О внесении изменений в Положение об удостоверяющем центре службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза

Решение Коллегии Евразийской экономической комиссии от 24 декабря 2025 года № 136

В соответствии с пунктами 18 и 30 Протокола об информационно-коммуникационных технологиях и информационном взаимодействии в рамках Евразийского экономического союза (приложение № 3 к Договору о Евразийском экономическом союзе от 29 мая 2014 года) Коллегия Евразийской экономической комиссии **решила:**

1. Внести в Положение об удостоверяющем центре службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза, утвержденное Решением Коллегии Евразийской экономической комиссии от 25 сентября 2018 г. № 154, изменения согласно приложению.

2. Настоящее Решение вступает в силу по истечении 30 календарных дней с даты его официального опубликования.

Председатель Коллегии
Евразийской экономической комиссии *Б. Сагинтаев*

ПРИЛОЖЕНИЕ
к Решению Коллегии
Евразийской экономической комиссии
от 24 декабря 2025 г. № 136

ИЗМЕНЕНИЯ,
вносимые в Положение об удостоверяющем центре службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза

1. По тексту слово "выпуск" в соответствующем падеже заменить словом "издание" в соответствующем падеже, слово "выпущенный" в соответствующих числе и падеже заменить словом "изданный" в соответствующих числе и падеже.

2. Пункт 3 после абзаца первого дополнить абзацами следующего содержания:

"внешний сервис штампов времени" – сервис штампов времени удостоверяющего центра службы ДТС, предназначенный для использования внешними доверенными третьими сторонами;

"внешняя доверенная третья сторона" – уполномоченная доверенная третья сторона государства-члена, не входящая в состав интегрированной информационной системы Союза;".

3. В пункте 9:

1) в подпункте "е" слово "созданных" заменить словом "изданных";

2) в подпункте "и" слово "созданных" заменить словом "изданных", слово " выпущены" заменить словом "изданы".

4. В Регламенте удостоверяющего центра службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза (приложение к указанному Положению):

1) в абзацах пятом, седьмом и тринадцатом пункта 1.2.1 слово "создание" в соответствующем падеже заменить словом "издание" в соответствующем падеже;

2) в абзаце седьмом пункта 1.2.2 слово "изготовление" заменить словом "издание";

3) абзац десятый пункта 1.2.2.1 изложить в следующей редакции:

"Внешние доверенные третьи стороны (далее – ДТС-В) являются смежными системами по отношению к службе ДТС и в целях взаимной проверки подлинности сертификатов ключей проверки ЭЦП сервиса ДТС-В используют списки отозванных сертификатов, предоставляемые УЦ службы ДТС.";

4) пункт 1.2.3 изложить в следующей редакции:

"1.2.3. Использование сертификатов

УЦ службы ДТС издает следующие типы сертификатов ключей проверки ЭЦП, которые используются операторами ДТС:

сертификаты ключей проверки ЭЦП сервиса сертификации УЦ службы ДТС (сертификаты уполномоченных лиц УЦ и корневые сертификаты УЦ) – предназначены для проверки ЭЦП в сертификатах и списках отозванных сертификатов;

сертификаты ключей проверки ЭЦП сервиса подтверждения подлинности (далее – СПП) – предназначены для проверки ЭЦП в квитанциях и идентификации сервера СПП, сервера СПП ДТС-В. Такие сертификаты также используются для проверки подписи запросов на издание и отзыв сертификатов, поступающих в УЦ службы ДТС от операторов ДТС и ДТС-В;

сертификаты ключей проверки ЭЦП сервиса проверки статуса сертификата (далее – СПСС) – предназначены для проверки ЭЦП в ответах, выдаваемых СПСС;

сертификаты ключей проверки ЭЦП сервиса штампов времени (далее – СШВ) – предназначены для проверки ЭЦП в штампах времени, выдаваемых СШВ интеграционного и национальных сегментов интегрированной системы;

сертификаты ключей проверки ЭЦП СПП ДТС-В – предназначены для проверки ЭЦП в квитанциях и идентификации сервера СПП ДТС-В. Такие сертификаты также используются для проверки подписи запросов на издание и отзыв сертификатов, поступающих в УЦ службы ДТС от операторов ДТС-В;

сертификаты ключей проверки ЭЦП внешнего сервиса штампов времени (далее – СШВ-В) – предназначены для проверки ЭЦП в штампах времени, выдаваемых СШВ-В для ДТС-В;

сертификаты ключей проверки ЭЦП сервиса штампов времени внешней доверенной третьей стороны (далее – СШВ ДТС-В) – предназначены для проверки ЭЦП в штампах времени, выдаваемых СШВ ДТС-В.

Сертификаты, издаваемые УЦ службы ДТС, запросы на издание таких сертификатов и списки отозванных сертификатов создаются по шаблонам согласно приложению № 1.

Использование сертификатов, изданных УЦ службы ДТС, должно осуществляться в соответствии с их предназначением, определенным настоящим Регламентом и утверждаемыми руководителем УЦ службы ДТС политиками применения сертификатов.

При каждой проверке действительности сертификатов, изданных УЦ службы ДТС, соответствующим сервисом ДТС должен проводиться анализ (разбор) сертификата с обязательной проверкой всех полей, в том числе всех критических и некритических расширений.";

5) в пункте 2:

абзац третий дополнить словами ", внешний сервис штампов времени";

в предложении втором абзаца двенадцатого слово "создание" заменить словом " издание";

абзац тринадцатый изложить в следующей редакции:

"Сервис сертификации обеспечивает хранение эталонной базы сертификатов ключей проверки ЭЦП и СОС. Сервис используется для формирования ключей ЭЦП, записи ключевой информации на ключевые носители, создания и обработки запросов на издание и изменение статуса сертификатов ключей проверки ЭЦП, издания сертификатов ключей проверки ЭЦП и СОС.";

в абзаце восемнадцатом слова "СДТС Комиссии" заменить словами " уполномоченных ДТС Комиссии и государств-членов", слово "созданных" заменить словом "изданных";

в абзаце двадцать третьем слово "создание" заменить словом "издание";

6) пункт 3 изложить в следующей редакции:

"3. Права и обязанности УЦ службы ДТС

УЦ службы ДТС имеет право:

отказать в принятии заявления и издании сертификата, если заявителем представлены документы не в полном объеме в соответствии с настоящим Регламентом , документы содержат неполную и (или) некорректную информацию, представленные документы имеют признаки фальсификации;

отказать в принятии запроса на издание сертификата, если средства ЭЦП, при помощи которых сгенерированы ключи и запрос, не совместимы со средствами ЭЦП УЦ службы ДТС;

отказать в издании сертификата в следующих случаях:

информация о заявителе, содержащаяся в запросе на издание сертификата, не соответствует сведениям, указанным в заявлении на издание сертификата;

срок действия ключа ЭЦП, содержащегося в запросе, не соответствует требованиям настоящего Регламента;

формат запроса на издание сертификата не отвечает требованиям, установленным настоящим Регламентом;

отказать в отзыве сертификата, если владелец не прошел аутентификацию при запросе на отзыв или истек установленный срок действия соответствующего ключа ЭЦП.

УЦ службы ДТС обязан:

использовать ключ ЭЦП администратора сертификации только для формирования ЭЦП в издаваемых сертификатах и СОС;

обеспечивать конфиденциальность ключа ЭЦП уполномоченного лица УЦ службы ДТС;

предоставлять пользователям УЦ службы ДТС сертификат уполномоченного лица в форме электронного документа;

поддерживать СОС в актуальном состоянии в соответствии с настоящим Регламентом;

обеспечивать уникальность серийных номеров и ключей проверки ЭЦП в издаваемых сертификатах;

отозвать сертификат по запросу его владельца в минимально возможный срок в соответствии с настоящим Регламентом;

опубликовать настоящий Регламент в репозитории УЦ и актуализировать его в случае изменений.";

7) в пункте 4:

абзац четырнадцатый дополнить словами ", не указывать в качестве окончания срока действия ключа ЭЦП значение, которое соответствует более поздней дате, чем дата окончания срока действия ключа ЭЦП, соответствующего корневому сертификату УЦ службы ДТС";

абзац шестнадцатый дополнить словами ", изданных УЦ службы ДТС";

абзац восемнадцатый после слов "уведомить УЦ" дополнить словами "службы ДТС ";

8) в пункте 9.1:

абзац третий после слов "службы ДТС" дополнить словами ", а также организаций-операторов уполномоченных ДТС, не входящих в состав интегрированной системы, взаимодействующих с УЦ службы ДТС,";

абзацы четвертый и пятый изложить в следующей редакции:

"Заявления на издание сертификатов СПП (СПП ДТС-В), СШВ (СШВ ДТС-В) могут подаваться только уполномоченными сотрудниками организации-оператора ДТС (ДТС-В).

