Организация Объединенных Наций ECE/TRADE/C/CEFACT/2023/10

Экономический и Социальный Совет

Distr.: General
31 August 2023
Russian
Original: English

Европейская экономическая комиссия

Исполнительный комитет

Центр по упрощению процедур торговли и электронным деловым операциям

Двадцать девятая сессия
Женева, 9 и 10 ноября 2023 года
Пункт 6 c) i) предварительной повестки дня
Рекомендации, стандарты и результаты, поддерживающие внедрение: результаты для поддержки внедрения: доклады и руководства

Доклад направления «Упрощение процедур торговли» и агропродовольственного направления — обмен цифровыми сертификатами соответствия продукции*

Представлен Бюро

Резюме

В данном докладе рассматриваются проблемы и предлагаются принципы, регулирующие выдачу сертификатов соответствия и обмен ими между участниками цепочки поставок из частного и государственного секторов. Эти принципы должны обеспечить выдачу и распространение сертификатов соответствия таким образом, чтобы сохранить поддающуюся проверке связь с физической поставкой продукции, а также заложить основу для независимой цифровой проверки статуса выданного свидетельства и полномочий, на основании которых оно было выдано. В качестве одного из способов решения существующих проблем предлагается использовать технологию, позволяющую связать сертификаты соответствия с физической поставкой продукции.

Документ ECE/TRADE/C/CEFACT/2023/10 представляется на пленарном заседании двадцать девятой сессии СЕФАКТ ООН для принятия к сведению.

* Настоящий документ выпускается без официального редактирования.

Содержание

I. Резюме

1. Обмен сертификатами соответствия между участниками цепочки поставок представляет собой важнейший элемент современной мировой торговли. Существующие бумажные процедуры имеют общепризнанные проблемы. Однако необходимые процедуры, семантика и правовая база для перехода к полностью цифровым системам аттестации до сих пор не согласованы.

2. В настоящем документе рассматриваются новые возможности, возникающие в тех случаях, когда проблема формулируется в терминах доступа к сертификатам соответствия (а не обмена ими). В качестве одного из способов решения существующих проблем предлагается использовать технологию, позволяющую связать сертификаты соответствия с физической поставкой продукции. В документе также указывается на то, что это может стать естественной структурой для будущего перехода к полностью цифровым системам, но при этом отмечается, что детальное изучение этого вопроса выходит за рамки настоящего документа.

3. В документе делаются следующие выводы:

- необходимо связать сертификаты соответствия с физической продукцией и контролировать процесс пересмотра и статус выдавшего органа (см. главу III, раздел C);
- отсутствие каких-либо согласованных процессов обмена сертификатами соответствия является препятствием для интероперабельности (см. главу III, раздел D);
- обмен бумажными сертификатами соответствия по своей природе сопряжен с юридическими двусмысленностями и лазейками, которые могут усугубить другие недостатки процесса (см. главу III, раздел E);
- в существующей правовой базе трансграничного обмена данными имеются пробелы. Поэтому любая работа по созданию систем обмена цифровыми сертификатами соответствия должна проводиться с учетом того, что среда точно не определена и может измениться, и это может повлиять на будущий выбор идентификаторов и конкретных цифровых технологий (см. главу III, раздел F);
- поскольку среди важнейших элементов данных, связанных с обменом сертификатами соответствия, преобладают идентификаторы, необходима дальнейшая работа по анализу моделей данных Центра Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ/ООН), имеющих потенциальное отношение к представляющим интерес идентификаторам. Кроме того, отмечается, что для создания связей, необходимых для решения поставленной задачи, уже существуют отлаженные системы, предусматривающие, в том числе использование уникальных глобальных идентификаторов (см. главу IV, раздел A.1);
- регулирование статуса пересмотра является более сложной задачей, чем может показаться на первый взгляд, и для ее решения используются различные несовместимые подходы. Важным моментом является то, что органы, проводящие оценку соответствия (ООС) или стороны (например, владельцы схем), действующие от их имени при предоставлении доступа к данным о соответствии, занимают центральное место в этом процессе и что обмен ссылками на сертификаты может быть более эффективным, чем обмен самими сертификатами (см. главу IV, раздел B);
- набор взаимодополняющих процессов, основанных на увязанных между собой данных, может быть выражен в общих терминах, используемых для решения поставленной задачи (см. главу IV, раздел C.3); и
- несмотря на то, что для выборочного исключения конфиденциальных данных существует технология, она не может применяться последовательно в силу

того, что процесс обмен сертификатами соответствия сегодня не отличается целостностью. Наделение ООС более важной ролью может способствовать более последовательному применению технологии с точки зрения процесса (см. главу IV, раздел D).

4. Сформулирован ряд общих принципов, которые могут служить «ориентирами» для дальнейшей работы. При этом признается, что, хотя некоторые вопросы еще предстоит решить, технологии и системы, необходимые для устранения недостатков существующих «аналоговых» систем, уже имеются и что ООС могут играть центральную роль в будущих цифровых торговых системах. В качестве следующего шага рекомендуется разработать спецификацию требований ведения деловых операций (СТДО) СЕФАКТ ООН, которая позволит более детально и содержательно раскрыть концепции, рассмотренные в данном документе. Кроме того, внимание обращается на возможность сотрудничества между соответствующими глобальными органами, отвечающими за торговлю и соответствие продукции требованиям, с тем чтобы в ходе будущей работы не допустить формирования раздробленных или изолированных систем.

II. Введение

5. Данная глава служит введением в рассматриваемую проблему. Также даются некоторые пояснения по терминологии, используемой в настоящем документе.

A. Терминология

6. В рассматриваемом проекте рассматриваются сертификаты соответствия, выдаваемые третьими сторонами при проведении испытаний, инспекций и сертификации (ИИС), сокращенно именуемые в докладе «сертификатами соответствия».

7. Термин «сертификат» охватывает любой документированный результат оценки соответствия, включая сертификат, описывающий область применения и стандарты, на соответствие которым сертифицирована продукция, или протокол испытаний, в котором указаны результаты испытаний на соответствие стандарту. В настоящем документе важными признаются все виды испытаний и инспекций продукции, однако анализируются лишь те виды сертификации, которые касаются системы управления или рассматриваемой продукции.

B. Постановка задачи

8. Процессы ИИС лежат в основе глобальной системы подтверждения соответствия продукции и процессов. ИИС позволяют доказательно подходить к обоснованию утверждений о продукции, в том числе утверждений о качестве, происхождении и безопасности, и утверждений экологического/социального/управленческого характера. Международные рынки и потребители полагаются на обширную глобальную экосистему систем и услуг ИИС. Передача сертификатов соответствия продукции исторически основывалась на обмене бумажными или факсимильными электронными документами.

9. Однако проверить подлинность бумажных документов, подтверждающих соответствие, и убедиться в том, что содержащиеся в них утверждения представляют собой текущую версию подлинного документа, а также в том, что лица, делающие такие утверждения, обладают соответствующими полномочиями, может быть затруднительно. В результате продукция может быть ошибочно принята как соответствующая назначению, но при этом сопровождаться поддельными, измененными или устаревшими сертификатами, сертификатами, не имеющими четкой связи с физической партией продукции, а также сертификаты, выданные сторонами, не имеющими соответствующих полномочий.

10. Эти уязвимости присущи бумажным системам ИИС и представляют собой «подводные камни» для сторон, сталкивающихся со слабыми процессами подтверждения соответствия, когда сертификат соответствия принимается без проверки его легитимности. Эти вопросы особенно сложны в контексте международной торговли, когда как выдающие, так и запрашивающие стороны неизвестны друг другу.

11. Учитывая огромный объем данных о соответствии, связанных с торгуемой продукцией, проверка всех предоставленных подтверждений соответствия в ручном режиме никогда не была возможной. Вследствие этого ручная верификация часто применяется в торговых ситуациях, когда доверие между сторонами еще не достигнуто, или для продукции с высоким уровнем риска. Переход на цифровые системы чреват ухудшением ситуации, если не будет должным образом решена проблема цифровой проверки сертификатов соответствия продукции.

12. Цель данного документа — обсудить, как сертификаты соответствия продукции могут быть адаптированы к безбумажной торговой среде, что позволит оптимизировать преимущества цифровых технологий и принести пользу обществу, гарантировав пользователям и регулирующим органам достоверность и прозрачность сведений о продукции.

13. Непроверенные сведения о товаре, касающиеся его эксплуатационных характеристик или других свойств, таких как экологическое или социальное воздействие, мало что значат в мировой торговле. Необходимо обеспечить, чтобы потенциал международных систем подтверждения соответствия продукции отвечал требованиям цифрового мира, а также возможность их применения в различных юрисдикциях в рамках глобальной цепочки поставок.

C. Охват настоящего доклада

14. В данном документе рассматривается обмен сертификатами соответствия, выдаваемыми на торгуемые физические товары. Эта информация о соответствии может быть запрошена как коммерческими организациями, так и государственными структурами. Такие процессы являются частью коммерческих процедур, определяемых в Справочной модели международной цепочки поставок (СММЦП) СЕФАКТ ООН и находящих отражение в справочных моделях данных СЕФАКТ ООН «покупка — отгрузка — оплата» (ПОО).

15. В данном документе рассматриваются проблемы и предлагаются принципы, регулирующие выдачу сертификатов соответствия и обмен ими между участниками цепочки поставок из частного и государственного секторов. Эти принципы должны обеспечить выдачу и распространение сертификатов соответствия таким образом, чтобы сохранить поддающуюся проверке связь с физической поставкой продукции, а также заложить основу для независимой цифровой проверки статуса выданного свидетельства и полномочий, на основании которых оно было выдано. Определение всех элементов данных, содержащихся в сертификатах соответствия (для обеспечения возможности обмена контентом в цифровом виде), не рассматривается как необходимое условие достижения поставленной цели, однако оно открывает дополнительные возможности, которые не рассматриваются подробно в рамках данного документа.

