ANEXO
EJEMPLOS DE DISPOSICIONES SOBRE LA IDENTIDAD DIGITAL QUE PODRÍAN INCLUIRSE EN LOS ACUERDOS COMERCIALES[1]

ARTÍCULO 1: RECONOCIMIENTO MUTUO DE IDENTIDADES DIGITALES DE CONFIANZA

1. Las Partes reconocen que los sistemas de identidad digital de confianza contribuyen a crear cadenas de suministro más seguras y ágiles y pueden ser un catalizador para facilitar el comercio.

2. Las Partes convienen en elaborar o mantener un marco jurídico que haga posible el funcionamiento de un sistema de identificación digital de confianza. Ese marco deberá ser compatible con los principios de la CNUDMI y otros principios y normas pertinentes que ya existen.

3. Las Partes convienen en adoptar procedimientos mutuamente reconocidos para la emisión y verificación de identidades (a través de entidades legalmente constituidas en las jurisdicciones de las Partes), entre ellos, los siguientes:

   (a) Acuerdo sobre el nivel mínimo y el tipo de información (o atributos) que deben ser verificados y validados para la emisión de identidades de confianza. Este "identificador digital"[2] constará de uno o más atributos que solo pueden caracterizar a una entidad.

   (b) Acuerdo sobre la información electrónica o las fuentes de datos que han de utilizarse para documentar que una entidad es una persona jurídica bajo la jurisdicción específica de las Partes.

   (c) Todas las Partes deben asegurarse de que se mantengan continuamente y comuniquen de inmediato las actualizaciones de la condición jurídica de una entidad. Tan pronto como cambie la condición jurídica de una entidad, esta nueva información se facilitará en línea a todas las partes interesadas que tengan la intención de interactuar con la persona jurídica.

   (d) Cada Parte tiene derecho a autorizar a un organismo (parte de confianza) para que apruebe el establecimiento de una persona jurídica dentro de su jurisdicción.

   (e) Las Partes convienen en determinar qué instituciones pueden actuar como parte de confianza (por ejemplo, las instituciones financieras) para confirmar la validez de una prueba física de constitución (y posteriormente emitir una identidad digital). Esas partes de confianza tienen que ser ratificadas como tales mediante acuerdo de todas las Partes.

   (f) Las nuevas partes de confianza que se propongan deberán ser aceptadas por todas las Partes en el Acuerdo.

   (g) Si aún no hay un proceso de digitalización en marcha, las autoridades de confianza de cada Parte tomarán medidas para digitalizar el proceso de incorporación de personas jurídicas lo antes posible.

4. Cada Parte procurará evitar toda carga reglamentaria innecesaria.

5. Las Partes procurarán recomendar la utilización de las normas existentes cuando sea posible y elaborar normas comunes cuando sea necesario.

6. Todas las Partes deberán adoptar o mantener leyes y reglamentos para la protección de la información personal facilitada. El sistema de identidad digital de confianza deberá funcionar de manera que permita a las instituciones participantes proteger los datos sensibles y reconocer las expectativas culturales y éticas sobre la protección de los datos y la privacidad. Asimismo, tomará debidamente en consideración las normas internacionales de protección de datos.

7. El reconocimiento mutuo de los sistemas de identidad digital de confianza puede interrumpirse temporalmente o suspenderse por completo si los sistemas y procesos gubernamentales de emisión de identidades corren peligro o han sido destruidos o corrompidos. Las Partes procurarán evaluar alternativas u otros mecanismos que puedan estar disponibles.

8. Nada impedirá que una Parte adopte o mantenga medidas incompatibles con las disposiciones anteriores para alcanzar un objetivo legítimo de política pública.

9. La autenticación de la identidad de una persona jurídica solo es un primer paso hacia el comercio sin papel. Un segundo paso consistiría en utilizar el sistema para autorizar y expedir documentos comerciales como licencias y certificados. Las Partes tal vez deseen considerar la posibilidad de incluir en su ACR un texto similar al siguiente, además de las disposiciones enumeradas *supra*.

ARTÍCULO 2: ASEGURAR LA PROTECCIÓN DE LOS DOCUMENTOS COMERCIALES MEDIANTE FIRMAS DIGITALIZADAS DE CONFIANZA

1. Las Partes reconocen la importancia de asegurar que los documentos comerciales firmados digitalmente sean expedidos por un agente autorizado, que no hayan sido manipulados y que solo las entidades autorizadas tengan acceso a ellos.

2. Las Partes convienen de común acuerdo qué autoridades públicas u otras organizaciones están autorizadas para firmar documentos comerciales, enviar transacciones y emitir esos documentos. Esas autoridades públicas deben ser reconocidas como dignas de confianza por todas las Partes.

3. En relación con los documentos comerciales, las Partes convienen de mutuo acuerdo en aceptar las firmas electrónicas que se consideren de efectos jurídicos equivalentes a los de una firma manuscrita con arreglo a la legislación de una de las Partes, a menos que una Parte pueda demostrar que existe una duda razonable sobre la fiabilidad de la firma electrónica.

4. Un agente del país importador puede verificar que el agente exportador que ha firmado digitalmente el documento comercial es un emisor autorizado de un documento específico sujeto a la jurisdicción del país exportador.

ARTÍCULO 3: COOPERACIÓN

1. Las Partes procurarán mantener un diálogo sobre las cuestiones de reglamentación planteadas por los sistemas de identidad digital de confianza. En particular, procurarán:

   (a) Intercambiar información y buenas prácticas sobre:

   (i) el funcionamiento y la gestión de los sistemas de identidad digital de confianza;

   (ii) las políticas, los reglamentos y las medidas de observancia y cumplimiento relativos a la forma en que se aseguran los sistemas de tecnología de la información.

   (b) Cooperar para abordar los obstáculos legislativos, reglamentarios y técnicos lo antes posible.

2. Las Partes colaborarán para ayudar a las pymes a participar plenamente en esos sistemas.

3. Las Partes reafirman la importancia de participar activamente en los foros pertinentes, incluidos los foros multilaterales, para promover el desarrollo de sistemas de identidad digital de confianza y la emisión de documentos comerciales acreditados mediante firmas digitales de confianza.

También debe considerarse la posibilidad de incluir disposiciones similares en otros acuerdos comerciales, empezando por el nuevo conjunto de normas que se están elaborando en el contexto de la iniciativa relativa a la Declaración Conjunta sobre el Comercio Electrónico de la OMC.

NOTAS FINALES

1. Basados en https://www.unescap.org/sites/default/files/86%20Final-Team%20Hanna%20Norberg-Sweden.pdf.
2. Un identificador digital está compuesto por uno o varios atributos que caracterizan solo a una entidad en un contexto específico. Es utilizado por las Partes como clave por la que expresan su acuerdo sobre la entidad representada (ISO/CEI 29115:2013).