accuracy of the date and time it indicates and the integrity of the data to which the date and time are bound.

Article 52

Requirements for qualified electronic time stamp

1. A qualified electronic time stamp shall meet the following requirements:

a) it binds the date and time to the data in such a manner as to reasonably prevent the possibility of undetectable alteration of the data;

b) it is based on an accurate time source linked to Coordinated Universal Time (UTC);

c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal, provided by a qualified trust service provider, or by an equivalent method.

2. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the binding of the date and time to the data and the accuracy of the time source comply with the standards, specifications and procedures referred to in paragraph 3 of this Article.

3. The reference standards and, where necessary, the specifications and procedures for the binding of the date and time to data and for determining the accuracy of time sources shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

SECTION 7

ELECTRONIC REGISTERED DELIVERY SERVICES

Article 53

Legal effects of providing electronic registered delivery services

1. Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form or that it does not meet the requirements for a qualified electronic registered delivery service.

2. Data sent and received by means of a qualified electronic registered delivery service shall benefit from the presumption of the integrity of the data, of the sending of the data by the identified sender, of the receipt of the data by the identified addressee, and of the accuracy of the date and time of sending and receipt, as evidenced by the qualified electronic registered delivery service.

Article 54

Requirements for the provision of qualified electronic registered delivery services

1. A qualified electronic registered delivery service shall meet the following requirements:
a) it is provided by one or more qualified trust service providers;
b) it ensures a high level of security in identifying the sender;
c) it ensures identification of the addressee prior to the delivery of data;
ç) the sending and receipt of data are secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider, in such a way as to prevent any detectable alteration of the data;
d) any change to the data necessary for the purpose of sending or receiving the data is clearly indicated to the sender and the addressee;
dh) the date and time of sending and receipt of the data, as well as any changes thereto, are indicated by a qualified electronic time stamp.
2. Where data are transferred between two or more qualified trust service providers, the requirements laid down in paragraph 1 of this Article shall apply to all such qualified trust service providers.
3. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the sending and receiving processes comply with the standards, specifications and procedures referred to in paragraph 4 of this Article.
4. The reference standards and, where necessary, the specifications and procedures for the processes for sending and receiving data shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.
5. Qualified electronic registered delivery service providers may agree on the interoperability of the qualified electronic registered delivery services they provide. Such interoperability shall comply with the requirements laid down in paragraph 1 of this Article and compliance shall be confirmed by a conformity assessment body.
6. The reference standards and, where necessary, the specifications and procedures for the interoperability framework referred to in paragraph 5 of this Article shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission. The technical specifications and content of the standards shall be cost-effective and proportionate.

SECTION 8

WEBSITE AUTHENTICATION

Article 55

Requirements for qualified website authentication certificates

1. Qualified website authentication certificates shall meet the requirements laid down in paragraph 2 of this Article. The conformity assessment of those requirements shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 5 of this Article.

2. Qualified website authentication certificates shall contain:

a) an indication, in a form suitable for automated processing, that the certificate has been issued as a qualified website authentication certificate;

b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates, including at least the State in which that provider is established and:

i. for a legal person: the name and, where applicable, the registration number (NUIS) as stated in the official records;

ii. for a natural person: the person's name;

c) for natural persons, at least the name of the person to whom the certificate is issued or a pseudonym, and where a pseudonym is used it shall be clearly indicated;

ç) for legal persons, a unique set of data unambiguously representing the legal person to whom the certificate is issued, including at least the name of the legal person and, where applicable, the registration number (NUIS) as stated in the official records;

d) the address, including city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as recorded in official records;

dh) the *domain* name(s) managed by the natural or legal person to whom the certificate is issued;

e) the beginning and end of the period of validity of the certificate;

ë) the certificate identity code, which shall be unique for the qualified trust service provider;

f) the advanced electronic signature or advanced electronic seal of the qualified trust service provider issuing the qualified certificate;

g) the location of the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (f), made available free of charge;

gj) information on, or the location of, services used to verify the validity status of the certificate.