При подаче заявлений на издание сертификата СПП (СПП ДТС-В), СШВ (СШВ ДТС-В) уполномоченным сотрудником организации-оператора ДТС (ДТС-В) учитывается наличие в ДТС основного и резервного серверов сервисов ДТС (ДТС-В). Для обеспечения сертификатами сервисов одной ДТС в УЦ службы ДТС подаются 4 заявления:";

9) пункт 9.2 после абзаца четвертого дополнить абзацем следующего содержания:

"дата окончания срока действия ключа ЭЦП не превышает дату окончания срока действия ключа ЭЦП соответствующего корневого сертификата;";

10) пункты 10.1 – 10.3 изложить в следующей редакции:

"10.1. Издание сертификата СПП (СПП ДТС-В)

При издании сертификата СПП (СПП ДТС-В) заявитель предоставляет в УЦ службы ДТС файл запроса в установленном формате, сгенерированный заявителем непосредственно на сервере функционирования СПП (СПП ДТС-В). Администратор сертификации УЦ службы ДТС проверяет наличие идентификационной информации из заявления в базе данных УЦ службы ДТС и осуществляет издание сертификата на основе файла запроса.

10.2. Издание сертификата СПСС

При издании сертификата СПСС заявитель предоставляет в УЦ службы ДТС файл запроса в установленном формате, сгенерированный заявителем непосредственно на сервере СПСС. Администратор сертификации УЦ службы ДТС проверяет наличие идентификационной информации из заявления в базе данных УЦ службы ДТС и осуществляет издание сертификата на основе файла запроса.

10.3. Издание сертификата СШВ (СШВ-В, СШВ ДТС-В)

При издании сертификата СШВ (СШВ-В, СШВ ДТС-В) заявитель предоставляет в УЦ службы ДТС файл запроса в установленном формате, сгенерированный заявителем непосредственно на сервере функционирования СШВ (СШВ-В, СШВ ДТС-В). Администратор сертификации УЦ службы ДТС проверяет наличие идентификационной информации из заявления в базе данных УЦ службы ДТС и осуществляет издание сертификата на основе файла запроса.";

11) в пункте 10.4 по тексту слова "о выпуске" заменить словами "об издании";

12) в пункте 11.3 по тексту слово "создания" заменить словом "издания";

13) пункт 12.1 изложить в следующей редакции:

"12.1. Ключ и сертификат СПП (СПП ДТС-В)

Ключ ЭЦП СПП (СПП ДТС-В) используется исключительно для формирования ЭЦП в квитанциях проверки ЭЦП и запросах на проверку к СПП (СПП ДТС-В).

Сертификат СПП (СПП ДТС-В) включается в состав квитанций, запросов и используется для проверки ЭЦП в данных квитанциях и запросах, а также для идентификации сервера СПП (СПП ДТС-В).";

14) в абзацах первом и втором пункта 12.2 слово "сервера" исключить;

15) пункт 12.3 изложить в следующей редакции:

"12.3. Ключ и сертификат СШВ (СШВ-В)

Ключ ЭЦП СШВ (СШВ-В) используется только для формирования ЭЦП в штампах времени, выдаваемых службой по запросам ДТС (ДТС-В).

Сертификат СШВ (СШВ-В) включается в состав выдаваемых штампов времени и используется для проверки ЭЦП в штампах времени и идентификации службы.";

16) в предложении втором абзаца второго пункта 13 и абзаце втором пункта 17.1 слово "выпускается" заменить словом "издается";

17) предложение первое абзаца второго пункта 17.2 после слов "службы ДТС" дополнить словами "и на информационном портале Союза в информационно-коммуникационной сети "Интернет";

18) пункт 20.2 изложить в следующей редакции:

"20.2. Доступность сервисов. Балансировка нагрузки на серверы УЦ службы ДТС

Услуги по проверке статусов сертификатов доступны 24 часа в сутки, 7 дней в неделю.

Сервисы СОС, СШВ, СШВ-В и СПСС УЦ службы ДТС одновременно функционируют на нескольких серверах УЦ службы ДТС, каждый из которых предоставляет для указанных сервисов отдельные адреса для приема запросов от ДТС интеграционного и национальных сегментов интегрированной системы. Список адресов каждого сервиса УЦ службы ДТС приведен в таблице 1.

Таблица 1

Адреса сервисов УЦ службы ДТС

Сервис	Адреса для приема запросов
СОС	http://ca-srv1.dts.eec/public/RootTTPCA<индекс сертификата УЦ службы ДТС>.crl http://ca-srv2.dts.eec/public/RootTTPCA<индекс сертификата УЦ службы ДТС>.crl
СОС для ДТС-В	http://pki.eaeunion.org/public/RootTTPCA<индекс сертификата УЦ службы ДТС>.crl
СШВ	http://ca-srv1.dts.eec/tsp http://ca-srv2.dts.eec/tsp
СПСС	http://ca-srv1.dts.eec/ocsp http://ca-srv2.dts.eec/ocsp
СШВ-В	http://pki.eaeunion.org/tsa

Равномерное распределение запросов между серверами УЦ службы ДТС при обращении к сервисам СОС, СШВ, СШВ-В и СПСС осуществляется с использованием

HTTP-сервера, работающего в режиме балансировщика нагрузки с применением метода наименьшего числа соединений (Least Connections) (далее – балансировщик нагрузки). Метод работает путем маршрутизации каждого нового запроса к сервисам СОС, СШВ, СШВ-В и СПСС на сервер УЦ службы ДТС с наименьшим количеством активных соединений в данный момент времени.

Выбор сервера УЦ службы ДТС для обработки очередного запроса осуществляется в следующем порядке:

балансировщик нагрузки отслеживает количество активных соединений на каждом сервере УЦ службы ДТС;

при поступлении нового запроса к сервису СОС, СШВ, СШВ-В или СПСС балансировщик проверяет текущее количество активных соединений на каждом сервере УЦ службы ДТС;

балансировщик нагрузки направляет запрос на сервер УЦ службы ДТС с наименьшим количеством активных соединений;

по мере завершения запроса и закрытия соединения балансировщик нагрузки обновляет свои записи для отражения текущего количества соединений на каждом сервере УЦ службы ДТС.

Применение механизма балансировки позволяет достичь равномерности нагрузки на серверы УЦ службы ДТС и уменьшить время обработки каждого запроса к сервисам СОС, СШВ, СШВ-В и СПСС.";

19) пункт 22 изложить в следующей редакции:

"22. Репозиторий

Репозиторий является совокупностью файлов и каталогов, размещенных на сервере УЦ службы ДТС.

Вся информация, опубликованная УЦ службы ДТС в репозитории, доступна по следующим адресам:

http://ca-srv1.dts.eec;

http://ca-srv2.dts.eec.

Репозиторий содержит следующую информацию:

все изданные УЦ службы ДТС сертификаты;

актуальные СОС;

политики применения сертификатов, утвержденные руководителем УЦ службы ДТС;

актуальная версия настоящего Регламента.

Информация в репозитории публикуется со следующей периодичностью:

сертификаты, изданные УЦ службы ДТС, – непосредственно сразу после издания сертификата;

СОС – не реже 1 раза в 3 месяца и немедленно в случае отзыва ранее изданных сертификатов;

актуальные версии настоящего Регламента и политик применения сертификатов – после их утверждения.

УЦ службы ДТС использует механизмы защиты, предотвращающие несанкционированное добавление, удаление или изменение записей в репозитории.

Доступ к репозиторию обеспечивается 24 часа в сутки, 7 дней в неделю из национальных и интеграционного сегментов интегрированной системы через защищенную сеть передачи данных.

УЦ службы ДТС предоставляет доступ к репозиторию по протоколу HTTP/1.1 (RFC 2616).

