Экономический и Социальный Совет

Distr.: General
3 December 2020
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Рабочая группа по таможенным вопросам, связанным с транспортом

Группа экспертов по концептуальным и техническим аспектам компьютеризации процедуры МДП

Первая сессия
Женева, 27–29 января 2021 года
Пункт 6 a) предварительной повестки дня
Международная система eTIR:
Доклад о ходе разработки международной системы eTIR

Веб-службы eTIR — Обзор, безопасность и доступ*

Записка секретариата

I. Введение — Мандат

1. Комитет по внутреннему транспорту на своей восемьдесят второй сессии (23–28 февраля 2020 года) одобрил (ECE/TRANS/294, п. 84[1]) учреждение Группы экспертов по концептуальным и техническим аспектам компьютеризации процедуры МДП (WP.30/GE.1) и утвердил ее КВ[2] (ECE/TRANS/WP30/2019/9 и ECE/TRANS/WP.30/2019/9/Corr.1) в ожидании одобрения Исполнительным комитетом ЕЭК ООН (Исполком). В ходе дистанционного неофициального совещания членов Исполнительного комитета (20 мая 2020 года) Исполком одобрил учреждение Группы экспертов по концептуальным и техническим аспектам компьютеризации процедуры МДП (WP.30/GE.1) на период до 2022 года на основе круга ведения, содержащегося в документе ECE/TRANS/WP.30/2019/9 и Corr.1, что отражено в документе ECE/TRANS/294 (ECE/EX/2020/L.2, п. 5 b))[3].

* Настоящий документ был представлен для обработки с опозданием, поскольку для получения санкции на его окончательную доработку потребовалось больше времени, чем предполагалось.

[1] Решение Комитета по внутреннему транспорту, п. 84/ECE/TRANS/294 https://unece.org/fileadmin/DAM/trans/doc/2020/itc/ECE-TRANS-294e.pdf.

[2] Круг ведения вновь созданной Группы, утвержденный Комитетом по внутреннему транспорту и Исполнительным комитетом (Исполкомом) ЕЭК ООН https://unece.org/fileadmin/DAM/trans/bcf/wp30/documents/2019/ECE-TRANS-WP30-2019-09e.pdf и исправление https://unece.org/fileadmin/DAM/trans/bcf/wp30/documents/2019/ECE-TRANS-WP30-2019-09c1e.pdf.

[3] Решение Исполнительного комитета, ECE/EX/2020/L.2/п. 5 b) https://unece.org/fileadmin/DAM/commission/EXCOM/Agenda/2020/Remote_informal_mtg_20_05_2020/Item_4_ECE_EX_2020_L.2_ITC_Sub_bodies_E.pdf.

2. Круг ведения Группы предусматривает, что Группе следует сосредоточить свою работу на подготовке новой версии спецификаций eTIR в ожидании официального создания ОТО. В частности, по просьбе WP.30 Группе следует: a) подготовить новую версию технических спецификаций процедуры eTIR и поправки к ним для обеспечения их соответствия функциональным спецификациям процедуры eTIR; b) подготовить новую версию функциональных спецификаций процедуры eTIR и поправки к ним для обеспечения их соответствия концептуальным спецификациям процедуры eTIR; c) подготовить поправки к концептуальным спецификациям процедуры eTIR.

3. В настоящем документе представлен обзор веб-служб eTIR, способов доступа к этим услугам, детальной информации об аспектах безопасности процедуры eTIR, а также технические аспекты внедрения и тестирования сообщений eTIR. Настоящий документ действует в отношении международной системы eTIR (версия 1.0), которая была разработана на основе спецификаций eTIR (версия 4.3a).

II. Цель

4. В документе описываются веб-службы международной системы eTIR: в частности, предполагаемая целевая аудитория, системная архитектура, различные сообщения и их последовательность, аспекты безопасности, доступ, а также контакты в целях поддержки. В нем не рассматриваются вопросы детальной реализации, необходимой в случае каждого сообщения, которую можно найти в документах, посвященных каждому из сообщений eTIR. В нем, скорее, описываются компоненты и процессы, которые следует внедрить в национальные таможенные системы, с тем чтобы они могли эффективно взаимодействовать с международной системой eTIR.

III. Целевая аудитория

5. Настоящее руководство предназначено для группы ИКТ в таможенных органах, которая занимается процессами МДП и отвечает за связь их национальных таможенных систем с международной системой eTIR.

IV. Предварительные условия

6. Настоящий документ следует изучить после ознакомления с концепцией eTIR[4], а также после ознакомления и соблюдения проекта руководящих принципов подключения к eTIR, предназначенного для таможенных органов[5]. В этой связи исключительно важно понять этапы реализации, описанные в вышеуказанных руководящих принципах, а также уяснить для себя, на каком этапе процесса реализации вы находитесь в данный момент.

7. Для того чтобы обеспечить такой вариант реализации, который позволил бы добиться наибольшей отдачи и оказать таможенным органам как можно лучшие услуги, мы настоятельно рекомендуем включить в группу по ИКТ соответствующего эксперта по тематике МДП, как это указано в проекте руководящих принципов подключения к eTIR таможенных органов.

V. Критический анализ документации eTIR

8. Международная система eTIR строится на Конвенции МДП, поэтому в основу документации eTIR положены ее статьи и приложения, а также иные различные ключевые документы, доступные в режиме онлайн и представленные ниже.

[4] https://unece.org/fileadmin/DAM/trans/bcf/adhoc/conc_tech/documents/id17-06e.pdf.

[5] https://wiki.unece.org/download/attachments/106299939/Project Guidelines for customs to connect to the eTIR international system.pdf.

Некоторые из этих документов необходимо изучить и хорошо вникнуть в их суть, в то время как другие носят справочный характер и в этой связи ими можно воспользоваться в случае необходимости. Этот раздел поможет вам лучше понять, что они содержат и в каком порядке мы рекомендуем их читать.

a) Проект руководящих принципов подключения таможен к eTIR: данный документ является отправной точкой для таможенных органов любой договаривающейся стороны, и в этой связи с ним необходимо ознакомиться в первую очередь. Если вы не знакомы с проблемами перевозок и упрощения порядка пересечения границ, мы настоятельно рекомендуем вам ознакомиться со следующими документами:

b) Справочник по Конвенции МДП[6]: этот документ содержит все правовые элементы, которые лежат в основе Конвенции МДП (включая комментарии и пояснительные записки). В нем также описываются процессы, которым должны следовать таможенные органы, национальные объединения и держатели книжек МДП.

c) Приложение 11 к Конвенции МДП[7]: в приложении 11 к Конвенции МДП описывается процедура eTIR, излагается порядок адаптации процессов для целей компьютеризации и устанавливаются нормативно-правовые положения реализации и использования на практике международной системы eTIR.

9. После того как вы хорошо уясните нормативно-правовой контекст МДП и ключевые процессы, мы настоятельно рекомендуем прочитать:

d) Вводную часть документации, посвященной концептуальным, функциональным и техническим спецификациям[8]: этот документ дает возможность вникнуть в суть концептуальной, функциональной и технической проблематики проекта компьютеризации процедур МДП в соответствии с методологией моделирования Центра Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ ООН). Это первый документ, который следует прочитать, для того чтобы лучше понять, каким образом была задумана eTIR в качестве дополнения к Конвенции МДП.

e) Концепции eTIR[9]: в этом документе содержится описание подхода и основных концепций, используемых для поддержки бизнес-логики и реализации международной системы eTIR. Этот документ также является своего рода справочным документом, в котором описаны все случаи использования и все правила ведения деловых операций, которые применяются в целях претворения в жизнь технических проектов.

f) Функциональные спецификации eTIR[10]: данный документ является наиболее важным в плане ознакомления, поскольку он позволяет глубже понять механизмы, используемые для реализации международной системы eTIR. Нынешняя версия (4.2) в настоящее время получает более широкое отражение в рабочем документе ({etir-spec-version}) и уточняется по мере продвижения работы и получения отзывов в связи с работой по моделированию, которая проводится Неофициальной специальной группой экспертов по концептуальным и техническим аспектам компьютеризации процедуры МДП (GE.1) и всеми координаторами eTIR. Эти спецификации (которые в свое время назывались справочной моделью) также относятся к следующим дополнительным документам и спискам:

[6] https://www.unece.org/tir/tir-hb.html.
[7] https://unece.org/fileadmin/DAM/trans/bcf/ac2/documents/2020/ECE-TRANS-WP30-AC2-147e.pdf#page=12.
[8] https://unece.org/fileadmin/DAM/trans/bcf/adhoc/conc_tech/documents/id17-05e.pdf.
[9] https://unece.org/fileadmin/DAM/trans/bcf/adhoc/conc_tech/documents/id17-06e.pdf.
[10] https://unece.org/fileadmin/DAM/trans/bcf/adhoc/conc_tech/documents/id17-07e.pdf.

i) XML-схемы eTIR[11];

ii) списки кодов eTIR[12];

iii) список кодов ошибок eTIR[13].

