الأمم المتحدة

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

الجمعية العامة

Distr.: Limited
30 September 2020
Arabic
Original: English

لجنة الأمم المتحدة للقانون التجاري الدولي
الفريق العامل الرابع (المعني بالتجارة الإلكترونية)
الدورة الستون
فيينا (عبر الإنترنت)، 19-23 تشرين الأول/أكتوبر 2020

إعادة النظر في النهج المتبع إزاء إدارة الهوية وخدمات توفير الثقة

ورقة مقدمة من الولايات المتحدة الأمريكية

مذكرة من الأمانة

قدمت الولايات المتحدة الأمريكية ورقة لكي ينظر فيها الفريق العامل خلال دورته الســـتين. وترد في مرفق هذه المذكرة ترجمة لصيغتها التي تلقتها بها الأمانة.

141020 141020 V.20-05626 (A)

المرفق

إعادة النظر في النهج المتبع إزاء إدارة الهوية وخدمات توفير الثقة

1- يسر الولايات المتحدة أن تقدم هذه الورقة عن المشروع الذي يضطلع به حاليا الفريق العامل الرابع بشأن نظم إدارة الهوية وخدمات توفير الثقة. وتنقسم هذه الورقة إلى ثلاثة أقسام، يقدم القسم الأول منها لمحة عامة عن القسمين التاليين وخلاصة وافية لهما. ويعرض القسم الثاني معلومات أساسية عن نظم إدارة الهوية وقواعد تشغيلها. وأخيرا، يقدم القسم الثالث لمحة عامة عن الإطار القانوني الذي يستند إليه تشغيل جميع نظم إدارة الهوية عموما، كما يقدم إطارا مفاهيميا للكيفية التي يمكن بها للفريق العامل أن يعدل مشاريع الأحكام الواردة في الوثيقة WP.162 بحيث تعالج بفعالية موضوع نظم إدارة الهوية التابعة للقطاع الخاص.

2- ولأغراض هذه الورقة، يقتصر تركيز الولايات المتحدة على موضوع نظم إدارة الهوية وكيف يمكن للفريق العامل أن يعالج هذا الموضوع بفعالية. ومع ذلك، ترحب الولايات المتحدة بإجراء مناقشة مماثلة في الفريق العامل حول الجزء المتعلق بخدمات توفير الثقة من مشاريع الأحكام الواردة في الوثيقة WP.162، حيث نعتقد أن ذلك الجزء يثير العديد من المسائل المفاهيمية نفسها، كما هو مبين أدناه فيما يتعلق بالأحكام التي تتناول نظم إدارة الهوية.

أولا- لمحة عامة وخلاصة وافية

3- من منظور عام، توجد لدى الولايات المتحدة شواغل أساسية بشأن النهج الذي يتبعه الفريق العامل حاليا فيما يتعلق بمسألة نظم إدارة الهوية كما يتجسد في الوثيقة WP.162 (انظر التذييل [بالإنكليزية])، وترى أن من الضروري إجراء مناقشة في الفريق العامل على المستوى المفاهيمي من أجل معالجة هذه الشواغل.

4- وينبغي أن تتمثل مهمة الأونسيترال في توفير إطار يمكن أن يساعد الدول على معالجة المسائل القانونية التي قد تنشأ فيما يتعلق بنظم إدارة الهوية التابعة للقطاع الخاص، ولا سيما في سياق المجالات التي لا يمكن أن تتناولها قواعد التشغيل التعاقدية التي يختص بها كل نظام من نظم إدارة الهوية. ويمكن أن ينطوي ذلك على تنقيح الأحكام القانونية الوطنية القائمة لإزالة ما يرد فيها من المعوقات وأوجه عدم اليقين، أو سد ما قد يوجد في الأحكام القانونية القائمة المتعلقة بنظم إدارة الهوية من ثغرات لا يمكن معالجتها عن طريق التعاقد، أو معالجة مسائل جديدة يمكن أن تعزز تطوير نظم الهوية التابعة للقطاع الخاص. بيد أن الوثيقة WP.162 تتبع نهجا يختلف عن ذلك كثيرا، وهو نهج ترى الولايات المتحدة أنه غير قابل للتطبيق عمليا.

ألف- ما هي نظم إدارة الهوية؟

5- تنطوي **إدارة الهوية** على مجموعة من السياسات والعمليات والإجراءات التي تتيح تحديد هوية شخص ما أو كيان ما (أي إجابة السؤال: "من أنت؟") والتوثق من تلك الهوية (أي إجابة السؤال: "كيف يمكنك أن تثبت ذلك؟"). وكما هو مبين على نحو أوفى في القسم الثاني أدناه، فإن **معاملة الهوية** هي عملية اتصال تحمل بعض المعلومات عن هوية الكيان المعني إلى طرف معوِّل، بطريقة توثق العلاقة بين المعلومات المقدمة والكيان المعني. وتُستخدم نظم إدارة الهوية لتيسير إجراء **معاملات الهوية** من هذا القبيل. و**نظم إدارة الهوية** هي ترتيبات معقدة تنطوي على توليفة متناسقة من الكيانات المشاركة والعمليات والتكنولوجيا، بحيث يضطلع كل طرف مشارك في النظام بالمسؤوليات المنوطة بدور واحد أو أكثر من جملة أدوار محددة مسبقا، وفقا لمجموعة محددة مسبقا من العمليات والسياسات والإجراءات الملزمة قانونا، بغرض تيسير إجراء معاملات الهوية على نحو يتيح لفرد منتسب إلى النظام تحديد هويته لدى كيانات متعددة غير منتسبة إلى النظام.

6- وحتى يكون ذلك ممكنا، يتطلب كل نظام من نظم إدارة الهوية مجموعة من قواعد التشغيل الواجبة الإنفاذ. وكما هو مبين على نحو أوفى في القسم الثاني أدناه، فإن قواعد التشغيل تحكم تشغيل نظام بعينه لإدارة الهوية، حيث تحدد كيفية إجراء عمليات إدارة الهوية ومعاملات الهوية المناظرة لها، كما تحدد حقوق ومسؤوليات مختلف الأطراف المشاركة في النظام. وبالنظر إلى اختلاف كل نظام من نظم إدارة الهوية عن غيره، يتطلب كل نظام مجموعة فريدة من قواعد التشغيل المصممة خصيصا بمراعاة الغرض منه وهيكله وقاعدة الأطراف المشاركة فيه وأنماط المخاطر التي يواجهها.

7- وفي حالة نظم إدارة الهوية التابعة للقطاع العام، عادة ما يُنص على قواعد التشغيل في تشريع أو لائحة، ومن ثم تكتسب صفة الإلزام للأطراف المشاركة بقوة القانون. أما في حالة نظم إدارة الهوية التابعة للقطاع الخاص، فترد قواعد التشغيل في وثيقة يحررها مشغل النظام (أو شخص أو كيان آخر)، ومن ثم تكتسب صفة الإلزام للأطراف المشاركة عن طريق التعاقد.

باء- ما الذي ينبغي أن يتناوله الصك الذي تعده الأونسيترال؟

8- ينبغي لأي صك تضعه الأونسيترال بشأن نظم إدارة الهوية التابعة للقطاع الخاص أن يأخذ في الحسبان كلا من الأحكام القانونية الوطنية القائمة وقواعد التشغيل التعاقدية التي تختلف باختلاف نظام إدارة الهوية المحدد الذي تُستخدم فيه. وعلى وجه التحديد، ينبغي للصك الذي تعده الأونسيترال أن يعالج المسائل المتعلقة بانطباق الأحكام القانونية الوطنية القائمة على نظم إدارة الهوية التابعة للقطاع الخاص في إحدى حالتين: '1' إذا كانت تلك المسائل لا يمكن أن تتناولها قواعد التشغيل التعاقدية التي يختص بها كل نظام من نظم إدارة الهوية، أو '2' إذا كانت تلك المسائل تتسبب في مشاكل تؤثر في جميع نظم إدارة الهوية التابعة للقطاع الخاص. ومن ثم فمن أمثلة المجالات التي ينبغي تناولها في صك من إعداد الأونسيترال ما يلي: الاعتراف القانوني بمعاملات الهوية التي تجريها نظم إدارة الهوية التابعة للقطاع الخاص؛ والشروط التي يتقرر على أساسها ما إذا كانت معاملات الهوية التي يجريها نظام تابع للقطاع الخاص تستوفي المتطلبات القانونية المنطبقة فيما يخص تحديد هوية شخص ما؛ ومدى انطباق الأحكام القانونية التي لا يمكن تعديلها بمقتضى قواعد تشغيل نظم إدارة الهوية، مثل الأحكام المنصوص عليها في القوانين المتعلقة باستخدام محددات الهوية الصادرة من الحكومة، والقوانين المعنية بحماية المستهلك وبالمسؤولية التقصيرية.

