Naciones Unidas A/CN.9/WG.IV/WP.141

Asamblea General

Distr. limitada
30 de enero de 2017
Español
Original: ruso

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo IV (Comercio Electrónico)
55º período de sesiones
Nueva York, 24 a 28 de abril de 2017

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

Nota de la Secretaría

La Federación de Rusia presentó a la Secretaría un documento para su examen en el 55º período de sesiones del Grupo de Trabajo. El texto recibido por la Secretaría se reproduce como anexo de la presente nota.

V.17-00123 (S) 150217 150217

Anexo

Propuesta de la Federación de Rusia

Mejora del sistema de gestión de la identidad mediante el uso de un entorno transfronterizo de confianza y una infraestructura de confianza común para las operaciones electrónicas transfronteriza

Introducción

El Acuerdo Marco sobre la Facilitación del Comercio Transfronterizo sin Soporte de Papel en la Región de Asia y el Pacífico fue aprobado el 24 de mayo de 2016 en el 72º período de sesiones de la Comisión Económica y Social para Asia y el Pacífico (CESPAP).

El objetivo del Acuerdo Marco es "promover el comercio transfronterizo sin soporte de papel permitiendo para ello el intercambio y el reconocimiento mutuo de datos y documentos relacionados con el comercio y facilitando la interoperabilidad entre las ventanillas únicas nacionales y subregionales y otros sistemas de comercio sin soporte de papel, con la finalidad de que las operaciones comerciales internacionales sean más eficientes y transparentes y al mismo tiempo se mejore el cumplimiento de los reglamentos".

El artículo 5 del Acuerdo Marco establece "la mejora del entorno de confianza transfronterizo" (párrafo 1 g)) como uno de los principios generales por los que se guía el Acuerdo.

El presente documento tiene por objeto continuar la labor de mejora del entorno de confianza transfronterizo en el comercio electrónico, un tema importante del programa de la CESPAP y de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI).

Se presentó al Grupo de Trabajo III (Solución de Controversias en Línea) de la CNUDMI una versión anterior de la propuesta, que figura en el documento A/CN.9/WG.III/WP.136, para su examen en su 32º período de sesiones celebrado en Viena (30 de noviembre a 4 de diciembre de 2015). Por recomendación de los participantes en el Grupo de Trabajo, se transmitió el documento al Grupo de Trabajo IV (Comercio Electrónico) para su examen debido a su pertinencia para el programa de ese Grupo de Trabajo. Las principales esferas de interés son los mecanismos técnicos, organizativos, y jurídicos para fortalecer el entorno de confianza transfronterizo para el comercio electrónico en la región de Asia y el Pacífico. En el 53º período de sesiones del Grupo de Trabajo IV la delegación de la Federación de Rusia expresó su intención de presentar una propuesta al Grupo de Trabajo sobre la gestión de la identidad para que la examinara en su siguiente período de sesiones, con sujeción a que la Comisión confirmase que la gestión de la identidad se incluiría en el programa del Grupo de Trabajo en ese período de sesiones. Se invitó a las delegaciones a que presentaran información sobre la gestión de la identidad con miras a facilitar el examen del tema.

Garantizar la seguridad del intercambio transfronterizo de documentos electrónicos es una cuestión sumamente importante que se ha puesto de relieve en declaraciones mundiales y regionales, concretamente:

- "Promover la investigación y cooperación que permitan el uso eficaz de datos y programas informáticos, en particular documentos y operaciones electrónicos, incluidos medios electrónicos de autenticación, y el mejoramiento de los

métodos de seguridad (Documento “WSIS+10 Perspectiva para la CMSI después de 2015. C5. Creación de confianza y seguridad en la utilización de las TIC”, apartado f);

- [...] promover la confianza en los entornos electrónicos en todo el mundo alentando las corrientes de información transfronterizas seguras, incluidos los documentos electrónicos[, y promover] las actividades encaminadas a ampliar y reforzar la Infraestructura de la Información de Asia y el Pacífico y a crear confianza y seguridad en el uso de las TIC (Declaración de Vladivostok (Declaración de los Dirigentes del Foro de Cooperación Económica de Asia y el Pacífico (APEC), 2012): “Integrar para Crecer, Innovar para Prosperar”).”

A nivel mundial existen en la actualidad varios ejemplos de buenas prácticas para ocuparse de la cuestión:

- En la Comisión Europea: sobre la base del Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS)[1];
- En la Unión Económica de Eurasia: sobre la base del Tratado de la Unión Económica de Eurasia y del Concepto de la utilización de servicios y documentos electrónicos con efectos jurídicos en interacciones informáticas entre Estados[2];
- En la región de Asia y el Pacífico, sobre la base de la Alianza Panasiática de Comercio Electrónico (PAA)[3].

El fomento de la economía mundial requiere, especialmente en períodos de crisis, la mejora de los procesos de integración en distintas esferas económicas y sociales, entre otras cosas mediante el uso innovador de las actuales tecnologías de la información y las comunicaciones (TIC).

Una de las cuestiones principales que se plantean con respecto al comercio transfronterizo es la seguridad y la confidencialidad de la información transmitida por Internet. Se utiliza un sistema de gestión de la identidad para resolver esa cuestión. La gestión de la identidad es un conjunto de funciones y medios (por ejemplo, administración, gestión y mantenimiento, descubrimiento, intercambios de comunicación, correlación y consolidación, ejecución de políticas, autenticación y aseveraciones) que se utiliza para:

- Garantía de la información sobre la identidad (por ejemplo, identificadores, credenciales, atributos);
- Garantía de la identidad de una entidad (por ejemplo: usuarios/suscriptores, grupos, dispositivos de usuarios, organizaciones, proveedores de redes y servicios, elementos y objetos de redes y objetos virtuales); y
- Apoyo a aplicaciones empresariales y de seguridad[4].

Los objetivos de la gestión de la identidad son:

- Control del acceso (solo deberían acceder a los equipos informáticos los usuarios autorizados y para los fines previstos por los propietarios);

[1] http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond.
[2] www.eurasiancommission.org/docs/Download.aspx?IsDlg=0&print=1&ID=5713.
[3] www.paa.net/.
[4] https://www.itu.int/rec/T-REC-X.1252-201004-I/es.

- Confidencialidad del acceso;
- Integridad del sistema de gestión de la identidad.

