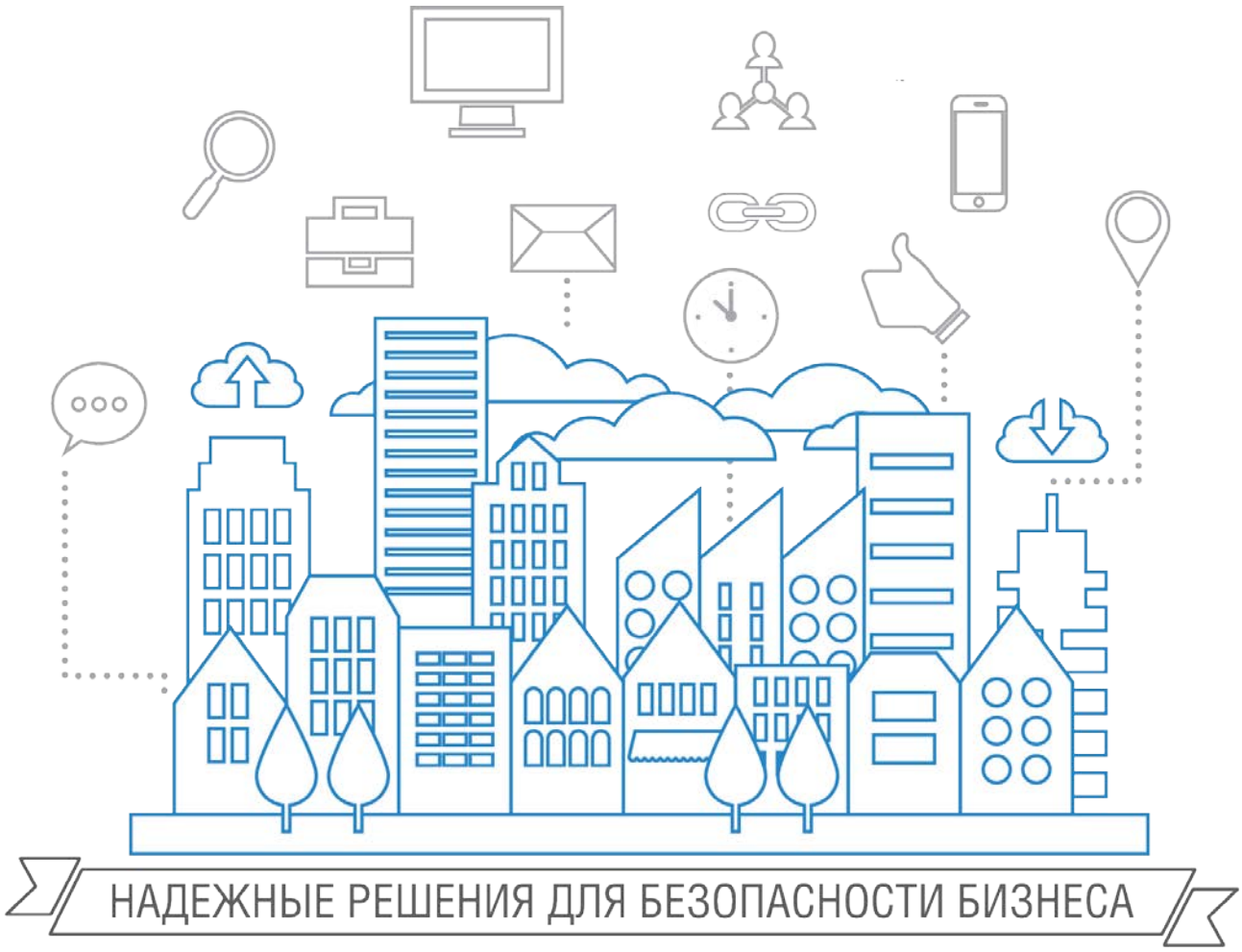
ГАЗИНФОРМСЕРВИС

198096, г. Санкт-Петербург, ул. Кронштадтская, д.10, лит. А, тел.: (812) 677-20-50, факс: (812) 677-20-51
Почтовый адрес: 198096, г. Санкт-Петербург, а/я 59, e-mail: resp@gaz-is.ru, www.gaz-is.ru
р/с 40702810800000001703 Ф-л Банка ГПБ (АО) в г. Санкт-Петербурге БИК 044030827,
к/с 30101810200000000827, ОКПО 72410666, ОГРН 1047833006099, ИНН/КПП 7838017968/783450001

Криптографическая платформа «Litoria Crypto Platform»

Описание применения



Санкт-Петербург, 2017

Аннотация

Настоящий документ содержит описание применения криптографической платформы «Litoria Crypto Platform» (далее криптоплатформа или платформа «Litoria Crypto Platform»).

В документе приведено назначение криптоплатформы и перечислены предоставляемые возможности.

