United Nations A/CN.9/WG.IV/WP.155

General Assembly

Distr.: Limited
13 September 2018

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-seventh session
Vienna, 19–23 November 2018

Draft Instrument on Cross-Border Legal Recognition of Identity Management and Trust Services — Proposal by Germany

Note by the Secretariat

Germany submitted to the Secretariat a paper for consideration at the fifty-seventh session of the Working Group. The paper is reproduced as an annex to this note in the form in which it was received by the Secretariat.

V.18-06084 (E)

Annex

DRAFT INSTRUMENT ON CROSS-BORDER LEGAL RECOGNITION OF IDENTITY MANAGEMENT AND TRUST SERVICES

Reaffirming their conviction that the development of information and communication technologies is a prerequisite to sustainable economic growth and improvement of the quality of life in general;

Noting that electronic communication improves the efficiency of state management and commercial activities, strengthens foreign economic relations, provides access to new opportunities for parties and markets previously remote, and thereby plays a fundamental role in economic development, both nationally and internationally;

Given that the uncertainty about the technological and legal regulation of electronic document flow in the interaction between state and municipal bodies, individuals, and organizations of the States Parties to the [draft instrument][1] constitutes an obstacle to the development of electronic interaction;

Being convinced that the establishment of trust between all participants of electronic interaction is a necessary condition of its development;

Assuming that uniform rules shall be based on respect for the freedom of parties to choose appropriate media, technologies, identification and trust services, taking into account the principles of technological neutrality and functional equivalence, to the extent in which the means selected by the parties are relevant to the purpose of the existing law;

Recognizing the opportunity and feasibility of both centralized and decentralized systems of trust, and their utilization to accelerate progress and digital economy, including the trusted implementation of e-commerce and transport, electronic dispute settlement, creation of e-government and electronic public services, development of online training courses, e-healthcare, various electronic registries, electronic financial services;

Have agreed as follows:

Section I. Scope of application

Article 1. Scope of application

1. This [draft instrument] defines basic characteristics of the transboundary environment of trust, which is a collection of normative, organizational, and technical conditions for establishing trust in cross-border information exchange between public authorities, individuals and corporate bodies in an electronic form.

2. Neither the state affiliation of transboundary electronic interaction participants, nor their civil and legal status, nor the nature of electronic documents and electronic messages that they exchange are taken into account in determining the scope of application of this [draft instrument].

3. The transboundary environment of trust includes the following segments:

(1) Centralized, which encompasses the regulatory, organizational, and technical conditions for establishing trust in the electronic document exchange, which involves setting binding requirements to the Parties' control of the activity of the trust service operators, software and hardware used by those operators in the cross-border

[1] The [draft instrument] is a placeholder for the actual text whose form shall be decided by UNCITRAL.

electronic interaction, trust services, procedures for conformity assessment of the trust service operators, and software and hardware;

(2) Self-regulating, which encompasses the regulatory, organizational, and technical conditions for establishing trust in the electronic message exchange through distributed databases and the creation of data units that suggest the self-regulatory nature of the transboundary electronic interaction.

4. The transboundary environment of trust is used by its participants to ensure the necessary level of trust between the electronic interaction parties. The choice of a particular segment of the transboundary environment of trust, or a combination of its segments, according to article 1, paragraph 3, of this [draft instrument], depends on the nature of specific digital services which require trust to be provided by the transboundary environment of trust.

