Организация Объединенных Наций A/CN.9/WG.IV/WP.165

Генеральная Ассамблея

Distr.: Limited
30 September 2020
Russian
Original: English

Комиссия Организации Объединенных Наций по праву международной торговли
Рабочая группа IV (Электронная торговля)
Шестидесятая сессия
Вена (онлайн), 19–23 октября 2020 года

Пересмотр подхода к управлению идентификационными данными и удостоверительными услугами

Представление Соединенных Штатов Америки

Записка Секретариата

Соединенные Штаты Америки представили документ для рассмотрения на шестидесятой сессии Рабочей группы. Этот документ воспроизводится в качестве приложения к настоящей записке в том виде, в котором он был получен Секретариатом.

V.20-05630 (R) 131020 131020

Приложение

Пересмотр подхода к управлению идентификационными данными и удостоверительными услугами

1. Соединенные Штаты рады представить настоящий документ, касающийся текущего проекта Рабочей группы IV по системам управления идентификационными данными (УИД) и удостоверительными услугами. Настоящий документ состоит из трех разделов. В первом разделе настоящего документа содержится общий обзор и резюме последующих разделов. Во втором разделе приведена справочная информация о системах УИД и правилах их функционирования. Наконец, в третьем разделе содержится обзор правовой базы, на основе которой как правило функционируют все системы УИД, а также изложены концептуальные рамки, при помощи которых Рабочая группа могла бы адаптировать текст документа WP.162 для эффективного решения вопросов, связанных с системами УИД в частном секторе.

2. В настоящем документе Соединенные Штаты Америки уделяют основное внимание только системам УИД и тому, каким образом Рабочая группа может эффективно решать вопросы, связанные с такими системами. При этом Соединенные Штаты приветствовали бы проведение в Рабочей группе аналогичного обсуждения по той части документа WP.162, которая посвящена удостоверительным услугам, поскольку, по нашему мнению, в связи с этой частью возникают многие аналогичные концептуальные вопросы, которые затрагиваются ниже в отношении положений об УИД.

I. Обзор и резюме

3. В качестве общего замечания Соединенные Штаты Америки выражают сильную обеспокоенность в связи с нынешним подходом Рабочей группы к системам УИД, который отражен в документе WP.162 (см. добавление), и считают, что для преодоления этой обеспокоенности в Рабочей группе необходимо провести обсуждение на концептуальном уровне.

4. Задача ЮНСИТРАЛ должна заключаться в создании основы, призванной помочь государствам в решении правовых вопросов, которые могут возникнуть в связи с системами УИД в частном секторе, в частности в тех областях, которые не могут быть охвачены установленными в отдельных договорах правилами, регулирующими функционирование конкретной системы УИД. Это может включать пересмотр действующего национального законодательства с целью устранения барьеров и неопределенности и заполнения пробелов в действующем законодательстве, касающемся систем УИД, которые не могут быть преодолены на договорной основе, или для решение новых вопросов, которые могут способствовать развитию систем идентификационных данных в частном секторе. Тем не менее в документе WP.162 принят существенно иной, и, по мнению США, неэффективный подход.

A. Что такое системы УИД?

5. **Управление идентификационными данными** включает комплекс мер, процессов и процедур, позволяющих идентифицировать физическое или юридическое лицо (т.е. установить «Кто вы?») и удостоверить подлинность идентификационных данных (т.е. определить «Как вы можете это доказать?»). Как более подробно описывается в разделе II ниже, **операция с идентификационными данными** представляет собой сообщение, в котором полагающаяся сторона получает определенную часть идентификационной информации о субъекте таким образом, который удостоверяет подлинность связи между этой

идентификационной информацией и данным субъектом. Системы УИД облегчают проведение **операций с идентификационными данными**. **Системы УИД** представляют собой сложные механизмы, которые предполагают согласованное сочетание участвующих субъектов, процессов и технологий, когда каждый участвующий элемент выполняет одну или несколько заранее определенных функций в соответствии с заранее установленным набором юридически обязательных процессов, мер и процедур с целью облегчения операций с идентификационными данными, которые позволят лицу идентифицировать себя для нескольких несвязанных субъектов.

6. Для этого каждая система УИД нуждается в определенном наборе правил функционирования, подлежащих обязательному соблюдению. Как более подробно описано в разделе II ниже, правила функционирования регулируют работу конкретной системы УИД, устанавливая, как будут осуществляться процессы управления идентификационными данными и соответствующие операции с идентификационными данными, а также права и обязанности различных участников этого механизма. Поскольку все системы УИД различаются, для каждой из них требуется уникальный свод правил функционирования, адаптированных к ее целям, структуре, базе участников и параметрам рисков.

7. В случае систем УИД в публичном секторе правила функционирования обычно излагаются в законодательном или нормативном акте и таким образом становятся обязательными для участников в силу закона. В случае систем УИД в частного секторе правила функционирования излагаются в документе, составленном оператором системы (или каким-либо другим физическим или юридическим лицом), и становятся обязательными для участников на основании договора.

