Naciones Unidas A/CN.9/WG.IV/WP.150

Asamblea General

Distr. limitada
6 de febrero de 2018
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
56º período de sesiones
Nueva York, 16 a 20 de abril de 2018

Cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza

Términos y conceptos relativos a la gestión de la identidad y los servicios de confianza

Nota de la Secretaría

Índice

Página

I. Introducción 2
I. Términos y conceptos relativos a la gestión de la identidad y los servicios de confianza 3
A. Definiciones pertinentes para la gestión de la identidad 3
B. Definiciones pertinentes para los servicios de confianza 10

V.18-00560 (S) 190218 190218

Se ruega reciclar

I. Introducción

1. En su 48º período de sesiones, celebrado en 2015, la Comisión encargó a la Secretaría que llevase a cabo una labor preparatoria en relación con la gestión de la identidad y los servicios de confianza, la computación en la nube y el comercio móvil, entre otras cosas mediante la organización de coloquios y reuniones de grupos de expertos, para que el Grupo de Trabajo la examinase en un futuro. La Comisión también pidió a la Secretaría que informara al Grupo de Trabajo IV de los resultados de esa labor preparatoria, con miras a obtener recomendaciones sobre el alcance exacto, la posible metodología y las prioridades que se someterían a consideración de la Comisión en su 49º período de sesiones[1].

2. En su 49º período de sesiones, celebrado en 2016, la Comisión tuvo ante sí una nota de la Secretaría sobre los aspectos jurídicos relacionados con la gestión de la identidad y los servicios de confianza (A/CN.9/891), en la que se resumían las deliberaciones mantenidas durante el Coloquio de la CNUDMI sobre las cuestiones jurídicas relacionadas con la gestión de la identidad y los servicios de confianza, celebrado en Viena los días 21 y 22 de abril de 2016, y otro material complementario. También se informó a la Comisión de que se había comenzado a trabajar a nivel de expertos en lo relativo a los aspectos contractuales de la computación en la nube, sobre la base de una propuesta (A/CN.9/856) presentada en el 48º período de sesiones de la Comisión, en 2015.

3. En ese período de sesiones la Comisión convino en que los temas de la gestión de la identidad y los servicios de confianza, así como el de la computación en la nube, siguieran figurando en el programa de trabajo, y que sería prematuro asignar prioridad a uno antes que al otro. La Comisión confirmó su decisión de autorizar al Grupo de Trabajo a que comenzara a examinar esos temas una vez que hubiese finalizado su labor relativa a la ley modelo sobre los documentos transmisibles electrónicos. En ese contexto, se pidió a la Secretaría, siempre y cuando dispusiera de los recursos necesarios, y al Grupo de Trabajo que prosiguieran la labor preparatoria y de actualización sobre ambos temas, incluso en cuanto a la viabilidad de abordarlos en forma paralela y flexible, y que presentaran un informe a la Comisión para que esta pudiera adoptar una decisión fundamentada en un futuro período de sesiones, incluso con respecto a la prioridad que habría de darse a cada tema[2].

4. En su 50º período de sesiones, celebrado en 2017, la Comisión, tras deliberar, reafirmó el mandato que había encomendado al Grupo de Trabajo en su 49º período de sesiones, celebrado en 2016 (véase el párr. 3 *supra*). Decidió reexaminar ese mandato en su 51er período de sesiones, en particular si surgía la necesidad de establecer prioridades entre los temas o de otorgar un mandato más específico al Grupo de Trabajo sobre su labor en la esfera de la gestión de la identidad y los servicios de confianza[3].

5. En su 55º período de sesiones (Nueva York, 24 a 28 de abril de 2017), el Grupo de Trabajo tuvo ante sí una nota en la que se enumeraban términos y conceptos pertinentes para el examen de la gestión de la identidad y los servicios de confianza (A/CN.9/WG.IV/WP.143). En ese período de sesiones el Grupo de Trabajo pidió a la Secretaría que revisara esa nota e incluyera las definiciones y los conceptos que figuraban en el párrafo 20 del documento A/CN.9/WG.IV/WP.144[4].

6. En la presente nota figuran las definiciones de algunos términos relacionados con la gestión de la identidad y los servicios de confianza. Los términos se presentan con miras a facilitar un debate basado en el entendimiento común de los conceptos fundamentales, y no con el fin de proponer que se examinen definiciones jurídicamente vinculantes de esos conceptos. Del mismo modo, los términos no pretenden indicar el

[1] *Documentos Oficiales de la Asamblea General, septuagésimo período de sesiones, Suplemento núm. 17* (A/70/17), párr. 358.
[2] *Ibid., septuagésimo primer período de sesiones, Suplemento núm. 17* (A/71/17), párr. 229.
[3] *Ibid., septuagésimo segundo período de sesiones, Suplemento núm. 17* (A/72/17), párr. 127.
[4] A/CN.9/902, párr. 92.

alcance que debería tener la labor futura de la CNUDMI en la esfera de la gestión de la identidad y los servicios de confianza.

