РЕСПУБЛИКАНСКОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАЦИОНАЛЬНЫЙ ЦЕНТР ЭЛЕКТРОННЫХ УСЛУГ»

Утверждена директором
государственного
предприятия «НЦЭУ»
21.01.2021
С изменениями от 06.11.2024

РЕГЛАМЕНТ
доверенной третьей стороны Республики Беларусь

Минск 2021

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ В РЕГЛАМЕНТ

1.1. Общие положения

Настоящий Регламент доверенной третьей стороны Республики Беларусь (далее – Регламент) устанавливает порядок взаимодействия с поставщиком услуг иностранного государства и субъектами информационного взаимодействия Республики Беларусь, проведения процедур проверки подлинности электронной цифровой подписи (далее – ЭЦП), требования к техническому, программному, информационному взаимодействию, а также меры по защите информации.

Положения Регламента не распространяются на деятельность по проверке ЭЦП в электронных документах (далее – ЭД) при межгосударственном обмене в интегрированной информационной системе Евразийского экономического союза.

Для целей Регламента термины и определения используются в значениях, определенных Законом Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи», СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей», СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов», СТБ 34.101.69-2014 «Информационные технологии и безопасность. Криптология. Термины и определения», СТБ 34.101.81-2019 «Информационные технологии и безопасность. Протоколы службы заверения данных», международными рекомендациями RFC 3029. Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (Data Validation and Certification Server Protocols серии международных стандартов IETF), а также следующие термины и их определения:

аттестат заверения (квитанция проверки ЭЦП (далее – Квитанция)) – ЭД, удостоверенный ЭЦП сервиса заверения данных оператора доверенной третьей стороны Республики Беларусь (далее - ДТС), содержащий результат проверки ЭЦП, созданной в иностранном государстве, а также содержащий информацию о результатах обработки запроса Потребителя;

АСН.1 – абстрактно-синтаксическая нотация версии 1 (ГОСТ 34.973);

прикладной программный интерфейс сервиса ДТС (от Application Programming Interface (далее – API сервиса ДТС)) - программный интерфейс приложения для взаимодействия с сервисом ДТС (размещен на сайте Оператора по адресу: https://nces.by/wp-content/uploads/DVCS-Client-API.docx);

DVCS (от Data Validation and Certification Server) запрос – запрос, на проверку ЭЦП в ЭД и (или) сертификата открытого ключа (далее – СОК);

CMS или PKCS #7 (от Cryptographic Message Syntax) – формат подписанных и (или) зашифрованных сообщений, установленный в СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений» с уточнениями в СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»;

порядок оказания услуг ДТС (далее – Порядок ДТС) – документ, устанавливающий правила взаимодействия между оператором ДТС и потребителем услуг ДТС при оказании услуг ДТС;

потребитель услуг ДТС (далее – Потребитель(и)) – физическое или юридическое лицо, которому оператор ДТС оказывает услугу(и) ДТС;

услуга(и) ДТС (далее – Услуга(и)) – электронная(ые) услуга(и), оказываемая(ые) оператором ДТС Потребителю по признанию подлинности ЭД при межгосударственном электронном взаимодействии.

1.2. **Оператор ДТС**

В соответствии с Указом Президента Республики Беларусь от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь» функции национального оператора ДТС по признанию подлинности ЭД при межгосударственном электронном взаимодействии осуществляет республиканское унитарное предприятие «Национальный центр электронных услуг» (далее - Оператор).

Юридический адрес Оператора:
Республика Беларусь, 220140, г. Минск, ул. Притыцкого, 64.
Адрес местонахождения Оператора:
Республика Беларусь, 220140, г. Минск, ул. Притыцкого, 64.
Контактные данные Оператора:

телефон:	(017) 331 30 00;
факс:	(017) 33130 06;
e-mail:	info@nces.by

адрес Интернет-сайта/ресурса: https://nces.by/pki/dts/ (далее – Интернет-сайт Оператора).

1.3. **Применение Регламента и присоединение к нему**

Оказание Услуг осуществляется Оператором на возмездной основе.

Стоимость Услуг определяются тарифами, утвержденными Оператором и размещенными на Интернет-сайте Оператора.

Потребители присоединяются к Регламенту путем заключения договора с Оператором на предоставление Услуг (далее – Договор). Форма Договора определяется Оператором. Факт заключения Договора является

полным принятием Потребителем условий Регламента и всех его приложений.