B. Какие вопросы следует рассмотреть в документе ЮНСИТРАЛ?

8. Любой документ, разработанный ЮНСИТРАЛ для систем УИД в частном секторе, должен учитывать как действующее национальное законодательство, так и различные основанные на договоре правила функционирования, используемые для каждой отдельной системы УИД. В частности, в документе ЮНСИТРАЛ следует рассмотреть вопросы, касающиеся применимости действующего национального законодательства к системам УИД в частном секторе, которые i) не могут быть решены в отдельных договорных правилах функционирования, принятых для конкретной системы УИД, или ii) иным образом создают проблемы для всех систем УИД в частном секторе. Поэтому примеры областей, которые следует рассмотреть в документе ЮНСИТРАЛ, будут включать: правовое признание операций с идентификационными данными с использованием систем УИД в частном секторе, требования в отношении определения соответствия операции с идентификационными данными частного сектора применимым юридическим требованиям в отношении идентификации личности, а также применимость законодательства, которое не может быть изменено правилами функционирования систем УИД, например законодательства, касающегося использования правительственных идентификаторов, законодательства о защите прав потребителей и законодательства о гражданских правонарушениях.

9. Подобный подход основан на признании того, что системы УИД в частном секторе регулируются трехуровневой правовой базой, в верхней части которой находится действующее национальное законодательство (уровень 1), а в нижней части — отдельные основанные на договоре правила функционирования систем УИД (уровень 3). Средний уровень этой правовой базы (уровень 2) будет служить мостом между уровнем 1 и уровнем 3. Задача ЮНСИТРАЛ должна заключаться в разработке документа, содержащего рекомендации для государств относительно того, что будет содержать второй правовой уровень. Такая правовая база более подробно описана в разделе III ниже (включая рисунок 1, на котором

наглядно показаны эти три правовых уровня и их взаимосвязь). В разделе III приводится также подробный план в отношении возможных подходов ЮНСИТРАЛ к содержанию такого документа.

10. В документе WP.162 такая правовая база не признается и вместо этого применяется существенно иной и, по нашему мнению, неэффективный подход. Хотя в этом документе рассматриваются некоторые вопросы, которые можно было бы надлежащим образом охватить в документе, посвященном уровню 2, в нем объединяются и смешиваются многие вопросы, которые уместнее урегулировать в договорных правилах функционирования конкретной системы УИД (уровень 3). В результате этого в нем часто используется универсальный подход по вопросам, которые будут существенно различаться в отдельных договорных правилах функционирования, регулирующих конкретные системы УИД. По мере продвижения работы по согласованию проекта текста становится все более очевидным, что такой подход не работает.

11. В качестве концептуальной модели в документе WP.162 используются правила функционирования системы УИД для публичного сектора (т.е. eIDAS), которые предлагается распространить на все системы УИД в глобальном масштабе. Правила e-IDAS действительно представляют собой весьма новаторский подход к регулированию систем УИД, и они в значительной степени содействовали углублению понимания во всем мире того, как могут работать системы УИД и как их можно регулировать для использования в публичном секторе. Проблема, однако, заключается в том, что eIDAS является уникальным сводом правил функционирования для единой системы УИД в публичном секторе (состоящей из различных поставщиков идентификационных данных в странах ЕС). Таки образом, эти правила являются предназначенным для публичного сектора эквивалентом договорных правил функционирования, регулирующих конкретную систему УИД в частном секторе. Попытка навязать использование таких правил функционирования во всех других системах УИД не оправдана.

12. Иначе говоря, поскольку eIDAS представляет собой свод правил функционирования, регулирующих *одну систему УИД* (уровень 3), ЮНСИТРАЛ следует разработать документ, который будет применяться ко *всем системам УИД* (уровень 2). Поскольку eIDAS представляет собой свод правил функционирования для системы УИД *в публичном секторе* (т.е. правил, регулирующих операции с идентификационными данными для использования в публичном секторе), ЮНСИТРАЛ следует разработать документ, который будет применяться к системам УИД *в частном секторе*. Документ ЮНСИТРАЛ должен, в частности, служить мостом между договорными правилами функционирования, регулирующими каждую отдельную систему УИД в частном секторе (уровень 3), и теми аспектами действующего национального законодательства (уровень 1), которые отрицательно сказываются на всех системах УИД, но не могут быть урегулированы в рамках правил функционирования для отдельных систем УИД (например, юридическое признание операций с идентификационными данными или гражданско-правовая ответственность)[1].

13. Вместо этого в документе WP.162 устанавливаются правила по ряду вопросов, которые обычно регулируются договорными правилами функционирования каждой отдельной системы УИД. К ним относятся такие вопросы, как обязанности поставщиков услуг УИД (в статье 6), обязанности в случае нарушения (в статье 7), обязанности абонентов (в статье 8) или ответственность поставщика услуг УИД (в статье 12). В то же время в нем отсутствует четкое определение

[1] Хотя eIDAS, вероятно, включает в себя как элементы уровня 2, так и элементы уровня 3 для различных поставщиков идентификационных данных стран ЕС, которые согласны участвовать в единой структуре ЕС, мы считаем, что ЮНСИТРАЛ должна сосредоточиться исключительно на разработке документа, посвященного уровню 2, который будет применяться ко всем поставщикам услуг УИД в частном секторе. Кроме того, поскольку eIDAS функционирует в качестве системы УИД для использования в публичном секторе, задача ЮНСИТРАЛ заключается в разработке документа, который будет применяться к системам УИД в частном секторе.

того, в каких случаях стороны договора могут отступать от действующего законодательства по этим вопросам и в каких случаях они должны соблюдать действующее законодательство.