16. В документе не рассматриваются процессы подтверждения соответствия, для которых применимая нормативная база предполагает иные виды аттестации, отличные от испытаний, инспекции или сертификации. Вопрос разработки унифицированных и гармонизированных сертификатов с точки зрения структуры и наборов данных также не рассматривается в данном документе.

17. В документе указаны концепции, которые могут быть применимы независимо от типа отрасли, вида продукции или географии и которые обеспечивают доступ к данным о соответствии, по крайней мере в принципе, для всех типов пользователей, включая участников цепочки поставок.

18. В частности, в документе рассматривается роль испытаний, инспекций и сертификации, проводимых третьей стороной (подробности см. в разделе 2.1), хотя вполне вероятно, что некоторые принципы и концепции будут хотя бы частично применимы к деятельности по подтверждению соответствия первой и второй сторон (см. рис. 1 в следующей главе), а также к формам подтверждения соответствия (например, верификации и валидации), отличным от испытаний, инспекций и сертификации.

III. Обмен сертификатами соответствия

19. Данные, используемые для подтверждения соответствия, являются результатом ряда процессов, известных под общим названием «оценка соответствия», которые позволяют обосновать утверждения о продукции и обеспечить доверие к выбираемой продукции. В этой главе рассматривается, как в настоящее время осуществляется обмен сертификатами соответствия, и указывается на некоторые связанные с этим проблемы.

A. Виды сертификатов соответствия

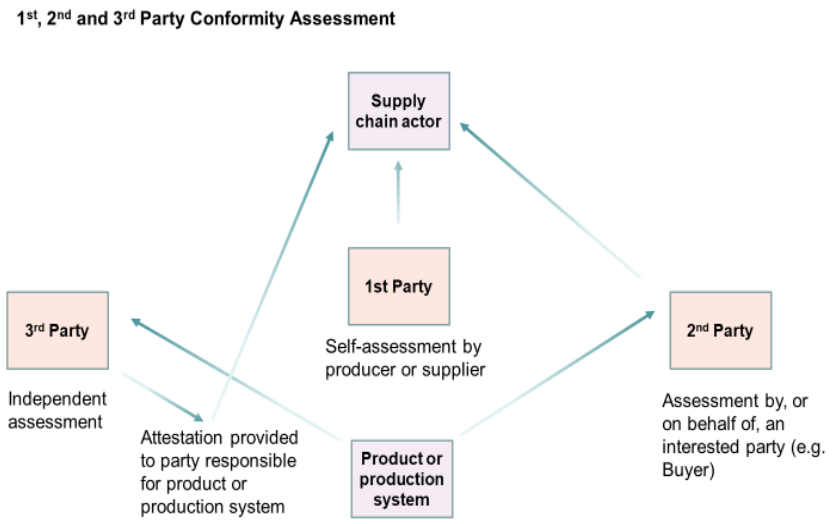
20. Наиболее распространенные виды формальной оценки соответствия, по итогам которой составляется сертификат соответствия, определены в стандарте ИСО/МЭК 17000-2020: «Оценка соответствия. Словарь и общие принципы» следующим образом:

- проведение испытаний: определение одной или нескольких характеристик объекта оценки соответствия согласно процедуре;
- инспекция: проверка объекта оценки соответствия и определение его соответствия четко определенным требованиям или общим требованиям на основе профессионального суждения; и
- сертификация: аттестация третьей стороной, относящаяся к объекту оценки соответствия, за исключением аккредитации.

21. ООС проводят оценку соответствия в соответствии с процессами, методами и требованиями, определенными в применимых стандартах, таких как стандарты ИСО/МЭК 17000[1]. В зависимости от отношений между поставщиком услуг по оценке соответствия и интересующей продукцией могут применяться различные услуги по оценке соответствия; услуги первой стороны, второй стороны и третьей стороны, как показано ниже. Данный документ посвящен исключительно обмену сертификатами соответствия, выдаваемыми третьей стороной.

[1] https://casco.iso.org/toolbox.html.

Рис. 1



22. Законодательная база, в которой работают ООС, может требовать аккредитации или юридического одобрения с учетом специфики той или иной экономики или вида продукции. В соответствии с законодательной базой некоторых юрисдикций сертификаты соответствия должны выдаваться ООС, аккредитованными органами, которые подписали глобальные соглашения о взаимном признании, действующие под эгидой Международного форума по аккредитации (МФА) и Организации по международному сотрудничеству в области аккредитации лабораторий (ИЛАК). Поэтому идентичность органа по аккредитации (когда это применимо) может быть важным элементом данных для валидации выданного сертификата. Более подробно использование таких идентификаторов будет рассмотрено в главе IV, раздел A.1.

B. Участники цепочки поставок, задействованные в обмене

23. В обмене сертификатами соответствия потенциально участвует множество различных участников цепочки поставок. Участники цепочки поставок могут стремиться получить доступ к сертификатам соответствия в силу своей роли в цепочке поставок. Информация обычно передается по цепочке от производителя к оптовику, экспортеру, импортеру, дистрибьютору, розничному продавцу, потребителю, и у разных участников цепочки поставок есть свои причины для получения сертификата соответствия. На следующей схеме приведен пример работы простой производственно-сбытовой цепочки.

Рис. 2

- Кроме производителя, другие участники цепочки, как правило, обращаются за сертификатом соответствия для принятия решений о покупке.
- Кроме потребителя, участники цепочки стремятся получить сертификат соответствия, чтобы иметь возможность продемонстрировать следующему участнику цепочки, что товары, предназначенные для продажи, соответствуют своему назначению.
- Государственные органы и уполномоченные организации как в странах-импортерах и странах-экспортерах, так и в странах транзита часто нуждаются

в доступе к данным сертификации для тех категорий продукции, к которым предъявляются законодательные требования.

- Потребитель, как правило, получает не сертификат соответствия, а производную форму гарантии соответствия установленному стандарту или нормативу.

24. В случае с сырьем или другими исходными материалами обмен сертификатами соответствия может потребоваться только до момента объединения или преобразования материалов или продуктов в новую продукцию. Но даже в таких ситуациях покупатели готовой продукции могут быть заинтересованы и/или обязаны удостовериться в том, что все исходные материалы для производства продукции соответствуют определенным критериям (так называемое отслеживание происхождения).

C. Недостатки существующей системы

25. Помимо фальшивых сертификатов соответствия продукции, описанных Советом по ИИС[2], существует множество других способов искажения сведений о соответствии. Важно отметить, что различные процессы обмена сертификатами соответствии в цепочке поставок существенно отличаются друг от друга с точки зрения их уязвимости к конкретным видам злоупотреблений или мошенничества.

26. Наиболее часто встречающиеся проблемы с достоверностью при обмене сертификатами соответствия можно свести к следующему:

1. Слабость или отсутствие связи между сертификатом соответствия и его объектом

27. За исключением некоторых процессов, в ходе которых правительство или орган власти официально фиксируют связь между товаром и представленным сертификатом соответствия (см. главу III, раздел D), порой трудно установить, связан ли сертификат соответствия с конкретным физическим товаром. Одна из трудностей заключается в том, чтобы определить, к какому товару относится сертификат: к отдельному изделию, к товарной партии или к торговой единице. Другая трудность связана с необходимостью установить, является ли такая связь достоверной и/или проверяемой. Например, результаты лабораторных исследований обычно относятся либо к проверяемому образцу, либо к товарной партии; однако некоторые нерадивые (или недобросовестные) поставщики могут быть заинтересованы в том, чтобы распространять сертификаты соответствия на продолжающую поставляться продукцию (или даже на родственную, но другую продукцию). Отделение деятельности по отбору образцов от деятельности по их тестированию, и, как следствие, практика составления отчетов о результатах тестирования на основе полученных образцов порождает проблемы в этом отношении, поскольку получатели из третьих сторон, скорее всего, не знакомы с контекстом, в котором проводилось тестирование. Вопрос установления связи между сертификатами соответствия и продукцией актуален и в противоположном направлении, т. е. для обеспечения поиска достоверных данных о соответствии, связанных с конкретным товаром, товарной партией или торговой единицей.

2. «Изменением статуса» (отзыв/внесение изменений/истечение срока действия) сертификата

28. Трудно определить, является ли сертификат соответствия актуальным, устаревшим или отозванным. Еще сложнее с уверенностью сказать, было ли полученное в прошлом подтверждение актуальным на момент использования товара. Например, монтаж строительной продукции несколькими годами ранее мог быть

[2] TIC Council Anti-counterfeiting Committee White Paper, Falsified: Test reports and certificates, TIC Council publication, June 2020.

выполнен в соответствии с действующей на тот момент сертификацией, несмотря на последующие изменения в стандартах или правилах.

29. После получения данных о соответствии в цепочке поставок ключевой задачей становится проверка этих данных в источнике. Например, для отслеживания текущих изменений в статусе информации о соответствии продукции необходимо следить за изменением или отзывом сертификатов, а также изменением соответствующих полномочий или статуса их держателей, учитывая при этом, что такие изменения вряд ли будут доводиться до сведения всех заинтересованных сторон. Эти вопросы возникают независимо от формы сертификата соответствия — традиционной (т. е. человекочитаемой) или кодированной, поэтому решения должны быть применимы для обоих сценариев.

3. Выдающий орган и юрисдикционная значимость

30. Необходимо определить, в рамках какого органа действует или действовало в момент выдачи сертификата лицо, ответственное за его выдачу. Разрешения, выдаваемые органам ИИС, как правило, распространяются на определенные виды продукции и стандарты оценки, что усложняет процесс валидации. Сертификат соответствия, выданный без опоры на официальный орган, может оказаться бесполезным с точки зрения удовлетворения требований рынка или запросов потребителей. Несмотря на существование глобальных механизмов взаимного признания деятельности по оценке соответствия, ситуация не всегда очевидна.

