List of Definitions

Arranged Alphabetically as of the Albanian version

1. “Advanced electronic seal” is an electronic seal that meets the requirements laid down in Article 44 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
2. “Advanced electronic signatures” are electronic signatures that meet the requirements laid down in Article 32 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
3. “Attribute” is a characteristic, quality, right or permission of a natural or legal person or of an object.
4. “Authentic source” is a repository or system held under the responsibility of a public-sector body or private entity, which contains and provides attributes concerning a natural person, a legal person or an object and which is considered to be the primary source of that information or is recognised as authentic in accordance with the applicable legislation in force or European Union law, including administrative practice.
5. “Authentication” is 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.
6. “Authority” is the authority responsible for the regulation and supervision of the field of electronic identification, trust services and the digital identity wallet, established by Law No. 25/2024 “On Cybersecurity”.
7. “Authority responsible for cybersecurity” is the National Cyber Security Authority, the public body responsible for the implementation and supervision of Law No. 25/2024 “On Cybersecurity”, hereinafter referred to as the Authority.
8. “Bodies governed by public law” are bodies that meet the following characteristics: a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; b) they have legal personality; c) they are financed, for the most part, by the State, regional or local authorities, or other bodies governed by public law, or are subject to management supervision by those 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.
9. “Business user” is any natural or legal person acting in a commercial or professional capacity and using core platform services for the purpose of, or in the course of, providing goods or services to end users.
10. “CERT” is the Cybersecurity Emergency Response Team within the Authority.
11. “Certificate for electronic seal” is an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person.
12. “Certificate for electronic signature” is an electronic attestation that links electronic signature validation data to a natural person and confirms at least the name or pseudonym of that person.
13. “Certificate for website authentication” is an electronic attestation that enables the authentication of a website and links the website to the natural or legal person to whom the certificate is issued.
14. “Cloud computing service” is a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where those resources are distributed across several locations.
15. “Conformity assessment bodies” are competent bodies carrying out conformity assessment activities, including calibration, testing, certification and inspection, accredited under the legislation in force on accreditation, which assess the conformity of the activities of a qualified trust service provider or the trust services provided by it, or certify the digital identity wallet or electronic identification means.
16. “Content delivery network” is a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or rapid delivery of digital content and services to internet users on behalf of content and service providers.
17. “Content harmful to children”, under Law No. 25/2024 “On Cybersecurity”, has the same meaning as the definition provided in the legislation in force on the rights and protection of the child.
18. “Cooperation Group” is a body established by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 for the purpose of supporting and facilitating strategic cooperation and the exchange of information among EU Member States.

19. “Core platform services” are the following services: a) online intermediation services; b) online search engines; c) online social networking services; d) video-sharing platform services; e) number-independent interpersonal communications services; f) operating systems; g) web browsers; h) virtual assistants; i) cloud computing services; j) online advertising services, including any advertising networks, advertising exchanges or other advertising intermediation services provided by an undertaking that provides any of the core platform services listed in points (a) to (i) of this definition.
20. “Creator of an electronic seal” is a legal person who creates an electronic seal.
21. “Critical information infrastructure” is the set of network and information systems owned by a public or private authority that provide services whose compromise or destruction would have a serious impact on the health, safety and economic well-being of citizens and on the effective functioning of the economy in the Republic of Albania.
22. “CSIRT at operators” is the cybersecurity incident response team established at operators of critical and important information infrastructures.
23. “CSIRTs network” is the network established by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, composed of the national CSIRTs of the EU Member States, for the purpose of promoting swift and effective operational cooperation among them.
24. “Cyber resilience” is the ability of information systems to protect data from cyberattacks, as well as the ability to resume normal operations within a period that does not affect the activity of the operator of critical or important information infrastructure in the event of a cyberattack.
25. “Cyber threat” is any potential circumstance, event or action that could damage, disrupt or otherwise adversely affect network and information systems, their users and other persons.
26. “Cybersecurity” means the activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats.
27. “Cybersecurity certificate” is a document issued by a cybersecurity conformity assessment body, certifying that an ICT product, service or process has been assessed for compliance with the specific security requirements laid down in the cybersecurity certification scheme.
28. “Cybersecurity certification scheme” is the set of rules, technical requirements, standards and procedures applicable to the certification or conformity assessment of ICT products, services and processes relating to cybersecurity.
29. “Cybersecurity conformity assessment bodies” are national or international legal persons accredited by the institution responsible for accreditation to carry out conformity assessments of ICT products, services and processes relating to cybersecurity, as well as assessments of the cybersecurity measures implemented by critical and important information infrastructures.
30. “Cybersecurity crisis” is a situation in which the security of information in information systems or the security of electronic communications networks is seriously endangered, thereby endangering the public interest of the Republic of Albania.
31. “Cybersecurity emergency” is a situation in which the security of information in information systems or the security of electronic communications networks has been compromised, thereby endangering the public interest of the Republic of Albania.
32. “Cybersecurity incident” is any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data, or of services offered by or accessible through network and information systems.
33. “Cybersecurity incident handling” means all procedures necessary for the prevention, identification, analysis, response to and recovery from a cybersecurity incident.
34. “Cybersecurity measures” are the set of actions aimed at increasing information security in information systems and the availability and reliability of communications network services in cyberspace.
35. “Cybersecurity risk” is an identifiable event with a potential adverse effect on the security of network and information systems.
36. “Cyberspace” is the digital environment capable of creating, processing and exchanging the electronic communication of information generated by networks and information systems, even when they are not connected to the internet.