Para poder alcanzar esos objetivos, un sistema de gestión de la identidad debería:

- Garantizar el funcionamiento necesario del sistema con indicadores de resiliencia establecidos;
- Garantizar la función de gestión de los datos de identificación (creación, alteración, congelación, archivado o supresión de información de identificación);
- Garantizar la protección de los datos de identificación;
- Garantizar la utilización de mecanismos de identificación y autenticación seguros (por ejemplo, firma electrónica, protección mediante contraseña de dos pasos y autenticación biométrica);
- Garantizar la interoperabilidad de las soluciones de seguridad utilizadas;
- Garantizar la integridad del sistema de gestión de la identidad y de la información de identificación.

Existen dos tipos de sistemas de gestión de la identidad: los centrados en la aplicación y los centrados en el usuario[5].

En los sistemas de gestión de la identidad de gran escala, el sistema de gestión de la identidad centrado en la aplicación significa que los servicios y políticas en materia de identidad han sido concebidos para satisfacer los requisitos de los proveedores de servicios de identidad y optimizados para los requisitos de las aplicaciones, por ejemplo, el suministro de la información de la cuenta de un usuario. En el sistema de gestión de la identidad centrado en la aplicación existen un proveedor de servicios de identidad y una parte confiante. Cuando se presta un servicio de identidad para el usuario, el intercambio de identidad suele tener lugar entre esas dos entidades. Por "identidad" se entiende la representación de una entidad en forma de uno o varios elementos de información que permiten distinguir suficientemente a la entidad o entidades dentro del contexto. A los efectos de la gestión de la identidad, se entiende que "identidad" constituye una identidad contextual (subconjunto de atributos), es decir, que la diversidad de atributos está limitada por un marco con fronteras definidas (el contexto) en el cual la entidad existe e interactúa. Históricamente, las tecnologías de gestión de la identidad y el acceso se han centrado principalmente en la autenticación de los usuarios finales para el acceso federado a aplicaciones y servicios (en el modelo de acceso federado existen varios proveedores de servicios de identidad en los que los usuarios pueden confiar y que pueden gestionar la información parcial de la identidad de los usuarios en caso necesario. La información de la identidad del usuario en cada proveedor de servicios de identidad puede compartirse). Por lo tanto, el requisito de seguridad se limita al perímetro de sus dominios de aplicación.

El sistema de gestión de la identidad centrado en el usuario se concentra en los usuarios finales y está optimizado para los requisitos de esos usuarios concretos, lo que significa que el principal objetivo de un sistema de gestión de la identidad es proporcionar servicios de identidad convenientes y completos a los usuarios. La característica principal es que permiten al usuario el control pleno de su identidad. Cuando se difunde la información de la identidad de un usuario, debe pasar a través del usuario para que este tenga la oportunidad de hacer cumplir alguna política personal en caso necesario; por ejemplo, una elección de preferencias personales en relación con la confidencialidad o la autorización personal. En el sistema de gestión de

[5] https://www.itu.int/rec/T-REC-X.1252-201009-I/es.

la identidad centrado en el usuario, hay que instalar en el entorno informático del usuario un programa cliente que interactúa con el servidor de gestión de la identidad para recuperar información de la identidad. Por lo tanto, se necesitan directrices de seguridad fáciles y amplias a fin de guiar al usuario para que instale y utilice los programas informáticos pertinentes en condiciones de seguridad. Los programas deben gestionar alguna de la información del usuario relacionada con la seguridad. La concentración en el usuario se distingue de otros modelos de gestión de la identidad al hacer hincapié en que el usuario, y no una autoridad, mantiene el control sobre la forma en que se crean, difunden, actualizan y extinguen los atributos de identidad de un usuario. Esto supone que el usuario tiene plena autoridad durante el ciclo de vida de su identidad. El nivel de control lo pueden determinar los requisitos de privacidad del usuario.

Las cuestiones relacionadas con la gestión de la identidad fueron examinadas por primera vez en el marco de la Unión Internacional de Telecomunicaciones (UIT) y su Sector de Normalización de las Telecomunicaciones (UIT-T) en 2006, cuando el Grupo de Estudio 17 de la UIT-T, que trabaja en cuestiones de seguridad de las telecomunicaciones y las TIC, estableció el Grupo Temático de gestión de identidad. Las actividades del Grupo Temático evolucionaron hasta llegar a ser una iniciativa mundial de gestión de la identidad de la UIT que se puso en marcha en 2008. Colaboraron en esa iniciativa los grupos de estudio 2, 9, 11, 13, 16 y 17 de la UIT-T. El Grupo de Estudio 17 ha dirigido la Actividad Conjunta de Coordinación de la Gestión de la Identidad (JCA-IdM) desde 2009. Mediante la Actividad se ha elaborado una hoja de ruta de normas sobre gestión de la identidad que incluye aportaciones pertinentes de las siguientes organizaciones: la Alianza para Soluciones de la Industria de las Telecomunicaciones (ATIS), el Instituto Europeo de Normas de Telecomunicaciones (ETSI), el Grupo de Tareas sobre Ingeniería de Internet (IETF), la Organización Internacional de Normalización (ISO)/Comisión Electrotécnica Internacional (CEI), la UIT, el Instituto Nacional de Normas y Tecnología (NIST), la Organization for the Advancement of Structured Information Standards (OASIS), la Iniciativa de Kantara y el Proyecto de Alianzas de Tercera Generación (3GPP) (en el sitio web de la UIT (http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part06.aspx) figura una descripción de las actividades realizadas y las normas en materia de gestión de la identidad emitidas por la UIT y esas organizaciones).

El establecimiento de un entorno de confianza transfronterizo (ECT) en la esfera del comercio electrónico contribuirá a la simplificación de los trámites y al desarrollo del comercio internacional, y permitirá a los países participantes simplificar el proceso de identificación y la gestión de la identidad. Por “confianza” en el contexto de la seguridad puede entenderse la certidumbre en relación con la fiabilidad y la veracidad de la información o en relación con la capacidad y la voluntad de una entidad de actuar de forma apropiada en una situación dada. Así pues, la creación de un entorno de confianza entre los Estados ayudará a armonizar la utilización de mecanismos de seguridad (por ejemplo, todos los países utilizarán un enfoque común de la selección de mecanismos como firmas electrónicas y protección mediante la verificación de contraseñas en dos pasos) y también permitirá aumentar el nivel de confianza (confianza continua y mensurable en la reputación, las capacidades, la validez o la autenticidad de alguien o de algo) entre los participantes en el comercio electrónico.

Se propone que por entorno de confianza transfronterizo se entienda una combinación de condiciones jurídicas, organizativas y técnicas recomendadas por los organismos especializados de las Naciones Unidas y las organizaciones internacionales competentes con miras a asegurar la confianza en el intercambio internacional de documentos y datos electrónicos entre partes (entidades) que interactúan electrónicamente al realizar operaciones de comercio electrónico.