14. Кроме того, в то время как система eIDAS, лежащая в основе документа WP.162, опирается на централизованный механизм регулирования, установления стандартов и сертификации систем УИД, в глобальном плане не существует такого централизованного механизма для подкрепления положений такого документа ЮНСИТРАЛ, как WP.162. Документ WP.162 просто исходит из того, что такой глобальный механизм существует. В отсутствие такого глобального механизма положения документа WP.162, касающиеся стандартов трансграничного признания и надежности, вызывают ряд вопросов, остающихся без ответа и требующих дальнейшего обсуждения в Рабочей группе. В действительности eIDAS предусматривает признание удостоверительных услуг поставщиками за пределами ЕС только в том случае, если существует соглашение конкретного типа, заключенное между ЕС и третьей страной (статья 14.1 eIDAS).

15. Помимо несоответствия с моделью eIDAS, неуместным является и использование в документе WP.162 в качестве образца Типового закона ЮНСИТРАЛ об электронных подписях. Электронные подписи имеют относительно простой и стандартизированный характер, в то время как системы УИД являются более сложными и многоуровневыми. Например, электронные подписи предполагают участие, как правило, двух сторон, а системы УИД, как правило, — многих сторон. Правила Типового закона об электронных подписях просто не работают в отношении систем УИД.

16. В этой связи возникают весьма простые, но очень важные вопросы: каким образом подход, нашедший отражение в документе WP.162, будет полезен государствам после его принятия? Каким образом в отсутствие централизованного механизма регулирования или сертификации систем УИД или удостоверительных услуг этот текст будет выполнять те функции, которые в нем определяются, например, в отношении трансграничного признания или стандартов надежности? И, если, как это понимают Соединенные Штаты, цель документа WP.162 заключается в том, чтобы он применялся к системам УИД в частном секторе, то каким образом установленные в нем правила соотносятся с правилами функционирования, установленными участниками договора, который регулирует систему УИД?

17. Соединенные Штаты ранее высказывались в отношении проекта положений Секретариата и направляли письменные ответы на последний текст, и в добавлении к настоящему документу содержится постатейный анализ текста в документе WP.162. Вместе с тем, по мнению США, прежде чем предпринимать дальнейшие шаги на основе документа WP.162, Рабочей группе следует сначала провести концептуальное обсуждение для уточнения того, каким образом этот документ будет вписываться в общую правовую базу, регулирующую системы УИД. Хотя Соединенные Штаты высоко оценивают тот факт, что в процессе подготовки документа WP.162 была проделана значительная работа и что были предприняты усилия по достижению консенсуса в отношении этого документа, будет жаль, если Рабочая группа продолжит идти по пути подготовки документа, который будет редко использоваться государствами-членами или системами УИД в частном секторе.

18. Как указано в настоящем документе, существует ряд областей, в которых вопросы, рассматриваемые в документе WP.162, вполне уместны и имеют прямое отношение к системам УИД, но в которых этот подход не работает, и в этих областях Рабочая группа, возможно, сможет опираться на существующие положения документа WP.162 и включить в них концептуальные изменения. В других областях могут быть оправданы более значительные изменения или исключения.

19. В разделе III ниже в качестве плана Соединенные Штаты предлагают конкретную основу, которую можно использовать для проведения концептуального обсуждения и которая поможет определить направление дальнейших действий.

II. Исходная информация по системам УИД

20. Мы считаем, что целью этого проекта должно быть создание правовой базы, которая позволит сформировать и далее развивать надежную экосистему идентификационных данных, в рамках которой в частном секторе могут успешно функционировать многие системы УИД всех типов, которые будут поддерживать национальную и глобальную торговлю. Для этого потребуется уделить особое внимание выявлению любых препятствий или пробелов в действующем национальном законодательстве, которые необходимо устранить. Кроме того, для поощрения разработки новых и разных систем УИД, важно, чтобы Рабочая группа избегала универсальных подходов к урегулированию вопросов и проблем, которые должны решаться на основе уникальных договорных правил функционирования, установленных для конкретных систем УИД.

21. Для выявления препятствий и пробелов в правовой базе управления идентификационными данными, которые необходимо устранить, нам прежде всего необходимо сделать следующее:

- изучить концепции операций с идентификационными данными и систем УИД;
- изучить необходимость и роль правил функционирования, которые регулируют работу каждой отдельной системы УИД в частном секторе; и
- осмыслить общую правовую базу, регулирующую системы УИД, а также понять то, когда и каким образом документ ЮНСИТРАЛ мог оказаться полезным дополнением, совместимым с такой базой.

22. С учетом этой исходной информации Рабочая группа сможет затем определить правовые вопросы, которые не могут быть решены с помощью уникальных договорных правил функционирования, являющихся частью каждой системы УИД, и которые поэтому необходимо решать путем внесения дополнений и изменений в национальное законодательство с использованием правового документа, разработанного ЮНСИТРАЛ.

A. Операции с идентификационными данными

23. Операция с идентификационными данными представляет собой сообщение, посредством которого полагающаяся сторона получает определенную идентификационную информации о данном лице[2] (идентификация) наряду с проверкой того, что лицо, заявляющее о себе как о данном лице, на самом деле является таким лицом (удостоверение подлинности). Обычно это делается для того, чтобы: 1) заключить какую-либо сделку с конкретным субъектом (например, заключить договор, предоставить выгоды, передать информацию и т.д.) или 2) предоставить субъекту доступ к какому-либо цифровому или физическому объекту (например, к веб-сайту, базе данных, зданию и т.д.).