7. Las fuentes de los términos definidos, si se conocen, se indican expresamente. Dado que existen diversas fuentes, un mismo término puede tener más de una definición. Si no se indica ninguna fuente, la definición fue sugerida durante las consultas mantenidas con los expertos. Se ha dado preferencia a los términos definidos a nivel internacional. Existen otras fuentes de los términos definidos, especialmente a nivel nacional.

8. Los términos definidos se enumeran en distintas secciones para facilitar su presentación y sin perjuicio de lo que pueda resolver el Grupo de Trabajo en cuanto a su pertinencia para las deliberaciones sobre los aspectos jurídicos de la gestión de la identidad o los servicios de confianza.

9. Los términos definidos tienen orígenes diferentes y, por tanto, no deben leerse como un conjunto coherente de términos interrelacionados. Más bien, cada término debe leerse por separado como una definición independiente y, como tal, se presenta como una posible referencia para las deliberaciones del Grupo de Trabajo. Cuando se conoce la fuente de los términos definidos, se indica para que pueda obtenerse más información del documento original.

10. Los sinónimos se indican solamente por una cuestión de conveniencia, en razón de su uso. No todos los sinónimos son términos definidos en esta nota.

11. Los términos se enumeran en orden alfabético en la versión en inglés de esta nota. Ese mismo orden se mantiene en las versiones en los demás idiomas, para que haya correspondencia entre los párrafos y facilitar así las referencias durante las deliberaciones del Grupo de Trabajo.

II. Términos y conceptos relativos a la gestión de la identidad y los servicios de confianza

A. Definiciones pertinentes para la gestión de la identidad

12. Por “nivel de garantía” (*assurance level*) se entiende el nivel de confianza en la vinculación entre una entidad y la información de identidad presentada. Fuente: Recomendación UIT-T X.1252. Sinónimo: garantía de identidad; nivel de seguridad.

13. Por “atributo” (*attribute*) se entiende un elemento de información o datos asociados a un sujeto. Ejemplos de atributos son, en el caso de una persona física, información como el nombre, la dirección, la edad, el sexo, el cargo, el sueldo, el patrimonio neto, el número de la licencia de conducir, el número de seguridad social, la dirección de correo electrónico, el número de teléfono móvil y datos como la presencia del sujeto en la red, el dispositivo utilizado por el sujeto, el domicilio habitual del sujeto tal como figure en una red, etc.; en el caso de una persona jurídica, su denominación oficial, el domicilio de la sede principal, el nombre con el que está registrada, la jurisdicción en la que está inscrita, etc.; y, en el caso de un dispositivo, la marca y el modelo, el número de serie, la ubicación, la capacidad, el tipo de dispositivo, etc. Sinónimo: atributo de identidad.

14. Por “proveedor de atributos” (*attribute provider*) se entiende una empresa o un organismo público que actúa como fuente de uno o más de los atributos de identidad de un sujeto. Un proveedor de atributos suele ser la entidad responsable de asignar, recopilar o mantener dichos atributos. Como ejemplos de proveedores de atributos cabe citar un organismo público que lleve un registro de nacimientos o un registro de la propiedad, una agencia nacional de información sobre solvencia crediticia, una empresa que lleve una base de datos de comercialización o un registro de sociedades, y entidades como operadores de telefonía móvil, bancos, empresas de servicios públicos y proveedores de servicios de salud que poseen datos verificados de los usuarios y que

verifican o proporcionan esos atributos a terceros (posiblemente, a condición de que el usuario preste su consentimiento).

15. Por “autenticación” (*authentication*) se entiende: a) el proceso utilizado para obtener una confianza suficiente en la vinculación entre la entidad y la identidad presentada. Fuente: Recomendación UIT-T X.1252; b) el proceso de asociar la identidad declarada por un sujeto con el sujeto real, mediante la confirmación de la asociación del sujeto con una credencial, ya sea directamente (autenticación activa) o a través del entorno en que el sujeto está interactuando (“autenticación pasiva” o “autenticación adaptativa”). Por ejemplo, se supone que cuando se introduce una contraseña secreta asociada a un nombre de usuario se confirma que la persona que introduce la contraseña secreta es la persona a quien se asignó el nombre de usuario. Del mismo modo, se compara el aspecto de una persona que presenta un pasaporte con la fotografía que aparece en este para autenticar (es decir, confirmar) que esa persona es la persona descrita en el pasaporte; c) el proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico. Fuente: Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (“eIDAS”), artículo 3, párrafo 5. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

16. Por “garantía de autenticación” (*authentication assurance*) se entiende el grado de confianza al que se llega en el proceso de autenticación en que el asociado de la comunicación es la entidad que declara ser o se espera que sea. Nota: La confianza se basa en el grado de confianza de la relación entre la entidad que comunica y la entidad que está presente. Fuente: Recomendación UIT-T X.1252. Nota: En algunos casos, los conceptos de “garantía de identidad” y “garantía de autenticación” se consideran componentes independientes del concepto general de “nivel de seguridad”.