Su finalidad principal es proporcionar a los usuarios varios niveles de servicios de confianza (básicos, medianos, altos) con ayuda de un sistema de gestión de la identidad en el curso de su interacción electrónica. Con ello se permitirá dar efectos jurídicos a la interacción electrónica a discreción de los usuarios, al margen de su ubicación geográfica y su jurisdicción. Uno de los aspectos más importantes de la investigación en esta esfera será el análisis de los posibles mecanismos de gestión de la identidad.

Se propone que por "partes (entidades) que interactúan electrónicamente" se entienda la totalidad de las autoridades públicas y personas naturales y jurídicas que interactúan en el marco de una relación dimanada de la creación, el envío, la transmisión, la recepción, el almacenamiento y el uso de documentos y datos electrónicos al realizar operaciones de comercio electrónico.

La finalidad de las propuestas es determinar los enfoques y cuestiones que se deben debatir en el contexto de la elaboración de una serie de recomendaciones sobre el establecimiento y funcionamiento de un entorno de confianza transfronterizo (recomendaciones sobre un ECT en la esfera del comercio electrónico) en los organismos correspondientes de las Naciones Unidas. Han sido concebidas para facilitar el establecimiento de una infraestructura tecnológica, institucional y jurídica para la puesta en práctica de las recomendaciones sobre un ECT en la esfera del comercio electrónico y, en particular, para simplificar el sistema de gestión de la identidad para la seguridad de las operaciones de comercio electrónico.

Enfoques conceptuales

1. Se propone que las recomendaciones sobre un ECT en la esfera del comercio electrónico se centren en garantizar los derechos e intereses jurídicos de los ciudadanos y las organizaciones bajo la jurisdicción de los Estados Miembros de las Naciones Unidas en relación con la realización de operaciones de información con efectos jurídicos en forma electrónica utilizando Internet y otros sistemas abiertos de TIC de uso masivo.

2. Esas garantías institucionales se proporcionarían en el marco de las actividades comerciales de los operadores especializados que:

- Presten a los usuarios una serie de servicios de TIC de confianza para la aplicación de la gestión de la identidad;
- Funcionen en el marco de regímenes jurídicos establecidos que incluyan, entre otras cosas, restricciones impuestas al procesamiento de datos personales.

3. Se propone ofrecer una descripción de los diversos regímenes jurídicos posibles:

- Los basados en acuerdos (instrumentos) internacionales o reglamentos internacionales de aplicación directa;
- Los basados en acuerdos comerciales o prácticas comerciales comunes;
- Los que no tienen una reglamentación internacional específica.

Los regímenes jurídicos también pueden recibir el apoyo de instituciones tradicionales (órganos gubernamentales, soluciones judiciales, seguro de riesgos, notarios, etc.) mediante el reconocimiento recíproco de los documentos electrónicos autenticados por servicios de TIC de confianza.

Los regímenes jurídicos establecidos también pueden prever la imposición de requisitos especiales en relación con el apoyo material y financiero de las actividades comerciales de los operadores especializados en caso de daños causados por estos a los usuarios, incluidos los casos en que se pongan en peligro los datos personales.

Se propone que las cuestiones relacionadas con las garantías institucionales y los regímenes jurídicos con respecto al establecimiento y funcionamiento de agrupaciones regionales y mundiales de ECT en la esfera del comercio electrónico, así como los servicios funcionales prestados en el marco de esas agrupaciones, se traten en una recomendación de la CNUDMI por separado.

4. Se sugiere que se ofrezca una descripción de los posibles conjuntos de servicios de infraestructura de TIC de confianza con arreglo al nivel de importancia de las aplicaciones funcionales. Una de las esferas de investigación más importantes a ese respecto será el análisis de los posibles mecanismos de gestión de la identidad. Los operadores de los sistemas de información funcionales (los operadores que organizan o llevan a cabo el almacenamiento y procesamiento en un sistema de información y que definen los objetivos y acciones (operaciones) aplicados utilizando los datos de identidad en ese sistema de información) pueden determinar los servicios de TIC y los niveles disponibles de confianza en esos servicios en función de las amenazas, los riesgos, los regímenes jurídicos y las necesidades de los usuarios. Para garantizar los niveles de confianza requeridos, los operadores de servicios de gestión de la identidad pueden trabajar en un entorno internacional neutral, definido por regímenes jurídicos determinados. Se propone que se describan las infraestructuras organizativas necesarias para establecer y mantener un entorno internacional neutral de esa índole.

Las disposiciones comunes sobre el establecimiento y funcionamiento de agrupaciones mundiales y regionales de ECT en la esfera del comercio electrónico, los servicios funcionales prestados en el marco de esas agrupaciones y los conjuntos de servicios de infraestructura de TIC de confianza se podrían examinar en el contexto de la recomendación conjunta del Centro de las Naciones Unidas de Facilitación del Comercio y las Transacciones Electrónicas (CEFACT-ONU) y la Comisión Económica para Europa (CEPE) para garantizar operaciones electrónicas transfronterizas con efectos jurídicos de confianza.

La implantación de la gestión de la identidad y la descripción de servicios de TIC de confianza concretos podría ser objeto de normas y recomendaciones técnicas de la UIT, el Comité Técnico Conjunto 1 (CTC 1) de la ISO/CEI, el Instituto Europeo de Normas de Telecomunicaciones y otros órganos.

5. Los conjuntos de atributos a efectos de la gestión de la identidad deberían ser definidos por los regímenes jurídicos que regulan las actividades comerciales de los operadores especializados en realizar tareas de identificación y los operadores funcionales, y pueden ser apoyados por los servicios de TIC de confianza apropiados. Las actividades de los operadores pueden regularse mediante requisitos organizativos y técnicos centrados en la protección de los datos personales, entre otras cosas.

Los conjuntos de atributos a efectos de la gestión de la identidad y los propios procedimientos de identificación pueden servir de base para la definición de los niveles de confianza de los sistemas de identificación. Esos niveles de confianza podrían revestir la máxima importancia en la reglamentación de la interacción entre diferentes agrupaciones de confianza (véase el párrafo 9).

