Recommendation 14 Revision Working Group

Survey on definitions and levels – Consolidation of responses as of 01 Feb 2013

For reference, all relevant documents are on the Confluence website:
http://www1.unece.org/cefact/platform/display/CNP/Revision+of+Recommendation+14%2C+Authentication+of+Trade+Documents+by+Means+other+than+Signature

Point for discussion: LEVELS OF *ASSURANCE* / CONFIDENCE …?

When considering the alternative electronic authentication methods, a risk assessment is performed. Based on this, the method should be chosen. The choice should not systematically be towards the 'most secure' method, but **correspond to the needs of the transaction and the business partners**. In order to illustrate this, we have been speaking of **LEVELS**. (256-286 which also references other parts of the draft such as 185-254)
ISO 29115 presents **levels of assurance** for entity authentication. However our present work (Rec14) is on document authentication. It is not certain that the ISO 29115 model can be used as-is in Rec14.
Could you please indicate your feeling on this?

NL-(JS)
I have my doubts whether we should use the ISO 29115 in Rec14. As a reference or example it can be taken on board. If we want t to use ISO 29115 in Rec14, it is only useful if we copy in substantial parts of it (e.g. Chapter 6 about the levels of assurance).

IT-(RM)
For a Trading Partners to authenticate a document they must be identified and provided with credentials. So in our recommendation we can't ignore the concept of identity and whether the identity is "strong" or "weak" or "strong enough" for a particular transaction.
In my humble opinion, referring to ISO 29115 clearly, help to get away from vague assurance of quality.

FR-(CP)
For me we should talk about security level.
This level of security is based on the document, the importance of this document, the risks associated with this document.
ISO 29115 does not really seem appropriate

CH-(JK)
I think it is better to keep distinct the levels of assurance for entity authentication with the levels of assurance for document authentication. They serve a different purpose.

SE-(AN)
We agree that the ISO model is likely inappropriate to use as is.

US-(NH)
Lance, I am not familiar with ISO29115 and don't think I could become proficient enough before the next meeting, but it does seem to me to be quite a difference between entity authentication and document authentication, therefore if this difference is not outlined and or addressed in ISO29115, I don't think it should be used.

SE-(AT)
I think that this summary of the discussion is very accurate and to the point.
I was confused by all the possible levels (LEVELS OF ASSURANCE / CONFIDENCE …?) and as I work with eSignatures I incorrectly assumed that this was = LoA (ISO 29115). But, the task at hand is to revise Rec14 which is "AUTHENTICATION OF TRADE DOCUMENTS BY MEANS OTHER THAN SIGNATURE" and nothing else.

Please return on or before January 31st, 2013 to lance.thompson@conex.net

So I have a gut feeling that we are talking about "levels" of "Authenticated trade documents" – and this is very different from LoA (ISO 29115). I therefore propose that LoA = Levels of Assurance **is not used** as you correctly conclude above as this would create confusion.

AT-(PK)
We would regard ISO 29115 as less applicable and not really adequate. It might confuse, if mixing between authentication in online processes (what 29115 is mainly addressing) and eDocuments.

ES-(CL)
There are differences between entity and document authentication that the REC14 should face:
Document authentication: Authenticity is a property of the electronic document that informs on:

- It's full, so there has not been amended without the knowledge of the author or recipient.
- It comes from an identified and recognized source (entity authenticaion)
- The document is attributable to the person as an author or another function also known as concrete.

IN-(PR)
In the cross-border scenario, level of assurance based entity authentication may not be sufficient. Only entity authentication may reduce the available option in the different typologies of electronic equivalents. Since present work requires both entity & document level confidence, I think, we should add one more level to ISO 29115

Assurance level	Entity	Resource/document
Low	Little or no confidence in the claimed or asserted identity	Little or no confidence in the authenticity of the content.
Medium	Some confidence in the claimed or asserted identity	Some confidence in the authenticity of the content and/or the commitment of the signatory.
High	Veracity of the claimed or asserted identity proven	High level of authenticity of the content and of the commitment of the signatory.
Very High	Veracity of the claimed or asserted identity proven and witnessed by a verifying organism	Very high authenticity of the content, of the commitment and any changes in the document can be detected after it was signed

Assurance is *what we provide through* and confidence is *something we get*. There may be some gap. The risk analysis and audit trail will determine the actual assurance. If we wish to go with lower side we can choose "confidence". However, if we prefer to have minimum deviation with ISO, we should choose "Assurance".
I prefer Assurance over Confidence

US-(TS)
My sense is that ISO 29115 may be relevant to determining the level of confidence in the identity of the signer of a trade document, but not to the authentication (or signature) of the trade document itself. It feels like we are mixing up two different (although related) concepts which happen to use the same word ("authentication"). ISO 29115 defines authentication as the "Process of corroborating an identity or attribute with a specified or understood level of assurance." (emphasis added). My sense is that much more is required for document authentication in this case – e.g., identity, intent, and integrity.