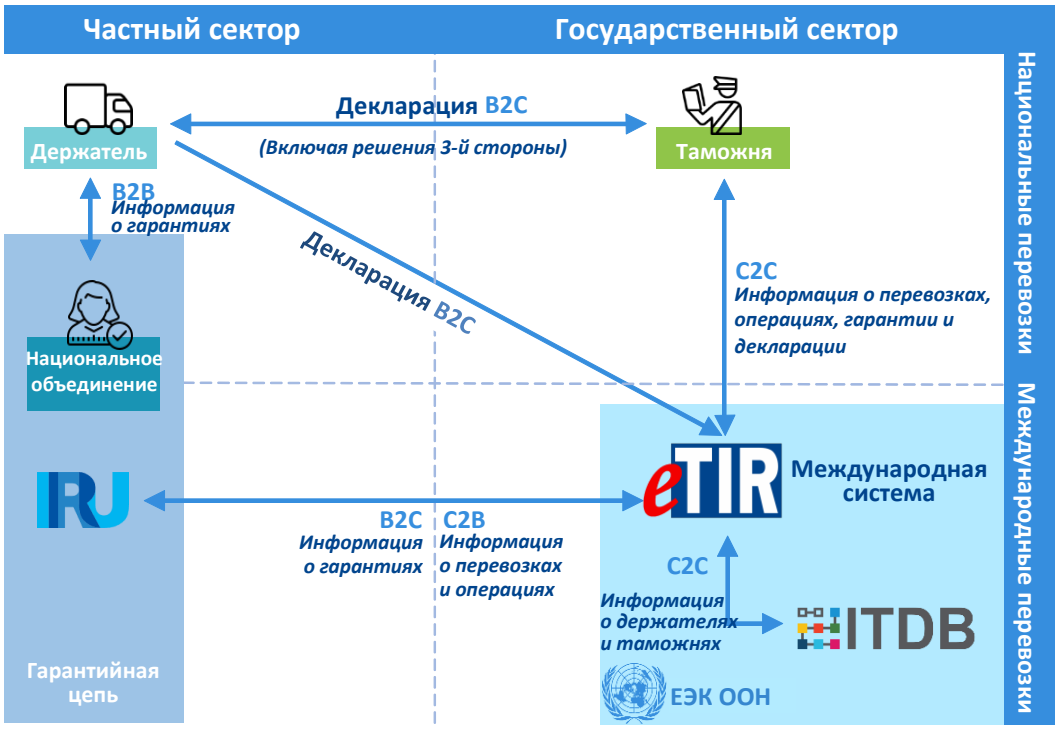
g) И в заключение, если вы хотите связаться с другими договаривающимися сторонами в ходе этой работы по реализации, просьба обратить внимание на страницу координаторов eTIR, где вы найдете нужные вам контактные данные[14].

VI. Обзор веб-служб eTIR

A. Высокоуровневая архитектура

10. Международная система eTIR строится на следующей функциональной схеме обзора.

Рис. I
Высокоуровневая архитектура eTIR



* Просьба обратить внимание на следующие аббревиатуры, означающие:

B2B: операции между коммерческими структурами (когда бизнес относится к частному сектору).

C2B: операции между таможней и коммерческими структурами (когда бизнес относится к частному сектору).

B2C: Операции между коммерческими структурами и таможней (когда бизнес относится к частному сектору).

C2C: Операции между таможнями.

[11] https://wiki.unece.org/display/ED/Technical+artefacts.
[12] https://unece.org/fileadmin/DAM/trans/bcf/eTIR/documents/CodeLists0_4.pdf.
[13] https://wiki.unece.org/display/ED/Error+Management.
[14] https://www.unece.org/trans/bcf/etir/focals.html.

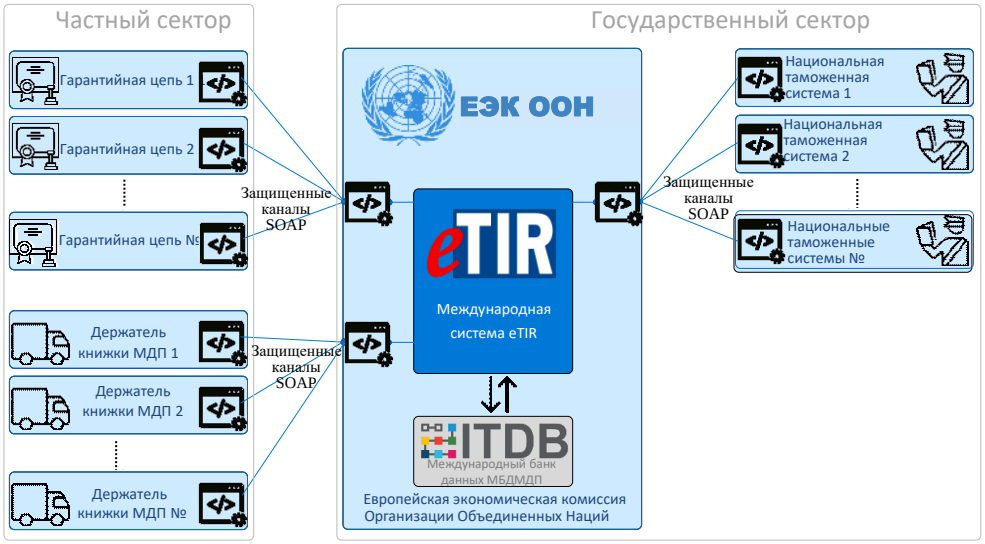
11. Комплекс технологий: международная система eTIR была введена в действие с использованием следующих технологий:

- язык программирования «Java»[15];
- база данных «PostgreSQL»[16];
- «Фреймворк с открытым исходным кодом»[17];
- «ActiveMQ»[18];
- веб-службы «SOAP-XML»[19];
- «Apache CFX»[20];
- «Apache Camel»[21].

12. Хотя эти технологии перечислены только для информации, тем не менее, если у читателя возникнут вопросы по методам внедрения и/или по комплексу технологий, которые используются для целей внедрения в практику международной системы eTIR, просьба связаться со службой поддержки eTIR по адресу etir@un.org.

13. Международная система eTIR оставляет открытыми конечные точки веб-службы как с государственными, так и с частными партнерами, как показано на диаграмме ниже:

Рис. II
Конечные точки eTIR



14. Следует отметить, что в настоящее время существует только одна действующая гарантийная цепь (а именно гарантийная цепь Международного союза автомобильного транспорта), но Конвенция МДП не ограничивается только ею одной.

[15] https://docs.oracle.com/javase/7/docs/technotes/guides/language/.
[16] https://www.postgresql.org/.
[17] https://spring.io/.
[18] http://activemq.apache.org/.
[19] https://www.w3.org/TR/soap/.
[20] http://cxf.apache.org/.
[21] https://camel.apache.org/.

B. Обзор программных интерфейсов для передачи сообщений

15. Перечень сообщений eTIR распределяется по категориям на внутреннем уровне на основе отправителя/адресата сообщения и на основе маршрутизации сообщения (в централизованном порядке на уровне eTIR):

- Все коды сообщений начинаются:
    - на «I» для внутреннего пользования (внутренний для государственного сектора, т. е. между международной системой eTIR и либо национальной таможенной системой, либо МБДМДП);
    - на «E» для внешнего пользования (внешний для государственного сектора, т. е. между eTIR и либо гарантийной цепью, либо держателями книжек МДП).
- Все сообщения действуют на спаренной основе (запрос–ответ) и все их коды также заканчиваются:
    - либо «нечетным номером» в случае инициирования/вызова/запросного сообщения;
    - либо «четным номером» в случае ответа/подтверждения сообщения.

16. Ниже приведен список всех внутренних и внешних сообщений:

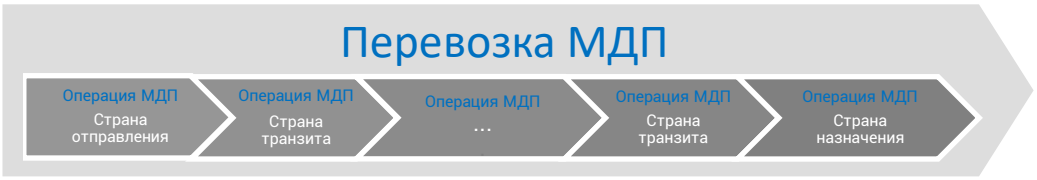
Внешние сообщения	*Внутренние сообщения*
E1 - Регистрация гарантии	**I1 - Принятие гарантии**
E2 - *Результаты регистрации*	I2 - *Результаты принятия*
E3 - Отмена гарантии	**I3 - Получение информации о держателе**
E4 - *Результаты отмены*	I4 - *Информация о держателе*
E5 - Запрос в отношении гарантии	**I5 - Запрос в отношении гарантии**
E6 - *Результаты запроса*	E6 - *Результаты запроса*
E7 - Уведомление гарантийной цепи	**I7 - Данные зарегистрированной декларации**
E8 - *Подтверждение уведомления*	I8 - *Результаты проверки данных зарегистрированной декларации*
E9 - Предварительные данные МДП	**I9 - Начало операции МДП**
E10 - *Результаты проверки предварительных данных МДП*	I10 - *Результаты начала операции*
E11 - Предварительные данные об изменениях	**I11 - Прекращение действия МДП**
E12 - *Результаты проверки предварительных данных об изменениях*	I12 - *Результаты прекращения*
E13 - Отмена предварительных данных	**I13 - Завершение операции МДП**
E14 - *Результаты отмены предварительных данных*	I14 - *Результаты завершения*
	I15 - Уведомление таможни
	E16 - *Подтверждение уведомления*
	I17 - Отказ начать операцию МДП
	I18 - *Результаты отказа*
	I19 - Проверка таможен
	I20 - *Валидация таможенных органов*

17. Цель международной системы eTIR заключается в обеспечении безопасного обмена между национальными таможенными системами информацией, касающейся международной транзитной перевозки грузов, транспортных средств и контейнеров в соответствии с положениями Конвенции МДП, а также в предоставлении таможенным органам возможности управлять данными по гарантиям, выданным гарантийными цепями держателям книжек МДП, уполномоченным использовать систему МДП.

C. Перевозка МДП и использование МДП в системе eTIR

18. На приведенной ниже схеме выделены важные концепции перевозок МДП и операций МДП и приводится соответствующий пример, который их иллюстрирует:

Рис. III
Краткая справка по перевозке МДП



19. Важно отметить, что в ходе перевозки в режиме МДП может быть задействовано несколько пунктов погрузки и разгрузки и, естественно, несколько пунктов пересечения границы. Каждый из них представляет собой пункт разделения операций МДП. Следует также отметить, что пункты пересечения границы, разделяющие операции МДП, находятся между каждой таможенной территорией (это может быть отдельная страна или общая таможенная территория, как в случае с Европейским Союзом). Более подробную информацию по этому вопросу можно найти на специальной странице вводного документа eTIR[22].