6. Se propone que se faciliten descripciones de los mecanismos de interacción de determinados Estados y sus alianzas internacionales con otros órganos internacionales en el marco del establecimiento de un ECT común en la esfera del comercio electrónico:

6.1. Sobre la base de la adhesión a un régimen jurídico vigente que ofrezca garantías institucionales a las entidades que interactúen electrónicamente:

- La adhesión total de un Estado a un régimen jurídico vigente, sobre la base de tratados internacionales o reglamentos internacionales de aplicación directa, en los que se prevea o se disponga el establecimiento de un ECT regional en la esfera del comercio electrónico, incluidos los servicios funcionales previstos o establecidos en el marco de ese ECT;

- La adhesión parcial de un Estado a un régimen jurídico vigente sobre la base de tratados internacionales o reglamentos internacionales de aplicación directa mediante la adopción de disposiciones concretas relativas al establecimiento de un ECT regional o funcional en la esfera del comercio electrónico;

6.2. Sobre la base de la interacción entre diversas alianzas internacionales:

- En la primera fase, un grupo de Estados crea una agrupación regional de ECT en la esfera del comercio electrónico aislada, con inclusión de servicios funcionales de ECT en la esfera del comercio electrónico prestados en el marco de ese ECT, que ofrezca garantías institucionales a las entidades que interactúen electrónicamente en el marco del régimen jurídico especificado por esos Estados y que garantice la seguridad de las operaciones de comercio electrónico;

- En la segunda fase se definen los protocolos y mecanismos de interacción de confianza con otras alianzas internacionales en lo relativo al reconocimiento recíproco de los distintos regímenes jurídicos. Para ese reconocimiento recíproco se deberían tener en cuenta las garantías institucionales y los requisitos de seguridad de la información correspondientes a cada uno de esos órganos internacionales, posiblemente sobre la base de pasarelas de seguridad de la información (PSI) que funcionen en el marco de un régimen jurídico especial y que estén encargadas de la gestión de la identidad;

6.3. Sobre la base de la interacción entre un Estado y otros Estados o alianzas internacionales:

- En la primera fase, un Estado crea una agrupación nacional de ECT en la esfera del comercio electrónico aislada que funciona en el marco de un régimen jurídico nacional determinado por ese Estado;

- En la segunda fase se definen los protocolos de la interacción de confianza con otros Estados o alianzas internacionales en lo relativo al reconocimiento recíproco de regímenes jurídicos diferentes. En ese reconocimiento recíproco se deberían tener en cuenta las garantías institucionales y los requisitos de seguridad de la información correspondientes a esos Estados y órganos internacionales, posiblemente sobre la base de pasarelas de seguridad de la información (PSI) que funcionen en el marco de un régimen jurídico especial y que estén encargadas de la gestión de la identidad.

7. Se propone que se ofrezca una descripción de los mecanismos de formación de agrupaciones, similares a los que se describen en el párrafo 6, para los regímenes jurídicos basados en acuerdos comerciales o en la práctica comercial común.

8. Se propone que se ofrezca una descripción de los mecanismos para establecer un ECT mundial en la esfera del comercio electrónico sobre la base de la integración de diversas agrupaciones en una sola matriz formada de conformidad con los siguientes parámetros de información de entrada:

- Tipos de servicios funcionales y alcance regional;

- Tipos de regímenes jurídicos y sus variantes.

9. Se propone que se ofrezca una descripción de los enfoques para el establecimiento de varios tipos de pasarelas de seguridad de la información (PSI) como elementos fundamentales para la creación de una matriz mundial de un ECT en la esfera del comercio electrónico a fin de garantizar la seguridad de las operaciones de comercio electrónico.

Garantizar que se cumplan las condiciones para la interacción entre distintas agrupaciones del ECT mundial en el comercio electrónico y que esa interacción sea segura podría ser uno de los objetivos del establecimiento de esas pasarelas de seguridad de la información (PSI). Todos los aspectos tecnológicos, organizativos y jurídicos necesarios se podrían considerar al establecer las pasarelas de seguridad de la información (PSI).

En los enfoques para establecer pasarelas de seguridad de la información (PSI) genéricas se deberían tener en cuenta los distintos niveles posibles de interacción entre distintas agrupaciones de ECT en la esfera del comercio electrónico. El establecimiento de pasarelas que realizan la gestión de la identidad, por ejemplo, se puede realizar ya sea únicamente a nivel jurídico y organizativo, o bien a un nivel más complejo, que abarque los aspectos jurídicos, organizativos y tecnológicos.

En los enfoques para establecer pasarelas de seguridad de la información (PSI) genéricas se debería tener en cuenta el uso de perfiles de transición que describan y definan la transición de una agrupación a otra. En esos perfiles de transición se podría tener en cuenta el nivel de confianza en los sistemas de identificación utilizados en las agrupaciones que interactúan entre sí (véase el párrafo 5).

La descripción de diversos tipos de pasarelas de seguridad de la información (PSI) podría estar sujeta a recomendaciones y normas técnicas de la UIT y el CTC-1.

Establecimiento de un ECT en la esfera del comercio electrónico mediante una infraestructura de confianza unificada

Como se ha expuesto anteriormente, el principal objetivo del establecimiento de un ECT en la esfera del comercio electrónico es prestar a los usuarios servicios de confianza de varios niveles (básico, mediano y alto) con la ayuda de un sistema de gestión de la identidad durante el curso de su interacción electrónica.

El ECT en la esfera del comercio electrónico es una plataforma fundamental, fácilmente ampliable, que ofrece un acceso unificado y seguro a servicios de confianza electrónicos mediante el uso de un sistema de gestión de la identidad. Como se tienen en cuenta los sistemas electrónicos de gestión de la identidad existentes, se prevé que los requisitos para la mejora de esos sistemas y mecanismos a fin de que puedan incluirse en el ECT en la esfera del comercio electrónico serían mínimos.

Durante la elaboración del sistema de ECT en la esfera del comercio electrónico se propuso una arquitectura de infraestructura de confianza común (ICC), se describieron las interconexiones entre sus distintos componentes y su interacción con los usuarios y, simultáneamente, se llevaron a cabo trabajos en tres esferas, a saber, la tecnológica, la organizativa y la jurídica. Mediante un análisis de las opciones para la aplicación práctica y las hipótesis de una ICC se pudo producir una lista de la documentación necesaria para una especificación completa del sistema. La arquitectura de la ICC fue diseñada de forma que fuera fácil ajustarla a escala. Puede ampliarse fácilmente a cualquier nivel mediante la adición de nuevos componentes, como nuevos sistemas jurídicos, nuevos participantes supranacionales o nuevos operadores de servicios de confianza y de datos de identidad.