What **wording** should be used to describe these levels? (levels of assurance, levels of assessment,

levels of confidence, confidence continuum…)

NL-(JS)
I suggest to use the wording: level of assurance . That covers it all. By assessing the risks you are able to create a level of assurance.

IT-(RM)
In my opinion, defined a transaction context ,what we are suggesting is to conduct a risk assessment then define the appropriate Level of assurance required by the transaction (as described in 284 …) and then select the technology strong enough for that Level of Assurance.
The wording "Level of assurance" as defined in ISO and used in Risk assessment process is the better choice because bears the meaning of the level of confidence that an electronic data in a document represent s the real-world identity it purports to.

FR-(CP)
I can propose : Security levels.

CH-(JK)
Levels of assurance, i.e. having the same wording as in ISO 29115, seems to me the best option, highlighting a commonality in the methodology and thus easier understanding.

SE-(AN)
Level of assurance is good.

US-(NH)
I think level of security , or simply security type would best describe. I.e., type A would be documents that require the highest security

SE-(AT)
What we want to elaborate on in the Rec14 is different levels of authenticated trade documents. These levels could for example be documents authenticated with:

- An electronic signature
- An interchange agreement (Odette, etc.)
- An electronic seal
- Etc.

I think that this perhaps is = "**Means of Authentication**"? When using the word "levels" we have to say that one is higher and one is lower. This is very difficult as what is used is very dependent on business requirements and one might not be lower than another.

AT-(PK)
It might be called levels of assurance. The matrix-like approach together with the technical considerations and technologies in 297 ff. seem to significantly increase complexity compared to limiting to a few levels.

ES-(CL)
Levels of assurance or trust levels

IN-(PR)
As mentioned above, Level of assurance if required to have conformity with ISO, otherwise level of confidence

US-(TS)
I'm not sure that formalizing the concept of "levels" of assurance/confidence etc. is what we want to do here, as this may require that we get down to the level of defining specific requirements for each "level"

Should we reference within Rec14 (on document authentication) the ISO recommendation 29115 (levels of assurance as it pertains to entity authentication) in this domain?
If so, where and how? Please be specific as to any points which will need to be reworded or changed.

NL-(JS)
No specific preference, but it seems obvious. My opinion is that incorporating Chapter 6 in this Rec14 is simply too much. I also am not sure you can copy and paste certain parts from ISO 29115 and forget about the rest (you will lose the text coherency . Instead of rewording or rewriting the text from ISO 29115 we better look for alternatives that better fit in Rec 14. We can always make a reference to ISO 29115 as an example of best practice.

IT-(RM)
It looks like we already did. The first column in table (line 285) has almost the same wording. We'd map the ISO recommendation here.

CH-(JK)
We should reference, possibly in a footnote, to highlight both the similarity in the methodology, as well as the differences (document versus entity authentication) for clarity purpose, when introducing the levels of assurance for document authentication.

SE-(AN)
No

US-(NH)
n/c from me

SE-(AT)
I think that ISO 29115 only should be mentioned in the context of authenticating electronic signatories.

AT-(PK)
We would not suggest to quote 29115, as it focuses on entity authentication and as we do also have problems with the ISA 29115 content-wise.

ES-(CL)
Yes I think it is a very interesting reference and it gives soundness to the Rec/14
Maybe a new section called "Definitions"?
It also could fit at 2b. Authenticity, merging it with 2e. Document Authenticity

IN-(PR)
I think we should not. If any change in the ISO 29115 or a new version, in respect of level of assurance, may invalidate this document. **This document should be self-contained even though we adopt or enhance the text mentioned in the ISO 29115**

US-(TS)

As noted above, I'm not sure that formalizing the concept of "levels" of assurance/confidence etc. is what we want to do here. While it deserves more thought, my initial sense is not to reference ISO 29115.