В разделе «Условия применения» указаны условия, необходимые для использования криптоплатформы, и требования к аппаратным и программным средствам рабочих станций, на которых будет использоваться «Litoria Crypto Platform».

В разделе «Описание задачи» описана задача, решаемая при применении криптоплатформы, а также ее основные функции, и приведены примеры алгоритмов ее решения.

В разделе «Входные и выходные данные» указаны входные и выходные данные платформы «Litoria Crypto Platform».

В конце документа приведен список использованных сокращений и основных терминов.

Содержание

1 Назначение криптоплатформы «Litoria Crypto Platform»

Криптографическая платформа «Litoria Crypto Platform» является ядром усовершенствованной электронной подписи (УЭП) и предназначена для интеграции в различные системы документооборота, порталы и на серверы приложений с использованием российских и иностранных криптографических алгоритмов с возможностью трансграничного взаимодействия.

При использовании криптографической платформы «Litoria Crypto Platform» разработчику доступны следующие возможности:

- создание, добавление, заверение и проверка электронной подписи (ЭП) различного типа (простая, усовершенствованная, отделенная);
- создание и добавление ЭП документа без предоставления данных (подпись хеша документа);
- шифрование, расшифровывание, гарантированное удаление файлов;
- работа с ключевой информацией и сертификатами:
  - создание ключевой пары и запроса на сертификат;
  - создание ключевой пары и запроса на сертификат, с использованием уже существующего сертификата;
  - установка сертификата в хранилище «Личное» и в контейнер;
  - создание связки открытый-закрытый ключ;
  - создание самоподписанного сертификата;
  - создание пользовательского сертификата;
  - создание атрибутного сертификата;
  - установка сертификата в заданное хранилище;
  - получение сертификата из хранилища;
  - получение информации о сертификате;
  - проверка статуса сертификата по спискам отзыва сертификатов (СОС) и по Online Certificate Status Protocol (OCSP);
- управление списками отзыва сертификатов: создание, импорт, экспорт, удаление, детальный просмотр;
- применение для работы с ЭП различных криптопровайдеров, как программных (Base CSP, КриптоПро CSP, ViPNet CSP, ВАЛИДАТА CSP, Avest CSP и др.), так и аппаратных (JaCarta, eToken ГОСТ, РУТОКЕН ЭЦП);
- реализация функций службы актуальных статусов сертификатов согласно RFC2560 «Online Certificate Status Protocol (OCSP)»;
- реализация функций службы штампов времени согласно RFC3161 «Time-Stamp Protocol (TSP)»;
- формирование и проверка ЭП электронных сообщений в соответствии со спецификацией RFC3029 «Data Validation and Certification Server Protocol (DVCS)»;
- интеграция сервисов пролонгации;
- интеграция в системы электронного документооборота, включая SharePoint, Citrix, веб-сервер MS IIS (Internet Information Servies);
- предоставление интерфейсов (Com, Java, C#, SilverLight, ASP.net) для встраивания в различные среды и системы.

2 Условия применения

2.1 Требования к техническим средствам

Минимальные требования к рабочей станции, на которую устанавливается криптографическая платформа «Litoria Crypto Platform», обусловлены применением ОС: процессор с тактовой частотой 1 ГГц, RAM 2 Гб, HDD 20Гб, видеоадаптер SVGA, свободный USB-порт при использовании электронных идентификаторов или других USB-устройств для хранения цифровых сертификатов.

2.2 Требования к программному обеспечению

Криптографическая платформа «Litoria Crypto Platform» функционирует под управлением следующих ОС:

- MS Windows 2000/XP/2003/Vista/2008/7/2008R2/8/2012/8.1/2012R2 (32- и 64-bit);
- Linux, удовлетворяющие стандарту LSB 4.x/3.x;
- Mac OS X (x64);
- iOS версии 4.2 и выше.

Для работы платформы «Litoria Crypto Platform» требуется установка следующего программного обеспечения:

1. Криптопровайдера, реализованного в соответствии с технологией Microsoft CSP, или драйверов к используемому аппаратному криптопровайдеру.
2. Драйверов к электронному идентификатору, использующемуся для хранения цифровых сертификатов.

Если электронный идентификатор используется как для хранения сертификатов, так и в качестве аппаратного криптопровайдера, то драйвера к нему устанавливаются один раз.

3 Описание задачи

3.1 Определение задачи

Электронный документооборот – механизм по работе с документами в электронном виде, т.е. движение документов в организации с момента их создания (или получения) до завершения исполнения (или отправления), а также способ организации работы с документами, при котором основная масса документов организации (предприятия) используется в электронном виде и хранится централизованно.

Электронный документооборот является неотъемлемой частью информационной системы любого предприятия. На данный момент получили распространение корпоративные интернет-порталы, предназначенные для организации защищенного юридически-значимого электронного документооборота.

