Naciones Unidas A/CN.9/WG.IV/WP.165

Asamblea General

Distr. limitada
30 de septiembre de 2020
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
60º período de sesiones
Viena (en línea), 19 a 23 de octubre de 2020

Reconsideración del enfoque con respecto a los sistemas de gestión de la identidad y los servicios de confianza

Comunicación de los Estados Unidos de América

Nota de la Secretaría

Los Estados Unidos de América presentaron un documento para que el Grupo de Trabajo lo examinara en su 60º período de sesiones. En el anexo de la presente nota figura la traducción al español del documento en inglés que recibió la Secretaría.

V.20-05631 (S) 131020 131020

Anexo

Reconsideración del enfoque con respecto a los sistemas de gestión de la identidad y los servicios de confianza

1. Los Estados Unidos de América se complacen en presentar este documento sobre el actual proyecto del Grupo de Trabajo IV en materia de sistemas de gestión de la identidad y servicios de confianza. El presente documento está dividido en tres secciones. En la primera sección se describe en líneas generales y se resume el contenido de las otras secciones. En la segunda sección se facilita información de antecedentes sobre los sistemas de gestión de la identidad y sus reglas de funcionamiento. Por último, en la tercera sección se presenta a grandes rasgos el marco jurídico dentro del cual suelen operar todos los sistemas de gestión de la identidad, así como un marco conceptual sobre el modo en que el Grupo de Trabajo podría adaptar el proyecto que figura en el documento A/CN.9/WG.IV/WP.162 (en adelante, "el proyecto") para que regulara eficazmente los sistemas de gestión de la identidad del sector privado.

2. A los efectos del presente documento, los Estados Unidos se centran exclusivamente en los sistemas de gestión de la identidad y en la forma en que el Grupo de Trabajo podría regular estos sistemas de manera eficaz. Dicho esto, los Estados Unidos celebrarían que se entablara un debate similar en el seno del Grupo de Trabajo acerca de la parte del proyecto dedicada a los servicios de confianza, por cuanto creemos que plantea muchas de las mismas cuestiones conceptuales que se analizan a continuación en relación con las disposiciones sobre la gestión de la identidad.

I. Descripción general y resumen

3. Como cuestión de alcance general, los Estados Unidos albergan inquietudes sobre aspectos fundamentales del enfoque actual del Grupo de Trabajo en materia de sistemas de gestión de la identidad recogido en el proyecto (véase el apéndice) y consideran necesario que haya un debate conceptual en el Grupo de Trabajo a fin de dar respuesta a esas inquietudes.

4. La CNUDMI debería tratar de ofrecer un marco que pueda ayudar a los Estados a navegar por las cuestiones jurídicas que pueden plantearse con los sistemas de gestión de la identidad del sector privado, en particular en aquellos ámbitos que no pueden abarcar las reglas de funcionamiento de base contractual por las que se rige cada sistema. Una parte de esta tarea podría consistir en revisar la legislación nacional vigente a fin de eliminar las barreras y la inseguridad que genera la legislación vigente, colmar las lagunas de la legislación actual relevantes para los sistemas de gestión de la identidad que no pueden resolverse por contrato o regular cuestiones nuevas que pueden promover el desarrollo de sistemas de gestión de la identidad del sector privado. Sin embargo, en el proyecto se adopta un enfoque considerablemente diferente y, en opinión de los Estados Unidos, inviable.

A. ¿Qué son los sistemas de gestión de la identidad?

5. La **gestión de la identidad** abarca un conjunto de políticas, procesos y procedimientos que permiten identificar a una persona o entidad (es decir, responder a la pregunta "¿quién es?") y autenticar esa identidad (es decir, responder a la pregunta "¿cómo puede demostrarlo?"). Como se describe con mayor detalle en la sección II *infra*, una **operación de identidad** es una comunicación que facilita esa información de identidad sobre un sujeto a una parte que confía de manera que autentica la relación entre esa información de identidad y el sujeto. Los sistemas de gestión de la identidad facilitan estas **operaciones de identidad**. Los **sistemas de gestión de la identidad** son mecanismos complejos que conllevan una combinación coherente de entidades participantes, procesos y tecnología, en los cuales cada participante ejerce las responsabilidades de uno o más papeles predefinidos, de conformidad con un conjunto

predefinido de procesos, políticas y procedimientos jurídicamente vinculantes, con el fin de facilitar operaciones de identidad que permitirán a una persona identificarse con múltiples entidades con las que no guarda relación alguna.

6. Para que funcione, cada sistema de gestión de la identidad necesita un conjunto ejecutable de reglas de funcionamiento. Como se describe con mayor detalle en la sección II *infra*, las reglas de funcionamiento regulan el funcionamiento de un determinado sistema de gestión de la identidad, especificando cómo deben ejecutarse sus procesos de gestión de la identidad y las correspondientes operaciones de identidad y precisando los derechos y las responsabilidades de las diversas partes que participan en el mecanismo. Habida cuenta de que cada sistema de gestión de la identidad es diferente, cada uno necesita un conjunto singular de reglas de funcionamiento adaptadas a su propósito, estructura, base de participantes y perfil de riesgo.

7. En el caso de los sistemas de gestión de la identidad del sector público, las reglas de funcionamiento suelen estar recogidas en una ley o reglamento y, por ende, son vinculantes para los participantes por efecto de la ley. En el caso de los sistemas de gestión de la identidad del sector privado, las reglas de funcionamiento están recogidas en un documento escrito por el operador del sistema (o alguna otra persona o entidad) y adquieren carácter vinculante para los participantes por contrato.

B. ¿Qué debería regular el instrumento de la CNUDMI?

8. Todo instrumento sobre los sistemas de gestión de la identidad del sector privado que elabore la CNUDMI debería tener en cuenta tanto la legislación nacional vigente como las distintas reglas de funcionamiento de base contractual que utiliza cada sistema de gestión de la identidad. Específicamente, el instrumento de la CNUDMI debería regular cuestiones relativas a la aplicabilidad de la legislación nacional vigente a los sistemas de gestión de la identidad del sector privado que i) no puedan regirse por las distintas reglas de funcionamiento de base contractual adoptadas por cada sistema o ii) creen de otro modo problemas para todos los sistemas de gestión de la identidad del sector privado. Por tanto, el instrumento de la CNUDMI regularía, entre otros, estos ámbitos: el reconocimiento jurídico de las operaciones de identidad originadas en los sistemas de gestión de la identidad del sector privado; los requisitos para determinar si una operación de identidad del sector privado satisface las exigencias legales aplicables para identificar a una persona, y la aplicabilidad de las leyes que no pueden ser modificadas por las reglas de funcionamiento del sistema de gestión de la identidad, como las leyes que regulan el uso de identificadores públicos, la legislación en materia de protección del consumidor y el derecho de la responsabilidad civil extracontractual.

9. Este enfoque se basa en el reconocimiento de que los sistemas de gestión de la identidad del sector privado se rigen por un marco jurídico de tres niveles, en cuya cima se sitúa la legislación nacional vigente (nivel 1) y en cuya base se encuentran las reglas de funcionamiento de base contractual de los distintos sistemas de gestión de la identidad (nivel 3). La capa intermedia de ese marco jurídico (nivel 2) serviría de puente entre el nivel 1 y el nivel 3. La CNUDMI debería tener por objetivo la elaboración de un instrumento que orientara a los Estados en cuanto al contenido del nivel 2. Se describe con mayor detalle este marco jurídico en la sección III *infra* (en particular en la Figura 1, que representa gráficamente estos tres niveles de reglamentación y su relación). En la sección III también se detalla el plan que podría seguir la CNUDMI para reflexionar sobre los contenidos de un instrumento de esa índole.

10. El proyecto no reconoce este marco jurídico, sino que adopta un enfoque fundamentalmente diferente y, a nuestro parecer, inviable. Si bien regula algunas cuestiones que quedarían comprendidas correctamente en un instrumento de nivel 2, las combina y confunde con numerosas cuestiones que deberían regirse en su lugar por las reglas de funcionamiento de base contractual de cada sistema de gestión de la identidad (nivel 3). Por consiguiente, adopta un enfoque único para cuestiones que variarán enormemente entre las diversas reglas de funcionamiento de base contractual por las que se rijan los distintos sistemas de gestión de la identidad. A medida que han ido

avanzando las negociaciones en torno al proyecto de texto, se ha ido haciendo más patente que se trata de un enfoque inviable.

11. El proyecto utiliza las reglas de funcionamiento de un sistema de gestión de la identidad del sector público (eIDAS) como modelo conceptual y trata de expandirlo globalmente a todos los sistemas de gestión de la identidad. Ciertamente, eIDAS es un enfoque sumamente innovador en la regulación de los sistemas de gestión de la identidad y ha contribuido notablemente a que se comprenda en todo el mundo cómo podrían funcionar esos sistemas y cómo se podrían regular para su uso en el sector público. Sin embargo, el problema radica en que eIDAS es un conjunto singular de reglas de funcionamiento para un único sistema de gestión de la identidad del sector público (compuesto por los proveedores de identidad de los distintos países de la Unión Europea). Por tanto, es el equivalente del sector público de las reglas de funcionamiento de base contractual por las que se regiría un sistema específico de gestión de la identidad del sector privado. No conviene tratar de imponer esas reglas de funcionamiento a todos los demás sistemas de gestión de la identidad.