3. Qualified website authentication certificates issued in accordance with paragraph 1 of this Article shall be recognised by *web browser providers*. *Web browser providers* shall ensure that identity data and any additional attributes indicated in the certificate are easily accessible to users. *Web browser providers* shall ensure support for and interoperability with qualified website authentication certificates referred to in paragraph 1 of this Article, with the exception of micro and small enterprises, in accordance with applicable legislation on small and medium-sized enterprises, during the first five years of their operation as web browser service providers.

4. Qualified website authentication certificates shall not be subject to any mandatory requirements other than those laid down in paragraph 2 of this Article.

5. The reference standards and, where necessary, the specifications and procedures for qualified website authentication certificates referred to in paragraph 1 of this Article shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

Article 56

Preventive cybersecurity measures

1. Web browser providers shall not take any measures contrary to the obligations laid down in Article 55 of this Law, in particular the requirements relating to the recognition of qualified website authentication certificates and the display of identity data provided, in such a way that they are easily accessible to users.

2. By way of derogation from paragraph 1 of this Article, and only where concerns are raised regarding security breaches or loss of integrity of a certificate or identified group of certificates, web browser providers may take preventive measures in relation to that certificate or group of certificates.

3. Where a web browser provider takes preventive measures in accordance with paragraph 2 of this Article, it shall immediately notify the Authority, the subject to whom the certificate has been issued, and the qualified trust service provider that issued that certificate or group of certificates, in writing, of the issues concerned, together with a description of the measures taken to mitigate those issues. Upon receipt of such notification, the Authority shall confirm receipt thereof to the web browser provider.

4. The Authority shall verify the issues raised in the notification received in accordance with Article 70(3)(i) of this Law. Where, following such verification, the Authority finds that there are no grounds for withdrawal of the qualified status of the certificate, it shall inform the web browser provider accordingly and request that the provider terminate the preventive measures referred to in paragraph 2 of this Article.

SECTION 9

ELECTRONIC ATTESTATION OF ATTRIBUTES

Article 57

Legal effects of electronic attestation of attributes

1. An electronic attestation of attributes shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form or that it does not meet the requirements for qualified electronic attestations of attributes.
2. A qualified electronic attestation of attributes and an attestation of attributes issued by, or on behalf of, a public sector body responsible for an authentic source shall have the same legal effect as attestations issued in paper form.

Article 58

Electronic attestation of attributes in public services

1. For *online* services provided by a public sector body for which electronic identification through a means of electronic identification and authentication is required, the identity data contained in an electronic attestation of attributes shall not replace electronic identification through a means of electronic identification and authentication for electronic identification purposes, unless expressly permitted by applicable law. This provision shall also apply to qualified electronic attestations of attributes.
2. The Authority shall ensure that appropriate measures are taken to enable qualified trust service providers issuing electronic attestations of attributes to verify, by electronic means and upon request of the user, the authenticity of the following attributes against the relevant authentic source at national level or through designated intermediaries at national level, in accordance with national law, where such attributes are supported by public sector authentic sources:
a) address;
b) age;
c) gender;
ç) marital status;
d) family composition as recorded in the family certificate;
dh) nationality or citizenship;
e) educational qualifications, degrees and licences;
ë) professional qualifications, titles and licences;
f) competencies and authorisations to represent natural or legal persons;

g) public permits and licences;
gj) financial and company data relating to legal persons.