37. “Data centre service” is a service encompassing structures or groups of structures dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, data processing and transport services, together with all facilities and infrastructures for power distribution and environmental control.
38. “Data record” means electronic data recorded together with the relevant metadata supporting the processing of the data.
39. “Digital identity wallet” (hereinafter referred to as the wallet) is an electronic identification means that allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of digital identity wallets, and to sign by means of qualified electronic signatures or seal by means of qualified electronic seals.
40. “Digital identity wallet trust mark” is a verifiable, simple and recognisable indicator that clearly communicates that the digital identity wallet has been provided in accordance with the provisions of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
41. “Digital service” is any information society service, as defined in the legislation on electronic commerce.
42. “DNS service provider” is an entity that provides: a) publicly available recursive domain name resolution services for internet end users; b) authoritative domain name resolution services for use by third parties, with the exception of root name servers.
43. “Domain name system (DNS)” is a hierarchical distributed naming system that enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources.
44. “Electronic archiving” is a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility, as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period.
45. “Electronic attestation of attributes” means an attestation in electronic form that allows attributes to be authenticated.
46. “Electronic attestation of attributes issued by or on behalf of a public-sector body responsible for an authentic source” is an electronic attestation of attributes issued by a public-sector body responsible for an authentic source, or by a public-sector body designated as such to issue those attestations of attributes on behalf of public-sector bodies responsible for authentic sources, in accordance with Article 60 and point (a) of paragraph 1 of Article 61 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
47. “Electronic communications service” has the same meaning as the definition provided in the legislation in force on electronic communications.
48. “Electronic document” is any content stored in electronic form, in particular in the form of text or sound, or a visual or audiovisual recording.
49. “Electronic identification” is the process of using person identification data in electronic form that uniquely represent a natural or legal person, or a natural person representing another natural person or a legal person.
50. “Electronic identification means” are tangible or intangible units containing person identification data or characteristics which together form identifiers and enable authentication for an online service or, where appropriate, an offline service.
51. “Electronic identification scheme” is a system for electronic identification under which electronic identification means are issued to natural or legal persons, or to natural persons representing other natural or legal persons.
52. “Electronic ledger” is a sequence of electronic data records that ensures the integrity and accuracy of the chronological ordering of those records.
53. “Electronic registered delivery service” is a service that enables data to be transmitted between third parties by electronic means, provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and protects the transmitted data against the risk of loss, theft, damage or any unauthorised alteration.
54. “Electronic seal” means data in electronic form which are attached to or logically associated with other data in electronic form to ensure the origin and integrity of the latter.
55. “Electronic seal creation data” are unique data used by the creator of the electronic seal to create an electronic seal.