31. Существующие проблемы можно обобщить следующим образом:

- поддельные или измененные сертификаты соответствия;
- действительные сертификаты соответствия прилагаются к товарам, к которым они не относятся (включая повторное использование сертификатов охвата ими большего количества товаров, чем было предусмотрено, или других моделей в товарной группе);
- отметки товарной сертификации наносятся на продукцию без разрешения (включая подмену аутентичной продукции подделками);
- сертификаты соответствия представляются в условиях, когда полномочия выдавшего их органа сомнительны или искажены;
- сертификат соответствия предполагает целевое использование, отличное о того, для которого предназначалась продаваемая продукция; и
- продолжение использования ранее действовавших сертификатов или отметок, несмотря последующее вступление в силу ограничений на их использование.

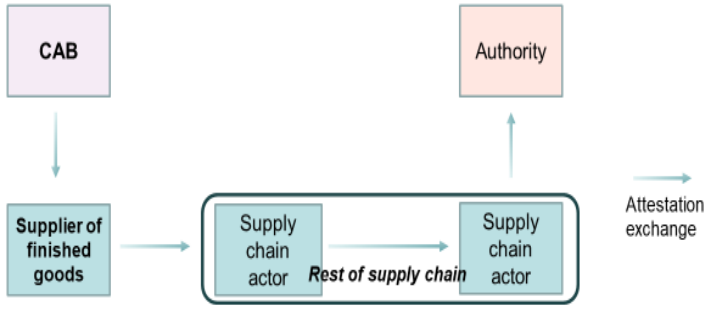
Вывод 1: Необходимо увязывать сертификаты соответствия с физической продукцией и контролировать процесс пересмотра и статус выдавшего органа.

D. Процессы обмена сертификатами соответствия

32. За пределами сообщества, занимающегося оценкой соответствия, процессы, в рамках которых происходит обмен сертификатами соответствия, в целом не очень хорошо понятны. Сертификат соответствия, как правило, первоначально предоставляется структуре, которая заказала проведение оценки соответствия (обычно это производитель или импортер продукции). Однако после выдачи сертификата порядок обмена им между участниками цепочки поставок сильно различается в зависимости от типа сертификата, вида продукции и юрисдикции. Ниже в упрощенном виде описаны и изображены различные существующие процессы (примеры 1–5).

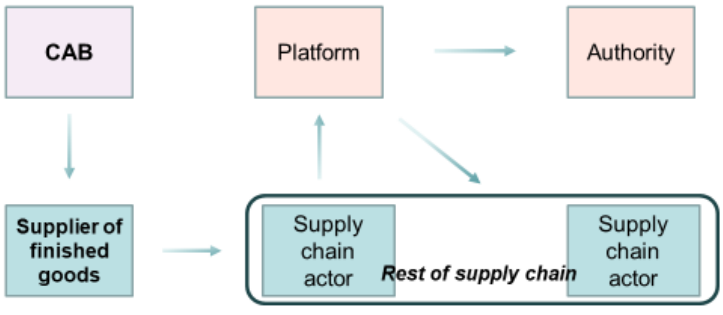
Пример 1

Получатель сертификата соответствия непосредственно направляет его (или предоставляет иным образом) покупателям или пользователям продукции, которые в свою очередь могут предоставлять информацию другим участникам цепочки поставок. Установление связи с физическими товарами обычно предполагает ручную проверку данных (как правило, путем сравнения таких параметров, как тип модели или номер партии). Подобная схема обмена характерна для таких категорий товаров, как строительные материалы, в которых участие государства не столь важно, как в некоторых областях, связанных с продуктами питания и здравоохранением.



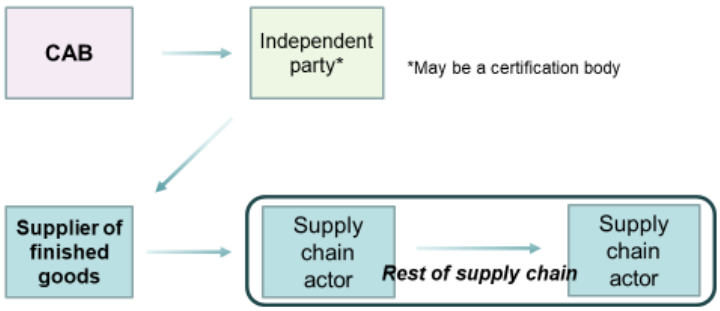
Пример 2

Получатель сертификата соответствия (или последующий участник цепочки поставок) вводит сертификат или ключевую информацию из него в платформу обмена данными и подтверждает все связи с товарами, к которым сертификат, как считается, применим (с дополнительной проверкой или надзором, или без них), как, например, в некоторых системах таможенного оформления по принципу «одного окна».



Пример 3

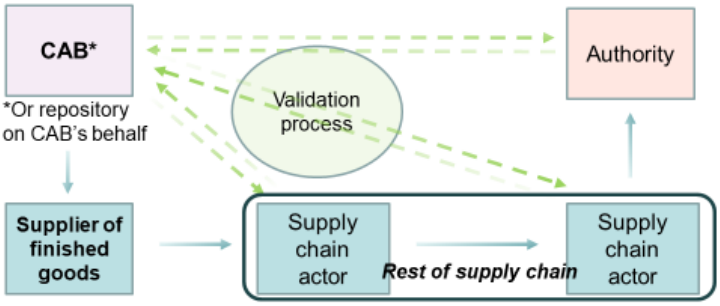
Независимая сторона (это может быть регулирующий орган или сертификатор продукции) утверждает конкретные ООС для предоставления информации о соответствии собирающей их структуре. Примеры применения этой модели можно увидеть как в регулируемом (например, тестирование импортируемых продуктов питания), так и в нерегулируемом пространстве (например, отраслевые программы одобрения продукции с привлечением субподрядчиков).



Пример 4

Обеспечение верификации в источнике выдаваемого ООС сертификата с помощью процессов, которые могут включать ручную онлайн-проверку или цифровую подпись с использованием шифрования с открытым/закрытым ключом. Это стало реакцией ООС, стремящихся защитить своих клиентов от мошеннического изменения выданных сертификатов. Хотя технологии не описаны, в докладе Совета по ИИК указывается ряд верификационных баз данных, созданных крупнейшими ООС[3].

Еще одним важным событием стало недавнее распространение сторонних сервисов цифровой подписи, позволяющих эмитентам документов, таким как ООС, внедрять их без особых капитальных вложений. Разновидностью такого подхода является предоставление уполномоченным органом платформы для валидации от имени ООС, такой как портал индийского Национального совета по аккредитации испытательных и калибровочных лабораторий (НАБЛ), предлагаемый от имени аккредитованных им испытательных и калибровочных лабораторий, или платформа «CertSearch» Международного форума по аккредитации, предоставляемая сертификаторам управленческих систем во всем мире.

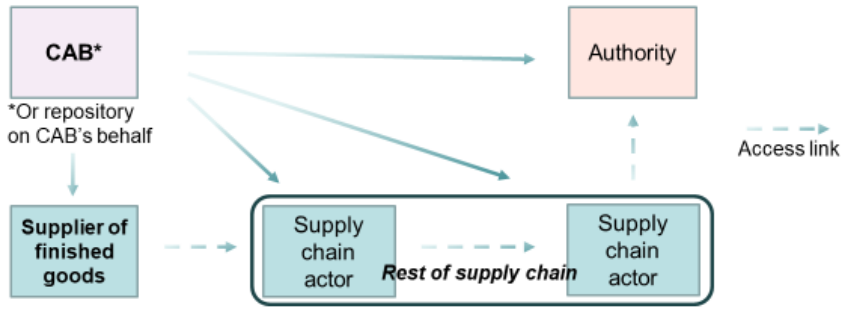


[3] Там же, TIC Council, page 12.

Пример 5

Хотя в настоящее время этот путь не является общепринятым, некоторые ООС, управляющие базами данных для верификации [предыдущая ссылка], выпускают штрих-коды, содержащие веб-адрес, по которому соответствующий сертификат соответствия может быть просмотрен любым пользователем, и это означает, что обмен самим сертификатом больше не требуется, при условии что штрих-код (или другая ссылка) передается участниками цепочки поставок.

Определенные особенности этого пути представляются ценными с точки зрения некоторых идей, рассматриваемых в данном документе, и его, возможно, легче адаптировать к чисто цифровым процессам в будущем, о чем кратко говорится в разделе C главы IV.



33. Важно понимать, что реальная цепочка поставок продукции обычно включает перерабатывающие и сборочные операции и состоит из сложной сети участников, в которую, как правило, входит многие ООС. Настоящие цепочки поставок, как правило, включают в себя комбинацию описанных выше процессов, а возможно, и все эти процессы одновременно.

34. Эта сложность, присущая процессу обмена, затрудняет моделирование потока данных в цепочке поставок и является препятствием для достижения совместимости систем обмена внутри цепочки поставок и тем более между различными цепочками поставок. Из приведенных примеров можно сделать вывод, что существующие процессы проверки и валидации данных для подтверждения соответствия вращаются вокруг ООС (или других сторон, действующих от их имени). Эта центральная роль ООС в проверке данных имеет значение для последующих разделов данного документа, где рассматривается вопрос о привязке сертификатов соответствия к физической поставке продукции.

35. Для полноты картины важно также признать, что существуют контрпримеры, в которых происходящий обмен сертификатами соответствия может не иметь решающего значения для установления соответствия продукции.

1. Отсутствие оценки соответствия

36. В некоторых нормативных системах существуют примеры, когда подлинность или эксплуатационные характеристики продукции могут быть установлены в рамках нормативной системы без применения оценки соответствия. Это может относиться к инновационной продукции, для которой не существует установленного стандарта, например, к продукции, отражающей результат инженерного решения для конкретного строительного объекта. В этих обстоятельствах, скорее всего, потребуется сертификат для подтверждения соответствия регуляторным требованиям, но не того типа, о котором идет речь в данном документе.