17. Por “factor de autenticación” (*authentication factor*) se entiende: a) un fragmento de información y/o procedimiento utilizado para autenticar o verificar la identidad de una entidad. Fuente: ISO/IEC 19790. Nota: Los factores de autenticación se dividen en cuatro categorías: i) algo que la entidad tiene (por ejemplo, firma de dispositivo, pasaporte, dispositivo físico que contiene una credencial o clave privada); ii) algo que la entidad sabe (por ejemplo, contraseña, PIN); iii) algo intrínseco a la entidad (por ejemplo, características biométricas); o iv) algo que la entidad suele hacer (por ejemplo, patrón de conducta). Fuente: Recomendación UIT-T X.1254; b) un factor confirmado como vinculado a una persona, que se encuentra en alguna de las categorías siguientes: i) ‘factor de autenticación basado en la posesión’, factor de autenticación en el que el sujeto está obligado a demostrar posesión del mismo; ii) ‘factor de autenticación basado en el conocimiento’, factor de autenticación en el que el sujeto está obligado a demostrar conocimiento del mismo; y iii) ‘factor de autenticación inherente’, factor de autenticación que se basa en un atributo físico de una persona física del cual el sujeto está obligado a demostrar su posesión. Fuente: Reglamento de Ejecución (UE) 2015/1502 de la Comisión, anexo, artículo 1, párrafo 2.

18. Por “autenticador” (*authenticator*) se entiende cualquier cosa que se utilice para verificar la relación entre un sujeto y una credencial. Un autenticador activo suele ser algo que el sujeto conoce (como una contraseña secreta), algo que el sujeto tiene (como una tarjeta inteligente) o algo intrínseco al sujeto (como una fotografía u otra información biométrica), que se utiliza para vincular al sujeto con una credencial de identidad. Por ejemplo, una contraseña hace las veces de autenticador de un nombre de usuario y una fotografía sirve como autenticador de un pasaporte o una licencia de conducir. Un autenticador pasivo suele ser algo que el entorno sabe, por ejemplo, la red móvil sabe que el usuario está conectado a la red, que se encuentra en el lugar habitual, que utiliza el dispositivo móvil habitual, que no se le ha prohibido utilizar la red, etc.

19. Se entiende: a) por “fuente fidedigna”, un depósito reconocido por ser una fuente de información precisa y actualizada. Fuente: Recomendación UIT-T X.1254 (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.); y b) por “fuente auténtica”,

cualquier fuente, independientemente de la forma, en la que se pueda confiar para proporcionar datos, información o pruebas exactos que se puedan utilizar para demostrar la identidad. Fuente: Reglamento de Ejecución (UE) 2015/1502 de la Comisión, anexo, artículo 1, párrafo 1. (Las dos variantes citadas en español corresponden al término "*authoritative source*" en inglés).

20. Por "autorización" (*authorization*) se entiende: a) el proceso de otorgamiento de derechos y privilegios a los sujetos que han sido objetos de autenticación basándose en criterios determinados generalmente por la parte receptora. Por ejemplo, una vez que el sujeto es autenticado, se le puede conceder acceso a una base de datos confidenciales. Fuente: A/CN.9/WG.IV/WP.120, anexo; b) la atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso. Fuentes: Recomendaciones UIT-T Y.2720 y UIT-T X.800.

21. Por "credencial" (*credential*) se entiende: a) un conjunto de datos presentado como evidencia de una identidad y/o unos derechos declarados. Fuente: Recomendación UIT-T X.1252; b) datos en forma digital o tangible presentados como prueba de la identidad que declara un sujeto. Entre los ejemplos de credenciales en papel cabe citar el pasaporte, la partida de nacimiento, la licencia de conducir y la tarjeta de identificación de un empleado. Entre los ejemplos de credenciales digitales figuran los nombres de usuario, las tarjetas inteligentes, la identidad móvil y los certificados digitales. Fuente: A/CN.9/WG.IV/WP.120, anexo. Sinónimos: medio de identificación electrónica; credencial de identidad.