It has been discussed that these levels or this continuum should be considered as a matrix (see lines 271-286). Do you agree?
If so, what should be the values that should be considered to create this matrix?

NL-(JS)
Looking at the matrix I have my doubts about the added value. Without specific references to criteria which lead to the valuation low-medium-high, it is very difficult to understand and appreciate what is in the matrix. If we need a matrix like this we might as well look at ISO 29115.

IT-(RM)
Yes, a matrix is of better comprehension.

FR-(CP)
YES completely
I propose : Security levels.

CH-(JK)
3 to 4 values should suffice (very high, high, medium, low). These levels should be more precisely defined with examples for each.

SE-(AN)
A matrix could be used to exemplify different levels, but in reality it will be a sliding scale.

US-(NH)
I do agree with a matrix.

a) Do we need to state what the signatory roles can be? Ie.,low= anyone in employment, medium =anyone in a management position, high=any officer of the company, very high=only CEO or chairman?

I think the wording should be changed to little or no NEED FOR confidence, as opposed to little or no confidence. I may have very high confidence but this particular document does not require such level.

SE-(AT)
I think that a matrix like this is very dangerous as any conclusions must have a national legal base. It also uses the low, medium, etc. from ISO 29115 which are very general. If it on the other hand would be a matrix of MoA = "Means of Authentication" (people just love abbreviations and this is not used in this context what I know of, so I think we can use it) the entries would be different. What you perhaps want to evaluate in a possible matrix is things as pre-arranged agreements, technical compatibility, how to evaluate a signature, etc.

AT-(PK)
As indicated above, it seems adding complexity:
For the higher levels, legal certainty is given in an increasing number of states. Technologies exist including assessment methods. The added value of an additional classification scheme isn't seen. For lower levels with low assurance, undergoing lengthy risk assessment and signature token classification might hinder take-up (the assets at stake obviously are low-value anyhow).

ES-(CL)
Columns: Trust levels

Recommendation 14 Revision Working Group

Survey on definitions and levels – Consolidation of responses as of 01 Feb 2013

Rows: types of authentication
From this matrix one can define the overall level as the highest of the matrix
Another matrix:
Columns: Overall trust levels
Rows: list of trade documents / transactions

IN-(PR)

I feel the main document should be a high level specification and the implementation details should available in the annexure.

It is better to specify the values to enhance the interoperability and also to remove ambiguity .

Recommendation 14 Revision Working Group

Survey on definitions and levels – Consolidation of responses as of 01 Feb 2013

For reference, all relevant documents are on the Confluence website:
http://www1.unece.org/cefact/platform/display/CNP/Revision+of+Recommendation+14%2C+Authentication+of+Trade+Documents+by+Means+other+than+Signature

Point for discussion: DEFINITIONS

FI-(LR)

"Review of definitions of "Writing", "Signature" and "Document" employed in multinational conventions and agreements relating to international trade, submitted by the Legal Working Group (LWG), Revision of Document Trade/WP.4/R.1096 dated 22 July 1994; TRADE/CEFACT) Geneva, October 2001, ECE/TRADE/240."

US-(BL)

here is a link to UNCITRAL Working Paper 94 that lists and comments on a number of international agreements:
A/CN.9/WG.IV/WP.94 - Legal barriers to the development of electronic commerce in international instruments relating to international trade
It was prepared for the March 2002 session of Working Group IV - Electronic Commerce (I was involved in developing this.) All of the Working Papers and other materials from Working Group IV are located at
http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html

US-(TS)

General Comment: As I have missed several calls, my comments may reflect an ignorance of the prior discussions and the intent of the project. My general sense, however, is that the 0.4 draft document seems to confuse the terms authentication, authenticity, and signature. In some cases it talks about "authentication" as if it is synonymous with "signature" and in other cases it treats "authentication" in the more traditional sense as the process of establishing or confirming that something is what it purports to be. At its essence, however, the document seems to be focused on a discussion of how to select the appropriate form of electronic signature for a given trade document. If that is indeed the intent perhaps that could be clarified.

DE-(KR)

Given all the discussions around identification and identity you may be interested in consulting another WG 5 standard:
ISO/IEC 24760-1:2011 Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts
It is even freely available on
http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

In the context of the v0.4 of the draft, is the **definition of authentication** sufficient (line 118-121)? (Y/N) If no, could you please provide either an alternative definition or propose further elements which should be considered?