2. Подтверждение соответствия в рамках юрисдикции через законодательный процесс

37. В некоторых законодательных системах для некоторых видов продукции отменено требование дальнейшего обмена выходными данными ООС в цепочке поставок после определенного момента, когда регулирующий или иной орган берет на себя контроль соответствия продукции. Примерами такой законодательной системы являются некоторые государственные схемы товарной сертификации, сертификации компетентным органом перерабатывающих предприятий (часто связанных с пищевыми продуктами) или процессы санитарной и фитосанитарной сертификации. Даже в таких случаях передача данных о соответствии в различных точках цепочки поставок до установления законодательного контроля может рассматриваться как актуальная для данного документа. Европейский знак «CE» является одним из примеров государственной системы сертификации продукции, когда необходимость в доступе к соответствующим данным о соответствии может иметь значение только для целей экспорта (для удовлетворения требований неевропейского рынка). Тем не менее даже на европейском рынке продукция, подлежащая сертификации «CE», может потребовать оценки соответствия по различным атрибутам (например, «ESG» (экология, социальная политика и корпоративное управление)), которые остаются актуальными для рассматриваемых в данном документе вопросов.

Вывод 2: Отсутствие каких-либо согласованных процессов обмена сертификатами соответствия является препятствием для интероперабельности.

E. Правовые аспекты трансграничного обмена

38. Нормативно-правовой контекст выдачи сертификатов соответствия и обмена ими определяется национальным, региональным и международным законодательством, стандартами и передовым промышленным опытом. Применительно к трансграничному обмену сертификатами можно выделить три важных аспекта:

- совокупность норм регулирования, содержащихся в правилах Всемирной торговой организации (ВТО), региональных или двусторонних соглашениях о свободной торговле (ССТ) или национальных законах, а также международных стандартов и примеров передовой практики, которые широко используются предприятиями;
- взаимное переплетение на практике законов и нормативных актов в нескольких правовых категориях (например, аутентификация, защита прав потребителей и безопасность данных); и
- наборы вертикальных нормативных документов, разработанных государством для бизнеса, и горизонтальных договорных соглашений между коммерческими предприятиями, которые в совокупности могут обеспечить доверие к процессу обмена сертификатами соответствия и поддержку его прослеживаемости и целостности.

39. Соглашение ВТО по техническим барьерам в торговле (ТБТ) устанавливает основополагающие принципы, применимые к процедурам оценки соответствия, с тем чтобы не создавать ненужных препятствий для торговли[4], соблюдать конфиденциальность информации о продукции, происходящей из иностранного государства, так же как информации об отечественной продукции, и защищать законные коммерческие интересы[5].

40. Принимая к сведению рекомендации, содержащиеся в вышеуказанных принципах, следует отметить, что существующие системы обмена сертификатами

[4] Соглашение ВТО по ТБТ 3-е издание, статья 5.1.2.

[5] Там же, ВТО, статья 5.2.4.

соответствия по-прежнему отличаются правовой неопределенностью. Например, могут возникнуть споры по поводу наличия или статуса выданных сертификатов соответствии:

- в связи с риском раскрытия информации, составляющей коммерческую тайну (например, идентификатора поставщиков), не вся необходимая информация может быть своевременно предоставлена сторонами, что может привести к принятию неверных решений или возникновению споров;
- вне определенных законодательных рамок статус информации из сертификатов соответствия, как правило, подлежит пересмотру, при этом отсутствуют признанные процессы уведомления участников цепочки поставок об изменениях и четкая юридическая ответственность за распространение такой информации; и
- возможна также коллизия норм законодательства, основанная на локализации обработки данных сертификатов соответствия.

41. В тех случаях, когда возникают споры относительно наличия, действительности, актуальности или статуса сертификатов соответствия, правоприменение может быть затруднено по следующим причинам:

- последовательных характер контрактов купли-продажи в цепочке поставок означает, что конечному потребителю, желающему получить судебную компенсацию за некачественную продукцию, может потребоваться ряд последовательных судебных разбирательств, которые могут отбить у пострадавшей стороны желание добиваться возмещения ущерба;
- такая атмосфера размытой ответственности может также способствовать незаконному изменению данных, что чревато формированием ложных связей между данными оценки соответствия и физической продукцией, а также недобросовестным заявлениям о полномочиях, на основании которых были выданы сертификаты соответствия. В некоторых странах в отношении некоторых видов продукции существует законодательная база, возлагающая бремя ответственности на каждого субъекта, удостоверяющего подлинность данных о продукции и передающего данные, влияющие на соответствие продукции установленным требованиям, однако такие механизмы не получили широкого распространения; и
- правоприменение может быть осложнено проблемами, возникающими в связи с коллизией законов различных юрисдикций.

42. Для цифрового обмена сертификатами соответствия необходима надежная структура, которая устраняла бы все вышеперечисленные юридические сложности. Цифровые процессы потенциально способны смягчить многие из этих факторов неопределенности за счет обмена данными, которые достоверно связаны как с продуктом, так и с органом, выдавшим сертификат.

Вывод 3: Обмен бумажными сертификатами соответствия по своей природе сопряжен с юридическими двусмысленностями и лазейками, которые могут усугубить другие недостатки процесса.

F. Правовые аспекты, применимые к трансграничной цифровой интероперабильности

43. Меры по обеспечению обмена сертификатами соответствия продукции или доступа к ним должны выходить за рамки создания цифрового изображения документа, который проходит электронную аутентификацию, подписывается электронной подписью и распространяется в электронном виде с использованием признанного формата и технологии. Они должны обеспечить достижение всех следующих результатов:

- установлению связи между сертификатами соответствия и физическим товаром;
- проверке полномочий и статуса эмитентов сертификатов; и
- постоянную возможность проверки по всей цепочке поставок того, что сертификат является подлинным и отражает текущий статус проблемы.

44. Достижение этих результатов в условиях цифровизации сопряжено с законодательными проблемами, по крайней мере, в четырех областях:

- сотрудничества по процедурам оценки соответствия в цифровой торговле;
- цифровых правовых идентификаторов;
- безопасности и целостности данных; и
- нахождения баланса между прозрачностью и конфиденциальностью информации.

45. Существующие трансграничные положения о процедурах оценки соответствия, как правило, не учитывают контекст цифровой торговли. Исключение составляет недавно заключенное соглашение о партнерстве в области цифровой экономики (далее — СПЦЭ), подписанное Сингапуром, Чили и Новой Зеландией 12 июня 2020 года и вступившее в силу для Новой Зеландии и Сингапура 7 января 2021 года; Сингапурско-австралийское соглашение о цифровой экономике; и Сингапурско-южнокорейское соглашение о цифровой экономике. Эти положения заслуживают одобрения, однако они носят двусторонний характер и не могут обеспечить взаимосвязь и взаимодействие между несколькими странами в глобальной цепочке поставок.

46. Идентификаторы субъектов являются важным элементом при обсуждении обмена сертификатами соответствия, поскольку необходимо проверять идентичность коммерческих сторон и ООС из разных стран. Однако лишь немногие международные торговые соглашения предусматривают положения о согласованной правовой идентичности. СПЦЭ, Сингапурско-австралийское соглашение о партнерстве в области цифровой экономики и Сингапурско-южнокорейское соглашение о цифровом партнерстве являются одними из первых международных соглашений, в которых поднимается этот вопрос. Все они содержат аналогичное положение, согласно которому стороны соглашений должны содействовать совместимости своих режимов использования цифровых идентификаторов путем обеспечения технической совместимости, единых стандартов или признания нормативно-правовой базы или регуляторного воздействия друг друга (например, ст. 7.1 СПЦЭ, ст. 29 Сингапурско-австралийского соглашения о цифровой экономике, ст. 14.30 Сингапурско-южнокорейского соглашения о партнерстве в области цифровой экономики). Однако эти положения не могут принести выгоды коммерческим организациям, находящимся за пределами этих государств-членов.

47. Кибербезопасность и защита данных также являются ключевыми моментами в обеспечении безопасности и целостности данных сертификатов соответствия в будущих системах цифрового обмена. В ведущих соглашениях о ЗСТ, такие как Всеобъемлющее и прогрессивное соглашение о Транстихоокеанском партнерстве (ВТПТП), Соглашение между США, Мексикой и Канадой и Соглашение Ассоциации государств Юго-Восточной Азии (АСЕАН) об электронной торговле, признается, что угрозы кибербезопасности подрывают доверие к глобальной цепочке поставок [например, статья 14.16 ВТПТП, статья 19.15 Соглашения между США, Мексикой и Канадой и статья 8 Соглашения АСЕАН об электронной торговле]. Однако конкретные меры, относящиеся к цифровому обмену сертификатами соответствия, на данный момент не определены.

48. Наконец, обмен сертификатами соответствия в глобальной цепочке поставок также требует тщательного соблюдения баланса между требованиями прозрачности и защиты конфиденциальности. Конфиденциальность должна быть гарантирована как производителям, так и потребителям. Последние могут использовать свои персональные устройства для сканирования QR-кода на упаковке товара или для

получения данных о соответствии на сайте ООС. Инструменты защиты конфиденциальности в цифровом контексте разрабатывались на различных международных форумах, в том числе в рамках Организации экономического сотрудничества и развития (ОЭСР) (Руководство по защите конфиденциальности), ЕС (Общий регламент по защите данных, ОРЗД) и Азиатско-Тихоокеанского экономического сотрудничества (АТЭС) (Рамочная программа защиты конфиденциальности). Кроме того, соответствующие положения можно найти и в других документах более общего характера, например, в документе «Перечень правил, стандартов и принципов цифровой торговли» ОЭСР (Digital Trade Inventory — Rules, Standards and Principles, page 19) и в статье 4.2.3 СПЦЭ. Однако эти документы в основном содержат принципы и положения о максимальных усилиях, а детальные правила защиты конфиденциальности оставлены на усмотрение национальных законодательств, где могут существовать значительные несоответствия.

