ГАЗИНФОРМСЕРВИС

Внедрение ЭП в автоматизированные трансграничные системы документооборота

Кирюшкин Сергей Анатольевич, к.т.н.
Советник генерального директора
Kiryushkin-S@gaz-is.ru

Петров Сергей Владимирович,
Начальник отдела разработки средств защиты департамента разработки и испытаний
Petrov-S@gaz-is.ru

www.gaz-is.ru
Тел. +7(812)305-20-50

Библиотека «BHCryptography»

Назначение

- Обеспечение стандартного и простого способа реализации функционала ЭЦП и шифрования в прикладных системах;
- Обеспечение поддержки усовершенствованной ЭЦП (ETSI TS 101 733);
- Поддержка сервисов ДТС: OCSP, DVCS, TSP;
- Обеспечение поддержки множества СКЗИ;

Библиотека «BHCryptography»

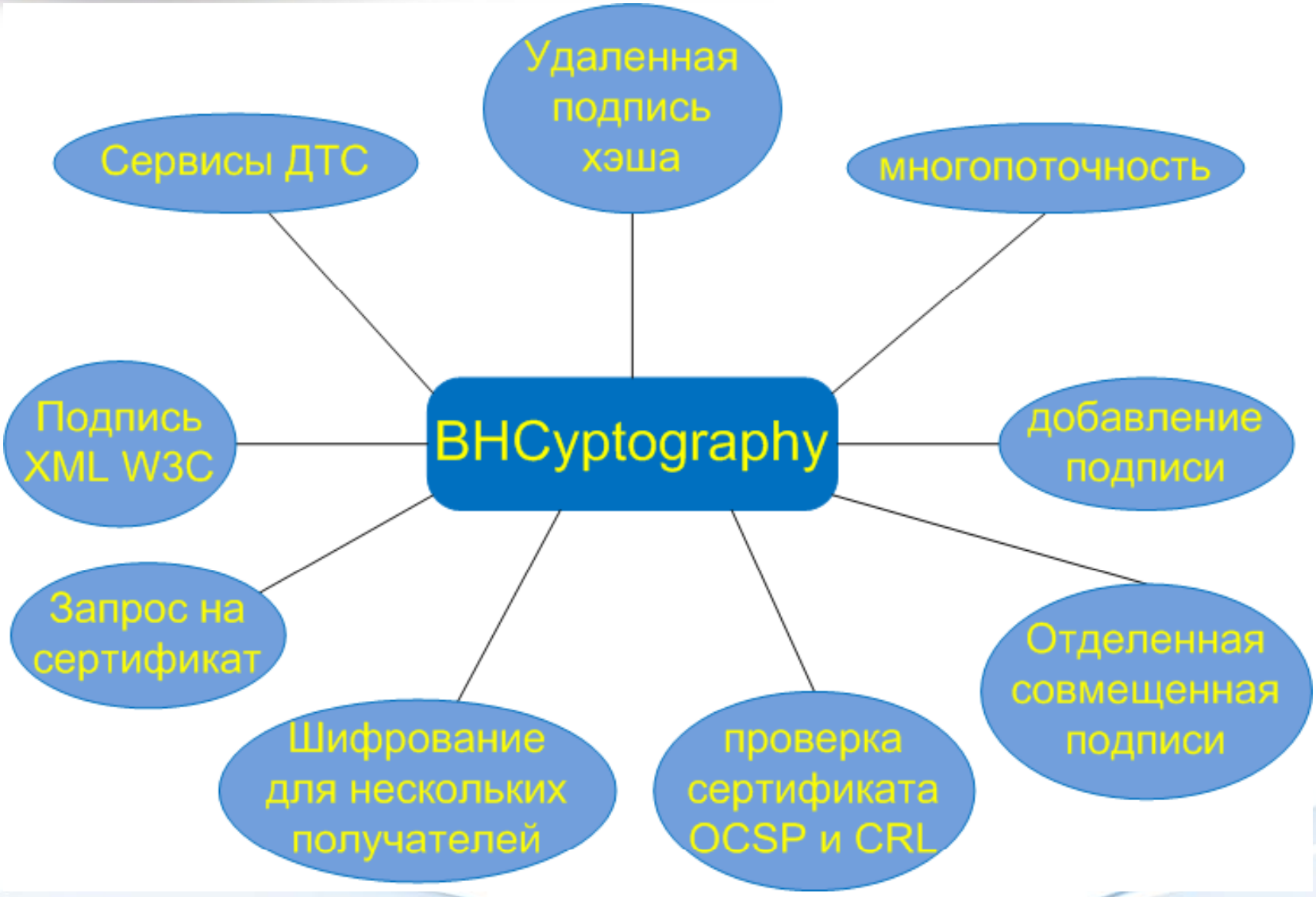
Архитектура решения

ГАЗИНФОРМСЕРВИС

Библиотека «BHCryptography»