12. En otras palabras, mientras que eIDAS es un conjunto de reglas de funcionamiento que regula un *sistema de gestión de la identidad* (nivel 3), la CNUDMI debería elaborar un instrumento que se aplicara a *todos los sistemas de gestión de la identidad* (nivel 2). Mientras que eIDAS es un conjunto de reglas de funcionamiento para un sistema de gestión de la identidad del *sector público* (es decir, que regulan las operaciones de identidad para su uso en el sector público), la CNUDMI debería elaborar un instrumento que se aplicara a los sistemas de gestión de la identidad del *sector privado*. Específicamente, el instrumento de la CNUDMI debería servir de puente entre las reglas de funcionamiento de base contractual por las que se rigen los distintos sistemas de gestión de la identidad del sector privado (nivel 3) y aquellos aspectos de la legislación nacional vigente (nivel 1) que inciden adversamente en todos los sistemas de gestión de la identidad pero que no pueden resolver las reglas de funcionamiento de los distintos sistemas de gestión de la identidad (como el reconocimiento jurídico de las operaciones de identidad o la responsabilidad civil extracontractual)[1].

13. En cambio, el proyecto establece reglas con respecto a diversas cuestiones que normalmente se regirían por las reglas de funcionamiento de base contractual de cada sistema de gestión de la identidad. Se trata de cuestiones como, por ejemplo, las obligaciones de los proveedores de servicios de gestión de la identidad (art. 6), las obligaciones en caso de violación (art. 7), las obligaciones de los abonados (art. 8) o la responsabilidad de los proveedores de servicios de gestión de la identidad (art. 12). Al mismo tiempo, no define con claridad en qué situaciones las partes contratantes pueden apartarse de la legislación vigente en relación con estos temas y en qué situaciones deben atenerse a la legislación vigente.

14. Además, mientras que el marco de eIDAS, en el cual se basa el proyecto, parte de un mecanismo centralizado para regular, fijar normas y certificar sistemas de gestión de la identidad, no existe un mecanismo centralizado de esa índole con alcance mundial que pueda sustentar un instrumento de la CNUDMI como el que se propone. El proyecto se limita a presuponer que existe dicho mecanismo mundial. A falta de mecanismo, las disposiciones del proyecto relativas al reconocimiento transfronterizo y las normas de fiabilidad plantean una serie de preguntas sin respuesta que exigen un mayor debate en el seno del Grupo de Trabajo. En realidad, eIDAS prevé el reconocimiento de los servicios de confianza prestados por proveedores establecidos fuera de la Unión Europea únicamente cuando se haya celebrado un tipo de acuerdo especificado entre la Unión Europea y el tercer país (art. 14, párr. 1, del Reglamento eIDAS).

[1] Si bien podría decirse que eIDAS incluye elementos del nivel 2 y del nivel 3 para los proveedores de identidad de los distintos países de la Unión Europea que aceptan participar en el marco único de la Unión Europea, creemos que la CNUDMI debería centrarse exclusivamente en elaborar un instrumento de nivel 2 que se aplicara a todos los proveedores de servicios de gestión de la identidad del sector privado. Además, eIDAS funciona como un sistema de gestión de la identidad para su uso en el sector público, mientras que la tarea de la CNUDMI consiste en elaborar un instrumento que se aplique a los sistemas de gestión de la identidad del sector privado.

15. El hecho de que el proyecto siga el patrón de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas no solo es incongruente con el modelo eIDAS, sino que también resulta inapropiado. Las firmas electrónicas son relativamente simples y están estandarizadas, mientras que los sistemas de gestión de la identidad son más complejos y tienen múltiples dimensiones. Por ejemplo, en las firmas electrónicas suelen intervenir dos partes, mientras que en los sistemas de gestión de la identidad participan muchas partes. Las normas que contiene la Ley Modelo sobre las Firmas Electrónicas simplemente no funcionan para los sistemas de gestión de la identidad.

16. Estas cuestiones fundamentales plantean interrogantes muy básicos pero esenciales: ¿de qué manera se beneficiarían los Estados del enfoque reflejado en el proyecto una vez que se adoptara? A falta de mecanismo centralizado que regule o certifique los sistemas de gestión de identidad o los servicios de confianza, ¿cómo logrará el texto alcanzar los objetivos planteados, por ejemplo en relación con el reconocimiento transfronterizo o las normas de fiabilidad? Si, por lo que entienden los Estados Unidos, la intención es que el proyecto se aplique a los sistemas de gestión de la identidad del sector privado, ¿qué relación guardan las normas establecidas en el proyecto con las reglas de funcionamiento establecidas por las partes contratantes por las cuales se rige un sistema de gestión de la identidad?

17. Los Estados Unidos dieron a conocer anteriormente su postura con respecto al modelo de la Secretaría y respondieron por escrito a la versión más reciente del texto, y el apéndice de la presente nota contiene un análisis del proyecto artículo por artículo. Sin embargo, los Estados Unidos opinan que, antes de seguir avanzando en el proyecto, el Grupo de Trabajo debería acometer un debate conceptual para aclarar cómo encajará el proyecto en el marco jurídico general por el que se rigen los sistemas de gestión de la identidad. Si bien los Estados Unidos agradecen la ingente labor que ha supuesto la elaboración del proyecto y los esfuerzos que se han hecho por consensuar el documento, cabría lamentar que el Grupo de Trabajo se adentrara en un camino que desembocara un instrumento de escasa utilidad para los Estados Miembros o los sistemas de gestión de la identidad del sector privado.

18. Como se apunta en el presente documento, existen diversos ámbitos en los que el proyecto regula temas que son apropiados y pertinentes para la cuestión de los sistemas de gestión de la identidad pero en los que el enfoque resulta inviable, y es en esos ámbitos en los que el Grupo de Trabajo tal vez pueda tomar el proyecto como punto de partida e incorporar cambios conceptuales en las disposiciones actuales. En otros ámbitos, estaría justificado introducir cambios de mayor calado o suprimir algunos elementos.

19. Los Estados Unidos ofrecen el marco que figura en la sección III *infra* como guía del debate conceptual que ayudará a trazar la senda de cara al futuro.

II. Información de antecedentes sobre los sistemas de gestión de la identidad

20. Creemos que este proyecto debería tener como objetivo el establecimiento de un marco jurídico que permitiera y fomentara el desarrollo de un ecosistema robusto en materia de identidad, en el cual pudieran prosperar múltiples sistemas de gestión de la identidad de toda clase procedentes del sector privado y estos pudieran respaldar el comercio nacional e internacional. Para ello, es necesario centrarse en identificar las barreras o las lagunas de la legislación nacional vigente que deben solventarse. Además, a fin de fomentar el desarrollo de sistemas de gestión de la identidad nuevos y diferentes, es importante que el Grupo de Trabajo evite soluciones únicas para las cuestiones y los problemas que deberían regirse por las reglas de funcionamiento singulares de base contractual establecidas por los distintos sistemas de gestión de la identidad.

21. Con objeto de identificar las barreras y las lagunas en el marco jurídico de la gestión de la identidad que deben resolverse, en primer lugar es necesario emprender las siguientes acciones:

- Examinar los conceptos de “operación de identidad” y “sistema de gestión de la identidad”;
- Examinar la necesidad de disponer de reglas de funcionamiento por las que se rija el funcionamiento de cada sistema de gestión de la identidad del sector privado, así como la función de dichas reglas; y
- Comprender el marco jurídico general por el que se rigen los sistemas de gestión de la identidad, así como los casos y la forma en que el instrumento de la CNUDMI podría ayudar o encajar.

22. Una vez puesto en antecedentes, el Grupo de Trabajo puede proceder a determinar las cuestiones jurídicas que no pueden resolverse en las reglas de funcionamiento singulares de base contractual que forman parte de cada sistema de gestión de la identidad y que, por ende, tienen que ser reguladas mediante adiciones y cambios en la legislación nacional utilizando a tal fin un instrumento jurídico elaborado por la CNUDMI.

A. Operaciones de identidad

23. Las operaciones de identidad son comunicaciones en las que una parte que confía recibe información de identidad sobre un individuo [2] (identificación), junto con la verificación de que la persona que alega ser dicho individuo es, de hecho, dicho individuo (autenticación). Suelen llevarse a cabo a los efectos de: 1) participar en algún tipo de operación con el sujeto (por ejemplo, celebrar un contrato, realizar alguna prestación, comunicar información, etc.) o 2) conferir al sujeto acceso a algún tipo de instalación digital o física (por ejemplo, sitio web, base de datos, edificio, etc.).