Section II. General provisions

Article 2. Definitions

1. For the purposes of this [draft instrument]:

(1) “Participants in the transboundary environment of trust” means public authorities, the Coordinating Council, trust service operators, distributed databases operators, and individuals and organizations;

(2) “Electronic message” means any information generated, sent, received, or stored using information and telecommunication networks;

(3) “Electronic document” means an electronic message possessing the necessary and sufficient requisites for the recognition of its legal significance, which veracity and genuineness is confirmed by the trust service operator in accordance with this [draft instrument];

(4) “Transaction records” mean the electronic messages authenticated by distributed database operators and included by these operators in a meaningful (valid) data block;

(5) “Meaningful (valid) data block” means a set of transaction records generated according to the rules established by the distributed database operator; not subject to alteration and addition;

(6) “Trust services” mean services which confirm the veracity and genuineness of electronic documents and/or their details, including but not limited to services related to the creation and use of electronic signatures, electronic seals, electronic timestamps, electronic delivery and authentication of websites;

(7) “Transboundary electronic interaction” means an exchange of electronic messages and/or electronic documents through the information systems between participants of the transboundary environment of trust;

(8) “The Coordinating Council” means the body created in accordance with this [draft instrument] that sets the general requirements, binding for the Members, for the activities of the trust service operators, software and hardware used by the trust service operators to implement the transboundary electronic interaction, and the procedures for conformity assessment of the trust service operators and hardware and software with the requirements; and it performs other functions established by this [draft instrument];

(9) “Location” means a place specified by a transboundary environment of trust party as a place of residence, and in the absence of such — a place of residence of an individual or a place of incorporation of a legal entity;

(10) “Trust service operator” means an individual or a legal entity which complies with the requirements established by the Coordinating Council, holds a confirmation of compliance obtained through a procedure established by the

Coordinating Council, and provides trust services within the centralized segment of the transboundary environment of trust;

(11) “The distributed database operators (the miners)” means individuals or legal entities (including those acting anonymously) which use the necessary software and hardware to participate in the self-regulated segment of the transboundary environment of trust by recording transactions and checking them for genuineness, by forming blocks of data in distributed databases and checking them for completeness;

(12) “User” means a public authority, an individual, or an organization which is a sender or a receiver of electronic messages and/or electronic documents, including those sent through the services provided within the self-regulatory segment of the transboundary environment of trust;

(13) “Information systems” mean the sum of information technologies and equipment designed and used to create, send, receive, store, or otherwise process electronic messages, including electronic documents, in the transboundary electronic interaction;

(14) “Electronic signature/seal” means electronic data, physically attached to or logically associated with other electronic data, which is used by the signatory to sign and which documents a certain relationship between the signatory and this other electronic data in such a way that a third party can verify the existence of this relationship later on;

(15) “Signatory” means an individual (for an electronic signature) or legal entity (for an electronic seal) which signs an electronic document with its electronic signature/seal;

(16) “Qualified certificate of an electronic signature/seal” means an electronic confirmation linking data with a physical person (signature) or legal entity (seal) to verify the electronic signature/seal, and confirming at least its identity; issued by the trust service operator which passed the procedure of conformity pursuant to article 8, paragraph 6 of this [draft instrument], and which meets the requirements established by the Coordinating Council;

(17) “Electronic timestamp” means electronic data that binds other electronic data to a specific time and records the existence of that electronic data at that point of time, allowing participants of the electronic interaction or a third party to ascertain this fact later;

(18) “Electronic registered delivery service” means a service which allows electronic data transfer between third parties and production of proof regarding the processing of transmitted data, including proof of dispatch and receipt of data; and which protects the transmitted data against loss, theft, damage, or unauthorized alteration;

(19) “A qualified website authentication certificate” means an electronic confirmation that allows website authentication linking websites to a physical person or legal entity to which this confirmation was issued by the trust service operator which passed the conformity procedure pursuant to article 8, paragraph 6, of this [draft instrument], and which complies with the requirements of the Coordinating Council;

(20) “Identity” means information about a specific subject (here: User) in the form of one or more attributes that allow the subject to be sufficiently distinguished within a particular context;

(21) “Identification means” means a material and/or immaterial unit containing identity of a specific subject (here: User);

(22) “Identity management” means a set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

(i) assurance of identity information (e.g., identifiers, credentials, attributes); (ii) assurance of the identity of an entity; and (iii) enabling business and security applications;

(23) "Primary (fundamental) identification" means the process of collecting, verifying, and validating sufficient identity attributes about a specific subject (here: User) to define and confirm its identity without any specific context.