[22] https://unece.org/fileadmin/DAM/tir/handbook/english/newtirhand/TIR-6Rev11e.pdf#page=21.

Рис. IV

Пример перевозки МДП

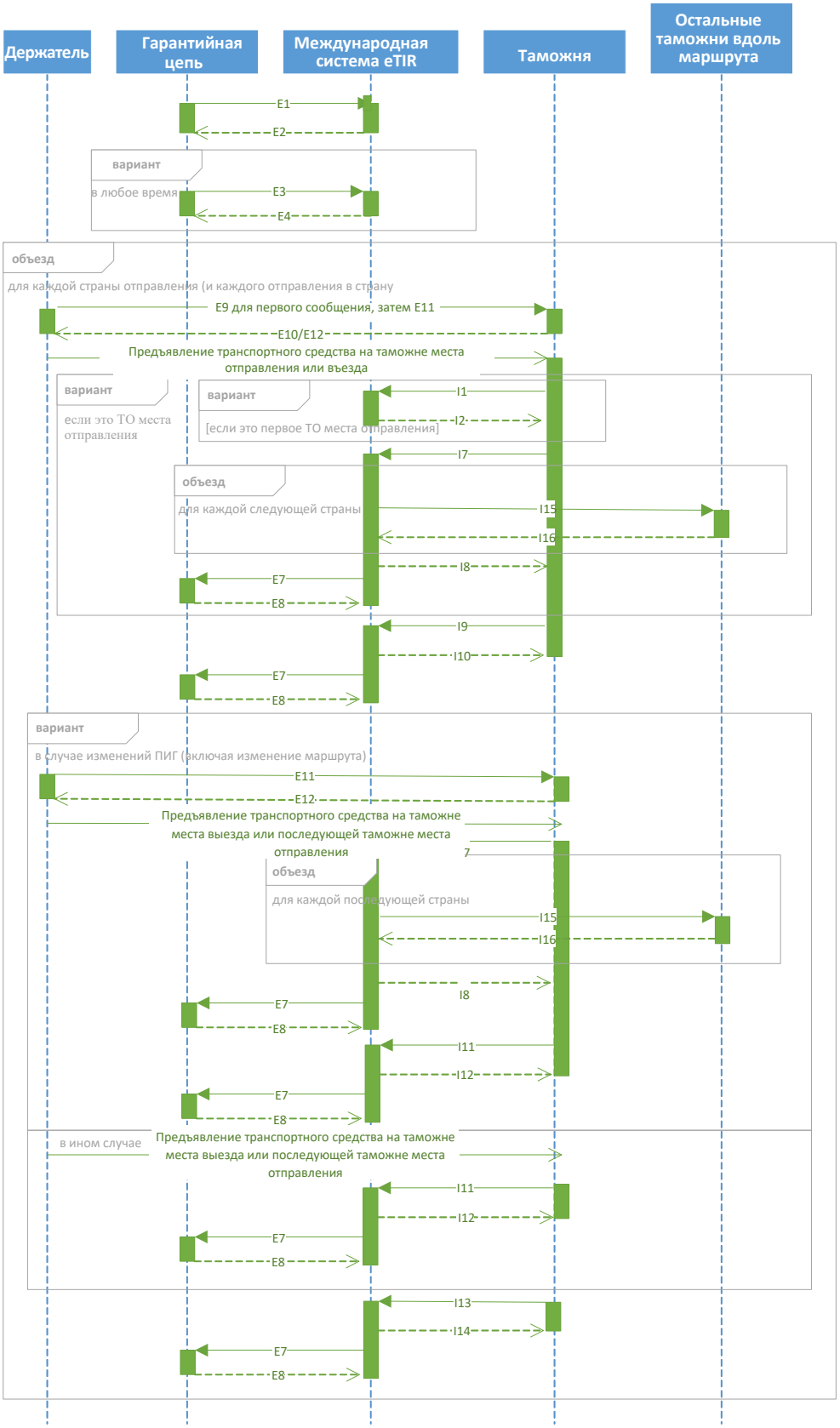
Указанные на этих картах границы и названия, а также используемые на них обозначения не подразумевают их официального одобрения или признания со стороны Организации Объединенных Наций

D. Диаграммы последовательности eTIR

20. Использование сообщений eTIR описывается на следующих диаграммах последовательности eTIR для стран отправления, транзита и назначения.

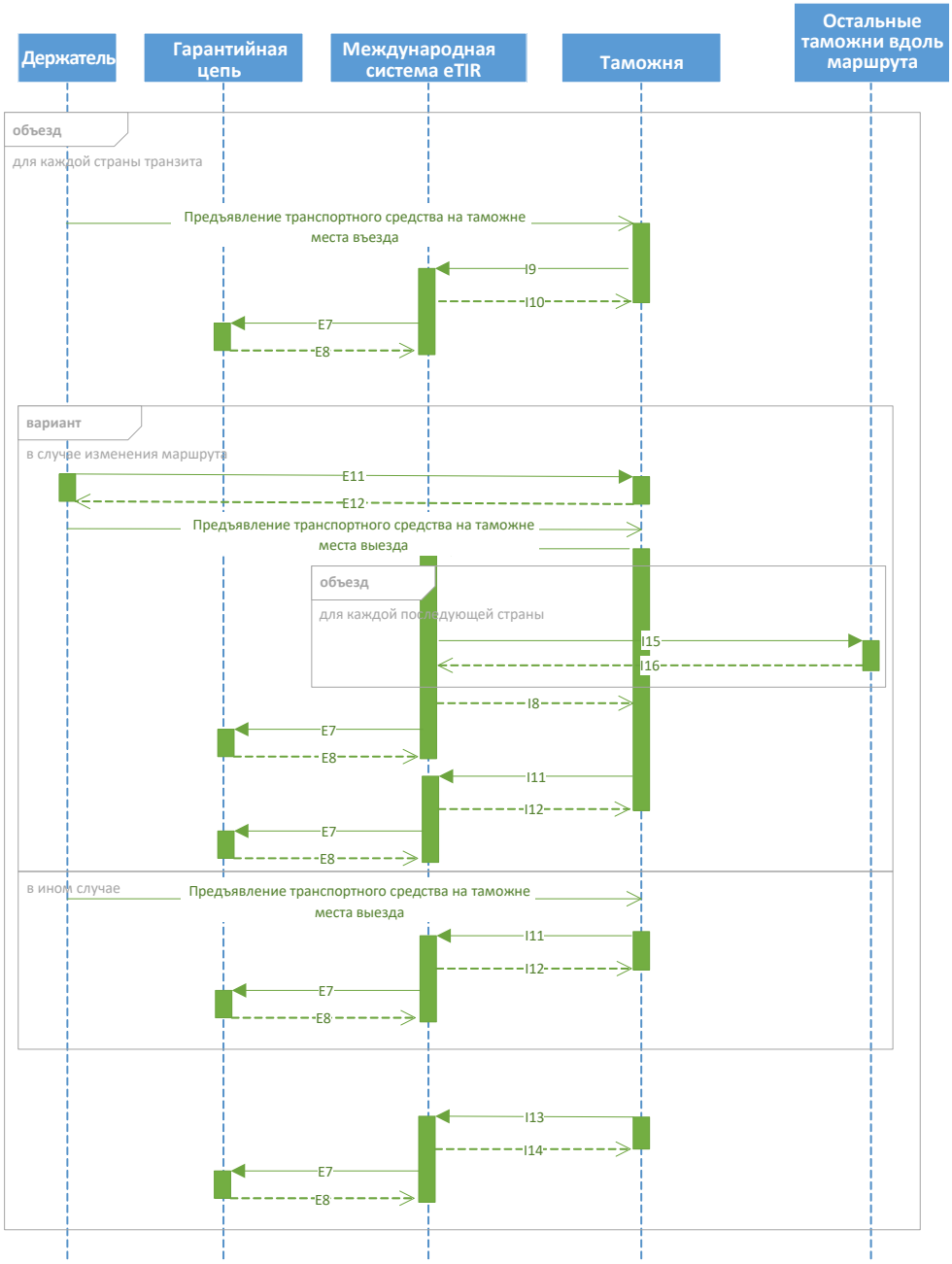
1. Последовательность сообщений для стран отправления