24. Las operaciones de identidad suelen requerir 1) la recopilación y verificación de información (atributos) sobre un determinado sujeto de datos (un proceso de identificación), 2) la emisión de una credencial que contenga uno o varios de esos atributos (un proceso de emisión de la credencial) y 3) la asociación de los atributos de identidad que figuran en esa credencial con una persona específica, que a menudo es remota (es decir, un proceso de autenticación). A través de esos procesos, las operaciones de identidad están diseñadas para verificar la identidad de un individuo y autenticar la relación de esa identidad con una persona específica.

25. Así, por ejemplo, la acción de presentar el pasaporte en la frontera para poder ser admitido en un país es una operación de identidad. En ese caso, a la parte que confía (el agente de control fronterizo) se le presentan atributos de identidad verificados anteriormente acerca de un individuo (que constan en el pasaporte), junto con un método para verificar que la persona que presenta el pasaporte es el individuo designado en el pasaporte (es decir, a través de la fotografía o de los datos de las huellas dactilares integrados en el pasaporte). Del mismo modo, el proceso de iniciar sesión en una red en línea con un nombre de usuario y una contraseña a fin de poder acceder a una base de datos es una operación de identidad. Conlleva la asociación (a través de la contraseña secreta) de atributos de identidad verificados anteriormente acerca de un individuo (designado a través del nombre de usuario) con una persona que pretende hacerse pasar por dicho individuo (es decir, la persona que introduce el nombre de usuario).

[2] El sujeto de la operación de identidad podría ser una persona física, una entidad, un dispositivo o un objeto digital. El presente documento se centrará en las personas físicas, puesto que hasta la fecha el debate del Grupo de Trabajo se ha centrado en ellas.

B. Los sistemas de gestión de la identidad son sistemas multipartitos diseñados para facilitar las operaciones de identidad

26. Los **sistemas de gestión de la identidad** son combinaciones coherentes de entidades participantes, procesos y tecnología, en las cuales cada participante ejerce las responsabilidades de uno o más papeles predefinidos[3], de conformidad con un conjunto predefinido de procesos, políticas y procedimientos jurídicamente vinculantes, con el fin de facilitar operaciones de identidad.

27. Los sistemas de gestión de la identidad son sistemas multipartitos complejos. Intervienen en ellos múltiples participantes que ejercen varios papeles, como autoridades de registro, comprobadores de identidad, proveedores de atributos, proveedores de servicios de confianza, proveedores de identidad, proveedores de credenciales, proveedores de servicios de verificación, *hubs*, etc. Coordinan la labor necesaria para recopilar y verificar la identidad (atributos) de un sujeto de datos, emitir una credencial que contenga uno o varios de esos atributos y autenticar esos atributos de identidad con una persona específica en el contexto de una operación de identidad. Estos participantes trabajan juntos con objeto de facilitar las operaciones de identidad para múltiples partes que confían.

28. En cuanto a la complejidad de la estructura, los sistemas de gestión de la identidad presentan analogías con los sistemas de tarjetas de crédito establecidos con la finalidad de facilitar las operaciones de crédito (como MasterCard o Visa) o con los sistemas de pagos electrónicos establecidos con la finalidad de facilitar las operaciones de pago (como SWIFT o ACH). Si bien cada uno de estos sistemas está diseñado utilizando una estructura diferente y sirve un propósito distinto, todos ellos son sistemas multipartitos diseñados para facilitar un determinado tipo de operación económica (operaciones con una tarjeta de crédito, de pago o de identidad).

29. La estructura de los sistemas de gestión de la identidad puede variar considerablemente. Por ejemplo, los sistemas de gestión de la identidad pueden ser sistemas centralizados (un único proveedor de identidad facilita las operaciones de identidad para múltiples partes que confían), sistemas federados (un conjunto limitado de proveedores de identidad almacenan y proveen de manera centralizada información de identidad de los usuarios a fin de facilitar las operaciones de identidad con una o múltiples partes que confían) o sistemas descentralizados (múltiples proveedores de identidad autentican la información de identidad almacenada localmente por los usuarios a fin de facilitar las operaciones de identidad con múltiples partes que confían). Esta variedad en la estructura de los sistemas de gestión de la identidad es una de las razones fundamentales por las que el instrumento elaborado por el Grupo de Trabajo no puede adoptar un enfoque único con respecto a numerosas cuestiones.

C. Los sistemas de gestión de la identidad necesitan reglas de funcionamiento jurídicamente vinculantes

30. Habida cuenta de que los sistemas de gestión de la identidad son sistemas multipartitos complejos, la coordinación y la cooperación de las entidades participantes resultan imprescindibles para lograr el objetivo deseado. Por tanto, los sistemas de gestión de la identidad requieren una estructura organizada, orientada a los objetivos e integrada por entidades participantes interrelacionadas e interdependientes que desempeñen diversos papeles, ejecuten un conjunto de procesos detallados y se atengan a un conjunto de políticas y procedimientos, diseñados en su conjunto para lograr un objetivo específico: facilitar las operaciones de identidad.

[3] A modo de ejemplo, se pueden citar, entre otros, los papeles de autoridad de registro, comprobador de identidad, proveedor de identidad, intermediario, *hub*, proveedor de atributos y parte que confía.

31. Asimismo, dado que en los sistemas de gestión de la identidad intervienen múltiples entidades participantes independientes que pueden interactuar entre sí para ejecutar una serie de operaciones complejas, los sistemas de gestión de la identidad no funcionan automáticamente por sí solos, sino que cada uno de los participantes debe guiarse por un conjunto de reglas o instrucciones que le indiquen cómo debería actuar para ejercer su papel. Normalmente, el cumplimiento de esas reglas debe ser jurídicamente exigible a fin de garantizar que todos los participantes satisfagan los requisitos que les sean aplicables y puedan tener la confianza de que los demás participantes observarán esas reglas y generarán un resultado de fiar.

32. Por consiguiente, cada sistema de gestión de la identidad necesita un conjunto de **reglas de funcionamiento**[4] jurídicamente exigible que regule su funcionamiento. Esas reglas cumplen tres funciones importantes:

- Garantizan que el sistema de gestión de la identidad **funcione debidamente**, es decir, especifican las políticas, los procedimientos y los procesos necesarios para el funcionamiento del sistema a fin de que el sistema de gestión de la identidad "opere" como se espera;
- Definen los **deberes y las obligaciones** de cada uno de los papeles ejercidos por los participantes (por ejemplo, para que cada participante sepa qué hacer), así como sus responsabilidades legales y (si corresponde) definen y asignan equitativamente los riesgos en materia de responsabilidad civil; y
- Especifican los requisitos adicionales que contribuyen a hacer que el sistema de gestión de la identidad sea "**de fiar**" para el propósito que se persigue, es decir, imponen requisitos que van más allá de garantizar que el sistema de gestión de la identidad sea meramente funcional, y aplican medidas adicionales para que los participantes tengan confianza en las operaciones de identidad resultantes y estén dispuestos a fiarse de ellas.

33. Con el fin de lograr esos objetivos, las reglas de funcionamiento suelen estar diseñadas de modo que regulan las cuestiones comerciales, técnicas y jurídicas específicas que se plantean durante el funcionamiento de un determinado sistema de gestión de la identidad. Se trata de cuestiones como, por ejemplo, los requisitos de participación; las definiciones y responsabilidades de cada papel; los procesos y procedimientos para la inscripción del sujeto de datos; la comprobación de identidad; la emisión de credenciales, la autenticación de la identidad, las especificaciones y los estándares técnicos, los requisitos de seguridad de los datos, las garantías, la distribución de la responsabilidad, los procedimientos de solución de controversias y los derechos de terminación. Las reglas de funcionamiento también regulan la gobernanza del sistema de gestión de la identidad en aspectos como las cualificaciones para participar en él, el cumplimiento forzoso de las reglas y las revisiones de las reglas. Constituyen el marco de gobernanza del sistema de gestión de la identidad. Además, habida cuenta de que la estructura, la tecnología y el propósito de cada sistema de gestión de la identidad pueden ser diferentes, es probable que haya diferencias considerables entre las reglas de funcionamiento de cada sistema.

34. Para que las reglas de funcionamiento del sistema de gestión de la identidad sean jurídicamente vinculantes y exigibles, pueden revestir la forma de ley, reglamento o contrato.

35. En el caso de los sistemas de gestión de la identidad del **sector público**, las reglas de funcionamiento suelen adoptar la forma de **ley** o reglamento detallado. A título de ejemplo, pueden citarse los casos de la Ley Aadhaar de la India[5], la Ley de Documentos

[4] Las reglas de funcionamiento también reciben con frecuencia otros nombres como marco de gobernanza, marco de confianza o reglas del sistema.