9- ويستند هذا النهج إلى التسليم بأن نظم إدارة الهوية التابعة للقطاع الخاص تخضع لإطار قانوني من ثلاث طبقات، تحتل أعلاها الأحكام القانونية الوطنية القائمة (الطبقة 1)، وتأتي في أسفلها قواعد التشغيل التعاقدية التي يختص بها كل نظام من نظم إدارة الهوية (الطبقة 3). وتؤدي الطبقة الوسطى في هذا الإطار القانوني (الطبقة 2) دور الجسر بين الطبقتين 1 و3. وينبغي أن يكون هدف الأونسيترال هو وضع صك يقدم إرشادات للدول بشأن ما يمكن أن ينص عليه قانون من الطبقة 2. ويرد وصف هذا الإطار القانوني على نحو أوفى في القسم الثالث أدناه (بما في ذلك الشكل 1، الذي يقدم رسما توضيحيا لهذه الطبقات القانونية الثلاث والعلاقة بينها). ويقدم القسم الثالث أيضا خريطة طريق مفصلة عن الكيفية التي يمكن بها للأونسيترال أن تنظر في محتويات ذلك الصك.

10- ولا تنطلق مشاريع الأحكام الواردة في الوثيقة WP.162 من التسليم بهذا الإطار القانوني، بل تتبع نهجا مختلفا جوهريا، وهو نهج غير قابل للتطبيق عمليا في رأينا. ففي حين تتناول مشاريع الأحكام بعض المسائل التي من شأن صك من الطبقة 2 أن يشملها عن حق، فإنها تقرن هذه المسائل وتخلط بينها وبين العديد من المسائل التي من الأنسب أن تعالجها قواعد التشغيل التعاقدية التي تخص نظاما بعينه من نظم إدارة الهوية (الطبقة 3). ونتيجة لذلك، تتبع مشاريع الأحكام في كثير من الأحيان نهجا يفترض وجود حل واحد

يصلح لكل الحالات في سياق معالجة مسائل من شأنها أن تتفاوت تفاوتا كبيرا فيما بين قواعد التشغيل التعاقدية المختلفة التي تحكم نظم إدارة الهوية المتعددة. وكلما تقدمت المفاوضات بشأن مشروع النص، يتضح أكثر فأكثر أن هذا النهج لن يكون قابلا للتطبيق عمليا.

11- وتتوخى مشاريع الأحكام الواردة في الوثيقة WP.162 نموذجا مفاهيميا مستمدا من قواعد تشغيل وُضعت لنظام لإدارة الهوية تابع للقطاع العام (لائحة الاتحاد الأوروبي بشأن تعيين الهويات الإلكترونية وخدمات توفير الثقة ("اللائحة الأوروبية") (eIDAS))، وتسعى إلى التوسع في تطبيق ذلك النموذج عالميا على جميع نظم إدارة الهوية. والواقع أن اللائحة الأوروبية تجسد بالفعل نهجا مبتكرا للغاية في تنظيم نظم إدارة الهوية، وقد قدمت إسهاما كبيرا في تكوين الفهم العالمي لكيفية تشغيل نظم إدارة الهوية وكيفية تنظيمها للاستخدام في القطاع العام. غير أن المشكلة هي أن اللائحة الأوروبية هي مجموعة فريدة من قواعد التشغيل الخاصة بنظام واحد لإدارة الهوية تابع للقطاع العام (يضم الجهات المتعددة التي توفر الهويات في بلدان الاتحاد الأوروبي). ومن ثم فالوظيفة التي تؤديها اللائحة الأوروبية في نظام تابع للقطاع العام تكافئ وظيفة قواعد التشغيل التعاقدية التي تحكم نظاما بعينه من نظم إدارة الهوية التابعة للقطاع الخاص، ولا تصح محاولة فرض هذه القواعد على جميع نظم إدارة الهوية الأخرى.

12- وبعبارة أخرى، ففي حين أن اللائحة الأوروبية هي مجموعة من قواعد التشغيل التي تحكم *نظاما واحدا من نظم إدارة الهوية* (الطبقة 3)، ينبغي أن تعمل الأونسيترال على وضع صك ينطبق على جميع *نظم إدارة الهوية* (الطبقة 2). وفي حين أن اللائحة الأوروبية هي مجموعة من قواعد التشغيل الخاصة بنظام لإدارة الهوية *تابع للقطاع العام* (أي أنها تنظم معاملات الهوية لأغراض استخدامها في القطاع العام)، ينبغي أن تعمل الأونسيترال على وضع صك ينطبق على نظم إدارة الهوية *التابعة للقطاع الخاص*. وعلى وجه التحديد، ينبغي أن يوفر الصك الذي تضعه الأونسيترال جسرا يربط قواعد التشغيل التعاقدية التي يختص بها كل نظام من نظم إدارة الهوية التابعة للقطاع الخاص (الطبقة 3)، بجوانب الأحكام القانونية الوطنية القائمة (الطبقة 1) التي لها تأثير سلبي في جميع نظم إدارة الهوية ولكن لا يمكن تسويتها عن طريق قواعد التشغيل الخاصة بفرادى نظم إدارة الهوية (مثل الاعتراف القانوني بمعاملات الهوية أو المسؤولية التقصيرية).[(1)]

13- وبدلا من ذلك، تنص مشاريع الأحكام الواردة في الوثيقة WP.162 على قواعد تتعلق بعدد من المسائل التي عادة ما تعالجها قواعد التشغيل التعاقدية التي يختص بها كل نظام من نظم إدارة الهوية. ويشمل ذلك مواضيع مثل التزامات مقدمي خدمات إدارة الهوية (في المادة 6)، والتزامات مقدمي الخدمات في حال انتهاك سرية البيانات (في المادة 7)، والتزامات المشتركين (في المادة 8)، ومسؤولية مقدمي خدمات إدارة الهوية (في المادة 12). وفي الوقت نفسه، لا تحدد مشاريع الأحكام بوضوح الأحوال التي يجوز فيها للأطراف أن تحيد في العقود التي تبرمها عن الأحكام القانونية القائمة فيما يتعلق بهذه المواضيع، والأحوال التي يجب عليهم فيها التصرف على نحو مطابق لتلك الأحكام.

14- وبالإضافة إلى ذلك، ففي حين أن إطار اللائحة الأوروبية، الذي تستند إليه مشاريع الأحكام الواردة في الوثيقة WP.162، يعتمد على آلية مركزية لتنظيم نظم إدارة الهوية ووضع المعايير لها واعتمادها، فلا توجد على الصعيد العالمي آلية مركزية من هذا القبيل لتؤدي الدور نفسه فيما يخص صكا تضعه الأونسيترال على غرار

(1) في حين يمكن القول إن اللائحة الأوروبية تتضمن عناصر من كل من الطبقتين 2 و 3 فيما يخص الجهات المتعددة التي توفر الهويات في بلدان الاتحاد الأوروبي والتي توافق على المشاركة في الإطار الموحد الخاص بالاتحاد الأوروبي، فإننا نعتقد أن تركيز الأونسيترال ينبغي أن يقتصر على وضع صك من الطبقة 2 ينطبق على جميع مقدمي خدمات نظم إدارة الهوية التابعة للقطاع الخاص. وبالإضافة إلى ذلك، فوظيفة اللائحة الأوروبية هي أن تحكم نظاما لإدارة الهوية لأغراض الاستخدام في القطاع العام، في حين أن مهمة الأونسيترال هي وضع صك ينطبق على نظم إدارة الهوية التابعة للقطاع الخاص.