Primary identification is usually performed by an authority issuing then the related primary identity certificate (e.g. birth certificate, national identification card, passport, etc.);

(24) "Secondary (transactional) identification" means the process of collecting, verifying, and validating sufficient identity attributes about a specific subject (here: User) to define and confirm its identity within a specific context.

Secondary identification is performed by a trust service operator and can be either (a) applicant's identification at enrolment in order to become user of trust service(s) provided by the trust service operator, or (b) user's identification for using a particular trust service.

(a) For the purpose of the applicant's identification at enrolment, the trust service operator usually uses either a primary identity certificate or an already existing result of other previous applicant's identification. After successful applicant's identification, the trust service operator creates/issues its own secondary user's identity record (secondary identity certificate);

(b) For the purpose of the user's identification for using a particular trust service, the trust service operator requires the user, who already possesses his user's identity according to letter (a) of this definition, to identify himself using his secondary identity certificate (by knowledge, by possession (including biometrical)).

(25) "Identification system" means an (online) environment for identification transactions governed by a set of system rules where a natural or legal person can trust each other because authoritative sources establish and authenticate their identities. An identification system involves (a) a set of rules, methods, procedures and routines, technology, standards, policies, and processes, (b) applicable to a group of participating entities, (c) governing the collection, verification, storage, exchange, authentication, and reliance on identity attribute information about a natural or legal person, (d) for the purpose of facilitating identification transactions;

(26) "Identification transaction" means any transaction involving two or more participants which involves establishing, verifying, issuing, asserting, revoking, communicating, or relying on identity information;

(27) "Identification provider" mean (a) an entity responsible for the identification of natural or legal persons, the issuance of corresponding identification means, and the maintenance and management of such identity information;

(28) "Notified identification system" means an identification system which (a) complies with the requirements of the Coordinating Council, and (b) was notified by the identification provider operating this identification system to the Coordinating Council as laid down in article 5, paragraph 2, of this [draft instrument];

(29) "Level of assurance of a notified identification system" means an attribute (a characteristic) of a notified identification system determined by the identification provider operating this identification system according to the requirements of the Coordinating Council as laid down in article 5, paragraph 2, of this [draft instrument];

(30) "Member" (of Coordinating Council) means a legal entity (i) possessing the legal power and authority in the context of the related national law for executing the legal recognition of identity management and trust services, and (ii) having formally recognized all provisions of this [draft instrument].

Article 3. Interpretation

1. In the interpretation of this [draft instrument], regard is to be given to its international character and to the need to promote uniformity in its application and the observance of good faith in transboundary electronic interaction and other principles set out in article 5 of this [draft instrument].

2. Questions concerning matters governed by this [draft instrument] which are not expressly settled in it are to be settled in conformity with the general principles on which it is based or, in the absence of such principles, in conformity with the law applicable by virtue of the rules of private international law.

Article 4. Principles

Transboundary electronic interaction within the transboundary environment of trust is based on the following principles, which apply to both segments of the transboundary environment of trust:

(1) Technological neutrality;

(2) Functional equivalence with respect to identity management and the trust services provided;

(3) Protection of restricted information, that is, information protected by the international law and national legislation of the States Parties, including commercial secret and personal data, in the transboundary electronic interaction;

(4) The use of any information, documents, and messages, including blocks of data in distributed databases, is solely for purposes not contradictory to the international law and national legislation of the States Parties;

(5) Economic neutrality leading to cost-efficiency and non-distortiveness with respect to identity management and the trust services provided;

(6) Proportionality, id est, the content and form of actions must be in keeping with the aim pursued;

(7) Party autonomy: the freedom of participants to choose media, technologies, identification and trust services appropriate for their concrete business requirements;

(8) Non-discrimination.