Вывод 4: В существующей правовой базе трансграничного обмена данными имеются пробелы. Поэтому любая работа по созданию систем обмена цифровыми сертификатами соответствия должна проводиться с учетом того, что среда точно не определена и может измениться, и это может повлиять на будущий выбор идентификаторов и конкретных цифровых технологий.

IV. Технология обмена информацией из сертификатов

49. Чтобы сделать необходимую информацию из сертификатов доступной для различных участников цепочки поставок, потребуются технологические структурные элементы, отвечающие различным требованиям в поисках общего решения. В последующих разделах этой главы рассматриваются необходимые структурные элементы, выявленные в ходе работы над данным документом.

A. Цифровые идентификаторы

1. Минимальная информация о данных

50. Сертификаты соответствия содержат большое количество элементов данных, которые также могут существенно различаться в зависимости от типа сертификата. В задачи данного доклада не входит гармонизация сертификатов или их элементов данных. В данном случае речь идет о том, что необходимо определить ограниченный набор элементов данных, которые являются основополагающими для обмена такими сертификатами:

- идентификаторы для конкретного изделия/модели;
- идентификаторы (если применимо) для партии, торговой единицы или отдельного изделия, требующего оценки соответствия;
- идентификатор для каждого отдельного сертификата соответствия;
- статус пересмотра сертификата;
- идентификатор выдающей стороны (т. е. ООС); и
- наименование стороны (если применимо), от имени которой действует выдающая сертификат сторона (например, орган по аккредитации).

51. Существующие модели справочных данных, такие как Справочная модель данных СЕФАКТ ООН, Модель данных Всемирной таможенной организации, содержат гармонизированные элементы данных, включая идентификаторы продукции, дистрибьюторов, документов и т. д. Необходимо провести углубленный анализ, чтобы определить, какие идентификаторы из этих моделей применимы для сектора ИИС, и выявить недостатки в этих моделях данных. Ожидается, что некоторые элементы данных потребуют большей детализации для использования в секторе ИИС.

52. Хотя в данном документе приводятся примеры подходящих типов идентификаторов для товаров и сертификатов, они скорее иллюстрируют общие принципы, чем предписывают их. Примеры конкретных типов идентификаторов для сторон (таких, как ООС и органы аккредитации) в данном документе не приводятся, однако существует несколько общепризнанных альтернативных вариантов, которые могут быть использованы, и выбор предпочтительного варианта выходит за рамки данного документа.

53. В следующих разделах рассматриваются несколько классов идентификаторов, которые могут стать подходящими моделями для достижения верифицируемого цифрового обмена данными о соответствии, связанного также с физическим потоком продукции.

2. Использование идентификаторов для увязывания данных

54. Первый вопрос, на который следует обратить внимание — это необходимость идентификации как сертификата, так и физического товара, к которому относится сертификат относится.

55. При сертификации товара идентификатор продукции обычно относится к производимой продукции в целом, но в случае с результатами испытаний или инспекций может потребоваться идентификатор продукции, относящейся к отдельной партии (или даже логистический идентификатор, если это становится актуальным, например, для определения места проведения испытаний груза). Существуют глобальные схемы идентификации продукции[6], которые варьируются от идентификаторов общих товарных категорий, таких как Гармонизированная система, разработанная для классификации товаров для таможенного оформления[7], до идентификаторов, однозначно идентифицирующих конкретные товарные позиции отдельных производителей и даже отдельные партии или лоты данного товара, наиболее распространенным примером которых является Международный идентификационный номер товара (GTIN), соответствующий стандарту ИСО/МЭК 15459-6[8]. Физическое нанесение уникального идентификатора товара на упаковку и/или сам товар является стандартной практикой для розничных товаров (обычно включают GTIN). Имеются дополнительные логистические идентификаторы[9], позволяющие однозначно идентифицировать логистические единицы (например, транспортные контейнеры), грузы и даже отдельные товарные позиции, и все они основаны на стандартах серии ИСО 15459. В тех случаях, когда сертификат соответствия связан с отгрузкой, использование стандартной отгрузочной маркировки[10], описанной в Рекомендации ЕЭК № 18, может стать способом дополнительной увязки.

56. Существуют также глобальные схемы идентификации организационных единиц (основанные на стандартах ИСО), которые могут быть полезными, когда требуется указать отдельного производителя, возможно, в сочетании с конкретной производственной площадкой, которая может быть идентифицирована с помощью глобальных схем, основанных на стандартах ИСО. В случае сертификации систем подтверждения качества, безопасности и охраны окружающей среды связь между сертификатом и отдельным товаром имеет смысл, но является косвенной, поскольку такие сертификаты распространяются не непосредственно на товар, а на производителя (в частности, на сертифицированные производственные площадки). Поэтому, хотя в таких сертификатах не должно быть прямых ссылок на идентификаторы продукции, ссылки в сертификате соответствия на конкретные места расположения объектов должны, в принципе, обеспечивать возможность увязки

[6] E Ganne and H Nuygen, Standards Toolkit for Cross-border Paperless Trade, Joint WTO/ICC publication, March 2022.

[7] https://www.wcoomd.org/en/topics/nomenclature/overview/what-is-the-harmonized-system.aspx.

[8] ИСО/МЭК 15459-6:2014 «Информационные технологии. Технологии автоматической идентификации и сбора данных — Уникальная идентификация — Часть 6: Группы».

[9] https://www.gs1.org/sites/default/files/docs/gs1_iso_brochure.pdf.

[10] https://unece.org/fileadmin/DAM/cefact/recommendations/rec18/rec18_ecetrd271e.pdf.

данных с физическими поставками продукции (возможно, с использованием таких концепций, как концепция связанных данных).

57. Существует также требование идентификации самой сертификации, поскольку связь данных с физическими товарами должна быть увязана с конкретными сертификатами, необходимыми для обоснования любого утверждения о товаре. Хотя все ООС, как правило, придерживаются принципа уникальной идентификации выданных сертификатов, они почти всегда опираются на внутренние идентификаторы, которые в свою очередь требуют того или иного индекса или реестра для однозначного установления связи между сертификатом и физическим товаром. Это может стать отправной точкой для определения бизнес-процессов, которые позволяют связать сертификаты соответствия с физической поставкой и которые могут быть доступны любому участнику цепочки поставок.

58. Важно признать, что в настоящее время уже существует очень много различных сертификатов. Кроме того, существующие базы данных и услуги, предлагаемые владельцами схем или органами сертификации, не начнут сразу опираться на единую глобальную схему уникальных идентификаторов. Поэтому глобальные схемы идентификации и существующие схемы идентификации будут продолжать сосуществовать, но им необходимо перейти от «аналоговых» схем к цифровым. В то же время важно ориентироваться на глобальные идентификаторы, используемые торговыми кругами, как частными, так и государственными, чтобы избегать дублирования. Поэтому в данном докладе рекомендуется использовать идентификаторы, основанные на глобальных стандартах данных, таких как стандарты ИСО или Организации Объединенных Наций. При этом существует возможность использовать глобальные идентификаторы в первую очередь для обмена информацией между системами, в то время как существующие идентификаторы могут продолжать использоваться людьми в качестве «интуитивных» идентификаторов. Кроме того, существует возможность использовать децентрализованную архитектуру для получения доступа к таким объектам, как верифицируемые учетные данные (ВУД), для облегчения цифрового взаимодействия между различными платформами, при условии что будет достигнуто общее понимание сущностей и идентификаторов (дополнительную информацию можно почерпнуть из Белой книги СЕФАКТ ООН)[11].

59. Различные заинтересованные стороны будут иметь разные ожидания относительно того, какие данные могут им понадобиться в отношении того или иного товара. Хотя для некоторых видов сертификатов (как правило, тех, которые участники цепочки поставок могут получить в свободном доступе) это не является проблемой, недостатки могут проявиться в тех случаях, когда доступ к содержанию сертификатов блокируется для защиты части содержания по коммерческим соображениям. Более подробно эта проблема рассматривается в разделе D главы IV.

Вывод 5: Поскольку среди важнейших элементов данных, связанных с обменом сертификатами соответствия, преобладают идентификаторы, необходима дальнейшая работа по анализу моделей данных СЕФАКТ/ООН, имеющих потенциальное отношение к представляющим интерес идентификаторам. Кроме того, отмечается, что для формирования связей, необходимых для решения поставленной задачи, уже существуют отлаженные системы, предусматривающие в том числе использование уникальных глобальных идентификаторов.

B. Управление жизненным циклом данных о соответствии

60. Выданный однажды сертификат соответствия может менять статус в течение своего жизненного цикла в зависимости от вида сертификата. Оцифровка информации о статусе в контексте подтверждения соответствия требует дальнейшего изучения, поскольку существующие определения статусов сертификатов, содержащиеся в

[11] https://unece.org/sites/default/files/2022-06/010_Verifiable-Credentials-CBT.pdf.

документе СЕФАКТ ООН e-Cert BRS, глава V, раздел C.3, которые отражают трансграничные операции, связанные с экспортными сертификатами, не учитывают процессы, характерные для сектора ИИС. Как правило, протоколы испытаний, контроля и калибровки остаются действительными, если они не отозваны выдавшим их органом (например, в результате замены для исправления ранее допущенной ошибки). Другие виды сертификатов, такие как товарные сертификаты, могут иметь определенный срок действия (который может быть продлен), хотя такие сертификаты также могут быть приостановлены или отозваны выдавшим их органом (если соответствие больше не гарантируется) или пересмотрены, если соответствующая продукция изменилась и требуется проведение повторной оценки в той или иной форме. Однако правила отдельных схем могут определять конкретные статусы, применимые к сертификатам, выпущенным в рамках данной схемы, что еще больше осложняет ситуацию.

