УЦ ГАЗИНФОРМ СЕРВИС

РЕГЛАМЕНТ

предоставления сервисов DVCS

Общества с ограниченной ответственностью «Удостоверяющий центр ГАЗИНФОРМСЕРВИС»

Утвержден приказом № 2 от «2» марта 2015 г.

Редакция 1.0

Санкт-Петербург

2015 г.

Оглавление

1. ВВЕДЕНИЕ

Регламент предоставления сервисов DVCS (далее – Регламент) предназначен для участников электронного юридически значимого документооборота.

Регламент описывает:

- порядок предоставления сервисов DVCS;
- порядок идентификации и аутентификации пользователей сервисов DVCS;
- требования к использованию сервисов DVCS;
- форматы запросов, обрабатываемых сервисами DVCS;
- организационно-технические и административные меры обеспечения безопасности сервисов DVCS.

Регламент подготовлен в соответствии с рекомендациями RFC 3647. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC 3029. Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols.

1.1. Обзор

Настоящий документ определяет правила, механизмы и условия предоставления и использования услуг доверенной третьей стороны, включая права, обязанности и ответственность владельцев и пользователей сертификатов ключей проверки электронной подписи, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, включая, но не ограничиваясь, такие операции, как формирование, передача запросов на проверку электронной подписи и сертификатов, получение, хранение и использование квитанций о проверке электронной подписи и сертификатов.

1.2. Наименование и идентификация документа

Регламент предоставления сервисов DVCS (далее - Регламент) Общества с ограниченной ответственностью «Удостоверяющий центр ГАЗИНФОРМСЕРВИС» (далее - ООО «УЦ ГИС»)

Объектный идентификатор: 1.2.643.3.190.1.2-1.0

Версия документа: 1.0 Дата:

02.03.2015

Актуальная редакция настоящего документа доступна по ссылке: http://ca.gisca.ru/repository/cpsDVCS.pdf.

1.3. Участники

1.3.1. Удостоверяющий центр

Удостоверяющий центр (УЦ) – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом № 63-ФЗ от 06 апреля 2011 года.

1.3.2. Сервер проверки данных и сертификации

Сервер проверки данных и сертификации (DVCS) – третья доверенная сторона, обеспечивающая сервисы проверки данных, подтверждающих корректность документов с электронной подписью, действительность сертификатов ключей проверки электронных подписей, существования данных или факт обладания ими.

1.3.3. Владелец сертификата ключа проверки электронной подписи

Владелец сертификата ключа проверки электронной подписи – лицо, которому в порядке, установленном Федеральным законом № 63-ФЗ от 06 апреля 2011 года, выдан сертификат ключа проверки электронной подписи.

1.3.4. Пользователь сертификата ключа проверки электронной подписи

Пользователь сертификата ключа проверки электронной подписи – физическое лицо или автоматизированная система, использующие полученные в удостоверяющем центре сведения о сертификате ключа проверки электронной подписи для проверки принадлежности электронной подписи владельцу сертификата ключа проверки электронной подписи.

Пользователь сертификата ключа проверки электронной подписи может не являться владельцем сертификата ключа проверки электронной подписи.

1.3.5. Другие участники

Другими участниками могут являться уполномоченный федеральный орган исполнительной власти в сфере использования электронной подписи, осуществляющий ведение Единого государственного реестра квалифицированных сертификатов ключей проверки электронных подписей удостоверяющих центров в соответствии с действующим законодательством РФ, серверы DVCS других удостоверяющих центров, серверы служб OCSP и TSP.

1.3.6. Пользователи сервисов DVCS

Пользователи сервисов DVCS – это физические лица или информационные системы, зарегистрированные в системе DVCS, являющиеся владельцами сертификатов ключей проверки электронной подписи и формирующие запросы на проверку данных.

1.3.7. Оператор услуг DVCS

Оператором услуг DVCS является ООО «УЦ ГИС», осуществляющее эксплуатацию программных и технических средств информационной системы DVCS.

1.4. Использование сервисов DVCS

По результатам проверки запросов, DVCS формирует квитанции проверки данных (DVC), которые могут использоваться для доказательства действительности и корректности заявлений участников о фактах обладания данными, обеспечения неотказуемости от авторства лица, подписавшего данные, действительности сертификатов ключей проверки электронных подписей участников электронного документооборота, целостности документов с электронными подписями., математической корректности электронной подписи.