Актуальные СОС для ДТС-В доступны в информационно-коммуникационной сети "Интернет" по адресу: http://pki.eaeunion.org.";

20) в пункте 23.1.1:

в абзаце четвертом слова "таблице 1" заменить словами "таблице 2";

после абзаца четвертого слова "Таблица 1" заменить словами "Таблица 2";

в таблице 1 позицию "CommonName (CN)" в графе второй изложить в следующей редакции:

"значение поля зависит от политики, в соответствии с которой издан сертификат:

<наименование сервиса ДТС> – сертификат сервиса подтверждения подлинности;

<наименование сервиса ДТС-В> – сертификат сервиса подтверждения подлинности ДТС-В;

<псевдоним СПСС> – сертификат сервиса проверки статуса сертификата;

<псевдоним СШВ> – сертификат службы штампов времени;

<псевдоним СШВ-В> – сертификат службы внешнего сервиса штампов времени;

<псевдоним СШВ ДТС-В> – сертификат службы штампов времени ДТС-В;

<фамилия, имя, отчество> – сертификат администратора или оператора";

21) в абзаце втором пункта 23.1.2 слово "выпускает" заменить словом "издает";

22) в абзаце первом пункта 23.2.1 слово "сервера" исключить;

23) в пункте 26.1:

абзацы четвертый и пятый изложить в следующей редакции:

"сохранение запроса на издание сертификата ключа проверки ЭЦП в базу данных центра регистрации;

импорт запроса на издание сертификата ключа проверки ЭЦП;";

абзац седьмой изложить в следующей редакции:

"отклонение запроса на издание сертификата ключа проверки ЭЦП;";

24) в абзаце третьем пункта 29 слова "на СДТС" исключить;

25) в абзаце пятом пункта 32.1.3 по тексту слово "сертификат" заменить словами " издание сертификата";

26) в абзаце третьем пункта 32.1.4 слово "выпускаемых" заменить словом " издаваемых";

27) пункт 32.1.14 изложить в следующей редакции:

"32.1.14. Сроки действия ключей ЭЦП и сертификатов

Срок действия ключа ЭЦП, соответствующего корневому сертификату ключа проверки ЭЦП (сертификату уполномоченного лица УЦ службы ДТС), составляет 3 года.

Срок действия ключей ЭЦП иных сертификатов ключа проверки ЭЦП, издаваемых УЦ службы ДТС, ограничивается сроком действия ключа ЭЦП, соответствующего корневому сертификату УЦ службы ДТС, но не может превышать 3 лет.

Срок действия корневого сертификата ключа проверки ЭЦП составляет 7 лет.

Срок действия иных сертификатов ключа проверки ЭЦП, издаваемых УЦ службы ДТС, ограничивается сроком действия соответствующего корневого сертификата УЦ службы ДТС, но не может превышать 7 лет.

Технические средства УЦ службы ДТС запрещают издание сертификатов ключа проверки ЭЦП по запросам, в которых указана более поздняя дата окончания срока действия ключа ЭЦП, чем дата окончания срока действия ключа ЭЦП соответствующего корневого сертификата УЦ службы ДТС.";

28) в абзаце втором пункта 34 слова "QP OC" исключить;

29) приложение № 1 к указанному Регламенту изложить в следующей редакции:

"ПРИЛОЖЕНИЕ № 1
к Регламенту
удостоверяющего центра
службы доверенной третьей
стороны интегрированной
информационной системы
Евразийского экономического союза
(в редакции Решения Коллегии
Евразийской экономической комиссии
от 24 декабря 2025 г. № 136)

ШАБЛОНЫ
запросов на издание сертификатов, сертификатов и списка отозванных сертификатов

I. Шаблон запроса на издание сертификата

1. Запрос на издание сертификата ключа проверки электронной цифровой подписи (электронной подписи) (далее соответственно – сертификат, ЭЦП) представляет собой структуру в формате PKCS #10 (RFC2986) и является последовательностью трех полей, из которых первое содержит основное тело запроса (certificationRequestInfo), второе – информацию о типе алгоритма, использованного для подписания запроса на издание сертификата (signatureAlgorithm), а третье – ЭЦП, которой подписан запрос (signatureValue).

2. Запрос на издание сертификата удостоверяющего центра (далее – УЦ) службы доверенной третьей стороны интегрированной информационной системы Евразийского

экономического союза (далее – служба ДТС) содержит как минимум следующие основные поля:

а) Version: первая версия (v1(0)) формата запроса на издание сертификата;

б) Subject: уникальное имя (DN) конечного пользователя, получающего сертификат;

в) Subject Public Key Info: значение открытого ключа вместе с идентификатором алгоритма;

г) Attributes: коллекция атрибутов, которые могут содержать информацию о расширениях, сохраняемых в сертификат.

3. Значения основных полей и расширений запроса на издание сертификата определяются назначением сертификата и политикой его применения.

4. Структура запроса на издание сертификата сервиса подтверждения подлинности (далее – СПП) приведена в таблице 1.

Таблица 1

Структура запроса на издание сертификата СПП

Название поля (OID)	Значение или ограничения значения
Version (версия)	Version 1
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN, OID 2.5.4.3) = <Наименование сервиса ДТС>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора программно-аппаратного комплекса доверенной третьей стороны >
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
Key Usage (использование ключа) – содержится в Attributes (OID 2.5.29.15)	critical, digitalSignature, nonRepudiation
Extended Key Usage (расширенная область использования ключа) – содержится в Attributes (OID 2.5.29.37)	critical, id-kp-dvcs (OID 1.3.6.1.5.5.7.3.10)

privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject Key Identifier – содержится в Attributes (OID 2.5.29.14)	уникальный идентификатор открытого ключа субъекта
signatureAlgorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Signature (подпись)	подпись запроса на издание сертификата генерируется и кодируется в соответствии с требованиями, определенными в RFC 2986

5. Структура запроса на издание сертификата СПП внешней доверенной третьей стороны (далее – ДТС-В) приведена в таблице 2.

Таблица 2

Структура запроса на издание сертификата СПП ДТС-В

Название поля (OID)	Значение или ограничения значения
Version (версия)	Version 1
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN, OID 2.5.4.3) = <Наименование сервиса ДТС-В>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора программно-аппаратного комплекса доверенной третьей стороны> Country (C, OID 2.5.4.6) = <код страны в соответствии с ГОСТ 7.67-2003>
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа субъекта: 1024 бит; значение открытого ключа субъекта
Key Usage (использование ключа) – содержится в Attributes (OID 2.5.29.15)	critical, digitalSignature, nonRepudiation
Extended Key Usage (расширенная область использования ключа) – содержится в Attributes (OID 2.5.29.37)	critical, id-kp-dvcs (OID 1.3.6.1.5.5.7.3.10)

privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject Key Identifier – содержится в Attributes (OID 2.5.29.14)	уникальный идентификатор открытого ключа субъекта
signatureAlgorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Signature (подпись)	подпись запроса на издание сертификата генерируется и кодируется в соответствии с требованиями, определенными в RFC 2986

6. Структура запроса на издание сертификата сервиса проверки статуса сертификата (далее – СПСС) приведена в таблице 3.

Таблица 3

Структура запроса на издание сертификата СПСС

Название поля (OID)	Значение или ограничения значения
Version (версия)	Version 1
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN, OID 2.5.4.3) = <Псевдоним СПСС>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора OCSP сервера>
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
Key Usage (использование ключа) – содержится в Attributes (OID 2.5.29.15)	critical, digitalSignature, nonRepudiation,
Extended Key Usage (расширенная область использования ключа) – содержится в Attributes (OID 2.5.29.37)	critical, id-kp-OCSPSigning (OID 1.3.6.1.5.5.7.3.9)
privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT

Subject Key Identifier – содержится в Attributes (OID 2.5.29.14)	уникальный идентификатор открытого ключа субъекта
signatureAlgorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Signature (подпись)	подпись запроса на издание сертификата генерируется и кодируется в соответствии с требованиями, определенными в RFC 2986

7. Структура запроса на издание сертификата сервиса штампов времени (далее – СШВ) приведена в таблице 4.

Таблица 4

Структура запроса на издание сертификата СШВ

Название поля (OID)	Значение или ограничения значения
Version (версия)	Version 1
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN, OID 2.5.4.3) = <Псевдоним СШВ>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора TSP сервера>
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
Key Usage (использование ключа) – содержится в Attributes (OID 2.5.29.15)	critical, digitalSignature, nonRepudiation,
Extended Key Usage (расширенная область использования ключа) – содержится в Attributes (OID 2.5.29.37)	critical, id-kp-timeStamping (OID 1.3.6.1.5.5.7.3.8)
privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject Key Identifier – содержится в Attributes (OID 2.5.29.14)	уникальный идентификатор открытого ключа субъекта
signatureAlgorithm	

(алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Signature (подпись)	подпись запроса на издание сертификата генерируется и кодируется в соответствии с требованиями, определенными в RFC 2986

8. Структура запроса на издание сертификата внешнего сервиса штампов времени (далее – СШВ-В) приведена в таблице 5.