Выполнение требований Регламента становится обязательным для Оператора и Потребителей с момента заключения Договора.

1.4. Внесение изменений в Регламент

Внесение изменений и (или) дополнений в Регламент проводится Оператором самостоятельно, по согласованию с Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ).

Уведомление присоединившегося к Регламенту Потребителя о внесении изменений и (или) дополнений в Регламент осуществляется путем размещения текста обновленной версии Регламента в глобальной компьютерной сети Интернет на Интернет-сайте Оператора.

Все изменения и (или) дополнения, вносимые в Регламент и не связанные с изменением законодательства Республики Беларусь, вступают в силу и становятся обязательными для присоединившегося к Регламенту Потребителя с даты размещения текста измененного Регламента на Интернет-сайте Оператора.

Все изменения и (или) дополнения, вносимые в Регламент в связи с изменением нормативных правовых актов, обязательных к применению, вступают в силу в соответствии с требованиями нормативных правовых актов, повлекших изменение и (или) дополнение Регламента.

2. ПОРЯДОК ТЕХНИЧЕСКОГО, ПРОГРАММНОГО И ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

2.1. Общие положения

Оператор оказывает Услуги при межгосударственном и трансграничном электронном взаимодействии.

Сторонами межгосударственного и трансграничного электронного взаимодействия выступают: Потребители, Республиканский удостоверяющий центр Государственной системы управления открытыми ключами проверки ЭЦП Республики Беларусь (далее – РУЦ), Оператор, поставщики услуг иностранного государства или оператор ДТС иностранного государства, взаимодействующий с поставщиками услуг иностранного государства.

2.2. **Взаимодействие с Республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь**

Для проверки СОК, изданных РУЦ, Оператор использует СОК РУЦ и корневого удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – КУЦ) и списки отозванных сертификатов, размещенные на Интернет-сайте Оператора.

2.3. **Порядок взаимодействия с поставщиком услуг иностранного государства**

Оператор устанавливает доверие к СОК, изданному поставщиком услуг иностранного государства, путем проведения оценки в соответствии с подпунктом 1.3 пункта 1 приказа ОАЦ от 8 февраля 2019 г. № 45 «О дополнительных мерах по реализации Закона Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи» (далее — приказ ОАЦ № 45). Поставщиком услуг иностранного государства может являться оператор ДТС этого государства.

По результатам оценки, предусмотренной частью первой подпункта 1.3 пункта 1 приказа ОАЦ № 45, Оператором с поставщиком услуг иностранного государства заключается соглашение об установлении доверия к СОК, издаваемым в юрисдикции взаимодействующих сторон (далее - Соглашение). В Соглашении также устанавливаются используемые при взаимодействии между Оператором и поставщиком услуг иностранного государства средства ЭЦП, криптографические алгоритмы и механизмы, протоколы информационного взаимодействия и форматы обмена данными.

Перечень поставщиков услуг иностранного государства, с которыми у Оператора заключено Соглашение, размещен на Интернет-сайте Оператора.

Оператор на основе полученного от Потребителя ЭД, в соответствии с п. 2.4. настоящего Регламента, для проверки формирует и направляет в ДТС иностранного государства DVCS запрос, подписанной с помощью средства ЭЦП (криптографического алгоритма ЭЦП), установленного в Соглашении, методом POST.

DVCS запрос представляет собой CMS-сообщение в виде DER-кодированного модуля АСН.1, описанного в СТБ 34.101.81. DVCS запрос содержит дату и время генерации этого запроса. Структура DVCS запроса определяется в Соглашении в соответствии с международными рекомендациями RFC 3029. Образец структуры DVCS запроса представлен в приложении 1 настоящего Регламента.

Результат проверки от ДТС иностранного государства поступает в виде Квитанции, подписанной с помощью средства ЭЦП (криптографического алгоритма ЭЦП), установленного в Соглашении.

Структура Квитанции определяется в Соглашении в соответствии с международными рекомендациями RFC 3029. Образец структуры Квитанции представлен в приложении 2 настоящего Регламента.

2.4. Порядок взаимодействия с Потребителем

Правила взаимодействия между Оператором и Потребителем при оказании Услуг определяются Порядком ДТС, размещенным на Интернет-сайте Оператора.