24. Операции с идентификационными данными, как правило, предусматривают 1) сбор и проверку информации (атрибутов) об отдельном субъекте данных (процесс идентификации), 2) выдачу идентификационных учетных данных, содержащих один или несколько таких атрибутов (процесс выдачи идентификационных учетных данных), и 3) соотнесения идентификационных атрибутов в этих идентификационных учетных данных с конкретным лицом, которое обычно находится на удалении (т.е. процесс удостоверения подлинности). В рамках этих процессов операции с идентификационными данными предназначены для

[2] Субъектом операции с идентификационными данными может быть физическое лицо, организация, устройство или цифровой объект. В настоящем документе основное внимание будет уделяться физическим лицам, поскольку до настоящего времени они являлись главным предметом обсуждения в Рабочей группе.

проверки идентификационных данных лица и удостоверения подлинности связи таких идентификационных данных с конкретным лицом.

25. Так, например, предъявление паспорта на границе для получения разрешения на въезд в страну является операцией с идентификационными данными. В этом случае полагающаяся сторона (сотрудник пограничной службы) получает предварительно проверенные идентификационные атрибуты лица (указанные в паспорте), а также средства проверки того, что лицо, предъявляющее паспорт, является тем лицом, которое указано в паспорте (т.е. фотографию или данные об отпечатках пальцев, внесенные в паспорт). Операцией с идентификационными данными является также процесс входа в онлайновую сеть с именем пользователя и паролем для получения доступа к базе данных. Эта операция связана с соотнесением (через секретный пароль) ранее проверенных идентификационных атрибутов данного лица (сверяемых через имя пользователя) с лицом, заявляющим о себе как о данном лице (т.е. лицом, вводящим имя пользователя).

B. Системы УИД представляют собой многосторонние системы, предназначенные для упрощения операций с идентификационными данными

26. **Система управления идентификационными данными (УИД)** представляет собой согласованное сочетание участвующих субъектов, процессов и технологий, когда каждый участвующий элемент выполняет одну или несколько заранее определенных функций[3] в соответствии с заранее определенным набором юридически обязательных процессов, принципов и процедур с целью облегчения операций с идентификационными данными.

27. Системы УИД — это сложные многосторонние системы. Они предполагают наличие многих участников, которые выполняют различные функции, например, функции регистрационных органов, контролеров достоверности идентификационных данных, поставщиков атрибутов, поставщиков удостоверительных услуг, поставщиков идентификационных данных, поставщиков услуг по выдаче идентификационных учетных данных, поставщиков услуг по проверке, концентраторов и т.д. Они координируют работу, необходимую для сбора и проверки идентификационных данных (атрибутов) об отдельном субъекте данных, выдают идентификационные учетные данные, содержащие один или несколько таких атрибутов, и удостоверяют подлинность этих идентификационных атрибутов для конкретного лица в рамках операции с идентификационными данными. Эти участники работают совместно с целью облегчения операций с идентификационными данными для многих полагающихся сторон.

28. В плане сложности структуры система УИД аналогична системе кредитных карт, созданной с целью облегчения кредитных операций (например, MasterCard или Visa), или системе электронных платежей, созданной с целью облегчения платежных операций (например, SWIFT или ACH). Хотя каждый из этих видов систем разработан с использованием различной структуры и для разных целей, все они являются многосторонними системами, призванными облегчить экономические операции определенного типа (например, операции с кредитными картами, платежные операции или операции с идентификационными данными).

29. Структуры систем УИД могут существенно различаться. Например, системы УИД могут быть централизованными (с одним поставщиком идентификационных данных, который облегчает проведение операций с идентификационными данными для многих полагающихся сторон), интегрированными (с ограниченным числом поставщиков идентификационных данных, которые

[3] Такие функции могут включать, например, функции регистрационного органа, контролера достоверности идентификационных данных, поставщика идентификационных данных, брокера, концентратора, поставщика атрибутов, полагающейся стороны и т. д.

централизованно хранят и предоставляют идентификационные данные пользователей для облегчения операций с идентификационными данными с одной или несколькими полагающимися сторонами) или распределенными (со многими поставщиками идентификационных данных, которые удостоверяют подлинность идентификационной информации, хранимой пользователями на местном уровне, для облегчения операций с идентификационными данными со многими полагающимися сторонами). Такое разнообразие структур системы УИД является одним из главных оснований, указывающих на то, что в документе, разрабатываемом Рабочей группой, нельзя использовать один универсальный подход для решения многочисленных вопросов.

C. Системы УИД требуют применения юридически обязательных правил функционирования

30. Поскольку системы УИД являются сложными многосторонними системами, важное значение для достижения желаемой цели имеет координация и сотрудничество участвующих субъектов. Поэтому для систем УИД требуется организованная, целенаправленная структура, которая состоит из взаимосвязанных и взаимозависимых участвующих субъектов, выполняющих различные функции, осуществляющих комплекс подробно определенных процессов и соблюдающих комплекс мер и процедур, которые направлены на достижение конкретной цели, а именно на облегчение операций с идентификационными данными.