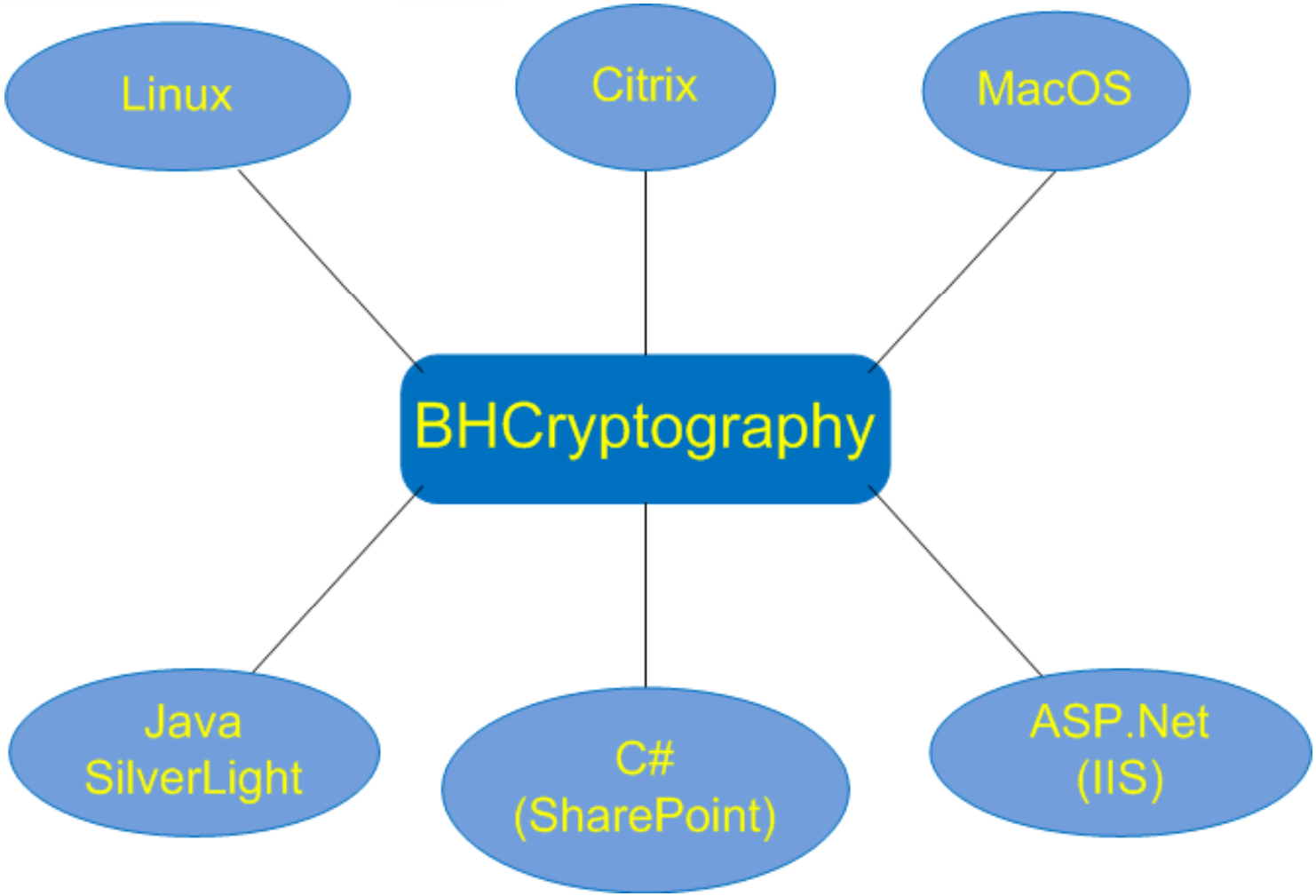
Функциональные возможности

ГАЗИНФОРМСЕРВИС



Библиотека «BHCryptography»
Возможности интеграции и совместимости

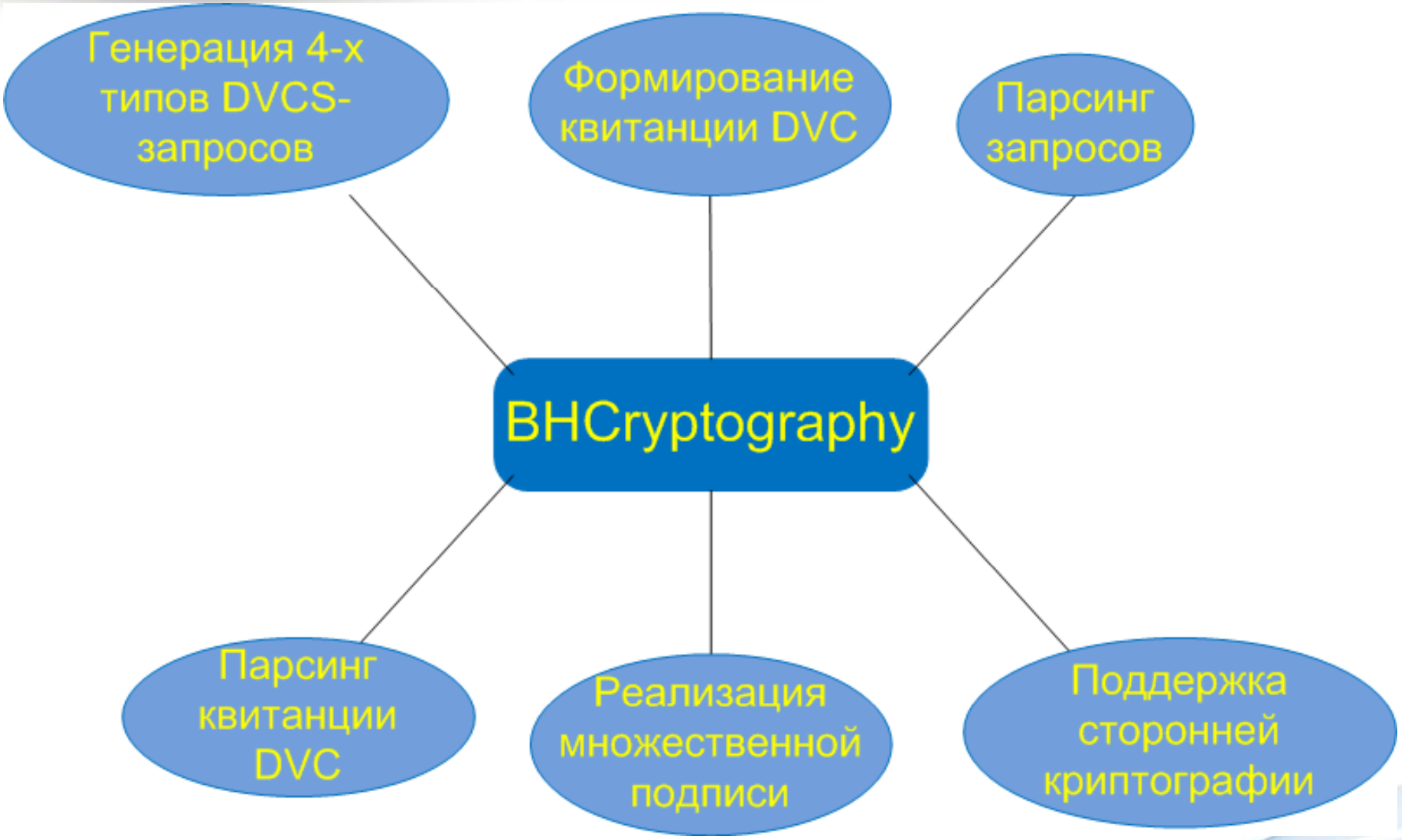
ГАЗИНФОРМСЕРВИС



Библиотека «BHCryptography»