Article 59

Requirements for qualified electronic attestation of attributes

1. Qualified electronic attestations of attributes shall meet the requirements laid down in paragraph 2 of this Article.
2. Qualified electronic attestations of attributes shall contain:
a) an indication, in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes;
b) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes, including the State in which that provider is established and:
i. for a legal person: the name and the registration number (NUIS) as stated in the official records;
ii. for a natural person: the person's name;
c) a set of data representing the subject to whom the attested attributes relate, and where a pseudonym is used, it shall be clearly indicated;
ç) the attested attribute or attributes, including, where applicable, the information necessary to identify the purpose of those attributes;
d) the beginning and end date of the period of validity of the attestation;
dh) the identification code of the attestation, which shall be unique for the qualified trust service provider and, where applicable, an indication of the attestation scheme to which the attestation of attributes belongs;
e) the qualified electronic signature or the qualified electronic seal of the qualified trust service provider;
ë) the location of the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (e), made available free of charge;
f) information on, or the location of, services used to determine the validity status of the qualified attestation.
3. The conformity assessment of the requirements laid down in paragraph 2 of this Article shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 6 of this Article.
4. Qualified electronic attestations of attributes shall not be subject to any mandatory requirements other than those laid down in paragraph 2 of this Article.
5. Where a qualified electronic attestation of attributes has been revoked after its initial issuance, it shall cease to be valid from the moment of revocation and its status shall not under any circumstances be reinstated.
6. The reference standards and, where necessary, the specifications and procedures for qualified electronic attestations of attributes shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission.

Article 60

Verification of attributes against authentic sources

1. The Authority shall ensure that, within 24 months from the date of entry into force of the secondary legislation referred to in Article 6(23) and Article 8(6) of this Law, for the attributes referred to in Article 58(2) of this Law, wherever such attributes are supported by authentic sources within the public sector, measures are taken to enable qualified trust service providers issuing electronic

attestations of attributes to verify those attributes by electronic means, upon request of the user, in accordance with the provisions of this Law.
2. The reference standards and, where necessary, the specifications and procedures for the attribute catalogue, as well as the attribute attestation schemes and verification procedures for qualified electronic attestations of attributes, implementing paragraph 1 of this Article, shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission. This secondary legislation shall also be consistent with the Council of Ministers' decision referred to in Article 6(22) of this Law concerning the implementation of the wallet.

Article 61

Requirements for electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source

1. An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall meet the following requirements:
a) the electronic attestation of attributes shall contain:
i. an indication, in a form suitable for automated processing, that the attestation has been issued as an electronic attestation of attributes by or on behalf of a public sector body responsible for an authentic source;
ii. a set of data unambiguously representing the public sector body responsible for issuing the electronic attestation of attributes, including the State in which that public sector body is established, its name and, where applicable, its registration number as recorded in official registers;
iii. a set of data unambiguously representing the subject to whom the attested attributes relate, and where a pseudonym is used, it shall be clearly indicated;
iv. the attested attribute or attributes, including, where applicable, the information necessary to identify the purpose of those attributes;
v. the beginning and end of the period of validity of the attestation;
vi. the identification code of the attestation, which shall be unique for the issuing public sector body and, where applicable, an indication of the attestation scheme to which the attestation belongs;
vii. the qualified electronic signature or qualified electronic seal of the issuing authority;
viii. the location of the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (vii), made available free of charge;
ix. information on, or the location of, services used to determine the validity status of the attestation.
b) the qualified certificate supporting the qualified electronic signature or qualified electronic seal of the public sector body, referred to in Article 3(59) of this Law, identifying the issuer referred to paragraph (1)(a)(ii) of this Article, shall contain a specific set of attributes certified in a form suitable for automated processing:
i. indicating that the issuing body has been established in accordance with the provisions of the legislation in force, as responsible for the authentic source on the basis of which the electronic attestation of attributes has been issued or as the body designated to act on its behalf;
ii . by providing a set of data, which clearly represents the authentic source, referred to in subindent (i)" of this paragraph;
iii . identifying the legislation referred to in subindent (i) of thispoint.
2. Public sector bodies, referred to Article 3 (59) of this Law, which issue electronic attestation of attributes, shall meet a level of security equivalent to qualified trust service providers, in accordance with Article 30 of this Law.
3. The Authority shall publish the list of public sector bodies referred to Article 3(59) of this Law. This list shall include the conformity assessment report issued by a conformity assessment body confirming that the requirements set out in paragraphs 1, 2 and 6 of this Article have been met.

