United Nations A/CN.9/WG.IV/WP.155/Add.1

General Assembly

Distr.: Limited
19 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.18-06090 (E)

Annex

Coverage of the **'Roadmap for discussion of legal aspects of IdM and trust services' (see A/CN.9/936, para. 58)** by the **Draft Instrument on Cross-Border Legal Recognition of Identity Management and Trust Services (see A/CN.9/WG.IV/WP.155)** and by the **Regulation (EU) No 910/2014 (eIDAS).**

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
1. Scope: cross-border trade	MLEC and MLES scope is not limited to commercial exchanges	Art. 1 and 2		Art. 1 Art. 1.3 additionally refers to (i) centralized and (ii) self-regulating (e.g. based on the block-chain technology) segments
a. Participating entities: persons and objects? – Decision by WG IV: first, natural and legal persons only	-	Art. 3-(3)		Art. 1.4 (ref. to 'participants', defined by Art. 2.1-1) Art. 7 to 11
b. transactions (G2G excluded?) – Decision by WG IV: B2B, B2C, B2G in focus, but G2G not explicitly to exclude, if not necessary	See above.	Art. 2 applicable only for: - Id-schemes notified by Member States; - publicly available trust services		Art. 1.2
2. general principles	-	no dedicated article		Art. 4 Additional principles: - Protection of restricted information

[1] ECC = United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005); MLETR = UNCITRAL Model Law on Electronic Transferable Records (2017); MLES = UNCITRAL Model Law on Electronic Signatures (2001); MLEC = UNCITRAL Model Law on Electronic Commerce (1996).

[2] A provision source shall be clearly identifiable, e.g. by a prefix.

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
				- non-contradiction to the international law and national legislation of the State Parties
a. technological and economic neutrality	Technology neutrality achieved through definitions based on the notion of "data message"—see, e.g., art. 4(c) ECC: "Data message means information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy".	Art. 12.3-(a): technological neutrality Preamble-(16) economic neutrality is not addressed		Art. 4: technological and economic neutrality Art. 12: technological neutrality
b. party autonomy and proportionality	Party autonomy is generally recognised (see art. 4 MLEC: "(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement. (2) Paragraph (1) does not affect any right that	neither autonomy nor proportionality are addressed		party autonomy: Art. 4, Preamble: 'the freedom of parties to choose appropriate media, technologies, identification and trust services' proportionality: Art. 4, Preamble ('to the extent in which the means

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	may exist to modify by agreement any rule of law referred to in chapter II.") within limits of mandatory law (see paras. 46-52 Explanatory Note to MLETR).			selected by the parties are relevant to the purpose of the existing law')
c. functional equivalence rule for identification duties? and trust services	The most recent version of the functional equivalence provision for e-signatures is contained in art. 9 MLETR: "Where the law requires or permits a signature of a person, that requirement is met by an electronic transferable record if a reliable method is used to identify that person and to indicate that person's intention in respect of the information contained in the electronic transferable record.". Art. 10 MLEC provide a functional equivalence rule on retention of data messages: "(1) Where the law requires that certain documents, records or information be retained, that requirement is met by	For IdM: Art. 6 For TS: Art. 25.2 (eSign) Art. 35.2 (eSeal) Art. 41.2 (eTSS) Art. 43.2 (eRDS)		For IdM: Art. 4 (as general principle) For TS: Art. 4 (as general principle), Art. 15.3 (eSign), Art. 16.3 (eSeal), Art. 17.2 (eTSS[3]), Art. 18.2 (eRDS[4])

[3] el. time stamping service.
[4] el. registered delivery service.

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	retaining data messages, provided that the following conditions are satisfied: (a) the information contained therein is accessible so as to be usable for subsequent reference; and (b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and (c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received. (2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.			