Услуги, предоставляемые DVCS, не заменяют использования списков отозванных сертификатов (далее – COC) и сервисов актуальных статусов сертификатов (OCSP) для проверки статуса сертификатов ключей проверки электронных подписей в больших открытых системах, из-за возможности масштабирования протокола проверки.

Сервисы DVCS могут использоваться для обеспечения неотказуемости от авторства лиц, подписавших электронный документ, или как дополнения к более традиционным сервисам, используемым в электронном документообороте.

Наличие квитанции проверки данных обеспечивает неотказуемость путем подтверждения того факта, что документ с электронной подписью или сертификат ключа проверки электронной подписи были действительны на момент времени, зафиксированный в квитанции.

1.5. Управление документом

1.5.1. Организация, ответственная за содержание документа

ООО «УЦ ГИС»
198097, Россия, Санкт-Петербург, ул. Кронштадтская, д.10, Лит. А, а/я 60.

1.5.2. Контактное лицо

Заместитель генерального директора ООО «УЦ ГИС»
198096, Россия, Санкт-Петербург, ул. Кронштадтская, д.10, Лит. А, а/я 60.
+7 (812) 67-777-68, 8-800-50-50-50-2 uc@gisca.ru

1.5.3. Лица, утверждающие изменения

Изменения регламента утверждаются Генеральным директором ООО «УЦ ГИС».

1.5.4. Процедура утверждения изменений

Изменения в регламент вносятся сотрудниками ООО «УЦ ГИС» по указанию Генерального директора или Уполномоченного Федерального органа и утверждаются генеральным директором ООО «УЦ ГИС».

Официальным уведомлением участников информационных систем об утверждении изменений регламента является его публикация на интернет-сайте ООО «УЦ ГИС» по ссылке: http://ca.gisca.ru/repository/cpsDVCS.pdf.

Все изменения, вносимые в регламент, вступают в силу и становятся обязательными к исполнению всеми потребителями услуг ООО «УЦ ГИС» немедленно после их публикации.

1.6. Определения и сокращения

Удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом[1].

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи

COC – список отозванных (аннулированных) сертификатов.

OCSP – online certificate status protocol, протокол онлайновой проверки статуса сертификата.

TSP – time stamping protocol, протокол меток времени.

2. Сервисы предоставляемые DVCS

Документ определяет 4 основных типа сервисов DVCS:

- Сертификация обладания данными (cpd);
- Сертификация факта обладания данными (ccpd);
- Проверка документа с электронной подписью (vsd);
- Проверка сертификата ключа проверки электронной подписи (vpkc).

По результатам предоставления любого сервиса DVCS формирует квитанцию проверки данных – документ, подписанный электронной подписью DVCS и содержащий результаты проверок и доверенную информацию о времени их проведения (штамп времени).

2.1. Сертификация обладания данными

Сервис сертификации обладания данными обеспечивает документальное доказательство того, что заявитель обладает определенными данными в конкретный момент времени и что актуальные данные были предоставлены серверу DVCS.

[1] Федеральный закон «Об электронной подписи» №63-ФЗ от 06.04.2011 г.

2.2. Сертификация факта обладания данными

Сервис сертификации факта обладания данными аналогичен предыдущему сервису за исключением того, что заявитель предоставляет не сами данные, а только значение хэш-функции от этих данных.

2.3. Проверка документа с электронной подписью

Сервис проверки документа с электронной подписью используется в случаях, когда необходимо документально подтвердить достоверность документа, подписанного электронной подписью.

DVCS проверяет все подписи присоединенные к документу, используя все сертификаты ключей проверки электронных подписей и всю необходимую информацию об их статусе, включая электронные подписи под запросами.

DVCS проверяет математическую корректность всех подписей, присоединенных к документу, а также уровень доверия к автору документа, например, путем проверки всей цепочки сертификации от конечного пользователя до точки доверия (т.е. корневого УЦ в иерархии; УЦ, выдавшего сертификат другому DVCS и т.п.).

DVCS может обращаться к соответствующим спискам отзыва сертификатов (CRL) или дополнять их путем обращения к более детальной информации об актуальных статусах сертификатов, предоставляемой удостоверяющими центрами, например, с использованием сервиса (протокола) актуальных статусов сертификатов (OCSP), сервисов доверенного каталога или сервисов других DVCS.