22. Por "proveedor de credenciales" (*credential provider*) o "proveedor de servicio de credenciales" (*credential service provider*) se entiende: a) una entidad que expide credenciales a los sujetos; b) un actor de confianza que expide y/o gestiona credenciales. Nota: Un proveedor de servicio de credenciales puede comprender tanto las autoridades de registro como los verificadores cuyos servicios administre. Un proveedor de servicio de credenciales puede ser un tercero independiente, o puede expedir credenciales para su propio uso. Fuente: Recomendación UIT-T X.1254.

23. Por "identificación electrónica" (*electronic identification*) se entiende el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica. Fuente: eIDAS, artículo 3, párrafo 1. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

24. Por "medios de identificación electrónica" (*electronic identification means*) se entiende la unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea. Fuente: eIDAS, artículo 3, párrafo 2. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

25. Por "sistema de identificación electrónica" (*electronic identification scheme*) se entiende el régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica. Fuente: eIDAS, artículo 3, párrafo 4. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

26. Por "inscripción" (*enrolment*) se entiende: a) el proceso de inauguración de una entidad en un contexto. Nota 1: La inscripción podría incluir la verificación de la identidad de la entidad y el establecimiento de una identidad contextual. Nota 2: Asimismo, la inscripción es un prerrequisito para el registro. En muchos casos esta última expresión se utiliza para describir ambos procesos. Fuente: Recomendación UIT-T X.1252; b) el proceso por el que un proveedor de credenciales (o sus agentes) verifica la identidad que declara un sujeto antes de expedirle una credencial.

27. Por "entidad" (*entity*) se entiende cualquier cosa que tenga una existencia autónoma y bien definida y pueda ser identificada en un contexto. Nota: Una entidad puede ser una persona física, un animal, una persona jurídica, una organización, una cosa activa o pasiva, un dispositivo, una aplicación informática, un servicio, etc., o un grupo de estos elementos. En el contexto de las telecomunicaciones, como ejemplos de

entidades cabe mencionar puntos de acceso, abonados, usuarios, elementos de red, redes, aplicaciones informáticas, servicios y dispositivos, interfaces, etc. Fuente: Recomendación UIT-T X.1252. Una entidad puede tener múltiples identificadores.

28. Por “federación” (*federation*) se entiende: a) una asociación de usuarios, proveedores de servicios y proveedores de servicios de identidad. Fuente: Recomendación UIT-T X.1252; b) un grupo de proveedores de identidad, partes receptoras, sujetos y otras personas que convienen en actuar con arreglo a políticas, normas y tecnologías compatibles especificadas en las normas del sistema (o en un marco de confianza) con el fin de que las partes receptoras puedan comprender la información facilitada por los proveedores de identidad sobre la identidad de los sujetos y confiar en ella. Sinónimos: sistema de identidad federado; sistema de identidad multipartito.

29. Por “identificación” (*identification*) se entiende el proceso de reunión, verificación y validación de información de atributos adecuada acerca de un sujeto concreto para definir y confirmar su identidad en un contexto específico. Sinónimos: demostración de identidad; registro.

30. Por “identificador” (*identifier*) se entiende: a) uno o más de los atributos utilizados para identificar a una entidad dentro de un contexto. Fuente: Recomendación UIT-T X.1252; b) uno o varios atributos que caracterizan inequívocamente una entidad en un determinado contexto. Fuente: Recomendación UIT-T X.1254.

31. Por “identidad” (*identity*) se entiende: a) un conjunto de atributos relativos a una entidad. Fuente: ISO/IEC 24760; b) información acerca de un sujeto concreto en forma de uno o más atributos que permiten que el sujeto sea debidamente diferenciado en un contexto particular; c) un conjunto de atributos relativos a una persona que la describen de manera inequívoca en un contexto dado. Sinónimo: identidad digital.

32. Por “aseveración de identidad” (*identity assertion*) se entiende un documento electrónico que se origina en un proveedor de identidad y se envía a una parte receptora, que contiene el identificador del sujeto (por ejemplo, nombre, número de cuenta, número de teléfono móvil, ubicación, etc.), el estado de autenticación y los atributos de identidad aplicables. Los atributos normalmente consisten en información de carácter personal y no personal sobre el sujeto que resulta pertinente para la transacción solicitada por la parte receptora.

33. Por “garantía de identidad” (*identity assurance*) se entiende el grado de confianza en el proceso de validación y verificación de la identidad utilizado para determinar la identidad de la entidad para la cual se expide la credencial, y el grado de confianza en que la entidad que utiliza la credencial es dicha entidad o la entidad a la cual se le expidió o asignó la credencial. Fuente: Recomendación UIT-T X.1252. Sinónimos: nivel de garantía; nivel de seguridad. Nota: En algunos casos, los conceptos de “garantía de identidad” y “garantía de autenticación” se consideran componentes independientes del concepto general de “nivel de seguridad”.