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.”			
(d.) non-discrimination	Generally recognised. Latest formulation may be found in art. 7 (1) MLETR: “An electronic transferable record shall not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form.”.	Art. 12.3-(a)		Art. 4
3. definitions (WP.150)	Art. 2(a) MLES: “Electronic signature” means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message”.	Art. 3		Art. 2 The current set of definitions seems to be self-contained. It can be supplemented / modified with respect to WP.150, if necessary.
a. primary / secondary determination of identity	-	No explicit distinction, no explicit definitions		Art. 2-22), 2-23)

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
		for implicit distinction see item #4-a below		
b. open-ended definition of trust services	-	Art. 3 (16) No open-ended definition of trust services: the set of TS covered is confined.		Art. 2-6) see also Art. 20
4. mutual legal recognition requirements and mechanisms: - decentralized[5], - respect for national law, - basic conditions (e.g. LoA requirement, participation in recognition mechanism, e.g. notification), - legal effects	See below for e-signatures	see below		see below
a. IdM i. mapping against generic LoAs: specifications and procedures, relevant elements (enrolment, e-id mean management, authentication, management and organization)	-	primary determination of identity eligible for notification and, hence, for mutual recognition: Art. 7 - decentralized implementation of IdM schemes (each MS[6] is responsible for its IdM-scheme): Art. 7		primary determination of identity: Art. 5.2-A; - decentralized implementation of IdM schemes: Art. 5.2-A-1)

[5] *not in the sense 'bilateral or multilateral'.*

[6] Member State.

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
ii. levels of assurance of identity management schemes (s. item #6)		- respect for national law: Art. 7, Art. 9 (notification of IdM-schemes) - basic conditions for IdM: Art. 7 - mutual recognition of Id-results (or means): Art. 6 - legal effects (also valid for item #6.b below): Art. 6 assurance levels for IdM schemes (item #4-a-ii, also valid for item #6 below; primary determination of identity): Art. 8 ------- secondary determination of identity: - for subscriber's enrolment: Art. 24.1 - for transactions: - eSign: Art. 26 (c) - eSeal: Art. 36 (c)		- respect for national law: as a general principle in Art. 4-4); Art. 5.2-A-1) - basic conditions for IdM: Art. 5.2-A-5) - mutual recognition of Id-results (or means): Art. 5.2, Art. 5.2-A-4) - legal effects (also valid for item #6.b below): Art. 5.2-A-4) assurance levels for IdM schemes (item #4-a-ii, also valid for item #6 below; primary determination of identity): Art. 5.2-A-4) ------- secondary determination of identity: - for subscriber's enrolment: Art. 5.2-A-6)

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
		- eRDS: Art. 44.1 (b), (c)		- for transactions: - eSign: Art. 15.2 c) - eSeal: Art. 16.2 c) - eRDS: Art. 18.3 b), c)
b. trust services i. qualified / not qualified? ii. existing UNCITRAL provisions iii. levels of qualification of trust services (s. item #6)	Art. 9(3) ECC contains a functional equivalence rule that operates across borders: "Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if: (a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and (b) The method used is either:	- decentralized implementation of TS (each TSP[7] is responsible for TS provision): Art. 19 (for all TSPs), Art. 24 (for qualified TSPs) - respect for national law: Preamble (22), Art. 17, Art. 20 (by supervision activities by national SBs[8], Art. 17.1) - basic conditions for TS: Art. 19 (for all TSPs), Art.		- decentralized implementation of TS (each TSO[11] is responsible for TS provision): Art. 8, Art. 5.2-B-1) (Coordinating Council sets merely requirements on TSPs) - respect for national law: Art. 4-3), -4); supervision provisions are not explicitly stated, but might be delegated to the Coordinating Council in the context of Art. 5.2-B-1), 5.2-B-2), 5.2-B-3); Art. 8.3, Art. 8.6 - basic conditions for TS: Art. 8, Art. 12; the

[7] Trust service provider (synonym of trust service operator in 'Possible Draft Provisions').
[8] Supervisory Body.
[11] Trust service operator (synonym of trust service provider in eIDAS).