31. Кроме того, поскольку системы УИД предполагают наличие многих независимых участвующих субъектов, потенциально взаимодействующих друг с другом для осуществления ряда сложных операций, они, как таковые, не работают в автоматическом режиме. Каждый из участников должен руководствоваться сводом правил или инструкций, касающихся того, как он должен действовать в соответствии со своей конкретной ролью. И такие правила, как правило, должны иметь обязательную юридическую силу, чтобы все участники соблюдали применимые к ним требования и могли рассчитывать на то, что все остальные участники будут следовать этим правилам и обеспечивать надежный результат.

32. Соответственно, каждая система УИД требует наличия юридически обязательного свода **правил функционирования**[4], регулирующих ее работу. Такие правила функционирования выполняют три важные функции:

- они обеспечивают **правильную работу** системы УИД, а именно определяют принципы, процедуры и процессы, необходимые для работы системы УИД, чтобы она «работала», как это предусмотрено;
- они определяют **обязанности и обязательства** каждого участника (например, для того чтобы каждый участник знал, что делать), а также его юридическую ответственность и (если это необходимо) определяют и справедливо распределяют риски ответственности; и
- они устанавливают дополнительные требования, которые содействуют обеспечению «**надежности**» системы УИД для установленной цели, т.е. они устанавливают требования, которые выходят за рамки обеспечения лишь работоспособности системы УИД, и предусматривают дополнительные меры для обеспечения уверенности участников в результате операций с идентификационными данными и их готовности полагаться на них.

33. Для достижения этих целей правила функционирования обычно разрабатываются для решения конкретных коммерческих, технических и юридических

[4] Правила функционирования также часто имеют различные другие названия, такие как «Основы управления», «Основы удостоверения», «Правила схемы» и «Системные правила».

вопросов, которые возникают при эксплуатации конкретной системы УИД. К таким вопросам могут, например, относиться вопросы, касающиеся требований к участию, определения функций и обязанностей, процессов и процедур подключения субъектов данных, подтверждения подлинности идентификационных данных, выдачи идентификационных учетных данных и удостоверения их подлинности, технических спецификаций и стандартов, требований к обеспечению безопасности данных, гарантий, распределения ответственности, порядка урегулирования споров и прав на прекращение договора. В правилах функционирования рассматриваются также вопросы управления системой УИД, такие как квалификационные данные для участия, обеспечение соблюдения правил и пересмотр правил. Они определяют основы управления системой УИД. Кроме того, поскольку структура, технология и цель каждой системы УИД могут быть различными, правила функционирования каждой отдельной системы УИД, скорее всего, будут существенно различаться.

34. Для обеспечения того, чтобы правила функционирования системы УИД были юридически обязательными и подлежащими исполнению, они могут принимать форму законодательного или нормативного акта, или договора.

35. В случае систем УИД в **публичном секторе** правила функционирования обычно составляются в форме подробного **закона** или нормативного акта. В качестве примеров можно привести Закон Аадхаара[5] в Индии, Закон об идентификационных документах в Эстонии[6] и Постановление о eIDAS в ЕС[7]. В то же время некоторые системы УИД, например система УИД GOV.UK.Verify, функционируют на договорной основе[8].

36. В случае систем УИД в **частном секторе** правила функционирования принимают форму **договора**, положения которого являются обязательными для участников системы (так же, как участники системы использования кредитных карт или платежной системы соглашаются посредством договора с условиями правил функционирования, применимыми к их функции). Примерами правил функционирования системы УИД в частном секторе являются, в частности, Основы удостоверения идентификационных данных SAFE[9], Основы управления Sovrin[10] и Основы пан-канадской системы удостоверения идентификационных данных[11]. См. также “A Guide to Trust Frameworks and Interoperability” («Руководство по основе систем удостоверения идентификационных данных и функциональной совместимости»)[12].

---

[5] Аадхаар (Целевое предоставление финансовых и других субсидий, льгот и услуг), 2016 год, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

[6] Закон об идентификационных документах, принят 15.02.1999, RT I 1999, 25, 365, вступил в силу 01.01.2000 https://www.riigiteataja.ee/en/eli/ee/504112013003/consolide.

[7] Постановление (ЕС) N°910/2014 об электронной идентификации и удостоверительных услугах в отношении электронных операций на внутреннем рынке (Постановление eIDAS), принятое 23 июля 2014 года, обеспечивает предсказуемую нормативную среду, позволяющую безопасно и бесперебойно осуществлять электронное взаимодействие между коммерческими структурами, гражданами и государственными органами; см. 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/1XmjhQJZKWmRkaTtE2f43ISntD7jE6D5/view.

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

D. Правила функционирования являются уникальными для каждой системы УИД

37. Каждая система УИД отличается от других и, следовательно, требует уникального набора правил функционирования, приспособленных к ее структуре, технологии, цели, рыночному профилю и профилю риска.

38. В системах УИД в частном секторе используются самые разные **структуры и технологии** и все они требуют различных подходов к составлению правил функционирования. Попытки навязать единый универсальный набор таких правил для всех систем будут мешать развитию таких систем УИД в частном секторе.