56. “Electronic seal creation device” is configured software or hardware used to create an electronic seal.
57. “Electronic signature” means data in electronic form which are attached to or logically associated with other data in electronic form and which are used by the signatory to sign.
58. “Electronic signature creation data” are unique data used by the signatory to create an electronic signature.
59. “Electronic signature creation devices” are configured hardware and software products used to create an electronic signature.
60. “Electronic time stamp” means data in electronic form that bind other data in electronic form to a particular time, establishing evidence that those data existed at that time.
61. “ENISA” is the European Union Agency for Cybersecurity.
62. “European Cyber Crises Liaison Organisation Network (EU-CyCLONe)” is the network established by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 for the purpose of supporting the coordinated management of large-scale cybersecurity incidents and crises at operational level and ensuring the regular exchange of relevant information among EU Member States and Union institutions, bodies, offices and agencies.
63. “European Digital Identity Cooperation Group” is a body established by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 to support and facilitate cooperation and the exchange of information concerning trust services, digital identity wallets and electronic identification schemes among the Member States of the European Union.
64. “Gatekeeper” is an undertaking that provides core platform services and meets the following criteria: a) it has a significant impact on the internal market; b) it provides a core platform service that serves as an important gateway for business users to reach end users; c) it enjoys an entrenched and durable position in its operations, or it is foreseeable that it will enjoy such a position in the near future.
65. “Government CSIRT” is the sectoral CSIRT that manages all critical and important information infrastructures in the government sector.
66. “ICT processes” are a set of activities performed to design, develop, provide or maintain an ICT product or service.
67. “ICT product” is an element or a group of elements of a network or information system.
68. “ICT service” is a service consisting fully or mainly of the transmission, storage, retrieval or processing of information by means of network and information systems.
69. “Identity matching” is a process whereby person identification data or electronic identification means are matched or linked to an existing account belonging to the same person.
70. “Important information infrastructure” is the set of network and information systems owned by a public or private authority that is not part of critical information infrastructure, but whose compromise of information security may jeopardise or restrict the provision of services and business continuity.
71. “Internet exchange point” is a network facility that enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic, provides interconnection only to autonomous systems, and neither requires the internet traffic passing between any two participating autonomous systems to pass through a third autonomous system nor alters or otherwise interferes with such traffic.
72. “Logs” are messages or data concerning events related to cybersecurity.
73. “Managed security service provider” is a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management.
74. “Managed service provider” is an entity that provides services relating to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, through assistance or active administration carried out either on customers’ premises or remotely.
75. “National CSIRT” is the Cybersecurity Incident Response Team within the Authority.
76. “National Cybersecurity Strategy” is a policy document setting out objectives, plans and strategic priorities concerning the security of network and information systems and the creation of secure cyberspaces for society at national level.

77. “Network and information system” means: a) an electronic communications network, as defined in the legislation in force on electronic communications; b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; c) digital data stored, processed, retrieved or transmitted by the elements referred to in points (a) and (b) for the purposes of their operation, use, protection and maintenance.
78. “Offline mode” is an interaction between a user and a third party at a physical location, using proximity-processing technologies, where the digital identity wallet is not required to access remote systems through electronic communications networks for the purpose of the interaction.
79. “Online marketplace” is a service using software, including a website, part of a website or an application, operated by or on behalf of a trader, which allows consumers to conclude distance contracts with traders or other consumers.
80. “Online search engine” is a digital service that allows users to submit queries in order to perform searches of, in principle, all websites or all websites in a particular language on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found.
81. “Operator of critical information infrastructure” is any natural or legal person that manages critical information infrastructure and meets the requirements laid down in Law No. 25/2024 “On Cybersecurity”.
82. “Operator of important information infrastructure” is any natural or legal person that manages important information infrastructure and meets the requirements laid down in Law No. 25/2024 “On Cybersecurity”.
83. “Other entities responsible in the field of cybersecurity” are the superior or regulatory institutions responsible for the fields of activity of the sectors according to which critical and important information infrastructures are categorised.
84. “Person identification data” are a set of data that enable the identification of a natural person or a legal person, or of a natural person representing a legal person.
85. “Personal data” has the same meaning as the definition provided in the legislation in force on the protection of personal data.
86. “Playbooks” are guides setting out a well-defined procedure to be followed for the management of each category of cybersecurity incident.
87. “Proactive scanning” is the performance of one or more advanced preliminary actions that enable the identification, detection and recording of risks with a significant impact before they materialise.
88. “Product” means hardware or software, or the relevant hardware or software components, used for the provision of trust services and electronic identification.
89. “Public electronic communications network” has the same meaning as the definition provided in the legislation in force on electronic communications.
90. “Public-sector body” is a state authority at central, regional or local level, associations formed by one or more such authorities, as well as private entities authorised to provide a public electronic service within the meaning of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
91. “Qualified certificate for electronic seal” is a certificate for an electronic seal issued by a qualified trust service provider and meeting the requirements laid down in point 2 of Article 46 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
92. “Qualified certificate for electronic signature” is a certificate for electronic signature issued by a qualified trust service provider and meeting the conditions laid down in point 2 of Article 34 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
93. “Qualified certificate for website authentication” is a certificate for website authentication issued by a qualified trust service provider and meeting the requirements laid down in point 2 of Article 55 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
94. “Qualified electronic archiving service” means an electronic archiving service provided by a qualified trust service provider and meeting the requirements laid down in Article 65 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
95. “Qualified electronic attestation of attributes” is an electronic attestation of attributes issued by a qualified trust service provider and meeting the requirements laid down in point 2 of Article 59 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.