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	(i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or (ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.". Art. 12 MLES contains a rule on geographic non-discrimination of simple and qualified e-signatures: "1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had: (a) To the geographic location where the certificate is issued or the electronic signature created or used; or	20, 21, 24 (for qualified TSPs) - mutual recognition of TS-results: - eSign: in Art. 25.3, 27.1, 27.2 - eSeal: in Art. 35.3, 37.1, 37.2 - eTSS: in Art. 41.3 - mutual recognition of the results of application other TS is not explicitly regulated, see Preamble (22) - legal effects (also valid for item #6.b below): - Preamble (22)[9]: general statement - Art. 25 (eSign) - Art. 35 (eSeal) - Art. 41 (eTSS)		definition of further basic conditions is delegated to the Coordinating Council, see Art. 5.2-B-1), 5.2-B-2), 5.2-B-3) - mutual recognition of TS-results: - Art. 5.2 (general provision) - eSign: in Art. 15.4 - eSeal: in Art. 16.4 - eTSS: in Art. 17.4 - eRDS: in Art. 18.4 - Website auth.: in Art. 19.2 - all other TS: a general provision in Art. 20.3 - legal effects (also valid for item #6.b below): - Art. 15.1, 15.3 (eSign) - Art. 16.1, 16.3 (eSeal)

[9] 'It is for the national law to define the legal effect of trust services, except if otherwise provided in this Regulation'.

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	(b) To the geographic location of the place of business of the issuer or signatory. 2. A certificate issued outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate issued in [the enacting State] if it offers a substantially equivalent level of reliability. 3. An electronic signature created or used outside [the enacting State] shall have the same legal effect in [the enacting State] as an electronic signature created or used in [the enacting State] if it offers a substantially equivalent level of reliability. 4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards	- Art. 43 (eRDS) - Art. 46 (eDoc[10]) levels of qualification of TS (item #4-b-iii, also valid for item #6 below): - Art. 3 (16), (17); (19), (20): for TS and TSPs generally (non-qualified vs. qualified TS) - for eSign: Art. 3 (10), (11), (12): simple vs. advanced vs. qualified - for eSeal: Art. 3 (25), (26), (27): simple vs. advanced vs. qualified - for eTSS: Art. 3 (33), (34): simple vs. qualified - for eRDS: Art. 3 (36), (37): simple vs. qualified - for certificate for website authentication:		- Art. 17.1, 17.2 (eTSS) - Art. 18.1, 18.2 (eRDS) levels of qualification of TS (item #4-b-iii, also valid for item #6 below): - no explicit statement for TSPs: all TSPs in the centralized segment have to undergo a compliance assessment, see Art. 8.6; the compliance criteria (to be issued by the Coordinating Council, Art. 5.2-B-1)) <u>may foresee different qualification levels for TSPs</u> - for eSign: Art. 2-14), Art. 15.2, 15.3: simple vs. advanced vs. qualified

[10] Electronic documents.

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	and to any other relevant factors. 5. Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.”.	Art. 3 (38), (39): simple vs. qualified		- for eSeal: Art. 2-14), Art. 16.2, 16.3: simple vs. advanced vs. qualified - for eTSS: Art. 2-17), Art. 17.3: simple vs. qualified - for eRDS: Art. 2-18), Art. 18.3: simple vs. qualified - for certificate for website authentication: Art. 2-19): simple vs. qualified
5. certification of identity management schemes and trust services: effects, mandatory / optional for qualification (items #5, #7 and #12 belong together)	Optional. For e-sign: may be taken into consideration in assessing trustworthiness of the CSP: art. 10(f) MLES: “For the purposes of article 9, paragraph 1 (f), of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors: […]	For IdM: primary determination of identity (delegated to MS): Art. 7 (eligibility for notification) and Art. 9 (notification) implicitly delegate a certification of IdM schemes to be notified to MS. Art. 6: provisions for mutual recognition of IdM-schemes --- secondary determination of identity (certification is		For IdM: primary determination of identity: see item #4a above; - certification of national IdM-schemes: Art. 5.2-A-1; - mutual recognition of IdM-schemes: Art. 5.2, Art. 5.2-A-4)

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	(e) Regularity and extent of audit by an independent body; (f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; […]".	obligatory only for qTSP[12]): - for subscriber's enrolment: shall be certified by CAB[13] acc. to Art. 20.1 - for transactions: - eSign: Art. 26 (c) - eSeal: Art. 36 (c) - eRDS: Art. 44.1 (b), (c) shall be certified by CAB acc. to Art. 20.1 For TS (certification is obligatory only for qTS[14]):		------- secondary determination of identity: - for subscriber's enrolment: see item #4a above; shall be certified by CCB[15]: Art. 8.6; Art. 5.2-A-6), 5.2-B-3) require the Coordinating Council to set related requirements and procedures - for transactions: - eSign: Art. 15.2 c) - eSeal: Art. 16.2 c) - eRDS: Art. 18.3 b), c) shall be certified by CCB: Art. 8.6; Art. 5.2-B-1), 5.2-B-3)

[12] qualified TSP (trust service providers).
[13] (accredited) Conformity Assessment Body acc. Art. 3 (18) of eIDAS.
[14] qualified TS (trust services).
[15] Compliance Confirmation Body acc. to Art. 5.2-B-6) of Convention.