Таблица 5

Структура запроса на издание сертификата СШВ-В

Название поля (OID)	Значение или ограничения значения
Version (версия)	Version 1
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN, OID 2.5.4.3) = <Псевдоним СШВ-В>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора TSP сервера> Country (C, OID 2.5.4.6) = <код страны в соответствии с ГОСТ 7.67-2003>
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
Key Usage (использование ключа) – содержится в Attributes (OID 2.5.29.15)	critical, digitalSignature, nonRepudiation,
Extended Key Usage (расширенная область использования ключа) – содержится в Attributes (OID 2.5.29.37)	critical, id-kp-timeStamping (OID 1.3.6.1.5.5.7.3.8)
privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject Key Identifier – содержится в Attributes (OID 2.5.29.14)	уникальный идентификатор открытого ключа субъекта
signatureAlgorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)

Signature (подпись)	подпись запроса на издание сертификата генерируется и кодируется в соответствии с требованиями, определенными в RFC 2986

9. Структура запроса на издание сертификата СШВ ДТС-В приведена в таблице 6.

Таблица 6

Структура запроса на издание сертификата СШВ ДТС-В

Название поля (OID)	Значение или ограничения значения
Version (версия)	Version 1
Subject (субъект, имя DN)	имя DN соответствует требованиям X.501. Common Name (CN, OID 2.5.4.3) = <Псевдоним СШВ ДТС-В>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора TSP сервера> Country (C, OID 2.5.4.6) = <код страны в соответствии с ГОСТ 7.67-2003>
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
Key Usage (использование ключа) – содержится в Attributes (OID 2.5.29.15)	critical, digitalSignature, nonRepudiation,
Extended Key Usage (расширенная область использования ключа) – содержится в Attributes (OID 2.5.29.37)	critical, id-kp-timeStamping (OID 1.3.6.1.5.5.7.3.8)
privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject Key Identifier – содержится в Attributes (OID 2.5.29.14)	уникальный идентификатор открытого ключа субъекта
signatureAlgorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Signature (подпись)	подпись запроса на издание сертификата генерируется и кодируется в соответствии с требованиями, определенными в RFC 2986

II. Шаблон сертификата ключа проверки ЭЦП

1. Структура сертификата ключа проверки ЭЦП

10. Сертификат в соответствии со стандартом X.509 v.3 является электронным документом, состоящим из последовательности трех полей, из которых первое содержит содержимое сертификата (tbsCertificate), второе – информацию о типе алгоритма, использованного для подписания сертификата (signatureAlgorithm), а третье – ЭЦП, которой подписан сертификат (signatureValue).

11. Сертификаты УЦ службы ДТС содержат как минимум следующие основные поля:

а) Version: третья версия формата сертификата (X.509 v.3);

б) Serial Number: серийный номер сертификата, уникальный в рамках УЦ;

в) signatureAlgorithm: идентификатор алгоритма, применяемого УЦ, издающим сертификаты, для подписания сертификата;

г) Issuer: уникальное имя (DN) УЦ;

д) Validity: срок действия сертификата, определенный началом (notBefore) и окончанием (notAfter) действия сертификата;

е) Subject: уникальное имя (DN) конечного пользователя, получающего сертификат;

ж) Subject Public Key Info: значение открытого ключа вместе с идентификатором алгоритма;

з) Signature: подпись генерируется и кодируется в соответствии с RFC 5280.

12. Значения основных полей и расширений сертификата определяются его назначением и политикой применения.

13. Значения основных полей и расширений сертификата уполномоченного лица УЦ службы ДТС приведены в таблице 7.

Таблица 7

Структура сертификата уполномоченного лица УЦ службы ДТС

Название поля (OID)	Значение или ограничения значения
Базовые поля сертификата	
Version (версия)	V3
Serial Number (серийный номер)	уникальный серийный номер сертификата
signatureAlgorithm (алгоритм ЭЦП)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (издатель сертификата)	Common Name (CN, OID 2.5.4.3) = УЦ службы ДТС, Organization (O, OID 2.5.4.10) = ЕЭК, Organization Unit (OU, OID 2.5.4.11) = ИТ, Country (C, OID 2.5.4.6) = RU

Validity (срок действия сертификата)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject (субъект, владелец сертификата)	Common Name (CN, OID 2.5.4.3) = УЦ службы ДТС, Organization (O, OID 2.5.4.10) = ЕЭК, Organization Unit (OU, OID 2.5.4.11) = ИТ, mailAddress (E, OID 1.2.840.113549.1.9.1) = info@eecommission.org
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
signatureValue (ЭЦП издателя сертификата)	подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата	
Subject Key Identifier (идентификатор ключа проверки ЭЦП субъекта) (OID 2.5.29.14)	идентификатор ключа проверки ЭЦП уполномоченного лица УЦ службы ДТС, соответствующего данному сертификату
Key Usage (использование ключа) (OID 2.5.29.15)	critical, keyCertSign (5), cRLSign (6)
Basic Constraints (основные ограничения) (OID 2.5.29.19)	critical, Тип субъекта=ЦС, ограничение на длину пути=0
CA version (версия УЦ) (OID 1.3.6.1.4.1.311.21.1)	v<индекс сертификата УЦ службы ДТС>.<индекс пары ключей сертификата УЦ службы ДТС>

14. Значения основных полей и расширений сертификата СПП приведены в таблице 8.

Таблица 8

Структура сертификата СПП

Название поля (OID)	Значение или ограничения значения
Базовые поля сертификата	
Version (версия)	V3
Serial Number (серийный номер)	уникальный серийный номер сертификата
signatureAlgorithm (алгоритм ЭЦП)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
	Common Name (CN, OID 2.5.4.3) = УЦ службы ДТС,

Issuer (издатель сертификата)	Organization (O, OID 2.5.4.10) = ЕЭК, Organization Unit (OU, OID 2.5.4.11) = ИТ, Country (C, OID 2.5.4.6) = RU
Validity (срок действия сертификата)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT. действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject (субъект, владелец сертификата)	Common Name (CN, OID 2.5.4.3) = <Наименование сервиса ДТС>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора сервиса доверенной третьей стороны>
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
signatureValue (ЭЦП издателя сертификата)	подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата	
Authority Information Access (доступ к информации об УЦ) (OID 1.3.6.1.5.5.7.1.1)	[1] Доступ к сведениям центра сертификации метод доступа=Протокол определения состояния сертификата через сеть (OID 1.3.6.1.5.5.7.48.1) Дополнительное имя: http://ca-srv1.dts.eec/ocsp [2] Доступ к сведениям центра сертификации Метод доступа=Протокол определения состояния сертификата через сеть (OID 1.3.6.1.5.5.7.48.1) Дополнительное имя: http://ca-srv2.dts.eec/ocsp
Subject Key Identifier (идентификатор ключа проверки ЭЦП субъекта) (OID 2.5.29.14)	уникальный идентификатор ключа проверки ЭЦП субъекта
Key Usage (использование ключа) (OID 2.5.29.15)	critical, digitalSignature (0), nonRepudiation (1)
Extended Key Usage (расширенная область использования ключа) (OID 2.5.29.37)	critical, id-kp-dvcs (OID 1.3.6.1.5.5.7.3.10)

privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Basic Constraints (основные ограничения) (OID 2.5.29.19)	тип субъекта=Конечный субъект
CRL Distribution Points (точка распространения СОС) (OID 2.5.29.31)	точки распространения списков отзыва (CRL) [1] Точка распределения списка отзыва (CRL) имя точки распространения: полное имя: http://ca-srv1.dts.eec/public/RootTTPCA <индекс сертификата УЦ службы ДТС>.crl, [2] Точка распределения списка отзыва (CRL) имя точки распространения: полное имя: http://ca-srv2.dts.eec/public/RootTTPCA <индекс сертификата УЦ службы ДТС>.crl
Certificate Policies (политика сертификата) (OID 2.5.29.32)	[1] Политика применения сертификата: OID=1.3.239.1.1.1.1. URL= http://ca-srv1.dts.eec/public/cps.pdf URL= http://ca-srv2.dts.eec/public/cps.pdf
Authority Key Identifier (идентификатор ключа проверки ЭЦП издателя) (OID 2.5.29.35)	идентификатор ключа проверки ЭЦП, соответствующий ключу ЭЦП издателя сертификата

15. Значения основных полей и расширений сертификата СПП ДТС-В приведены в таблице 9.