Известные угрозы для систем электронного документооборота (СЭД) могут быть классифицированы следующим образом:

- угрозы нарушения целостности – угрозы, при реализации которых происходит повреждение, уничтожение и/или искажение информации;
- угрозы нарушения конфиденциальности – угрозы несанкционированного доступа;
- угрозы нарушения работоспособности системы – всевозможные угрозы, реализация которых приведет к нарушению или прекращению работы системы (умышленные атаки, ошибки пользователей, а также сбои в оборудовании и программном обеспечении и др.).

При встраивании криптографической платформы «Litoria Crypto Platform» непосредственно в систему электронного документооборота и/или корпоративный портал и использовании ее основных функций осуществляется защита СЭД от угрозы нарушения целостности и конфиденциальности.

На рисунке 3.1.1 представлена схема передачи документа в незащищенной системе документооборота.

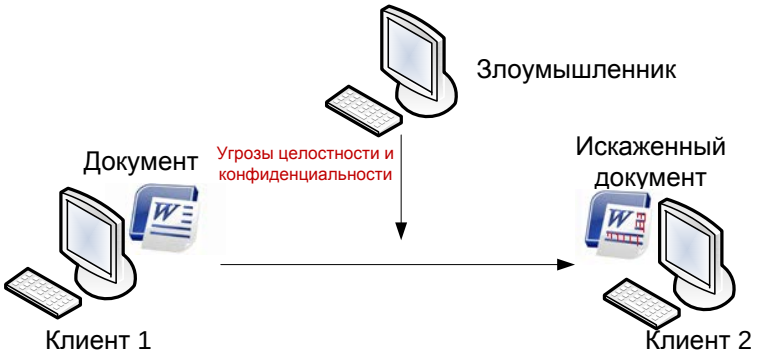


Рисунок 3.1.1. Схема передачи документа в незащищенной системе документооборота

В защищенной системе документооборота над передаваемыми данными с помощью криптографической платформы «Litoria Crypto Platform» и криптопровайдера осуществляются криптографические операции, такие как шифрование/расшифровывание и создание/добавление/проверка электронной подписи. Схема защищенной СЭД представлена на рисунке 3.1.2.

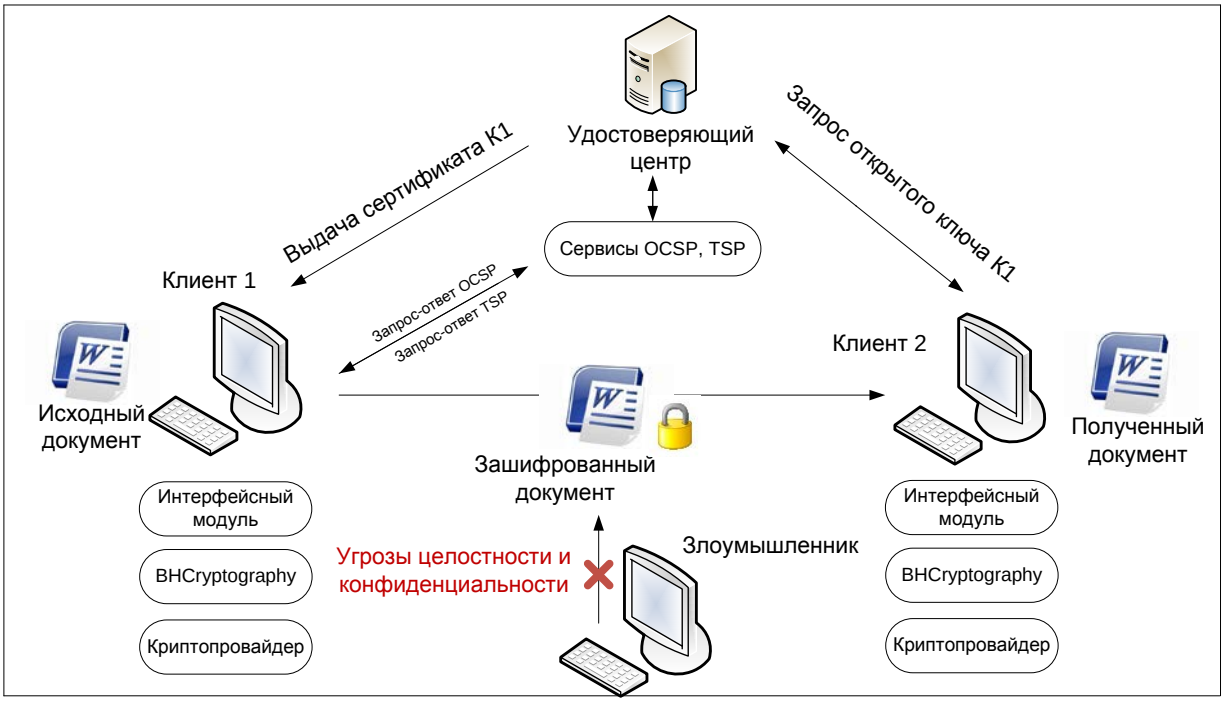


Рисунок 3.1.2. Схема защищенной СЭД

При использовании иностранных криптографических алгоритмов для создания и проверки ЭП в системе документооборота криптографическая платформа «Litoria Crypto Platform» может быть применена для реализации системы доверенной третьей стороны (ДТС). Подробное описание системы ДТС представлено в разделе 3.3.3.