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
		each qTS provided by qTSP shall be certified by CAB acc. to Art. 20.1		require the Coordinating Council to set related requirements and procedures For TS: each qTS provided by TSP shall be certified by CCB acc. to Art. 8.6.
6. levels of assurance of identity management schemes and trust services (s. items #4-a-ii and #4-b-iii)	see below	see below		see below
a. generic description / outcome-based	UNCITRAL provisions dealing with e-signatures are based on the functional equivalence principle. Art. 6 MLES adopts a “two-tier” approach: general / advanced (possibly similar to art. 25 eIDAS): “1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the	For IdM (assurance levels for primary determination of identity): s. item #4-a-ii above For TS (qualification levels): s. item #4-b-iii above		For IdM (assurance levels for primary determination of identity): s. item #4-a-ii above For TS (qualification levels): s. item #4-b-iii above

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	light of all the circumstances, including any relevant agreement. […] 3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if: (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person; (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person; (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information			

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	after the time of signing is detectable. 4. Paragraph 3 does not limit the ability of any person: (a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or (b) To adduce evidence of the non-reliability of an electronic signature [...]".			
b. associated legal effects	Art. 6 MLES associates a presumption with advanced e-sign (see above).	For IdM (assurance levels for primary determination of identity – legal effects): s. item #4-a above For TS (qualification levels – legal effects): s. item #4-b above		For IdM (assurance levels for primary determination of identity – legal effects): s. item #4-a above For TS (qualification levels – legal effects): s. item #4-b above
7. liability (items #5, #7 and #12 belong together)	see below	see below		see below

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
a. left to national law i. identification of applicable law in cross-border transactions	-	IdM providers - primary determination of identity: Art. 11.4 TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: Art. 13.3 indemnity insurance for qualified TSPs: Art. 24.2 (c); a minimum insurance coverage may be regulated by national law		IdM providers - primary determination of identity: delegated to the Coordinating Council, see item #4.a above; Art. 5.2-A-2); the Coordinating Council may decide to refer to national laws. TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: delegated to the Coordinating Council, see Art. 5.2-B-4); the Coordinating Council may decide to refer to national laws. indemnity insurance for TSPs: delegated to the Coordinating Council, see Art. 5.2-B-1) Art. 8.5, Art. 9.3 a minimum insurance coverage may be directly agreed by the Coordinating Council or

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
				regulated by reference national laws
b. uniform law	-	IdM providers - primary determination of identity: Art. 11.1, 11.2, 11.3, 11.5 TSPs as (i) IdM providers for secondary determination of identity and as (ii) TS providers: Art. 13.1 and 13.2 indemnity insurance for qualified TSP: see item #7.a above		IdM providers - primary determination of identity: see item #7.a above TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: see item #7.a above indemnity insurance for qualified TSP: see item #7.a above
c. liable entity: issuer, operator, other party	MLES spells out obligations and associated liability of signatory (art. 8), certification service provider (arts. 9 and 10) and relying party (art. 11): Article 8. Conduct of the signatory 1. Where signature creation data can be used to create a signature that	IdM providers - primary determination of identity: Art. 11.1 (notifying Member States) Art. 11.2 (issuers of the el. identification means) Art. 11.3 (operators of identification procedures)		IdM providers - primary determination of identity: see item #7.a above

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	has legal effect, each signatory shall: (a) Exercise reasonable care to avoid unauthorized use of its signature creation data; (b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if: (i) The signatory knows that the signature creation data have been compromised; or (ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised; (c) Where a certificate is used to support the electronic signature, exercise reasonable care	TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: TSPs, see Art. 13.1		TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: delegated to the Coordinating Council, see Art. 5.2-B-4); the Coordinating Council may decide to refer to national laws.