Таблица 9

Структура сертификата СПП ДТС-В

Название поля (OID)	Значение или ограничения значения
Базовые поля сертификата	
Version (версия)	V3
Serial Number (серийный номер)	уникальный серийный номер сертификата
signatureAlgorithm (алгоритм ЭЦП)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (издатель сертификата)	Common Name (CN, OID 2.5.4.3) = УЦ службы ДТС, Organization (O, OID 2.5.4.10) = ЕЭК, Organization Unit (OU, OID 2.5.4.11) = ИТ, Country (C, OID 2.5.4.6) = RU
Validity (срок действия сертификата)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT

Subject (субъект, владелец сертификата)	Common Name (CN, OID 2.5.4.3) = <Наименование сервиса ДТС-В>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора сервиса доверенной третьей стороны> Country (C, OID 2.5.4.6) = <код страны в соответствии с ГОСТ 7.67-2003>
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
signatureValue (ЭЦП издателя сертификата)	подпись издателя в соответствии с ГОСТ Р 34.11/ 34.10-2012
Расширения сертификата	
Subject Key Identifier (идентификатор ключа проверки) ЭЦП субъекта (OID 2.5.29.14)	уникальный идентификатор ключа проверки ЭЦП субъекта
Key Usage (использование ключа) (OID 2.5.29.15)	critical, digitalSignature (0), nonRepudiation (1)
Extended Key Usage (расширенная область использования ключа) (OID 2.5.29.37)	critical, id-kp-dvcs (OID 1.3.6.1.5.5.7.3.10)
privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Basic Constraints (основные ограничения) (OID 2.5.29.19)	тип субъекта=Конечный субъект
CRL Distribution Points (точка распространения СОС) (OID 2.5.29.31)	точки распространения списков отзыва (CRL) [1]Точка распределения списка отзыва (CRL) имя точки распространения: полное имя: http://pki.eaeunion.org/public/RootTTPCA <индекс сертификата УЦ службы ДТС>.crl,
Certificate Policies (политика сертификата) (OID 2.5.29.32)	[1] Политика применения сертификата: OID=1.3.239.1.1.1.4 URL= http://pki.eaeunion.org/public/cps.pdf
Authority Key Identifier	

(идентификатор ключа проверки ЭЦП издателя) (OID 2.5.29.35)	идентификатор ключа проверки ЭЦП, соответствующий ключу ЭЦП издателя сертификата

16. Значения основных полей и расширений сертификата СПСС приведены в таблице 10.

Таблица 10

Структура сертификата СПСС

Название поля (OID)	Значение или ограничения значения
Базовые поля сертификата	
Version (версия)	V3
Serial Number (серийный номер)	уникальный серийный номер сертификата
signatureAlgorithm (алгоритм ЭЦП)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (издатель сертификата)	Common Name (CN, OID 2.5.4.3) = УЦ службы ДТС, Organization (O, OID 2.5.4.10) = ЕЭК, Organization Unit (OU, OID 2.5.4.11) = ИТ, Country (C, OID 2.5.4.6) = RU
Validity (срок действия сертификата)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject (субъект, владелец сертификата)	Common Name (CN, OID 2.5.4.3) = <Псевдоним СПСС>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора OCSP сервера>
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
signatureValue (ЭЦП издателя сертификата)	подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата	
Authority Information Access (доступ к информации об УЦ)	[1] Доступ к сведениям центра сертификации метод доступа=Протокол определения состояния сертификата через сеть (OID 1.3.6.1.5.5.7.48.1). дополнительное имя: http://ca-srv1.dts.eec/ocsp

(OID 1.3.6.1.5.5.7.1.1)	[2] Доступ к сведениям центра сертификации метод доступа=Протокол определения состояния сертификата через сеть (OID 1.3.6.1.5.5.7.48.1) дополнительное имя: http://ca-srv2.dts.eec/ocsp
Subject Key Identifier (идентификатор ключа проверки ЭЦП субъекта) (OID 2.5.29.14)	уникальный идентификатор ключа проверки ЭЦП субъекта
Key Usage (использование ключа) (OID 2.5.29.15)	critical, digitalSignature (0), nonRepudiation (1)
privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Basic Constraints (основные ограничения) (OID 2.5.29.19)	тип субъекта=Конечный субъект
CRL Distribution Points (точка распространения СОС) (OID 2.5.29.31)	[1] Точка распределения списка отзыва (CRL) имя точки распространения: полное имя: http://ca-srv1.dts.eec/public/RootTTPCA <индекс сертификата УЦ службы ДТС>.crl, [2] Точка распределения списка отзыва (CRL) имя точки распространения: полное имя: http://ca-srv2.dts.eec/public/RootTTPCA <индекс сертификата УЦ службы ДТС>.crl
Certificate Policies (политика сертификата) (OID 2.5.29.32)	[1] Политика применения сертификата: OID=1.3.239.1.1.1.2 URL= http://ca-srv1.dts.eec/public/cps.pdf URL= http://ca-srv2.dts.eec/public/cps.pdf
Authority Key Identifier (идентификатор ключа проверки ЭЦП издателя) (OID 2.5.29.35)	идентификатор ключа проверки ЭЦП, соответствующий ключу ЭЦП издателя сертификата
Extended Key Usage (расширенная область использования ключа) (OID 2.5.29.37)	critical, id-kp-OCSPSigning (OID 1.3.6.1.5.5.7.3.9)

17. Значения основных полей и расширений сертификата СШВ приведены в таблице 11.

Таблица 11

Структура сертификата СШВ

Название поля (OID)	Значение или ограничения значения
Базовые поля сертификата	
Version (версия)	V3
Serial Number	

(серийный номер)	уникальный серийный номер сертификата
signatureAlgorithm (алгоритм ЭЦП)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (издатель сертификата)	Common Name (CN, OID 2.5.4.3) = УЦ службы ДТС, Organization (O, OID 2.5.4.10) = ЕЭК, Organization Unit (OU, OID 2.5.4.11) = ИТ, Country (C, OID 2.5.4.6) = RU
Validity (срок действия сертификата)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject (субъект, владелец сертификата)	Common Name (CN, OID 2.5.4.3) = <Псевдоним СШВ>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора TSP- сервера>
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
signatureValue (ЭЦП издателя сертификата)	подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата	
Authority Information Access (доступ к информации об УЦ) (OID 1.3.6.1.5.5.7.1.1)	[1] Доступ к сведениям центра сертификации метод доступа=Протокол определения состояния сертификата через сеть (OID 1.3.6.1.5.5.7.48.1) дополнительное имя: http://ca-srv1.dts.eec/ocsp [2] Доступ к сведениям центра сертификации метод доступа=Протокол определения состояния сертификата через сеть (OID 1.3.6.1.5.5.7.48.1) дополнительное имя: http://ca-srv2.dts.eec/ocsp
Subject Key Identifier (идентификатор ключа проверки ЭЦП субъекта) (OID 2.5.29.14)	уникальный идентификатор ключа проверки ЭЦП субъекта
Key Usage (назначение ключа) (OID 2.5.29.15)	critical, digitalSignature (0), nonRepudiation (1)

privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Basic Constraints (основные ограничения) (OID 2.5.29.19)	тип субъекта=Конечный субъект
CRL Distribution Points (точка распространения СОС) (OID 2.5.29.31)	[1] Точка распределения списка отзыва (CRL) имя точки распространения: полное имя: http://ca-srv1.dts.eec/public/RootTTPCA <индекс сертификата УЦ службы ДТС>.crl, [2] Точка распределения списка отзыва (CRL) имя точки распространения: полное имя: http://ca-srv2.dts.eec/public/RootTTPCA <индекс сертификата УЦ службы ДТС>.crl
Certificate Policies (политика сертификата) (OID 2.5.29.32)	[1] Политика применения сертификата: OID=1.3.239.1.1.1.3 URL= http://ca-srv1.dts.eec/public/cps.pdf URL= http://ca-srv2.dts.eec/public/cps.pdf
Authority Key Identifier (идентификатор ключа проверки ЭЦП издателя) (OID 2.5.29.35)	идентификатор ключа проверки ЭЦП, соответствующий ключу ЭЦП издателя сертификата
Extended Key Usage (расширенная область использования ключа) (OID 2.5.29.37)	critical, id-kp-timeStamping (OID 1.3.6.1.5.5.7.3.8)

18. Значения основных полей и расширений сертификата СШВ-В приведены в таблице 12.

