N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL01	Rec37 WG	15/10/2012	The title should encompass the word “manual” or “ink” to clarify the scope of the document in order to not lead to misinterpretation.	Should probably rethink the title completely. Wait until recommendation is developped before generating a title. "Authentication of trade & other documents…" or "Electronic documents…"	
DL02	Rec14 v1979	01/03/1979	Main recommendation is: * eliminate all signatures and authentication unless essential for the function of the data/document transmitted * when signature is necessary, enable electronic means of replacing the manual signature	Confirmed (should discuss e-seal separately at a later time)	
DL03	Vienna Forum & UNCITRAL "Promoting Confidence…" & FI Min Transport/Tel	18/09/2012	Additional recommendation: * choice of electronic solution should be proportionate to the level of security called for by the data/document transmitted (not everything has to be certified…) This can also be called "security assurance levels" as presented in FI Ministry of Transport & Telecommunication comments	levels of assurance - chapter 5 (not part of the top level recommendation but clearly within the text)	5
DL04	Rec37 WG	15/10/2012	Request was made to make a clear distinction between document certification with signature on the one hand and process certification on the other. Suggest that this could enter into Part 2, chapter 5; furthermore, this can complete a ‘typology’ provided by UNCITRAL in their “Promoting Confidence…” document for example for the annex B on technological solutions.	Addressed in chapter 2 (document authenticity) and in chapter 5 as on e of the typologies	5
DL05	L.Thompson (FR)	24/10/2012	Part 2 Chapter 4 (signature and proof of authenticity, integrity and veracity) are aspects of the function of a signature and should therefore be presented in Chapter 2 (definition & function of signature)	authenticity acheived when levels of the three functions of a signature are at a certain (hgih) level. Integrity is part of evidentiary function. Veracity of signatories and their identity claims is part of identification function…	2
DL06	L.Thompson (FR)	24/10/2012	Part 2 Chapter 6 (approval, registration and authorization to use other authentication methods) - it is unclear if this is pertinent to all forms of electronic signature. Are scanned signatures registered and approved? Are ID/password systematically approved or can they be individually generated by user?	Approval, registration and authorization are no longer in the title of chapter 6. If and when pertinent, they can be addressed in the repository of Annex. B	B

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL07	L.Thompson (FR)	24/10/2012	Part 2 Chapter 7 (security of data, including transmission). I believe that this title needs to be reworked. Perhaps merged with a chapter on archiving and retrieval of data…	Chapter 6 title has become "Security of data, transmission ,archiving, retrieval." The archiving/retrieval aspects are being addressed on an equal footing, but it is acknowledged as not being the core aspect here.	6
DL08	Vienna Forum	18/09/2012	From the Vienna meeting, it seems that a chapter on archiving and retrieval of data will be necessary.	idem	6
DL09	L.Thompson (FR)	24/10/2012	Part 2 proposed new chapter on archiving and retrieval of data. If the use of an electronic signature is obvious when transmitting data, it also must be able to be used in order to archive and retrieve data at a later time. Perhaps this should/could be presented with the chapter on "security of data, including transmission"	idem	6
DL10	L.Thompson (FR)	24/10/2012	Part 2 Chapter 9 (data transmission issues who, what, when, where, how). Though the title is very clear, I am not sure that this will pertain to all forms of electronic signature (an ID/password will not give elements of when and where it was associated to electronic data, for example). The information on "who" should be addressed in chapter 2 (function of signature). The information on "what" and "how" should be addressed in the "other methods"chapter.	Can be eliminated since it is being discussed elsewhere.	
DL11	L.Thompson (FR)	24/10/2012	Should the “checklists” be presented in Part 2 of the Recommendation, or in the corresponding annexes?	Probably for the Annex A as part of an introduction	A
DL12	L.Thompson (FR)	24/10/2012	Initial draft of Annex A (legally enabling environment) template for submissions	Template completed	A
DL13	Vienna Forum	18/09/2012	Initial suggestion that Annex B (technological solutions) be organized in "Typologies" as found in UNCITRAL main document * digital signatures [further divided into fail-stop digital signatures, blind signatures, undeniable digital signatures], * biometric methods, * passwords and hybrid methods, * scanned or typed signatures) and adding at least two further categories: * complete elimintation of signature, * authenticiation through means of transmission (VPN, fax, etc.)	Chapter 5 is structured around these and more typologies and Annex B will most likely be organized according to this same organization.	B
DL14	UNCITRAL & FI Ministry of Transport +Telecommunications	24/10/2012	Technological neutratility is very important for the recommendation. There should be alternative options and technologies available for the authentication of the trade documents	technology Neutrality is an integral part of chapter 5 and will be kept in mind.	5

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL15	WCO DMPT	16/10/2012	Is this recommendation solely concerned with trade documents, or also object authentication (ie container seals)?	only trade documents.	
DL16	conf call	24/10/2012	Part 2, chapters 5 & 6 should be moved up inbetween chapters 1 & 2 of Part 2	approved	
DL17	conf call Marco	24/10/2012	Party autonomy & agreeing on a principle of electronic exchange to be perhaps included as a chapter in Part 2	To be further discussed, perhaps with some more legal input.	
DL18	M.Dadashov (LT)	Conf.Call.2 20/11/2012	Another point that has not been emphasized in the initial document yet, the the Recommendations/solutions should have been formulated in language understandable to the targeted audience, in other words we should present our solutions in a way understandable to contractual parties	Key terms should be addressed in chapter 2 (definition of signature) ; target audience is also government agencies. Language should be kept understandable to all and not just initiated.	2
DL19	M.Dadashov (LT)	Conf.Call.2 20/11/2012	With these in mind [above point & technology neutrality], I'd suggest restructuring the "Proposed organization of received solutions" as follows: 1. Signature-based Authentication Methods 1.1 High Assurance Solutions 1.2 Mutually Agreed Solutions 1.3 Combined Signature Solutions (e.g. Single signature contracting-joining an unsigned generic contract) 2. Delivery (e-delivery) based authentication solutions 2.1 Mutually authenticated peer-to-peer e-delivery (no third party involved) 2.2 Third party (trusted third party) authenticated store and forward e-delivery 3. …?	Structure of chapter 3 is proposed to be based on typologies (B2B, B2C, B2G, G2B, G2G…)	3
DL20	UNCITRAL	Conf.Call.2 20/11/2012	Article 7 (1): Where the law requires a signature of a person, that requirement is met in relation to a data message if: a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement. UNCITRAL Model Law on Electronic Commerce	(background material)	2
DL21	Rec14 1979+	Conf.Call.2 20/11/2012	Recommendation 14 recommends: a) Eliminate signature and all forms of authentication whenever possible (when not essential for the function of the document/data transmitted) b) When signature is necessary, enable electronic means of replacing the manual signature c) Choice of electronic solution should be proportionate to the level of security called for by the data transmitted (not everything needs to be certified) – [not yet confirmed as part of the main recommendation]	(background material)	2