61. Поэтому в будущем предлагается разработать общий набор статусов, применимых к сертификатам соответствия, опираясь, насколько это возможно, на существующие определения СЕФАКТ ООН и предусматривая возможность признания эквивалентных терминов для обозначения того или иного статуса (например, аннулированный/отозванный/отмененный или пересмотренный/измененный или выданный/текущий), чтобы учесть различия в языке разных схем.

62. В любом случае актуальная информация о статусе сертификата соответствия является неотъемлемым аспектом его действительности и поэтому должна быть доступна органам надзора и регулирования рынка, таможенным органам, импортерам, оптовым продавцам и потребителям. Необходимая степень прозрачности может зависеть от требований стороны, запрашивающей оценку соответствия, или применимых правил схемы (где это уместно), а также в зависимости от последствий изменения статуса, от требований законодательства.

63. В целом, требования к аккредитации обязывают ООС информировать сторону, которой был выдан сертификат (иногда именуемую держателем сертификата), о том, что сертификат более не действителен, и могут позволить органу самостоятельно выбрать подходящий канал связи. Однако в зависимости от типа связи эта обновленная информация может не распространяться по цепочке поставок и не достигать всех заинтересованных сторон, таких как регулирующие органы и конечные потребители.

64. Выдающие сертификаты органы используют разные подходы, позволяющие аутентифицировать их сертификаты, многие из которых включают процессы шифрования на основе открытых или закрытых ключей. Эти процессы, известные как «цифровые подписи», обеспечивают аутентификацию на момент времени, когда был выдан сертификат соответствия, и представляют собой средство защиты от изменений. Сама по себе цифровая подпись представляет собой математическую конструкцию (алгоритм хеширования), которая продолжает действовать до тех пор, пока не будет отозван «цифровой сертификат», имеющийся у подписавшей стороны, однако они не очень точно отражают изменения в статусе сертификата. Существуют и другие примеры, когда органы, выдающие сертификаты, владельцы сертификационных схем или другие организации предоставляют информацию о текущем статусе сертификации либо через центральную базу данных, либо через центральный список, например список отозванных сертификатов.

65. Альтернативным вариантом является обмен ссылками на сертификат, а не самим сертификатом, и это означает, что в каждом случае доступ предоставляется непосредственно к действительной версии. Использование связанных данных или преобразователей цифровых ссылок представляет собой пример такого подхода, который может быть адаптирован к более разнообразным ситуациям, включая возможность отсылки к различной сопутствующей информации в дополнение к самому сертификату. Преобразователи цифровых ссылок могут использоваться в качестве «индекса», и доступ к ним может осуществляться исключительно или практически исключительно через уникальный глобальный идентификатор элемента/субъекта, который активирует ссылку/ссылку на онлайновый сервис, содержащий связанные данные по этому идентификатору. Для сертификатов соответствия данные, хранящиеся в преобразователе цифровых ссылок, могут быть

ограничены уникальными идентификаторами сертификата и URL (плюс идентификатор, используемый целевым онлайн-сервисом). Некоторые децентрализованные методы, такие как упомянутые в разделе A.2 главы IV верифицируемые учетные данные, которые могут обмениваться и храниться в «цифровых кошельках», могут предложить аналогичные преимущества, обеспечивая при этом дополнительный контроль и безопасность.

66. Независимо от этого, одним из важных принципов при управлении жизненным циклом данных о соответствии является признание того, что выдавшая сертификат сторона сохраняет все права на этот сертификат, с тем чтобы обеспечить определенность в отношении статуса (например, отзыв, изменение, истечение срока действия) сертификата в течение всего срока его действия.

Вывод 6: Регулирование статуса пересмотра является более сложной задачей, чем может показаться на первый взгляд, и для ее решения используются различные несовместимые подходы. Важным моментом является то, что ООС или стороны (например, владельцы схем), действующие от их имени при предоставлении доступа к данным о соответствии, занимают центральное место в этом процессе и что обмен ссылками на сертификаты может быть более эффективным, чем обмен самими сертификатами.

C. Способы получения доступа к данным о соответствии на основе физических идентификаторов

1. Физические идентификаторы

67. Существует целый ряд процессов, с помощью которых на физических объектах (например, изделиях или документах) могут быть размещены идентификаторы, считываемые как человеком, так и машиной. Преобладают две технологии: штрих-коды и радиочастотная идентификация. Более непосредственное отношение к данному документу имеют штрих-коды, среди которых можно выделить два основных вида: линейные и двумерные (2D) штрих-коды. Одним из преимуществ двумерных штрих-кодов (семейство, включающее широко используемый QR-код) является то, что они содержат достаточно места для отображения множества различных элементов данных, которые могут быть считаны и интерпретированы при одном сканировании штрих-кода с использованием глобальных стандартов данных, описанных, например в руководстве GS1 Scan4Transport[12]. Кроме того, возможности двумерных штрих-кодов позволяют заинтересованным сторонам включать в них унифицированный идентификатор ресурса (URI), создавая цифровую ссылку на физический объект, которую иногда называют «цифровым двойником» этого объекта.

68. Двухмерные штрихкоды, размещаемые на продукции, могут содержать ссылку на собственный веб-сайт производителя; в то же время в таблице ниже показано, как штрихкод может также кодировать веб-сайт сертификата соответствия с указанием на центральную хостинговую организацию или без нее.

Штрих-код справа содержит кодированную ссылку/URI

https://resolver-dv1.gs1.org/253/871423175000060012051.

Значение, следующее за «253/», указывает на GS1 GDTI (8714231750000600120 51) — уникальный глобальный идентификатор. Первая часть адреса указывает на внешний «индекс», в котором эмитент может зарегистрировать факт выдачи аттестата, а также целевой URI, где размещен сертификат. В рамках такого «индекса» могут быть созданы дополнительные ссылки на другую информацию (см. главу IV, раздел C.2).

[12] https://www.gs1.org/industries/transport-and-logistics/scan4transport.

В качестве альтернативы эмитент может просто закодировать прямые ссылки на свой собственный веб-индекс сертификатов. Используемые идентификаторы могут использовать глобальные системы идентификации, например описанные в стандарте ИСО/МЭК 15418[13], или быть защищенными правами собственности (в последнем случае они могут быть основаны на синтаксисе и семантике, описанных в стандарте ИСО 8000-115)[14].

2. Связь сертификата соответствия с товаром и разрешительной документацией

69. Существует множество примеров[15] URI-ссылок в сертификатах соответствия на сайт органа, выдавшего сертификат. Однако доступная информация, как правило, не распространяется на сопутствующие товары (т. е. не выходит за рамки сведений о соответствии), и доступ к сопутствующим данным с помощью таких инструментов представляет собой достаточно новую область исследований. По-видимому, нет причин, по которым испытательные лаборатории, например, не могли бы включать наносимые на продукцию идентификационные штрих-коды в выдаваемые сертификаты, и по которым органы сертификации продукции не могли бы аналогичным образом указывать идентификационные коды продукции вместе со стандартами, на соответствие которым она была сертифицирована. Действительно, существуют примеры[16] кодирования идентификатора, соответствующего стандарту ИСО 15459 (в частности, GTDI), в выпускаемых протоколах испытаний для установления цифровой связи с конкретной товарной партией продукции, являющейся предметом протокола испытаний.

70. Данный подход также указывает на то, что пользователь может провести независимую оценку компетенции (где это применимо) органа, выдающего сертификат, прецеденты чего уже существуют. В настоящее время индийский орган по аккредитации лабораторий НАБЛ продвигает включение QR-кода во все отчеты калибровочных и испытательных лабораторий со ссылкой на соответствующую информацию об аккредитации, размещенную на сайте НАБЛ. Некоторые национальные органы также активно развивают процессы, связанные с использованием криптографически проверяемых цифровых подписей, отсылающих к назначенному органу по аккредитации.

71. Расширяя общую концепцию, можно сказать, что в условиях доступа к сертификатам (а не обмена ими) пользователь, желающий просмотреть/проверить сертификат, будет обращаться к приложению, управляемому органом-эмитентом или

[13] ИСО/МЭК 15418: 2016 Информационные технологии — Технологии автоматической идентификации и сбора данных — Идентификаторы применения GS1 и идентификаторы данных ASC MH10 и их ведение.

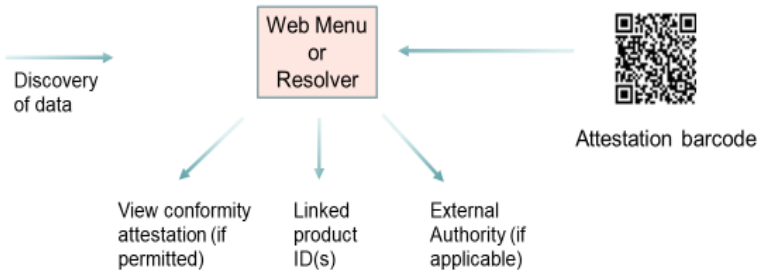
[14] ИСО 8000-115:2018 Качество данных — Часть 115 — Основные данные. Обмен идентификаторами качества. Синтаксические, семантические требования и требования к разрешению.

[15] Там же, TIC Council, page 12.

[16] Digitalisation of Product Certificates, Claims and Credentials, NATA/JAS-ANZ/GS1 joint publication, October 2022, page 21.

другим органом, что даст возможность получить дополнительные ссылки на полномочия/компетенцию этого органа-эмитента.

Рис. 3



72. Как показано выше, веб-меню или преобразователь может функционировать в рамках как ООС, так и платформы поставок третьей стороны или даже национального реестра. Для сертификатов, находящихся в открытом доступе, предоставлять нужно не сам сертификат, а лишь штрих-код (или другой тип ссылки).