Таблица 12

Структура сертификата СШВ-В

Название поля (OID)	Значение или ограничения значения
Базовые поля сертификата	
Version (версия)	V3
Serial Number (серийный номер)	уникальный серийный номер сертификата
signatureAlgorithm (алгоритм ЭЦП)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (издатель сертификата)	Common Name (CN, OID 2.5.4.3) = УЦ службы ДТС, Organization (O, OID 2.5.4.10) = ЕЭК, Organization Unit (OU, OID 2.5.4.11) = ИТ, Country (C, OID 2.5.4.6) = RU
Validity	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT,

(срок действия сертификата)	действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject (субъект, владелец сертификата)	Common Name (CN, OID 2.5.4.3) = <Псевдоним СШВ-В>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора TSP- сервера> Country (C, OID 2.5.4.6) = <код страны в соответствии с ГОСТ 7.67-2003>
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
signatureValue (ЭЦП издателя сертификата)	подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата	
Subject Key Identifier (идентификатор ключа проверки ЭЦП субъекта) (OID 2.5.29.14)	уникальный идентификатор ключа проверки ЭЦП субъекта
Key Usage (назначение ключа) (OID 2.5.29.15)	critical, digitalSignature (0), nonRepudiation (1)
privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Basic Constraints (основные ограничения) (OID 2.5.29.19)	тип субъекта=Конечный субъект
CRL Distribution Points (точка распространения СОС) (OID 2.5.29.31)	[1] Точка распределения списка отзыва (CRL) имя точки распространения: полное имя: http://pki.eaeunion.org/public/RootTTPCA <индекс сертификата УЦ службы ДТС>.crl
Certificate Policies (политика сертификата) (OID 2.5.29.32)	[1] Политика применения сертификата: OID=1.3.239.1.1.1.5 URL= http://pki.eaeunion.org/public/cps.pdf
Authority Key Identifier (идентификатор ключа проверки ЭЦП издателя) (OID 2.5.29.35)	идентификатор ключа проверки ЭЦП, соответствующий ключу ЭЦП издателя сертификата
Extended Key Usage	

(расширенная область использования ключа) (OID 2.5.29.37)	critical, id-kp-timeStamping (OID 1.3.6.1.5.5.7.3.8)

19. Значения основных полей и расширений сертификата СШВ ДТС-В приведены в таблице 13.

Таблица 13

Структура сертификата СШВ ДТС-В

Название поля (OID)	Значение или ограничения значения
Базовые поля сертификата	
Version (версия)	V3
Serial Number (серийный номер)	уникальный серийный номер сертификата
signatureAlgorithm (алгоритм ЭЦП)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (издатель сертификата)	Common Name (CN, OID 2.5.4.3) = УЦ службы ДТС, Organization (O, OID 2.5.4.10) = ЕЭК, Organization Unit (OU, OID 2.5.4.11) = ИТ, Country (C, OID 2.5.4.6) = RU
Validity (срок действия сертификата)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Subject (субъект, владелец сертификата)	Common Name (CN, OID 2.5.4.3) = <Псевдоним СШВ ДТС-В>, Organization (O, OID 2.5.4.10) = <Сокращенное наименование организации>, Organization Unit (OU, OID 2.5.4.11) = < Наименование подразделения>, mailAddress (E, OID 1.2.840.113549.1.9.1) = <адрес электронной почты администратора TSP- сервера> Country (C, OID 2.5.4.6) = <код страны в соответствии с ГОСТ 7.67-2003>
Subject Public Key Info (открытый ключ субъекта)	идентификатор открытого ключа: id-tc26-gost3410-2012-512 (OID 1.2.643.7.1.1.1.2); параметры открытого ключа: id-tc26-gost-3410-2012-512-paramSetA (OID 1.2.643.7.1.2.1.2.1), id-tc26-gost3411-2012-512 (OID 1.2.643.7.1.1.2.3); длина открытого ключа: 1024 бит; значение открытого ключа
signatureValue (ЭЦП издателя сертификата)	подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения сертификата	
Subject Key Identifier (идентификатор ключа проверки ЭЦП субъекта) (OID 2.5.29.14)	уникальный идентификатор ключа проверки ЭЦП субъекта

Key Usage (назначение ключа) (OID 2.5.29.15)	critical, digitalSignature (0), nonRepudiation (1)
privateKeyUsagePeriod (срок действия ключа ЭЦП субъекта) (OID 2.5.29.16)	действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT, действителен по (notAfter): дд.мм.гггг чч:мм:сс GMT
Basic Constraints (основные ограничения) (OID 2.5.29.19)	тип субъекта=Конечный субъект
CRL Distribution Points (точка распространения СОС) (OID 2.5.29.31)	[1] Точка распределения списка отзыва (CRL) имя точки распространения: полное имя: http://pki.eaeunion.org/public/RootTTPCA <индекс сертификата УЦ службы ДТС>.crl
Certificate Policies (политика сертификата) (OID 2.5.29.32)	[1] Политика применения сертификата: OID=1.3.239.1.1.1.6 URL= http://pki.eaeunion.org/public/cps.pdf
Authority Key Identifier (идентификатор ключа проверки ЭЦП издателя) (OID 2.5.29.35)	идентификатор ключа проверки ЭЦП, соответствующий ключу ЭЦП издателя сертификата
Extended Key Usage (расширенная область использования ключа) (OID 2.5.29.37)	critical, id-kp-timeStamping (OID 1.3.6.1.5.5.7.3.8)

2. Номер версии

20. Все сертификаты издаются УЦ службы ДТС в соответствии с версией X.509 v.3.

3. Расширения сертификата

21. Функция каждого расширения сертификата определена стандартным значением связанного с ним идентификатора объекта (object identifier). Расширение сертификата в зависимости от опции, выбранной УЦ службы ДТС, может быть критическим или некритическим. Приложение, использующее сертификаты, должно отклонять сертификат, если обнаруживает критическое расширение, которое оно не может распознать. Каждое некритическое расширение сертификата может игнорироваться.

22. Версия УЦ (CA version)

Расширение "CA Version" (OID 1.3.6.1.4.1.311.21.1) предназначено для обеспечения связанности изданных УЦ службы ДТС сертификатов, а также списков отозванных сертификатов (далее – СОС) с сертификатом уполномоченного лица УЦ службы ДТС, ключом ЭЦП которого они были подписаны, и используется только в сертификате уполномоченного лица УЦ службы ДТС.

Расширение имеет формат "v<индекс сертификата УЦ службы ДТС>.<индекс пары ключей сертификата УЦ службы ДТС>". При установке УЦ службы ДТС (первичном

издании сертификата уполномоченного лица УЦ службы ДТС) индекс сертификата УЦ службы ДТС равен нулю, а индекс пары ключей сертификата УЦ службы ДТС – "" (пустая строка). Каждый раз, когда сертификат уполномоченного лица УЦ службы ДТС обновляется, индекс сертификата УЦ службы ДТС увеличивается на единицу. В связи с тем, что регламент УЦ службы ДТС предусматривает обновление сертификатов уполномоченного лица УЦ службы ДТС только с использованием новой пары ключей, индекс пары ключей всегда принимает значение индекса сертификата УЦ службы ДТС.

23. Использование ключа (Key Usage)

Расширение "Использование ключа" может быть критическим или некритическим. Данное расширение определяет способ применения ключа (например, ключ для шифрования данных, ключ для ЭЦП и т. д.). Значение данного расширения зависит от назначения сертификата и политики его применения.

В сертификате уполномоченного лица УЦ службы ДТС расширение " Использование ключа" помечается как критическое (critical) и имеет следующие значения:

keyCertSign (5) – ключ для подписи сертификатов;

cRLSign (6) – ключ для подписи СОС.

В сертификате СПП расширение "Использование ключа" помечается как критическое (critical) и имеет следующие значения:

digitalSignature (0) – ключ для реализации ЭЦП (идентификации субъекта или данных);

nonRepudiation (1) – ключ, связанный с реализацией неотрекаемости.

В сертификате СПСС расширение "Использование ключа" помечается как критическое (critical) и имеет следующие значения:

digitalSignature (0) – ключ для реализации ЭЦП (идентификации субъекта или данных);

nonRepudiation (1) – ключ, связанный с реализацией неотрекаемости.

В сертификатах СШВ, СШВ-В и СШВ ДТС-В расширение "Использование ключа" помечается как критическое (critical) и имеет следующие значения:

digitalSignature (0) – ключ для реализации ЭЦП (идентификации субъекта или данных);

nonRepudiation (1) – ключ, связанный с реализацией неотрекаемости.

24. Расширенная область использования ключа (Extended Key Usage)

Расширение "Расширенная область использования ключа" может быть критическим или некритическим. Данное расширение определяет одну или более областей в дополнение к основному применению, установленному в поле Key Usage, в пределах которых может быть использован сертификат. Данное поле следует интерпретировать

как ограничение допустимой области применения ключа, определенного в поле Key Usage. Конкретные значения расширения зависят от назначения сертификата и политики его применения.

В сертификате уполномоченного лица УЦ службы ДТС расширение "Расширенная область использования ключа" не используется.

В сертификатах СПП и СПП ДТС-В расширение "Расширенная область использования ключа" помечается как критическое и содержит объектный идентификатор назначения "Подпись ответов службы DVCS" (id-kp-dvcs): OID 1.3.6.1.5.5.7.3.10.

В сертификате СПСС расширение "Расширенная область использования ключа" помечается как критическое и содержит объектный идентификатор назначения " Подпись ответов службы OCSP" (id-kp-OCSPSigning): OID 1.3.6.1.5.5.7.3.9.

В сертификатах СШВ, СШВ-В и СШВ ДТС-В расширение "Расширенная область использования ключа" помечается как критическое и содержит объектный идентификатор назначения "Подпись штампов времени" (id-kp-timeStamping): OID 1.3.6.1.5.5.7.3.8.