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL22	A.Sazonov (RCC)	Conf.Call.2 20/11/2012	1. A document in electronic form, as well as a paper one, is to fulfil its legal function. 2. The discrete (electronic) nature of a document eliminates the difference between a document's original and copy. Such speculations on this topic are given in UNCITRAL Secretariat's Note A/CN.9/WG.IV/WP.115 - Legal issues relating to the use of electronic transferable records. In this document two essentially different approaches to ensuring e-document's uniqueness are considered: a. ensuring document's technical uniqueness; b. identification of an authentic copy of a document. Identification of requirements for ensuring authenticity of an e-document is difficult at the present stage due to the fact that there is no univocal understanding of the term "electronic document". The concept of "electronic document" is one of the points at issue of the new Recommendation for Trusted trans-boundary electronic trade document exchange. After formulating the concept of "electronic document" it will be possible to identify the requirements for ensuring authenticity.	UNCITRAL is being used as the base for electronic signature definition. Function in three aspects: identification, evidentiary and attribution. Document authenticity is proposed in chapter 2 (definition / function of signature) The technical aspects (authenticity, uniqueness) will depend on the amount of each function is inherent in the signature.	2
DL23	H.Putteneers (BE)	Conf.Call.2 20/11/2012	Electronic signatures, when carefully implemented, can offer a higher degree of reliability and can be used to ascertain the content of the document is authentic. However, given the multitude of methods and systems, maintenance of a verification infrastructure can be a cumbersome and costly task.	Acknowledged Integrated into the idea of levels of assurance.	5
DL24	J.Salo (FI)	Conf.Call.2 20/11/2012	Technological neutrality is very important for the recommendation. There should be alternative options and technologies available for the authentication of the trade documents	Technology neutrality: common understanding of semantics of information being exchanged. –does not promote one technology over another. Must not create stringent requirements which would put in doubt the validity and enforceability of transactions. To achieve the technology neutrality, the law should not discriminate between forms of technology. Interoperability to be addressed in Annex B repository of implementations.	5
DL25	M.Dadashov (LT)	Conf.Call.2 20/11/2012	It's been recognized that the Recommendations should be technologically neutral however. o fulfill this recognition the final Recommendations should have solutions/proposals structured in a technologically neutral way as well.	idem	5
DL26	J.Stoopen (NL)	Conf.Call.2 20/11/2012	Without hinting at certain or specific solutions, it might be an idea to emphasize the importance of the use of agreed (technical) standards. Especially for governments it might be more cost effective to limit themselves to one or two standards. The spin-off effect of that is that for business and public it will be easier (user friendly) and cheaper if they only have to deal with a limited number of standards	idem	5

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL27	S. Lennartsson (SE)	Conf.Call.2 20/11/2012	new rec 14 is maintained at a level such that the document works regardless of technology choice in the individual case, ie, whether paper, electronic mail, mobile technology or other similar technology-related uses. [Compare - we try to keep the law technology-neutral in Sweden.]	idem	5
DL28	UNCITRAL	Conf.Call.2 20/11/2012	"Electronic authentication and signature methods may be classified in three categories: - those based on the knowledge of the user or the recipient (e.g. passwords, personal identification numbers (PINs)), - those based on the physical features of the user (e.g. biometrics) and - those based on the possession of an object by the user (e.g. codes or other information stored on a magnetic card). UNCITRAL, Model Law on elec sign, part 2 §13	(background material)	3
DL29	UNCITRAL	Conf.Call.2 20/11/2012	Typologies of electronic signatures: "… four main signature and authentication methods will be discussed - digital signatures - biometric methods, - passwords and hybrid methods and - scanned or typed signatures." UNCITRAL, Promoting Confidence, p.17 §24 "The digital signature has many different appearances such as - fial stop digital signatures, - blind signatures and - undeniable digital signatures." UNCITRAL, Promoting Confidence, p.18 §25.	(background material)	3

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL30	A.Sazonov (RCC)	Conf.Call.2 20/11/2012	The following question is to be answered: In what way a distinctive mark, characteristic, etc, that identifies a person or thing ensures for a document: a) the property of being genuine b) the ability to be verified c) the ability to be trusted The consequent speculations are to be grounded on the fact that in case of paper document a handwritten signature is made directly on a document itself and is its integral (inalienable) part. A handwritten signature on a paper document is a distinctive mark identifying a signer. And in this quality it can ensure only document's property of being genuine. In case when a handwritten signature is used the ability to be verified and the ability to be trusted are ensured by a third party, which can be: a) a competent government body – issues a passport, in which subject's handwritten signature is associated with identification characteristics thereof (name, photograph, citizenship, date of birth etc); and additionally it can be b) an organization – issues a certificate, a license or another document in which subject's name is associated with subject's powers.	The three functions of a signature are on variable scales and can be higher or lower. The aspects described here are most probably higher on each scale. The use of a trusted third party is not systematic and will depend on the risk assessment of the needs of the transaction both on the level of the process (trade document) and the legal constraints. cf chapter 5. The level of assurance necessary for the transaction.	2
DL31	UNCITRAL	Conf.Call.2 20/11/2012	"It is often neglected … that a very large number, if not the majority, of business communications exchanged throughout the world do not make use of any particular authentication or signature technology." (UNCITRAL, Promoting Confidence, p.30 §65) Exchanges with no form of authentication are common business practice in interest of ease, expediency and cost-effectiveness (e.g. e-mails). Must not create stringent requirements which would but in doubt the validity and enforceability of these transactions… UNCITRAL, Promoting Confidence, p.30 §66.	(background material)	3