[5] Ley de Aadhaar (Entrega Específica de Ayudas Financieras y Otros Subsidios, Prestaciones y Servicios) de 2016 (https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf).

de Identidad de Estonia[6] y el Reglamento eIDAS de la Unión Europea[7]. Sin embargo, algunos sistemas de gestión de la identidad del sector público, como el sistema GOV.UK Verify, han recurrido a los contratos[8].

36. En el caso de los sistemas de gestión de la identidad del **sector privado**, las reglas de funcionamiento revisten la forma de **contrato** vinculante para los participantes en el sistema (del mismo modo que los participantes en un sistema de tarjetas de crédito o en un sistema de pagos acuerdan por vía contractual las condiciones de las reglas de funcionamiento aplicables a su papel). El Trust Framework de SAFE Identity[9], el Sovrin Governance Framework[10] y el Pan-Canadian Trust Framework[11] son algunos ejemplos de reglas de funcionamiento de sistemas de gestión de la identidad del sector privado. Véase también "A Guide to Trust Frameworks and Interoperability"[12].

D. Las reglas de funcionamiento son singulares para cada sistema de gestión de la identidad

37. Cada sistema de gestión de la identidad es diferente, por lo que necesita un conjunto singular de reglas de funcionamiento adaptadas a su estructura, tecnología, propósito, mercado y perfil de riesgo.

38. Los sistemas de gestión de la identidad del sector privado emplean una amplia variedad de **estructuras y tecnologías**, cada una de las cuales necesitará diferentes enfoques con respecto a las reglas de funcionamiento. Si se intenta imponer un único conjunto uniforme de reglas a todos los sistemas, se obstaculizará la creación de esos sistemas de gestión de la identidad del sector privado.

- Entre las distintas **estructuras de los sistemas** de gestión de la identidad identificadas por el Foro Económico Mundial en 2016[13] se encuentran los sistemas de gestión de la identidad de carácter interno, los sistemas de gestión de la identidad con autenticación externa, los sistemas de gestión de la identidad centralizados, los sistemas de gestión de la identidad federados y los sistemas de gestión de la identidad descentralizados. Los sistemas de gestión de la identidad basados en *hubs*, los sistemas de gestión de la identidad autosoberana y los sistemas de gestión de la identidad que se están desarrollando con los teléfonos móviles son algunos ejemplos de las otras estructuras de los sistemas de gestión de la identidad que se han desplegado recientemente. Cada sistema exigirá un enfoque distinto con respecto a las reglas de funcionamiento y se resentirá de los intentos de imponer un conjunto uniforme de reglas a todos los sistemas.
- Entre los ejemplos de las diferentes **tecnologías utilizadas para los sistemas** de gestión de la identidad se pueden citar los sistemas de gestión de la identidad basados en infraestructura de clave pública, los sistemas basados en tecnologías

[6] Ley de Documentos de Identidad, aprobado el 15 de febrero de 1999, RT I 1999, 25, 365, en vigor desde el 1 de enero de 2000 (www.riigiteataja.ee/en/eli/ee/504112013003/consolide).

[7] El Reglamento (UE) núm. 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS), aprobado el 23 de julio de 2014, establece un marco normativo previsible que permite las interacciones electrónicas seguras y sin solución de continuidad entre las empresas, los ciudadanos y las autoridades públicas (https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014).

[8] www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

[9] www.globenewswire.com/news-release/2020/05/19/2035512/0/en/SAFE-Identity-Announces-Revamped-SAFE-Biopharma-Trust-Framework-and-New-Services-to-Expand-and-Evolve-Digital-Trust-in-Healthcare-Sector.html.

[10] https://sovrin.org/library/sovrin-governance-framework.

[11] https://drive.google.com/file/d/1Xmjh8QJZKWmRkaTtE2f43ISntD7jE6D5/view.

[12] Open Identity Exchange, "A Guide to Trust Frameworks and Interoperability" (https://openidentityexchange.org/guide-trust-frameworks-interoperability).

[13] Véase Foro Económico Mundial, "A Blueprint for Digital Identity", agosto de 2016 (http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf).

de cadenas de bloques y los sistemas que utilizan los estándares OAuth y OpenID Connect, cada uno de los cuales necesitará un enfoque distinto con respecto a las reglas de funcionamiento y se resentirá de los intentos de imponer un conjunto uniforme de reglas a todos los sistemas.

39. Los sistemas de gestión de la identidad del sector privado también suelen diseñarse para diversos **propósitos o mercados**, de modo que se requerirán varios enfoques, requisitos de confianza y asignación de riesgos en sus reglas de funcionamiento. Si se intenta imponer un único conjunto uniforme de reglas a todos esos sistemas de gestión de la identidad, se obstaculizará su creación.

- Entre los ejemplos de sistemas de gestión de la identidad diseñados para diferentes **propósitos y mercados** figuran los siguientes: el sistema InCommon diseñado para su uso en el ámbito educativo (por ejemplo, universidades y alumnado), el sistema SAFE BioPharma diseñado para la industria farmacéutica, el sistema CertiPath diseñado para la industria aeroespacial internacional, el sistema CA Browser Forum diseñado para identificar a los operadores de sitios web, el sistema Zenkey diseñado para la identidad móvil y los sistemas ligeros de Google, LinkedIn y Facebook diseñados para el acceso a sitios web de bajo riesgo.

40. Dado que están diseñados para satisfacer los requisitos singulares de un determinado sistema de gestión de la identidad, las cuestiones reguladas en esas reglas de funcionamiento deberían quedar excluidas del ámbito de aplicación del instrumento que elabora el Grupo de Trabajo.

41. Habida cuenta de que las reglas de funcionamiento de los sistemas de gestión de la identidad del sector privado tienen una base contractual y están vinculadas a los requisitos singulares de un determinado sistema, es importante que todo instrumento que elabore la CNUDMI no trate de duplicar esas reglas de funcionamiento con un enfoque único aplicable a todos los sistemas de gestión de la identidad. Por tanto, el reto que tendrá ante sí el Grupo de Trabajo consistirá en elaborar un instrumento que no merme u obstaculice la necesidad o la capacidad de un sistema de gestión de la identidad del sector privado de elaborar sus propias reglas de funcionamiento sin dejar de establecer con claridad los requisitos legales que deben satisfacer las reglas de funcionamiento de base contractual.

III. El marco jurídico por el que se rigen los sistemas de gestión de la identidad del sector privado y un posible instrumento de la CNUDMI

A. El marco jurídico general

42. Como requisito previo a la elaboración del tipo de instrumento previsto en el proyecto, creemos que el Grupo de Trabajo debe examinar la estructura del marco jurídico general por el que se rigen los sistemas de gestión de la identidad del sector privado. Específicamente, el Grupo de Trabajo debería examinar cómo encajarían en ese marco tanto i) las reglas de funcionamiento de los distintos sistemas de gestión de la identidad del sector privado como ii) el instrumento de la CNUDMI que se propone. Es un paso importante a fin de determinar las cuestiones que deberían regularse en el instrumento de la CNUDMI.

43. Los sistemas de gestión de la identidad del sector privado, como la mayor parte de los sistemas comerciales multipartitos de operaciones, suelen regirse por un marco jurídico integrado por una combinación de i) derecho de creación estatal y ii) arreglos contractuales de las entidades participantes. El **derecho de creación estatal** está formado por las normas promulgadas como leyes por el poder legislativo, aprobadas como reglamentos por los organismos públicos o establecidas mediante resoluciones judiciales. El **derecho de base contractual** está compuesto por las normas redactadas por uno o más participantes o por los órganos de gobierno del sistema de gestión de la

identidad (las reglas de funcionamiento del sistema de gestión de la identidad), que adquieren carácter vinculante para los participantes en el sistema por contrato.