مشاريع الأحكام الواردة في الوثيقة WP.162 وفي حين تفترض الوثيقة WP.162 ببساطة وجود تلك الآلية العالمية، فإن عدم وجودها يعني أن الأحكام الواردة في تلك الوثيقة بشأن الاعتراف عبر الحدود ومعايير الموثوقية تثير عددا من الأسئلة التي لم يُجب عنها والتي تتطلب مزيدا من المناقشة في الفريق العامل. والواقع أن اللائحة الأوروبية لا تكفل الاعتراف بخدمات توفير الثقة المقدمة من جهات خارج الاتحاد الأوروبي إلا إذا كان هناك اتفاق من نوع معين مبرم بين الاتحاد الأوروبي والبلد الثالث المعني (المادة 14-1 من اللائحة الأوروبية).

15- وبالإضافة إلى تنافر الغرض من أحكام المشاريع الواردة الوثيقة WP.162 مع نموذج اللائحة الأوروبية، فاعتماد تلك الوثيقة على قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية كقالب نموذجي ليس في محله. فموضوع التوقيعات الإلكترونية هو موضوع بسيط وموحَّد نسبيا، في حين أن نظم إدارة الهوية تتسم بقدر أكبر من التعقُّد وتعدد المستويات. وعلى سبيل المثال، ففي حين أن التوقيعات الإلكترونية عادة ما تنطوي على طرفين اثنين، فإن نظم إدارة الهوية عادة ما تنطوي على أطراف عديدة. وببساطة، فالقواعد المنصوص عليها في القانون النموذجي بشأن التوقيعات الإلكترونية لا تصلح لنظم إدارة الهوية.

16- وتثير هذه الشواغل الجوهرية أسئلة مبدئية للغاية ولكنها بالغة الأهمية: كيف سيكون النهج المعمول به في مشاريع الأحكام الواردة في الوثيقة WP.162 مفيدا للدول لدى اعتمادها؟ وفي ظل عدم وجود آلية مركزية لتنظيم نظم إدارة الهوية أو خدمات توفير الثقة، أو اعتماد تلك النظم أو الخدمات، كيف سيحقق هذا النص الأهداف التي يسعى إلى تحقيقها، على سبيل المثال فيما يتعلق بالاعتراف عبر الحدود أو معايير الموثوقية؟ وإذا كان المقصود، حسب فهم الولايات المتحدة، هو أن تنطبق مشاريع الأحكام الواردة في الوثيقة WP.162 على نظم إدارة الهوية التابعة للقطاع الخاص، فما هي إذن العلاقة بين القواعد المنصوص عليها في تلك الأحكام وقواعد التشغيل التي ينص عليها أطراف نظام لإدارة الهوية في العقد الذي يحكم ذلك النظام؟

17- وقد سبق للولايات المتحدة أن تجاوبت مع القالب النموذجي الذي طرحته الأمانة وقدمت ردودا مكتوبة على آخر نص، ويرد في تذييل هذه الورقة تحليل لمشاريع الأحكام الواردة في الوثيقة WP.162 يتناول كل مادة على حدة. ومع ذلك، ترى الولايات المتحدة أنه قبل المضي قدما في العمل على أساس الوثيقة WP.162، ينبغي أن يجري الفريق العامل أولا مناقشة مفاهيمية لتوضيح موقع مشاريع الأحكام الواردة في تلك الوثيقة من الإطار القانوني العام الذي يحكم نظم إدارة الهوية. وفي حين تعرب الولايات المتحدة عن تقديرها للعمل الكبير الذي اضطُلع به في إعداد الوثيقة WP.162، وللجهود التي بُذلت من أجل التوصل إلى توافق في الآراء حول تلك الوثيقة، فسيكون من المؤسف أن يواصل الفريق العامل السير على طريق إعداد صك لا ترتجى منه فائدة تُذكر للدول الأعضاء أو لنظم إدارة الهوية التابعة للقطاع الخاص.

18- وكما هو مبين في هذه الورقة، فهناك عدد من المجالات التي تتناول فيها الأحكام الواردة في الوثيقة WP.162 مواضيع مناسبة ووثيقة الصلة بمسألة نظم إدارة الهوية، ومن ثم ففي الحالات المنطوية على اتباع نهج غير قابل للتطبيق عمليا في سياق تلك المجالات، قد يتمكن الفريق العامل من الاستناد إلى الوثيقة وإدراج التغييرات المفاهيمية في الأحكام القائمة. أما الحالات الواقعة ضمن مجالات أخرى فقد تتطلب التغيير أو الحذف على نطاق أوسع.

19- وتقدم الولايات المتحدة الإطار الوارد في القسم الثالث أدناه كخريطة طريق يُسترشد بها في إجراء مناقشة مفاهيمية تساعد على تحديد سبيل المضي قدما.

ثانيا- معلومات أساسية عن نظم إدارة الهوية

20- إننا نعتقد أن الهدف من هذا المشروع ينبغي أن يتمثل في وضع إطار قانوني يتيح ويشجع إرساء منظومة مُحكمة في مجال إدارة الهوية تضم العديد من نظم إدارة الهوية التابعة للقطاع الخاص بجميع أنواعها، وتكفل لتلك النظم أن تزدهر وتدعم التجارة على الصعيدين الوطني والعالمي. ويتطلب ذلك التركيز على تبيُّن أي معوقات أو ثغرات يلزم معالجتها في الأحكام القانونية الوطنية القائمة. وبالإضافة على ذلك، وبغية التشجيع على استحداث نظم جديدة ومختلفة لإدارة الهوية، فمن المهم أن يتجنب الفريق العامل افتراض وجود حل واحد يصلح لجميع الحالات فيما يتعلق بالمسائل والمشاكل التي ينبغي تناولها في قواعد التشغيل التعاقدية الفريدة التي توضع لكل نظام من نظم إدارة الهوية على حدة.

21- وبغية تبيُّن أي معوقات أو ثغرات يلزم معالجتها في الإطار القانوني لإدارة الهوية، يتعين علينا أولا القيام بما يلي:

- دراسة مفهومي معاملات الهوية ونظم إدارة الهوية؛
- دراسة الحاجة إلى قواعد التشغيل التي تحكم تشغيل كل نظام من نظم إدارة الهوية التابعة للقطاع الخاص، والدور الذي تؤديه هذه القواعد؛
- فهم الإطار القانوني العام الذي يحكم نظم إدارة الهوية، والموقع الذي يمكن أن يحتله صك تضعه الأونسيترال من ذلك الإطار والإسهام الذي يمكن أن يقدمه إليه.

22- واستنادا إلى هذه المعلومات الأساسية، يمكن للفريق العامل أن يحدد المسائل القانونية التي لا يمكن معالجتها من خلال قواعد التشغيل التعاقدية الفريدة التي تشكل جزءا من كل نظام لإدارة الهوية، ومن ثم يلزم معالجتها بإدخال إضافات وتغييرات على الأحكام القانونية الوطنية باستخدام صك قانوني تضعه الأونسيترال.

ألف- معاملات الهوية

23- معاملة الهوية هي عبارة عن عملية اتصال يتلقى بموجبها طرف معوِّل بعض المعلومات عن هوية فرد ما[(2)] (تحديد الهوية)، إلى جانب التحقق من أن ذلك الفرد هو فعلا الشخص الذي يزعم ذلك (التوثق من الهوية). وغالبا ما تُجرى معاملات الهوية لتحقيق غرض من اثنين: إما (1) الدخول في معاملة ما مع الكيان المعني (مثل إبرام العقود أو تقديم المزايا أو إبلاغ المعلومات أو غير ذلك)، أو (2) منح الكيان المعني إمكانية الدخول إلى مرفق رقمي أو مادي (على سبيل المثال موقع شبكي أو قاعدة بيانات أو مبنى أو غير ذلك).

24- تتطلب معاملات الهوية عموما ما يلي: (1) جمع المعلومات (النعوت) الخاصة بكيان معني واحد والتحقق منها (عملية تحديد الهوية)، (2) إصدار إثبات هوية يحتوي على نعت واحد أو أكثر من هذه النعوت (عملية إصدار إثباتات الهوية)، (3) الربط بين نعوت الهوية الواردة في إثبات الهوية وفرد محدد، غالبا عن بُعد (عملية التوثق من الهوية). ومن خلال هذه العمليات، تهدف معاملات الهوية إلى التحقق من هوية الفرد المعني، والتوثق من علاقة تلك الهوية بشخص محدد.