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL32	UNCITRAL	Conf.Call.2 20/11/2012	Article 7 (1): Where the law requires a signature of a person, that requirement is met in relation to a data message if: a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement. UNCITRAL Model Law on Electronic Commerce "…more appropriate to graduate security requirements in steps similar to the degrees of legal security encountered in the paper world." UNCITRAL, Promoting confidence, p.40 §90. "…not all applications may require a security level comparable with that provided by certain specified techniques, such as digital signature." UNCITRAL, Promoting confidence, p.40 §91	(background material)	3
DL33	J.Salo (FI)	Conf.Call.2 20/11/2012	The revision of recommendation 14 aims to ease the authentication of the trade documents. The objective is that other means than signature will also be available. Starting point would be the signature is not mainly required for the trade documentation. To achieve these objectives, conditions and requirements for the other means than signature should not be too strict	"Removal of the requirements for a signature except where essential for the function of the document" is an integral part of the recommendation… Should avoid suggesting complete elimination of signature out of context.	5
DL34	J.Salo (FI)	Conf.Call.2 20/11/2012	Discussions about the security assurance levels diminish the technological neutrality of the recommendation. Security assurance levels would have an impact for the number of the acceptable other options than signature. UNCITRAL does not define the security assurance levels	Technology neutrality must be kept in mind when speaking of levels of assurance	5
DL35	A.Caccia (IT)	Conf.Call.2 20/11/2012	LEVEL OF SECURITY + LEVEL OF INTEROPERABILITY = technology to be used.	idem	5
DL35	C.vanderValk (SE)	Conf.Call.2 20/11/2012	Security levels (examples of today's environment) - lowest for processes and transactions that have no significant value and/or that are not legally critical - Secured transparent – secured by one party to allow the other to perform operations in an environment the first party secures (ID+Password, purchases in secure networks [https, PKI signature ensured by the first party only with no sharing of keys…], etc.) - "soft" public keys – third party issued PKI keys that can be stored on user's computer or on that party's service provider system (which is then accessed by the party usually using ID+Password) - Highest level – reversal of burden of proof, credentials typically stored on hardware devices (smartcard, USB key, etc.)	Looking to allign with ISO/IEC ongoing work on lovels of assurance Solution needs to allow for risk-assessment & practical implementation. – parameters and guidelines that everyone can use. If we go into too much detail of the different levels, it will need to become technical (and may go against technology neutrality). Could use the idea of the context in which it should be used (context of the document)…	3

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL35	G.Galler (EU)	Conf.Call.2 20/11/2012	It is more a continuum more than levels. (Galler – EU) What is present in the lowest level e-signature is present also in qualified. It is more security assurance levels. All electronic signatures are equivalent to a hand-written signature.	idem	5
DL35	J.Baiamonte (US)	Conf.Call.2 20/11/2012	Legacy systems have resulted in different technology levels. In the US as well, it is considered a continuum. (J. Baiamonte, US)	idem	3
DL36	A.Sceia (UN)	Conf.Call.2 20/11/2012	Alternatively [to PKI technology…], for information that does not take the form of an electronic document (in the sense of an electronic file), a secured connection between parties (e.g. VPN) would also allow the identification of the parties that exchange the information (messages). In that sense the encryption of the channel ensures the integrity of the data and the encryption keys identify the parties. The technology behind a VNP remains very similar to a PKI though	Typologies of electronic methods: PKI, Communication channel and the possibility of combination of methods.	5
DL37	UNCITRAL	Conf.Call.2 20/11/2012	Government approach oriented towards interaction with physical persons. Commercial applications need to take into account use of automated machines… UNCITRAL, Promoting confidence, p.31 §70.	(background material)	3
DL38	G.Galler (EU)	Conf.Call.2 20/11/2012	[EU draft regulation on e-signature Art.3 (20)] 'electronic seal' means data in electronic form which are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data	Electronic seal was identified as a typology of electronic method that can replace a manual-ink signature	5
DL39	G.Galler (EU)	Conf.Call.2 20/11/2012	[EU draft regulation on e-signature Art.19] 'creator of a seal' means a legal person who creates an electronic seal	Electronic seal was identified as a typology of electronic method that can replace a manual-ink signature	5
DL40	G.Galler (EU)	Conf.Call.2 20/11/2012	[EU draft regulation on e-signature Art.20] 'advanced electronic seal' means an electronic seal which meets the following requirements: a) it is uniquely linked to the creator of the seal; b) it is capable of identifying the creator of the seal; c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable	Electronic seal was identified as a typology of electronic method that can replace a manual-ink signature	5
DL41	G.Galler (EU)	Conf.Call.2 20/11/2012	[EU draft regulation on e-signature Art.22] 'qualified electronic seal' means an advanced electronic seal which is created by a qualified electronic seal creation device, and which is based on a qualified certificate for electronic seal	Electronic seal was identified as a typology of electronic method that can replace a manual-ink signature	5

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL42	G.Galler (EU)	Conf.Call.2 20/11/2012	In the paper world, there are concepts such as "envelopes" and "certified mail" that can be confidence-raising for document delivery	Chapter 6 : transmission of data, confirmation of sending / Confirmation of receipt of the transmission	6
DL43	Rec14 v1979	Conf.Call.2 20/11/2012	"Signature" has been defined on many occasions, and a number of definitions given in legal and literary dictionaries are shown in Annex 1. Nearly all definitions require that the signatory write his name by hand. In court hearings the decision as to what constitutes a signature, is a question of fact which the judge decides himself. Some legal decisions about what constitutes a signature, taken from Belgian jurisprudence, are shown in part 2 of Annex I. Although the United Nations Convention on the Carriage of Goods by Sea, 1978 (Hamburg Rules), states in Article 14 (3) that a signature may be in handwriting, printed in facsimile, perforated, stamped, in symbols or made by any other mechanical or electronic means (if not inconsistent with relevant national law), this study is based on the generally-accepted meaning given to the word in international trade and legal circles.	(background material)	4
DL44	UNCITRAL	Conf.Call.2 20/11/2012	"Regardless of the particular legal tradition, a signature, with very few exceptions, is not self-standing. Its legal effect will depend on the link between the signature and the person to whom the signature is attributed. UNCITRAL, Promoting confidence, p.5 §9	(background material)	4
DL45	A.Sazonov (RCC)	Conf.Call.2 20/11/2012	[Signature can be defined] a distinctive mark, characteristic, etc, that identifies a person or thing. Excerpt Collins English Dictionary 2009.	identification function	2
DL46	H.Putteneers (BE)	Conf.Call.2 20/11/2012	The classical handwritten signature is just one of a range of methods that try to establish the authenticity of signed documents by relying on certain formalisms. Comparable methods in the same league include the use of company letterhead paper, specially crafted stamps, watermarked paper, seals, ea. I think it may be worth pointing out that the trust which is often assigned to these methods is overly optimistic. Verification can be cumbersome.	Functions of a signatures are on variable scale, so admittedly low in each of these cases. Document authenticity also responds partly to this comment (origin & integrity of document)	2
DL47	UNCITRAL	Conf.Call.2 20/11/2012	"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" UNCITRAL, Model Law on Electronic Signatures, article 2.	(background material)	4
DL48	CMR – Additional Protocol, Art.1	Conf.Call.2 20/11/2012	"Electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.	Authentication, following UNCITRAL terminology, was deemed out of scope of the definition and function of a signature.	4