Функциональные возможности ДТС

ГАЗИНФОРМСЕРВИС

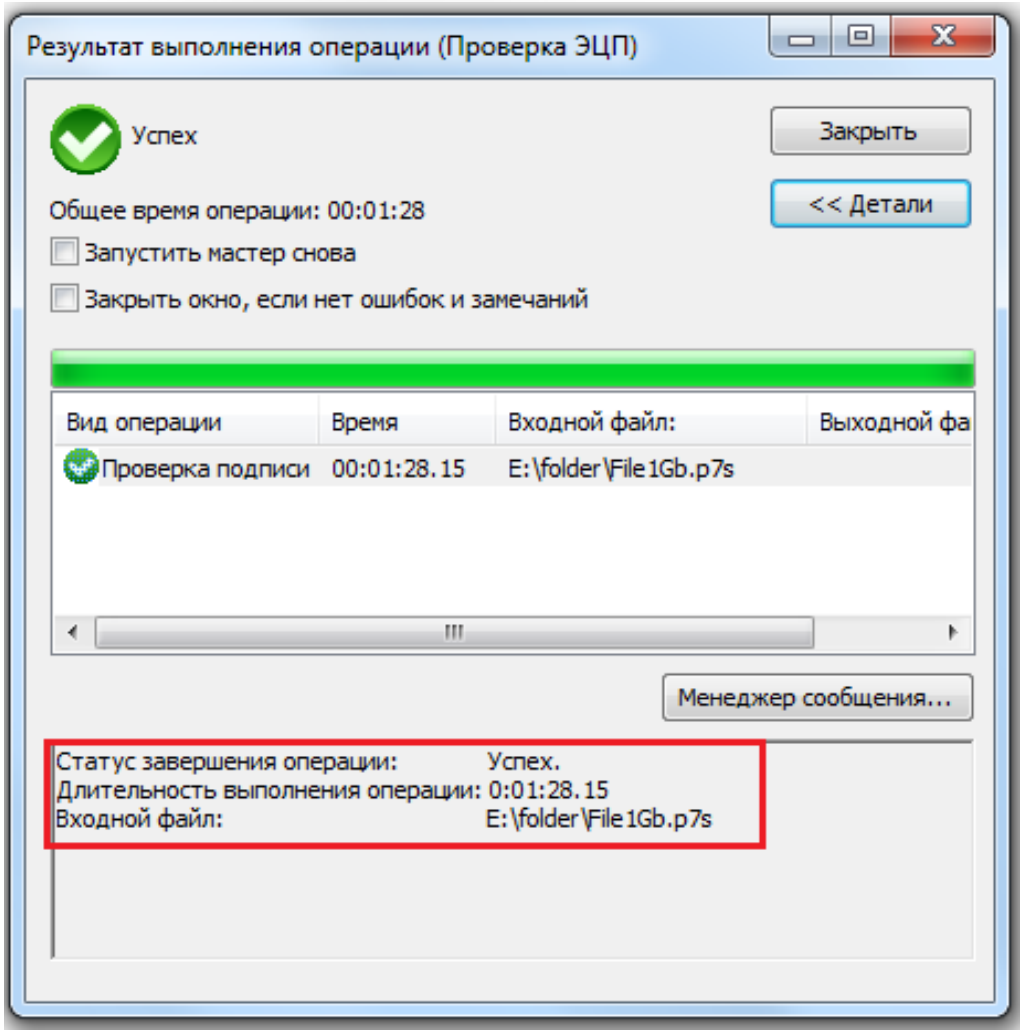


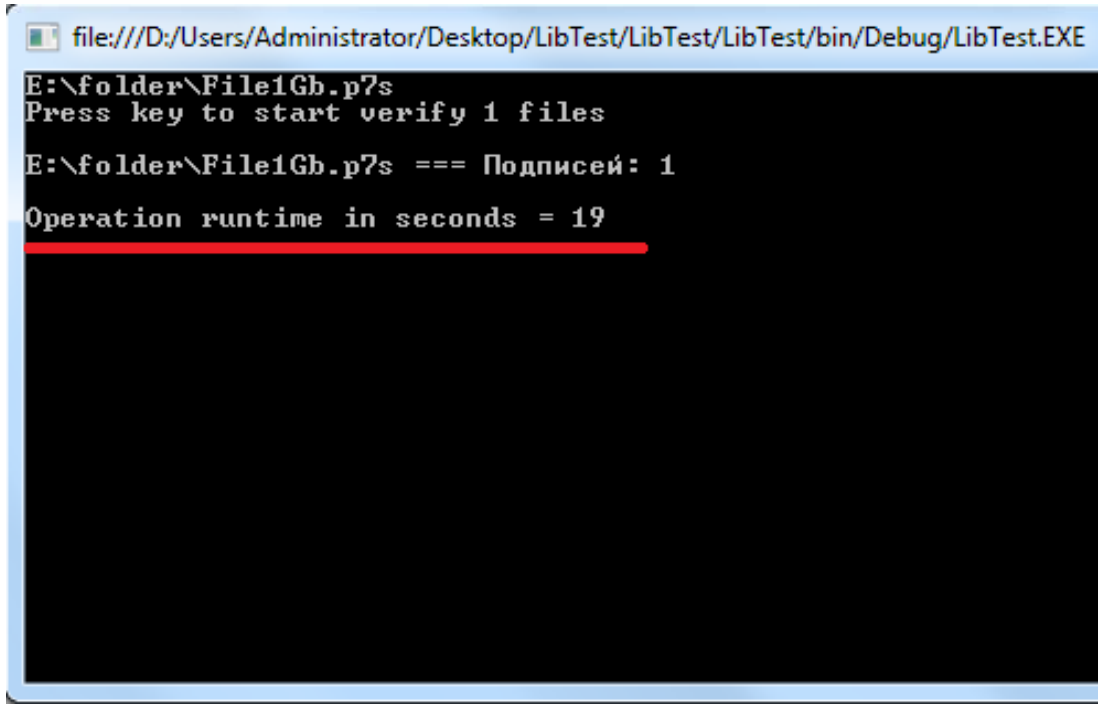
Библиотека «BHCryptography»
Ответственность сторон в процессе встраивания