3.2 Основные функции криптоплатформы «Litoria Crypto Platform»

Криптографическая платформа «Litoria Crypto Platform» обеспечивает реализацию следующих основных функций:

- управление ключевой информацией и сертификатами;
- управление списками отзыва сертификатов;
- создание УЭП;
- добавление УЭП;
- заверка УЭП;
- проверка УЭП;
- сервисы ДТС;
- шифрование файла;
- расшифровывание файла;
- гарантированное удаление файла;
- реализация функций службы штампов времени;
- сервис пролонгации.

3.2.1 Управление ключевой информацией и сертификатами

С помощью криптоплатформы можно создать приложение, которое будет выполнять следующие функции с сертификатами:

- создание ключевой пары и запроса на сертификат;
- создание ключевой пары и запроса на сертификат, с использованием уже существующего сертификата;
- установка сертификата в хранилище «Личное» и в контейнер USB-устройства;
- создание связки открытый-закрытый ключ;

- создание самоподписанного сертификата;
- создание пользовательского сертификата;
- создание атрибутного сертификата;
- установка сертификата в заданное хранилище;
- получение сертификата из хранилища;
- получение информации о сертификате;
- проверка статуса сертификата по COC и OCSP.

3.2.2 Управление списками отзыва сертификатов

Криптоплатформа предоставляет интерфейс создания списка отзыва для приложений с функциями УЦ. Для пользовательских приложений платформа «Litoria Crypto Platform» предоставляет функции импорта, экспорта, удаления и просмотра списков отзыва.

3.2.3 Создание УЭП

УЭП представляет собой структурированную запись в формате ASN.1 (X.209: «Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)»). В усовершенствованную подпись включаются следующие элементы:

- подписываемый документ;
- подписываемые атрибуты (хеш-код сообщения, хеш-коды отдельных полей сертификата, тип документа и др.);
- подпись документа;
- штамп времени, полученный на данные, указанные выше;
- ссылки на сертификаты и OCSP-ответ;
- штамп времени, полученный на данные, указанные выше;
- полный сертификат пользователя и данные отзыва.

Таким образом, усовершенствованная подпись содержит в себе не только все доказательства подлинности подписи в электронном документе (принадлежность подписи владельцу, отсутствие искажений в документе), но и подтверждение момента подписи, а также действительности сертификата ключа подписи на момент создания подписи.

Для создания УЭП должен быть осуществлен выбор сертификата открытого ключа и параметры создания подписи. К таким параметрам относятся:

- добавление в подпись сертификата подписывающего лица;
- добавление штампа времени;
- создание усовершенствованной подписи;
- выбор формата файла на выходе.

Общая схема создания УЭП приведена на рисунке 3.2.1.

Рисунок 3.2.1. Схема создания УЭП

3.2.4 Добавление УЭП

Если в подписании документа участвует несколько лиц, и каждый должен поставить в нем свою подпись (например, в листе согласования), используется операция добавления УЭП.

В отличие от операции создания УЭП, добавление подписи производится в уже подписанный ранее документ.

В криптографической платформе «Litoria Crypto Platform» существует возможность добавления подписи, созданной на криптографическом алгоритме, отличном от ГОСТ, например, RSA или AES. Основной областью применения такой подписи является система доверенной третьей стороны. Среди отличительных особенностей таких систем можно выделить необходимость юридически-значимого документооборота между различными странами или регионами, в которых используются национальные криптографические стандарты.

3.2.5 Заверка УЭП

Помимо операций создания и добавления УЭП, криптографическая платформа «Litoria Crypto Platform» предоставляет возможность создания заверяющей подписи. Под заверяющей УЭП понимается электронная подпись, утверждающая подпись другого пользователя, подписавшего документ.

Чтобы представить, как это выглядит, можно привести пример: подпись директора организации на финансовом документе никогда не появится раньше подписи главного бухгалтера, также как одна лишь подпись главного бухгалтера без подписи директора не будет иметь юридической ценности. То есть это – подпись подписи.

Для создания заверяющей подписи необходимо вначале произвести проверку УЭП, чтобы было достоверно известно, какие подписи уже существуют в документе, а также их статус.

Дальнейшая операция по заверке подписей для пользователя аналогична созданию УЭП. Заверка УЭП возможно лишь на подписанных ранее файлах.

3.2.6 Проверка УЭП

Проверка УЭП подразумевает подтверждение подлинности усовершенствованной подписи в электронном документе, то есть:

- подтверждение принадлежности ЭП в электронном документе владельцу сертификата ключа подписи;
- подтверждение отсутствия искажений в подписанном данной ЭП электронном документе;
- подтверждение момента подписи;
- подтверждение действительности сертификата ключа подписи на момент создания подписи.