Рис. V
Диаграмма временно́й последовательности — страны отправления



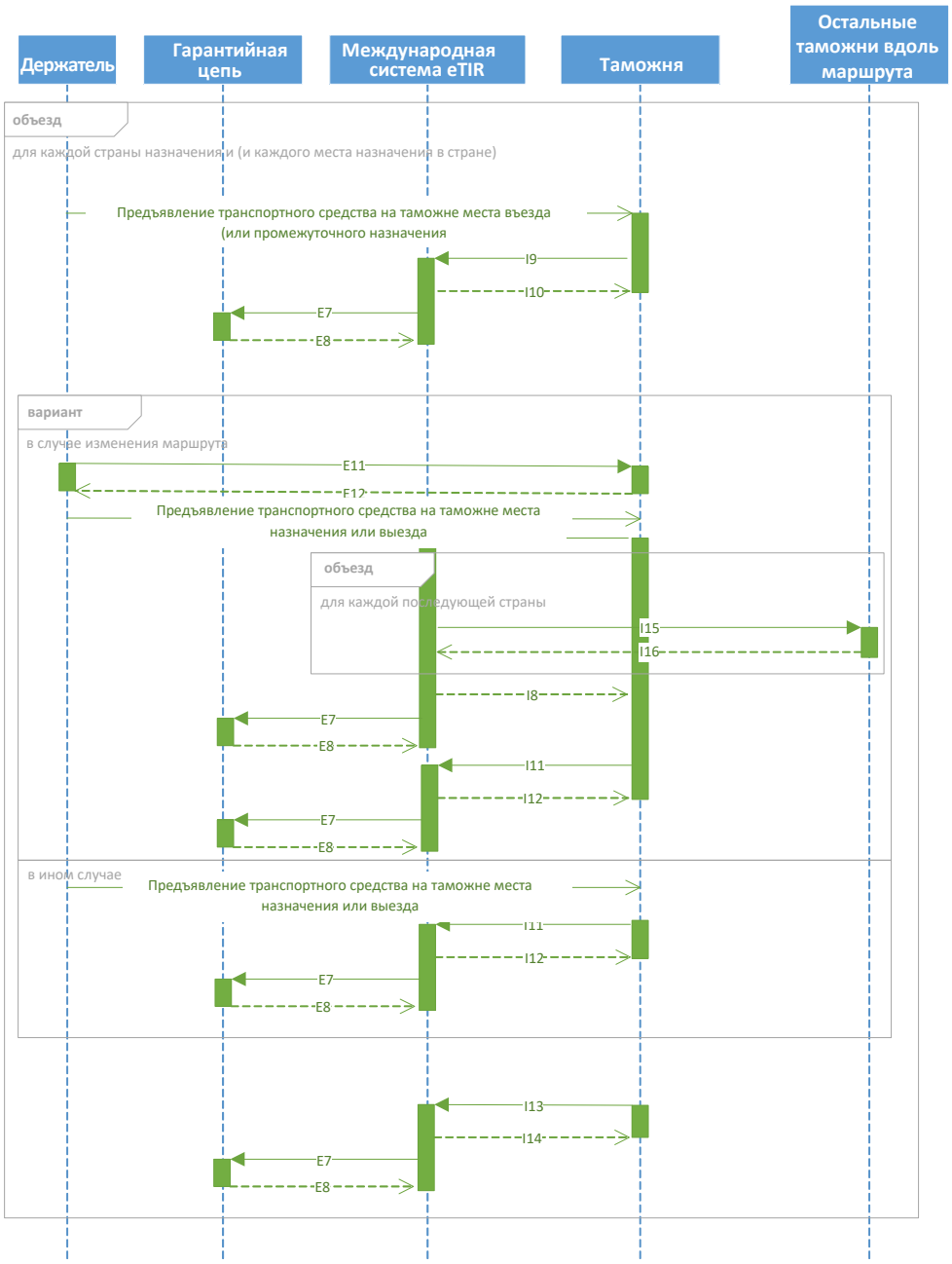
2. Последовательность сообщений для стран транзита

Рис. VI
Диаграмма временно́й последовательности — страны транзита



3. Последовательность сообщений для стран назначения

Рис. VII
Диаграмма временно́й последовательности — страны назначения



VII. Аспекты безопасности

21. В международных веб-службах системы eTIR для электронной подписи сообщений используется система «WS-Security» («ВС-безопасность»). Для шифрования сообщения система «WS-Security» («ВС-безопасность») не используется. Эти рамочные принципы были изданы в марте 2004 года в качестве полностью признанной отраслевой рекомендации.

22. Цифровая подпись на основе сертификатов X.509 (версия 3) используется для идентификации вызывающего абонента в веб-службе и исключает возможность отказа. Для отправки сообщений по протоколу HTTPS используется протокол шифрования (TLS v1.2 или v1.3), который обеспечивает конфиденциальность

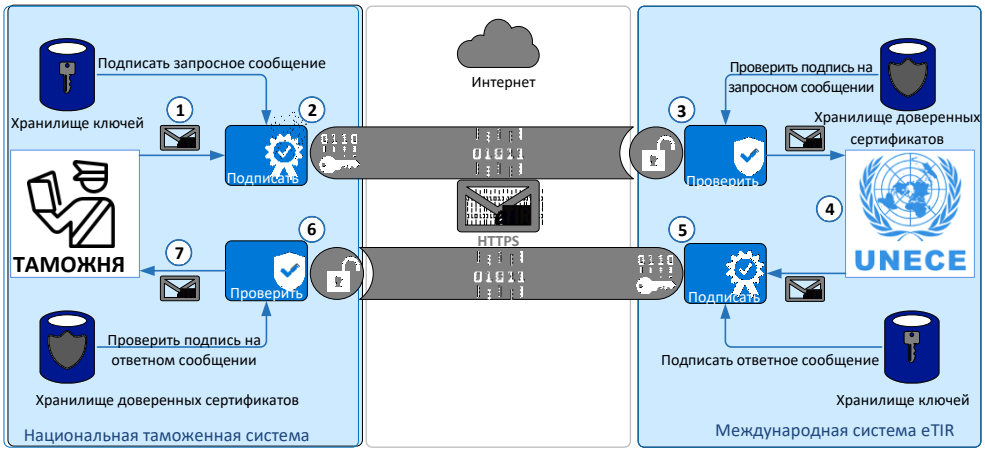
информации, обмениваемой в сообщениях. Следует отметить, что в цифровой подписи и протоколе шифрования (TLS) используются разные асимметричные пары ключей.

23. В следующих пунктах содержится описание веб-служб, терминов и понятий, связанных с безопасностью, которые используются на протяжении всего срока действия документа. В них часто упоминаются такие термины, как «Безопасность веб-сервисов (ВС-безопасность)», маркер «X.509», «хранилище ключей» и «хранилище доверенных сертификатов», которые подробно объясняются в Глоссарии.

A. Модель безопасности eTIR

24. На рисунке ниже показана модель «ВС-безопасность», а в настоящем разделе иллюстрируется в общих чертах принцип работы этой модели безопасности.

Рис. VIII
Модель безопасности eTIR



25. Просьба иметь в виду, что, хотя на этой диаграмме представлено большинство случаев использования, все же в ряде других случаев международная система eTIR фактически играет роль клиента, а национальные таможенные системы — роль поставщика услуг.

26. В приведенном выше примере в качестве первого шага в хранилище доверенных сертификатов международной системы eTIR устанавливается сертификат X.509 национальных таможенных систем. Аналогичным образом, сертификат международной системы eTIR устанавливается в хранилище доверенных сертификатов национальных таможенных систем. Этот обязательный начальный шаг позволяет подтвердить подлинность цифровых подписей, которые передаются в качестве маркеров безопасности во всех SOAP-сообщениях, которыми обмениваются в контексте процедуры eTIR.

27. Ниже приводится описание того, каким образом национальные таможенные системы направляют запрос в международную систему eTIR и каким образом отправляется соответствующий ответ адресату:

a) Национальная таможенная система генерирует запросное сообщение для отправки в международную веб-службу системы eTIR.

b) Это запросное сообщение подписывается закрытым ключом сертификата национальной таможенной системы X.509 (который содержится в хранилище ключей) и отправляется с использованием протокола шифрования (TLS) по протоколу HTTPS.

c) Международная система eTIR получает запросное сообщение, проверяет подпись сообщения с использованием открытого ключа отправителя в порядке его аутентификации и подтверждения его целостности.

d) Международная система eTIR обрабатывает запросное сообщение и в ответ генерирует ответное сообщение.

e) Это ответное сообщение подписывается закрытым ключом сертификата международной системы eTIR (который содержится в хранилище ключей) и отправляется с использованием протокола шифрования (TLS) по протоколу HTTPS.

f) Национальная таможенная система получает ответное сообщение и проверяет подпись сообщения с использованием открытого ключа поставщика услуг в порядке его аутентификации и подтверждения его целостности.

28. Завершение этого процесса иллюстрирует реализацию на практике четырех аспектов безопасности, которую желает обеспечить международная система eTIR с помощью этой модели безопасности: аутентификация, целостность, конфиденциальность и исключение возможности отказа.

B. Аутентификация, целостность и исключение возможности отказа

29. Аутентификация используется с целью убедиться в том, что различные стороны сделки действительно являются теми, за кого они себя выдают. Именно для этого требуется соответствующее подтверждение идентичности. Подтвердить этот факт можно различными способами. Одним из простых примеров является предоставление ИД пользователя вместе с секретным паролем. Более безопасный метод состоит в использовании сертификата X.509, выданного доверенным сертификационным органом (ниже и далее в этом разделе он именуется как «CO»). Сертификат X.509 идентифицирует конечного пользователя. В дополнение к функции аутентификации закрытый ключ к сертификату X.509 также используется для подписи SOAP-сообщений. Эта электронная подпись не только обеспечивает идентичность отправителя, но и гарантирует, что содержание сообщения не было подделано во время передачи, что обеспечивает тем самым его целостность. Отправитель использует свой закрытый ключ для подписи сообщения (точнее, контрольную сумму сообщения), а получатель сообщения использует открытый ключ отправителя для проверки подписи, тем самым предоставляя доказательства невозможности отказа.

1. Этапы аутентификации с использованием сертификата X.509

Рис. IX
Этапы аутентификации

- Клиентское приложение (национальная таможенная система) отправляет сообщение поставщику услуг (международная система eTIR — этап № 1). Сообщение включает в себя учетные данные клиентского приложения, подписанные закрытым ключом, который спарен с открытым ключом в сертификате X.509 клиентского приложения. Поставщик услуг подтверждает сертификат посредством проведения ряда проверок (этап № 2), в том числе:
- Проверку того, что срок действия сертификата не истек. Если срок действия сертификата истек, то он больше недействителен.
- Проверку внутреннего соответствия сертификата. Служба удостоверяется в том, что данные в сертификате не были подделаны, посредством проверки содержания сертификата на соответствие подписи выдавшего его CO.
- Проверка CO, выдавшего клиентский сертификат X.509. Это делается путем сравнения подписи эмитента на сертификате клиентского приложения X.509 с

сертификатом X.509 выдающего СО. Для правильной работы на этом этапе данные Сертификационного органа, который выдал клиентский сертификат X.509, должны соответствовать данным как клиентского приложения, так и провайдера услуг.