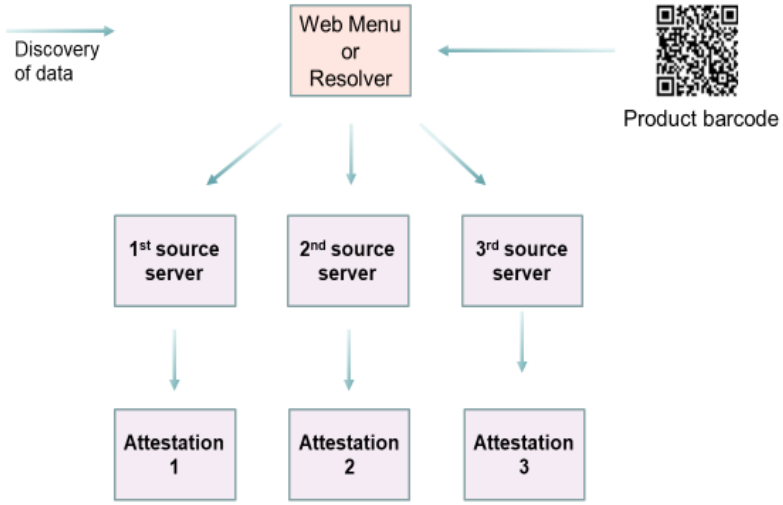
3. Связь сертификата соответствия с данными о продукции

73. Получение доступа к сертификатам соответствия (в их источнике) по идентификатору товара представляет собой более сложную задачу, но является логическим продолжением идей, изложенных ранее в данном документе. Это также согласуется с действующим и разрабатываемым в некоторых юрисдикциях законодательством, направленным на повышение прозрачности связей между маркировкой продукции и информацией, лежащей в основе оценки соответствия.

74. Цель предоставления такого доступа к данным заключается в том, чтобы дать участникам цепочки поставок и потребителям больше возможностей для проверки достоверности информации о товаре при его поставке, а также дать возможность специалистам определить характеристики товара на этапе его спецификации, чтобы убедиться в его пригодности для использования по назначению (что во многих случаях это также необходимо для выполнения нормативных требований). Возможность обеспечить цифровую связь между выбранным товаром и сопровождающим сертификатом соответствия позволяет наладить надежный процесс аутентификации. Это еще более важно в тех случаях, когда компоненты поставляются для установки в систему, что особенно осложняет их отслеживание.

75. URI, например веб-адреса, обычно наносятся на продукцию или ее упаковку для увязывания массивов информации, которые могут включать данные о соответствии, с продукцией. Такие URI, как правило, отсылают к сайту производителя, но без последующих отсылок к независимым источникам данных. Это осложняет независимую проверку данных и не позволяет решить проблему установления конкретной связи между полученными сертификатами и интересующей физической партией продукции.

Рис. 4



76. Как показано выше, веб-меню или преобразователь может функционировать в рамках как производителя, так и платформы поставок третьей стороны или даже национального реестра.

Вывод 7: Набор взаимодополняющих процессов, основанных на увязанных между собой данных, может быть выражен в общих терминах, используемых для решения поставленной задачи.

D. Определение уровней доступа к цифровой информации

77. В разделе A.1 главы IV рассматривается информация, минимально необходимая для установления некоторых ключевых связей с сертификатом соответствия с целью решения поставленной задачи. Потенциальные схемы доступа к данным, описанные в предыдущем разделе, были представлены с точки зрения обеспечения максимальной прозрачности данных для всех участников цепочки поставок. Однако в реальности не все сертификаты соответствия могут свободно распространяться таким образом, поскольку могут содержать защищенную коммерческую информацию, а существующие процессы обмена сертификатами не предусматривают такой функции.

78. Цифровизация открывает новые потенциальные возможности для учета этого аспекта. В заключительной части главы IV этот вопрос будет рассмотрен с точки зрения гармонизации с другими элементами, которые уже были изучены, при этом следует отметить, что полное рассмотрение столь сложной области выходит за рамки данного документа.

79. Минимально необходимая информация представляет собой набор данных, которые могут быть связаны с сертификатом в цифровом виде. Однако это не означает, что остальное содержание сертификата соответствия также должно свободно сообщаться. Существует много примеров цифровых запросов ограниченных для распространения данных. В транспортной сфере к ним относятся коносаменты на платформе eFBL ФИАТА[17], где для подтверждения подлинности выданного документа можно найти некоторые ограниченные данные, такие как дата выдачи, сторона, выдавшая документ, или статус выдачи. Таким же образом можно установить цифровую корреляцию между сертификатами соответствия и реальными процессами/

[17] https://www.efbl.fiata.org/efbl.

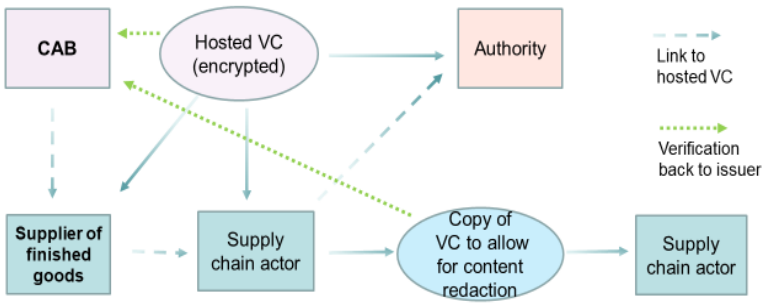
событиями, не раскрывая человекочитаемый сертификат. Но это только начало пути к полной цифровизации.

80. Хотя это и выходит за рамки данного документа, определение элементов данных, составляющих полное содержание сертификата соответствия, открывает возможность для обмена данными с произвольным уровнем дискриминации, опираясь на структуры выдачи разрешений, отражающих базовые протоколы кодирования данных. Полное цифровое кодирование существует для сертификатов калибровки по стандарту ИСО/МЭК 17025[18] и разрабатывается для оценки соответствия по стандарту ИСО/МЭК 17065[19] применительно к оборудованию для законодательной метрологии, а также в законодательно регулируемой области взрывозащиты. Технологической основой этих инициатив является язык Extensible Markup Language (XML).

81. Существуют и другие перспективные технологии, которые можно развивать на основе только что описанных достижений в цифровизации. К ним можно отнести возможность создания верифицируемых учетных данных (ВУЗ), кодирующих сертификаты, которые могут храниться централизованно (и доступ к которым можно получить по закрытой ссылке), но которые при необходимости могут быть скопированы и отредактированы, чтобы скрыть конфиденциальную информацию для последующих участников цепочки поставок, сохраняя при этом возможность криптографической проверки всеми сторонами на подлинность и актуальность. Это, вероятно, станет интересным направлением будущей деятельности, поскольку децентрализованные подходы могут предложить решение проблемы сокрытия чувствительной коммерческой информации без ухудшения процесса обмена.

82. Ниже приведена схема, показывающая один из возможных вариантов обмена с редактированием в будущем. Редактирование требуется не для всех сертификатов, но гибкость, позволяющая такое редактирование в случае необходимости, является ключевым фактором. Основная цель данной схемы — подчеркнуть структурное сходство с процессом, рассмотренным в качестве примера 5 в разделе D главы III, а также обратить внимание на расширенный функционал, которого можно добиться благодаря децентрализованному цифровому обмену.

Рис. 5



83. Идеи, изложенные в данном заключительном подразделе, посвященном технологии, показывают, что принятие идей, изложенных в документе (в частности, о центральной роли ООС или назначенного им органа в валидации сертификатов), может позволить в будущем внедрить гораздо более мощные инструменты, что в настоящее время не представляется возможным из-за фрагментации нынешнего процесса обмена сертификатами как внутри цепочек поставок, так и между различными цепочками поставок.

[18] Hackel, S. et al., The fundamental architecture of the DCC, Measurement: Sensors, Volume 18, 2021, 100354, doi: 10.1016/j.measen.2021.100354; наиболее актуальную информацию см. на сайте www.ptb.de/dcc.

[19] *NoBoMet project group 'Digital certificates'*, публикация ожидается.

Вывод 8: Несмотря на то, что для выборочного исключения конфиденциальных данных существует технология, она не может применяться последовательно в силу того, что процесс обмен сертификатами соответствия сегодня не отличается целостностью. Наделение ООС более важной ролью может способствовать более последовательному применению технологии с точки зрения процесса.

V. Выводы и последующие шаги

84. Анализ, проведенный в данном документе, позволяет сделать ряд выводов, касающихся в том числе существующих проблем и путей их решения. Они кратко изложены в этой заключительной главе, в которой также сформулированы некоторые принципы и перспективы реализации предложений.

A. Резюме

85. Проблемы, связанные с существующими системами обмена сертификатами соответствия в цепочках поставок, объясняются (глава III, раздел C) в основном отсутствием надежных связей (т. е. связи сертификатов с физической продукцией, с органом, выдавшим сертификат, и статусом пересмотра). Отсутствие сколь-либо согласованного механизма доступа к сертификатам соответствия (глава III, раздел D) или четко определенных вспомогательных правовых механизмов (глава III, раздел F) также рассматривается как препятствие для поиска системных и интероперабельных решений.

86. В разделе 4 рассматривается ряд идей, намечающих возможные пути решения поставленной задачи. Раздел A главы IV дает представление о том, как можно связать сертификаты соответствия с физической продукцией, используя существующие идентификаторы и широко применяемые технологии. Рассматривается возможность обмена ссылками на сертификаты, а не самими аттестатами (глава IV, раздел B), что наделяет ООС или назначенного им субъекта (например, владельца схемы или другой орган) центральной ролью как источника, так и проверяющего органа для сертификатов соответствия. Расширенная концепция (глава IV, раздел C) включает в себя потенциальную систему, предполагающую доступ к сертификатам соответствия (а не обмен ими), в том числе возможность цифровой привязки к сертификатам физических товаров, имеющих штрих-коды (или другие идентификаторы). Вопрос о защите данных, составляющих коммерческую тайну, которая может потребоваться для некоторых видов сертификатов, рассматривается в разделе D главы IV, где отмечается, что описанная ранее структура обмена может быть адаптирована и для решения этой проблемы с использованием существующих технологий.