Section III. The Coordinating Council

Article 5. Functions of the Coordinating Council

1. The Coordinating Council is the body that performs the functions of a governing body in the centralized segment of the transboundary environment of trust, and of a facilitator in the self-regulating segment of the transboundary environment of trust.

2. Within the centralized segment of the transboundary environment of trust, the Coordinating Council shall approve at least the following set of requirements, procedures, policies and conditions whose evident fulfilment by participants enables the mutual recognition of identification results and identification means as well as of the results of the usage of trust services:

A. Identity management

(1) Requirements for the properties and characteristics of identification systems used for performing primary identification eligible for notification.

These requirements shall pay regard to that identification systems are established and operated in the national context of the States Parties and have to respect the related national legislation, including national provisions for the certification of identification systems.

These requirements shall pay regard to an opportunity to define different levels of assurance of the notified identification systems;

(2) Liability scope of the identification providers of the notified identification systems for any losses;

(3) Procedures for the mutual recognition of identification results gained and identification means issued by identification providers of the notified identification systems;

(4) Determination of legal effects — for the purpose of this [draft instrument] — substantiated in the usage of notified identification systems, including the mutual recognition of identification results gained and identification means issued by identification providers of the notified identification systems; this shall pay regard to the different levels of assurance of the notified identification systems;

(5) Basic conditions of the use of the notified identification systems;

(6) Requirements for the properties and characteristics of identification systems used for performing secondary identification of users by trust service operators;

(7) Rules of dispute settlement.

B. Trust services

(1) Requirements for the operating procedures of the trust service operators, including civil liability insurance and the trust service operators audit;

(2) Requirements for software and hardware used in the transboundary electronic interaction;

(3) Procedures for conformity assessment for the trust service operators, including the conformity assessment of identification systems used for performing secondary identification of users, and hardware and software (audit);

(4) Liability scope of the trust service operators for any losses;

(5) Rules of dispute settlement;

(6) Requirements for the bodies and (or) individuals engaged in the compliance confirmation of the trust service operators, including the conformity assessment of identification systems used for performing secondary identification of users, and hardware and software (audit);

(7) Basic conditions of the use of the trust services defined in articles 15, 16, 17, 18, 19 and 20 of this [draft instrument].

C. Other documents provided for in this [draft instrument]

3. The Members agree under this [draft instrument] to execute or to enforce the acts of the Coordinating Council made in accordance with paragraph 2 of this article by public entities and local self-governments, users, operators, and trust services under their jurisdiction.

4. In the self-regulating segment of the transboundary environment of trust, the Coordinating Council:

(1) Approves a recommended procedure of confirming the joining of the distributed databases operators to the corresponding databases;

(2) Approves the procedure of notification to the Coordinating Council concerning distributed database information incidents, i.e. the use of electronic messages, transaction records, blocks of data in distributed databases in a manner contrary to the international law and national legislations of the Members;

(3) Organizes the procedure of notification from the distributed databases operators to the Coordinating Council of the voluntary assumption of the

commitments of the latter to implement the requirements of this [draft instrument] in ensuring the use of any information, documents, and messages, including blocks of data in distributed databases, only for the purposes not contradictory to international law and national legislations of the Members; and to inform the Coordinating Council about distributed database information incidents.

5. Decisions and documents adopted by the Coordinating Council concerning the self-regulated segment of the transboundary environment of trust are advisory in nature.

Article 6. The establishment and procedure of the Coordinating Council

1. The Coordinating Council is comprised of its Members for a term of four years. Each Member may nominate one authorized representative.

2. The Coordinating Council may establish subsidiary bodies as it deems necessary for the performance of its functions.

3. Each member of the Coordinating Council shall have one vote.

4. The decisions of the Coordinating Council on the regulation of its work shall be made by an affirmative vote of not less than two thirds of its members.

5. The decisions of the Coordinating Council on the adoption of the acts referred to in article 5, paragraph 2, shall require a unanimous vote.