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate. 2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1. Article 9. Conduct of the certification service provider 1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall: (a) Act in accordance with representations made by it with respect to its policies and practices; (b) Exercise reasonable care to ensure the accuracy and completeness of all			

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate; (c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate: (i) The identity of the certification service provider; (ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued; (iii) That signature creation data were valid at or before the time when the certificate was issued; (d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise: (i) The method used to identify the signatory; (ii) Any limitation on the purpose or value for			

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	which the signature creation data or the certificate may be used; (iii) That the signature creation data are valid and have not been compromised; (iv) Any limitation on the scope or extent of liability stipulated by the certification service provider; (v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law; (vi) Whether a timely revocation service is offered; (e) Where services under subparagraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service; (f) Utilize trustworthy systems, procedures and			

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	human resources in performing its services. 2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1. Article 10. Trustworthiness For the purposes of article 9, paragraph 1 (f), of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors: (a) Financial and human resources, including existence of assets; (b) Quality of hardware and software systems; (c) Procedures for processing of certificates and applications for certificates and retention of records;			

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	(d) Availability of information to signatories identified in certificates and to potential relying parties; (e) Regularity and extent of audit by an independent body; (f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or (g) Any other relevant factor. Article 11. Conduct of the relying party A relying party shall bear the legal consequences of its failure: (a) To take reasonable steps to verify the reliability of an electronic signature; or (b) Where an electronic signature is supported by a certificate, to take reasonable steps:			

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
	(i) To verify the validity, suspension or revocation of the certificate; and (ii) To observe any limitation with respect to the certificate.			
d. Liability of public providers	-	Liability is regulated without prejudice to public or private nature of service providers (incl. IdM service providers), but dependent only on latter's function, see item #7.c above.		The definition of liability provisions is <u>delegated</u> to the Coordinating Council, see Art. 5.2-A-2), Art. 5.2-B-4). The Coordinating Council may decide to regulate liability without prejudice to public or private nature of service providers (incl. IdM service providers), but dependent only on latter's function.
e. Consequences of compliance: i. exemption for compliance; ii. reversal of burden of proof.	-	IdM providers - primary determination of identity: Art. 6.1: <u>only</u> those electronic identification means <u>shall</u> be mutually recognized, if they are notified acc. Art. 9 and corresponds to the assurance level substantial or high. An optional exemption: Art. 6.2.		IdM providers - primary determination of identity: <u>delegated</u> to the Coordinating Council, see item #4.a above; the Coordinating Council should decide on exemptions and the reversal of burden of proof.

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
		For all those IdM-providers (primary determination of identity), the burden of proof is not explicitly regulated, s. Art. 11. TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: <u>Only</u> qualified TSPs may provide qualified TS, Art. 3-(20) Reversal of burden of proof depending on the current TSP qualification status: Art. 13.1 (for non-qualified: subscriber has to prove the TSP guilty; for qualified: TSP has to prove its innocence) <u>only</u> qualified TS enjoy mutual recognition[16]:		TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: see item #4.b above Provisions on burden of proof may be <u>delegated</u> to the Coordinating Council, Art. 5.2 <u>only</u> qualified TS enjoy mutual recognition[17]: - for eSign: Art. 15.4 - for eSeal: Art. 16.4 - for eTSS: Art. 17.4

[16] Pay attention also to Preamble (22): 'It is for the national law to define the legal effect of trust services, except if otherwise provided in this Regulation'.
[17] Pay attention also to Art. 20.3: 'It is for the national law to define the legal effect of trust services, except if otherwise provided in this Convention'.

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
		- for eSign: Art. 25.3 - for eSeal: Art. 35.3 - for eTSS: Art. 41.3 - for eRDS: Art. 43.2		- for eRDS: Art. 18.4 - for Website auth.: Art. 19.2 optional exemptions for advanced (but not qualified) eSign and eSeal: - for eSign: Art. 15.3 - for eSeal: Art. 16.3
f. Contractual limitation of liability	Possible for e-signatures according to art. 9(1)(d)(ii) MLES: "Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall […] provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise […] any limitation on the purpose or value for which the signature creation data or the certificate may be used".	IdM providers - primary determination of identity: no provisions TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: Art. 13.2, see also Art. 24.2 (d)		IdM providers - primary determination of identity: delegated to the Coordinating Council, see item #4.a above; TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: delegated to the Coordinating Council, see item #4.a and #4.b above.