Общая схема проверки УЭП приведена на рисунке 3.2.2.

Рисунок 3.2.2. Схема проверки УЭП

Проверка отделенной усовершенствованной подписи – проверка корректности самого файла подписи.

Если во время проверки сертификат подписчика не был найден в локальном хранилище, то этот сертификат извлекается из подписанного файла и устанавливается автоматически в локальное хранилище.

3.2.7 Сервисы ДТС

Криптографическая платформа «Litoria Crypto Platform» предоставляет следующие сервисы согласно RFC3029:

1) Создание и отправка 4-х типов DVCS-запросов:
   - подтверждение электронной подписи электронного документа (Validation of Digitally Signed Document – VSD);
   - подтверждение действительности сертификата ключа подписи (Validation of Public Key Certificates – VPKC);
   - удостоверение обладания информацией в указанный момент времени с предоставлением ее сервису (Certification of Possession of Data – CPD);
   - удостоверение обладания информацией без предоставления ее сервису (по хеш) (Certification of Claim of Possession of Data – CCPD).
2) Формирование DVC-квитанции.
3) Анализ DVC-квитанции и вывод информации.

3.2.8 Шифрование файла

Шифрование производится на открытом ключе, содержащемся в сертификате. Закрытый ключ есть только у владельца использованного сертификата открытого ключа. Таким образом, при шифровании файла никто, кроме владельца закрытого ключа, не сможет расшифровать файл.

Криптоплатформа может производить шифрование файла сразу для нескольких будущих получателей файла. Для каждого сертификата получателей пользователь может просмотреть статус, чтобы на его основании сделать вывод о пригодности данного сертификата к шифрованию.

3.2.9 Расшифровывание файла

Расшифровывание документа пройдет успешно при наличии закрытого ключа, связанного с одним из открытых ключей, на которых производилось шифрование файла. Если пользователь располагает несколькими закрытыми ключами, которым соответствуют несколько открытых ключей, участвующих при шифровании, то расшифровывание будет выполнено на первом из закрытых ключей. После расшифровывания пользователь может получить информацию о том, на каком сертификате была произведена операция расшифровывания.

3.2.10 Гарантированное удаление файла

Удаление файлов происходит трехкратным затиранием содержимого по специальному алгоритму, исключающему считывание остаточной информации на диске после удаления.

3.2.11 Реализация функций службы штампов времени

Криптоплатформа предоставляет функции как для создания запроса в службу штампов времени, так и для создания программного обеспечения, которое осуществляет функции сервера службы штампов времени.

3.2.12 Сервис пролонгации

Для реализации сервисов пролонгации УЭП поддерживается стандарт CAdES-A.

3.3 Алгоритм решения задачи

Программный уровень криптографической платформы «Litoria Crypto Platform» предоставляет возможность интеграции в следующие системы документооборота с возможностью трансграничного взаимодействия:

- интеграция с решениями терминального доступа на основе Citrix;
- интеграция с порталами SharePoint;
- интеграция с веб-серверами IIS.

Для интеграции в различные среды и системы поддерживаются интерфейсы Com, Java, C#, SilverLight, ASP.net.

Алгоритм решения задачи встраивания отображен на рисунке 3.3.1.