NL-(JS)

I suggest to delete : legally accepted context because it is the same as legal value. In this definition legal value covers it all.

FI-(JS)

Yes

IT-(RM)

Yes the definition is correct as a general statement but in the context we are in (electronic data transfer) a better definition could be:
Authentication is the electronic process that allow the validation of the origin and integrity of electronic data.

FR-(CP)
Yes

SE-(AN)
I think it's vague to refer to "legal value". Is it not rather that a document meets certain requirements by law (which means that is has "legal value" in that context)?

US-(NH)
I believe so

AT-(PK)
Authentication should rather be described as the corroboration of the origin of data.

ES-(CL)
I would feel more comfortable with an existing and widely accepted definition such as (RFC 4949):
"The process of verifying a claim that a system entity or system resource has a certain attribute value»
(NOTE: "system" understood in broad sense).
« Tutorial: Security services frequently depend on authentication of the identity of users, but authentication may involve any type of attribute that is recognized by a system. A claim may be made by a subject about itself (e.g., at login, a user typically asserts its identity) or a claim may be made on behalf of a subject or object by some other system entity (e.g., a user may claim that a data object originates from a specific source, or that a data object is classified at a specific security level).

An authentication process consists of two basic steps:

- Identification step: Presenting the claimed attribute value (e.g., a user identifier) to the authentication subsystem.
- Verification step: Presenting or generating authentication information (e.g., a value signed with a private key) that acts as evidence to prove the binding between the attribute and that for which it is claimed. (See: verification.) »

NIST Special Publication 800-63 Version 1.0.2:
"Authentication simply establishes identity, or in some cases verified personal attributes (for example the subscriber is a US Citizen, is a student at a particular university, or is assigned a particular number or code by an agency or organization), not what that identity is authorized to do or what access privileges he or she has; this is a separate decision."

IN-(PR)
I feel, we also may have to make modification in the definition of Authentication in the context of present work. Also It is appropriate not to have contradicting definition in two international work on same topic. ***Authentication*** mentioned in the ISO can be referred as **entity authentication** .The document authentication should also be defined .
Every mention of authentication in this document should be prefixed with "entity" or " document"
The definition drafted for the purpose of this document is given below. Some/part may be useful.
Identity refers to *the whole* of the characteristics of a resource that uniquely identify and distinguish from any other resource

integrity refers to the resource is untampered with, uncorrupted and complete in all its essential respects after the act of signature is carried out.
Authenticity is the status of being dependable in regard to evidence of identity and integrity in accordance with the agreed level of assurance.
Authenticity is an auditable process that ensures an agreed level of quality in the results by maintaining evidence of the identity and/or integrity of resource in accordance with the agreed level of assurance.
(1)Resource(document) authentications is the activity that provides means for demonstration the authenticity of resource in accordance with the agreed level of assurance.
(2) Resource(document) authentications is the process of establishing confidence in the authenticity of resource in accordance with the agreed level of assurance
Entity Authentication : The process of establishing confidence in user identities or typologies in accordance with the agreed level of assurance
Authentication is the act of performing resource authentication and entity authentication.

US-(TS)
My sense is that a different word is needed here, as what is being described seems to be signing. From my perspective, ***authentication*** typically refers to **the process of establishing or confirming that something is what it purports to be (or in the case of a person, the process of establishing or confirming that someone is who they claim to be)**. And that is the sense in which the term "authenticity" seems to be defined in lines 180-183. It seems as though the term authentication is being used for a different purpose here – more like the term "signing" than authentication (although sometimes those two terms are used synonymously).

In the case of a trade document, authentication of the document would seem to include the processes required to establish both (1) that the signature on the document is genuine and made by a specific authorized person with the intent to sign the document and (2) that the contents of the document have not been altered since it was signed.

Thus, use of the term "authentication" in lines 118-121 seems somewhat confusing. Is it possible that what is intended to be covered by lines 118-121 might be better described as "signing"?

