Attachment

I. Introduction

States and other organisations are invited to use this template to provide comments to the Secretariat on the draft provisions on the use and cross‑border recognition of identity management and trust services set out in document [A/CN.9/WG.IV/WP.162](https://undocs.org/A/CN.9/WG.IV/WP.162) (“draft provisions”), which is available on the webpage of Working Group IV (<https://uncitral.un.org/en/working_groups/4/electronic_commerce>) in all United Nations official languages. A note with comments on the draft provisions submitted by the World Bank (A/CN.9/WG.IV/WP.163) is also available on the webpage.

Table 1 may be used to provide article‑by‑article comments, while table 2 may be used to provide general comments. Comments may be submitted to the Secretariat in one of the six official languages of the United Nations by email to [uncitral@un.org](mailto:uncitral@un.org) not later than **30 June 2020**. Comments will **not** be published individually, but will be used for preparing pre-session documents, with a view to allowing the Working Group to officially resume its work at the re-scheduled sixtieth session of Working Group IV.

This attachment is available in word format on the English, French and Spanish language versions of the webpage of Working Group IV.

II. Comments

Name of State/observer: [*insert*]

Table 1

**Article‑by‑article comments on draft provisions**

| *Article* | *Non-exhaustive list of questions to consider (drawn from WP.162)* | *Comments* |
| --- | --- | --- |
|  |  |  |
|  | | |
| **Chapter I. General provisions** | | |
|  | | |
| *Article 1. Definitions* | 1. According to the terminology used in WP.162, the IdM process is made up of two stages (or phases), “identity proofing” and “electronic identification” (see para. 2 of WP.162). Are these terms adequate to describe the stages of the IdM process? Are the definitions of these terms accurate?  2. Is the new definition of “authentication” in the context of trust services (articles 21 and 22) acceptable (see footnote 3 of WP.162)?  3. Is it necessary to include a definition of “electronic identification factors” (as used in article 6)? If so, is the definition in footnote 6 of WP.162 acceptable?  4. Is it necessary to include a definition of “electronic identification mechanisms” (as used in article 6)? If so, is the definition in footnote 7 of WP.162 acceptable?  5. Should the definition of “Identity management (IdM) services” refer to ““services consisting of managing identity proofing or electronic identification of [subjects][persons] *in part or in full* in electronic form;” to include in that definition any step (e.g. identity proofing) that may be carried out offline. (As to the choice between [subject] and [person], see footnote 14.)  6. Is it necessary to add a clarification (either in a definition – for instance, of “identity” or of “identity proofing” – or in an explanatory document) to indicate that records from civil registration and vital statistics (CRVS) systems may be a reliable source of attributes of physical persons and, similarly, a dedicated registry may be a reliable source of attributes of legal persons?  7. Is it necessary to insert a definition of the term “level of assurance”, as used in articles 10(1)(b), 11(3) and 27(c)? The following definition of “level of assurance” was proposed in article 4(g) of A/CN.9/WG.IV/WP.157: “‘Level of assurance’ means a designation of the degree of confidence in the identification and authentication processes –i.e., (a) the degree of confidence in the vetting process used to establish the identity of a subject to whom a credential was issued, and (b) the degree of confidence that the subject using the credential is the subject to whom the credential was issued. The assurance reflects the reliability of methods, processes and technologies used;”. | [*insert*] |
|  | | |
| *Article 2. Scope of application* | — | [*insert*] |
|  | | |
| *Article 3. Voluntary use of IdM and trust services* | 1. There have been questions about the relationship between articles 2 and 3. Would their relationship be clearer by recasting article 3 to state that “Nothing in this [instrument] requires a [person][relying party] to accept the electronic identification of a subject or to rely on a trust service without the [person’s][relying party’s] consent.”? | [*insert*] |
|  | | |
| *Article 4. Interpretation* | — | [*insert*] |
|  | | |
| **Chapter II. Identity management** | | |
|  | | |
| *Article 5. Legal recognition of IdM*  Note: Article 5 is formulated along the lines of article 13. | — | [*insert*] |
|  | | |
| *Article 6. Obligations of IdM service providers* | 1. Is it desirable to retain the words “at a minimum” in the chapeau? | [*insert*] |
|  | | |
| *Article 7. Obligations of IdM service providers in case of data breach*  Note: Article 7 is formulated along the lines of article 14(2) | 1. Is “containing” a security breach the desired objective of the steps taken by the IdM service provider to respond to the breach, as required by article 7(1)(a) (see article 14(2) and footnotes 28 and 43 of WP.162)? | [*insert*] |
|  | | |
| *Article 8. Obligations of subscribers*  Note: Article 8 is formulated along the lines of article 15 | 1. After the revision of the definition of “user”, which now refers to “subscriber” (see footnote 15), the draft provisions do not contain any reference to relying third parties. The Working Group decided not to impose any obligation on relying third parties absent a contractual agreement with IdM service providers (A/CN.9/1005, para. 95). Are there any circumstances in which rights and obligations of relying third parties should be addressed in the draft provisions (e.g., to notify breaches of which they are aware)? | [*insert*] |
|  | | |
| *Article 9. Identification using IdM* | 1. Which option for article 9(1) is preferable (see footnotes 30 to 32 of WP.162)?  2. What is the relationship between article 2(3) and article 9?  3. Is it necessary to retain a functional equivalence provision for identification, or are the identification components of electronic signatures and electronic seals sufficient to achieve the desired goal of establishing functional equivalence standards for identification?  4. If article 9 is retained, should the reliability standard of the method referred to in article 9 be qualified as “reliable as appropriate” to better reflect the varying standards for offline identification?  5. In practice, a relying party may use its own IdM service for the electronic identification of a subject, in which case, the relying party is the IdM service provider. Is it desirable to insert a provision to acknowledge that the IdM service provider might be the person seeking to rely on the electronic identification? (Compare article 10(3) MLEC for the reverse situation.) | [*insert*] |