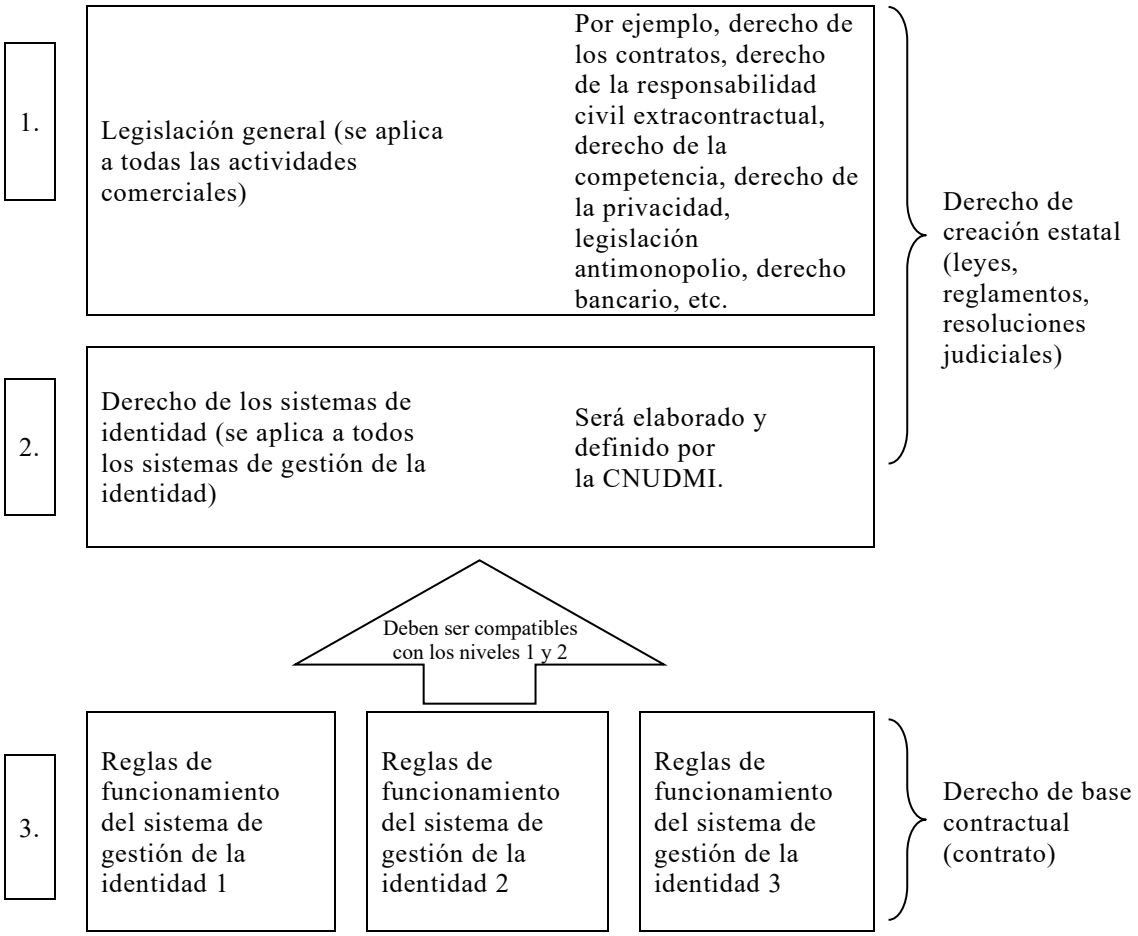
44. El marco jurídico en el que operan los sistemas de gestión de la identidad del sector privado suele constar de tres niveles de derecho, cada uno de los cuales va regulando los sistemas de gestión de la identidad con mayor grado de especificidad. A continuación se describen los tres niveles del marco jurídico (representados en el diagrama que figura en la página siguiente):

- **(Nivel 1) Legislación vigente**: El nivel superior, y el más general, es simplemente la **legislación nacional vigente**. Se trata del derecho de creación estatal, que incluye leyes, reglamentos y resoluciones judiciales. Este derecho regula todos los tipos de actividades comerciales, no fue concebido específicamente para los sistemas de gestión de la identidad y, en algunos casos, puede tener siglos de antigüedad. Sin embargo, resulta aplicable con frecuencia a las actividades de los sistemas de gestión de la identidad del sector privado. En esta categoría quedan comprendidas ramas como el derecho general de los contratos, el derecho de la responsabilidad civil extracontractual, el derecho de la privacidad, el derecho de fiscalización de las exportaciones, el derecho de las garantías, el derecho de protección del consumidor, el derecho de la competencia, el derecho bancario y otras ramas similares.
- **(Nivel 2) Derecho de los sistemas de identidad**: El segundo nivel del marco por el que se rigen los sistemas de gestión de la identidad del sector privado puede denominarse "**derecho de los sistemas de identidad**". Se concibe expresamente para regular ***todos*** los sistemas de gestión de la identidad del sector privado, con independencia del tipo, estructura, tecnología o propósito. El derecho de los sistemas de identidad situado en el nivel 2 también es derecho de creación estatal, está concebido para resolver los problemas que la legislación vigente del nivel 1 ocasiona a todos los sistemas de gestión de la identidad y puede colmar algunas de las lagunas que el derecho del nivel 1 simplemente deja sin regular. Debería encajar entre la legislación vigente, situada en el nivel 1, y las reglas de funcionamiento de base contractual de los distintos sistemas de gestión de la identidad, situadas en el nivel 3.
- **(Nivel 3) Reglas de funcionamiento de los distintos sistemas de gestión de la identidad**: El tercer nivel del derecho por el que se rigen los sistemas de gestión de la identidad del sector privado está formado por las reglas de funcionamiento de base contractual concebidas específicamente por cada sistema de gestión de la identidad del sector privado para regular su propio entorno. A diferencia del derecho de los sistemas de identidad situado en el nivel 2, que se aplica a todos los sistemas de gestión de la identidad, las reglas de funcionamiento del nivel 3 están diseñadas para dar respuesta a los requisitos singulares de un determinado sistema de gestión de la identidad[14]. Estas reglas de funcionamiento pueden ser muy detalladas, pero deben ser compatibles con el derecho situado en el nivel 1 y en el nivel 2.

45. La tarea que tiene ante sí el Grupo de Trabajo consiste en elaborar un instrumento que defina los elementos integrantes del derecho situado en el nivel 2.

[14] Nótese que, en el caso de los sistemas de gestión de la identidad del sector público, como el sistema nacional de identidad, las reglas de funcionamiento específicas del sistema están contenidas en una ley o reglamento. Por tanto, se combinan el derecho del nivel 2 y el derecho del nivel 3.

Figura 1
Marco jurídico de los sistemas de gestión de la identidad del sector privado: tres niveles de derecho



B. ¿Qué debería hacer el instrumento de la CNUDMI?

46. A fin de evitar que se adopte un enfoque único que obstaculice el desarrollo de sistemas de gestión de la identidad del sector privado y las actividades comerciales conexas, el Grupo de Trabajo debería elaborar un instrumento que abordara solo las cuestiones que no puedan regularse en las reglas de funcionamiento de los distintos sistemas de gestión de la identidad. Además, debería limitarse a modificar o complementar la legislación nacional vigente situada en el nivel 1 únicamente en la medida en que fuese necesario para fomentar y promover el desarrollo de sistemas de gestión de la identidad del sector privado a fin de apoyar la actividad comercial en línea. Es decir, debería diseñar un instrumento de nivel 2 que:

- eliminara las barreras y la inseguridad derivadas de la legislación vigente del nivel 1 que obstaculizan el desarrollo de sistemas de gestión de la identidad del sector privado;
- colmara las lagunas de la legislación vigente del nivel 1 que son importantes para el éxito de los sistemas de gestión de la identidad del sector privado pero que no pueden resolverse por contrato; y
- regulara nuevas cuestiones de aplicación universal a fin de promover el desarrollo de todos los sistemas de gestión de la identidad del sector privado.

47. Asimismo, dada la variedad que presentan los sistemas de gestión de la identidad y las necesidades particulares de cada uno, el instrumento de nivel 2 que elabore el Grupo de Trabajo debería respetar los principios de neutralidad tecnológica y de

neutralidad del sistema de identidad. En particular, la neutralidad del sistema de identidad es imprescindible en vista de la diversidad de estructuras, tecnologías, propósitos y mercados utilizados por los sistemas de gestión de la identidad del sector privado que se ha señalado anteriormente.

48. En cambio, el proyecto está concebido de tal manera que impone reglas en materia de *obligaciones de los proveedores de servicios de gestión de la identidad* (art. 6), *obligaciones de los proveedores de servicios de gestión de la identidad en caso de violación de los datos* (art. 7), *obligaciones de los abonados* (art. 8) o *responsabilidad de los proveedores de servicios de gestión de la identidad* (art. 12). Los sistemas de gestión de la identidad del sector privado tienen que resolver estas cuestiones en sus particulares reglas de funcionamiento. Cada una de esas cuestiones requerirá un enfoque propio adaptado a la estructura, la tecnología, el propósito y el mercado implicado de cada uno de los sistemas de gestión de la identidad. Cualquier intento de regular cuestiones como las anteriores será problemático porque es probable que estas varíen considerablemente de un sistema a otro, y la imposición de un enfoque único para todos los sistemas tan solo logrará que se obstaculice el desarrollo de sistemas de gestión de la identidad del sector privado.