25. Основные ограничения (Basic Constraints)

Расширение "Основные ограничения" является критическим в сертификатах УЦ и может быть критическим или некритическим в сертификатах конечных пользователей. Расширение позволяет определить, является ли субъект сертификата УЦ (поле CA), а также сколько максимально (принимая иерархическую систематизацию УЦ) может быть УЦ на пути, ведущем от рассматриваемого УЦ до конечного пользователя (поле pathLength).

Значение поля pathLength, равное 0, означает, что сертификат принадлежит УЦ, который может издавать сертификаты только для конечных пользователей.

В сертификатах СПП, СПП ДТС-В, СПСС, СШВ, СШВ-В и СШВ ДТС-В в расширение "Основные ограничения" вносится пустая последовательность без указания в ней поля CA и поля pathLength.

26. Точки доступа к СОС (CRL Distribution Points)

Расширение "Точки доступа к СОС" не является критическим. Поле определяет протоколы и сетевые адреса, по которым можно получить актуальный СОС, выданный издателем сертификата, в котором находится данное расширение.

27. Доступ к информации об УЦ (Authority Information Access)

Расширение "Доступ к информации об УЦ" не является критическим. Поле указывает, каким образом передаются данные и услуги издателем сертификата, в сертификате которого имеется данное расширение. Данное расширение содержит URL адреса услуги OCSP проверки статуса сертификата.

28. Идентификатор ключа проверки ЭЦП издателя (Authority Key Identifier)

Расширение "Идентификатор ключа проверки ЭЦП издателя" позволяет однозначно идентифицировать ключ проверки ЭЦП, соответствующий ключу ЭЦП, используемому для подписи сертификата. Расширение используется для облегчения построения путей сертификации.

29. Идентификатор ключа проверки ЭЦП субъекта (Subject Key Identifier)

Расширение "Идентификатор ключа проверки ЭЦП субъекта" позволяет однозначно идентифицировать ключ проверки ЭЦП, содержащийся в сертификате. Используется для построения цепочек доверия и управления процессами отзыва сертификатов.

30. Идентификатор алгоритма (signatureAlgorithm)

Расширение "Идентификатор алгоритма" содержит идентификатор криптографического алгоритма, описывающего алгоритм, применяемый для реализации ЭЦП, которую ставит УЦ службы ДТС на сертификате.

Для сертификатов, издаваемых УЦ службы ДТС, поле имеет следующее значение:

id-tc26-gost3410-2012-512 OBJECT IDENTIFIER ::= id-tc26-signwithdigest-gost3410-2012-512 OBJECT IDENTIFIER ::= { iso(1) member-body(2) ru(643) rosstandart(7) tc26(1) algorithms(1) signwithdigest(3) gost3410-2012-512(3) }.

31. Формы имен

УЦ службы ДТС издает сертификаты, содержащие имена издателя и субъекта, издаваемые в соответствии с правилами, описанными в Регламенте удостоверяющего центра службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза.

32. Политики применения сертификата (Certificate Policies)

Расширение "Политики применения сертификата" (Certificate Policies) содержит информацию типа PolicyInformation (идентификатор, электронный адрес) о политике, используемой УЦ службы ДТС, для издания сертификата. Расширение "Политики применения сертификата" не является критическим.

В сертификатах, издаваемых УЦ службы ДТС, возможно указание идентификаторов политик применения сертификата в зависимости от типа и назначения сертификата, представленных в таблице 14.

Таблица 14

Идентификаторы политик применения сертификата

Идентификатор политики	Краткое наименование политики применения сертификата	Полное наименование политики применения сертификата
1.3.239.1.1.1.1	политика применения сертификатов СПП	УЦ службы ДТС интегрированной информационной системы Евразийского экономического союза. Политика применения сертификатов ключей проверки ЭЦП СПП

1.3.239.1.1.1.2	политика применения сертификатов СПСС	УЦ службы ДТС интегрированной информационной системы Евразийского экономического союза. Политика применения сертификатов ключей проверки ЭЦП СПСС
1.3.239.1.1.1.3	политика применения сертификатов СШВ	УЦ службы ДТС интегрированной информационной системы Евразийского экономического союза. Политика применения сертификатов ключей проверки ЭЦП СШВ
1.3.239.1.1.1.4	политика применения сертификатов СПП ДТС-В	УЦ службы ДТС интегрированной информационной системы Евразийского экономического союза. Политика применения сертификатов ключей проверки ЭЦП СПП ДТС, не входящей в состав интегрированной информационной системы
1.3.239.1.1.1.5	политика применения сертификатов СШВ-В	УЦ службы ДТС интегрированной информационной системы Евразийского экономического союза. Политика применения сертификатов ключей проверки ЭЦП СШВ, предназначенного для использования ДТС, не входящими в состав интегрированной информационной системы
1.3.239.1.1.1.6	политика применения сертификатов СШВ ДТС-В	УЦ службы ДТС интегрированной информационной системы Евразийского экономического союза. Политика применения сертификатов ключей проверки ЭЦП СШВ ДТС, не входящих в состав интегрированной информационной системы

В сертификатах СПП, СПП ДТС-В, СПСС, СШВ, СШВ-В и СШВ ДТС-В, издаваемых УЦ службы ДТС, содержатся квалификаторы политик применения сертификата в виде указателей на опубликованные в репозитории УЦ службы ДТС политики применения сертификатов, утвержденные руководителем УЦ службы ДТС.

III. Список отозванных сертификатов

1. Структура СОС

33. УЦ службы ДТС формирует СОС (CRL) в электронной форме в формате, основанном на рекомендациях ITU-T X.509v3 и RFC 5280.

СОС состоит из последовательности трех полей. Первое поле (tbsCertList) содержит информацию об отозванных сертификатах, второе (signatureAlgorithm) и третье (signatureValue) поля – соответственно информацию о типе алгоритма, примененного для подписания списка и ЭЦП, которая ставится на сертификате УЦ службы ДТС. Значение двух последних полей полностью совпадает, как и в сертификате. Информационное поле tbsCertList является последовательностью обязательных и опциональных полей. Обязательные поля идентифицируют издателя СОС, а необязательные содержат информацию об отозванных сертификатах и расширениях СОС.

Значения основных полей и расширений СОС приведены в таблице 15.

Таблица 15

Структура СОС

Название поля (OID)	Значение или ограничения значения
Базовые поля	
Version (версия)	V2
signatureAlgorithm (алгоритм подписи)	ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.3.3)
Issuer (издатель СОС)	Common Name (CN, OID 2.5.4.3) = УЦ службы ДТС, Organization (O, OID 2.5.4.10) = ЕЭК, Organization Unit (OU, OID 2.5.4.11) = ИТ, Country (C, OID 2.5.4.6) = RU
thisUpdate (время издания СОС)	дд.мм.гггг чч:мм:сс GMT
nextUpdate (время, по которое действителен СОС)	дд.мм.гггг чч:мм:сс GMT
revokedCertificates (СОС)	последовательность элементов следующего вида: 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на отзыв сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) в соответствии с RFC 5280: "1" Компрометация ключа (keyCompromise); "5" Прекращение работы (cessationOfOperation)
signatureValue (ЭЦП издателя СОС)	подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения СОС	
CA version (версия УЦ) (OID 1.3.6.1.4.1.311.21.1)	v<индекс сертификата УЦ службы ДТС>. <CRL и индекс ключа службы ДТС>
cRLNumber	

(номер СОС) (OID 2.5.29.20)	последовательно увеличиваемый номер СОС
Authority Key Identifier (идентификатор ключа проверки ЭЦП издателя) (OID 2.5.29.35)	идентификатор ключа проверки ЭЦП издателя СОС

2. Номер версии

34. СОС, издаваемые УЦ службы ДТС, соответствуют X.509 v2.

3. Расширения СОС

35. Среди множества расширений CRL самыми важными являются расширения Authority Key Identifier и cRLNumber.

Поле Authority Key Identifier позволяет идентифицировать ключ проверки ЭЦП, соответствующий ключу ЭЦП, примененному для подписания СОС.

Поле cRLNumber содержит постепенно увеличиваемый номер списка CRL, издаваемого УЦ службы ДТС, что позволяет определить, когда один CRL заменил другой CRL.

IV. Служба СПСС

36. Служба СПСС применяется УЦ службы ДТС и позволяет определить состояние сертификата с использованием протокола проверки статуса сертификата в оперативном режиме (OCSP). Структура запросов и ответов СПСС соответствует RFC 6960. В связи с этим единственным разрешенным номером версии является 0 (это соответствует версии v1). СПСС УЦ службы ДТС работает в режиме авторизованного ответчика.