RU-(AS)
1.3
The same problems take place with definition of *authentication* in section 2.
"Authentication can be considered here as the act of giving a legally accepted context or a legal value to a trade document. For example, an order form which is filled out may not have a legal value unless it has been authenticated (signed by the requester)."
The definition above concerns not *authentication*, but *legal significance*. *Legal significance* may be a consequence (a result) of a successful *authentication* (and other necessary factors). But *Legal significance* is not *authentication* on its own.
Thereby, successful *authentication* (along with other factors) can be only one of the necessary conditions or prerequisites of *legal significance*. That is why terms *authentication* and *legal significance* shall be separated.
OR ALTERNATIVELY SECOND APPROACH:
Authentication – a process of verification of authenticity in a trusted way.
Note:
The *entity* can be a document, a record, an identifier etc.
In *trusted* way means undoubted acceptance (for a given application) of process mechanisms and results. It is achieved by some legal, organizational and technological infrastructure implementing.
Undoubted acceptance depends on a concrete application: a trusted way, being acceptable for one

application, may be not acceptable for other application. It is a matter of the Operational Policy of an application, which way is considered as *trusted*.

In the context of the v0.4 of the draft, is the **definition of a signature** sufficient (line 124-137)? (Y/N) If no, could you please provide either an alternative definition or propose further elements which should be considered?

NL-(JS)
Yes

FI-(JS)
Yes

IT-(RM)
Yes as a general statement

FR-(CP)
Yes

SE-(AN)
OK

US-(NH)
I believe so

AT-(PK)
Seems too explanatory. Is a definition of "signature" needed at all? The document is on "…. Means Other Than (a Manual-Ink) Signature", i.e. electronic signature – which anyhow si well defined.

ES-(CL)
Yes

IN-(PR)

- It is difficult to establish a signing model that correspond with what occurs in the paper-based environment. The verification mechanism exists in the electronic signature cannot be seen in the paper-based environment
- achieving functional equivalence, which means that, as far as possible, paper based commerce and electronic commerce should be treated equally by the law.
- I think, the word "electronic equivalent" is not sufficient for electronic signature

Attempt -1 def of signature
A signature is a traditional ink signature or its functional equivalent in the electronic world that associate with document by a signatory or authority of signatory to verify the genuineness of the document

US-(TS)
I agree that a signature can be manual or electronic. And I also agree that it creates a link between a person and a document. But I disagree with the statement that "This link can be considered having three inherent functions: an identification function, an evidentiary function and an attribution function." See my comments in the next section regarding the functions of a signature.

Rather, I would stress that a signature, whether electronic or on paper, is the means by which a person indicates an intent to associate himself with a document in a manner that has legal significance (e.g., to adopt or approve a specific statement regarding, or reason for signing, a

document). It constitutes legally-binding evidence of the signer's intention with regard to a document. See Article 9(3) of the UN Convention on the Use of Electronic Communications in International Contracts, which says that signature requirement is met when "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."

The indication of a party's intention – i.e., the reason for signing a document -- will vary with the transaction, and in most cases can be determined only by examining the context in which the signature was made. Generally, however, a person's reason for signing a document falls into one of the following categories:

- Approving, assenting to, or agreeing to the information in the document or record signed (e.g., agreeing to the terms of a contract or inter-agency memorandum);
- Certifying or affirming the accuracy of the information stated in the document or record signed (e.g., certifying that the statements in one's tax return are true and correct);
- Acknowledging access to or receipt of information set forth in the document or record signed (e.g., acknowledging receipt of a disclosure document);
- Witnessing the signature or other act of another (e.g., notarization); or
- Certifying the source of the information in the document or record signed (e.g., certifying data in a clinical trial record, certifying an inventory count, etc.)

Thus, a signature is used to provide evidence of a person's intent to approve or adopt a statement in, or reason for signing, a document in a legally binding way.

In the context of the v0.4 of the draft, are the **functions of a signature** sufficient (line 139-173)? (Y/N) If no, could you please provide either an alternative functions or propose further elements which should be considered?

NL-(JS)
Yes, it is important to link to already existing views on the functions of a signature. What is written here links to already existing legislation and documentation in the area of electronic signatures.

FI-(JS)
Yes

IT-(RM)
Yes as a general statement

FR-(CP)
Yes

SE-(AN)
AN: Is the identification function not to establish the origin of the document, i.e. the signatory or originator, rather than the "content". Can the content be identified? Is that not a matter of establishing the "integrity" of the content in that case, i.e. that the content has not been subsequently changed?

ES-(CL)
Yes, but I would also consider the signature functions outlined in CWA 14365-1 (Identification, authentication, declaration of knowledge, declaration of will) since they seem to me more canonical

IN-(PR)
Attribution functions of a signature.