4. Where an electronic attestation of attributes, issued by or on behalf of a public sector body responsible for an authentic resource, has been revoked after its initial issuance, it shall lose its validity from the moment of its revocation and its status shall not be reverted.

5. An electronic attestation of attributes, issued by or on behalf of a public sector body responsible for an authentic resource, shall be deemed to be in compliance with the requirements set out in paragraph 1 of this Article when it complies with the standards, specifications and procedures referred to in paragraph 6 of this Article.

6. The reference standards and, where necessary, the specifications and procedures for the electronic attestation of attributes, issued by or on behalf of a public sector body responsible for an authentic source, shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission. These sublegal acts shall also be in accordance with the implementing acts of the European Commission, referred to Article 6 (23) of this Law, for the implementation of the digital identity wallet.

7. The reference standards and, where necessary, the specifications and procedures, pursuant to paragraph 3 of this Article, shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission. These sublegal acts shall be in accordance with the acts issued by the European Commission, referred to Article 6(23) of this Law, for the implementation of the digital identity wallet.

8. The public sector bodies referred to Article 3(59) of this Law, which issue electronic attestation of attributes, shall provide an interface with the digital identity wallets, which are provided pursuant to Article 6 of this Law.

Article 62

Issuance of electronic attestation of attributes for Digital Identity Wallets

1. Providers of electronic attestations of attributes provide the digital identity wallet users with the possibility to request, obtain, store, and manage electronic attestations of attributes.

2. Providers of qualified electronic attestation of attributes shall provide an interface with digital identity wallets, which are provided pursuant to Article 6 of this Law.

Article 63

Additional rules for the provision of electronic attestation of attributes services

1. Qualified and non-qualified providers of electronic attestation of attributes services shall not combine personal data relating to the provision of these services with personal data from any other service provided by them or by other providers.

2. Personal data related to the provision of electronic attestation of attributes services shall be kept logically separate from other data held by the electronic attestation of attributes provider.

3. Providers of qualified electronic attestation of attribute services shall implement the provision of these qualified trusted services in a manner that is functionally separated from other services provided by them.

SECTION 10

ELECTRONIC ARCHIVING SERVICES

Article 64

Legal effect of electronic archiving services

1. Electronic data and electronic documents preserved using an electronic archiving service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that they are in electronic form or that they are not stored using a qualified electronic archiving service.

2. For electronic data and electronic documents stored using a qualified electronic archiving service, their integrity and origin are presumed for the duration of the preservation period by the qualified trust service provider.

Article 65

Requirements for qualified electronic archiving services

1. Qualified electronic archiving services meet the following requirements:

a) are provided by qualified trust service providers;

b) use appropriate procedures and technologies to guarantee the durability and legibility of electronic data and electronic documents beyond the period of technological validity and at least throughout the legal or contractual retention period, while preserving the integrity and accuracy of their origin;

c) ensure that those electronic data and electronic documents are stored in such a way as to be protected from loss and alteration, except for changes relating to their device (*medium*) or electronic format;

ç) allow authorized relying parties to obtain an automatic report confirming that electronic data and electronic documents retrieved from a qualified electronic archive enjoy the presumption of data integrity from the beginning of the preservation period until the moment of retrieval.

The report referred to in point (ç) of paragraph 1 of this Article must be provided in a reliable and efficient manner and must bear the qualified electronic signature or qualified electronic seal of the qualified electronic archiving service provider.

2. The reference standards and, where necessary, the specifications and procedures for qualified electronic archiving services shall be adopted by decision of the Council of Ministers in accordance with the implementing acts of the European Commission. Compliance with the requirements for qualified electronic archiving services shall be presumed where a qualified electronic archiving service complies with these standards, specifications and procedures.

SECTION 11

ELECTRONIC LEDGERS AND ELECTRONIC DOCUMENTS

Article 66

Legal effects of the electronic ledger

1. An electronic ledger shall not be denied legal effect or admissibility as evidence in legal proceedings solely because it is in electronic form or does not meet the requirements for qualified electronic ledger.