ГАЗИНФОРМСЕРВИС

Библиотека «BHCryptography»
Скорость проверки подписи
Файла размером 1 Гб

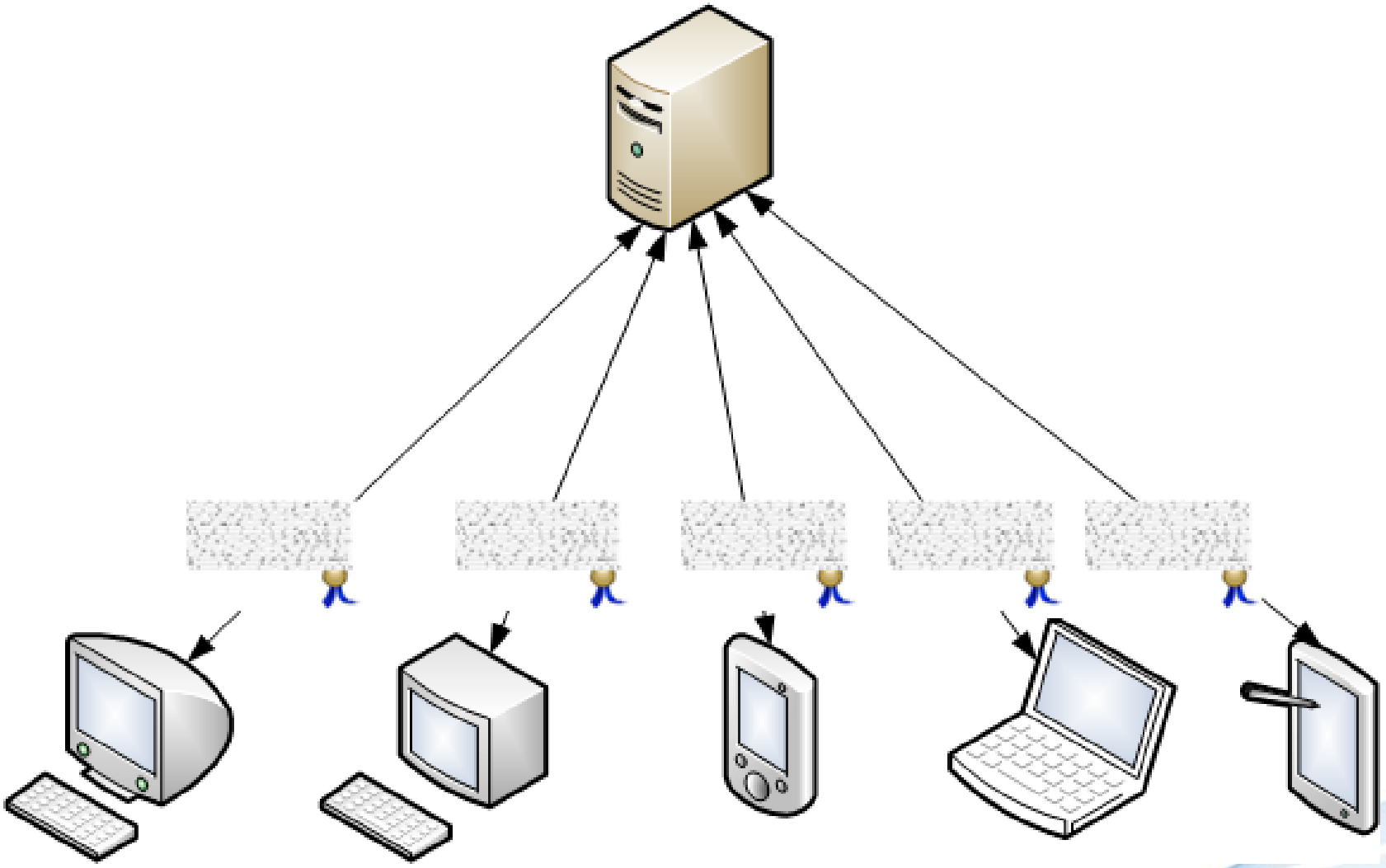
ГАЗИНФОРМСЕРВИС





Проверка подписи выполняется быстрее в 4 раза

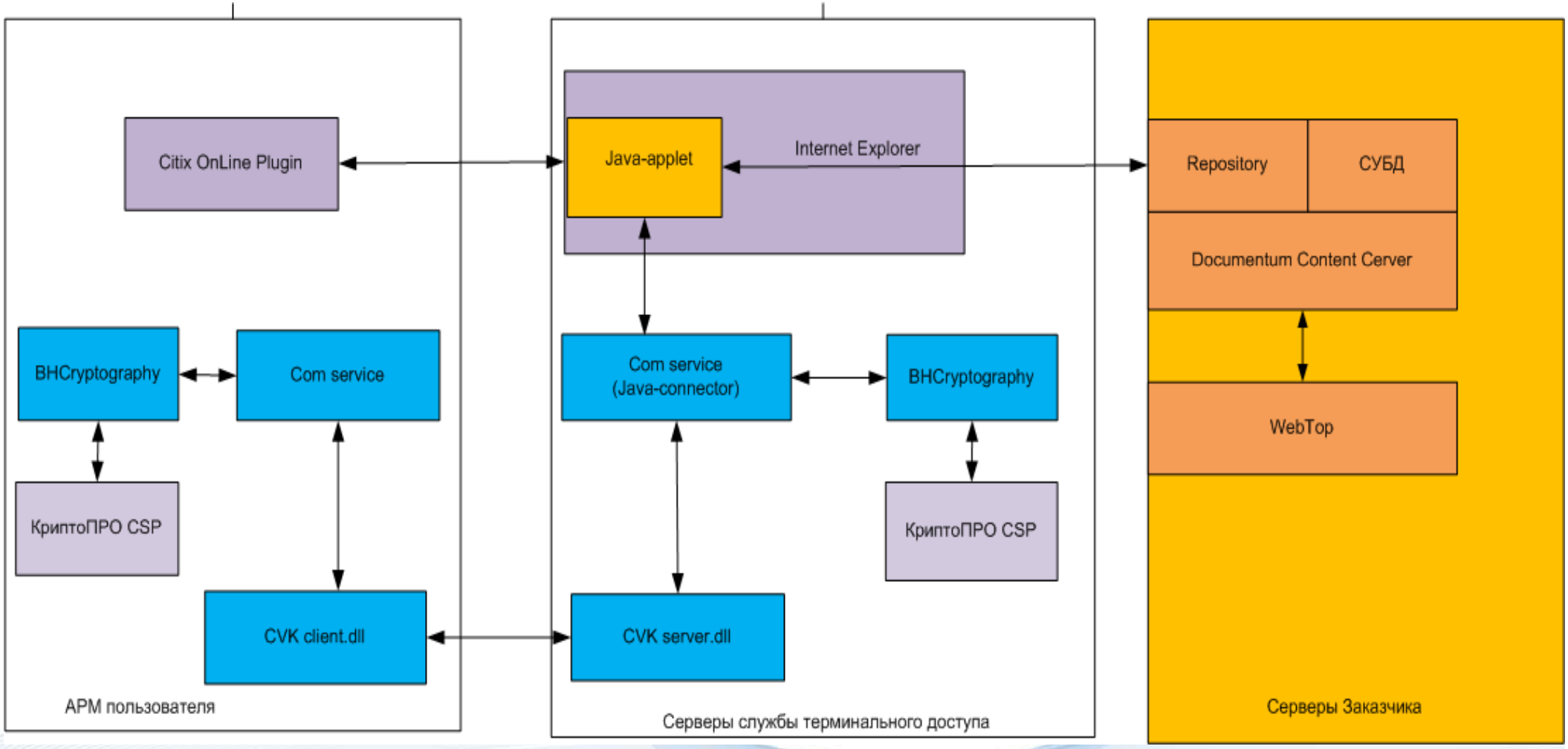
Параллельная обработка



Библиотека «BHCryptography»
Интеграция с Citrix
Функциональная схема

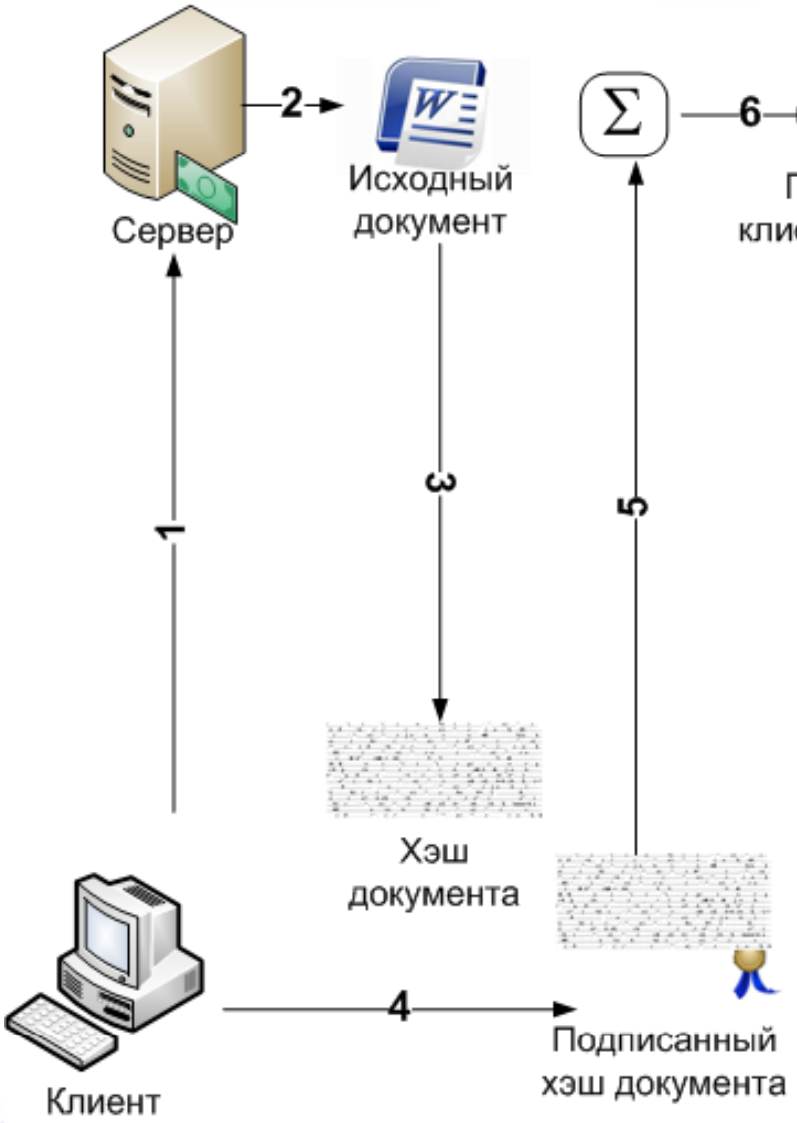
ГАЗИНФОРМСЕРВИС

Синим цветом показаны компоненты, разрабатываемые ГИС. Фиолетовым цветом – доп. устанавливаемые компоненты вендоров, которые будут использоваться компонентами ГИС. Желтым цветом – компоненты, разрабатываемые Заказчиком



Библиотека «BHCryptography»

Подпись хэша документа



1. Запрос документа на подпись
2. Чтение документа сервером
3. Отправка хэша документа клиенту
4. Подпись хэша документа
5. Отправка подписанного хэша серверу
6. Формирование подписанного документа

Библиотека «BHCryptography»
Встраивание на Web-сервер IIS, ASP.Net
Сервер DVCS.GAZ-IS.RU

ГАЗИНФОРМСЕРВИС

Служба Доверенной Третьей Стороны (тестовый режим)

Данная служба работает в режиме реального времени. Входным параметром службы является подписанный документ(С ПРИСОЕДИНЕННЫМИ ДАННЫМИ) в формате pkcs# 7. Результат проверки действительности подписей под документами представлен в виде формы с кратким описанием подписей и статусом проверки. Доказательством проверки является квитанция, полученная от службы ДТС.

Для формирования DVC-квитанции скачайте и сохраните тестовые документы, загрузите их в форму, нажмите «проверить». При наличии средств создания ЭП, вы можете создать такие документы самостоятельно.