- Проверка с целью убедиться в том, что СО-эмитент не отозвал сертификат. Провайдер услуг проверяет этот момент, убедившись в том, что сертификат X.509 не значится в списке отозванных сертификатов (СОС), публикуется СО-эмитентом. Служба может проверить статус отзыва сертификата, получив прямой доступ к нему из СО или проверив его по СОС, который был ранее загружен из СО-эмитента в хранилище сертификатов, используемое службой для поиска сертификатов X.509.
- Для проверки подписи клиентского приложения (этап № 3) провайдер услуг использует открытый ключ в сертификате X.509 клиентского приложения. Это позволяет провайдеру услуг проверить подлинность клиентского приложения и убедиться в том, что после подписания сообщения вписанные данные не были подделаны.

30. Если в ходе проверки подлинность не подтвердилась, то провайдер услуг отправляет ответное сообщение об ошибке HTTP 500. В случае положительного результата проверки он обработает содержание запроса и выдаст надлежащее ответное сообщение в соответствии со спецификациями eTIR (этап № 4), которые после их получения должны подвергнуться таким же проверкам, как описано выше (этап № 5).

2. Генерация спаренных ключей

31. Таможенные органы могут получить пару открытых и закрытых ключей от доверенного органа сертификации или создать самоподписанные ключи. Они должны сгенерировать спаренные ключи RSA и предоставить группе секретариата МДП ЕЭК ООН открытую часть (сертификат X.509) созданного ключа, а хорошо защищенную часть закрытого ключа держать в своем хранилище ключей. Описание двух способов генерации спаренных ключей RSA см. в приложении.

C. Конфиденциальность

32. Протокол защищенной передачи гипертекста (HTTPS), используемый для доступа к конечным точкам международной системы eTIR, представляет собой расширение Протокола передачи гипертекста (HTTP), в случае которого коммуникация шифруется с помощью Протокола безопасности на транспортном уровне (TLS) — криптографического протокола, предназначенного для обеспечения безопасной коммуникации в таких общедоступных сетях, как Интернет. Основной причиной использования протокола HTTPS является необходимость обеспечения конфиденциальности и целостности передаваемых данных в процессе их передачи. Он защищает от угроз информационной безопасности, таких как атака под названием «перехват канала связи». Двунаправленная система шифрования коммуникации между клиентом и сервером обеспечивает защиту от подслушивания и взлома канала связи. По этой причине безопасность связи между международной системой eTIR и национальными таможенными системами обеспечивается посредством двунаправленного шифрования с использованием протокола TLS (как минимум v1.2).

VIII. Доступ к веб-службам eTIR

A. Предварительные условия

1. Требования к сети

33. Национальные таможенные системы должны иметь доступ к Интернету, а все домены среды пользовательского приёмочного тестирования и эксплуатации,

описанные в разделе ниже, должны быть внесены в белый список сетевыми инженерами таможенных органов. Кроме того, в контексте международной системы eTIR введен в действие протокол SOAP, позволяющий пользоваться протоколом HTTPS на разъеме TCP/8083, в связи с чем этот протокол и разъем должны быть открыты в сетевых устройствах защиты таможенных органов, с тем чтобы ими можно было пользоваться на уровне национальных таможенных систем.

2. Сертификаты

34. Как поясняется в разделе «Аспекты безопасности», связь между международной системой eTIR и национальными таможенными системами предполагает, что обе стороны должны обмениваться своими сертификатами X.509 и хранить их на взаимной основе в своих хранилищах доверенных сертификатов.

35. Данная процедура должна быть завершена для каждой спаренной среды «клиент-служба» на этапе внедрения, при том что среда UAT (проверка приемлемости для пользователей) национальных таможенных систем должна быть сопряжена со средой UAT международной системы eTIR. После того как эксплуатационные среды обеих сторон будут готовых к работе, стороны должны обменяться специальными эксплуатационными сертификатами X.509, что позволит установить между ними канал коммуникации и после подтверждения готовности к его вводу в эксплуатацию использовать процедуру eTIR.

36. Обе системы (международная система eTIR и национальные таможенные системы) должны использовать разные сертификаты X.509 для своей соответствующей среды UAT и эксплуатационной среды. Следует также обратить внимание на то, что если в данной документации речь идет о методах генерации сертификатов на местном уровне с использованием соответствующего открытого приложения, которое можно использовать для целей тестирования и разработки, то сертификаты, генерируемые и распространяемые таможенной группой ИКТ, могут использоваться в полной мере по их усмотрению до тех пор, пока соблюдаются все требования и аспекты безопасности, упомянутые в данном документе.

37. В дополнение к сгенерированному сертификату X.509, в механизме шифрования (HTTPS) сообщения будет использоваться сертификат сервера ЕЭК (unece.org.cer). В зависимости от вашей ситуации вам, возможно, придется извлечь и сохранить его в своем хранилище доверенных сертификатов. В противном случае ваше приложение может извлечь его автоматически (предпочтительный вариант).

38. В процессе генерации сертификата, описанном в разделе «Хранилище ключей: поэтапная генерация спаренных ключей», необходимо правильно заполнить поле электронной почты, поскольку оно будет использоваться международной системой eTIR для отправки своих уведомлений по электронной почте.

3. Серверы, включенные в белые списки

39. Серверы национальных таможенных систем должны быть сначала включены в белый список группой ЕЭК по безопасности ИТ, с тем чтобы обеспечить их подключение к серверам международной системы eTIR. Для этого специалистам таможенных органов необходимо представить в секретариат МДП все IP-адреса серверов национальных таможенных систем, которые будут направлять запросы в международную систему eTIR. Аналогичным образом, секретариат МДП готов дать IP-адреса своих серверов для выполнения той же операции со стороны таможенных органов.

B. URL-адреса тестирования и эксплуатации

40. Нижеприведенный список содержит информацию о конечных точках веб-служб как для эксплуатационной среды, так и для среды UAT, а также сопровождающие их URL-адреса для файлов на языке описания веб-служб (WSDL).

- Базовый URL веб-службы UAT

  etir-uat-01.unece.org/etir/v4.3/customs

- WSDL для таможенных органов

  etir-uat-01.unece.org/etir/v4.3/customs?wsdl

- WSDL для гарантийных цепей

  etir-uat-01.unece.org/etir/v4.3/guaranateeChain?wsdl.

IX. Реализация и тестирование сообщений eTIR

A. Рекомендуемый общий подход

1. Цель

41. В настоящем разделе секретариат МДП хотел бы поделиться информацией о процессах разработки, имеющих целью обеспечить своевременную и качественную реализацию на практике международной системы eTIR, в надежде на то, что таким образом читатель сможет в свою очередь извлечь пользу из накопленного нами опыта.

2. Общий подход

42. Секретариат МДП принял гибкий подход, следуя принципам динамичного программного документа МДП. Члены группы по ИКТ проводят еженедельные встречи в целях анализа результатов работы, проделанной за предыдущую неделю, обсуждения той работы, которую необходимо проделать в течение текущей недели, а также обратить внимание на любые потенциальные препятствия, для устранения которых можно было бы воспользоваться помощью со стороны участников других группы. Для поддержки работы секретариата МДП внутренняя система управления базами знаний (СУБЗ) включает следующие компоненты:

- система отслеживания проблем, которая регулирует решение всех поставленных задач, что обеспечивает превосходную отслеживаемость и подотчетность;
- платформа документации, в которой находят отражение все аспекты проекта eTIR, связанные с разработкой, управлением и эксплуатацией;
- система управления исходным кодом, в которой размещены хранилища кода информационных систем МДП.

3. Непрерывная интеграция

43. Секретариат МДП также воспользовался передовым опытом, накопленным командой по разработке и эксплуатации. В частности, мы признаем важный дополнительный вклад системы автоматизации как можно большего количества процессов в жизненном цикле разработки программного обеспечения, что позволяет избавить людей от необходимости решения обыденных задач, повысить надежность результатов за счет снижения вероятности человеческих ошибок и резко повысить производительность труда.

44. Для того чтобы система была как можно более надежной, мы регулярно претворяем в жизнь принятый нами новый кодекс с помощью нашего «конвейера непрерывной интеграции» (КНИ). Мы также перестраиваем всю нашу кодовую базу каждый раз, когда в наше хранилище кодов передают на хранение новый код, с целью гарантировать такое положение, в котором каждый доведенный до конца функциональный параметр в любой момент времени действует так, как планировалось.

4. Масштабное тестирование

45. В целях ежедневной проверки нашего исходного кода на предмет его соответствия установленным сводам правил и передовым видам практики, разработанным отраслью информационных технологий, мы используем соответствующий автоматизированный инструмент статического анализа кода. Это позволяет обеспечить высокое качество исходного кода, а также непрерывную профессиональную подготовку членов команды по информационным технологиям.

46. Мы также поставили перед собой цель обеспечить индивидуальное тестирование функциональной базы кода на уровне 70 процентов, а также полный набор функциональных не регрессивных тестов, разработанных с помощью приложения «Apache JMeter». Комбинируя эти два вида тестов, мы гарантируем, что каждая часть международной системы eTIR будет работать так, как и планировалось, и тем самым предохраняем себя от возможных случаев регрессии при включении нового кода в нашу кодовую базу.

B. Набор инструментов: список того, что мы считаем полезным

47. В приведенном ниже списке представлены различные программные средства, которые, по нашему мнению, полезны в деле внедрения в практику соответствующего клиентского приложения к международной системе eTIR и с которыми у секретариата МДП есть соответствующий опыт работы:

- приложение для тестирования SOAP-UI: полезный инструмент, позволяющий проводить специальные тесты SOAP-сообщений (просьба иметь в виду, что этот инструмент можно найти в приложении к краткому руководству по использованию SOAP-UI);
- приложение «JMeter» для тестирования: полезный инструмент для автоматизации системы тестирования сообщений, применимый в случае большого количества сценариев;
- система контроля версий GIT: ведущая в отрасли система контроля версий, обеспечивающая правильную версию всех международных системных кодов eTIR и других элементов конфигурации;
- «IntelliJ IDEA» — одна из ведущих в отрасли интегрированных сред разработки (IDE), которая подходит для целого комплекса международных системных технологий eTIR и которая позволила нам повысить эффективность нашей работы в самых разных аспектах;
- инструмент статического анализа кода «SonarQube» — программное обеспечение, используемое для непрерывной проверки качества кода, которое осуществляет автоматический просмотр со статическим анализом кода на предмет выявления ошибок, так называемых «запахов кода» (которые представляют собой порочные методы кодирования), а также уязвимостей безопасности.