6. The Coordinating Council shall establish its rules of procedure, including the election procedure for its chairperson, the procedure for maintaining of mutual trust between the responsible representatives of the Members to the transboundary environment of trust, and the decision-making procedure relating to the approval of the documents specified in article 5 of this [draft instrument].

Section IV. Participants of the transboundary environment of trust

Article 7. Public authorities and local self-governments of the States Parties

1. Public authorities are involved in a transboundary electronic interaction for the performance of public functions imposed on them by the national law of the States Parties in accordance with the rules established by this [draft instrument] and acts of the Coordinating Council adopted in accordance with it.

2. Public authorities are entitled to make their own decision on their participation in the self-regulatory segment of the transboundary environment of trust.

3. Public authorities are entitled to set additional requirements compared to the requirements established by this [draft instrument] and acts of the Coordinating Council adopted in accordance with it but not contradictory to them, to have an electronic interaction, in the cases established by the Coordinating Council.

Article 8. The trust service operators

1. The trust service operators are participants of the centralized segment of the transboundary environment of trust.

2. The trust service operators can provide trust services within the boundaries of a certain Member and/or throughout the territory of all the States Parties.

3. The trust service operators are obligated to comply with the requirements established by the Coordinating Council, depending on the area (the whole territory of the States Parties or part of it), where the trust service operators provide services, and shall confirm their compliance with the requirements in the manner established by the Coordinating Council.

4. The trust service operators are required to publish on the Internet any information about their acquisition or alteration of the trust service operator status. The trust service operators are obliged to notify the competent authorities of the responsible Member of any alteration in trust service provision and of the trust service operator status. The trust service operators are obligated to provide any information related to transboundary electronic interaction incidents to the competent authorities of the Members and the Coordinating Council. The Coordinating Council establishes the procedure and terms of providing information related to the transboundary electronic interaction incidents.

5. The trust service operators are obligated to provide civil liability insurance or own sufficient financial cover according to the requirements established by the Coordinating Council.

6. The trust service operators are required to undergo an assessment procedure (independent audit) of conformity of the trust service operators, the trust services they provide, including the assessment of identification systems used for performing secondary identification of users, and hardware and software to the requirements of the Coordinating Council and in the manner prescribed by it.

Article 9. Independent compliance audit. Insurance

1. Only the trust service operators that have passed an independent audit of compliance shall have the right to provide trust services.

2. The bodies or institutions authorized in accordance with the procedure established by the Coordinating Council may carry out the compliance auditing.

3. The trust service operators provide civil liability insurance in accordance with the requirements established by the Coordinating Council.

Article 10. Distributed database operators

1. The distributed database operators are participants of the self-regulating segment of the transboundary environment of trust.

2. The distributed database operators organize transboundary electronic interaction with each other and with users based on the principles of self-regulation, and ensure compliance with this [draft instrument] concerning the use of any information, documents, and messages, including blocks of data in distributed databases, only for the purposes not contradictory to the international law and the national legislation of the States Parties, and concerning reporting the information incidents within distributed databases to the Coordinating Council.

3. The voluntary filing of the notification to the Coordinating Council for voluntary compliance with these requirements by the distributed database operator makes such an operator acknowledged as the one meeting the requirements of this [draft instrument] concerning the use of any information, documents, and messages, including blocks of data in distributed databases, only for the purposes not contradictory to international law and national legislation of the Members, and concerning reporting the information incidents within the distributed databases to the Coordinating Council. The procedure for filing such notifications and the procedure for maintaining a list of the distributed database operators of the Members to the transboundary environment of trust are established by the Coordinating Council.

The Coordinating Council has the right to refuse the notification of the distributed database operator on the list if it has information on the violation of international law and the national legislation of the States Parties made by the operator.

4. Interaction of the distributed database operators and the Coordinating Council, as well as the distributed database operators and users, can be carried out without the identification of legal entities and individuals who operate distributed databases and use them.