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL49	A.Sceia (UN)	Conf.Call.2 20/11/2012	A (n electronic) signatures should identify the person that signs and make sure that the signature is for a specific document	attribution function	2
DL50	A.Sceia (UN)	Conf.Call.2 20/11/2012	(Electronic) signatures should be recognized internationally (unless the document is securely exchanged among trusted parties)	Reworded to: An electronic signature should not be discriminated because of its origin (but may be discriminated because of its intrinsic qualities).	2
DL51	A.Sceia (UN)	Conf.Call.2 20/11/2012	It should be possible to detect any change in the document after it was signed	evidentiary function	2
DL52	G.Galler (EU)	Conf.Call.2 20/11/2012	[EU draft regulation on e-signature Art.3 (1)] 'electronic identification' means the process of using person identification data in electronic form unambiguously representing a natural or legal person	identification function	2
DL53	R. Migliorini (IT)	Conf.Call.2 20/11/2012	As a starting point in my opinion we should deal with "e-signature" as defined by UNCITRAL text while narrowing the methods that can be used. Generally, e-signatures are or digital signatures or electronic signatures differentiating by the presence or absence of PKC. The digital signature that relies on PKC (public Key Cryptography) is the most standard type of crypto-based digital signature with widespread acceptance and the most suitable to establish trust in an online world.	UNCITRAL is being used as the base for electronic signature definition. PKC is a specific technology identified in chapter 5; examples in a repository in Annex B will permit to discuss it further if necessary.	2
DL54	S. Lennartsson (SE)	Conf.Call.2 20/11/2012	use of the signature does not protect the confidential or sensitive information, the creation of an e-signature can certainly be based on an encryption mechanism, but this gives absolutely no lock protection for the document content as the signature is applied to.		2/6
DL55	UNCITRAL	Conf.Call.2 20/11/2012	"It should be noted […] that even though authenticity is often presumed by the existence of a signature, a signature alone does not 'authenticate' a document." UNCITRAL, Promoting confidence, p.5 §8 "… the vast majority of international written contracts […] are not necessarily accompanied by any special formality of authentication procedure." UNCITRAL, Promoting confidence, p.7 §12	(background material)	4
DL56	UNCITRAL	Conf.Call.2 20/11/2012	"…'electronic authentication' is used to refer to techniques that […] may involve various elements, such as identification of individuals, confirmation of a person's authority […] or prerogatives […] or as assurance as to the integrity of the information. In some cases, the focus is on identity only, but sometimes it extends to authority, or a combination of any or all of those elements." UNCITRAL, Promoting confidence, p.14 §18.	(background material)	4
DL57	UNCITRAL	Conf.Call.2 20/11/2012	[UNCITRAL documents don't use the term 'electronic authentication'…] "The Model Law on Electronic Commerce uses instead the notion of 'original form' to provide the criteria for the functional equivalence of 'authentic' electronic information." UNCITRAL, Promoting confidence, p.14 §19.	(background material)	4

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL58	G.Galler (EU)	Conf.Call.2 20/11/2012	Confusion should be avoided between persons and documents authentication: by clearly stating when it applies to authenticate (i.e. validate) the identity claim of the natural/legal person that has created a document (i.e. origin) from the authenticating a document (i.e. origin and integrity) of the document.	Chapter 2: Document authenticity – origin & integrity of document / quality of document / data	2
DL59	G.Galler (EU)	Conf.Call.2 20/11/2012	Confusion should also be avoided between identification of a person and authentication of his/her/its identity claim	Identification function is considered on a variable scale. Identity claim confirmation on higher level of this scale. (?)	2
DL60	G.Galler (EU)	Conf.Call.2 20/11/2012	In the draft regulation [of the EU future e-signature regulation…], we have introduced electronic seals that can be used instead of esignatures in a number of case where the origin and integrity of a document is what matters. Signature conveys in addition a consent/commitment which is not always needed. Seals should be easier to handle because, for us, a legal person can create seal while a signature (consent) can only be created by a human being	Document authenticity.Evidentiary function (consent) / Attribution function (commitment)	2
DL61	G.Galler (EU)	Conf.Call.2 20/11/2012	[EU draft regulation on e-signature Art.3 (4)] 'authentication' means an electronic process that allows the validation of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data	See notion of authenticity in chapter 2 where a certain level of identification, evidentiary and attribution are attained. The term 'authentication' in this context is not used in UNCITRAL documents.	2
DL62	A.Sazonov (RCC)	Conf.Call.2 20/11/2012	[Authentication can be defined] The property of being genuine and able to be verified and be trusted.	The term 'Authentication' in the sense of this comment and following UNCITRAL terminology, was deemed out of scope of the definition and function of a signature.	2
DL63	Rec.14 v1979	Conf.Call.2 20/11/2012	A signature on trade documents serves three main purposes: (i) It identifies the source of the document, i.e. the writer; (ii) It confirms the information in the documents; and (iii) It constitutes proof of the signatory's responsibility for the correctness and/or completion of the information in the document. The signature gives an element of proof which virtually amounts to undisputed legal validity of the document and the data transferred. Whereas the formal requirement is for a signed document, the essential function is that of authentication of data content. The need for verification may in certain cases also lead to requirements of composite authentication–that is to say, not only is the signature of the responsible part required, but also a signed declaration by some official or semi-official body endorsing the signature.	(background material)	4

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL64	Rec.14 v1979	Conf.Call.2 20/11/2012	Signature and proof 13. If it is perfectly possible to envisage replacing the signature, why are people still so attached to it? The explanation may be found in the value of proof which a signature provides. Documents produced before a Court of Law are only legally valid in so far as they are acknowledged by the person said to have signed them. A handwritten signature can be particularly useful in this respect. While forgeries are possible and a person may refuse to recognize a signature, it must be said that it is more difficult to deny responsibility for a document which bears a signature than for one which does not. 14. Whilst a signature is not usually indispensable on commercial documents, it is quite often required for official purposes. Because there are so many different national provisions, participants in international trade–fearing nonfulfillment of possible requirements–play safe by putting a signature on most documents. The guarantees thought to be provided by a signature mean that they are frequently used also on commercial documents, although less frequently, perhaps, when the parties are well known to each other.	(background material)	4
DL65	UNCITRAL	Conf.Call.2 20/11/2012	"Signatures […] perform three main functions in the paper-based environment: - Signatures make it possible to identify the signatory (identification function); - Signatures provide certainty as to the personal involvement of that person in the act of signing (evidentiary function); and - Signautres associate the signatory with the conent of the document (attribution function)." UNCITRAL, Promoting confidence, p. 5,§7	(background material) C.Praliaud (FR) agrees with these functions	4
DL66	CMR – Additional Protocol, Art.1	Conf.Call.2 20/11/2012	1. The electronic consignment note shall be authenticated by the parties to the contract of carriage by means of a reliable electronic signature that ensures its link with the electronic consignment note. The reliability of an electronic signature method is presumed, unless otherwise proved, if the electronic signature: (a) is uniquely linked to the signatory; (b) is capable of identifying the signatory; (c) is created using means that the signatory can maintain under his sole control; and (d) is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. 2. The electronic consignment note may also be authenticated by any other electronic authentication method permitted by the law of the country in which the electronic consignment note has been made out. 3. The particulars contained in the electronic consignment note shall be accessible to any party entitled thereto.	functions of a signature: identification, evidentiary (changes detectable). Authentication by means acceptable in legal context of the country… Accessibility only reserved to those entitled… perhaps should add the idea that the reliability is presumed unless otherwise proved.	4
DL67	R.Migliorini (IT)	Conf.Call.2 20/11/2012	Even if the e-signature is mainly what is known legally as an "affirmative act" in terms of REC 14 signature purposes I see two main goals: • Integrity of data • Proof of origin	Integrity is an aspect of the "Evidentiary Function" depending on the applicable legislation. Proof of origin is an aspect of "Identification function"	2