1) An electronic record or electronic signature is attributable to a signatory if it was the act of the person authorized by that signatory or programmed by, or on behalf of, the that signatory to operate automatically
2) Establish a link between the signatory or authorized by the signatory and the document which is signed
3) To ascertain whether the signature was that of the signatory,
   apply a procedure previously agreed to by the signatory or signature framework for that purpose OR

signatory or any other agent provide access to gain the method used by the signatory to identify signature as its own.

US-(TS)
I agree that a signature can be manual or electronic. And I also agree that it creates a link between a person and a document. But I disagree with the statement that "This link can be considered having three inherent functions: an identification function, an evidentiary function and an attribution function." See my comments in the next section regarding the functions of a signature.

Rather, I would stress that a signature, whether electronic or on paper, is the means by which a person indicates an intent to associate himself with a document in a manner that has legal significance (e.g., to adopt or approve a specific statement regarding, or reason for signing, a document). It constitutes legally-binding evidence of the signer's intention with regard to a document. See Article 9(3) of the UN Convention on the Use of Electronic Communications in International Contracts, which says that signature requirement is met when "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."

The indication of a party's intention – i.e., the reason for signing a document -- will vary with the transaction, and in most cases can be determined only by examining the context in which the signature was made. Generally, however, a person's reason for signing a document falls into one of the following categories:

- Approving, assenting to, or agreeing to the information in the document or record signed (e.g., agreeing to the terms of a contract or inter-agency memorandum);
- Certifying or affirming the accuracy of the information stated in the document or record signed (e.g., certifying that the statements in one's tax return are true and correct);
- Acknowledging access to or receipt of information set forth in the document or record signed (e.g., acknowledging receipt of a disclosure document);
- Witnessing the signature or other act of another (e.g., notarization); or
- Certifying the source of the information in the document or record signed (e.g., certifying data in a clinical trial record, certifying an inventory count, etc.)

Thus, a signature is used to provide evidence of a person's intent to approve or adopt a statement in, or reason for signing, a document in a legally binding way.

In the context of the v0.4 of the draft, is the **definition of authenticity** sufficient (line 174-183)? (Y/N) If no, could you please provide either an alternative definition or propose further elements which should be considered?

NL-(JS)
Yes, in relation with the previous paragraph about functions of a signature, it is perfectly clear what we mean to say with "authenticity".

FI-(JS)
Yes

IT-(RM)
Yes as a general statement

FR-(CP)
Yes

SE-(AN)
OK

US-(NH)
Yes, but you must have 2A inorder to have 2B. does an authentic signature on a document that isn't authentic still make it binding?

ES-(CL)
Yes

IN-(PR)
Authenticity is the property of being genuine and able to be verified and trusted.
I think the above text given in the document is perfect.
Some alternate text is given below
The trustworthiness of a resource to be what it purports to be, untampered with and uncorrupted
Authenticity is concerned with control over the information/document/record creation process and custody.

US-(TS)
I'm not sure I would equate "authenticity" with "original," although the rest of the definition in lines 180-183 seems OK.

Also, as noted above, the reference to "authentication" in lines 118-121 seems somewhat confusing with regard to the definition of "authenticity" in lines 174-183. Is it possible that what is intended to be covered by lines 118-121 might be better described as "signing"?

RU-(AS)
1.1
The Authenticity definition in section 2b.
"Authenticity is generally understood in law to refer to the genuineness of a document or record, that is, that the document is the "original" support of the information it contains, in the form it was recorded and without any alteration." Authenticity is the property of being genuine and able to be verified and trusted"
This definition may match jurisprudence (law) field well. But, it does not usual in the IT area. In the IT field, the definition above concerns more the term integrity. Integrity - the property of an entity to evidence not having been altered from that created by its issuer.
That's why this definition of authenticity (juristic, but not IT one) may cause problems.
And it is suggested to use the following definition as it is usually used in the IT area:
Authenticity - the property of an entity to evidence the identity of its issuer.
1.2
Genuineness is a separate concept in IT. And it can be defined as integrity + authenticity = the property of an entity to evidence:
(a) not having been altered from that created by its issuer
AND
(b) the identity of its issuer.
OR ALTERNATIVELY SECOND APPROACH:

Recommendation 14 Revision Working Group

Survey on definitions and levels – Consolidation of responses as of 01 Feb 2013

Authenticity - the property of an entity of being genuine and verifiable in a trusted way.