2. Recorded data included in a qualified electronic ledger enjoy the presumption that their sequential chronological ordering and integrity are unique and accurate.

Article 67

Requirements for qualified electronic ledgers

1. Qualified electronic ledgers meet the following requirements:

a) are created and managed by one or more qualified trust service providers;

b) determine the origin of data records in the ledger;

c) ensure the ordering of data records in the ledger in a chronological, unique and sequential manner;

ç) record data in such a way that any subsequent changes to the data are immediately identified, ensuring their integrity over time.

2. Compliance with the requirements set out in paragraph 1 of this Article is presumed when an electronic ledger meets the standards, specifications and procedures referred to in paragraph 3 of this Article.

3. The reference standards and, where necessary, the specifications and procedures for the requirements set out in paragraph 1 of this Article, shall be adopted by decision of the Council of Ministers in accordance with the acts issued by the European Commission.

Article 68

Legal effects of electronic documents

An electronic document shall not be denied the legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

CHAPTER V

Supervision

Article 69

Supervision of the legal framework of the digital identity wallet

1. The Authority is the body responsible for supervising the digital identity wallet in the Republic of Albania, which has the necessary powers and adequate resources to exercise its duties effectively.

2. Upon the accession of the Republic of Albania to the European Union, the Authority shall communicate to the European Commission the name and address of the supervisory body as defined in paragraph 1 of this Article and any subsequent changes thereto.

3. The Authority, pursuant to paragraph 1 of this Article, performs the following duties:

a) to supervise wallet providers and ensure that they meet the requirements set out in this Law;

b) to take action, if necessary, in relation to wallet providers when it is informed that the providers or the wallets they offer are in infringement of the provisions of this Law;

c) to cooperate with other supervisory bodies and provides them with assistance as defined in paragraph 2 of Article 71 and Article 72 of this Law;

ç) to request the necessary information to monitor the fulfillment of legal requirements as defined in this Law;

d) to inform about any significant security breaches or loss of integrity of which the Authority becomes aware in the course of performing its duties and in the case of a significant security breach or loss of integrity, relating to cross-border transactions, inform the single point of contact for electronic identification, trust services and wallet, as well as the single point of contact for cybersecurity of the affected state, for the purpose of informing the public or to request the wallet provider to notify the security breach or loss of integrity, which is in the public interest;

dh) to conduct on-site and remote inspections;

e) to require wallet providers to correct any deficiencies in meeting the requirements set out in this Law;

ë) to suspend or cancels the registration and inclusion of the relying parties in the mechanism referred to Article 7(7) of this Law in the case of illegal use of the wallet;

f) to cooperate with the Commissioner based on the legislation in force for the protection of personal data, in particular, by immediately informing when it is noticed that the personal data protection rules have been infringed and about security breaches that are noticed to constitute a personal data breach.

4. Where the Authority requires a wallet provider to remedy any deficiencies in compliance with the requirements under point (e) of paragraph 3 of this Article, and where the provider fails to act accordingly and where applicable within a time limit set by the Authority, the Authority shall order the provider to suspend or cease the provision of the wallet, taking into account the extent, duration and consequences of those deficiencies,. The Authority shall immediately inform the users of the wallet, the relying parties and, in the case of cross-border transactions, other countries of the decision to require the suspension or cessation of the provision of the wallet.

5. By March 31 of each year, the Authority shall draft a report on the main activities for the previous calendar year and publish it on its official website.

6. The format and manner of maintaining the report, referred to in paragraph 5 of this Article, shall be approved by decision of the Council of Ministers in accordance with the format determined by the European Commission.

Article 70

Supervision of trust services

1. The National Cyber Security Authority is the responsible supervisory authority for trust services.

2. Upon accession of the Republic of Albania to the European Union, the Authority shall communicate to the European Commission its name and address as the authority responsible for the supervision of trust services, as well as any subsequent changes to these data.