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL68	Rec.14 v1979	Conf.Call.2 20/11/2012	5. A signature may be required by virtue of a formal legal requirement, either in national law or international convention. It may serve a specific purpose, or the requirement may simply be based on commercial practice. Where there is a mandatory requirement, a signature is needed unless the law is amended or repealed. In order to make data transferred by electronic means acceptable as valid documents in law, the signature must be replaced by an alternative method of authentication. 6. In general, the following interests are affected: (a) commercial, (b) transport, (c) financial, and (d) official. Problems arise mainly with "documents that travel", often called "shipping documentation", i.e. documents that transfer data which are only available at dispatch and which are necessary for the clearance of goods at destination. Certain documents which actually accompany the goods, such as the ships' manifest or dangerous goods documentation, may not constitute problems. It should also be recalled that the information in some documents may be of interest to more parties than the originator and final recipient of the documents.	(background material)	5
DL69	J.Stoopen (NL)	Conf.Call.2 20/11/2012	Mention the necessity of having policies in place as catalyst for change in the area of authentication of (electronic) documents.	chapter 4: Policies can be catalyst for change in the area of electronic exchanges	4
DL70	J.Stoopen (NL)	Conf.Call.2 20/11/2012	Private law requirements need to be aligned with the current way of doing business and modern technology	Chapter 4: The chosen wording is "Public law need to be aligned with current way of doing business & with current best practices and standards"	4
DL71	J.Stoopen (NL)	Conf.Call.2 20/11/2012	Public law requirements need to be aligned with the current possibilities of information technology (recognition of a digital signature, the use of an E-identity, the use of an unique and recognizable access to systems, E-recognition, etc.)	Within the legal framework aspect of chapter 4, it is suggested that governments review their law regularly in order to align "with current ways of doing business & with current best practices and standards."	4
DL72	J.Stoopen (NL)	Conf.Call.2 20/11/2012	Private rules and agreements regarding the use of commercial documents and their authentication must be aligned with the current possibilities of information technology	No mention is made to current possibilities of information technology directly, but rather: "Choice of authentication methods will depend on the business process and a risk assessment of the needs of that process." And that the risk assessment should consider the context of the process (trade document) and ... the legal constraints"	4

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL73	J.Salo (FI)	Conf.Call.2 20/11/2012	The issue is quite complex, because there are different types of documents in use, and they do have different functions. Legally, the signature is generally associated with expression of will, but technically the signature requirement (such as e-invoicing as in many countries) is related to the origin and authentication of (trade) documents. In general, the focus should be set to the approach based on the reliability assumption, according to which the requirement of signature as a rule should be waived. The Recommendation should keep on encouraging this kind of development. For example the ICC's rules of the letter of credit takes quite liberal approach to the documents (mechanical signature allowed, flexible definition of the original document).	attribution function of signature & document authenticity. "Removal of the requirements for a signature except where essential for the function of the document" is an integral part of the recommendation… Should avoid suggesting complete elimination of signature out of context.	2
DL74	J.Stoopen (NL)	Conf.Call.2 20/11/2012	For making an analysis it might be useful to make a distinction between: • Business to Business; • Business to Government / Government to Business; • Business to consumers; • Public to Government / Government to Public.	Structure of chapter 3 is proposed to be based on typologies (B2B, B2C, B2G, G2B, G2G…)	3
DL75	J.Salo (FI)	Conf.Call.2 20/11/2012	The signature section (part 1 of Rec. 14) is split up into chapters for commercial documents, transport documents, financial documents and official documents. This has been a clear division into different documentation. However, if the aim of the Rec. 14 revision is that the signature is not mainly required for the trade documentation, there could be, instead of above mentioned chapters, only one chapter for the documents with the requirement for a signature On the other hand, if the present approach is chosen, there is at the moment no substantial need for the changes in approach and sequencing in the "Requirements for signature in trade documentation". Some textual editions and updates should naturally be made especially when finalizing and polishing the text and embedding it to the other contents of the recommendation All this leads to the conclusion that obviously the mentioned complexity has resulted situation where nothing much has been happened in this area (requirements) during the last 20+ years. Of course new electronic documents has been introduced along the years. However, the basic requirements related to signatures has always been adapted to the existing legislation and paper documents, maybe due to principle of equality of paper and electronic documents as well as electronic and manual signature	Structure of chapter 3 is proposed to be based on typologies (B2B, B2C, B2G, G2B, G2G…)	3

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL76	Rec.14 v1979	Conf.Call.2 20/11/2012	Commercial documents 7. The main principle of international trade law is that there is no formal requirement for a signature. Subject to an exceptional requirement of signature in national law, documents required for the practical performance of a contract, such as a commercial invoice, or a certificate regarding quality and quantity, need not therefore be signed. The parties concerned are mainly interested in identification of the documentation and verification of data content, which can be obtained from other sources and are not dependent on a signature. The same is true for the shipping advice/notification called for in most trade terms. There is therefore no reason to include a requirement of signature in the requirements for commercial information which is now often the case. Even if old habits are difficult to change, re-education is clearly the answer to this problem.	(background material)	5
DL77	Rec.14 v1979	Conf.Call.2 20/11/2012	Transport documents 8. Some international conventions prescribe signatures on transport contracts. Others, like the CIM for transport by rail, have dropped this requirement, which would seem to indicate that here is no legal need for authentication in such a document, except in instances where a signature is required by national law. The problem can then only be solved by action on the lines mentioned in paragraph 4 above, such as repeal of the legal requirement or the acceptance by the relevant authorities of data produced by electronic or other automatic means. In transport the position is, however, further complicated by the number of parties involved apart from the carriers themselves: exporters, importers, financiers, insurers and authorities. There would also appear to be several functions involved which give rise to demands for signed documents: a) evidence of the contractual undertaking of transport; b) evidence that goods have been accepted for transport; c) evidence of details of the goods transported; and d) evidence that the goods have been received in good condition. As mentioned in paragraph 3 above it is, rather, the verification of the data content conveyed by the signature than the signature per se that is needed, and various alternative methods of meeting this need are described in Part II of the present study. 9. The (negotiable) bill of lading poses a special problem since it constitutes a transport contact which is also a negotiable document of title. This is the classic example of a document which travels and which is of interest to parties other than the originator and the final recipient. There is no immediate, obvious solution to the legal problems involved. The best way to make possible the use of modern methods of data transmission in sea transport is to make the parties consider whether their commercial relations are such that they could replace the bill of lading by a non-negotiable transport document. Experience shows that such documents are an acceptable alternative in many instances.	(background material)	5