C. Esquema general del instrumento de la CNUDMI

49. En cambio, las cuestiones que podría abordar el Grupo de Trabajo se agrupan en las siguientes categorías[15]:

- el reconocimiento explícito del papel de las reglas de funcionamiento en la gobernanza del sistema de gestión de la identidad;
- las cuestiones que no están contempladas en la legislación vigente del nivel 1 que, por su naturaleza, no pueden ser reguladas en reglas de funcionamiento de base contractual. Se pueden citar, entre otros, estos ejemplos:
    - el reconocimiento jurídico de un sistema de gestión de la identidad[16];
    - los requisitos para determinar los casos en que una operación de identidad satisface las condiciones legales aplicables para identificar a alguien[17];
    - la conveniencia de evaluar la fiabilidad de los sistemas de gestión de la identidad del sector privado y el modo de hacerlo si fuera conveniente[18];
- las cuestiones contempladas hasta cierto punto en la legislación vigente situada en el nivel 1 pero de aplicabilidad incierta a los sistemas de gestión de la identidad, de modo que se crea una ambigüedad que puede suponer un problema para los sistemas en razón de la dificultad para regularlas en las reglas de funcionamiento de base contractual. Se pueden citar, entre otros, estos ejemplos:
    - la aplicabilidad del derecho vigente en materia de responsabilidad civil extracontractual a los participantes en los sistemas de gestión de la identidad;
    - la aplicabilidad del derecho de la falsedad negligente;
    - la aplicabilidad del derecho vigente en materia de garantías implícitas;

[15] Esta categorización se presenta a modo de lista preliminar de cuestiones que se podrían abordar en un instrumento de nivel 2, abierta a las ampliaciones y modificaciones que pudiera hacer el Grupo de Trabajo, sobre la base de las necesidades de los diversos regímenes nacionales existentes, entre otros factores.

[16] El art. 5 del proyecto pretende regular esta cuestión. Véanse nuestros comentarios sobre los problemas que plantea la redacción actual del art. 5 en el apéndice.

[17] El art. 9 del proyecto pretende regular esta cuestión. Véanse nuestros comentarios sobre los problemas que plantea la redacción actual del art. 9 en el apéndice.

[18] El art. 11 del proyecto pretende regular esta cuestión. Véanse nuestros comentarios sobre los problemas que plantea la redacción actual del art. 11 en el apéndice.

- las cuestiones que tal vez deban añadirse a la legislación vigente, como las que tratan sobre estos aspectos:
    - el derecho de los sistemas de gestión de la identidad a utilizar la información procedente de los sistemas de gestión de la identidad de las administraciones;
    - el derecho de los sistemas de gestión de la identidad a utilizar los identificadores emitidos por las administraciones (por ejemplo, número de la seguridad social, número de identificación nacional, etc.);
- las cuestiones que, con independencia de que se pudieran regular en reglas de funcionamiento de base contractual, deberían tener la misma regulación en todos los sistemas de gestión de la identidad en razón de consideraciones de orden público, como las siguientes:
    - la conveniencia de que esté previsto el reconocimiento transfronterizo y el modo de hacerlo si fuera conveniente[19];
    - la conveniencia de abordar la fiabilidad desde la perspectiva legal y el modo de hacerlo si fuera conveniente[20].

50. Un instrumento de la CNUDMI que contenga estos elementos ayudará a los Estados a conformar un derecho de los sistemas de identidad de nivel 2 diseñado para 1) fomentar el desarrollo de sistemas de gestión de la identidad del sector privado, 2) eliminar las barreras a ese desarrollo y 3) respetar y respaldar la necesidad que tiene cada uno de los sistemas de gestión de la identidad del sector privado de elaborar sus propias reglas de funcionamiento en la medida de lo posible.

[19] Los arts. 10 y 11 del proyecto pretenden regular esta cuestión. Véanse nuestros comentarios sobre los problemas que plantea la redacción actual de los arts. 10 y 11 en el apéndice.

[20] Los arts. 10 y 11 del proyecto pretenden regular esta cuestión. Véanse nuestros comentarios sobre los problemas que plantea la redacción actual de los arts. 10 y 11 en el apéndice.

Appendix[21]

Article-by Article Analysis of WP.162

In this appendix to our comments, we provide a detailed article-by-article commentary on WP 162. We reiterate, though, that we do not believe that a simple set of revisions to the text of WP 162 will result in a viable instrument. To achieve this, we believe the Working Group must make the conceptual and structural changes required to address the current reality of IdM systems that we set forth in Sections II and III of our comments.

Before turning to the article-by-article analysis, here is a summary of the U.S. concerns with WP.162:

(a) The definitions in WP 162 are both incomplete and based on a static model for IdM that is not reflective of the wide variety of actual IdM systems;

(b) WP.162 does not provide a basis for determining how and when the instrument would accede to or supersede existing laws that require identification in a specific form. The failure to provide guidance on this issue is compounded by the fact that articles 2, 5 and 9 contradict one another;

(c) The articles on obligations (art. 6–8) and liability (art 12) do not reflect the wide variations among types of IdM systems nor the multiple types of roles that may make up any specific IdM system. These one-size-fits all provisions do not accurately reflect the rights and obligations that different IdM system roles may have or expect in various IdM systems;

(d) We do not believe the provisions on cross-border recognition are workable without an enacting jurisdiction having some basis for assuming the reliability of a system in another jurisdiction. We do not believe this obligation is realistic.

Draft Article 1: Definitions

We believe the Working Group should revisit the definitions after the articles in the rest of the draft are concluded. Base on the current draft,[22] we make the following observations for consideration by the Working Group.

The term “electronic identification” may describe or be easily confused with the entire process of identity proofing, credential issuance, and authenticating the relationship between the credential data and an individual. Thus, we recommended that the Working Group consider whether there is an alternative term to “electronic identification” that could be used for the authentication process.

All the stages of the IdM process might collectively be defined as “identity verification.” The modifier “electronic” should not be used in this definition, however, since all or part of the stages of the IdM process might not be done electronically.

“Authentication” is used only in terms of trust services; it has the same meaning as “electronic identification”. We believe it could be misleading to have two terms for the same concept and would recommend using the same term for this concept throughout the draft. As noted above, however, we believe the term “electronic identification” itself may be misleading.

As to the secretariat’s inquiry whether there should be a definition of levels of assurance, we believe such a definition is unnecessary. We note the secretariat’s proposed language provides that “identification factors are those factors that are necessary to make an

[21] The Appendix has been provided to Member States in English only. However, significant portions of the substance of the Appendix are a reproduction of the U.S. response to the Secretariat’s questionnaire for A/CN.9/WG.IV/WP.162, which has been circulated in all official languages as A/CN.9/WG.IV/WP.164 and Add.1.

[22] A/CN.9/WG.IV/WP.162.

electronic identification" In other words, the proposed definition does not provide any guidance; it simply restates the obvious. Moreover, we believe this proposed language could cause confusion, as it implies that there are specific factors that an IdM service provider must manage. Depending on the nature of the identity system involved, there could be numerous such factors. The relevant factors, however, will vary from IdM system to IdM system, and the responsibility for managing these factors will vary from system role to system role.[23] We note also that the proposed definition appears to combine two very different concepts: identity attributes (that vary depending on purpose for which identity is used), and identity processes that are used for identity proofing, credential issuance, or authentication processes.

Draft Article 2: Scope of application

The draft instrument provides that it "applies to the use and cross border recognition of IdM systems and trust services in the context of commercial activities and trade related services." As we discuss below, we believe the Working Group needs to closely examine how the draft instrument will apply to cross-border transactions, and how the rules in this instrument relate to existing legal requirements regarding identification and authentication.

Draft article 2(3) provides that "[n]othing in this [instrument] affects a legal requirement that a [subject][person] be identified in accordance with a procedure defined or prescribed by law." We understand this exclusion as being necessary as most if not all jurisdictions have some mandatory requirements for the form in which identification is to be made.

The question then is whether this section can be reconciled with articles 5(a), which provides that "The electronic identification of a [subject][person] shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that …[t]he identity proofing and electronic identification are in electronic form" and article 9(1) option A, which provides that " Where a rule of law requires or permits the identification of a [subject][person], that rule is satisfied with respect to IdM if a reliable method is used for the electronic identification of the [subject][person]."

We believe article 2(3) and article 5(a) might be reconciled by expressly clarifying these two sections to indicate that article 5(a) is not intended to overrule any other law, but is only intended to provide that, as between the parties, the law will not block the choice of the parties to use an electronic means of identification if the law would otherwise allow this under freedom of contract. This reading would appear to narrow the scope of article 5, and if the Working Group intended article 5 to have this limited meaning, this needs to be clarified in the text and comments.

We do find a more serious problem reconciling draft article 2(3) with draft article 9(1) Option A. These two sections, we believe, cannot be reconciled. Were the instrument intended to supersede all laws that may require a specific mode of identification, the instrument would risk being non-enactable. In addition, this interpretation would expressly contradict the language of draft article 2(3). In our view, the draft instrument provides contradictory rules: electronic identification meets the requirements of other legal identification requirements, and the instrument does not displace any other legal identification requirements. These conflicting rules cannot co-exist if the draft instrument. We view Option B of draft article 9 as essentially restating the rule of Option A. We believe the Working Group must re-examine these draft articles and reformulate them to express a non-contradictory policy that respects the existing legal requirements that are recognized in draft article 2(3).

[23] This potential confusion raises the issue of whether draft article 6 may itself create minimum obligations that should not necessarily apply to all IDM service providers. In other words, article 6 may assume a one size fits all IDM service provider that does not reflect the multitude of existing and developing models.