Тестовые документы:

Подписи ГОСТ в формате pkcs# 7:

- Действительные данные, содержащие одну подпись
- Не действительные данные, содержащие одну подпись

Подписи СТБ РБ в формате pkcs# 7:

- Действительные данные, содержащие одну подпись

Подписи RSA в формате pkcs# 7:

- Действительные данные, содержащие одну подпись MS BASE
- Действительные данные, содержащие одну подпись Unizeto Technologies S.A.

Подписи, созданные с использованием нескольких алгоритмов в формате pkcs# 7 (множественные подписи):

- Действительные данные, содержащие 3 подписи: RSA, ГОСТ, СТБ РБ

Проверка документа:

Сюда загрузить проверяемый документ

Подписанный документ: Обзор...

Проверить

Предоставляемая услуга носит информационный характер и не может быть использована в качестве доказательств в судах различных инстанций.

Библиотека «BHCryptography»
DVC-квитанция - результат проверки множественной подписи ГОСТ, RSA, РБ

ГАЗИНФОРМСЕРВИС

Подлинность документа НЕ ПОДТВЕРЖДЕНА

Количество подписей в документе: 3

Результат проверки ЭЦП 1: Подпись ДЕЙСТВИТЕЛЬНА

Владелец сертификата : C=RU, CN=Test RSA

Уполномоченное лицо УЦ : CN=Test Center CRYPTO-PRO, O=CRYPTO-PRO, C=RU, E=info@cryptopro.ru

Результат проверки ЭЦП 2: Подпись ДЕЙСТВИТЕЛЬНА

Владелец сертификата : CN=Пашечко Антон Михайлович, E=pashechko_a@gaz-is.ru, O="ООО ""ГАЗИНФОРМСЕРВИС""", OU=ДРиС, T=Ведущий инженер-программист, L=Санкт-Петербург, C=RU

Уполномоченное лицо УЦ : CN=Test Center CRYPTO-PRO, O=CRYPTO-PRO, C=RU, E=info@cryptopro.ru

Результат проверки ЭЦП 3: Подпись НЕДЕЙСТВИТЕЛЬНА

При проверке возникли следующие ошибки :

Сертификат подписчика недействителен

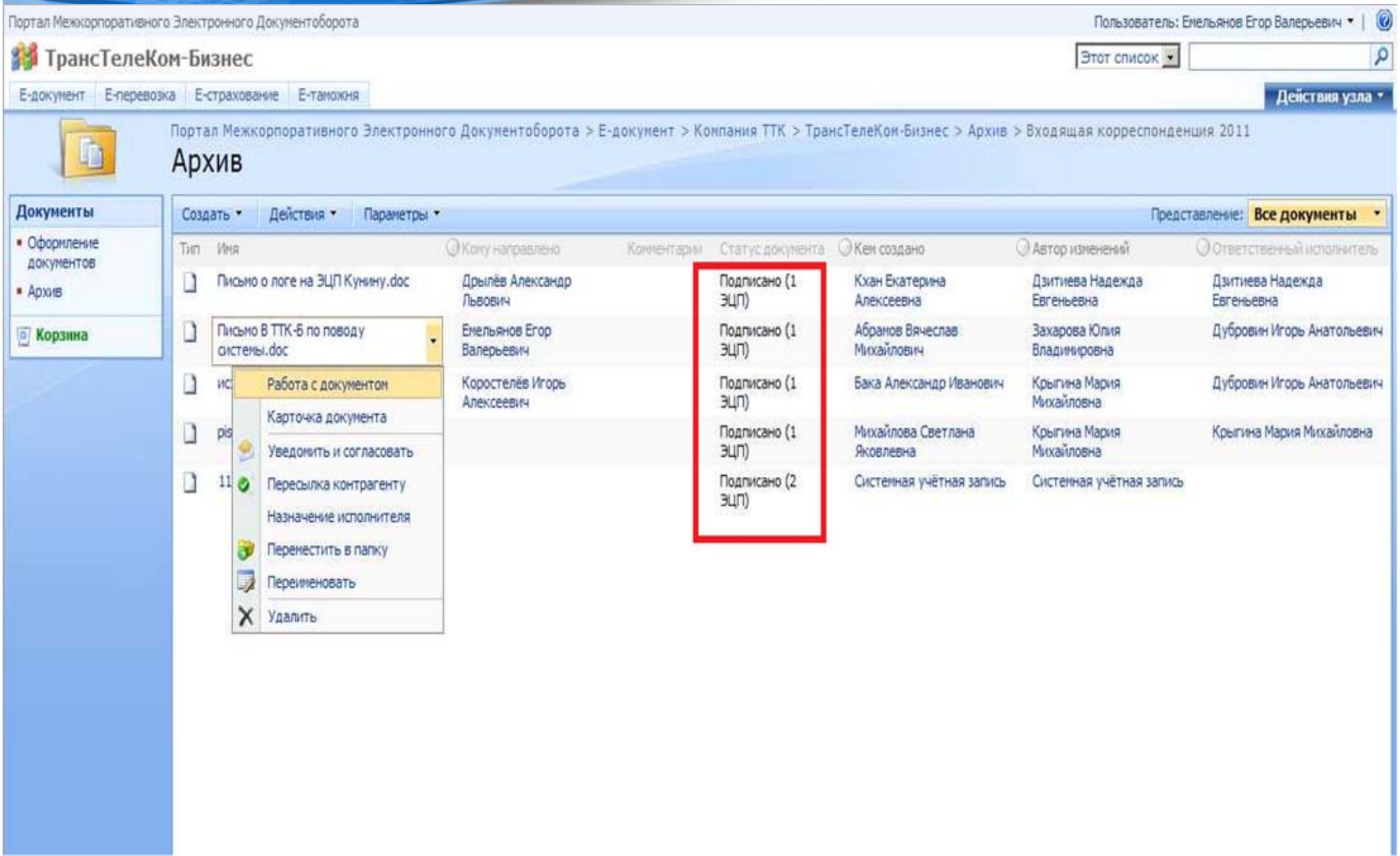
Владелец сертификата : E=nikolaev@ncmps.by, OID.2.5.4.41=Алексей Вячеславович, SN=Николаев, T=начальник сектора, OU=отдел информационных технологий, STREET="пр-т Победителей, 7, офис 1117", L=г. Минск, C=BY, O="РУП ""Национальный центр маркетинга и конъюнктуры цен""", CN="РУП ""Национальный центр маркетинга и конъюнктуры цен"""