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL78	S.Tahir (CH)	Conf.Call.2 20/11/2012	Air-transport documents are able to be sent B2B without any authentication (no signature, no authentication by means of the VPN…). • These documents are generally accepted B2G (by transport authorities and customs officials) in the framework of international agreements		A
DL79	Rec.14 v1979	Conf.Call.2 20/11/2012	Financial documents 10. Requirements for the authentication of financial documents such as letters of credit are outside the scope of this study, although problems could be created by the specific documentary provisions of the credit. The need to verify whether insurance is in force for a particular shipment could, in certain circumstances, lead to the need for a signed document. However, the growing trend for exporters themselves to make out insurance certificates under cover of a general policy and the availability of alternative methods of ensuring that adequate cover exists may lead to a reduction of this particular requirement. As an example, there is a growing tendency on the part of major exporters merely to state that cover has been effected under a blanket arrangement, without any specific document being issued in respect of individual shipments.	(background material)	5

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL80	Rec.14 v1979	Conf.Call.2 20/11/2012	Official documents 11. It would seem that the main need for authentication and acceptance of responsibility to meet official demand occurs at import in the country of final destination. These needs, however, often have a direct bearing on action in the country of purchase at the time of dispatch, or subsequently. Import procedures are usually based on a compulsory form which incorporates a declaration to be made by the importer or his agent, and thereby constitutes a legal undertaking of responsibility. Since this document is created and signed in the country of importation, it does not necessarily in itself constitute an obstacle to international trade facilitation. Moreover, there is a trend towards the speedy removal of goods from the place of importation, under simplified documentation, associated with physical examination of the goods in inland premises when the complete documentation is available. This in itself is a great step forward in Customs facilitation. Nevertheless, the position is often complicated by demands for supporting documents, most of them "documents that travel", such as certificates or invoices. 12. Customs authorities in some countries insist on a signed invoice, in the form of a commercial invoice, a consular invoice or a so-called Customs invoice. Where there is a legal requirement for a signed invoice, the need for such a document can only be overcome by the repeal of the relevant regulation. In other instances, import authorities, who have wide discretionary powers, may themselves educate traders and promote procedures to facilitate trade. The work in the Customs Co-operation Council contributes effectively to this objective. It must be said, however, that clearance procedures are often complex. The Customs authorities must not only be satisfied as to the identity and content of the goods but also as to the relevant economic criteria to be applied. In addition, they are often requested to examine goods to ensure that they meet requirements laid down for a variety of "non-Customs" reasons, such as health or safety. However, as to signatures, it would seem to be perfectly possible to solve the problem by the use of alternative methods.	It has already been established that this is too oriented towards customs procedures and should be opened to all agencies (if this type of organization is maintained) (background material)	5
DL81	Rec.14 v1979	Conf.Call.2 20/11/2012	19 Generally speaking, electronic and other automatic methods provide a highly accurate and reliable means of data transfer. Data can be safeguarded by ensuring that access to the system is limited by the use of, for example, passwords, code words, special badges, or other methods. It is certainly true to say that these systems can provide a degree of reliability for the content of the message which is as good as any traditional documentation. Confidentiality of files is safeguarded by the methods mentioned. Identification of the parties can be assured by means of pre-arranged codes.	(background material)	6
DL82	J.Baiamonte (US)	Conf.Call.2 20/11/2012	A first step is to identify the paper based process for which conversion to electronic signature is sought and to map out the paper process, including associated risks, gaps and any needed improvements	Mapping should probably be discussed in chapter 2. Risks will depend on *levels of confidence* .	6
DL83	J.Baiamonte (US)	Conf.Call.2 20/11/2012	Should provide guidance on issues countries consider when addressing transmission, archiving and retrieval of data.	Governments should create and maintain appropriate legislative frameworks.	6

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL84	J.Baiamonte (US)	Conf.Call.2 20/11/2012	Should establish processes in critical areas of interest which are sufficiently secure to protect the parties' interests in the event of litigation.	This leads back to a notion of *levels of confidence* . The security should be appropriate for the required/desired *level of confidence.*	6
DL85	J.Baiamonte (US)	Conf.Call.2 20/11/2012	Practical steps which take risk assessment as a guiding principle.	A checklist? Where should this be inserted? In Appendix A?	6
DL86	J.Baiamonte (US)	Conf.Call.2 20/11/2012	Establish legislative framework.	Governments should create and maintain appropriate legislative frameworks.	6
DL87	J.Stoopen (NL)	Conf.Call.2 20/11/2012	[Trust framework] Having a clear description of the legal responsibilities of the parties involved	Access to data should be limited to intended parties. See also attribution function of signature in chapter 2.	6
DL88	C.Salomone (IT)	Conf.Call.2 20/11/2012	When necessary, use trusted third party services in order to keep trusted evidence of content and time of transmitted documents or data, for all the time required by law and agreements (notarization)	Trusted 3rd party is identified as a typology in ch.5 and specifically mentioned in archiving.	6
DL89	Rec.14 v1979	Conf.Call.2 20/11/2012	Responsibility for data transmission 20. Apart from the access code mentioned above, the users of a system also require to know the way in which to structure their messages. The conditions of use of a system are often called "protocols". If the user accepts them, he will be bound by the system and could be held responsible for the use he makes of it. The acceptance of the conditions of use of the system could be made in a properly-signed agreement between the parties, in which case the proof before a Court of the transmission made in conformity with the agreement would acquire the validity of duly signed documents. The system would have to identify each user in an irrefutable manner. Where necessary, it would also have to serve as proof of disputed identity of the source of the message; the guarantee which it offers would need to be capable of verification by a court or by an expert designated for this purpose. It is possible that a computer log or inventory, which could be verified to confirm its reliability, held by the system and listing reference proper to each message and to its source, would serve the purpose. If the log recorded the full content of all messages handled by the system, security would be enhanced, but this could be expensive and it might not be necessary in every-day routine transactions. 21. A guaranteed and verifiable identification procedure, together with a signed protocol, could provide proof in a Court of Law which would be of as much value as a signature. It is not possible to ensure complete protection against fraudulent intentions, but it may well be easier to forge a signature than to falsify the identity of the source of a message in a well-designed computer system. However, the evidence held in the computer records would need to be retained in case it were required for use in court proceedings. Recent national data laws have a bearing on the retention period, but in practice a period of five years would seem to be sufficient for this purpose.	(background material)	6