Потребитель, получивший ЭД, соответствующий требованиям законодательства иностранного государства, в котором данный ЭД создан, может проверить его подлинность в рамках Услуг. Получение Услуг возможно только при наличии соответствующего Соглашения между Оператором и поставщиком услуг иностранного государства или оператором ДТС иностранного государства, взаимодействующего с поставщиками услуг иностранного государства.

Для оказания Услуг ЭД может быть передан Оператору в виде:

файла с прикрепленной ЭЦП (имеет CMS (PKCS # 7) - структуру в виде файла с расширением*.p7s (*.sgn));

двух файлов:

самого документа в электронном виде (формат может быть любым, позволяющим просматривать содержимое документа стандартными приложениями);

откреплённой ЭЦП (имеет CMS (PKCS # 7) - структуру в виде файла с расширением *.p7s (*.sgn)).

Взаимодействие Потребителя с автоматизированной информационной системой «ДТС» (далее – АИС ДТС) может осуществляться через web-интерфейс ДТС или по технологии «система-система» с использованием API сервиса ДТС.

По результатам проверки Оператор формирует ответ Потребителю в виде Квитанции, содержащий сведения о результатах проверки и подписанной ЭЦП с использованием личного ключа ДТС, СОК которого издан в РУЦ.

Квитанция представляет собой CMS-сообщение в виде DER-кодированного модуля АСН.1, описанного в СТБ 34.101.81. Структура Квитанции представлена в приложении 2 настоящего Регламента.

При взаимодействии Потребителя с АИС ДТС через web-интерфейс визуализация Квитанции осуществляется средствами самого web-интерфейса. Предусмотрена возможность сохранения Квитанции Потребителем.

При взаимодействии Потребителя с АИС ДТС по технологии «система-система» с использованием API сервиса ДТС визуализация Квитанции и возможность ее сохранения должны быть реализованы в системе Потребителя.

Подлинность ЭД иностранного государства считается удостоверенной, в случае получения Потребителем подлинной Квитанции со статусом «Действительна» (Подтверждено).

Для проверки подлинности Квитанции Потребитель должен проверить ЭЦП ДТС путем применения средств проверки ЭЦП, имеющих сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь по требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасности» (ТР 2013/027/BY)».

3. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ, ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ, А ТАКЖЕ МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Технические средства информационной системы Оператора размещены в одной контролируемой зоне, и обработка защищаемой информации осуществляется в пределах области действия комплекса средств безопасности объекта.

Система защиты информации АИС ДТС имеет действующий аттестат соответствия.

Оператором принимается политика информационной безопасности АИС ДТС, с которой ознакомлены все работники Оператора, на которых она распространяется.

У Оператора действуют документы по контролю физической безопасности помещений, в которых размещается АИС ДТС и ее активы, реализующие функции ДТС.

Все критические активы ДТС, требования и меры по их защите определены в задании по безопасности на АИС ДТС, на предмет соответствия которому проведена аттестация системы защиты информации АИС ДТС в реальных условиях эксплуатации.

В должностных инструкциях работников Оператора, принимающих участие в обеспечении функционирования АИС ДТС, определена их ответственность за поддержание основных мероприятий по управлению информационной безопасностью АИС ДТС.

На должности работников Оператора, принимающих участие в обеспечении функционирования АИС ДТС, назначаются лица, которые обладают необходимой квалификацией, опытом и прошли проверку на соответствие кадровой политике Оператора, что подтверждается

локальными правовыми актами Оператора. В должностных инструкциях указанных работников определены их функции, права и обязанности. Ответственность за обеспечение защиты информации, порядок доступа к защищаемой информации в соответствии с уровнем доступа к защищаемым сведениям, меры дисциплинарного воздействия, которые применяются в случае несанкционированных действий, отражены в политике информационной безопасности АИС ДТС.

Обязанности по обеспечению безопасности АИС ДТС реализуются Оператором с учетом требований задания по безопасности на АИС ДТС, политики информационной безопасности АИС ДТС, а также иных организационно-распорядительных документов Оператора.

В системе защиты информации применяются сертифицированные средства криптографической защиты информации для обеспечения конфиденциальности, контроля целостности (неизменности) и подлинности информации, распространение и (или) предоставление которой ограничено.

Управление доступом пользователей к информации и системным функциям приложений ограничивается в соответствии с политикой информационной безопасности АИС ДТС.

Управление системным доступом осуществляется с учетом требований задания по безопасности на АИС ДТС и политики информационной безопасности АИС ДТС.