- К примерам различающихся **структур систем** УИД, выявленных на Всемирном экономическом форуме в 2016 году[13], относятся, в частности, внутренние системы УИД, внешние системы УИД для удостоверения подлинности, централизованные идентификационные системы УИД, федеративные системы УИД и распределенные идентификационные системы УИД. Другие более новые структуры систем УИД включают системы УИД на базе концентратора и независимые системы УИД, а также системы УИД с использованием мобильных телефонов. Каждая из этих систем требует различного подхода к разработке правил функционирования и пострадает от попыток навязывания единого свода таких правил для всех систем.
- К примерам разных **технологий систем** УИД относятся, в частности, системы на основе ИПК, системы на основе распределенных реестров и системы, использующие стандарты OAuth и OpenID Connect, каждая из которых требует особого подхода к разработке правил функционирования и пострадает от попыток навязывания единого свода таких правил для всех систем.

39. Системы УИД в частном секторе обычно также разрабатываются для самых различных **целей и/или рынков**, что требует применения в их правилах функционирования самых различных подходов, требований к удостоверению и процедур распределения рисков. Попытки навязать единый универсальный свод правил для всех систем УИД будут сдерживать развитие таких систем УИД.

- Примеры систем УИД, разработанных для самых различных **целей и рынков**, включают: систему УИД InCommon, разработанную для использования в образовательных целях (например, для университетов и студентов); систему УИД SAFE BioPharma IdM, разработанную для фармацевтической промышленности; систему УИД CertiPath, разработанную для международной аэрокосмической промышленности; систему УИД CA Browser Forum, предназначенную для идентификации операторов веб-сайтов; систему ZenKey, разработанную для идентификации мобильных данных; и упрощенные системы УИД Google, LinkedIn и Facebook, разработанные для доступа к веб-сайтам с низким уровнем риска.

40. Поскольку вопросы, решаемые такими правилами функционирования, касаются удовлетворения уникальных потребностей конкретной системы УИД, они выходят за рамки документа, разрабатываемого Рабочей группой.

41. Поскольку правила функционирования систем УИД в частном секторе основываются на договорах и обусловлены уникальными потребностями конкретных систем УИД, важно, чтобы в любом документе, который разрабатывает ЮНСИТРАЛ, не предпринималось попыток дублировать эти правила функционирования посредством использования универсального подхода в отношении всех систем УИД. В этой связи одной из задач Рабочей группы является разработка документа, который не будет ограничивать возможности или способность

[13] See World Economic Forum, “A Blueprint for Digital Identity,” August 2016, at http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

системы УИД в частном секторе разрабатывать свои собственные правила функционирования и в то же время будет четко определять те правовые требования, которым должны соответствовать правила функционирования, основанные на договоре.

III. Правовая база, регулирующая системы УИД в частном секторе, и возможный документ ЮНСИТРАЛ

A. Общая правовая база

42. Мы считаем, что в качестве предварительного условия для разработки документа такого типа как документ WP.162, Рабочей группе необходимо рассмотреть структуру общей правовой базы, регулирующей системы УИД в частном секторе. В частности, Рабочей группе следует рассмотреть вопрос о том, каким образом i) отдельные правила функционирования различных систем УИД в частном секторе и ii) предлагаемый документ ЮНСИТРАЛ будут вписываться в эту базу. Это имеет важное значение для определения того, какие вопросы следует рассмотреть в документе ЮНСИТРАЛ.

43. Системы УИД в частном секторе, как и большинство коммерческих систем многосторонних операций, обычно регулируются правовой базой, состоящей из i) государственного законодательства и ii) основанных на договоре соглашений участвующих субъектов. **Государственное законодательство** состоит из норм, принятых в форме законодательных актов законодательными органами, принятых в форме подзаконных актов правительственными органами или определенных на основании судебного решения. **Договорное право** состоит из правил, разработанных одним или несколькими участниками или руководящими органами системы УИД, а именно правил функционирования системы УИД, которые становятся обязательными для участников системы УИД на основании договора.

44. Правовая база, в соответствии с которой функционирует любая система УИД в частном секторе, как правило, состоит максимум из трех уровней (или ступеней) законодательства, при этом каждый последующий уровень регулирования системы УИД является более конкретным. Три уровня правовой базы характеризуются следующим образом (и изображены на диаграмме на следующей странице):