48. Просьба иметь в виду, что установка и использование этих приложений не требуется. Тем не менее в процессе внедрения международной системы eTIR эти инструменты для группы секретариата МДП оказались полезными.

C. Генерация заголовков безопасности к SOAP-сообщениям

49. Международная система eTIR основана на обмене веб-сообщениями с использованием протокола SOAP v1.2. Веб-сервис «WS-Security» («ВС-безопасность») в качестве расширения SOAP генерирует элемент заголовка SOAP под названием «Безопасность», который предназначен для работы в качестве своего рода контейнера для хранения всей информации, связанной с безопасностью запросных и ответных SOAP-сообщений. Здесь речь идет о том, каким образом определяется элемент безопасности в схеме «WS-Security» («ВС-безопасность»).

1. Элементы безопасности

50. Элемент заголовка «wsse:Security» является своего рода механизмом включения информации, связанной с безопасностью, которая ориентирована на конкретного получателя, в виде субъекта/роли в оболочке SOAP. Этот элемент представляет собой порядок подписания автором соответствующего сообщения, которого он придерживается в процессе его создания. Это предиктивное правило гарантирует, что принимающее приложение может обрабатывать подэлементы в том порядке, в котором они выстроены в элементе заголовка «wsse:Security», поскольку никакой прямой зависимости между этими подэлементами не будет.

Элемент подписи

Элемент «**Подпись**» является корневым элементом подписи XML.

Определение схемы

```
<element name="Signature" type="ds:SignatureType"/>
  <complexType name="SignatureType">
    <sequence>
      <element ref="ds:SignedInfo"/>
      <element ref="ds:SignatureValue"/>
      <element ref="ds:KeyInfo" minOccurs="0"/>
      <element ref="ds:Object" minOccurs="0" maxOccurs="unbounded"/>
    </sequence>
    <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Пример в сообщении

```
<ds:Signature Id="SIG-AD473EF9595256C9D115409733594021 73"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces PrefixList="SOAP-ENV cus urn"
              xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="#id-AD473EF9595256C9D115409733594011 72">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces PrefixList="cus urn"
                  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>H2Ai···</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>bY65hsJdkxh40···
        </ds:SignatureValue>
        <ds:KeyInfo Id="KI-AD473EF9595256C9D115409733594011 70">
          <wsse:SecurityTokenReference wsu:Id="STR-AD473EF9595256C9D115409733594011 71">
            <wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary"
                                ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3">
              G9w0BAQsFAAN...
            </wsse:KeyIdentifier>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
```

Элемент «Анализ подписи» (SignatureValue)

51. Элемент «Анализ подписи» (электронная цифровая подпись) содержит информацию об открытом ключе отправителя, который необходим международной системе eTIR для подтверждения цифровой подписи вызывающего абонента. Он всегда кодируется в соответствии со стандартом «base64».

Определение схемы

```
<element name="SignatureValue" type="ds:SignatureValueType" />

  <complexType name="SignatureValueType">
    <simpleContent>
      <extension base="base64Binary">
        <attribute name="Id" type="ID" use="optional"/>
      </extension>
    </simpleContent>
  </complexType>
```

Пример в сообщении

```
<ds:SignatureValue>
    bY65hsJdkxh40⋯
</ds:SignatureValue>
```

52. Элемент «Анализ подписи» содержит подпись, которая относится только к элементу «Информация о подписи»: в хэш-сумму подписи включается только содержимое элемента «Информация о подписи».

Элемент «Информация о подписи»

53. Элемент «Информация о подписи» описывает, какая часть сообщения была использована для ее генерации. Ему присваивается атрибут Id, указывающий на основную часть подписанного SOAP-сообщения. Этот момент будет изложен более подробно в следующем элементе «Ссылка» (Reference). Структура элемента «Информация о подписи» включает в себя алгоритм каноникализации, алгоритм подписи и одну или несколько ссылок. Содержание элемента «Информация о подписи» можно разделить на две части: информация об элементе анализа подписи и информация о содержании приложения, как это можно увидеть из следующего фрагмента схемы XML:

Определение схемы

```
<element name="SignedInfo" type="ds:SignedInfoType"/>

  <complexType name="SignedInfoType">
    <sequence>
      <element ref="ds:CanonicalizationMethod"/>
      <element ref="ds:SignatureMethod"/>
      <element ref="ds:Reference" maxOccurs="unbounded"/>
    </sequence>
    <attribute name="Id" type="ID" use="optional"/>
  </complexType>
```

Пример в сообщении

```
<ds:SignedInfo>
  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
    <ec:InclusiveNamespaces PrefixList="SOAP-ENV cus urn"
      xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:CanonicalizationMethod>
  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
  <ds:Reference URI="#id-AD473EF9595256C9D11540973359401172">
    <ds:Transforms>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
        <ec:InclusiveNamespaces PrefixList="cus urn"
          xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>H2Ai⋯</ds:DigestValue>
  </ds:Reference>
</ds:SignedInfo>
```

54. Каноникализация или C14N (эксклюзивная XML-каноникализация) — это процесс выбора только одного способа из всевозможных вариантов вывода, вследствие чего отправитель и получатель могут генерировать одно и то же значение байта, независимо от использованного промежуточного программного обеспечения XML. Элемент «Информация о подписи/Метод каноникализации»

указывает, как воссоздать точный поток байтов. Элемент «Информация о подписи/Метод каноникализации» указывает, какой тип алгоритма (например, протокол «Kerberos» или RSA) используется для генерации подписи. Вместе эти два элемента описывают порядок создания «хэш-суммы» и как ее предохранить от любых модификаций.

55. На языке программирования «Java», ориентированного на клиента, этот порядок можно скомпоновать следующим образом:

```
org.apache.wss4j.dom.message.WSSecSignature wsSecSignature = new WSSecSignature();
//http://www.w3.org/2001/10/xml-exc-c14n#
wsSecSignature.setSigCanonicalization(WSConstants.C14N_EXCL_OMIT_COMMENTS);
//http://www.w3.org/2000/09/xmldsig#rsa-sha1
wsSecSignature.setSignatureAlgorithm(WSConstants.RSA_SHA1);
```

Элемент «Ссылка» (Reference)

56. Элемент «Ссылка» используется для перехода на другой информационный ресурс. Он содержит хэш-сумму содержимого, описание метода генерации этой хэш-суммы (например, посредством использования защищенного алгоритма хэширования SHA1) и точное указание способа преобразования этого содержимого, прежде чем создать хэш-сумму. Это преобразование обеспечивает элемент гибкости при формировании подписи XML.

Определение схемы

```
<element name="Reference" type="ds:ReferenceType"/>

  <complexType name="ReferenceType">
    <sequence>
      <element ref="ds:Transforms" minOccurs="0"/>
      <element ref="ds:DigestMethod"/>
      <element ref="ds:DigestValue"/>
    </sequence>
    <attribute name="Id" type="ID" use="optional"/>
    <attribute name="URI" type="anyURI" use="optional"/>
    <attribute name="Type" type="anyURI" use="optional"/>
  </complexType>
```

Пример в сообщении

```
<ds:Reference URI="#id-AD473EF9595256C9D11540973359401172">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
      <ec:InclusiveNamespaces PrefixList="cus urn"
        xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transform>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <ds:DigestValue>H2Ai…</ds:DigestValue>
</ds:Reference>
```

57. Элемент «Сводный метод» (DigestMethod) задает алгоритм хэширования, а элемент «Сводное значение» (DigestValue) задает значение хэш-суммы содержимого, закодированной с использованием стандарта «base64». Ключевой составляющей элемента «Ссылка» является набор вариантов преобразования, которые можно использовать для этой цели. Элемент «Преобразование» (Transforms) представляет собой список элементов преобразования, каждый из которых задает соответствующий шаг преобразования.

Элемент «Преобразование»

58. Эта схема определяет массив преобразований с одним элементом «XPath» с определенной структурой:

Определение схемы

```
<element name="Transforms" type="ds:TransformsType"/>
  <complexType name="TransformsType">
    <sequence>
      <element ref="ds:Transform" maxOccurs="unbounded"/>
    </sequence>
  </complexType>

<element name="Transform" type="ds:TransformType"/>
  <complexType name="TransformType" mixed="true">
    <choice minOccurs="0" maxOccurs="unbounded">
      <any namespace="##other" processContents="lax"/>
      <element name="XPath" type="string"/>
    </choice>
    <attribute name="Algorithm" type="anyURI" use="required"/>
  </complexType>
```

59. Содержимое в каком-либо элементе «Преобразование» будет зависеть от атрибута «Алгоритм». Например, если используется простой язык разметки XML, то, скорее всего, будет один элемент «Преобразование», который будет задавать алгоритм C14N:

Пример в сообщении

```
<ds:Transforms>
  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
    <ec:InclusiveNamespaces PrefixList="cus urn"
      xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:Transform>
</ds:Transforms>
```

Элемент «Информация о ключе» (KeyInfo)

60. Последним шагом является идентификация стороны с правом подписи или, по крайней мере, ключа, сгенерировавшего подпись (ключа, который предохраняет хэш-сумму от изменения). Эта задача решается с помощью элемента «Информация о ключе»:

Определение схемы