Aspectos técnicos y tecnológicos de la ICC

Puede haber muchos mecanismos tecnológicos para la prestación de servicios de gestión de la identidad y de confianza. El requisito principal que se aplica a los elementos de la ICC es que garanticen la interoperabilidad. La regulación a este nivel se facilitaría mediante diversas normas e instrucciones, que estarían previstas en la documentación de un Consejo de Coordinación de Reguladores del Intercambio de Confianza de Datos Electrónicos (CCRICDE). La utilización de un mecanismo de gestión de la identidad como por ejemplo, una firma electrónica en la interacción electrónica transfronteriza es un ejemplo del funcionamiento tecnológico de los servicios de confianza. A efectos de comparación, se presentan dos opciones de implantación de la ICC: un sistema descentralizado con un nivel de confianza nocionalmente bajo entre los participantes en la interacción informativa (véase el gráfico 1) y un sistema centralizado con un nivel mediano de confianza entre esos participantes (véase el gráfico 2).

En el cuadro 1 se exponen las características de los sistemas de ICC descentralizados y centralizados. En el cuadro 2 se describe el procedimiento para utilizar una firma electrónica como mecanismo del sistema de gestión de la identidad para los dos planes de implantación de la ICC.

Cuadro 1

Utilización de un mecanismo de gestión de la identidad en una ICC para interacción informativa, con niveles de confianza bajos y medianos

Nivel de confianza bajo (gráfico 3)	Nivel de confianza mediano (gráfico 4)
1. Los operadores nacionales de servicios de apostilla prestan servicios de apostilla. Esos operadores también pueden prestar otros servicios de gestión de la identidad. 2. Las organizaciones internacionales (operadores y reguladores) no participan. 3. Los reguladores nacionales interactúan directamente, intercambiando certificados de seguridad. 4. Los reguladores nacionales garantizan el funcionamiento de los operadores nacionales de servicios de confianza en su jurisdicción en relación con sus certificados y los de los reguladores nacionales en el marco de otras jurisdicciones.	1. Los operadores nacionales de servicios de apostilla prestan servicios de apostilla. Esos operadores también pueden prestar otros servicios de gestión de la identidad. 2. Las organizaciones internacionales participan: un regulador internacional de ICC y operadores internacionales de servicios de confianza. 3. Los reguladores nacionales de ICC se comunican únicamente a través del regulador supranacional de ICC. Los operadores nacionales de servicios de confianza también se comunican únicamente a través de sus respectivos operadores internacionales. 4. El regulador internacional de ICC proporciona la certificación centralizada de los operadores nacionales de servicios de confianza y los reguladores nacionales de ICC. 5. Los reguladores nacionales garantizan el funcionamiento de los operadores nacionales de servicios de confianza en su jurisdicción en relación con sus certificados y los certificados del regulador internacional.

Cuadro 2

Procedimiento para la utilización de firmas electrónicas como mecanismo del sistema de gestión de la identidad en planes con niveles de confianza bajos y medianos

Nivel de confianza bajo (gráfico 3)	Nivel de confianza mediano (gráfico 4)
1. La persona natural/jurídica I envía documentos con una firma electrónica en la jurisdicción J, seleccionando el nivel requerido de servicios de confianza prestados por la ICC (básico, mediano o alto).	1. La persona natural/jurídica I envía documentos con una firma electrónica en la jurisdicción J, seleccionando el nivel requerido de servicios de confianza prestados por la ICC (básico, mediano o alto).
2. Se envía una solicitud para verificar los documentos firmados electrónicamente en la jurisdicción J al operador del servicio nacional de apostilla en la jurisdicción Q.	2. Se envía una solicitud para verificar los documentos firmados electrónicamente en la jurisdicción J al operador internacional del servicio de apostilla I-J-Q.
3. La solicitud de verificación se reenvía al operador nacional del servicio de apostilla en la jurisdicción J.	3. En la jurisdicción J se lleva a cabo la verificación matemática de la firma electrónica.
4. En la jurisdicción J se lleva a cabo la verificación matemática de la firma electrónica.	4/5. Se envía al operador nacional de servicios de firma en la jurisdicción J una solicitud/respuesta en relación con la situación del certificado.
5/6. Se envía al operador nacional de servicios de firma en la jurisdicción J una solicitud/respuesta en relación con la situación del certificado.	6. El operador internacional del servicio de apostilla I-J-Q certifica la solicitud y la reenvía a la persona natural/jurídica 2.
7. El operador nacional del servicio de apostilla en la jurisdicción Q recibe la confirmación de que la firma electrónica es correcta en la jurisdicción J.	
8. El operador nacional del servicio de apostilla en la jurisdicción Q certifica la solicitud y la reenvía a la persona natural/jurídica 2.	

Gráfico 1

Verificación de la firma electrónica en el marco de un ECT con un nivel de confianza bajo (opción descentralizada)