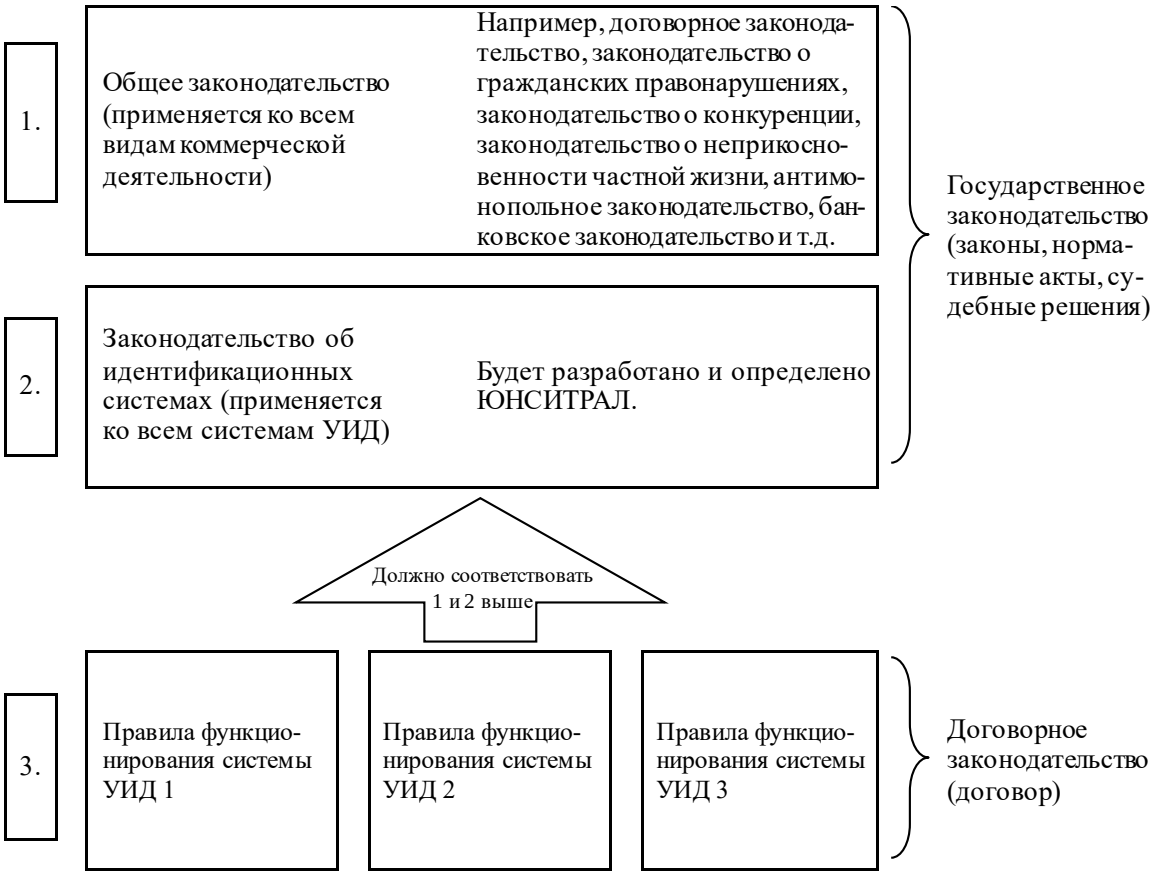
- **(Уровень 1) Действующее законодательство:** верхним и самым общим уровнем является просто **действующее национально законодательство**. Речь идет о государственном законодательстве, которое включает законодательные и нормативные акты, а также судебные решения. Это законодательство регулирует все виды коммерческой деятельности, и оно не предназначено специально для систем УИД, а в некоторых случаях принято сотни лет назад. Тем не менее, его часто применяют к деятельности систем УИД в частном секторе. Оно включает общее законодательство о договорах, законодательство о гражданских правонарушениях, законодательство о неприкосновенности частной жизни, законодательство о контроле над экспортом, гарантийное законодательство, законодательство о защите прав потребителей, законодательство о конкуренции, банковское законодательство и тому подобное.
- **(Уровень 2) Законодательство об идентификационных системах:** второй уровень законодательства, регулирующего системы УИД в частном секторе, можно назвать з**аконодательством об идентификационных системах**. Оно предназначено специально для того, чтобы регулировать ***все*** системы УИД в частном секторе, независимо от их типа, структуры, технологии или цели. Законодательство об идентификационных системах уровня 2 также является государственным законодательством, и оно

предназначено для решения проблем, которые создает действующее законодательство уровня 1 для всех систем УИД, и может заполнять некоторые пробелы, которые просто не охвачены законодательством уровня 1. Оно должно находится между действующим законодательством уровня 1 и отдельными договорными правилами функционирования систем УИД уровня 3.

- **(Уровень 3) Индивидуальные правила функционирования систем УИД:** Третий уровень законодательства, регулирующего системы УИД в частном секторе, состоит из договорных правил функционирования систем УИД, составленных специально для каждой системы УИД в частном секторе с целью регулирования ее собственной среды. В отличие от законодательства об идентификационных системах уровня 2, которое применяется ко всем системам УИД, правила функционирования уровня 3 разработаны с учетом уникальных потребностей конкретной системы УИД[14]. Такие правила функционирования могут быть достаточно подробными, но должны соответствовать законодательству уровня 1 и уровня 2.

45. Задача Рабочей группы заключается в разработке документа, в котором будут изложены элементы законодательства уровня 2.

Диаграмма 1
Правовая база для систем УИД в частном секторе: три уровня законодательства



[14] Следует отметить, что в случае систем УИД в публичном секторе, например, национальной системы удостоверения личности, правила функционирования таких систем закреплены в законодательном или нормативном акте. Таким образом, законодательство уровня 2 и законодательство уровня 3 объединены.

B. В чем должна состоять цель документа ЮНСИТРАЛ?

46. Во избежание применения универсального подхода, который будет сдерживать развитие систем УИД в частном секторе и связанной с ними коммерческой деятельности Рабочей группе следует разработать документ, который будет касаться только тех вопросов, которые не могут быть решены в индивидуальных правилах функционирования систем УИД. Кроме того, его сфера действия должна быть ограничена изменением и/или дополнением существующего национального законодательства уровня 1 только в той мере, в какой это необходимо для стимулирования и поддержки развития систем УИД в частном секторе для содействия коммерческой деятельности в режиме онлайн. Это предполагает разработку документа уровня 2, который обеспечит:

- устранение препятствий и неопределенности в действующем законодательстве уровня 1, сдерживающих развитие систем УИД в частном секторе;
- заполнение пробелов в действующем законодательстве уровня 1, что имеет важное значение для успешного развития систем УИД в частном секторе, но не может быть решено на договорной основе; и
- рассмотрение новых универсальных вопросов для содействия развитию всех систем УИД в частном секторе.