25- ومن ثم يُعدُّ من معاملات الهوية، على سبيل المثال، تقديم المرء جواز سفره على الحدود للحصول على حق الدخول إلى بلد ما. وفي تلك الحالة، تُقدَّم إلى الطرف المعوِّل (موظف مراقبة الحدود) نعوت سبق

(2) يمكن أن يكون الكيان المعني فردا أو كيانا أو جهازا أو شيئا رقميا. وتركز هذه الورقة على الأفراد، لأن ذلك كان محور مناقشات الفريق العامل حتى الآن.

التحقق منها تحدد هوية الفرد المعني (على النحو الوارد في جواز السفر)، ومعها طريقة للتحقق من أن الشخص الذي يقدم جواز السفر هو نفسه الفرد المسمى في الجواز (أي عن طريق الصورة أو بيانات البصمات المدمجة في جواز السفر). وبالمثل، تُعدُّ من معاملات الهوية عملية تسجيل الدخول إلى شبكة متاحة عبر الإنترنت بإدخال اسم المستخدم وكلمة المرور للحصول على حق الاطلاع على قاعدة بيانات. وتنطوي هذه العملية على الربط (عن طريق كلمة المرور السرية) بين نعوت سبق التحقق منها تحدد هوية الفرد المعني (يحيل إليها اسم المستخدم) والشخص الذي يزعم أنه ذلك الفرد (أي الشخص الذي يُدخل اسم المستخدم).

باء- نظم إدارة الهوية هي نظم متعددة الأطراف تهدف إلى تيسير إجراء معاملات الهوية

26- يتكون نظام إدارة الهوية من توليفة متناسقة من الكيانات المشاركة والعمليات والتكنولوجيا، يضطلع فيها كل طرف مشارك بالمسؤوليات المنوطة بدور واحد أو أكثر من جملة أدوار محددة مسبقا،[3] وفقا لمجموعة محددة مسبقا من العمليات والسياسات والإجراءات الملزمة قانونا، بغرض تسهيل إجراء معاملات الهوية.

27- ونظم إدارة الهوية هي نظم معقدة ومتعددة الأطراف. وهي تضم العديد من الأطراف المشاركة التي تؤدي أدوارا متنوعة، بما يشمل سلطات التسجيل ومدققي الهويات ومقدمي النعوت ومقدمي خدمات توفير الثقة وموفري الهويات ومقدمي إثباتات الهوية ومقدمي خدمات التحقق ومراكز تجميع البيانات وغيرها. وتتسق هذه النظم العمل اللازم لجمع معلومات (نعوت) الهوية الخاصة بكيان معني واحد، وإصدار إثبات الهوية الذي يحتوي على نعت أو أكثر من هذه النعوت، والتوثق من هذه النعوت عن طريق ربطها بفرد محدد في سياق معاملة هوية. وتعمل هذه الأطراف المشاركة سويا من أجل تيسير إجراء معاملات الهوية مع أطراف معوِّلة متعددة.

28- وتشبه نظم إدارة الهوية في تعقُّد هياكلها نظم البطاقات الائتمانية المصممة لتيسير المعاملات الائتمانية (مثل "ماستركارد" أو "فيزا")، أو نظم الدفع الإلكترونية المصممة لغرض تيسير إجراء معاملات الدفع (مثل نظام "سويفت" أو ACH). وفي حين أن كل نوع من هذه النظم يختلف عن غيره من حيث الهيكل المستخدم في تصميمه والغرض منه، فهي جميعا نظم متعددة الأطراف مصممة لتيسير نوع معين من المعاملات الاقتصادية (مثل المعاملات الائتمانية أو معاملات الدفع أو معاملات الهوية).

29- ويمكن أن تتباين الهياكل تباينا كبيرا فيما بين نظم إدارة الهوية. فعلى سبيل المثال، يمكن أن يكون هيكل نظام إدارة الهوية مركزيا (أي أن يتألف النظام من موفر هويات واحد ييسر معاملات الهوية مع أطراف معوِّلة متعددة)، أو اتحاديا (أي أن يتألف النظام من مجموعة محدودة من موفري الهويات الذين يخزنون معلومات الهوية الخاصة بالمستخدمين ويقدمونها بطريقة مركزية لتيسير إجراء معاملات الهوية مع طرف معوِّل واحد أو أطراف معوِّلة متعددة)، أو موزعا (أي أن يتألف النظام من موفري هويات متعددين يتوثقون من معلومات الهوية المخزنة لدى المستخدمين لتيسير إجراء معاملات الهوية مع أطراف معوِّلة متعددة). وهذا التنوع في هياكل نظم إدارة الهوية هو أحد الأسباب الرئيسية التي تمنع أن يتبع الصك الذي يضعه الفريق العامل نهجا يفترض وجود حل واحد يصلح لجميع الحالات فيما يتعلق بالعديد من المسائل.

جيم- نظم إدارة الهوية تتطلب قواعد تشغيل ملزمة قانونا

30- بما أن نظم إدارة الهوية هي نظم معقدة ومتعددة الأطراف، فلا بد من التنسيق والتعاون بين الكيانات المشاركة من أجل تحقيق الهدف المنشود. ولذلك تتطلب نظم إدارة الهوية وجود هيكل منظم ومحدد الهدف

(3) يمكن أن تشمل هذه الأدوار، على سبيل المثال، سلطة التسجيل ومدقق الهويات وموفر الهويات والوسيط ومركز تجميع البيانات ومقدم النعوت والطرف المعوِّل وغير ذلك.

يتألف من مجموعة مترابطة ومتكافلة من الكيانات المشـــاركة التي تؤدي أدوارا متنوعة وتنفذ مجموعة من العمليات المفصـلة وتتبع مجموعة من السـياسـات والإجراءات، وكل ذلك ابتغاء تحقيق هدف محدد هو تيسـير إجراء معاملات الهوية.

31- وبالإضـافة إلى ذلك، ولأن نظم إدارة الهوية تضـم كيانات مشاركة متعددة مستقلة يمكن أن تتفاعل مع بعضـها البعض لتنفيذ سلسلة من المعاملات المعقدة، فإن نظم إدارة الهوية لا تعمل بطريقة آلية من تلقاء ذاتها. ويجب أن تكون هناك مجموعة من القواعد أو التعليمات التي يسترشد بها كل طرف مشارك بشأن الطريقة التي ينبغي أن يؤدي بها الدور المحدد المنوط به. ويجب عادة أن تكون تلك القواعد واجبة الإنفاذ قانونا لضـــمان أن يمتثل كل طرف مشارك للمتطلبات المنطبقة عليه وأن يكون بوسعه أن يعول على أن جميع الأطراف المشاركة الأخرى سوف تلتزم بالقواعد وتقدم نتائج جديرة بالثقة.

32- ومن ثم فإن كل نظام من نظم إدارة الهوية يتطلب أن تحكم تشـغيله مجموعة من **قواعد التشـــغيل**[4] الواجبة الإنفاذ قانونا. وتؤدي هذه القواعد ثلاث وظائف هامة:

- تضـــمن قواعد التشـــغيل أن نظام إدارة الهوية **يعمل كما ينبغي** – أي أنها تنص على الســـياســـات والإجراءات والعمليات اللازمة لتشغيل نظام إدارة الهوية بحيث "يؤدي عمله" كما يُفترض أن يكون؛
- تحدد قواعد التشـغيل الواجبات والالتزامات المفروضـــة على الأطراف المشـــاركة كل بحســب الأدوار المسندة إليه (مثلا لكي يعرف كل طرف مشارك ما يتوجب عليه أن يفعله)، وتحدد أيضـا المسؤوليات القانونية ذات الصـــلة، وكذلك (عند الاقتضـــاء) المخاطر المتعلقة بالمسـؤولية القانونية وتوزعها على الأطراف المشاركة توزيعا عادلا؛
- تنص قواعد التشغيل على المتطلبات الإضـافية التي تساعد على جعل نظام إدارة الهوية "جديرا بالثقة" فيما يخص الغرض المتوخى منه – أي أنها تفرض متطلبات تتجاوز ضـــمان أن يؤدي نظام إدارة الهوية وظائفه فحســب، وتنفذ خطوات إضـــافية للتأكد من أن الأطراف المشـــاركة تثق في معاملات الهوية الناتجة من النظام وأنها مستعدة للتعويل عليها.