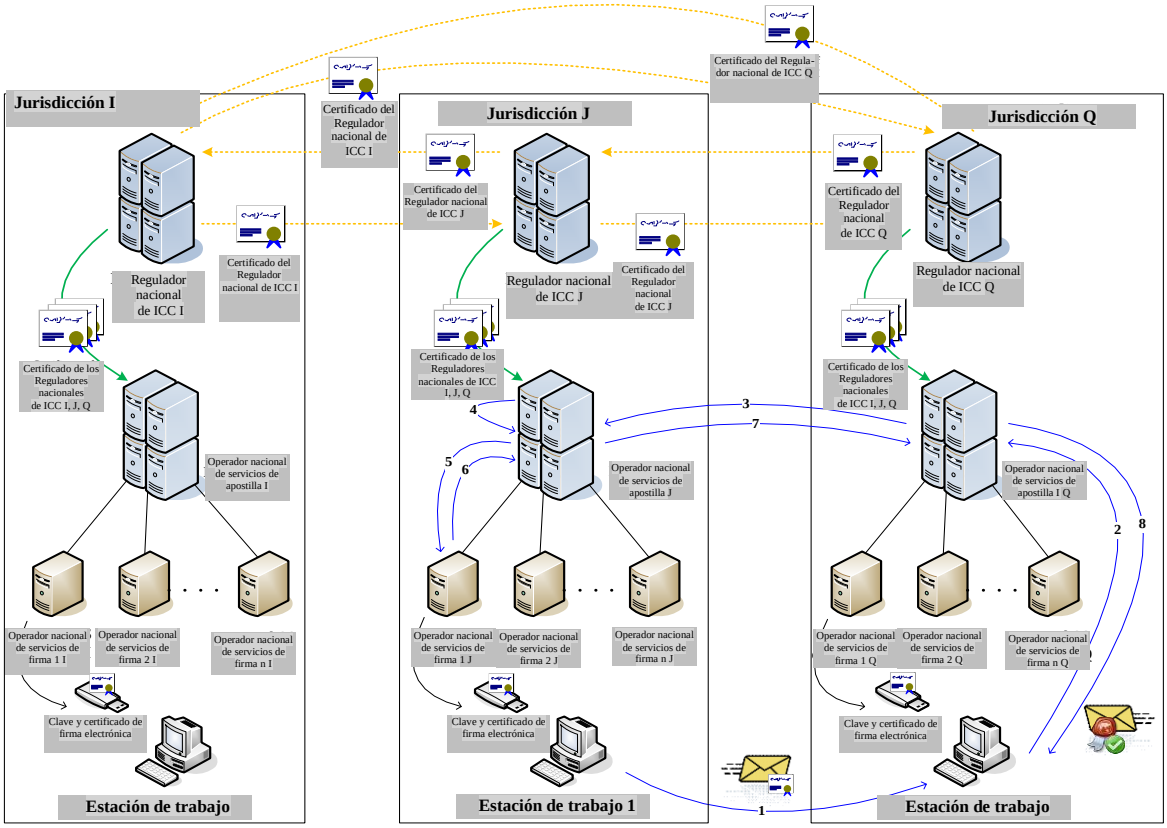
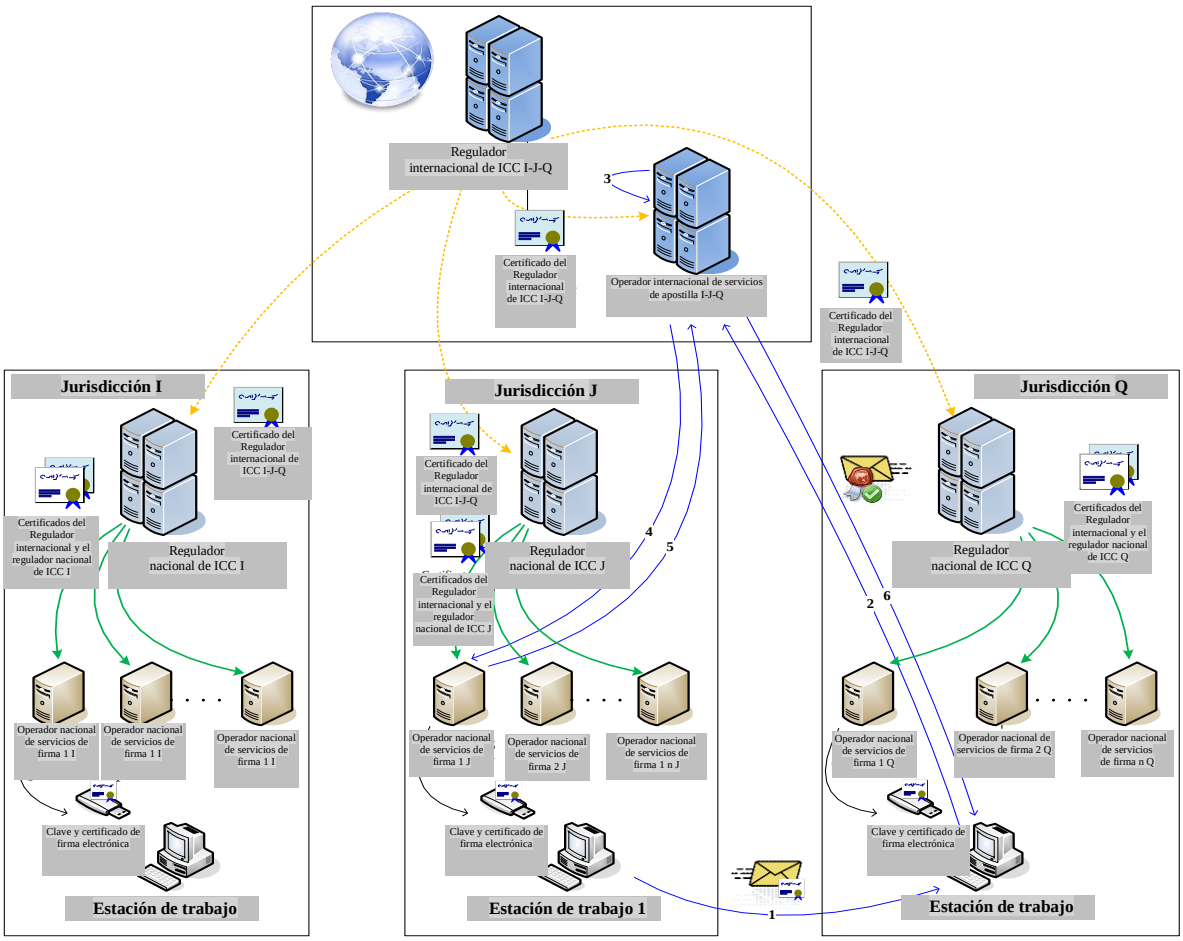


Gráfico 2

Verificación de la firma electrónica en el marco de un ECT con un nivel de confianza mediano (opción descentralizada)

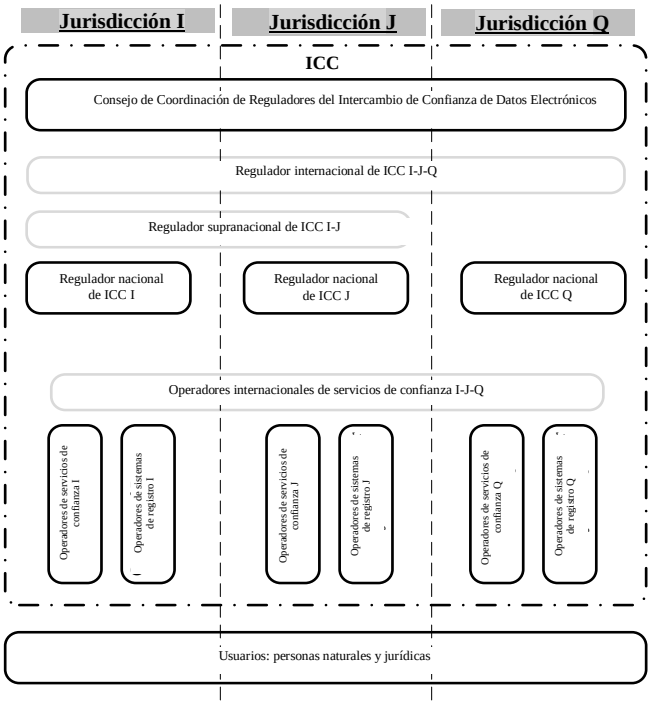


Aspectos de organización

El reconocimiento jurídico recíproco de servicios de gestión de la identidad y de confianza prestados en el marco de las jurisdicciones de diversos Estados se lograría mediante el establecimiento y funcionamiento de un Consejo de Coordinación de Reguladores del Intercambio de Confianza de Datos Electrónicos (CCRICDE). Las actividades de ese consejo de coordinación se regirían por sus estatutos, que todos sus miembros autorizados, es decir, los órganos encargados de regular el intercambio electrónico de datos, representados en primer lugar por los reguladores nacionales de ICC, reconocerían y firmarían.