34. Por “sistema de identidad federado” (*identity federation*) se entiende un grupo de proveedores de identidad, partes receptoras, sujetos y otras personas que convienen en actuar con arreglo a políticas, normas y tecnologías compatibles especificadas en las normas del sistema (o en un marco de confianza) con el fin de que las partes receptoras puedan comprender la información facilitada por los proveedores de identidad sobre la identidad de los sujetos y confiar en ella. Véase también: federación; sistema de identidad multipartito.

35. Por “gestión de la identidad” (*identity management*) se entiende: a) un conjunto de procesos para gestionar la identificación, autenticación y autorización de personas físicas, entidades jurídicas, dispositivos u otros sujetos en un contexto en línea. Fuente: A/CN.9/854, párrafo 6; b) un conjunto de funciones y capacidades (por ejemplo, administración, gestión y mantenimiento, descubrimiento, intercambios de comunicaciones, correlación y vinculación, cumplimiento de una política, autenticación y asertos) que se utilizan para: i) garantizar la información de identidad (por ejemplo,

identificadores, credenciales, atributos); ii) garantizar la identidad de una entidad; y iii) habilitar aplicaciones de negocios y de seguridad. Fuente: Recomendación UIT-T Y.2720.

36. Se entiende por "comprobación de identidad": a) el proceso de reunión, verificación y validación de información de atributos adecuada acerca de un sujeto concreto (persona física, persona jurídica, dispositivo, objeto digital u otro tipo de entidad) para definir y confirmar su identidad en un contexto específico. La identidad puede comprobarse mediante la aseveración realizada por la propia entidad o mediante comparación con registros existentes; y se entiende por "demostración de identidad": b) el proceso mediante el cual se valida y verifica información suficiente como para confirmar la identidad alegada por la entidad. Fuente: Recomendación UIT-T X.1252; c) el proceso mediante el cual la autoridad de registro (RA) obtiene y verifica suficiente información para identificar una entidad con un nivel de garantía o seguridad especificado o tácito. Fuente: Recomendación UIT-T X.1254. Sinónimos: identificación; registro. (Las dos variantes citadas en español corresponden al término "*identity proofing*" en inglés).

37. Por "proveedor de identidad" (*identity provider*) se entiende: a) una entidad encargada de la identificación de personas físicas, entidades jurídicas, dispositivos y objetos digitales, de la expedición de las credenciales de identidad correspondientes y del mantenimiento y la gestión de la información sobre la identidad de los distintos sujetos. Fuente: A/CN.9/WG.IV/WP.120, anexo; b) una entidad que crea, mantiene y gestiona información digna de confianza sobre la identidad de otras entidades (por ejemplo, usuarios/abonados, organizaciones y dispositivos) y ofrece servicios basados en la identidad, así como en la confianza, el negocio de que se trate y otros tipos de relaciones. Fuente: Recomendación UIT-T Y.2720. Sinónimos: proveedor de servicio de credenciales; proveedor de servicio de identidad.

38. Por "sistema de identidad" (*identity system*) se entiende un entorno en línea utilizado para la gestión de la identidad digital que se rige por un conjunto de reglas de funcionamiento (también conocido como marco de confianza) y en el que puede haber confianza recíproca entre individuos, organizaciones, servicios y dispositivos dado que fuentes autorizadas han establecido y autenticado sus identidades respectivas. Fuente: A/CN.9/WG.IV/WP.120, anexo. Un sistema de identidad comprende: a) un conjunto de reglas, métodos, procedimientos y rutinas, tecnologías, normas, políticas y procesos, b) aplicable a un grupo de entidades participantes, c) que rige la reunión, verificación, almacenamiento, intercambio y autenticación de información sobre los atributos de identidad de una persona física, una persona jurídica, un dispositivo o un objeto digital, así como la fiabilidad de esa información; d) con el fin de facilitar transacciones de identidad. Sinónimos: sistema de gestión de la identidad; sistema de identidad federado; sistema de identificación electrónica; sistema de gestión de la seguridad de la información.

39. Por "transacción de identidad" (*identity transaction*) se entiende cualquier transacción en la que intervengan dos o más participantes y que implique establecer, verificar, emitir, aseverar, revocar o comunicar información de identidad o confiar en ella.

40. Por "verificación de identidad" (*identity verification*) se entiende el proceso a tenor del cual se confirma que la identidad declarada es correcta mediante la comparación de las declaraciones de identidad ofrecidas con información previamente demostrada. Fuente: Recomendación UIT-T X.1252.