3. The competences of the Authority for the supervision of trust services are as follows:

a) to supervise qualified trust service providers established in the territory of the Republic of Albania, and ensures through supervisory activity, before and after obtaining qualified status, that qualified trust service providers and the qualified trust services provided by them meet the requirements set out in this Law;

b) to take action, if necessary, in relation to non-qualified trust service providers located in the territory of the Republic of Albania through supervisory activity when there is information that these non-qualified trust service providers or the trust services provided by them do not meet the requirements set out in this Law;

c) to inform the single points of contact of other states, according to the legislation in force on cybersecurity and the points of contact, according to the definitions in Article 71(2) of this law, in the case of significant security breaches or loss of integrity, and informs the public or requests the trust service provider to do so when it assesses that the security breach or loss of integrity is in the public interest;

ç) to cooperate with the supervisory authorities of trust services of other states within the scope of its responsibility;

d) to analyse the conformity assessment reports referred to Article 26(1) of this Law, and in Article 27(1) of this Law;

dh) upon the accession of the Republic of Albania to the European Union, the Authority shall report to the European Commission on the main activities in accordance with point (5) of this Article;

e) to carry out audits or request a conformity assessment body to conduct a conformity assessment of qualified trust service providers, according to the provisions of Article 26(2) of this Law;

ë) to cooperate with the Commissioner by immediately informing him/her in case of suspected breaches of personal data protection rules and security breaches, which appear to constitute personal data breaches;

f) to grant "qualified" status to trust service providers and the services they provide and withdraws "qualified" status according to the definitions of Articles 26 and 27 of this Law;

g) to publishe the national trusted list, according to the provisions of Article 28(2) of this Law, as well as its decisions on granting or withdrawing qualified status;

gj) to verify the existence and correct implementation of the provisions for the termination plan when the qualified trust service provider ceases its activity, including the manner in which information is kept accessible, in accordance with point (g) of Article 30(5) of this Law;

h) to require trust service providers to correct any failure in meeting the requirements set out in this Law;

i) to examine claims made by web browser providers according to the provisions of Article 56 of this Law, and, if necessary, takes measures.

4. The Authority ensures the establishment, maintenance and updating of a trust infrastructure.

5. By March 31 of each year, the Authority shall draft a report on the main activities of the trust services, which it shall present to the Council of Ministers, and upon accession to the European Union, this report shall also be communicated to the European Commission.

6. The format and manner of maintaining the report, referred to in paragraph 5 of this Article, shall be approved by decision of the Council of Ministers in accordance with the format determined by the European Commission.

Article 71

Single point of contact

1. The Authority is the single point of contact for trust services, wallets and electronic identification schemes.

2. The Authority shall coordinate and cooperate with the competent authorities of other countries for trust service providers, for wallet providers and, where appropriate, with the European Commission and ENISA.

3. The Authority shall immediately publish its name and address, as the single point of contact, designated in accordance with the provisions of paragraph 1 of this Article, as well as any subsequent changes.

Article 72

Mutual Assistance

1. In order to facilitate the supervision and enforcement of the obligations set out in this Law, the Authority shall cooperate with the supervisory authorities of trust services of other countries.

2. The Authority shall cooperate with the supervisory bodies of other countries for mutual assistance at least in relation to:

a) information and consultation on supervisory and enforcement measures;

b) supervisory measures and request to perform inspections regarding conformity assessment reports in accordance with the provisions of Articles 26 and 27 of this Law on the provision of trust services;

c) conducting joint inspections with staff of supervisory bodies of other countries, when appropriate.

3. The Authority signs agreements with supervisory authorities of other countries detailing the procedures, with the aim of achieving mutual assistance, according to the provisions of the legislation in force for international agreements.

4. In cases of submission of a request for assistance, the Authority may reject this request in cases where:

a) the requested assistance is not proportionate to the supervisory powers of the Authority, as defined in Articles 69 and 70 of this Law;

b) is not competent to provide the requested assistance;

c) the provision of the requested assistance is not in accordance with the provisions of this Law.