DVCS выполняет проверку всех подписей, присоединенных к документу. Ошибка проверки одной из подписей необязательно приводит к ошибке общей проверки, и наоборот ошибка общей проверки может произойти, если документ имеет недостаточное количество подписей.

2.4. Проверка сертификата ключа проверки электронной подписи

Сервис проверки сертификата ключа проверки электронной подписи используется для проверки и документального подтверждения действительности (в соответствии с RFC 5280 с обновлениями RFC 6818) одного или более сертификатов ключей проверки электронных подписей в определенное время.

В процессе проверки сертификата ключа проверки электронной подписи DVCS проверяет тот факт, что сертификат, включенный в запрос, является действительным. DVCS проверяет весь путь сертификации от издателя сертификата до корневого УЦ. В процессе проверки DVCS может использовать соответствующий CRL, OCSP, и другие DVCS.

3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1. Процедура первичной регистрации

Первичная регистрация пользователя DVCS производится при личном обращении в ООО «УЦ ГИС» за получением сертификата ключа проверки электронной подписи в соответствии с Регламентом удостоверяющего центра.

3.2. Идентификация и аутентификация заявителя при смене сертификата

3.2.1. Идентификация и аутентификация в случае плановой (очередной) смены сертификата

Идентификация и аутентификация пользователя DVCS при плановой замене (очередной) смене сертификата ключа проверки подписи производится в рамках перевыпуска сертификата в соответствии с Регламентом УЦ.

3.2.2. Идентификация и аутентификация в случае смены сертификата после отзыва (аннулирования)

Идентификация и аутентификация пользователя DVCS в случае замены сертификата после отзыва (аннулирования) производится в процессе перевыпуска сертификата в соответствии с пунктом 3.3 Регламента УЦ.

4. Требования к использованию сервисов DVCS

4.1. Запрос на проверку

4.1.1. Лица, имеющие право подавать запросы

Запрос на проверку могут формировать организации, эксплуатирующие информационные системы, или физические лица (в том числе представители юридических лиц), заключившие договор в ООО «УЦ ГИС» на предоставление сервисов DVCS, являющиеся владельцами сертификатов ключей проверки электронной подписи и зарегистрированные в информационной системе DVCS.

4.1.2. Процедура регистрации и обязательства

Под регистрацией понимается процесс внесения регистрационной информации о пользователе DVCS и его сертификате в информационную систему DVCS. Процедура регистрации применяется в отношении пользователей DVCS, являющихся владельцами сертификатов ключей проверки электронных подписей и заключивших договор на оказание соответствующих услуг.

После проверки оплаты услуг и выпуска сертификата администратор DVCS регистрирует пользователя в информационной системе DVCS и выдает ему данные аутентификации (логин и пароль) для доступа в личный кабинет сервиса DVCS.

ООО «УЦ ГИС» со своей стороны гарантирует конфиденциальность данных аутентификации.

4.1.3. Форматы запросов

Содержание запроса к сервису DVCS (DVCS-запрос) зависит от типа запроса. Типы запросов и соответствующие им данные приведены в таблице 4.1.

Таблица 4.1

Тип запроса	Данные
Запрос VSD (Проверка документа (данных) с электронной подписью)	1. Проверяемый документ (данные) с электронной подписью в формате CAdES/XAdES; 2. Параметры запроса; 3. Сертификат ключа проверки ЭП пользователя DVCS; 4. Адрес сервера проверки подлинности
Запрос VPKC (Проверка сертификата ключа проверки ЭП)	1. Файл проверяемого сертификата; 2. Параметры запроса; 3. Сертификат ключа проверки ЭП пользователя DVCS; 4. Адрес сервера проверки подлинности

Запросы CPD и CCPD (Сертификация обладания данными с предоставлением их и без предоставления сервису)	1. Файл любого типа, содержащий данные обладание которыми необходимо подтвердить или значение хэш-функции от таких данных; 2. Параметры запроса; 3. Сертификат ключа проверки ЭП пользователя DVCS; 4. Адрес сервера проверки подлинности

4.2. Обработка запроса на проверку

4.2.1. Процедура идентификации и аутентификации

Идентификация и аутентификация пользователя DVCS при обработке запроса осуществляется по сертификату ключа проверки ЭП пользователя DVCS, содержащемуся в составе запроса.