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
8. institutional cooperation mechanisms	see below	see below		see below
a. federations?	ECC does not have a Conference of the Parties, in line with UNCITRAL practice. The Commission does not perform those functions.	EU Regulations are issued on the basis of the valid EU primary legislation (Treaties). The EU-related Treaties constitute the EU itself and form the cooperation between the Member States. Art. 47: the European Commission can be considered as the 'assemblage point' for the purpose of eIDAS cooperation of IdM schemes (primary identification of identity): Art. 12 mutual assistance between Supervisory Bodies supervising TSPs: Art. 18		SECTION III: The Coordinating Council: - Art. 5: Functions of the Coordinating Council - Art. 6: The establishment and procedure of the Coordinating Council The Coordinating Council represents the 'assemblage point' for the purpose of the 'Possible Draft Provisions' (in centralized segment only) cooperation of IdM schemes (primary identification of identity): <u>delegated</u> to the Coordinating Council, see item #4.a above;

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
				cooperation between Representatives of the State Parties: Art. 5 and 6.
9. transparency	see below	see below		see below
a. disclosure duties with respect to services offered	-	IdM-providers - primary determination of identity: Art. 9: information on IdM-schemes to be notified: MS towards the Commission TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: Art. 24.2 (a): changes in and cease of the operation of TSP: towards national SB Art. 24.2 (d): terms & conditions and limitations of TS use (see also Art. 13.2): towards TS subscribers		IdM-providers - primary determination of identity: delegated to the Coordinating Council, see item #4.a above see also Art. 5.2-A-1) TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: Art. 8.4: - acquisition and alteration of TSP status: on the Internet - changes in the operation of TSP and of the TSP status: towards the competent authorities of the responsible State Party
b. notification of security breaches	For e-signatures, an optional breach notification mechanism is	IdM-providers - primary determination of identity:		IdM-providers - primary determination of identity:

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
i. types of breaches to be notified ii. entities to be notified	mentioned in art. 8(1)(b) MLES: "Where signature creation data can be used to create a signature that has legal effect, each signatory shall: […] (b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if: (i) The signatory knows that the signature creation data have been compromised; or (ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised […]".	Art. 10.1 and 10.2: security breaches: notifying MS towards other MS and the Commission; Art. 10.1: each types of breaches affecting the reliability of the cross-border authentication by that scheme TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: Art. 19.1: security incidents: towards stakeholders Art. 19.2: security breaches: towards national SB, national security and data protection authorities, TS subscribers types of breaches and security incidents: Art. 19.2: any breach of security or loss of integrity that has a significant impact on the trust service provided or		delegated to the Coordinating Council, see item #4.a above see also Art. 5.2-A-1) TSPs as (i) IdM providers of secondary determination of identity and as (ii) TS providers: Art. 8.4: - interaction incidents towards the competent authorities of the State Parties and the Coordinating Council

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
		on the personal data maintained therein.		types of incidents and procedures: Art. 8.4: delegated to the Coordinating Council, see also Art. 5.2-B-1)
10. no new obligation to identify[18], see also item #2.b above	No UNCITRAL text.	For IdM: primary determination of identity: Identification of natural and legal persons is not compulsory. However, natural or legal persons, who do not possess electronic identification means fulfilling the requirements of Art. 6, cannot enjoy the benefits of the mutual transboundary recognition of results of the identification; hence, non-possessing such identification means diminishes the transparency of market for TSPs and for trust service subscribers. ------- secondary determination of identity:		For IdM: primary determination of identity: delegated to the Coordinating Council, see item #4.a above ------- secondary determination of identity:

[18] *parties have to freely decide to use or not to use any IdM or trust services => parties autonomy, s. item #2.b.*