5. When the Coordinating Council receives the information about a distributed database operator violating the requirements of this [draft instrument] specified in paragraph 2 of this article, that distributed database operator may be excluded from the publicly available list of providers of distributed databases who are parties to the transboundary environment of trust.

Article 11. Users

1. Users are participants of both segments of the transboundary environment of trust.

2. Depending on the segment of the transboundary environment of trust, users exchange electronic messages and electronic documents in accordance with the rules established by the Coordinating Council and the trust service operators, or with the rules established by the distributed database operators, respectively.

Section V. The transboundary environment of trust infrastructure

Article 12. Hardware and software of the trust service operators

1. The trust service operators use only software and hardware that successfully passed the procedures for conformity assessment in accordance with article 8, paragraph 6, and article 9, paragraph 1, for rendering their services.

2. Functional requirements for the software and hardware of the trust service operators, and requirements for the software and hardware procedure for confirmation of conformity to the established functional requirements consistent with the principle of technological neutrality, are established by the Coordinating Council in accordance with article 8, paragraph 6, and article 9, paragraphs 1 and 2.

Article 13. Hardware and software of the distributed database operators

Distributed database operators independently determine software and hardware requirements needed for the verification of genuineness and completeness of the records of transaction, creation, storage, and verification of the completeness of data blocks.

Article 14. Software and hardware of the users

Users are required to make their own provisions for compliance of the software and hardware used in the transboundary electronic interaction with the requirements of the trust service operators.

Section VI. Trust services within the centralized segment of the transboundary environment of trust

Article 15. Electronic signature

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

2. An advanced electronic signature shall meet the following requirements:

(a) Shall be uniquely linked to the signatory;

(b) Shall be capable of identifying the signatory;

(c) Shall be created using electronic signature creation data, which the signer uses under his sole control;

(d) Shall be linked to data signed therewith in such a way that any subsequent change in the data is detectable.

3. A qualified electronic signature is an advanced electronic signature based on a qualified certificate of the electronic signature and created with software and hardware which are certified in accordance with article 8, paragraph 6. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

An advanced electronic signature which is not a qualified electronic signature shall have the equivalent legal effect of a handwritten signature in the cases determined by agreement of the parties on the use of such signature or the regulatory legal act of the States Parties.

4. A qualified electronic signature based on a qualified certificate issued under the jurisdiction of one Member shall be recognized as a qualified electronic signature by all other Members.

Article 16. 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 has an electronic form or does not meet the requirements of the qualified electronic seal.

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

(a) Shall be uniquely linked to the creator of the seal;

(b) Shall be capable of identifying the creator of the seal;

(c) Shall be created using electronic seal creation data, which the creator of the seal uses under his sole control;

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

3. A qualified electronic seal is an advanced electronic seal based on a qualified certificate of the electronic seal and created using software and hardware, which are certified in accordance with article 8, paragraph 6. 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.

An advanced electronic seal which is not 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 in the cases determined by agreement of the parties on the use of such seal or the regulatory legal act of the States Parties.

4. A qualified electronic seal based on a qualified certificate issued under the jurisdiction of one Member shall be recognized as a qualified electronic seal by all other Members.

Article 17. Electronic timestamp

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

2. The qualified electronic timestamp creates a presumption of accuracy of the specified date and time, and of the data integrity, which such qualified electronic timestamp certifies.

3. The qualified electronic timestamp shall meet the following requirements:

(a) It shall bind the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

(b) It shall be based on an accurate time source linked to the Coordinated Universal Time;

(c) It shall be signed using an advanced electronic signature or sealed with an advanced electronic seal of a trust service operator which passed the procedure for conformity pursuant to article 8, paragraph 6.

4. A qualified electronic timestamp issued under the jurisdiction of one Member shall be recognized as a qualified electronic timestamp by all other Members.