Article 73

European Digital Identity Cooperation Group

Upon the accession of the Republic of Albania to the European Union, the Authority participates in the activities of the European Commission's European Digital Identity Cooperation Group, composed of representatives of the European Union member states, to:

a) exchange of information and best practices on wallets, electronic identification means and trust services;

b) exchange of information, views and best practices on relevant aspects of cybersecurity in relation to wallets, electronic identification schemes and trust services;

c) exchange of best practices regarding the development and implementation of policies on the notification of security breaches, and common measures;

ç) exchange of relevant information regarding trust services and electronic identification regarding cyber threats, incidents, vulnerabilities, awareness-raising initiatives, training, exercises and skills, capacity building, standards and technical specifications.

Article 74

Reporting requirements

1. The Authority shall ensure the collection of statistics regarding the functioning of wallets and qualified trust services provided in the territory of the Republic of Albania.

2. The statistics collected, in accordance with paragraph 1 of this Article, include the following:

a) the number of natural and legal persons who have a valid wallet;

b) the type and number of services that accept the use of the wallet;

c) the number of user complaints and incidents of consumer protection or personal data processing in relation to the relying parties and the qualified trusted services;

ç) a summary report, which includes data on incidents that impede the use of the wallet;

d) a summary of significant security events, data breaches and affected users of wallets or qualified trusted services.

3. The statistics referred to in paragraph 2 of this Article shall be made available in a readable format to the public.

4. The Authority, upon the accession of the Republic of Albania to the European Union, shall submit to the Commission a report on the statistics collected in accordance with paragraph 2 of this Article.

CHAPTER VI

OBJECTIONS

Article 75

Administrative offenses

For the purposes of this Law, the following violations constitute administrative offenses:

a) when wallet providers do not notify users according to the provisions of Article 6(5) of this Law;

b) when the relying party fails to inform the Authority of any change in the information provided pursuant to the provisions of Article 7(2) of this Law;

c) when qualified service providers do not inform their clients in accordance with the provisions of Article 22(4) of this Law;

ç) when qualified or non-qualified providers of trust services do not notify the Authority according to the provisions of Article 24(2) of this Law;

d) when trust service providers fail to comply with the notification obligation under Article 24(3) of this Law;

dh) when non-qualified trust service providers do not meet the requirements set out in point (a) of Article 25(1) of this Law;

e) when qualified trust service providers do not undergo the audit by a conformity assessment body according to point 1 of Article 26 of this Law;

ë) when qualified trust service providers fail to submit the conformity assessment report according to the provisions of Article 26(1) of this Law;

f) when the qualified trust service provider fails to inform the Authority according to the provisions of Article 26(2) of this Law;

g) when the qualified trust service provider does not fulfill the obligations under points (a), (b), (c), (d), (dh), (e), (f), (g)" and (gj) of Article 30(5) of this Law;

gj) when the qualified trust service provider does not fulfill the obligations under points (ç) and (h) of Article 30(5)(6)(7) of this Law;

h) when qualified trust service providers do not fulfill the obligations set out in Article 54(2) of this Law in the event of data transfer.

Article 76

Administrative sanctions

When the Authority ascertains a violation of the provisions, which constitute an administrative offense under Article 75 of this Law, it imposes a fine as follows:

a) the administrative violation defined in Article 75(b) of this Law is punished with ALL 1,000,000;

b) administrative violations specified in Article 75(c)(ë)(f) of this Law are punished with ALL 10,000,000;

c) administrative violations specified in Article 75(dh)(e)(gj) of this Law are punished with ALL 20,000,000;

ç) administrative violations specified in Article 75(g) of this Law are punished with ALL 30,000,000;

d) administrative violations specified in Article 75(h) of this Law are punished with ALL 50,000,000;

dh) administrative violations specified in Article 75(a)(d) of this Law are punishable by ALL 100,000,000;

e) the administrative violation defined in Article 75(ç) of this Law is punished according to the legislation in force on cybersecurity.