41. Por "sistema de gestión de la seguridad de la información" (*information security management system*) se entiende el conjunto de procesos y procedimientos diseñados para gestionar a niveles aceptables los riesgos relacionados con la seguridad de la información. Fuente: Reglamento de Ejecución (UE) 2015/1502 de la Comisión, anexo, artículo 1, párrafo 1.

42. Por "nivel de seguridad" (*level of assurance*) se entiende una designación del grado de confianza en los procesos de identificación y autenticación, es decir: a) el grado de confianza en el proceso de análisis utilizado para establecer la identidad de una entidad a la que se ha expedido una credencial, y b) el grado de confianza en que la

entidad que utiliza la credencial es la entidad a la que se ha emitido esa credencial. La seguridad refleja la fiabilidad de los métodos, procesos y tecnologías empleados. Hay algunos sistemas que definen los niveles de seguridad mediante un número, a saber, del 1 al 4, donde el nivel 1 corresponde al menor nivel de seguridad y el nivel 4 corresponde al mayor nivel. En otros sistemas, los niveles de seguridad se definen como "bajo", "considerable" y "alto". Sinónimos: nivel de garantía; garantía de identidad; nivel de confianza.

43. Por "autenticación multifactorial" (*multifactor authentication*) se entiende la autenticación en la que se emplean como mínimo dos factores de autenticación independientes. Nota: los factores de autenticación se dividen en cuatro categorías: a) algo que la entidad tiene (por ejemplo, firma de dispositivo, pasaporte, dispositivo físico que contiene una credencial o clave privada); b) algo que la entidad sabe (por ejemplo, contraseña, PIN); c) algo intrínseco a la entidad (por ejemplo, características biométricas); o d) algo que la entidad suele hacer (por ejemplo, patrón de conducta). Fuentes: ISO/IEC 19790; Recomendación UIT-T X.1254.

44. Por "sistema de identidad multipartito" (*multi-party identity system*) se entiende un sistema de identidad, también denominado sistema de identidad federado, en el que un sujeto puede utilizar una credencial de identidad expedida por cualquiera de los distintos proveedores de identidad a efectos de autenticación en sistemas diferentes ante múltiples partes receptoras no relacionadas entre sí; un sistema de identidad que permite utilizar tanto las credenciales de identidad expedidas por uno o más proveedores de identidad con múltiples partes receptoras, como la información de identidad aseverada por uno o más de esos proveedores. Fuente: A/CN.9/WG.IV/WP.120, anexo. Sinónimo: sistema de identidad federado.

45. Por "participante" (*participant*) se entiende cualquier persona física o jurídica que participe en un sistema de identidad o en una transacción de identidad utilizando dicho sistema. Los participantes pueden ser sujetos, proveedores de identidad, proveedores de atributos, proveedores de credenciales, partes receptoras, operadores de sistemas de identidad y otros. Al igual que los participantes en un sistema de tarjetas de crédito, los participantes en un sistema de identidad suelen aceptar contractualmente un conjunto de normas del sistema (a menudo denominado marco de confianza) aplicable al papel que asumen.

46. Por "datos de identificación de la persona" (*person identification data*) se entiende el conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica. Fuente: eIDAS, artículo 3, párrafo 3. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

47. Por "demostración" (*proofing*) se entiende la verificación y validación de la información cuando se inscriben nuevas entidades en los sistemas de identidad. Fuente: Recomendación UIT-T X.1252. Sinónimos: comprobación de identidad; demostración de identidad; identificación.

48. Por "seudónimo" (*pseudonym*) se entiende un identificador cuya vinculación con una entidad no se conoce o solo se conoce hasta cierto grado dentro del contexto en el cual se utiliza. Nota: Los seudónimos pueden utilizarse para evitar o reducir los riesgos relativos a la privacidad que entraña la utilización de relaciones de identificador que pueden revelar la identidad de la entidad. Fuente: Recomendación UIT-T X.1252.

49. Por "registro" (*registration*) se entiende un proceso a tenor del cual una entidad solicita un privilegio para utilizar un servicio o un recurso y se le asigna dicho privilegio. Nota: La inscripción es un prerrequisito para el registro. Las funciones de inscripción y registro pueden estar combinadas o separadas. Fuente: Recomendación UIT-T X.1252.

50. Por "autoridad de registro" (*registration authority*) se entiende una entidad que presta servicios de inscripción y/o de demostración de identidad en el contexto de un sistema de identidad federado (es decir, multipartito), normalmente para un proveedor de identidad.