47. Кроме того, с учетом разнообразия систем УИД и уникальных потребностей каждой из них, любой документ уровня 2, разработанный Рабочей группой, должен учитывать принципы технической нейтральности и нейтральности идентификационных систем. Решающее значение, в частности, имеет нейтральность идентификационных систем с учетом широкого разнообразия структур, технологий, целей и рынков, используемых системами УИД в частном секторе, о чем говорилось выше.

48. Напротив, документ WP.162 составлен таким образом, что в нем устанавливаются жесткие правила, касающиеся *обязанностей поставщиков услуг УИД* (статья 6), *обязанностей поставщиков услуг УИД в случае нарушения безопасности данных* (статья 7), *обязанностей абонентов* (статья 8) или *ответственности поставщика услуг УИД* (статья 12). Для систем УИД в частном секторе такие вопросы должны решаться в их отдельных правилах функционирования систем. Решение каждого из этих вопросов требует применения уникального подхода, адаптированного к конкретной структуре, технологии, цели и соответствующему рынку системы УИД. Любые попытки решать вышеупомянутые вопросы будут сопряжены с проблемами, поскольку эти вопросы, вероятно, будут существенно различаться в конкретных системах УИД, и навязывание универсального подхода к системам УИД приведет только к сдерживанию развития систем УИД в частном секторе.

C. Характер документа ЮНСИТРАЛ

49. Вместо этого Рабочая группа могла бы рассмотреть вопросы, которые относятся к следующим категориям[15]:

- прямое признание роли правил функционирования для управления системами УИД;
- вопросы, не урегулированные в действующем законодательстве уровня 1, которые в силу их характера не могут быть решены в основанных на договоре правилах функционирования. Примерами являются:

[15] Это предварительный перечень возможных вопросов для рассмотрения в документе уровня 2, подлежащем разработке и уточнению Рабочей группой, который учитывает, в частности, потребности различных действующих режимов на национальном уровне.

- правовое признание УИД[16];
- требования в отношении определения условий, при которых операция с идентификационными данными удовлетворяет применимым юридическим требованиям в отношении идентификации какого-либо лица[17];
- целесообразность оценки (и если это целесообразно, то каким образом) надежности систем УИД в частном секторе[18];

• вопросы, частично рассматриваемые в действующем законодательстве уровня 1, но без конкретной применимости к системам УИД, что создает неопределенность, которая может создавать проблемы для систем УИД из-за сложности их урегулирования в договорных правилах функционирования. Примерами являются:

- применимость действующего законодательства о гражданских правонарушениях к участникам системы УИД;
- применимость законодательства о неумышленном введении в заблуждение;
- применимость действующего законодательства о косвенных гарантиях;

• вопросы, которые, возможно, потребуется включить в действующее законодательство, например:

- право систем УИД использовать информацию из государственных систем УИД;
- право систем УИД использовать идентификаторы, выданные правительством (например, SSN, национальный идентификационный номер и т. д.);

• вопросы, которые, независимо от возможности их решения в договорных правилах функционирования, должны решаться одинаково для всех систем УИД по соображениям публичного порядка, например:

- следует ли предусматривать трансграничное признание, и если да, то каким образом[19];
- следует ли рассматривать вопросы надежности с юридической точки зрения, и если да, то каким образом[20].

50. Документ ЮНСИТРАЛ, содержащий такие элементы, поможет государствам разработать законодательство об идентификационных системах уровня 2, которое позволит 1) стимулировать развитие систем УИД в частном секторе, 2) устранить препятствия на пути такого развития и 3) учесть и подтвердить, насколько это возможно, необходимость разработки для каждой системы УИД в частном секторе собственных правил функционирования.

---

[16] На решение этого вопроса направлена статья 5 документа WP.162. См. наши замечания в отношении проблем с нынешним проектом статьи 5 в добавлении.

[17] На решение этого вопроса направлена статья 9 документа WP.162. См. наши замечания в отношении проблем с нынешним проектом статьи 9 в добавлении.

[18] На решение этого вопроса направлена статья 11 документа WP.162. См. наши замечания в отношении проблем с нынешним проектом статьи 11 в добавлении.

[19] На решение этого вопроса направлены статьи 10 и 11 документа WP.162. См. наши замечания в отношении проблем с нынешними проектами статей 10 и 11 в добавлении.

[20] На решение этого вопроса направлены статьи 10 и 11 документа WP.162. См. наши замечания в отношении проблем с нынешними проектами статей 10 и 11 в добавлении.

Appendix[21]

Article-by Article Analysis of WP.162

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

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

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

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

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

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

Draft Article 1: Definitions

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

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

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

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

As to the secretariat’s inquiry whether there should be a definition of levels of assurance, we believe such a definition is unnecessary. We note the secretariat’s

[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.

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 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

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

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

---

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

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

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

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

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

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

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

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

Draft Article 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 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.

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

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

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

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 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

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

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

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.

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.

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

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

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.