4.2.2. Выдача и отказ в выдаче результата проверки

Результатом проверки является DVC-квитанция – DVCS-ответ с электронной подписью DVCS, содержащий информацию о проверке или уведомление об ошибке.

В случае успешной обработки запроса DVCS-ответ содержит данные, которые зависят от типа запроса. Типы запросов и данные содержащиеся в ответе приведены в таблице 4.2.

Таблица 4.2

Тип запроса	Данные в DVCS-квитанции
Запрос VSD (Проверка документа (данных) с электронной подписью)	1. Подлинность документа подтверждена/не подтверждена; 2. Количество электронных подписей в запросе; 3. Статус каждой ЭП – верна/не верна; 4. Информация о всех сертификатах ключей проверки ЭП – субъект, издатель, срок действия, алгоритм ключей; их статусе – действителен/не действителен; 5. Сертификат ключа проверки ЭП DVCS; 6. Время создания квитанции; 7. Серийный номер квитанции; 8. Информация о запросе.
Запрос VPKC (Проверка сертификата ключа проверки ЭП)	1. Подлинность сертификата – подтверждена/не подтверждена; 2. Статус сертификата – действителен/не действителен; 3. Информация о сертификате – субъект, издатель, срок действия, серийный номер, алгоритм ЭП в сертификате, алгоритм ключей, значение открытого ключа; 4. Информация о всех сертификатах УЦ в пути сертификации проверяемого сертификата ключа проверки ЭП; 5. Сертификат ключа проверки ЭП DVCS сервера; 6. Время создания квитанции; 7. Серийный номер квитанции; 8. Информация о запросе.
Запрос CPD (Сертификация обладания данными с предоставлением их сервису)	1. Статус обладания данными – подтверждено/не подтверждено; 2. Информация о хэш-функции (ее значение и алгоритм формирования) 3. Сертификат ключа проверки ЭП DVCS сервера; 4. Время создания квитанции; 5. Серийный номер квитанции; 6. Информация о запросе.

Запрос CCPD (Сертификация обладания данными без предоставления их сервису)	1. Статус обладания данными – подтверждено/не подтверждено; 2. Информация о хэш-функции (ее значение и алгоритм формирования) 3. Сертификат ключа проверки ЭП DVCS сервера; 4. Время создания квитанции; 5. Серийный номер квитанции; 6. Информация о запросе.

При возникновении ошибки DVCS-ответ содержит следующие данные:

- Статус транзакции;
- Статус отклонения;
- Причина возникновения ошибки:
    - Транзакция не допускается или не поддерживается;
    - Превышение допустимого интервала расхождения времени сервиса DVCS и пользователя; ○ Неверный формат данных;
    - Идентификаторы авторизации в запросе и ответе различаются; ○ Некорректная ЭП пользователя DVCS в запросе; Дополнительная информация об ошибке.

4.2.3. Сроки обработки запросов на проверку

Запросы на проверку обрабатываются в режиме реального времени.

4.3. Синхронизация времени

Для обеспечения точности времени на аппаратных средствах DVCS и используемого сервера меток времени (TSP) производится синхронизация внутренних таймеров аппаратных средств с ntp-серверами ГМЦ ГСВЧ ФГУП «ВНИИФТРИ» Stratum1, подключенных к государственному первичному эталону времени РФ.

4.4. Окончание пользования услугами DVCS

Участник информационной системы может закончить использование услуг ООО «УЦ ГИС» путем расторжения договора на оказание услуг, путем отзыва своего сертификата или отказа от смены ключей после окончания их срока действия, при этом он не освобождается от ранее взятых на себя обязательств перед удостоверяющим центром и другими участниками информационных систем.

5. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Для обеспечения безопасности DVCS применяются приведенные ниже меры, включающие в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

Защита информации от несанкционированного доступа осуществляется на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Защита информации от несанкционированного доступа предусматривает контроль эффективности средств защиты от несанкционированного доступа. Этот контроль выполняется администраторами безопасности не реже 1 раза в месяц.

5.1. Физические меры обеспечения безопасности

5.1.1. Здания и сооружения

Технические средства DVCS расположены таким образом, чтобы свести к минимуму возможность несанкционированного доступа, аварий и влияние природных явлений.