51. Se entiende: a) por “parte receptora”, la persona física o entidad jurídica que se basa en la credencial de identidad o la aseveración de identidad para decidir las medidas que deberá tomar en un contexto de aplicación determinado, por ejemplo, procesar una transacción o autorizar el acceso a información o a un sistema. Fuente: A/CN.9/WG.IV/WP.120, anexo; b) por “parte dependiente” o “parte confiante”, la entidad que confía en la representación o declaración de identidad de una entidad solicitante/aseverante en un contexto de petición. Fuente: Recomendación UIT-T X.1252; c) por “parte usuaria”, la persona física o jurídica que confía en la identificación electrónica o el servicio de confianza. Fuente: eIDAS, artículo 3, párrafo 6. (Las cuatro variantes citadas en español corresponden al término “*relying party*” en inglés).

52. Por “repositorio” (*repository*) se entiende una interfaz que acepta depósitos de entidades digitales, permite su almacenamiento y ofrece acceso seguro a las entidades digitales por medio de sus identificadores. Fuente: Recomendación UIT-T X.1255.

53. Por “papel” (*role*) se entiende un tipo (o categoría) de participante en un sistema de identidad, como un sujeto, un proveedor de identidad, un proveedor de credenciales, una parte receptora, etc. Un participante puede desempeñar varios papeles. Por ejemplo, con respecto a la identificación de sus empleados, un empleador puede actuar como proveedor de identidad y como parte receptora.

54. Por “identidad autoaseverada” (*self-asserted identity*) se entiende la entidad que asevera la propia entidad. Fuente: Recomendación UIT-T X.1252.

55. Por “sujeto” (*subject*) se entiende la persona física, entidad jurídica, dispositivo u objeto digital (es decir, la entidad) que es objeto de identificación en una credencial concreta y cuyos datos el proveedor de la identidad puede autenticar y certificar. Fuente: A/CN.9/WG.IV/WP.120, anexo. Sinónimos: usuario; sujeto de datos.

56. “Normas del sistema” (*system rules*): véase marco de confianza.

57. Por “confianza” (*trust*) se entiende la firme creencia en la fiabilidad y veracidad de la información, o en la habilidad y disposición de una entidad para actuar adecuadamente dentro de un contexto especificado. Fuente: Recomendación UIT-T X.1252.

58. Por “marco de confianza” (*trust framework*) se entiende: a) las reglas aplicables a un sistema de identidad formadas por las normas comerciales, técnicas y jurídicas que rigen la participación en un determinado sistema de identidad y su funcionamiento. Suelen ser elaboradas a nivel privado (por ejemplo, por el operador del sistema de identidad) y en virtud del contrato adquieren carácter vinculante y fuerza legal para los participantes. Fuente: A/CN.9/WG.IV/WP.120, anexo; b) un conjunto de requisitos y mecanismos de aplicación para las partes que intercambian información de identidad. Fuente: Recomendación UIT-T X.1254; c) un sistema de gestión de la identidad en el que cada una de las diversas partes en una transacción adquiere un conjunto de compromisos verificables con sus contrapartes; estos compromisos comprenden necesariamente: i) controles para ayudar a cumplir dichos compromisos; y ii) soluciones en caso de que no se cumplan. Fuente: Recomendación UIT-T X.1255. Sinónimos: normas del sistema; reglas de funcionamiento; reglas del sistema.

59. Por “proveedor de marco de confianza” (*trust framework provider*) se entiende la entidad u organización que crea o adopta las normas del sistema y la estructura contractual conexa de un sistema de identidad en particular. El proveedor del marco de confianza también puede certificar cuáles participantes cumplen las normas de ese sistema. Por ejemplo, los emisores de tarjetas de crédito y de débito pueden desempeñar un papel similar en el ámbito de las tarjetas de crédito y débito; establecen las normas del sistema y las hacen cumplir.

60. Por “tercero fiable” (*trusted third party*) se entiende: a) una autoridad o su agente, en la que confían otros actores en lo que respecta a actividades específicas (por ejemplo, actividades relacionadas con la seguridad). Fuente: Recomendación UIT-T X.1254; b) una entidad aceptada por todas las partes en una transacción como intermediaria imparcial y digna de confianza para facilitar la interacción entre dos o más partes.

61. Por “usuario” (*user*) se entiende: a) el sujeto de una credencial; un consumidor de los servicios ofrecidos por una parte receptora; b) cualquier entidad que utilice un recurso, por ejemplo, sistemas, equipos, terminales, procesos, aplicaciones o redes empresariales. Fuente: Recomendación UIT-T X.1252.

62. Por “validación” (*validation*) se entiende el proceso de verificar y confirmar la validez de una credencial de identidad (es decir, que no ha expirado ni ha sido revocada).