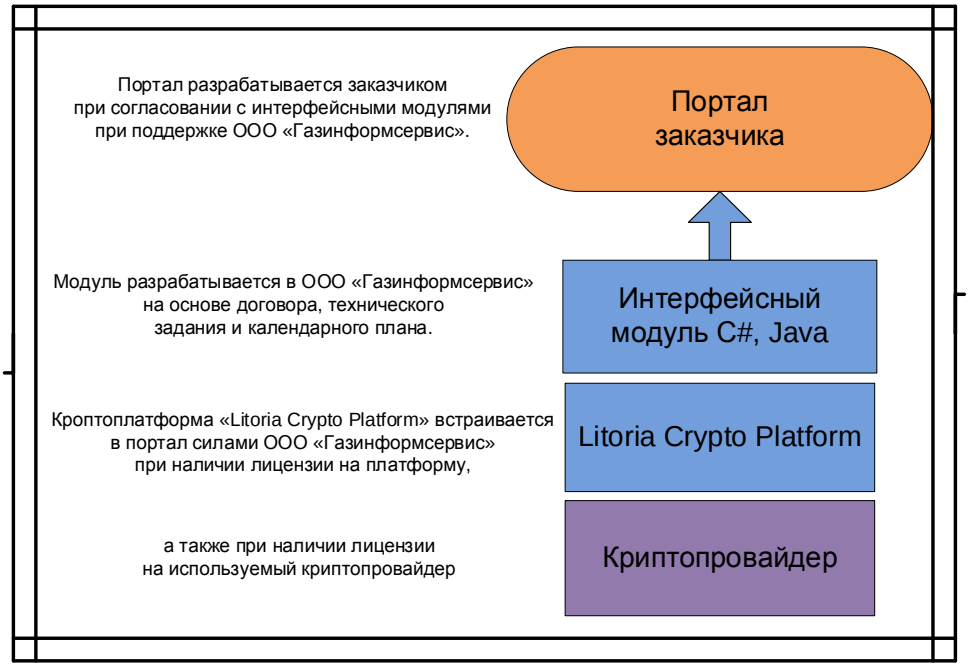


Рисунок 3.3.1. Решение встраивания

После встраивания платформы «Litoria Crypto Platform» в систему электронного документооборота каждый конечный пользователь этой системы может использовать определенные владельцем системы операции с использованием необходимых функций криптоплатформы. При этом конечный пользователь должен иметь свой цифровой сертификат (стандарта, соответствующего используемому криптопровайдеру) и соответствующую ключевую информацию. При этом личный сертификат пользователя должен быть установлен в хранилище сертификатов «Личное», а ключевая информация должна храниться в соответствии с регламентом системы. Сертификаты других доверенных пользователей, с которыми будет необходимо взаимодействовать, должны быть установлены в хранилище сертификатов «Другие пользователи».

3.3.1 Интеграция с решениями Citrix

Наиболее значимым решением встраивания криптоплатформы в систему документооборота является ее интеграция с решениями терминального доступа на основе Citrix Virtual Channel (CVC).

Схема интеграции приведена на рисунке 3.3.2.

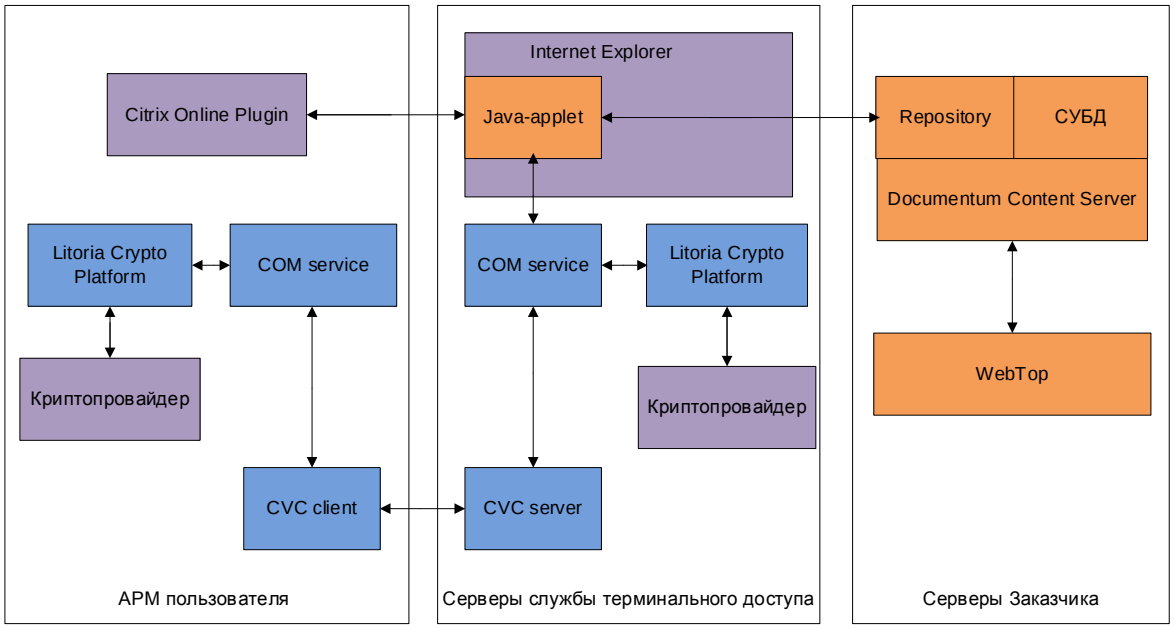


Рисунок 3.3.2. Интеграция с Citrix

На схеме синим цветом показаны компоненты, которые разработала компания «Газинформсервис»; фиолетовым – дополнительно устанавливаемые компоненты, которые используются компонентами компании «Газинформсервис»; оранжевым – компоненты, разрабатываемые Заказчиком.

В данном решении интерфейсный модуль реализован как COM сервер (на схеме – COM service), который посредством COM интерфейсов осуществляет связь между Java-апплетом и основными функциями криптографической платформы «Litoria Crypto Platform» и предоставляет доступ к каналу передачи данных (Citrix Virtual Channel). Над передаваемыми данными с использованием криптографической платформы «Litoria Crypto Platform» и криптопровайдера выполняются следующие криптографические операции:

- создание УЭП;
- добавление УЭП;
- проверка УЭП;
- шифрование файла;
- расшифровывание файла.

3.3.2 Интеграция с SharePoint

Применение криптографической платформы «Litoria Crypto Platform» для защиты электронного документооборота, реализованного на базе Microsoft SharePoint, является еще одним фундаментальным решением компании «Газинформсервис».