```
<element name="KeyInfo" type="ds:KeyInfoType"/>

  <complexType name="KeyInfoType" mixed="true">
    <choice maxOccurs="unbounded">
      <element ref="ds:KeyName"/>
      <element ref="ds:KeyValue"/>
      <element ref="ds:RetrievalMethod"/>
      <element ref="ds:X509Data"/>
      <element ref="ds:PGPData"/>
      <element ref="ds:SPKIData"/>
      <element ref="ds:MgmtData"/>
      <any processContents="lax" namespace="##other"/>
    </choice>
    <attribute name="Id" type="ID" use="optional"/>
  </complexType>
```

Пример в сообщении

```
<ds:KeyInfo Id="KI-AD473EF9595256C9D11540973359401170">
  <wsse:SecurityTokenReference wsu:Id="STR-AD473EF9595256C9D11540973359401171">
    <wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary"
                        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3">
              G9w0BAQsFAAN...
    </wsse:KeyIdentifier>
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
```

Элемент «Ссылка на маркеры безопасности» (SecurityTokenReference)

61. Операция с цифровой подписью предполагает необходимость указания соответствующего ключа. Элемент, содержащий данный ключ, может находиться в другом месте сообщения или полностью за его пределами. Элемент «Ссылка на

маркеры безопасности» представляет собой соответствующий механизм ссылки на маркеры безопасности и другие ключевые несущие элементы. Элемент «Ссылка на маркеры безопасности» представляет собой модель открытого содержимого для ссылок на ключевые несущие элементы. Он должен содержать либо элемент «Идентификатор ключа» (keyIdentifier), либо элемент «X509Data». Если мы не указываем настройки «Идентификатор ключ» по умолчанию, то элемент «wsse:SecurityTokenReference» будет содержать элемент «X509Data», означающий, что будут приняты оба элемента.

62. Следующая конфигурация позволит установить элемент «Идентификатор ключа» вместо использования элемента «X509Data»:

```
org.apache.wss4j.dom.message.WSSecSignature wsSecSignature = new WSSecSignature();
wsSecSignature.setKeyIdentifierType(WSConstants.X509_KEY_IDENTIFIER);
```

Элемент «Идентификатор ключа» (KeyIdentifier)

63. Маркер следует указывать с помощью элемента «KeyIdentifier». В нижеследующей таблице перечислены как типы кодировки, так и типы значений.

Фрагмент URI-идентификатора	Указатель URL
#Base64Binary	*http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary*
#X509v3	*http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3*

Пример в сообщении

```
<ds:KeyInfo Id="KI-AD473EF9595256C9D115409733594011 70">
  <wsse:SecurityTokenReference wsu:Id="STR-AD473EF9595256C9D115409733594011 71">
    <wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-
1.0#Base64Binary"
                        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3">
        G9w0BAQsFAAN...
    </wsse:KeyIdentifier>
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
```

Элемент «X509Data»

Определение схемы

```
<complexType name="X509IssuerSerialType">
  <sequence>
    <element name="X509IssuerName" type="string"/>
    <element name="X509SerialNumber" type="integer"/>
  </sequence>
</complexType>
```

64. Сертификаты X.509 поддерживаются с помощью элемента ds:X509Data. Этот элемент позволяет лицу с правом подписи встроить свой сертификат (закодированный в соответствии со стандартом «base64») или любой другой альтернативный способ проверки сертификата: имя субъекта, имя эмитента и серийный номер, идентификатор ключа или другой формат. Лицо с правом подписи может также включить текущую копию списка отзыва сертификатов (CRL) с целью подтвердить подлинность лица с правом подписи на момент подписания данного документа.

2. Пример сообщения SOAP eTIR

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:cus="etir:v4.3:customs" xmlns:etir=
"etir:I5:v4.3">
  <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
      xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
      <ds:Signature Id="SIG-AD473EF9595256C9D11540973359402173"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces PrefixList="soap wsa cus etir"
              xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:CanonicalizationMethod>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="#id-AD473EF9595256C9D11540973359401172">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces PrefixList="cus etir"
                  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
              </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>H2Ai···</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>bY65hsJdkxh40···
        </ds:SignatureValue>
        <ds:KeyInfo Id="KI-AD473EF9595256C9D11540973359401170">
          <wsse:SecurityTokenReference wsu:Id="STR-AD473EF9595256C9D11540973359401171">
            <wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3">
              G9w0BAQsFAAN...
            </wsse:KeyIdentifier>
          </wsse:SecurityTokenReference>
        </ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
    <wsa:Action>etir:v4.3:customs/queryGuarantee</wsa:Action>
    <wsa:MessageID>uuid:8a20af11-8170-495d-9563-6a89b32ef745</wsa:MessageID>
  </soap:Header>
  <soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id=
"id-942cd702-1de3-4f27-bfcd-6628ab5d3143">
    <cus:queryGuarantee>
      <etir:InterGov>
        <etir:FunctionCode>9</etir:FunctionCode>
        <etir:ID>656dbce8-e810-44ec-8f3d-5f8a9b425d99</etir:ID>
        <etir:TypeCode>I5</etir:TypeCode>
        <etir:ReplyTypeCode>00</etir:ReplyTypeCode>
        <etir:ObligationGuarantee>
          <etir:ReferenceID>XC95xxxxxx</etir:ReferenceID>
        </etir:ObligationGuarantee>
      </etir:InterGov>
    </cus:queryGuarantee>
  </soap:Body>
</soap:Envelope>
```

D. Введение в практику идентификатора сообщения/функциональной ссылки

1. Общие положения

65. Все отправленные и полученные сообщения однозначно идентифицируются с использованием поля «Message Identifier» (Идентификатор сообщения). Это поле должно быть установлено отправителем в запросном сообщении. Получатель устанавливает еще одно уникальное значение для поля «Идентификатор сообщения» ответного сообщения. В дополнение к этому получатель также устанавливает поле «Функциональная справка» для ответного сообщения со значением поля «Идентификатор сообщения» соответствующего запросного сообщения. Этот метод позволяет полностью отслеживать запросные/ответные сообщения.

2. Запросное сообщение

66. Получатель должен установить в сообщении поле «Идентификатор сообщения», используя следующий формат:

```
SenderID:UUID
```

67. Где:

- SenderID («Идентификатор отправителя»): уникальная величина, которая идентифицирует отправителя. Эта величина должно быть такой же, как и величина, установленная в поле сообщения «Идентификация отправителя».
- UUID: универсальный уникальный идентификатор v4, подробно описанный в стандарте RFC 4122. Версия 4 основана на псевдослучайных числах, в связи с чем для снижения вероятности коллизии сообщений, отправляемых различными субъектами eTIR, «Идентификатор отправителя» необходимо сохранить.

68. Для генерации UUID v4 основные языки программирования предусматривают оригинальные вспомогательные классы v4:

На языке программирования «Java»

```
java.util.UUID.randomUUID();
```

На языке программирования C#

```
System.Guid.NewGuid();
```

69 Здесь приведены некоторые примеры действительные значения поля «**Идентификатор сообщения»**:

Пример 1

```
<urn:ID>CustomsCountryA:6aca5f82-2285-4f00-b4ae-36269d4cc865</urn:ID>
```

Пример 2

```
<urn:ID>eTIRInternationalSystem:1486e5b7-c6ae-4d27-b794-44c4bf545fb3</urn:ID>
```

3. Ответное сообщение

70. Получатель получает запросное сообщение от отправителя и сохраняет значение поля «Идентификатор сообщения». При подготовке ответного сообщения получатель устанавливает новое значение поля для «Идентификатора сообщения» этого сообщения тем же способом, который описан выше. Затем сохраненное значение поля «Идентификатора сообщения» запросного сообщения устанавливается на «Функциональную ссылку» ответного сообщения, которое готовится в данный момент.

E. Оформление полей даты

71. Сообщения eTIR содержат несколько полей, в которые необходимо ввести даты. В случае некоторых из этих полей формат включает только дату, в то время как в случае ряда других полей — также время. В этом разделе более подробно объясняется, как правильно заполнять эти поля.

1. Поля только с датами

72. В файлах «XML Schema Definition (XSD)» этот тип называется «EtirDateType» и определяется наряду с родственными типами, которые ему предшествовали, следующим образом.

Определение «EtirDateType»

```
<xs:complexType name="EtirDateType">
  <xs:simpleContent>
    <xs:extension base="ds:DateTimeType_102_S">
      <xs:attribute name="formatCode" use="optional">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="102"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:simpleType name="DateTimeType_102_S">
  <xs:restriction base="ds:DateTimeType_S">
    <xs:pattern value="[1-9][0-9][0-9][0-9](([0][1|3|5|7|8])([0][1-9]|[1-2][0-9]|[3][0-1])|([0][4|6|9])([0][1-9]|[1-
2][0-9]|[3][0])|([0][2])([0][1-9]|[1-2][0-9])|([1][0|2])([0][1-9]|[1-2][0-9]|[3][0-1])|([1][1])([0][1-9]|[1-2][0-
9]|[3][0]))"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="DateTimeType_S">
  <xs:restriction base="xs:string">
    <xs:pattern value=".{1,35}"/>
  </xs:restriction>
</xs:simpleType>
```

73. Формат этого типа даты указывается в соответствии с кодом 102 формата ЭДИФАКТ ООН: CCYYMMDD,

где:

- год — четыре цифры. Примеры: 1979, 2020;
- MM: месяц — две цифры с 01 по 12 начиная с 01 для января;
- DD: день месяца — две цифры с 01 по 31.

Примеры:

- 01 января 1970 года кодируется как «19700101»;
- 29 февраля 2020 года кодируется как «20200229»;
- 31 декабря 2045 года кодируется как «20451231».

74. Поле даты также содержит необязательный атрибут под названием «formatCode» (код формата), значение которого во всех случаях одно и то же — «102». В этом формате нет понятия часового пояса, поэтому указанная дата должна считаться действительной во всех часовых поясах.

Следующий XML-код показывает только примерное поле даты.