63. Por “verificación” (*verification*) se entiende: a) el proceso de verificación de información comparando la información facilitada con la información corroborada previamente. Fuente: Recomendación UIT-T X.1254; b) el proceso o instancia que determina la autenticidad de algo. Nota: La verificación de la información (de identidad) puede implicar un análisis en lo que respecta a la validez, la fiabilidad de la fuente, lo original (inalterado), la corrección, la relación con la entidad, etc. Fuente: Recomendación UIT-T X.1252.

B. Definiciones pertinentes para los servicios de confianza

64. Las definiciones que figuran a continuación pueden ser especialmente pertinentes en las deliberaciones sobre los aspectos jurídicos de los servicios de confianza. No obstante, algunas de las definiciones enumeradas más arriba, consideradas pertinentes para los debates sobre los aspectos jurídicos de la gestión de la identidad, también pueden ser pertinentes para las deliberaciones sobre los aspectos jurídicos de los servicios de confianza (véase el párr. 8 *supra*).

65. Por “certificado de autenticación de sitio web” (*certificate for website authentication*) se entiende una declaración que permite autenticar un sitio web y vincula el sitio web con la persona física o jurídica a quien se ha expedido el certificado. Fuente: eIDAS, artículo 3, párrafo 38. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

66. Por “prestador de servicios de certificación” (*certification service provider*) se entiende la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas. Fuente: Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, artículo 2 e)[5].

67. Por “documento electrónico” (*electronic document*) se entiende todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual. Fuente: eIDAS, artículo 3, párrafo 35. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

68. Por “servicio de entrega electrónica certificada” (*electronic registered delivery service*) se entiende un servicio que permite transmitir datos entre partes terceras por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente a los riesgos de pérdida, robo, deterioro o alteración no autorizada. Fuente: eIDAS, artículo 3, párrafo 36. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

69. Por “sello electrónico” (*electronic seal*) se entiende datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos. Fuente: eIDAS, artículo 3, párrafo 25. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

70. Por “firma electrónica” (*electronic signature*) se entiende: a) los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar. Fuente: eIDAS, artículo 3, párrafo 10 (véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.); b) los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos

[5] Publicación de las Naciones Unidas, núm. de venta: S.02.V.8.

e indicar que el firmante aprueba la información recogida en el mensaje de datos. Fuente: Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, artículo 2 a). Nota: En el artículo 9, párrafo 3 a), de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (Nueva York, 2005)[6] se hace referencia a la indicación de la voluntad del firmante respecto de la información consignada en la comunicación electrónica.

71. Por "sello de tiempo electrónico" (*electronic time stamp*) se entiende los datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante. Fuente: eIDAS, artículo 3, párrafo 33. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

72. Por "servicio de confianza calificado" (*qualified trust service*) se entiende el servicio de confianza que cumple los requisitos aplicables establecidos en la presente [Convención] [Ley Modelo]. Fuente: A/CN.9/WG.IV/WP.144, párr. 20.

73. Se entiende a) por "parte que confía", la persona que pueda actuar sobre la base de un certificado o de una firma electrónica. Fuente: Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, artículo 2 f); y b) por "usuario", la persona física o jurídica que se fía de una identificación electrónica o de un servicio de confianza. Fuente: A/CN.9/WG.IV/WP.144, párr. 20. (Las dos variantes citadas en español corresponden al término "*relying party*" en inglés.)

74. Por "firmante" (*signatory*) se entiende: a) la persona física que crea una firma electrónica. Fuente: eIDAS, artículo 3, párrafo 9. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20); b) la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa. Fuente: Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, artículo 2 d).

75. Por "servicio de confianza" (*trust service*) se entiende el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o b) la creación, verificación y validación de certificados para la autenticación de sitios web, o c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios. Fuente: eIDAS, artículo 3, párrafo 16.

76. Por "prestador de servicios de confianza" (*trust service provider*) se entiende una persona física o jurídica que presta uno o más servicios de confianza [bien como prestador cualificado o como prestador no cualificado de servicios de confianza]. Fuente: eIDAS, artículo 3, párrafo 19. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

77. Por "sello de tiempo" (*time stamp*) se entiende un parámetro de tiempo variable y fiable, que indica un instante en el tiempo respecto de una referencia común. Fuente: Recomendación UIT-T X.1254.

78. Por "validación" (*validation*) se entiende el proceso de verificar y confirmar la validez de una firma o sello electrónicos. Fuente: eIDAS, artículo 3, párrafo 41. (Véase también el documento A/CN.9/WG.IV/WP.144, párr. 20.)

[6] Resolución 60/21 de la Asamblea General, anexo.