96. “Qualified electronic ledger” is an electronic ledger provided by a qualified trust service provider that meets the requirements laid down in Article 67 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
97. “Qualified electronic registered delivery service” is an electronic registered delivery service whose provision meets the requirements laid down in Article 54 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
98. “Qualified electronic seal” is an advanced electronic seal created by a qualified electronic seal creation device and based on a qualified certificate for an electronic seal.
99. “Qualified electronic seal creation device” is an electronic seal creation device that meets, to the extent possible, the requirements laid down in points 2 and 3 of Article 35 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
100. “Qualified electronic signature creation device” is an electronic signature creation device that meets the requirements laid down in points 2 and 3 of Article 35 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
101. “Qualified electronic signatures” are advanced electronic signatures created by a qualified electronic signature creation device and based on a qualified certificate for electronic signatures.
102. “Qualified electronic time stamp” is an electronic time stamp that meets the requirements laid down in Article 52 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
103. “Qualified trust service” is a trust service that meets the requirements laid down in Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
104. “Qualified trust service provider” is a trust service provider that provides one or more qualified trust services and has been granted qualified status by the Authority.
105. “Registry of .al top-level domain names” or “TLD.al domain name registry” is the registry of internet domain names registered in the Republic of Albania with the “.al” suffix, administered by the authority responsible for electronic and postal communications, which drafts, approves and applies a specific regulation for this purpose. The registry includes ccTLD.al domain names and subdomains, data concerning their holders, the history of actions involving .al domains and the ccTLD.al technical system, which includes the operation of servers and other necessary equipment, the maintenance of databases and the distribution of TLD zone files to make .al domain names accessible on the internet, as well as other elements included in the aforementioned regulation.
106. “Relying party” is a natural or legal person that relies upon electronic identification, digital identity wallets or other electronic identification means, or upon a trust service.
107. “Remote qualified electronic seal creation device” is an electronic seal creation device managed by a qualified trust service provider, in accordance with Article 48 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”, on behalf of a creator of an electronic seal.
108. “Remote qualified electronic signature creation device” is a qualified electronic signature creation device managed by a qualified trust service provider, in accordance with Article 36 of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”, on behalf of a signatory.
109. “Research organisation” is an entity whose primary objective is to conduct applied or experimental research and development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions.
110. “Sectoral CSIRT” is the person or cybersecurity incident response team for the relevant sector, in accordance with the provisions of the annexes to Law No. 25/2024 “On Cybersecurity”, established at an operator managing critical and important information infrastructures or at the responsible line institution.
111. “Security of network and information systems” is the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data, or of the related services offered by or accessible through those network and information systems.
112. “Signatory” is a natural person who creates an electronic signature.
113. “Social networking services platform” is a platform that enables end users to connect, share, discover and communicate with each other across multiple devices, particularly through chats, posts, videos and recommendations.

114. “Standard”, under Law No. 25/2024 “On Cybersecurity”, has the same meaning as the definition provided in the legislation in force on standardisation.
115. “Strong user authentication” is authentication based on the use of at least two authentication factors from different categories, such as knowledge, something only the user knows; possession, something only the user possesses; or inherence, something the user is, which are independent of one another, so that the breach of one does not compromise the reliability of the others, and which is designed in such a way as to protect the confidentiality of the authentication data.
116. “Technical specification” is a document that sets out the required characteristics of a product, such as levels of quality, performance and safety, including the requirements applicable to the product as regards the name under which the product is sold, terminology, symbols, testing methods, packaging, marking or labelling, and conformity assessment procedures. This term also covers production methods and processes.
117. “Trust service” is an electronic service normally provided for remuneration which consists of: a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services; c) the creation of electronic signatures or electronic seals; d) the validation of electronic signatures or electronic seals; e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals; f) the management of remote electronic signature creation devices or remote electronic seal creation devices; g) the issuance of electronic attestations of attributes; h) the validation of electronic attestations of attributes; i) the creation of electronic time stamps; j) the validation of electronic time stamps; k) the provision of electronic registered delivery services; l) the validation of data transmitted through electronic registered delivery services and the related evidence; m) the electronic archiving of electronic data and electronic documents; n) the recording of electronic data in an electronic ledger.
118. “Trust service provider” is a natural or legal person, whether public or private, who provides one or more trust services either as a qualified trust service provider or as a non-qualified trust service provider.
119. “Trusted infrastructure” is the set of organisational mechanisms that assist in creating, maintaining, supervising and improving the reliability and continuity of trust services, in accordance with the provisions of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
120. “User” is a natural or legal person, or a natural person representing another natural person or a legal person, who uses trust services or electronic identification means provided in accordance with Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
121. “Validation” is the process of verifying and confirming that data in electronic form are valid in accordance with the provisions of Law No. 51/2026 “On Electronic Identification, Trust Services and the Digital Identity Wallet”.
122. “Validation data” are data used to validate an electronic signature or an electronic seal.
123. “Vulnerability” is a weakness, susceptibility or flaw in ICT products or services that can be exploited by a cyber threat.