Уполномоченное лицо УЦ : E=ca@ncmps.by, STREET="пр-т Победителей, 7, оф.1119", L=г. Минск, C=BY, O="РУП ""Национальный центр маркетинга и конъюнктуры цен""", CN="Корневой удостоверяющий центр РУП ""Национальный центр маркетинга и конъюнктуры цен"""

Скачать DVC квитанцию в бинарном виде Скачать DVC квитанцию в текстовом виде

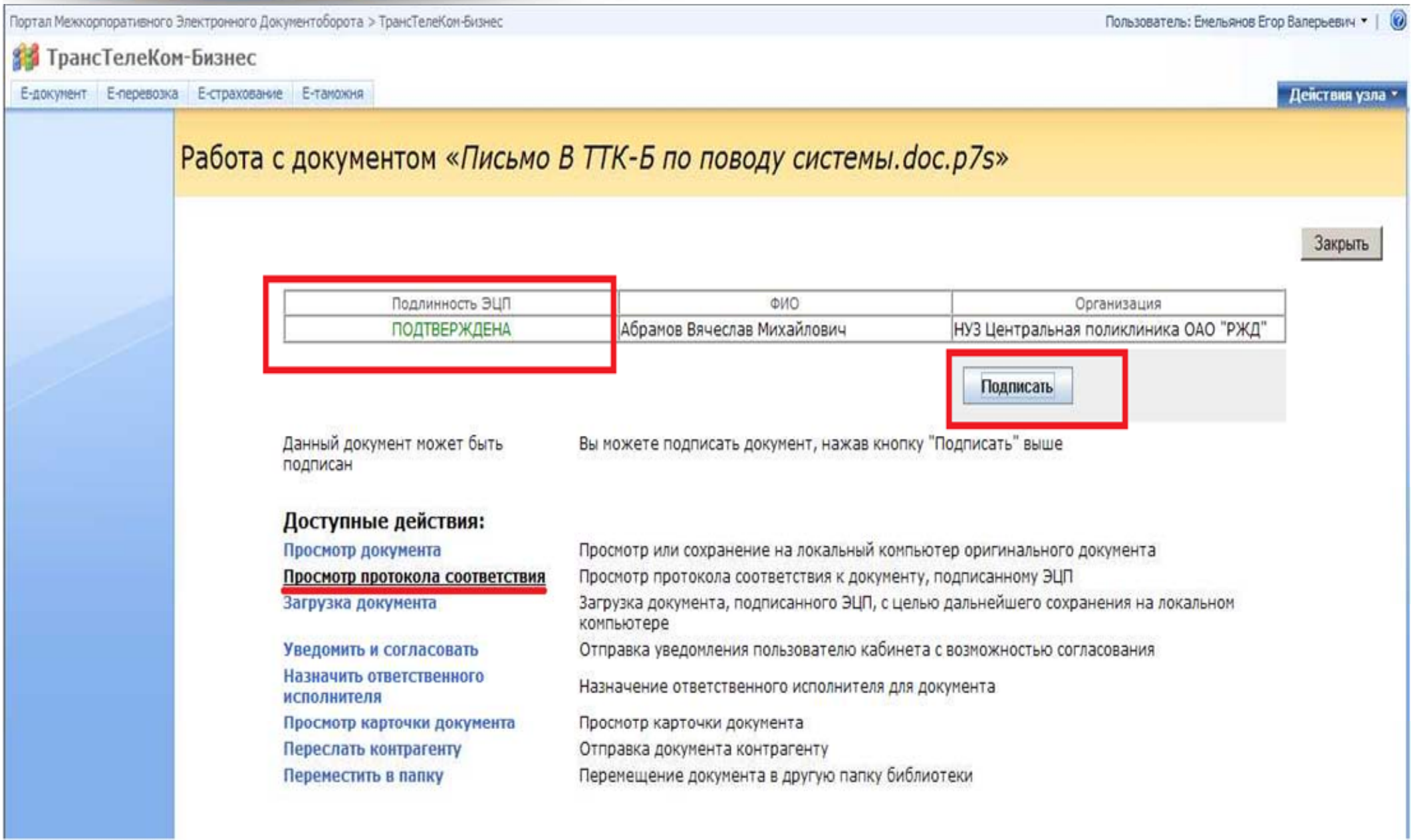
Библиотека «BHCryptography»
Пример встраивания: портал ООО «ТрансТелеком - Бизнес»