Общая схема взаимодействия компонент интеграции криптоплатформы с порталом Microsoft SharePoint представлена на рисунке 3.3.3.

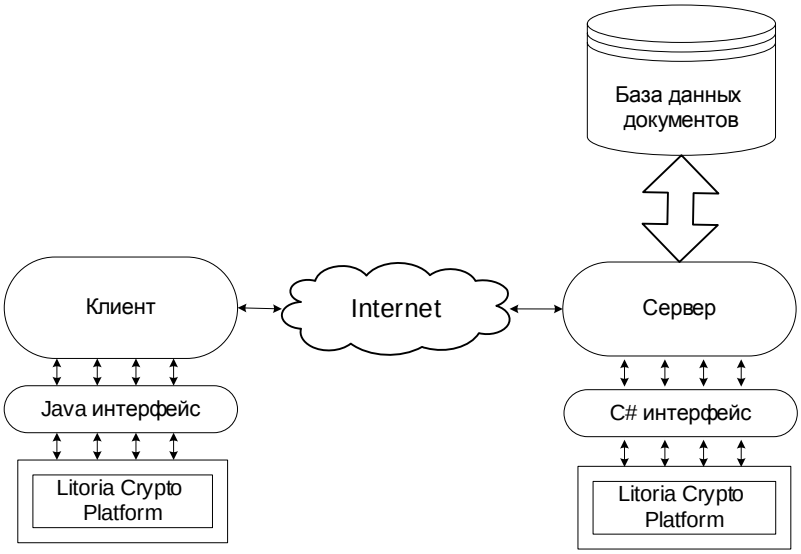


Рисунок 3.3.3. Интеграция с SharePoint

В данном решении для сервера создан интерфейсный модуль C#. Посредством его интерфейсов осуществляется связь между сервером и основными функциями криптоплатформы. Для пользователей создан интерфейсный модуль Java, с помощью которого пользователь указывает тип и параметры необходимой операции. Для пользователя доступны все криптографические функции криптографической платформы «Litoria Crypto Platform»:

- создание УЭП;
- добавление УЭП;
- проверка УЭП;
- шифрование файла;
- расшифровывание файлов.

3.3.3 Система ДТС

Система ДТС предназначена для обеспечения функционала подтверждения подписей, выполненных с использованием сертификатов, выданных различными (в том числе иностранными) удостоверяющими центрами.

Система интегрируется в инфраструктуру открытых ключей (ИОК) компании и используется ее клиентами, подразделениями и дочерними предприятиями при осуществлении бизнес-процессов, связанных с подтверждением подписи в электронных документах, защитой информации, обеспечением юридической силы и архивного хранения электронных документов.

Система ДТС предназначена для выполнения следующих функций:

- подтверждение электронной подписи сертификата ключа подписи, выданного доверенным удостоверяющим центром (список доверенных удостоверяющих центров определяется наличием соглашений о взаимном доверии с использующимся удостоверяющим центром, а также законодательством РФ);
- удостоверение обладания информацией в указанный момент времени;
- удостоверение обладания информацией без предоставления ее сервису (по хеш);
- подтверждение ЭП электронного документа.

Результатом выполнения той или иной функции ДТС служит созданная DVCS-сервером квитанция. Схема создания запроса на проверку подписи и предоставления отчета о проверки представлена на рисунке 3.3.4.