Оператор гарантирует, что в случае сбоя функционирование АИС ДТС будет восстановлено настолько быстро, насколько это возможно.

Оператор гарантирует, что:

потенциальные угрозы для участников информационного обмена будут сведены к минимуму в результате прекращения предоставления Услуг;

информация о запросах и Квитанциях будет сохранена для представления в суд (в случае необходимости).

Полученные от Потребителя запросы и выданные Потребителю Квитанции в обязательном порядке фиксируются в АИС ДТС.

Срок хранения запросов и Квитанций в АИС ДТС пять лет с даты оказания Услуги.

4. ОРГАНИЗАЦИОННЫЕ ПОЛОЖЕНИЯ

Ответственность и порядок рассмотрения споров предусматривается в Договоре, заключаемом Оператором с Потребителем, которому оказываются Услуги.

Оператор обладает необходимыми материальными и финансовыми возможностями, позволяющими ему надлежащим образом обеспечивать выполнение Регламента.

Приложение 1

СТРУКТУРА ЗАПРОСА DVCS

№№ п/п	Наименование поля сообщения	Тип поля сообщения	Обязательность поля сообщения	Примечание
1.	requestInformation->version	INTEGER	Нет	Версия запроса. По умолчанию 1
2.	requestInformation->service	ServiceType	Да	Нумерует тип запроса DVCS сервиса (cpd(1), vsd(2), vpkc(3), ccpd(4))
3.	requestInformation->nonce	INTEGER	Нет	Зарезервированное поле (не используется). Может быть использовано для обеспечения дополнительной защиты от атак, связанных с воспроизведением или подбором содержания.
4.	requestInformation->requestTime	DVCSTime	Нет	Может быть использовано для указания момента времени, в который подтверждена действительность подписи или СОК. Если это поле отсутствует, то применяется значение текущего времени.
5.	requestInformation-> requester	GeneralNames	Нет	Указывает на запрашиваемый объект. Может содержать одно из значений на выбор – otherName, rfc822Name, dNSName, x400Address, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress, registeredID
6.	requestInformation->requestPolicy	PolicyInformation	Нет	Политика запроса. Отсутствие этого поля указывает на то, что любая политика является приемлемой.
7.	requestlnformation->dvcs	GeneralNames	Нет	Может быть использовано для указания списка DVCS серверов, которые могут быть использованы для получения дополнительной информации или для выполнения дополнительных операций, необходимых для формирования ответа.
8.	requestInformation->dataLocations	GeneralNames	Нет	Может содержать одно из значений на выбор – otherName, rfc822Name, dNSName, x400Address, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress, registeredID
9.	requestInformation->extensions	Extensions	Нет	Дополнительная информация
10.	data	Data	Да	Проверяемые данные (хэш-значение проверяемых данных)
11.	transactionIdentifier	GeneralName	Да	Идентификатор транзакции

Приложение 2

СТРУКТУРА КВИТАНЦИИ

№№ п/п	Наименование поля сообщения	Тип поля сообщения	Обязательность поля сообщения	Примечание
1 – вариант ответа (результаты проверки)				
1.	dvCertInfo->version	Integer	Нет	Версия ответа. По умолчанию 1
2.	dvCertInfo->dvReqInfo	DVCSRequestInformation	Да	Информация о запросе
3.	dvCertInfo->messageImprint	DigestInfo	Да	Хэш-значение на данные из запроса
4.	dvCertInfo->serialNumber	Integer	Да	Уникальный идентификатор запроса
5.	dvCertInfo->responseTime	DVCSTime	Да	Указывает значение времени, связанное с ответом
6.	dvCertInfo->dvStatus	PKIStatusInfo	Нет	Содержит обобщенный результат проверки подлинности
7.	dvCertInfo->policy	PolicyInformation	Нет	Политика ответа
8.	dvCertInfo->reqSignature	SignerInfos	Нет	Подпись запроса
9.	dvCertInfo->certs	SEQUENCE SIZE (1..MAX) OF TargetEtcCliain	Нет	Сертификаты
10.	dvCertInfo->extensions	Extensions	Нет	Дополнительная информация
2 – вариант ответа (сообщения об ошибках)				
1.	dvErrorNote->transaction Status	PKIStatusInfo	Да	Статус ответа
2.	dvErrorNote->transactionIdentifier	GeneralName	Нет	Идентификатор транзакции