5.1.2. Физический доступ

Помещения ООО «УЦ ГИС», предоставляющего сервисы DVCS, расположены в отдельном крыле восьмиэтажного здания. Все помещения оборудованы системой контроля и управления доступом с идентификацией по смарт-картам, исполнительными устройствами системы контроля доступа электромеханического типа, системой видеонаблюдения.

Серверное оборудование размещается в центрах обработки данных и серверных помещениях, соответствующих требованиям действующего законодательства, предъявляемым к обеспечению безопасности удостоверяющих центров.

Помещения ООО «УЦ ГИС» круглосуточно находятся под охраной специализированной организации.

Идентификационные карты для доступа в помещения УЦ выдаются сотрудникам по распоряжению Генерального директора ООО «УЦ ГИС».

Посетители допускаются в помещения ООО «УЦ ГИС» только в назначенное им время в сопровождении персонала удостоверяющего центра. Доступ в серверные помещения для посетителей закрыт.

5.1.3. Электроснабжение и кондиционирование воздуха

Технические средства DVCS подключены к общегородской сети электроснабжения с использованием оборудования бесперебойного питания.

Электрические сети и электрооборудование, используемые в ООО «УЦ ГИС», отвечают требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

Помещения ООО «УЦ ГИС» оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

5.1.4. Подверженность воздействию влаги

Защита оборудования DVCS от влаги обеспечивается его размещением в специальных серверных шкафах.

5.1.5. Предупреждение и защита от возгорания

Помещения ООО «УЦ ГИС» оборудованы пожарной сигнализацией и средствами пожаротушения в соответствии с требованиями, установленными законодательством Российской федерации.

5.1.6. Хранение архивных документов и электронных носителей

Документальный фонд ООО «УЦ ГИС», как фондообразователя, хранится в соответствии с действующим законодательством по делопроизводству и архивному делу.

5.1.7. Уничтожение документированной информации

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками ООО «УЦ ГИС», обеспечивающими документирование.

Важные документы и материалы подвергаются уничтожению в специальном оборудовании перед утилизацией.

5.1.8. Резервная площадка

Резервная площадка расположена в центре обработки данных за пределами основных помещений ООО «УЦ ГИС».

5.2. Организационные меры обеспечения безопасности

В ООО «УЦ ГИС» разработаны все необходимые документы по защите персональных данных и конфиденциальной информации. Осуществляется периодический контроль знаний персонала по требованиям руководящих документов в области защиты информации и персональных данных.

5.3. Восстановление в случае аварий

5.3.1. Действия по предотвращению аварий

На аппаратных средствах DVCS осуществляется периодический контроль технического состояния, а также проводятся регламентные работы в соответствии с эксплуатационной документацией.

В ООО «УЦ ГИС» осуществляется регулярное резервное копирование данных, необходимых для восстановления работоспособности программных и технических средств DVCS.

5.3.2. Случаи повреждения оборудования, программных и/или аппаратных сбоев

В случае повреждения оборудования, программных и/или аппаратных средств производится восстановление работоспособности сервиса с использованием резервного оборудования и резервных копий в течение 24 часов.

5.4. Сроки действия ключей и сертификатов DVCS

Сроки действия ключей и сертификатов устанавливаются в соответствии с законодательством РФ, требованиями нормативных документов ФСБ России и эксплуатационной документации используемого средства ЭП.

Срок действия ключа электронной подписи DVCS сервиса – 12 месяцев.

Срок действия квалифицированного сертификата ключа проверки электронной подписи – 11 лет.

Период разрешенного использования ключа электронной подписи содержится в соответствующем расширении квалифицированного сертификата.

5.5. Порядок плановой замены ключей сертификата DVCS

Смена ключей и сертификатов DVCS сервиса производится ежегодно в период до окончания срока действия текущего ключа электронной подписи.

Администратор DVCS оформляет заявление на выпуск квалифицированного сертификата в соответствии с Регламентом УЦ и производит генерацию новой ключевой пары и запроса на квалифицированный сертификат в соответствии с эксплуатационной документацией ПАК DVCS.

Выпуск нового квалифицированного сертификата осуществляется в соответствии с Регламентом УЦ. При этом заменяемый сертификат не отзывается.

После выпуска сертификата администратор производит установку нового сертификата на сервер DVCS.