La regulación organizativa se ilustra en el siguiente diagrama (véase el gráfico 3):

Gráfico 3
Regulación organizativa del entorno de confianza transfronterizo
(los elementos optativos se indican en los recuadros de texto en gris)



El consejo de coordinación publicaría un conjunto de documentos, estando consagrada su facultad para hacerlo en sus estatutos:

- Requisitos de los miembros del consejo de coordinación, cuyo cumplimiento sería un requisito previo para ser miembro de pleno derecho del consejo de coordinación;
- Directrices para realizar supervisión preliminar “en la sombra” para ser admitido en el consejo de coordinación y auditorías mutuas periódicas a fin de mantener la condición de miembro voluntario;
- Criterios de cumplimiento para los operadores de servicios de ICC y para operadores de servicios de gestión de la identidad y de confianza, y la metodología para aplicar esos criterios;
- Un sistema para evaluar/verificar el cumplimiento de esos criterios por los operadores de servicios de ICC y los operadores de servicios de gestión de la identidad y de confianza.

En un ECT en la esfera del comercio electrónico, cada sistema jurídico está representado por un regulador nacional de ICC (véase el gráfico 3, reguladores nacionales de ICC I, J y Q), que regula las actividades de los operadores de servicios de confianza y de servicios de gestión de la identidad en su jurisdicción.

Es probable que grupos de Estados estrechamente integrados (como la Comunidad Económica de Eurasia o la Unión Europea) establezcan un regulador supranacional de ICC (véase el gráfico 3, “Regulador supranacional de ICC I-J”). Por tanto, un solo regulador nacional de ICC I-J sustituiría al grupo de reguladores nacionales de ICC I y J.

El procedimiento de admisión de nuevos miembros en el consejo de coordinación (nuevos sistemas jurídicos y participantes supranacionales) y el sistema para verificar el cumplimiento por los operadores de servicios de ICC y de gestión de la identidad de los criterios publicados por el consejo de coordinación (para nuevos operadores de servicios de gestión de la identidad y de servicios de confianza) permite que la ICC sea ampliable.

Si los miembros del consejo de coordinación (véase más abajo) han logrado un nivel de confianza nominalmente "mediano", pueden iniciar el establecimiento de un regulador internacional de ICC y de operadores internacionales de servicios de gestión de la identidad y de servicios de confianza (véase el gráfico 3; "Regulador internacional de ICC I-J-Q" y "Operadores internacionales de servicios de confianza I-J-Q"). El regulador internacional de ICC coordinaría la interacción entre los operadores internacionales de servicios de confianza, los reguladores nacionales de ICC (con arreglo a los estatutos del consejo de coordinación) o los reguladores supranacionales de ICC.

Para llegar a ser un operador nacional de servicios de confianza o un operador de sistemas de registro, los proveedores de esos servicios tendrían que obtener la acreditación a través del regulador nacional de ICC del mismo Estado. Los operadores internacionales de servicios de confianza tendrían que obtener la acreditación a través del regulador internacional de ICC. Los requisitos de acreditación para los operadores de servicios de confianza y de sistemas de registro y los requisitos aplicables a sus actividades estarían regulados por los criterios de cumplimiento publicados por el consejo de coordinación y posiblemente por suplementos nacionales publicados por el regulador correspondiente.

Tanto las personas naturales como las jurídicas pueden ser usuarios de servicios electrónicos en el marco del ECT en la esfera del comercio electrónico. Los usuarios elegirían el nivel necesario de servicio de confianza a discreción propia o mediante un acuerdo.

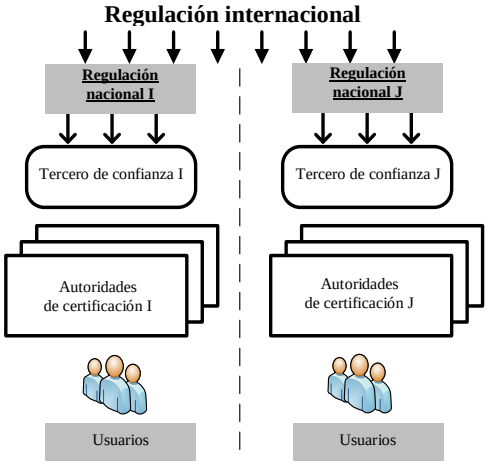
Los proveedores u operadores apropiados de servicios de confianza prestarían los servicios. En algunos casos, también podrían prestar servicios los operadores de sistemas de registro. Los operadores de servicios de confianza y de sistemas de registro estarían unidos por una infraestructura de confianza común.

Pueden existir varias opciones de implantación de servicios de confianza que formen parte del ECT en la esfera del comercio electrónico, según el nivel de confianza entre los participantes en la interacción informativa. Por ejemplo, a niveles de confianza recíproca nominalmente altos y medianos entre los miembros del consejo de coordinación, se podrán utilizar eficazmente servicios internacionales centralizados prestados de conformidad con normas convenidas. En el caso de un nivel de confianza nominalmente bajo, la prestación de servicios de confianza se realizaría con arreglo al principio de descentralización, es decir, en función de los servicios nacionales de cada Estado.

Aspectos jurídicos

Se puede construir un ECT en la esfera del comercio electrónico sobre la base de un solo dominio o varios dominios. Una base de varios dominios es la opción más compleja desde un punto de vista jurídico y organizativo. Un sistema de varios dominios exige la utilización de los recursos técnicos de un tercero de confianza. En el gráfico 4 se muestra una representación esquemática general de la regulación jurídica.

Gráfico 4
Regulación jurídica del entorno de confianza transfronterizo



La regulación jurídica de la interacción informativa transfronteriza puede dividirse en dos partes: internacional y nacional. La reglamentación jurídica internacional se llevaría a cabo sobre la base de los siguientes tipos de documentos:

- Tratados y acuerdos internacionales;
- Instrumentos de diversas organizaciones internacionales;
- Normas y reglas internacionales;
- Acuerdos entre participantes en interacción informativa transfronteriza sobre cuestiones específicas;
- Legislación modelo.

La regulación jurídica nacional se basaría de manera similar en un conjunto de instrumentos reguladores específicos de cada sistema jurídico concreto.