|  | | |
| *Article 10. Factors relevant to determining reliability*  Note: Article 23 is the corresponding provision for trust services | 1. Article 10(1)(d) aims at accommodating IdM systems governed by contractual rules such as trust frameworks. Its operation is limited to the parties to those contractual agreements. Is the provision sufficient for its intended purpose? Or does it require further specification (either in the provision itself or in an explanatory document)?  2. Does the title of article 10 adequately reflect its content? If not, should it be replaced by “Requirements for determining reliability”? Should the titles of articles 10 and 23 be aligned? | [*insert*] |
|  | | |
| *Article 11. Designation of reliable IdM systems*  Note: Article 11 is formulated along the lines of article 24 | — | [*insert*] |
|  | | |
| *Article 12. Liability of IdM service provider*  Note: Article 12 is formulated along the lines of article 25 | 1. Which option for article 12 is preferable (see footnote 35 of WP.162)?  2. If option A is preferred, is it necessary to include such provision on liability at all (see footnote 36 of WP.162)?  3. If option B or option C is preferred, is it necessary to include a provision waiving liability for public IdM service providers?  4. If option B or option C is preferred, is it desirable to treat differently the liability of an IdM service provider arising from the use of an IdM system that is designated pursuant to article 11? If so, how? | [*insert*] |
|  | | |
| **Chapter III. Trust services** | | |
|  | | |
| *Article 13.*  *Legal recognition of trust services* | 1. Is the first bracketed text in the chapeau acceptable (see footnote 40 of WP.162)? Would the purpose of the provision be better expressed by referring instead to the results of the use of a trust service? | [*insert*] |
|  | | |
| *Article 14. Obligations of trust service providers* | 1. Should the obligation in article 14(1)(b) be formulated along the lines of article 6(f) (see footnote 42 of WP.162)?  2. (See question to article 7.) | [*insert*] |
|  | | |
| *Article 15. Obligations of subscribers* | 1. After the revision of the definition of “user”, which now refers to “subscriber” (see footnote 15), the draft provisions do not contain any reference to relying third parties. Do relying third parties have rights and obligations that should be reflected in the draft provisions (e.g., to notify breaches they are aware of)? | [*insert*] |
|  | | |
| *Article 16. Electronic signatures* | 1. Should the reliability standard of the method referred to in article 16 be qualified as “reliable as appropriate” to better reflect the varying standards for offline identification? | [*insert*] |
|  | | |
| *Article 17. Electronic seals* | 1. Should the reliability standard of the method referred to in article 17 be qualified as “reliable as appropriate” to better reflect the varying standards for offline identification? | [*insert*] |
|  | | |
| *Article 18. Electronic timestamps* | — | [*insert*] |
|  | | |
| *Article 19. Electronic archiving* | — | [*insert*] |
|  | | |
| *Article 20. Electronic registered delivery services* | 1. Should Article 20 specify that additional functions of an electronic delivery service is (a) to assure the integrity of the data message and (b) to identify the sender and/or the recipient (see footnote 58 of WP.162)? | [*insert*] |
|  | | |
| *Article 21. Website authentication* | 1. Should there be a reference to the presumption of reliability and proof of reliability for website authentication? | [*insert*] |
|  | | |
| *Article 22. Object authentication* | 1. Is it desirable to deal with the identification of objects as a trust service, or should the provision be limited to linking objects with the persons controlling them (“object tracing”)? | [*insert*] |
|  | | |
| *Article 23. Reliability standard for trust services* | 1. Article 23(1)(h) aims at recognizing that the parties to a transaction may agree on the use of trust services, and that such agreement may be relevant in determining the reliability of the trust services among those parties. Should an explicit reference to “between the parties” be inserted (as it is in article 10(d))?  2. (See article 10.) | [*insert*] |
|  | | |
| *Article 24. Designation of reliable trust services* | — | [*insert*] |
|  | | |
| *Article 25. Liability of trust services providers* | 1. Which option for article 25 is preferable (see footnote 35 of WP.162)?  2. If option A is preferred, is it necessary to include such provision on liability at all (see footnote 66 of WP.162)?  3. If option B or option C is preferred, is it necessary to include a provision waiving liability for public trust service providers?  4. If option B or option C is preferred, is it desirable to treat differently the liability of a trust service provider arising from the use of a trust service that is designated pursuant to article 24? | [*insert*] |
|  | | |
| **Chapter IV. International aspects** | | |
|  | | |
| *Article 26. Cross-border recognition of IdM and trust services* | 1. The establishment of an effective mechanism for the cross-border recognition of IdM and trust services is a core objective of this project. The main provisions that pursue that objective are: article 26, on cross-border recognition of IdM systems and trust services; articles 10(2) and 23(3), on the reliability of the methods used; and articles 11(4) and 24(4), on non-geographic discrimination in designating reliable IdM systems and trust services. Do these provisions sufficiently pursue this objective? If not, which additional provisions should be introduced?  2. Are the existing provisions on cross-border recognition aligned? In particular, is it appropriate that articles 11(4), 24(4) and 26 focus on ‘IdM systems’ and ‘trust services’, while articles 10(2) and 23(3) focus on the reliability of the ‘methods’? | [*insert*] |
|  | | |
| *Article 27. Cooperation* | 1. Should article 27 apply to all entities involved in IdM and trust services? Does it fulfil a useful function, or should such activities be left to the initiative of the concerned entities? | [*insert*] |
|  |  |  |

Table 2

General comments on draft provisions

| *Comments* |
| --- |
|  |
| [*insert*] |