Article 18. Electronic registered delivery service

1. The 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 has an electronic form or does not meet the requirements of a qualified electronic registered delivery service.

2. The data sent and received using a qualified electronic registered delivery create a presumption of data integrity, of sending such data by an identified sender, of receipt of such data by an identified recipient, of the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

3. The qualified electronic registered delivery service shall meet the following requirements:

(a) It is provided by one or more trust service operators that have passed the procedure for conformity pursuant to article 8, paragraph 6, of this [draft instrument];

(b) They ensure with a high level of confidence the identification of the sender;

(c) They ensure the identification of the addressee before the delivery of the data;

(d) The sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service operator in such a manner as to preclude the possibility of the data being changed undetectably;

(e) Any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;

(f) The date and time of sending, receiving and any change of data are indicated by a qualified electronic timestamp.

4. The results of the use of qualified electronic registered delivery service gained under the jurisdiction of one Member shall be recognized as the results of the use of qualified electronic registered delivery service by all other Members.

Article 19. Website authentication

1. A qualified website authentication certificate 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 website authentication;

(b) A set of data unambiguously representing the trust service operator which issued the qualified certificate;

(c) For natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym; for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, the registration number as stated in the official register;

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

(e) The domain name(s) operated by the natural or legal person to whom the certificate is issued;

(f) Details of the beginning and end of the certificate’s period of validity;

(g) The certificate identity code, which must be unique for the trust service operator;

(h) The advanced electronic signature or advanced electronic seal of the issuing trust service operator which passed the conformity procedure pursuant to article 8, paragraph 6, of this [draft instrument];

(i) The location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.

2. The results of the use of website authentication trust service based on a qualified website authentication certificate issued under the jurisdiction of one Member shall be recognized as the results of the use of website authentication trust service based on a qualified website authentication certificate by all other Members.

Article 20. Other trust services

1. The Coordinating Council may additionally include in its scope of regulation other trust services not specified in articles 15–19 of the [draft instrument].

2. Regulation of other trust services should be similar to the regulation of the trust services referred to in articles 15–19 of the [draft instrument].

3. In order to contribute to their general cross-border use, it should be possible to use trust services as evidence in legal proceedings in all States Parties. It is for the national law to define the legal effect of trust services, except if otherwise provided in this [draft instrument].

Article 21. Recognition of trust services of third countries and international organizations

1. The trust services offered by operators authorized in accordance with the legislation of third countries or international organizations can be recognized as legally equivalent to the trust services offered by operators that have passed the conformity procedure pursuant to article 8, paragraph 6, of this [draft instrument] if so agreed between the Coordinating Council and an authorized body of a third country or an international organization in accordance with paragraph 2 of this article.

2. Agreements referred to in paragraph 1 of this article shall provide, among other things, that:

(1) The requirements for the trust service operators of a third country or an international organization are not set lower than the requirements of the trust service operators providing trust services in accordance with this [draft instrument];

(2) A third country or an international organization, which is a party to the agreement, recognizes in its territory (under its jurisdiction) a legal equivalence of the services provided by the trust service operators that have passed the conformity procedure pursuant to article 8, paragraph 6, of this [draft instrument], and of the services provided by the trust service operators authorized in accordance with the legislation of the third country or the international organization which signed the agreement.

Section VII. Protection of rights and interests of participants of transboundary electronic interaction

Article 22. Judicial protection

1. Electronic documents and electronic messages, including the results of the use of trust services described in articles 15–20 of the [draft instrument], are accepted as evidence in all courts and arbitration courts of the Members.

2. The legal right certified by an electronic document possesses the same enforceability as a right certified by a paper document.

Article 23. Dispute settlement

1. The Coordinating Council adopts rules for the administrative settling of disputes arising from the transboundary electronic interaction within the centralized segment of the transboundary environment of trust.

2. Participants in the transboundary electronic interaction have the right to make bilateral and multilateral agreements on the procedure for settlement of transboundary electronic interaction disputes.