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL90	J.Stoopen (NL)	Conf.Call.2 20/11/2012	[Trust framework] Agreement on the use of certain standards accepted and trusted by parties involved (service providers, business, government, public)	Appendix B to be split into 'Official international standards' and a repository of actual implementations (instead of mixing the two together) See also chapter 6, transmission: "In bilateral exchange, the two parties should explicitly agree on the method of communication and the method of authentication."	6
DL91	J.Stoopen (NL)	Conf.Call.2 20/11/2012	[Trust framework] Agreement on monitoring the trusted framework (new parties access, parties leaving the framework, operations under the framework etc.)	This will depend on the level of assurance. Chapter 6 forsees: "Access to data should be limited to intended parties." and "Depending on the level of assurance required, trusted 3rd parties should guarantee the corresponding level of confidence."	6
DL92	J.Stoopen (NL)	Conf.Call.2 20/11/2012	[Trust framework] Guaranteeing interoperability.	Minimal requirements for data transmission are presented in AnnexB with the appropriate technological solutions.	6
DL93	J.Baiamonte (US)	Conf.Call.2 20/11/2012	In terms of “transmission”, what must be demonstrated is a secure electronic process in terms of identifying (This chapter should also provide recommendations that would fit under each of the enumerated best practices)	Minimal requirements for data transmission are presented in AnnexB with the appropriate technological solutions.	6
DL93	J.Baiamonte (US)	Conf.Call.2 20/11/2012	1) “when” (i.e., date/time) the communication or transaction was sent or initiated; 2) the identity/location of the specific party who transmitted the information (this means an identifier traceable to both the person and the source of the transmission) 3) receipt of the communication, by whom it was received and when; 4) what the sender of the communication intended by it, and the date and time he or she signed it and 5) the complete contents of the communication, including any attachments; 6) proof that the information in the transmission was not altered (e.g., the electronic process includes a design to provide an audit trail); 7) some means of version control; 8) where applicable, proof that the individual has certified “to the truth and accuracy of the information submitted”; 9) any controlling statutes/regulations that impose record retention requirements. To that end, any electronic record must be a) retrievable in a form that can be viewed or printed (this means even if the agency later modifies its electronic process or if the document was originally encrypted or restricted by password); b) indexed in a manner sufficient to be able to retrieve needed data; and c) retained/retrievable in an electronic recordkeeping system for the length of time required by law/policy, etc.	Minimal requirements for data transmission are presented in AnnexB with the appropriate technological solutions.	6

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL94	S. Lennartsson (SE)	Conf.Call.2 20/11/2012	Beware of third-party intermediary rights (justified or unjustified) which allow for reading the information contained in the document in order to convert between formats for example…	Depending on the level of assurance required, trusted thrid parties should guarantee the corrseponding levels of assurance.	6
DL95	C.Salomone (IT)	Conf.Call.2 20/11/2012	Transmission networks and environments must ensure the identity of all the parties involved, and non repudiation of sending and receiving the data or documents transmitted	Minimal requirements for data transmission are presented in Annex B with the appropriate technological solutions.	6
DL96	C.Salomone (IT)	Conf.Call.2 20/11/2012	Archiving procedures must preserve the capability of retrieving data during all the archiving time span, keeping available the original technology and/or means used, or its functional equivalent, regardless of its commercial availability The same requirement of technology maintenance applies to credential and processing rules (algorithms), regardless of the availability of the hardware and software originally used	The technology used must be maintained during the entire period (or functional equivalent) ; OR must plan for the migration from one technology to another.	6
DL97	SP.Sahu (WCO)	Conf.Call.2 20/11/2012	Are we assuming that there is a signed document/contract between the parties for electronic authentication? (SP, WCO)	The parties should consider the level of assurance required when establishing this agreement. - depending on the necessary level, there may or may not be a signed contract between them. For the moment, there is no precision in the outline on this subject.	5
DL98	S.Tahir (CH)	Conf.Call.2 20/11/2012	In the paper world today, when not preprinted, the signature of the shipper or his agent (printed, signed or stamped) shall be inserted on the air waybill as per IATA CSC Resolution 600a. Air-transport documents are able to be sent electronically and authenticated through EDI addressing e.g. teletype addresses, PIMA, CCS (no signature, no authentication by means of the VPN…). On the business side, messages are authenticated by including for example the Shipper/Agent and Carrier/Agent name, place and date such as Air Waybill, Shippers Declaration for Dangerous Goods. These documents are generally accepted B2G (by transport authorities and customs officials) in the framework of international agreements. We believe this is sufficient and by making the digital signature mandatory may impede the adoption of e-commerce in the air transport industry. We support the UNCITRAL, Model Law on electronic signature, part 2 §13 where authentication can be based on the knowledge of the user or the recipient (e.g. passwords, personal identification numbers (PINs)) and UNCITRAL, Promoting Confidence, p.30 §66 where we must not create stringent requirements which would put in doubt the validity and enforceability of these transactions.	Rec14 remains technology neutral (chapter 5); multiple examples are given of other means of authentication. The IATA experience and examples would be very useful in the Respository of implementations.	B

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL99	Y.Lee (KR)	10/12/2012	Transmission history for sending and receiving messages should be managed for non-repudiation. The data to be transmitted should be packaged by the message structure defined in the transmission protocol. The message received should be validated, parsed, and extracted by the message structure defined in the transmission protocol. If a transmitter has fault in the process of message transmission, there should be an intermediator which could send the message in replace of the transmitter.	Requirements for transmission will depend on the method of authentication. Specific minimal requirements can be discussed in the Repository of implementations in Annex B.	B
DL100	Y.Lee (KR)	10/12/2012	Transmission A mechanism that trust and identify credibly the transmission party is required: certified e-address which is managed by an agency with legal authority. Current e-mail address cannot be trusted. A mechanism that prove legally sending/receiving message by a party is required. The mechanism should be based on the e-signature technology.	Identification function is an aspect of all signatures. This is considered in chapter 2 on a variable scale. The description in this comment is of the highest level. Such requirements will depend on the levels of assurance based on risk assessment of the process (trade document) and the legal constraints. Specific minimal requirements can be discussed in the Repository of implementation in Annex B.	B
DL101	Y.Lee (KR)	10/12/2012	Archiving. For the legal admissibility, the message transmitted or certificate for proving transmission could be archived in a third party repository. The archived message and certificate could be retrieved by a party which has permission.	Possible use of third-party archiving solution which take into consideration the above points.	6
DL102	Y.Lee (KR)	10/12/2012	Archival and Retrieve A message transmitted could be archived in 3rd party repository for legal admissibility. For proving that there are no changes after archiving the message, the message should be freeze at archiving time with the certificate of the 3rd party repository. When the message is retrieved, the history of retrieve should be recorded and a certificate which is legal document for proving the retrieval should be issued by the 3rd party repository.	Will depend on the level of confidence	6