Истечение гарантии 01 августа 2024 года

```
<ExpirationDateTime formatCode="102">20240801</ExpirationDateTime>
```

2. Поля только с датами

75. В файлах «XML Schema Definition (XSD)» этот тип называется «EtirDateTimeType» и определяется наряду с родственными типами, которые ему предшествовали, следующим образом:

Определение «EtirDateTimeType»

```
<xs:complexType name="EtirDateTimeType">
  <xs:simpleContent>
    <xs:extension base="ds:DateTimeType_208_S">
      <xs:attribute name="formatCode" use="optional">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="208"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
<xs:simpleType name="DateTimeType_208_S">
  <xs:restriction base="ds:DateTimeType_S">
    <xs:pattern value="[1-9][0-9][0-9][0-9](([0][1|3|5|7|8])([0][1-9]|[1-2][0-9]|[3][0-1])|([0][4|6|9])([0][1-9]|[1-
2][0-9]|[3][0])|([0][2])([0][1-9]|[1-2][0-9])|([1][0|2])([0][1-9]|[1-2][0-9]|[3][0-1])|([1][1])([0][1-9]|[1-2][0-
9]|[3][0]))([0-1][0-9])|(2[0-3]))[0-5][0-9](([0-5][0-9]|60))[\-+]((0[0-9])|(1[0-4]))[0-5][0-9]"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="DateTimeType_S">
  <xs:restriction base="xs:string">
    <xs:pattern value=".{1,35}"/>
  </xs:restriction>
</xs:simpleType>
```

76. Формат этого типа даты указывается в соответствии с кодом 208 формата ЭДИФАКТ ООН: CCYYMMDDHHMMSSZHHMM,

при этом данные позиции определяются в следующем порядке:

- год — четыре цифры. Примеры: 1979, 2020;
- ММ: месяц — две цифры с 01 по 12 начиная с 01 для января;
- ДД: день месяца — две цифры с 01 по 31.
- НН: час дня — две цифры с 00 (для полуночи) до 23 (для одиннадцати вечера);
- ММ: минуты дня — две цифры: с 00 до 59;
- SS: секунды дня — две цифры: с 00 до 59; 60 также допускается в случае скачка на секунду;
- Z: введение часового пояса в виде а “ или а '-'. Если смещения в данном часовом поясе нет, то можно использовать либо '-', либо “;
- НН: смещение в часах в данном часовом поясе от 01 до 14;
- ММ: смещение в минутах в данном часовом поясе от 00 до 59.

Примеры:

- 01 января 1970 года 00:00:00 в Лондоне (сдвиг по времени: +00:00) кодируется как «19700101000000+0000»;
- 29 февраля 2020 года 09:45:36 в Нью-Йорке (сдвиг по времени: –05:00) кодируется как «20200229094536-0500»;
- 31 декабря 2045 года 22:06:59 в Южной Тараве, Кирибати (сдвиг по времени: +14:00) кодируется как «20451231220659+1400».

77. Поле даты также содержит необязательный атрибут под названием «**formatCode**» (код формата), значение которого во всех случаях одно и то же — «208».

Следующий XML-код показывает только примерное поле даты.

Принятие гарантии 01 июля 2021 года 10:03:42 в Стамбуле (сдвиг по времени +03:00).

```
<ExpirationDateTime formatCode="102">20210701100342+0300</ExpirationDateTime>
```

F. Обработка ошибок

1. Введение к позиции «обработка ошибок»

78. Когда международная система eTIR получает и обрабатывает соответствующее сообщение, она производит ряд проверок на валидацию самого сообщения с учетом гарантии, держателя или перевозки и выдает ответ системе, которая отправила сообщение первой. Если в процессе проверки выявится какая-либо нестыковка, то в ответ будет отправлен соответствующий перечень ошибок. Каждая из этих ошибок оформляется в виде кода ошибки с указателем, который может быть использован для указания на определенный XML-элемент сообщения. Список всех кодов ошибок доступен на странице кодов ошибок (eTIR).

2. Оформление кодов ошибок

79. В случае eTIR перечень кодов ошибок носит специфичный характер, поскольку он позволяет ИТ-командам лучше понять ошибки, которые возникают в момент подключения к международной системе eTIR. Это должно привести к более оперативному введению данной системы в практику в целом и к более точной обработке ошибок в сообщениях, отправленных данной системой в международную систему eTIR. Кроме того, подробная система кодов ошибок позволит значительно упростить коммуникацию между заинтересованными сторонами и службой поддержки eTIR в случае какого-либо инцидента в целях выявления и урегулирования лежащей в его основе проблемы. Перечень кодов ошибок составлен на основе передового опыта ИТ-индустрии. Как и перечень кодов статуса HTTP, все коды ошибок состоят из трех цифр, причем тип ошибки определяется первой цифрой кода статуса:

- **1XX — Валидация**: валидация сообщения и его параметров;
- **2XX — Рабочий процесс**: проблемы, связанные с рабочим процессом;
- **3XX — Функциональные сбои**: другие функциональные проблемы;
- **4XX — Внутренние сбои**: внутренние проблемы международной системы eTIR.

80. Каждому типу ошибки присваивается соответствующий код ошибки по умолчанию, который указывает, как минимум, тип ошибки, если система не может послать более точное определение типа ошибки.

3. Примеры ошибок

81. Ниже приведен пример возврата одной ошибки:

Отсутствие требуемого элемента

```
<ns14:Error>
   <ns14:ValidationCode>101</ns14:ValidationCode>
   <ns14:Pointer>
      <ns14:SequenceNumeric>1</ns14:SequenceNumeric>
      <ns14:Location>/InterGov/ObligationGuarantee/ReferenceID</ns14:Location>
   </ns14:Pointer>
</ns14:Error>
```

82. В данном случае «ValidationCode» (код валидации) — это код ошибки, а элемент «DocumentSectionCode» (код раздела документа) внутри элемента «Pointer» (указатель) указывает на проблемный элемент запроса, использующий синтаксис XPath.

83. В случае возврата нескольких ошибок одного типа международная система eTIR возвращает один элемент ошибки со списком соответствующих элементов указателя.

Пример кратной нехватки требуемого элемента

```
<ns14:Error>
   <ns14:ValidationCode>101</ns14:ValidationCode>
   <ns14:Pointer>
      <ns14:SequenceNumeric>1</ns14:SequenceNumeric>
      <ns14:Location>/InterGov/ObligationGuarantee/ReferenceID</ns14:Location>
   </ns14:Pointer>
   <ns14:Pointer>
      <ns14:SequenceNumeric>2</ns14:SequenceNumeric>
      <ns14:Location>/InterGov/ObligationGuarantee/Surety/ID</ns14:Location>
   </ns14:Pointer>
</ns14:Error>
```

84. В заключение в качестве примера ниже приведен полный ответ на сообщение I1 — Принять сообщение о гарантии, содержащее несколько ошибок.

Пример полной позиции I2 — Результаты принятия основной части сообщения с возвратом кратных ошибок

```
<soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
          wsu:Id="id-30706360-7e18-4764-b080-05364eb55892">
    <ns3:acceptanceResults xmlns:ns4="etir:I2:v4.3" xmlns:ns5="etir:MetaData_DS:v4.3" >
        <ns4:InterGov>
            <ns4:FunctionCode>27</ns4:FunctionCode>
            <ns4:FunctionalReferenceID>bc26c1b8-7392-4d44-9899-317fd72206eb</ns4:FunctionCode>
            <ns4:TypeCode>I2</ns4:TypeCode>
            <ns4:Error>
               <ns5:ValidationCode>102</ns5:ValidationCode>
               <ns5:Pointer>
                  <ns5:SequenceNumeric>1</ns5:SequenceNumeric>
                  <ns5:Location>/InterGov/FunctionCode</ns5:Location>
               </ns5:Pointer>
               <ns5:Pointer>
                  <ns5:SequenceNumeric>2</ns5:SequenceNumeric>
                  <ns5:Location>/InterGov/TypeCode</ns5:Location>
               </ns5:Pointer>
            </ns4:Error>
            <ns4:Error>
               <ns5:ValidationCode>101</ns5:ValidationCode>
               <ns5:Pointer>
                  <ns5:SequenceNumeric>3</ns5:SequenceNumeric>
                  <ns5:Location>/InterGov/ObligationGuarantee/ReferenceID</ns5:Location>
               </ns5:Pointer>
               <ns5:Pointer>
                  <ns5:SequenceNumeric>4</ns5:SequenceNumeric>
                  <ns5:Location>/InterGov/ObligationGuarantee/Surety/ID</ns5:Location>
               </ns5:Pointer>
            </ns4:Error>
        </ns4:InterGov>
    </ns3:acceptanceResults>
</soap:Body>
```

4. Обработка ошибок

85. Каждая национальная таможенная система, которая связана с международной системой eTIR, должна надлежащим образом обрабатывать ошибки, возвращаемые в ответном сообщении. В процессе введения в практику различных парных сообщений eTIR разработчикам было бы удобно обратить внимание на страницу кодов ошибок eTIR, особенно на столбец «Замечания» в таблицах, и посмотреть, какие коды ошибок можно было бы применить. В процессе получения сообщений из международной системы eTIR с ошибками следует обращаться таким образом, чтобы соответствующая информация передавалась в соответствующие национальные таможенные системы. Поскольку все ошибки носят критический характер и означают неспособность обработать данное сообщение, пользователи национальных таможенных систем должны предпринять соответствующие последующие действия.

86. То же самое относится и к национальным таможенным системам, которые могут отправлять ошибки обратно в международную систему eTIR при получении запросов, на которые они не могут отреагировать должным образом (это может иметь место в случае следующих пар сообщений: I15/I16, E9/E10, E11/E12 и E13/E14). Национальные таможенные системы должны следовать тем же спецификациям, которые детально изложены выше: в тот момент, когда они направляют в международную систему eTIR ответные сообщения, они должны доводить до ее сведения и допущенные ошибки.