Draft Article 3: Voluntary use of IdM and trust services

We believe both the current text of the draft[24] as well as the proposed new language by the secretariat[25] shows confusion on the role of consent. We suggest the Working Group examine the rule on consent to determine which parties are required to consent and the relationship between article 3 on consent and how it works with both article 2 and 5 on freedom or lack of freedom to choose the mode of identity management.

Draft Article 4: Interpretation

Although we appreciate that this language has appeared in prior model laws,[26] we note this language was drawn from the United Nations Convention on Contracts for the International Sale of Goods,[27] and it is language specifically tailored for an international convention. As such, we are not sure that it is appropriate for a model law that is drafted for domestic legislation.

Thus, for example, we are not clear on what the "international character" of the draft model law refers to. As the draft instrument is neither derived from international instrument nor intended to be used primarily in international transactions, we do not know what constitutes the instrument's "international character".

Moreover, although uniformity of interpretation is a useful admonition for an international convention, [28] the utility of this interpretive rule is not clear in an instrument designed for domestic legislation. When, as with an international convention, an autonomous interpretation is useful to create a universal understanding that parties can rely upon in international commercial transactions, the application of this rule is unclear and probably redundant for a domestic law.

As for the rule that the instrument should be interpreted on the general principles on which it is based,[29] we suggest that either the draft provide the guidance of what these principles are[30] or this rule should be removed. To do otherwise creates the risk of vagueness and uncertainty in the text.[31]

Draft Article 5: Legal recognition of IdM

As we discussed above in our analysis of draft Article 2, we believe the Working Group needs to clarify how this rule is intended to work with identifications that are required to be in a specific form such as a driver's license or passport.

---

[24] A/CN.9/WG.IV/WP.162, draft article 3.

[25] "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. "?".

[26] UNCITRAL Model Law on Electronic Commerce (1996), article 3; UNCITRAL Model Law on Electronic Signatures (2001), article 4.

[27] United Nations Convention on Contracts for the International Sale of Goods (1980), article 7.

[28] We note this language is also derived from the CISG.

[29] A/CN.9/WG.IV/WP.162, footnote 23.

[30] We note that a statement of underlying principles was removed from the last draft.

[31] The Working Group may want to consider the comments of the World Bank in WP.163 to ensure that the Draft Provisions do not discriminate among IdM system models by including the concept of IdM system neutrality (or identity transaction neutrality). Because there are many different ways of conducting online identity transactions (e.g., single identity provider (IdP) systems, federated (multiple IdP) systems, user controlled/user centric systems, hub systems, DLT systems, systems without credentials, self-sovereign identity systems, etc.), it is important that these Draft Provisions do not require or assume a particular approach to the identification and/or authentication processes, or the system that delivers them. Thus, the Working Group should consider ways to ensure that these Draft Provisions do not imply and/or require a certain system model.

Draft Article 6: Obligations of IdM service providers

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

As noted in the World Bank's comments,[32] the obligations set out in draft article 6 for IdM service providers assume a model where the IdM service provider provides all the services. This may not always be the case. There could be several parties that contribute to or provide part of an IdM service (e.g., trust providers, registrars, enrolment agents, credential service providers, stewards, authentication providers, hubs, etc.). Given the increasing diversity of IdM system models, the Working Group should consider whether it is still appropriate to restrict the definition of the roles or to impose a one-size-fits-all set of IdM service provider obligations. We believe the Working Group needs to address article 6 to consider the potential multiple parties that may contribute to the IdM service, and to consider whether it is still appropriate to impose a one-size-fits-all set of IdM service provider obligations.

Draft Article 7: Obligation of IdM service providers where there is a breach

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems. We agree that there should be some obligations by an IdM service provider where there has been a breach of security. As we noted note our comments to draft article 6, however, there may be multiple parties involved in the IdM service provider process.[33] For this reason, we believe the Working Group should reconsider the language of draft article 7 to reflect the various parties that may be involved in IdM process and accordingly fix the obligations based on the respective nature and status of these parties consistent with which party is best placed to respond to the breach.

Draft article 7 is limited to breaches that have "a significant impact". We do not understand what "significant impact" means in this context. In addition to being a vague standard, we are not sure why a "breach" is not enough in and of itself to justify some remedial action by the entity that bore the risk the breach.

We are not sure what "remedies" are or should be available where there has been a breach of security.[34] We believe the Working Group should clarify this issue.

We do not know what "applicable law" refers to in 7(1)(c). If it refers to a notification obligation from the draft instrument, this obligation should be referred to. If this refers to law outside of the instrument, it is not clear what law would impose an obligation of notification.

[32] A/CN.9/WG.IV/WP.163.

[33] We agree with the comments by the World Bank in WP.163 that the current draft compresses and confuses the distinction between and the respective roles of IdM systems and IDM service providers.

[34] See Draft article 7(1)(b).

Draft Article 8: Obligation of subscribers

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

We agree with the comments by the World Bank that the duties imposed on subscribers (particularly individuals, such as data subjects) in Article 8 may not be reasonable in all circumstances.[35] For example, there may be situations where an individual subscriber may be aware of circumstances indicating there may have been a compromise, but simply does not understand their significance.

We believe Article 8 should be clarified that it is not intended to impose these duties on relying third parties that have no contractual relationship with the issuing IdM service provider but who may nonetheless rely on a credential because:

(a) it would be difficult to enforce as it will likely be hard to identify such relying third parties;

(b) it imposes an undue burden on relying third parties to police identity system credentials for an IdM service provider with whom they have no relationship; especially when their use of and reliance on such credentials may be sporadic at best; and

(c) it is not currently required by law applicable to paper-based credentials (e.g., the bartender who refuses entry to a person because he determines that the person has presented a false driver's license or someone else's driver's license is not required to report that to the issuing authority).[36]

The requirement to notify in cases of a "substantial" risk seems problematic, as subscribers will likely have no way of knowing (and in most cases will not even be qualified to determine) what constitutes a substantial risk as opposed to some lesser risk.

Draft Article 9: Identification of a person using IdM

We address our concerns on draft article 9 in our discussion of draft article 2 above.

Draft Article 10: Factors relevant in determining reliability

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

Draft article 10 provides an illustrative list of factors to determine the reliability of an IdM service. If article 10 only applies to systems governed by contractual rules, it is not clear what the purpose of the list of possible considerations serve. This list is not useful to explain and interpret an otherwise applicable contractual agreement. If draft article

[35] A/CN.9/WG.IV/WP.163.

[36] We also agree with the comments by the World Bank in WP.163 that if the draft is going to raise issues about third parties, more clarification would be useful as to which third parties are envisaged. We also note that if there is going to be a notification requirement on non-contracting parties, there needs to be some sanction for failure to notify, as otherwise the requirement is meaningless.

10 is intended to provide a minimal standard of reliability for IdM systems, then it is not clear how an illustrative and not a mandatory list would operate.

Moreover, it is not clear how this would override, if at all, otherwise agreed to contractual standards.

Moreover, in any given situation, there are numerous factors that may affect reliability. We question whether attempting to list them in these rules is appropriate in any event.

Draft Article 11: Designation of reliable IdM systems

Although this provision is made optional, as we note in our analysis of draft article 24, this section may impose quite a financial and administrative burden to implement by a jurisdiction that adopts this instrument. We recommend to the Working Group that this provision be bracketed with extensive commentary to explain how similar provisions have been implemented elsewhere and what an implementation would entail.

In addition, we believe this provision, as presently drafted, rests on the flawed assumptions that there are "recognized international standards and procedures" for determining the reliability of a IdM service, and that there is a centralized body that can make these determinations.

Draft Article 12: Liability of IdM service providers

As noted in Section III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

We do not believe any of the three options in the current draft are sufficient. Both Options A and B state, albeit unartfully, that an IdM service provider will be legally responsible under otherwise applicable law outside of this instrument. If liability rules are to be included in this instrument, some guidance would be necessary. The term "applicable law" is vague. Does this refer to contract law, tort law, privacy law, data security law, etc. or all of them? If the answer is it could apply to any law otherwise deemed to be appropriate, then no function is served by this provision. Likewise, we have no idea what type of guidance is intended by the phrase "legal consequences".

The word "damage" in option 3 we assume means "harm", but as with all the options in the current draft, we fear no real guidance or standards are provided.

We suggest that the rules governing liability should likely vary depending upon the nature of the identity system, and will most likely to be determined by the applicable trust framework (subject, of course, to any existing law that cannot be varied by agreement).

At a minimum, we believe a further discussion is warranted on what type of liability the rules of the draft would invoke. We think a discussion of liability should go beyond service providers and consider liability for all parties that may come within the scope of the draft. We also believe that a discussion on contractual waivers to liability should be included in any discussion on liability. Further, as noted above, we do not believe that a universal one-size-fits-all approach to liability is appropriate in any event, as identity systems, their purposes, and their participants will vary widely.