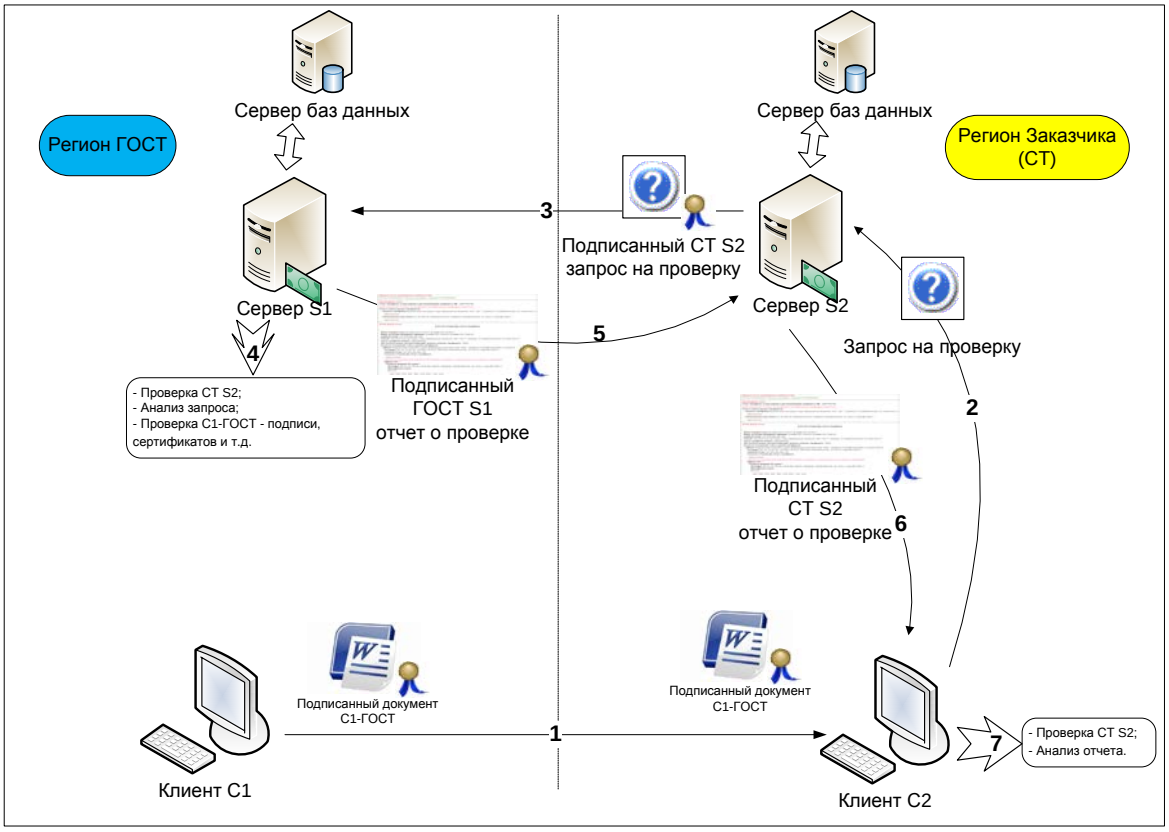


Рисунок 3.3.4. Схема запроса в инфраструктуре DVCS

Для осуществления проверки подписи, создания запроса на проверку и отчета о проверке на Клиентах С1, С2 и Серверах S1, S2 устанавливается криптографическая платформа «Litoria Crypto Platform».

В данном решении криптоплатформа, в соответствии с RFC3029, выполняет следующие функции:

- создание и отправка 4-х типов DVCS-запросов (CPD, CCPD, VSD, VPKC);
- формирование DVC-квитанции;
- анализ DVC-квитанции и вывод информации.

4 Входные и выходные данные

4.1 Входные данные

Криптографическая платформа «Litoria Crypto Platform» выполняет функции шифрования/расшифровывания и создания/проверки ЭП файлов следующего типа:

- файл любого типа *.* (для генерации УЭП);
- подписанные ЭП файлы, в которых ЭП совмещена с исходным файлом;
- подписанные ЭП файлы, в которых ЭП отделена от исходного файла;
- файл сертификата.

4.2 Выходные данные

На выходе криптографическая платформа «Litoria Crypto Platform» может формировать следующую информацию:

- байтовый массив данных (обработанный оригинал файла с ЭП);
- байтовый массив данных (файлы отделенных ЭП);
- сертификаты (из ЭП);
- четыре статуса проверок достоверности подписи (ЭП на документ, ЭП на штампе времени, ЭП на OCSP ответе, ЭП на «закрывающем» штампе);
- дату и время из штампа времени;
- сообщение об ошибке (если она имеет место).

Список сокращений

CCPD – Certification of Claim of Possession of Data (подтверждение требования владения данными)

COM – Component Object Model (модель компонентных объектов)

CPD – Certification of Possession of Data (подтверждение владения данными)

CSP – Cryptographic Service Provider (провайдер криптографических услуг, криптопровайдер)

CVC – Citrix Virtual Channel (виртуальный канал Citrix)

DVC – Data Validation and Certificate (подтверждение подлинности данных и сертификата)

DVCS – Data Validation and Certification Server (сервер сертификации и проверки достоверности данных)

HDD – Hard Disk Drive (жесткий диск)

IIS – Internet Information Services – до версии 5.1 Internet Information Server (набор серверов для нескольких служб интернета от компании Майкрософт)

LSB – Linux Standard Base (основной стандарт Linux)

MS – MicroSoft

OCSP – Online Certificate Status Protocol (протокол получения статуса сертификата в реальном времени)

RAM – Random Access Memory (запоминающее устройство с произвольным доступом)

RFC – Request For Comments

SVGA – Super Video Graphics Array (видеоадаптер, совместимый с VGA)

TSP – Time-Stamp Protocol (протокол штампов времени)

VKPC – Validation of Public Key Certificates (проверка открытого ключа сертификата)

VSD – Validation of digitally Signed Document (проверка цифрового подписанного документа)

ГОСТ – ГОсударственный СТандарт

ДТС – Доверенная Третья Сторона

ИОК – Инфраструктура Открытых Ключей

ОС – Операционная Система

РФ – Российская Федерация

СТ – СТандарт

СЭД – Система Электронного Документооборота

УЭП – Усовершенствованная Электронная Подпись

ЭП – Электронная Подпись