87. Признается, что необходимо продолжать работу по изучению возможности применения технологий для обмена сертификатами (особенно в части выборочного редактирования чувствительной информации). В то же время потенциальная ценность для глобальных цепочек поставок требует дальнейшего изучения представленных концепций.

88. Поскольку использование идентификаторов является основополагающей концепцией данного документа, рекомендуется провести дальнейшую работу по определению применимых идентификаторов из соответствующих БМД ООН/СЕФАКТ (и выявить пробелы в этих моделях данных, поскольку предполагается, что для использования некоторых элементов данных в секторе ИИС требуется более детальная детализация). По мере возможности рекомендуется также использовать уникальные глобальные идентификаторы, чтобы упростить обмен данными между разными платформами. Разработку СТДО СЕФАКТ ООН рекомендуется сделать приоритетом, чтобы внести большую ясность в эти концепции на межправительственном уровне.

B. Принципы

89. Было определено несколько принципов, которые могут поддержать будущие усилия по внедрению цифрового обмена сертификатами соответствия:

- признание того, что ООС обладают полномочиями в отношении содержания своих сертификатов и что URL-ссылки на выданные сертификаты должны в цифровом виде отсылать к ООС или к признанному ООС субъекту (которым может быть признанный национальный или международный компетентный орган);
- признание того, что полномочия ООС (где это применимо) на выдачу сертификатов должны подтверждаться цифровой ссылкой на назначенный аккредитационный орган, владельца схемы или национальный или международный компетентный орган;
- приоритет отдается повышению информированности и принятию интероперабельных международных стандартов данных во избежание дробления процессов верификации на отдельные блоки данных; и
- поддержка внедрения уникальных глобальных идентификаторов для товаров и сертификатов как способа упрощения процессов обмена данными.

C. Последствия и перспективы

90. Интерес к цифровым процессам получения и проверки сертификатов соответствия и спрос на них могут возрасти, поскольку ручная проверка сертификатов становится менее оправданной в условиях цифровой торговли, а правительства, регулирующие органы и другие участники цепочки поставок ищут более эффективные и действенные инструменты для ограничения случаев попадания на рынок не соответствующей требованиям продукции. Регуляторы или владельцы схем могут также требовать использования идентификаторов продукции в сертификатах соответствия, что способствовало бы укреплению доверия к их собственным процессам.

91. Основной вывод данного документа заключается в том, что ОСС занимают уникальное место в увязывании сертификатов соответствия с физическими товарами, а также в том, что ОСС можно поощрять к предоставлению URI-отсылок к выданным сертификатам, чтобы обеспечить возможность цифровой обработки информации об их связи с продукцией. Такие добровольные процессы могут быть реализованы на уровне отдельных ОСС, делегированы органам аккредитации или владельцам схем (когда это применимо), национальным или отраслевым органам, а для некоторых видов сертификатов — даже вынесены на глобальный уровень.

92. Во избежание сомнений не предлагается создавать никаких централизованных систем помимо тех, которые существуют в настоящее время. Скорее, предлагается возможность индексирования существующих баз данных. Считается, что для решения поставленной задачи может быть создана интегрированная экосистема ОСС, использующая существующие идентификаторы продукции (в той мере, в какой они имеются), что можно было бы поощрять в рамках глобальных механизмов, регламентирующих деятельность сектора оценки соответствия.

93. Следует признать возможные затраты ОСС на создание потенциала для увязывания товаров с сертификатами. Степень текущих затрат/последствий может зависеть от того, должна ли такая информация предоставляться только по запросу клиента или активно собирается в рабочем порядке. Кроме того, затраты могут возникнуть на обеспечение электронного доступа к сертификатам и соответствующей привязке к продукции, хотя многие из необходимых структур могут уже существовать в виде баз данных ОСС, владельца схемы, аккредитационного органа и других организаций, уже созданных для обмена подтвержденной информацией о соответствии.

94. Проведение исследований национальными институтами качества или неправительственными организациями для дальнейшей проверки концепций на глобальном уровне можно только приветствовать. Кроме того, существует возможность для взаимодействия и гармонизации с ОСС, отвечающими за калибровку инструментов для научных измерений (эти ОСС работают в той же системе аккредитации ИЛАК, в которой проводятся испытания), а также в таких тесно связанных с этим областях, таких как торговые измерения, где интенсивная работа по формализации выдачи цифровых сертификатов ведется такими органами, как Федеральное физико-техническое управление (Physikalisch-Technische Bundesanstalt) в Германии.

95. Продвижение этих идей потребует широкого взаимодействия с заинтересованными группами на международном уровне. Сотрудничество между глобальными органами, отвечающими за торговлю и соответствие продукции требованиям, будет иметь большое значение для того, чтобы не допускать появления разрозненных или изолированных систем в будущем.

Приложение

[English only]

Some relevant technologies

Technology	*Description*	*Relevance to digital conformity*
JSON and JSON-LD	JSON is an IETF specification for a simple representation of digital data using Javascript notation *[footnote https://www.rfc-editor.org/rfc/rfc7159]*. JSON is the most popular representation for digital data in web services in use today. JSON-LD is a W3C specification for Linked Data *[footnote https://www.w3.org/TR/json-ld11/]*.	Given its simplicity, wide tools support, and popularity amongst web developers, JSON is a worthy candidate for digital conformity data representation. Example {"CertificateNumber" : "871423175000060012051”} JSON-LD semantic tagging allows verifiers to consistently extract the data they need at runtime, irrespective of variations in certificate structure and content. The key idea is that any data element in any JSON document can be linked to a global standard vocabulary definition. So, the consumer of a document containing JSON-LD can be confident of consistent meaning assigned to a term irrespective of the document type that contains it.
XML	Extensible Markup Language (XML) was developed by a working group formed under the auspices of the World Wide Web Consortium (W3C) in 1996 *[footnote www.w3.org/TR/xml/]* and has established itself internationally as a widely accepted data exchange format. Conversion to other data exchange formats such as JSON is easily done. Furthermore, many established markup languages such as MathML are based on and can directly be included within XML structured data.	XML was originally designed as a document format and is therefore well-suited for documents such as digital certificates. It has been extensively used in IT for over 20 years. XML syntax allows for the definition of secure, simple and complex data types and provides the means for an automated validation of data structures and properties through XML schema files. Namespaces, reference IDs, and attributes allow an easy integration of semantic meaning to data and linking with other metadata. Cryptographic processes can be applied robustly and securely to XML data structures.
PKI	Public key infrastructure is a generic term for a wide variety of protocols and algorithms that are based on the use of public and private key-pairs to digitally sign and encrypt documents in order to support secure and high integrity data exchange.	Product conformity attestations exist to provide trust to the marketplace. Digitalisation of conformity attestations without corresponding digitalisation of trust would be of limited value. Public Key cryptography and digital signatures provide a means for the integrity of the attestation to be maintained irrespective of where it is stored or how it is shared.
DID and VC	The W3C has defined standards for Decentralized Identity (DID) and Verifiable Credentials (VC). These specifications are built upon JSON-LD and PKI and underpin a new and highly scalable decentralised framework for sharing of high integrity digital data. DIDs allow parties in the supply chain to prove their identity, and VC is a standard	Most supply chains will cross multiple industries and geographies, each with one or several distinct supply chain systems and platforms. There will never be one system to rule them all and so for digital product conformity claims to follow goods throughout the supply chain a scalable solution such as VCs is needed. Like the chip in an e-passport, a conformity attestation VC is issued to the holder and travels with the

Technology	*Description*	*Relevance to digital conformity*
	way to express verifiable claims made by issuer parties about any subject party or product.	products and can be verified manually or by systems. There is no dependency on shared platforms or technologies.
ZKP	Zero Knowledge Proofs represent a collection of cryptographic techniques for proving that something is true without revealing the underlying evidence.	Product conformity attestations may include commercially sensitive trader party and product information, along with the conformity results. ZKP provides the ability to share verifiable conformity claims without leaking sensitive information. There are some practical implementations associated with VC technology where ZKP is used for selective redaction or selective disclosure.
QR	A QR (Quick Response) is a two-dimensional (2D) barcode that is easily and cheaply printable on any product. Often the QR codes represent web URLs so that, when scanned by anyone with a smartphone, the user is taken to a website. QR codes can also embed further data, such as product specifications or secret keys.	QR codes provide a very effective means to bridge the paper-digital divide by supporting a hybrid model where links to digital conformity attestations can be printed on PDF certificates. This allows issuers to ‘go digital’ without dependency on consumer or verifier maturity.
Linked Data	Linked data is structured data which is interlinked with other data, so it becomes more useful, e.g., through semantic queries.	It builds upon standard web technologies such as hypertext transfer protocol (HTTP), Resource Description Framework (RDF) and URIs, but rather than using them to serve web pages only for human readers, it extends them to share information in a way that can be read automatically by computers. Part of the vision of linked data is for the internet to become a global database.
Digital Link Resolvers	Resolvers are online services based on Linked Data standards. These services ‘resolve’ identifiers to one or more sources of information about the identified item.	Resolvers can, for example, link a Product identifier to information about the product, including product conformity attestations to substantiate product claims. For hardware, they can link to things like instruction manuals and usage videos. At the same time, resolvers can link an identified item to information for business partners such as recall/revision status APIs, master data, (hazardous materials) handling instructions and much more.