37. Сертификат сервера СПСС должен содержать в себе расширение extKeyUsage, определенное в RFC 5280. Данное расширение должно быть обозначено как критическое и означает, что УЦ службы ДТС, издавая сертификат сервера OCSP, подтверждает своей подписью факт передачи ему права выдачи от его имени удостоверений о статусе сертификатов клиентов данного центра.

Сертификат может содержать также информацию о способе контакта с сервером СПСС. Данная информация содержится в поле расширения AuthorityInfoAccess.

Информация о статусе сертификата вносится в поле certStatus структуры SingleResponse. Она может принимать одно из трех разрешенных значений, определенных в Регламенте удостоверяющего центра службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза.

38. Шаблон запроса СПСС

Запрос СПСС принимает ASN.1-структуру в соответствии с RFC 6960 и имеет следующие ограничения.

Поле requestExtensions структуры tbsRequest содержит список расширений. Данный список должен содержать только расширение ocspNonce (OID 1.3.6.1.5.5.7.48.1.2).

Необязательное поле singleRequestExtensions структуры tbsRequest, содержащее список расширений для единичного запроса, должно отсутствовать.

В случае если поле optionalSignature структуры OCSPRequest задано, на него накладываются следующие ограничения:

поле signatureAlgorithm должно принимать значение "ГОСТ Р 34.11/34.10-2012" (OID 1.2.643.7.1.1.3.3);

поле certs должно включать сертификат для проверки ЭЦП запроса СПСС. Кроме того, поле requestorName из структуры tbsRequest должно присутствовать в обязательном порядке и представлять собой структуру directoryName, содержащую элемент CommonName (OID 2.5.4.3).

39. Шаблон ответа СПСС

Ответ СПСС принимает ASN.1-структуру в соответствии с RFC 6960 и имеет следующие ограничения.

Поле responseType содержит идентификатор типа ответа, который имеет значение 1.3.6.1.5.5.7.48.1.1. Поле response содержит структуру BasicOCSPResponse.

В случае если в соответствующем запросе СПСС присутствовало расширение ocspNonce, в ответе необязательное поле responseExtensions структуры ResponseData будет содержать расширение ocspNonce с аналогичным значением.

Поле signatureAlgorithm принимает значение "ГОСТ Р 34.11/34.10-2012" (OID 1.2.643.7.1.1.3.3).

В списке сертификатов certs содержится сертификат СПСС, необходимый для проверки ЭЦП.

Необязательное поле singleExtensions структуры SingleResponse, которое может содержать расширения OCSP-ответа, отсутствует.

V. Службы СШВ и СШВ-В

40. СШВ и СШВ-В УЦ службы ДТС подписывают ЭЦП выдаваемые ими же штампы времени при помощи ключей ЭЦП, специально зарезервированных для этой цели. В соответствии с рекомендацией RFC 5280 сертификаты СШВ и СШВ-В содержат поле, уточняющее узкое допустимое применение ключа (ExtKeyUsage), обозначенное как критическое. Это означает, что сертификат может быть использован СШВ и СШВ-В только для формирования ЭЦП в выдаваемых ими штампах времени.

41. Штампы времени, выданные СШВ и СШВ-В УЦ службы ДТС, содержат в себе информацию о штампе времени (структура TSTInfo), внесенную в структуру SignedData (в соответствии с RFC 2630), подписанную СШВ или СШВ-В и закрепленную в структуре ContentInfo. Штампы времени, выдаваемые СШВ и СШВ-В УЦ службы ДТС, соответствуют RFC 3161.

42. Шаблон запроса СШВ

Запрос СШВ представляет собой ASN.1-структуру в соответствии с RFC 2630 и имеет следующие ограничения:

необязательное поле reqPolicy структуры TimeStampReq отсутствует либо содержит идентификатор базовой политики (OID 0.4.0.2023.1.1);

необязательное поле nonce отсутствует либо содержит случайно сгенерированное 64-битное значение.

43. Шаблон ответа СШВ

Ответ СШВ представляет собой ASN.1-структуру в соответствии с RFC 2630 и имеет следующие ограничения:

поле digestAlgorithms структуры SignedData принимает значение "ГОСТ Р 34.11-2012 с длиной 512" (OID 1.2.643.7.1.1.2.3);

необязательное поле certificates структуры SignedData содержит сертификат службы TSP, если в TSP-запросе необязательное поле certReq структуры TimeStampReq содержит значение true;

необязательное поле crls структуры SignedData отсутствует;

поле policy структуры TSTInfo содержит идентификатор базовой политики (OID 0.4.0.2023.1.1);

необязательное поле nonce структуры TSTInfo содержит аналогичное значение, если в соответствующем TSP-запросе присутствует необязательное поле nonce;

необязательное поле tsa структуры TSTInfo отсутствует;

необязательное поле extensions структуры TSTInfo отсутствует;

поле digestAlgorithm структуры SignerInfo принимает значение "ГОСТ Р 34.11-2012 с длиной 512" (OID 1.2.643.7.1.1.2.3);

поле signedAttrs структуры SignerInfo содержит следующие объекты: тип подписываемого содержимого (OID 1.2.840.113549.1.9.16.1.4 (штамп времени)), значение хеш-функции штампа времени, информация о сертификате службы штампов времени;

поле signatureAlgorithm структуры SignerInfo принимает значение "ГОСТ Р 34.10-2012 с длиной 512".

44. Шаблон запроса СШВ-В

Запрос СШВ-В представляет собой ASN.1-структуру, аналогичную указанной в пункте 40 настоящего приложения.

45. Шаблон ответа СШВ-В

Ответ СШВ-В представляет собой ASN.1-структуру, аналогичную указанной в пункте 41 настоящего приложения.";

30) приложения № 3 и 4 к указанному Регламенту изложить в следующей редакции:

"ПРИЛОЖЕНИЕ № 3

к Регламенту

удостоверяющего центра
службы доверенной третьей стороны
интегрированной
информационной системы
Евразийского экономического союза
(в редакции Решения Коллегии
Евразийской экономической комиссии
от 24 декабря 2025 г. № 136)

ФОРМА ЗАЯВЛЕНИЯ
на издание сертификата ключа проверки ЭЦП

Евразийская экономическая комиссия
Руководителю удостоверяющего центра
службы доверенной третьей стороны
ИИС ЕАЭС

ЗАЯВЛЕНИЕ
на издание сертификата ключа проверки ЭЦП

Прошу издать сертификат ключа проверки ЭЦП в соответствии с указанными данными:

сокращенное наименование организации _____
предназначение сертификата (сервис) _____
Уполномоченный представитель:
Ф.И.О. _____
дата и место рождения _____
пол _____
серия и номер паспорта, кем и когда выдан: _____
подразделение, должность _____
электронная почта / телефон _____
юридический адрес организации _____
рабочее место расположено по адресу _____

Ознакомлен с требованиями Регламента удостоверяющего центра службы ДТС и обязуюсь соблюдать все его положения.

Приложение: CD-диск (DVD-диск, USB-диск и т. п.) с запросом на издание сертификата в 1 экз.

Уполномоченный представитель				
		(подпись)		(Ф.И.О.)

Сведения представлены на основании подлинных документов и являются достоверными.

(должность руководителя заявителя)				(Ф.И.О.)

		(подпись)		
"___" _____ ___ 20__ г.				
М.П.				

Примечание. Оттиск печати проставляется при наличии печати у организации. Оттиск печати не проставляется в случае использования фирменного бланка организации, изготовленного типографским способом и имеющего идентификационный номер на обороте бланка.

ПРИЛОЖЕНИЕ № 4
к Регламенту
удостоверяющего центра
службы доверенной третьей
стороны интегрированной
информационной системы
Евразийского экономического союза
(в редакции Решения Коллегии
Евразийской экономической комиссии
от 24 декабря 2025 г. № 136)

ФОРМА ЗАЯВЛЕНИЯ
на отзыв сертификата ключа проверки ЭЦП

Евразийская экономическая комиссия
Руководителю удостоверяющего центра
службы доверенной третьей стороны
ИИС ЕАЭС

ЗаявЛЕНИЕ
на отзыв сертификата ключа проверки ЭЦП

В связи _____
(причина отзыва сертификата)

прошу аннулировать и внести в список отозванных сертификатов сертификат ключа проверки ЭЦП:

серийный номер сертификата _____

предназначение сертификата (сервис) _____

(должность руководителя заявителя)		(подпись)		(Ф.И.О.)
"___" _____ ___ 20__ г.				
М.П.				

Примечание. Оттиск печати проставляется при наличии печати у организации. Оттиск печати не проставляется в случае использования фирменного бланка

организации, изготовленного типографским способом и имеющего идентификационный номер на обороте бланка.".