33- ولتحقيق هذه الأهداف، عادة ما تصـــمم قواعد التشـــغيل لمعالجة المســـائل التجارية والتقنية والقانونية المحددة التي تنشأ في سياق تشغيل نظام بعينه من نظم إدارة الهوية. وقد يشمل ذلك، على سبيل المثال، مسائل مثل متطلبات المشـــاركة، وتعريف الأدوار والمســـؤوليات المنوطة بها، والعمليات والإجراءات الخاصـــة بقيد الأشـــخاص المعنيين، وتدقيق الهويات، وإصـــدار إثباتات الهوية، والتوثق من الهويات، والمواصـــفات والمعايير التقنية، ومتطلبات أمن البيانات، والضمانات، وتوزيع المسؤوليات، وإجراءات تسوية المنازعات، وحقوق الإنهاء. وتتناول قواعد التشغيل أيضا حوكمة نظام إدارة الهوية، مثل المؤهلات المطلوبة للمشاركة، وإنفاذ القواعد، وتنقيح القواعد. وتشكل قواعد التشـغيل إطار الحوكمة الخاص بنظام إدارة الهوية. وبالإضـافة إلى ذلك، ولأن نظم إدارة الهوية قد تختلف من حيث الهيكل والتكنولوجيا المستخدمة والغرض، فمن المرجح أن تتباين قواعد التشغيل تباينا كبيرا فيما بين هذه النظم.

34- ولضـمان أن تكون قواعد تشـغيل نظم إدارة الهوية ملزمة وواجبة الإنفاذ قانونية، يمكن أن تتخذ شـكل تشريع أو لائحة أو عقد.

(4) كثيرا ما يُشار إلى قواعد التشغيل أيضا بمجموعة متنوعة من الأسماء الأخرى، مثل إطار الحوكمة وإطار توفير الثقة وقواعد المخطط وقواعد النظام.

35- وفي حالة نظم إدارة الهوية **التابعة للقطاع العام**، تتخذ قواعد التشغيل عادة شكل تشريع مفصل أو **لائحة**. ومن الأمثلة على ذلك قانون "آدهار" في الهند،[5] وقانون وثائق الهوية في إستونيا،[6] واللائحة الأوروبية في الاتحاد الأوروبي.[7] ومع ذلك، فقد استُخدمت العقود أيضا في بعض نظم إدارة الهوية التابعة للقطاع العام، مثل نظام GOV.UK IdM.[8]

36- أما في حالة نظم إدارة الهوية **التابعة للقطاع الخاص**، فتتخذ قواعد التشغيل شكل **عقد** ملزم للأطراف المشاركة في النظام (مثلما تتفق الأطراف المشاركة في نظم البطاقات الائتمانية أو نظم الدفع الإلكترونية عن طريق التعاقد على أحكام قواعد التشغيل المنطبقة على دور كل طرف منها). ومن أمثلة قواعد تشغيل نظم إدارة الهوية التابعة للقطاع الخاص إطار توفير الثقة الخاص بنظام SAFE Identity،[9] وإطار حوكمة نظام Sovrin،[10] والإطار الكندي العام لتوفير الثقة.[11] وانظر أيضا: "A Guide to Trust Frameworks and Interoperability" ("دليل إرشادي لأطر توفير الثقة وقابلية التشغيل المتبادل").[12]

دال- لكل نظام من نظم إدارة الهوية قواعد تشغيله التي ينفرد بها

37- يختلف كل نظام من نظم إدارة الهوية عن غيره، ومن ثم يتطلب كل نظام مجموعة فريدة من قواعد التشغيل المصممة خصيصا بمراعاة هيكله والتكنولوجيا المستخدمة فيه والغرض منه والسوق الذي يعمل فيه وأنماط المخاطر التي يواجهها.

38- وتستخدم نظم إدارة الهوية التابعة للقطاع الخاص طائفة واسعة من **الهياكل والتقنيات**، يتطلب كل منها اتباع نُهج مختلفة فيما يخص قواعد التشغيل. ومن ثم فالمحاولات الرامية إلى فرض مجموعة من القواعد الموحدة على جميع النظم بناء على افتراض وجود حل واحد يصلح لجميع الحالات من شأنها أن تعوق تطور نظم إدارة الهوية التابعة للقطاع الخاص.

- وقد حدد المنتدى الاقتصادي العالمي في عام 2016[13] أمثلة للأشكال المختلفة التي تتخذها **هياكل نظم** إدارة الهوية، ومنها النظم الداخلية، ونظم التوثق الخارجي، والنظم المركزية، والنظم الاتحادية، والنظم الموزعة. وهناك أشكال أخرى من هياكل نظم إدارة الهوية بدأ العمل بها في الآونة الأخيرة، ومنها النظم القائمة على مراكز تجميع البيانات، والنظم القائمة على تحكم المستخدمين أنفسهم،

(5) Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

(6) Identity Documents Act, Passed 15.02.1999, RT I 1999, 25, 365, Entry into force 01.01.2000 https://www.riigiteataja.ee/en/eli/ee/504112013003/consolide.

(7) توفر اللائحة رقم 910/2014 بشأن خدمات التحديد الإلكتروني للهوية وتوفير الثقة في المعاملات الإلكترونية في السوق الداخلية (eIDAS Regulation)، التي اعتُمدت في 23 تموز/يوليه 2014، بيئة تنظيمية يمكن التنبؤ بها للتمكين من إجراء معاملات إلكترونية آمنة وسلسة فيما بين الأعمال التجارية والمواطنين والسلطات العامة؛ متاحة على الرابط: https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014.

(8) www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

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

(10) https://sovrin.org/library/sovrin-governance-framework.

(11) https://drive.google.com/file/d/1Xmjh8QJZKWmRkaTtE2f43ISntD7jE6D5/view.

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

(13) انظر World Economic Forum, "A Blueprint for Digital Identity," August 2016، متاح على الرابط https://openidentityexchange.org/guide-trust-frameworks-interoperability.

وكذلك النظم التي يجري تطويرها باستخدام الهواتف المحمولة. ومن شأن كل نظام من هذه النظم أن يتطلب اتباع نهج مختلف إزاء قواعد التشغيل، وأن يعاني في حال محاولة فرض مجموعة موحدة من القواعد على جميع النظم.

- وتشمل أمثلة التكنولوجيات المختلفة المستخدمة في نظم إدارة الهوية، النظم القائمة على مرافق (المفاتيح العمومية PKI)، ونظم سلاسل الكتل (blockchain)، والنظم التي تستخدم معياري OAuth وOpenID Connect، ومن شأن كل نظام من هذه النظم أن يتطلب اتباع نهج مختلف إزاء قواعد التشغيل، وأن يعاني في حال محاولة فرض مجموعة موحدة من القواعد على جميع النظم.

39- كما أن نظم إدارة الهوية التابعة للقطاع الخاص عادة ما تختلف من حيث **الأغراض و/أو الأسواق** التي تصمم من أجلها، وهو ما يتطلب مراعاة طائفة متنوعة من النُّهج المختلفة ومتطلبات توفير الثقة وأساليب توزيع المخاطر في قواعد تشغيل هذه النظم. ومن ثم فالمحاولات الرامية إلى فرض مجموعة من القواعد الموحدة على هذه النظم المختلفة الأغراض و/أو الأسواق بناء على افتراض وجود حل واحد يصلح لجميع الحالات من شأنها أن تعوق تطور جميع هذه النظم.

- ومن أمثلة نظم إدارة الهوية المصممة من أجل طائفة متنوعة من **الأغراض والأسواق** المختلفة ما يلي: نظام InCommon المصمم للاستخدام في قطاع التعليم (مثل الجامعات والطلبة)؛ نظام SAFE BioPharma المصمم للاستخدام في قطاع الصناعات الصيدلانية؛ نظام CertiPath المصمم للاستخدام في قطاع الصناعات الفضائية الجوية الدولية؛ نظام CA Browser Forum المصمم لتحديد هوية مشغلي المواقع الشبكية؛ نظام ZenKey المصمم لأغراض تحديد الهوية عن طريق الأجهزة المحمولة؛ ونظم Google وLinkedIn وFacebook الخفيفة الوزن المصممة لإدارة الدخول إلى المواقع الشبكية المنخفضة المخاطر.