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
		secondary determination of identity: - for subscriber's enrolment: identification of natural and legal persons (TS subscribers) <u>is compulsory</u> by qualified TSPs i) issuing qualified certificates: Art. 24.1, ii) issuing means for advanced and qualified el. signatures and seals: Art. 26 (b) and 36 (b), resp., iii) providing eRDS: Art. 43.2 and 44.1 (b), (c), if a subscriber's enrolment procedure is foreseen by TSP. - for transactions: identification of natural and legal persons (subscribers) <u>is compulsory</u> for - advanced and qualified eSign: Art. 26 (c) - advanced and qualified eSeal: Art. 36 (c) - qualified eRDS: Art. 44.1 (b), (c)		- for subscriber's enrolment: <u>delegated</u> to the Coordinating Council, see item #4.a above - for transactions: identification of natural and legal persons (subscribers) <u>is compulsory</u> for - advanced and qualified eSign: Art. 15.2 c) - advanced and qualified eSeal: Art. 16.2 c) - qualified eRDS: Art. 18.3 b), c) For TS:

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
		For TS: Usage of qualified TS is <u>not</u> compulsory. However, the subscribers, who <u>do not use</u> qualified TS, <u>cannot</u> enjoy the benefits (i) of the mutual transboundary recognition and (ii) of the presumption of integrity and accuracy of results of the application of trust services according to: - eSign: Art. 25.2, 25.3 - eSeal: Art. 35.2, 35.3 - eTSS: Art. 41.2, 41.3 - eRDS: Art. 43.2; Non-usage of qualified TS diminishes the transparency of market for TSPs and for relying parties.		Usage of qualified TS is <u>not</u> compulsory. However, the subscribers, who <u>do not use</u> qualified TS, <u>cannot</u> enjoy the benefits (i) of the mutual transboundary recognition and (ii) of the presumption of integrity and accuracy of results of the application of trust services according to: - eSign: Art. 15.3, 15.4 - eSeal: Art. 16.3, 16.4 - eTSS: Art. 17.2, 17.4 - eRDS: Art. 18.2, 18.4 - Website auth.: Art. 19.2; Non-usage of qualified TS diminishes the transparency of market for TSPs and for relying parties.
11. data retention (perhaps more generally – data processing and	As noted above, art. 10 MLEC provides a functional equivalence rule on data retention. Retention time is	Provisions on data processing and protection: Art. 5 and Art. 24.2 (j)		Provisions on data processing and protection: Art. 4-3): as a general principle

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
protection? Data retention aspect usually represents a subset of this broader topic)	determined by the need to preserve electronic records for legal compliance purposes (e.g. limitation of action).	Art. 24.2 (h): keeping operational records by qualified TSP for an appropriate period of time; the term 'appropriate period of time' may be subject to interpretation by national law. Art. 24.2 (i): the cease of service – the termination plan may include provisions on data retention.		Establishing concrete provisions on this topic is delegated to the Coordinating Council, see Art. 5.2-A-1), Art. 5.2-B-1), 5.2-C; see also Art. 8.3 (TSP's obligation).
a. as a trust service?	-	no		no
b. Existing UNCITRAL provisions	See above.	-		-
12. supervision of service providers (items #5, #7 and #12 belong together)	Optional. For e-signatures, it may be taken into consideration in assessing trustworthiness of the CSP: art. 10(e) and (f) MLES (see above).	Art. 17.1: Supervision of qualified TSPs is performed by national Supervisory Bodies Art. 17.3, 17.4 and 17.5: the role and the tasks of SBs Art. 18: mutual assistance between SBs, see also Art. 17.4 (a).		supervision provisions are not explicitly stated, but might be delegated to the Coordinating Council in the context of Art. 5.2-B-1), 5.2-B-2), 5.2-B-3); Art. 8.3, Art. 8.6 The supervision task concerning TSPs

Roadmap	*Existing UNCITRAL provisions*[1]	*eIDAS*	*Provisions from other relevant regional or national laws (e.g. Virginia IdM Act)*[2]	*DRAFT INSTRUMENT (see A/CN.9/WG.IV/WP.155)*
		The supervision task stated in Art. 17.4 (b) is directly connected with the audits of qTSPs by CABs as required by Art. 20.1, see also item #5 above.		presumed to be defined by the Coordinating Council might be directly connected with the certification of TSPs by CCB[19]: Art. 8.6, see also item #5 above.

[19] Compliance Confirmation Body acc. to Art. 5.2-B-6) of draft instrument.