Resumen

El material presentado anteriormente muestra que el establecimiento de un ECT en la esfera del comercio electrónico ofrece los medios óptimos de mejorar el sistema de gestión de la identidad por los siguientes motivos:

- El establecimiento de agrupaciones de confianza nacionales, regionales e internacionales garantizaría una mayor interoperabilidad de los mecanismos de gestión de la identidad como, por ejemplo, las firmas electrónicas;
- El reconocimiento jurídico recíproco de los servicios de gestión de la identidad y de confianza prestados en el marco de la jurisdicción de diversos Estados permitiría formular un enfoque común de la normalización de los sistemas de gestión de la identidad;
- La adopción de tratados y acuerdos internacionales y normas y reglamentos internacionales sobre la utilización de un ECT permitiría aumentar el nivel de confianza de los participantes en el comercio electrónico, lo que a su vez permitiría simplificar la implantación de la gestión de la identidad;
- Las actividades del consejo de coordinación (CCRICDE) permitirían elaborar criterios de cumplimiento unificados que habrían de cumplir los operadores de servicios de gestión de la identidad y de servicios de confianza, así como la metodología para aplicar esos criterios.

La mejora de los sistemas de gestión de la identidad crearía a su vez condiciones seguras para las actividades comerciales internacionales transfronterizas. El establecimiento de un ECT en la esfera del comercio electrónico exige la ejecución de una serie de medidas relacionadas con el sistema, a saber;

- La implantación de soluciones técnicas para garantizar la seguridad y la confidencialidad de la información;
- La implantación de soluciones organizativas mediante el establecimiento de un órgano coordinador;
- La implantación de soluciones jurídicas y reglamentarias mediante la elaboración de tratados internacionales sobre la utilización de un ECT en la esfera del comercio electrónico.

La organización de un ECT en la esfera del comercio electrónico exigirá asimismo la coordinación entre las organizaciones cuya labor se refiera a cuestiones relacionadas con la gestión de la identidad y el comercio transfronterizo (entre ellas la ISO, la UIT, el Centro para la Facilitación de los Procedimientos y Prácticas para la Administración, el Comercio y el Transporte (CEFACT), la Comisión Económica para Europa (CEPE), la CNUDMI y el Foro APEC) con miras a elaborar un enfoque común de la normalización del uso de un ECT en la esfera del comercio electrónico como mecanismo de gestión de la identidad, así como de la utilización de un ECT en la esfera del comercio electrónico para la interacción electrónica transfronteriza y las actividades comerciales.

El siguiente paso para hacer progresar este proceso consistiría en un debate sobre la experiencia y los conocimientos especializados con diversos asociados (expertos y organizaciones) interesados en facilitar, simplificar y, al mismo tiempo, dar efecto jurídico a los servicios electrónicos transfronterizos.

Esos asociados interesados podrían ser en primer lugar organizaciones políticas o económicas[6]. Entre los órganos políticos que ya emprenden parcialmente labores en esa esfera figuran tanto organizaciones supranacionales (como la Comunidad de Estados Independientes (CEI), el Foro APEC, la Unión Europea y la Organización de Cooperación de Shanghai) como órganos establecidos en el marco de relaciones bilaterales entre determinados Estados. Entre los órganos económicos interesados en alcanzar ese objetivo figuran, por ejemplo, los órganos competentes de las Naciones Unidas, como el CEFACT, la CEPE, la CNUDMI (Grupos de Trabajo III y IV), el Espacio Económico Europeo y la Comunidad Económica de Eurasia. Cabe suponer que, debido a las características naturales específicas (incluidas las características históricas, culturales, políticas, económicas y técnicas) de las distintas regiones del mundo, diversas organizaciones internacionales o regionales de países establezcan sus órganos de coordinación (consejos de coordinación de reguladores del intercambio de confianza de datos electrónicos) y arquitectura de ICC propios, según el nivel de confianza en cada formato y las características antes mencionadas.

Creemos por tanto que, durante las primeras etapas de ejecución de este proyecto, no existirá un “dominio de confianza” mundial único (por ejemplo, a nivel de una de las organizaciones de las Naciones Unidas), sino antes bien varios dominios de confianza a nivel regional e, incluso, a nivel nacional[7]. No obstante, incluso el establecimiento de

[6] Otras organizaciones humanitarias también podrían estar interesadas en este producto –por ejemplo, en la esfera del derecho, la Conferencia de La Haya de Derecho Internacional Privado– así como organizaciones en las esferas de la medicina y la educación; sin embargo, en nuestra opinión, es más probable que esas organizaciones utilicen un ECT ya establecido en lugar de apoyar la elaboración de un nuevo producto.

[7] Un entorno informativo y jurídico en el que se utiliza la misma ICC.

dominios de confianza por separado mejoraría el sistema de gestión de la identidad, dada la necesidad de garantizar la interoperabilidad en los dominios de confianza.

Una vez que se haya determinado la arquitectura de la ICC (en el dominio de confianza pertinente), puede comenzar la labor de redacción de otro conjunto de documentos organizativos, reglamentarios y técnicos negociados en el marco del consejo de coordinación. Así, quedaría garantizada la interoperabilidad en el marco del dominio de confianza pertinente.

La adopción de ese conjunto de documentos por los miembros del consejo de coordinación (en el dominio de confianza pertinente) facilitaría la transición a la etapa final de implantación práctica de los sistemas para la interacción electrónica transfronteriza con efectos jurídicos.

Observaciones a la atención de los expertos del Grupo de Trabajo IV sobre Comercio Electrónico de la CNUDMI

El problema de garantizar la seguridad y la identificación de entidades y objetos en el comercio electrónico puede resolverse mediante el modelo propuesto más arriba (modelo para el establecimiento y funcionamiento de un ECT en la esfera del comercio electrónico en forma de una matriz construida sobre la base de agrupaciones regionales y mundiales interconectadas que incluyen los servicios funcionales prestados en el marco de ese ECT en la esfera del comercio electrónico) del siguiente modo:

- Se establecería una agrupación funcional de ECT en la esfera del comercio electrónico especializada en la creación de una zona de confianza para la gestión de la identidad en relación con las operaciones transfronterizas de comercio electrónico;
- En términos geográficos, podrían estar incluidos en esa agrupación todos los Estados Miembros de las Naciones Unidas;
- El funcionamiento de la agrupación estaría garantizado a través de las actividades comerciales de un operador especializado o grupo de operadores especializados interconectados;
- El suministro de conjuntos de servicios de gestión de la identidad de confianza basados en una serie de planes de identificación adoptados en el marco de plataformas de comercio electrónico podría ser una esfera de las actividades comerciales de los operadores especializados;
- El régimen jurídico de las actividades comerciales de los operadores especializados se establecería en el marco de acuerdos con plataformas de comercio electrónico.