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL103	Y.Lee (KR)	10/12/2012	For the reliability and authenticity of e-documents circulated, e-document circulation system should satisfy the following requirements: - Transmit entity and receipt entity circulating the e-document should send and receive the e-document by an agreed protocol. They should also contract the SLA (Service Level Agreement) of a management agency or an e-document intermediator. - The transmit entity and receipt entity circulating the e-document should be identifiable, and they should be prevented of denial of sent or received e-documents. - E-address for identifying the transmit entity and receipt entity should be certified publicly by a trusted registration agency for credibility. - If a transmit entity and a receipt entity circulate an e-document in the e-document circulation system, they should make a circulation certificate which should be stored their transmission system or third party e-document repository system. - All the e-document circulation is basically P2P (Peer to Peer) oriented, but there should be the other communication methods supportive. - In the e-document circulation system, besides the e-document exchange, additional services such as e-document perusal should be provided.	These types of requirements will depend on the method of authentication. Specific minimal requirements can be discussed in the Repository of implementations in Annex B.	B
DL104	Y.Lee (KR)	10/12/2012	TECF (Trustworthy e-document circulation framework) enables e-document circulation reliably and safely based on the certified e-address. Individual, company, or organization can send/receive e-documents to/from credible partners identified by certified e-address. TECF also enables to prove if the e-documents are transmitted without problem by circulation certificate, so that TECF provides the legal admissibility for e-document transmitted	This will be a valuable contribution for the Annex B Repository of implementations. The finalized submission letter is presently being finalized.	B
DL105	Y.Lee (KR)	10/12/2012	For making a certificate which prove transmitting a message, e-signature technology can be used.	Confirmation of sending / confirmation of receipt of the transmission is planned in Chapter 6.	6
DL106	L.Fratini Passi (IT)	07/12/2012	Financial Documents SWIFT has developed an interbanking system of digital signature for financial worldwide transactions which is a “bank signature”, and replaced previous authentication interbank keys. This solution has recently evolved to a “personal” PKCS7 digital signature and is named 3SKey, becoming a product for large corporates.		B
DL107	L.Thompson (FR)	Conf Call3 ch6 10/12/2012	In a bilateral exchange, the two parties should explicitly agree on the method of communication and the method of authentication. --> They should consider the level of confidence required when establishing this agreement.	Chapter 6, transmission: "In bilateral exchange, the two parties should explicitly agree on the method of communication and the method of authentication."	6
DL108	A.Caccia (IT)	Conf Call3 ch6 10/12/2012	Annex B should not mix together Standards (ISO or other) and actual implementations.	Suggestion to make Annex B on available standards and accompanied by a Repository of implementations.	B

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL109	L.Thompson (FR)	Conf Call3 ch6 10/12/2012	Levels of confidence or a similar concept will need to be presented in order to make recommendation readable.	levels of assurance - chapter 5	5
DL110	L.Thompson (FR)	Conf Call3 ch6 10/12/2012	Archiving method must correspond to at least an equivalent *level of confidence* as the authentication/signature method used	Chapter 6 "Archiving method must correspond to at least an equivalent level of assurance as the authentication / signature method used.	6
DL111	P.Prianceu (IN) A.Caccia (IT) A.Norden (SE)	Conf Call3 ch6 10/12/2012	The method of archiving should be auditable (checking the reliability – whether it works or not; checking correctness of retrieved data, readability [format used]; & encompassing the functional aspects of a authentication which is being accepted between the parties …)	approved	6
DL112	Y.Lee (KR)	Conf Call3 ch6 10/12/2012	Only authorized parties should be able to retrieve the data.	Integrated into chapter 6.	6
DL113	J.Baiamonte (US) A.Norden (SE)	Conf Call3 ch6 10/12/2012	For B2G transactions, government should clearly explain the level of confidence required (via laws, guidelines or other…)	recognized	6
DL114	L.Thompson (FR)	Conf Call3 ch6 10/12/2012	These legislative frameworks should be reviewed regularly (5 years?) in order to correspond to actual business practices	Chapter 4 Creation of legal framework. Idea of regular review was acknowledged, but a period of review would be difficult to define here as the legal process does not always lend itself for such regular upgrades.	4
DL115	J.Baiamonte (US)	Conf Call3 ch6 10/12/2012	These frameworks should ensure the acceptability in court of transmission methods, archiving processes, etc	approved	6
DL116	Y.Lee (KR)	Conf Call3 ch6 10/12/2012	In Korea, we need a credible e-address for identifying trusted transmitter and receiver. So, now our government side is making a low that enforce the credible e-address to some important area.	This will be a valuable contribution to Annex A of legally enabling environments	A
DL117	P.Prianceu (IN) A.Norden (SE)	Conf Call3 ch6 10/12/2012	Should privacy aspects be addressed in this recommendation?	Access to data should be limited to intended parties	6

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL118	C.Praliaud	13/12/2012	French Civil Law definition of signature (article 1316-4): The signature necessary for completion of a legally-binding act identifies the person. The signatory's (ies') consent to the obligations within the signed document is thus demonstrated. When the signature is made by a public representative, it attest to the authenticity of the act. When it is in electronic form, it consists in the use of a reliable identification process which guarantees the link to the corresponding document. When the electronic signature is created, the identity of the signatory established and the integrity of the signed document guaranteed within the conditions outlined in State Council Laws, the process is presumed reliable until proven otherwise. *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.* *Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.*	Evidentiary function (consent); authenticity will be determined by the mix of the three functions (identification, evidentiary, attribution).	2
DL119	S.Mason	23/11/2012	The purpose of a signature What is meant by a signature The functions of a signature The primary evidential function Secondary evidential functions Cautionary function Protective function Channelling function Record keeping function Disputing a manuscript signature Defences The format of the signature	without further details from the submitter on these chapter headings, it is impossible to consider them seriously,	2
DL120	J.Stoopen (NL)	12/12/2012	I think that it is important to limit the input via this Annex to official documents to be used for formalities between business and government and official documents to be used between business – business. What I try to avoid is that we at the end of the day get a lot of input on e-signatures/e-identity for communication between private persons and government. I know that such examples can provide us a lot of useful information as well, but I am convinced that a more specific request will have more added value when drafting the recommendation	It will be difficult to draw the line as to what has 'official' use and what does not. Most submissions will probably be for the target expressed in this comment; we should perhaps come back to this point if there are many comments outside of this.	A

N°	Proposer	date	Proposed change	Action taken	Relevant chapter
DL121	Quebec Law L.Castellani	13/12/2012	« 39. Quel que soit le support du document, la signature d'une personne peut servir à l'établissement d'un lien entre elle et un document. La signature peut être apposée au document au moyen de tout procédé qui permet de satisfaire aux exigences de l'article 2827 du Code civil. « La signature d'une personne apposée à un document technologique lui est opposable lorsqu'il s'agit d'un document dont l'intégrité est assurée et qu'au moment de la signature et depuis, le lien entre la signature et le document est maintenu. »	Idea of link between a person and a document is retained as a good starting point for the definition of a signature.	4