Article 77

Procedure for imposing an administrative penalty "fine"

The procedures for ascertaining, reviewing, appealing and executing administrative offenses are those provided for in the applicable law on administrative offenses.

CHAPTER VII

TRANSITIONAL AND FINAL PROVISIONS

Article 78

Sublegal acts

The Council of Ministers shall be charged with adopting, within 24 months from the entry into force of this Law, the sublegal acts implementing Articles 6, paragraph 4, point (ë), 6, 22, 23 and 24, 7, paragraph 11, 8, paragraphs 6, 8 and 9, 10, paragraph 5, 14, paragraph 3, 16, paragraph 4, 18, paragraph 3, 19, paragraph 5, 24, paragraph 7, 25, paragraph 2, 26 paragraph 9, 27, paragraphs 6 and 7, 28, paragraph 5, 30, paragraphs 4 and 9, 32, paragraph 2, 33, paragraph 4, 34, paragraphs 6 and 7, 35, paragraph 5, 36, paragraph 2, 37 paragraphs 5 and 6, 38, paragraph 3, 39, paragraph 3, 40, paragraph 3, 41, paragraph 2, 42, paragraph 3, 44, paragraph 2, 45, paragraph 4, 46, paragraphs 6 and 7, 52 paragraph 3, 54 paragraphs 4 and 6, 55, paragraph 5, 59, paragraph 6, 60 paragraph 2, 61, paragraphs 6 and 7, 65, paragraph 2, 67, paragraph 3, 69, paragraph 6 and 70, paragraph 6, of this Law.

Article 79

Repeals on the date of accession of the Republic of Albania to the European Union

1. On the date of accession of the Republic of Albania to the European Union, all provisions of this Law shall be repealed with the exception of Articles 4, 6, paragraph 24, 16, paragraphs 4, 27, paragraphs 7, 34, paragraphs 6, and 46, paragraphs 6, of this Law.
2. The Council of Ministers shall be charged with repealing the bylaws implementing this Law, with the exception of the bylaws issued in implementation of the articles specified in paragraph 1 of this Article, upon the accession of the Republic of Albania to the European Union.

Article 80

Repeals

1. Law No. 107/2015 “On electronic identification and trust services”, as amended, and Law No. 9880, dated 25.2.2008, “On electronic signature”, as amended, as well as any other provision that conflicts with this Law, are repealed.
2. The bylaws adopted in implementation of Law No. 107/2015 “On electronic identification and trust services”, as amended, and Law No. 9880, dated 25.2.2008, “On electronic signature”, as amended, shall remain in force even after the entry into force of this law, when they do not conflict with the provisions of this Law, until the adoption of the by-laws in implementation of this Law.

Article 81

Transitional provisions

1. On the day of entry into force of this Law, qualified trust service providers issuing qualified certificates for electronic signatures, registered under Law No. 9880, dated 25.2.2008, “On electronic signature”, as amended, continue to function as qualified trust service providers issuing qualified certificates for electronic signatures.

2. Trust service providers, referred to in paragraph 1 of this Article, are obliged to harmonize their activities with the provisions of this Law within 24 months from the date of entry into force of this Law, and to submit to the Authority a report issued by a conformity assessment body. Until the submission of the assessment report by the conformity assessment body, as well as until the completion of the assessment by the Authority, the trust service provider is considered a qualified trust service provider.

3. If a trust service provider, which issues qualified certificates, does not submit to the Authority the assessment report within the deadline set out in paragraph 2 of this Article, it shall not be considered a qualified trust service provider, according to this Law.

4. Qualified certificates for electronic signature, issued before the entry into force of this Law, will be valid 1 year after the entry into force of this Law.

Article 82

Entry into force

This Law shall enter into force 15 days after its publication in the Official Journal.

SPEAKER OF THE ASSEMBLY

Niko PELESHI

Adopted on 8.5.2026