40- وحيث إن قواعد التشغيل تصمم من أجل تلبية المتطلبات التي يختص بها نظام بعينه، ينبغي أن تكون المسائل التي تعالجها هذه القواعد خارج نطاق الصك الذي يعمل الفريق العامل على إعداده.

41- ونظرا لأن قواعد تشغيل نظم إدارة الهوية التابعة للقطاع الخاص توضع تعاقديا وترتبط بالمتطلبات الفريدة التي يختص بها نظام بعينه، فمن المهم ألا يحاول أي صك تضعه الأونسيترال أن يكرر محتويات هذه القواعد باتباع نهج يفترض وجود حل واحد ينطبق على جميع نظم إدارة الهوية. ومن ثم فإن أحد التحديات التي سيواجهها الفريق العامل يتمثل في وضع صك لا يمس بحاجة نظم إدارة الهوية في القطاع إلى وضع قواعد التشغيل الخاصة بها، ولا ينتقص من قدرتها على وضع تلك القواعد أو يمنعها من ذلك، على أن يوضح ذلك الصك في الوقت نفسه المتطلبات القانونية التي يجب أن تمتثل لها قواعد التشغيل التعاقدية.

ثالثا- الإطار القانوني الذي يحكم نظم إدارة الهوية التابعة للقطاع الخاص والصك الذي يحتمل أن تضعه الأونسيترال

ألف- الإطار القانوني العام

42- إننا نعتقد أنه حتى يمكن وضع صك من النوع المتوخى في الوثيقة WP.162، فلا بد أولا من أن ينظر الفريق العامل في هيكل الإطار القانوني العام الذي يحكم نظم إدارة الهوية التابعة للقطاع الخاص. وعلى وجه التحديد، ينبغي أن ينظر الفريق العامل في الموقع الذي سيحتله من ذلك الإطار العام كلٌّ من

’1‘ قواعد التشـــغيل التي يختص بها كل نظام من نظم إدارة الهوية المتعددة التابعة للقطاع الخاص، و’2‘ صك الأونسيترال المقترح. وسيكون ذلك مهما لتحديد المسائل التي ينبغي معالجتها في صك الأونسيترال.

43- وكما هو حال معظم نظم المعاملات التجارية المتعددة الأطراف، فإن نظم إدارة الهوية التابعة للقطاع الخاص يحكمها عادة إطار قانوني يتألف من مزيج من ’1‘ الأحكام القانونية الحكومية، و’2‘ الاتفاقات التعاقدية المبرمة بين الكيانات المشـــاركة. وتتألف **الأحكام القانونية الحكومية** من القواعد التي تســـنها الهيئات التشريعية في شكل تشريعات أو تعتمدها الأجهزة الحكومية في شكل لوائح أو تتقرر بناء على أحكام قضائية. وأما **الأحكام القانونية التعاقدية** فهي القواعد التي يصـــوغها طرف واحد أو أكثر من الأطراف المشـــاركة أو تصـــوغها الجهات التي تدير نظام إدارة الهوية – أي قواعد تشـــغيل نظام إدارة الهوية – والتي تكتســـب صـــفة الإلزام للأطراف المشاركة في نظام إدارة الهوية عن طريق التعاقد.

44- وعادة ما يتألف الإطار القانوني الذي يعمل ضـــمنه أي نظام من نظم إدارة الهوية التابعة للقطاع الخاص من ثلاث طبقات (أو ثلاثة مســـتويات) من الأحكام القانونية، بحيث تتناول كل طبقة نظم إدارة الهوية بقدر أكبر من التحديد مقارنة بالطبقة التي تســـبقها. ويمكن وصـــف الطبقات الثلاث التي يتألف منها الإطار القانوني على النحو التالي (كما يعرضها الرسم البياني الوارد في الصفحة التالية):

- **(الطبقة 1) الأحكام القانونية القائمة:** الطبقة العليا، والأكثر عمومية، هي ببســـاطة **الأحكام القانونية الوطنية القائمة**، أي الأحكام القانونية الحكومية بما في ذلك الأحكام المنصـــوص عليها في القوانين التشـريعية واللوائح والأحكام القضـائية. وتنطبق هذه الأحكام القانونية على جميع أنواع الأنشـطة التجارية، وهي ليســت موضـــوعة خصـــيصـــا لنظم إدارة الهوية، ويمكن في بعض الحالات أن يقدر عمرها بمئات السنين. ومع ذلك، فكثيرا ما تنطبق هذه الأحكام على أنشطة نظم إدارة الهوية التابعة للقطاع الخاص. وهي تشمل الأحكام المنصوص عليها في القوانين المعنية بالعقود العامة، والمسؤولية التقصيرية، والخصوصية، ومراقبة الصادرات، والضمانات، وحماية المستهلك، والمنافسة، والأعمال المصرفية، وما إلى ذلك.

- **(الطبقة 2) الأحكام القانونية المعنية بنظم الهوية:** يمكن الإشـــارة إلى المســـتوى الثاني من الأحكام القانونية التي تحكم نظم إدارة الهوية التابعة للقطاع الخاص باســـم الأحكام القانونية **المعنية بنظم الهوية**. وتوضـــع هذه الأحكام صـــراحة لكي تحكم جميع نظم إدارة الهوية التابعة للقطاع الخاص، بصـــرف النظر عن نوعها أو هيكلها أو التكنولوجيا المســـتخدمة فيها أو الغرض منها. والطبقة 2 المتمثلة في الأحكام القانونية المعنية بنظم الهوية هي أيضـــا أحكام قانونية حكومية، وهي تهدف إلى معالجة المشـــاكل التي تتســـبب فيها الطبقة 1 المتمثلة في الأحكام القانونية القائمة لجميع نظم إدارة الهوية، ويمكن أن تســـد بعض الثغرات التي لا تتناولها الأحكام القانونية من الطبقة 1. وينبغي أن تحتل موقعا وســـطا بين الطبقة 1 المتمثلة في الأحكام القانونية القائمة والطبقة 3 المتمثلة في قواعد التشغيل التعاقدية التي يختص بها كل نظام من نظم إدارة الهوية.