In the context of the v0.4 of the draft, is the **definition of electronic signature** sufficient (line 316-331)? (Y/N) If no, could you please provide either an alternative definition or propose further elements which should be considered?

NL-(JS)
Yes

FI-(JS)
Yes

IT-(RM)
"data in electronic form in, affixed to or logically associated with a data message and which are used by the signatory to sign"
~~which may be used to identify the signatory in relation to the data message and to indicate the signatory's intention in respect of the information contained in the data message."~~

FR-(CP)
Yes

SE-(AN)
OK

AT-(PK)
Yes

ES-(CL)
Yes

IN-(PR)

(1) Electronic signature: Data, in electronic form which are attached to or logically associated, generated with the intention to sign and also as a result of a predetermined action or method agreeable to intended person or environment (signature framework). The signature data created at signing and maintained during any transmission should be retained as long as a signature is needed or legal retention period

(2) Alternate -found on a thesis

An electronic signature is data appended to or logically associated to an electronic record that is affixed through a trusted mechanism such that the signer has confidence that the system being used to electronically sign the document was secure to ensure that the only document signed was the document that the signer intended to sign

US-(TS)
No. In place of lines 318-321 I would recommend using the definition of electronic signature in Section 9(3) of the UN Convention on the Use of Electronic Communications in International Contracts, as noted above. This seems to reflect the latest legal thinking on the subject, and recently came into force. Also, as noted above, I think it is important to recognize that the identification process can be separated from the form of signature used to indicate intent. In other words, that data affixed to the data message to indicate the signer's intent need not also identify the signer if a separate / different method (such as login ID) is used to do that.

In the context of the v0.4 of the draft, is the **definition of document authenticity** sufficient (line

333-344)? (Y/N) Should this definition be retained here (or in the Annex B)? Or should it be presented differently? If the definition is not sufficient, please provide an alternative definition or propose further elements which should be considered.

NL-(JS)
In my opinion there is no definition given under 4e. The text as it is does not add much value without concrete examples . I suggest to give 1 or 2 examples in order to clarify the text.

FI-(JS)
Yes

IT-(RM)
In my opinion authenticity is the outcome of being able to verify the origin and integrity of an electronic document.

FR-(CP)
Yes

SE-(AN)
OK

US-(NH)
Could the authenticity be tied to whether multiple methods are used? Wouldn't a digital signature that is transmitted thru a VPN with an ID/password and a third party validation be more secure than a typed signature?

ES-(CL)
Does ti make sense to consider document authenticity without taking into account a person behind the document? I can not imagine the scenario.
Alternative definition (see above-mentioned)
Document authentication: Authenticity is a property of the electronic document that informs on:

- It's full, so there has not been amended without the knowledge of the author or recipient.
- It comes from an identified and recognized source (entity authenticaion)
- The document is attributable to the person as an author or another function also known as concrete.

IN-(PR)
Authenticity is the status of being dependable in regard to evidence of identity and integrity in accordance with the agreed level of assurance.
Authenticity is an auditable process that ensures an agreed level of quality in the results by maintaining evidence of the identity and/or integrity of resource in accordance with the agreed level of assurance

US-(TS)
As noted above, ***authentication*** typically refers to **the process of establishing or confirming that something is what it purports to be (or in the case of a person, the process of establishing or confirming that someone is who they claim to be)**. The language in lines 333-344 seems confusing to me. I'm also not clear as to how the discussion of "authenticity of a document" in lines 174-183 relates to the discussion of "document authenticity" in lines 333-344.

RU-(AS)

1.4
Concerning *authentication of document by means of signature***.**
As we suggested in 1.1
Authenticity - the property of an entity to evidence the identity of its issuer.
and keeping in mind 1.3
we can formulate the following condition, when the signed document can be considered as a genuine one:
A document can be considered as genuine, if the levels of three signature functions are above a certain pre-defined scale.
And we want to stress again that *genuineness* concept is primary with respect to signature.

This approach would reduce ambiguity and cross of terminology and enable a smoother specification of the Recommendation later on.
OR ALTERNATIVELY SECOND APPROACH:
Authentication of document - a process of verification of document authenticity in a trusted way.
Authentication of document by mean of signature.
A document can be considered as authentic if the levels of three signature functions are above a certain pre-defined scale.
Here is the same as with *undoubted acceptance*: *a certain pre-defined scale* is a matter of the Operational Policy of an application: this certain scale shall be pre-defined there.