Draft Article 13: Legal recognition of trust services

As we have noted, we believe trust services should be addressed in a separate instrument.

This provision states that a trust service may be provided in electronic form. As the purpose of a trust service is, in fact, to verify electronic data, this provision would appear to be tautological and unnecessary. If the intent of draft article 13 is to make clear that a third party may provide a trust service, that should be clarified.

Draft Article 14: Obligations of trust service providers

As a conceptual matter, this draft provision raises two questions. First, how does this provision interact with contractual obligations that a trust service provider may have to remedy a breach of loss of integrity? If the intent of Article 14(2) is to impose obligations for breaches or losses of integrity that are not covered by contract (i.e., because it refers to impact on the trust service itself), this should be made clear.

If the intent is to impose some minimal obligation on trust service providers below which the parties cannot contract, this should be expressly stated. If that is the intent, we believe the Working Group should address the question of mandatory rules and their relationship to freedom of contract.

A second question unexamined in this draft provision is the question of the consequence for failing to meet the obligations set out in Article 14? If a trust service provider fails to fulfil a contractual obligation owed to a customer, then customer/other party to the contract could pursue a contract claim. Article 14 does not appear to impose any consequences or sanction for failure to fulfil the obligations set out therein, assuming they are distinct from contractual obligations.

Draft Article 15: Obligations of trust service providers

This draft article, as with draft article 14, purports to impose obligations without any corresponding sanctions. As we mentioned in our comments to draft article 12, we believe the Working Group needs to examine fully the question of liability throughout the draft instrument.

Draft Articles 16–20: Various trust services

Articles 16–20 address the issue of the validity of a data message (such as an e-signature) and not the use of a trust service to validate the data message. In some cases, such as with e-signature, there is already existing law that governs the validity of the data message itself (this was the subject of the United Nations Convention on the Use of Electronic Communications in International Contracts and the UNCITRAL Model Law on Electronic Signatures). But in any event, because these provisions are not concerned with trust services, they do not belong in this instrument.

Draft Article 21: Website authentication

As drafted, article 21 appears to confuse the authenticity of the website, which is the true concern, with the owner of the domain, which does not prove the authenticity of website itself. We believe the Working Group should reconsider this draft article to provide a rule that achieves its intended purpose.

Draft Article 22: Identification of objects

We do not believe the identification of objects should be covered in the draft. We also note that given the limited scope of trust services in the draft, that being to verify information (data messages), the identification of objects is more appropriately covered in the provisions on identity management and not trust services.

Draft Article 23: Reliability standards for trust service providers

While Art. 23(1) lists the contractual agreement involving a trust service provider as one of the factors among others to weigh in determining reliability, it is unclear how that should be weighed relative to the other factors listed or how these standards interact with contractual agreements. As contract underlies trust service relationships, we believe this is an essential clarification that the Working Group should explore.

Draft Article 24: Designation of reliable trust services

Although this provision is made optional, as we have noted in our analysis of draft article 11, this section may impose quite a financial and administrative burden to implement by a jurisdiction that adopts this instrument. We recommend to the Working Group that this provision be bracketed with extensive commentary to explain how similar provisions have been implemented elsewhere and what an implementation would entail.

As we noted with our analysis of draft article 11, this provision ought to be reconsidered as it rests on flawed assumptions. These assumptions include, for example, that there are "recognized international standards and procedures" for determining the reliability of a trust service, and that there is a centralized body that can make these determinations. Moreover, while Art. 23(1) lists the contractual agreement involving a trust service provider as one of the factors among others to weigh in determining reliability, it is unclear how that should be weighed relative to the other factors listed or how these standards interact altogether with contractual agreements.

Draft Article 25: Liability for trust service providers

We think this section needs to be reconsidered. Option A, which leaves liability to otherwise applicable law, should be clarified to state whether it includes both contact and torts, and if it includes contractual liability, the extent to which, if at all, the liability may be excluded. As with our concerns with Option A, we believe Option B is too vague because we are not sure what the scope of "legal consequences" entails. Option C provides tort liability but leaves open the question of contract responsibility. This should be clarified. We note we expressed similar concerns with the current drat of Article 12.

Draft Article 26(1): International aspects of the draft law

Given that modern commercial transactions often transcend national borders, we believe cross- border recognition is an admirable and hopefully achievable goal in this and any commercial law instrument. We are concerned, however, that the current draft does not provide adequate standards and guidance to achieve this goal.

Draft article 26(1) provides that: "An IdM system operated or a trust service provided outside [the enacting State] shall have the same legal effect in [the enacting State] as an IdM system operated or a trust service provided in [the enacting State] if it offers a substantially equivalent level of reliability." We believe this raises two issues that we believe deserve consideration by the Working Group.

First, the language of draft article 26(1) is derived from article 12 of the UNCITRAL Model Law on Electronic Signatures.[37] However these two articles serve significantly different functions. Article 12 of the MLES provides for non-discrimination of a certification service provider that verifies the public key of a PKI transaction. This quite limited function allows parties to choose a third-party certification provider to verify the authenticity of a signature between two parties who have chosen the third-party certifying provider. This is a simple application of freedom of contract.

[37] UNCITRAL Model Law on Electronic Signatures (2001), article 12.

Unlike article 12 of the MLES, draft Model Law article 26 would impose an obligation on all parties who rely on IDM systems and trust service providers that reside in other jurisdictions without these relying parties necessarily having the ability to choose the providers and therefore evaluate the risks attendant to the choice of a specific provider. These third parties in reliance on the IDM and trust services systems would not normally have any power to choose the providers and therefore would have to rely on assurances of providers outside the jurisdiction of the enacting state.

It is this broader scope of application of draft article 26 that suggests that article 12 of the MLES may not be the appropriate rule for IDM and trust services.

The second concern we have is whether the standard of "substantial equivalent level of reliability" (also taken from article 12 of the MLES) is either meaningful or realistic. The language itself is vague, but more importantly this standard raises a fact question that would be burdensome and expensive to prove or disprove. To meet the standard, a party would have to show both the level of reliability of the domestic system as well as the level of reliability the non-domestic system and then make some qualitative judgment on substantial equivalence. This, we believe would be unduly burdensome for parties.

We note that, for example, the recognition of foreign IDM and trust service providers under eIDAS requires an extensive and complex verification process in which each respective country in the European Union participates. This provides a level of reliability and certainty that minimizes the risks for parties relying on a non-domestic system. Thus, under the eIDAS, the "substantial equivalence" has already been established for parties relying on any respective system within the European Union. Outside such a closed system such as eIDAS, the burden on parties to prove or disprove "substantial equivalence" would itself be substantial. We think it is important to note that this is not primarily a legal but is a factual and technological question that is not easily resolved by a vague legal mandate.

This issue of "substantial equivalence" is further complicated, we believe, because what parties that use IDM and trust service systems understand about the systems is often quite different from the underlying technological structure of those systems. Most parties who must rely on IDM and trust services are not in a position to evaluate the reliability of the systems, and therefore the parties must assume reliability with the knowledge that if the systems are certified and responsible under the domestic law, the parties will have recourse under the domestic law in the case of failure. But where the domestic law, as in draft article 26 only provides protection to parties if the parties can show "substantial equivalence" of a foreign system.

Draft Article 26(2): International aspects of the draft law

Draft article 26(2) provides that "recognized international standards' shall be used to determine "substantial equivalence". We appreciate the aspirational nature of this provision. We believe, however, before adopting this provision, which was borrowed from article 12(4) of the MLES, this provision should be further discussed by the working group to determine its applicability to the draft law. We see two points which should be discussed. First, we are not certain at this time that there are generally recognized international standards in this evolving area of the law and technology. At best, we believe that the rule should also provide for evolving standards as a basis for determining equivalence. Guidance would be most useful in how these standards should be determined. Moreover, irrespective of the standard, we note that this involves a factual issue of technological reliability that creates a substantial burden on parties to prove what "international standards" are.

Draft article 27: International Aspects of the Draft Law

We find article 27 an admirable but possibly impractical rule as may place a burden on the enacting states of significant obligations to coordinate and cooperate with foreign entities. We would not want to discourage this cooperation, but merely to ensure that it is optional and not mandatory. Legislation that creates a significant financial burden on the state often creates an impediment to adoption. This section risks posing a financial burden on the governments of jurisdictions that adopt this law that go shifts the risks of using foreign IDM and trust services providers on the respective governments instead of the private parties that choose to use these systems.

Although this may be a useful and possibly mandatory provision in a law that is designed to provide government created or recognized IDM or trust services that may be used in cross-border transactions, we are not convinced that this burden on governments is not excessive for the draft law that is designed for privates users and private providers.

We suggest that if this provision is retained, it be placed in brackets with commentary that explains fully the obligations this article would impose on the enacting jurisdiction. We suggest this article be optional for those states that have or would be willing to develop the cooperative framework necessary to implement this article.