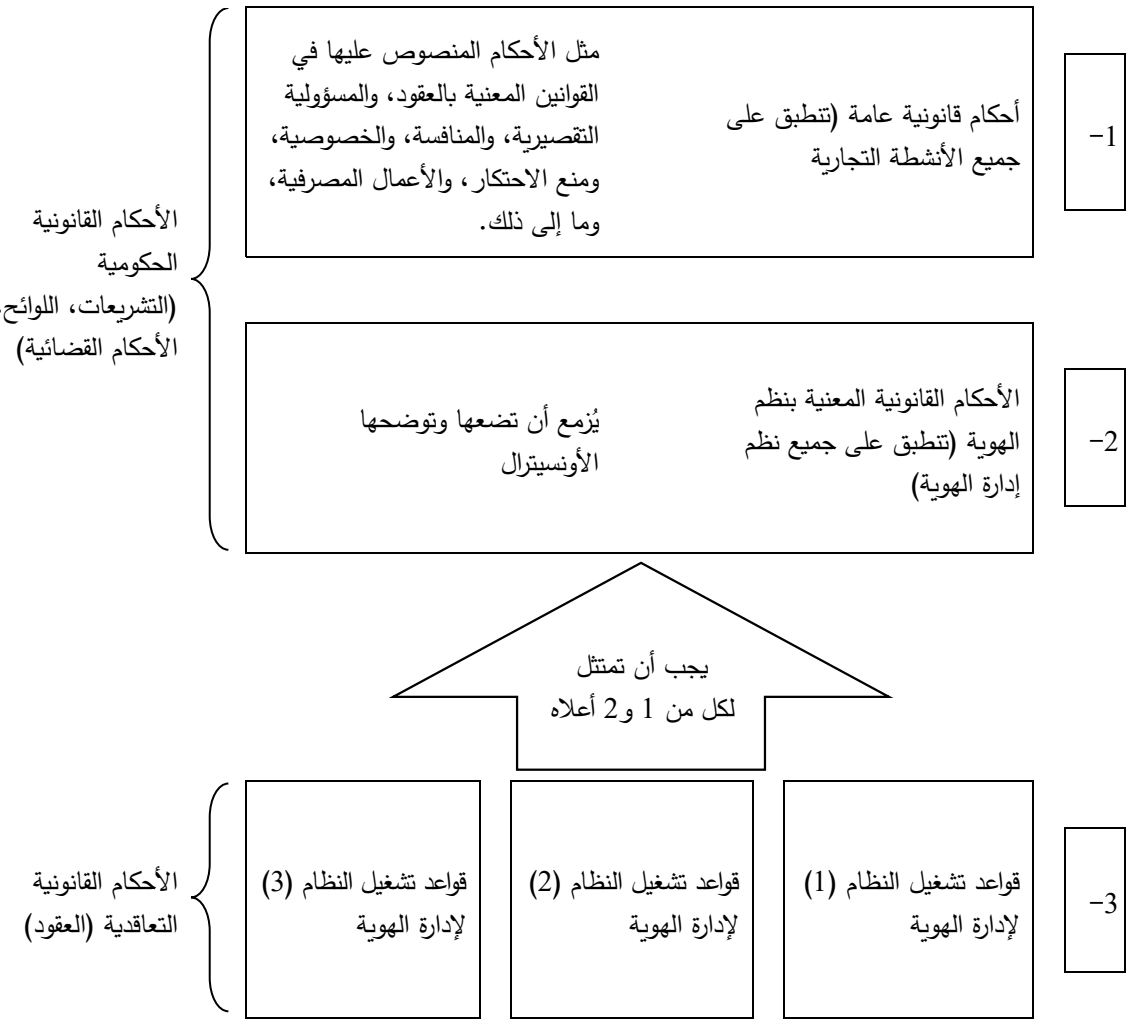
- **(الطبقة 3) قواعد التشـغيل الخاصـة بفرادى نظم إدارة الهوية:** تتألف ثالث طبقات الأحكام القانونية التي تحكم نظم إدارة الهوية التابعة للقطاع الخاص من قواعد التشغيل التعاقدية التي يضعها خصيصا كل نظام من نظم إدارة الهوية التابعة للقطاع الخاص لتنظيم بيئته الخاصـــة. وعلى العكس من الطبقة 2 المتمثلة في الأحكام القانونية المعنية بنظم الهوية، والتي تنطبق على جميع نظم إدارة الهوية، فإن الغرض من الطبقة 3 المتمثلة في القواعد التشـــغيلية هو معالجة المتطلبات الفريدة التي

يختص بها نظام بعينه.[14] ويمكن أن تكون هذه القواعد مفصلة للغاية، ولكن يجب أن تكون متوافقة مع الأحكام القانونية من الطبقتين 1 و2.

45- وتتمثل مهمة الفريق العامل في وضع صك يبين العناصر التي ينبغي أن تشتمل عليها الأحكام القانونية من الطبقة 2.

الشكل 1

الإطار القانوني لنظم إدارة الهوية التابعة للقطاع الخاص: ثلاث طبقات من الأحكام القانونية



باء- ما الدور الذي ينبغي أن يؤديه صك من إعداد الأونسيترال؟

46- بغية تجنب اتباع نهج يفترض وجود حل واحد يصلح لجميع الحالات، ومن ثم تعويق تطور نظم إدارة الهوية التابعة للقطاع الخاص وما يرتبط بها من الأنشطة التجارية، ينبغي أن يضع الفريق العامل صكا لا يتناول سوى المسائل التي لا يمكن معالجتها في قواعد التشغيل الخاصة بفرادى نظم إدارة الهوية. وبالإضافة إلى ذلك، ينبغي أن يقتصر ذلك الصك على تعديل و/أو استكمال الأحكام القانونية الوطنية القائمة من

(14) تجدر الإشارة إلى أنه في حالة نظم إدارة الهوية التابعة للقطاع العام، مثل نظم الهوية الوطنية، يُنص على قواعد التشغيل التي يختص بها النظام في تشريع أو لائحة. ومن ثم يُجمع بين الطبقتين 2 و3 من الأحكام القانونية.

الطبقة 1 في حدود ما يلزم لتشجيع وتعزيز تطور نظم إدارة الهوية التابعة للقطاع الخاص دعما للنشاط التجاري عبر شبكة الإنترنت. وينطوي ذلك على إعداد صك من الطبقة 2 يحقق ما يلي:

- إزالة ما يرد في الأحكام القانونية القائمة من الطبقة 1 من المعوقات وأوجه عدم اليقين التي تعوق تطور نظم إدارة الهوية التابعة للقطاع الخاص؛
- سد ما تنطوي عليه الأحكام القانونية القائمة من الطبقة 1 من الثغرات التي لها أهمية في إنجاح نظم إدارة الهوية التابعة للقطاع الخاص ولكن لا يمكن معالجتها تعاقديا؛
- معالجة المسائل المستجدة التي تنطبق على جميع نظم إدارة الهوية في القطاع الخاص من أجل تعزيز تطور هذه النظم.

47- وبالإضافة إلى ذلك، وبالنظر إلى تنوع نظم إدارة الهوية وتفرد كل منها باحتياجات تختلف عن احتياجات غيره، ينبغي لأي صك من الطبقة 2 يضعه الفريق العامل أن يلتزم بمبدأي الحياد التكنولوجي وحياد نظم الهوية. ولمبدأ حياد نظم الهوية تحديدا أهمية بالغة، في ضوء التنوع الواسع في نظم إدارة الهوية التابعة للقطاع الخاص من حيث هياكلها والتكنولوجيات المستخدمة فيها وأغراضها وأسواقها، كما هو مبين أعلاه.

48- وعلى النقيض من ذلك، فقد صيغت مشاريع الأحكام الواردة في الوثيقة WP.162 بطريقة تفرض قواعد معينة فيما يتعلق *بالتزامات مقدمي خدمات إدارة الهوية* (المادة 6)، *والتزامات مقدمي الخدمات في حال انتهاك سرية البيانات* (المادة 7)، *والتزامات المشتركين* (المادة 8)، *ومسؤولية مقدمي خدمات إدارة الهوية* (المادة 12). ويتعين أن تعالج نظم إدارة الهوية التابعة للقطاع الخاص هذه المسائل في قواعد التشغيل الخاصة بكل نظام على حدة. وتتطلب كل مسألة من هذه المسائل اتباع نهج فريد مصمم خصيصا بمراعاة خصائص نظام إدارة الهوية المعني من حيث هيكله والتكنولوجيا المستخدمة فيه والغرض منه والسوق الذي يعمل فيه. ومن شأن أي محاولات لمعالجة مسائل من قبيل ما سبق أن تكون إشكالية، لأنه من المرجح أن هذه المسائل سوف تتباين تباينا كبيرا من نظام إلى آخر، ولن يؤدي اتباع نهج يفترض وجود حل واحد يصلح لجميع الحالات وفرضه على جميع نظم إدارة الهوية إلا إلى تعويق تطور نظم إدارة الهوية التابعة للقطاع الخاص.

جيم- مخطط عام لصك من إعداد الأونسيترال

49- بدلا من النهج المتبع حاليا، تقع المسائل التي يمكن أن يتناولها الفريق العامل ضمن الفئات التالية:[15]

- الاعتراف الصريح بدور قواعد التشغيل في حوكمة نظم إدارة الهوية
- مسائل لا تتناولها الأحكام القانونية القائمة من الطبقة 1 ولا يمكن معالجتها، بحكم طبيعتها، في أحكام التشغيل التعاقدية. وتشمل الأمثلة على ذلك ما يلي:
  - الاعتراف القانوني بخدمات إدارة الهوية[16]

(15) الغرض من هذا المخطط العام هو تقديم قائمة أولية بالمسائل المحتملة التي يمكن أن يتناولها صك من الطبقة 2، رهنا بأن يطور الفريق العامل هذه القائمة ويحسنها بالاستناد إلى احتياجات النظم المتعددة القائمة على المستوى الوطني من بين عوامل أخرى.

(16) تسعى المادة 5 من مشاريع الأحكام الواردة في الوثيقة WP.162 إلى معالجة هذه المسألة. انظر تعليقاتنا الواردة في تذييل هذه الورقة بشأن المشاكل المتعلقة بمشروع المادة 5 بصيغته الحالية.

- الشروط التي يتقرر على أساسها ما إذا كانت معاملة الهوية تستوفي المتطلبات القانونية المنطبقة فيما يخص تحديد هوية شخص ما[17]
- ما إذا كان ينبغي تقييم موثوقية نظم إدارة الهوية التابعة للقطاع الخاص (وكيف يمكن القيام بذلك في حال استصوابه)[18]

• مسائل تتناولها الأحكام القانونية القائمة من الطبقة 1 بدرجة ما، ولكن انطباقها على نظم إدارة الهوية مشوب بعدم اليقين، ومن ثم تتسبب في غموض يمكن أن يشكل مشكلة لنظم إدارة الهوية بسبب صعوبة معالجة هذه المسائل في قواعد التشغيل التعاقدية. وتشمل الأمثلة على ذلك ما يلي:

- مدى انطباق الأحكام القانونية القائمة المتعلقة بالمسؤولية التقصيرية على الأطراف المشاركة في نظم إدارة الهوية؛
- مدى انطباق الأحكام القانونية المتعلقة بالادعاء الكاذب الناجم عن الإهمال؛
- مدى انطباق الأحكام القانونية القائمة المتعلقة بالضمانات الضمنية

• مسائل قد يلزم إضافتها إلى الأحكام القانونية القائمة، ومن ذلك معالجة ما يلي:

- حق نظم إدارة الهوية في استخدام المعلومات المستمدة من نظم إدارة الهوية التابعة للحكومة؛
- حق نظم إدارة الهوية في استخدام محددات الهوية الصادرة من الحكومة (مثل رقم التأمين الاجتماعي، ورقم الهوية القومي، وما إلى ذلك).

• مسائل ينبغي أن تعالجها جميع نظم إدارة الهوية بنفس الطريقة بسبب اعتبارات متعلقة بالنظام العام، بصرف النظر عما إذا كان يمكن معالجتها في قواعد التشغيل التعاقدية، مثل:

- ما إذا كان ينبغي إتاحة الاعتراف عبر الحدود (وكيف يمكن القيام بذلك في حال استصوابه)[19]
- ما إذا كان ينبغي معالجة الموثوقية من منظور قانوني (وكيف يمكن القيام بذلك في حال استصوابه).[20]

50- ومن شأن صك تضعه الأونسيترال وتضمنه هذه العناصر أن يساعد الدول على وضع أحكام قانونية معنية بنظم الهوية من الطبقة 2 بهدف تحقيق ما يلي: (1) تشجيع تطور نظم إدارة الهوية التابعة للقطاع الخاص، (2) إزالة المعوقات التي تعترض سبيل هذا التطور، (3) احترام حاجة كل نظام من نظم إدارة الهوية التابعة للقطاع الخاص إلى أن يضع قواعد التشغيل الخاصة به قدر الإمكان، ودعم تلبية هذه الحاجة.

(17) تسعى المادة 9 من مشاريع الأحكام الواردة في الوثيقة WP.162 إلى معالجة هذه المسألة. انظر تعليقاتنا الواردة في تذييل هذه الورقة بشأن المشاكل المتعلقة بمشروع المادة 9 بصيغته الحالية.

(18) تسعى المادة 11 من مشاريع الأحكام الواردة في الوثيقة WP.162 إلى معالجة هذه المسألة. انظر تعليقاتنا الواردة في تذييل هذه الورقة بشأن المشاكل المتعلقة بمشروع المادة 11 بصيغته الحالية.

(19) تسعى المادتان 10 و11 من مشاريع الأحكام الواردة في الوثيقة WP.162 إلى معالجة هذه المسألة. انظر تعليقاتنا الواردة في تذييل هذه الورقة بشأن المشاكل المتعلقة بمشروعي المادتين 10 و11 بصيغتهما الحالية.

(20) تسعى المادتان 10 و11 من مشاريع الأحكام الواردة في الوثيقة WP.162 إلى معالجة هذه المسألة. انظر تعليقاتنا الواردة في تذييل هذه الورقة بشأن المشاكل المتعلقة بمشروعي المادتين 10 و11 بصيغتهما الحالية.

Appendix[21]

Article-by Article Analysis of WP.162

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

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

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

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

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

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

Draft Article 1: Definitions

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

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

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

"Authentication" is used only in terms of trust services; it has the same meaning as "electronic identification". We believe it could be misleading to have two terms for the same concept and would recommend using the same term for this concept

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

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

throughout the draft. As noted above, however, we believe the term "electronic identification" itself may be misleading.

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

Draft Article 2: Scope of application

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

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

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

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

We do find a more serious problem reconciling draft article 2(3) with draft article 9(1) Option A. These two sections, we believe, cannot be reconciled. Were the instrument intended to supersede all laws that may require a specific mode of identification, the

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

instrument would risk being non-enactable. In addition, this interpretation would expressly contradict the language of draft article 2(3). In our view, the draft instrument provides contradictory rules: electronic identification meets the requirements of other legal identification requirements, and the instrument does not displace any other legal identification requirements. These conflicting rules cannot co-exist if the draft instrument. We view Option B of draft article 9 as essentially restating the rule of Option A. We believe the Working Group must re-examine these draft articles and reformulate them to express a non-contradictory policy that respects the existing legal requirements that are recognized in draft article 2(3).

Draft Article 3: Voluntary use of IdM and trust services

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

Draft Article 4: Interpretation

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

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

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

As for the rule that the instrument should be interpreted on the general principles on which it is based,[29] we suggest that either the draft provide the guidance of what these

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

[25] "There have been questions about the relationship between articles 2 and 3. Would their relationship be clearer by recasting article 3 to state that "Nothing in this [instrument] requires a [person][relying party] to accept the electronic identification of a subject or to rely on a trust service without the [person's][relying party's] consent. "?".

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

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

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

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

principles are[30] or this rule should be removed. To do otherwise creates the risk of vagueness and uncertainty in the text.[31]

Draft Article 5: Legal recognition of IdM

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

Draft Article 6: Obligations of IdM service providers

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

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

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

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

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

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

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

should be some obligations by an IdM service provider where there has been a breach of security. As we noted note our comments to draft article 6, however, there may be multiple parties involved in the IdM service provider process.[33] For this reason, we believe the Working Group should reconsider the language of draft article 7 to reflect the various parties that may be involved in IdM process and accordingly fix the obligations based on the respective nature and status of these parties consistent with which party is best placed to respond to the breach.

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

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

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

Draft Article 8: Obligation of subscribers

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

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

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

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

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

(c) it is not currently required by law applicable to paper-based credentials (e.g., the bartender who refuses entry to a person because he determines that the person

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

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

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

has presented a false driver's license or someone else's driver's license is not required to report that to the issuing authority).[36]

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

Draft Article 9: Identification of a person using IdM

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

Draft Article 10: Factors relevant in determining reliability

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

Draft article 10 provides an illustrative list of factors to determine the reliability of an IdM service. If article 10 only applies to systems governed by contractual rules, it is not clear what the purpose of the list of possible considerations serve. This list is not useful to explain and interpret an otherwise applicable contractual agreement. If draft article 10 is intended to provide a minimal standard of reliability for IdM systems, then it is not clear how an illustrative and not a mandatory list would operate.

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

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

Draft Article 11: Designation of reliable IdM systems

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

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

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

Draft Article 12: Liability of IdM service providers

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

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

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

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

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

Draft Article 13: Legal recognition of trust services

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

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

Draft Article 14: Obligations of trust service providers

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

If the intent is to impose some minimal obligation on trust service providers below which the parties cannot contract, this should be expressly stated. If that is the intent,

we believe the Working Group should address the question of mandatory rules and their relationship to freedom of contract.

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

Draft Article 15: Obligations of trust service providers

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

Draft Articles 16–20: Various trust services

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

Draft Article 21: Website authentication

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

Draft Article 22: Identification of objects

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

Draft Article 23: Reliability standards for trust service providers

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

Draft Article 24: Designation of reliable trust services

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

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

Draft Article 25: Liability for trust service providers

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

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

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

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

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

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

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

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

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

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

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

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

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

Draft article 27: International Aspects of the Draft Law

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

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

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