ГАЗИНФОРМСЕРВИС



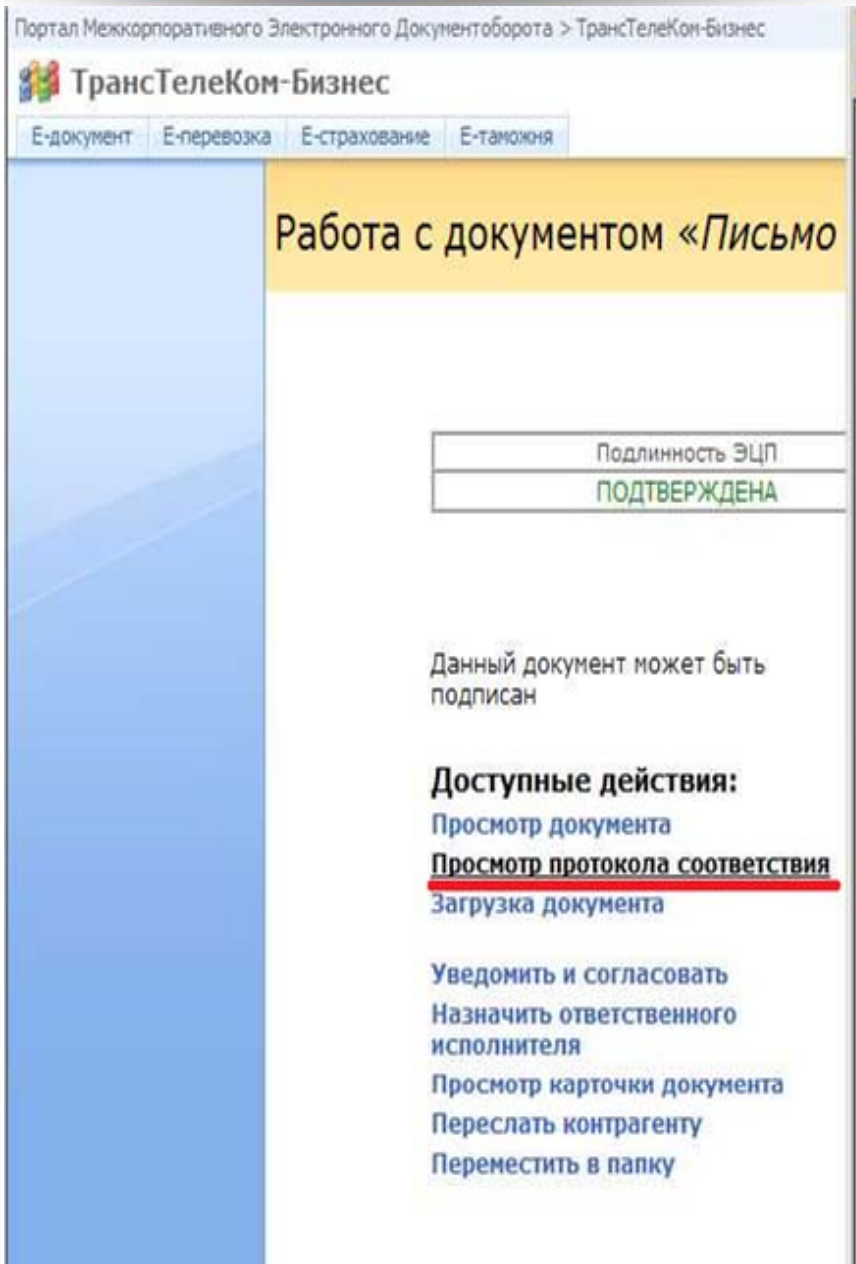
Библиотека «BHCryptography»
Пример встраивания: портал ООО «ТрансТелеком - Бизнес»

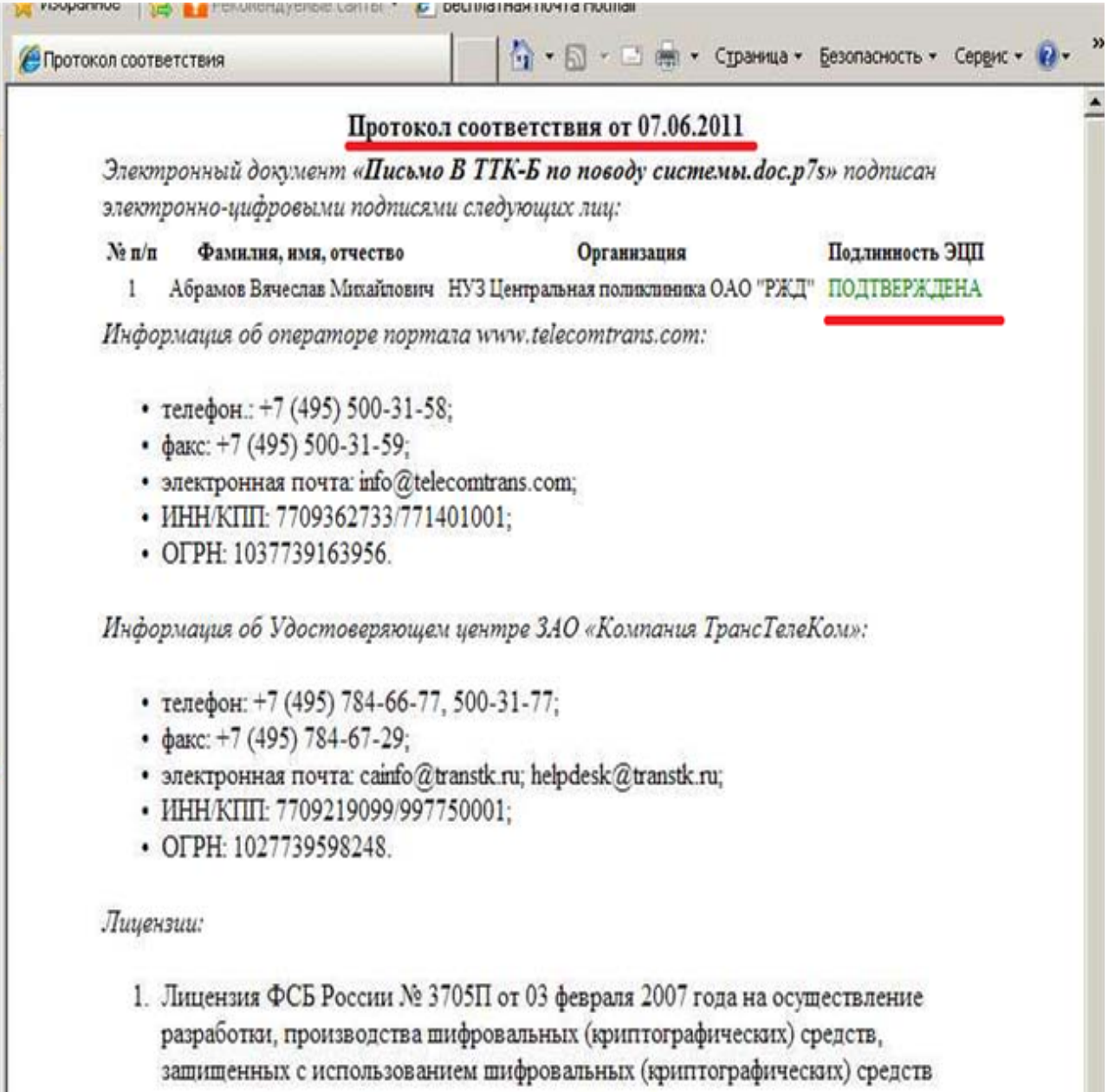
ГАЗИНФОРМСЕРВИС



Библиотека «BHCryptography»
Пример встраивания: портал ООО «ТрансТелеком - Бизнес»

ГАЗИНФОРМСЕРВИС





ГАЗИНФОРМСЕРВИС

Спасибо за внимание!

Кирюшкин Сергей Анатольевич, к.т.н.
Советник генерального директора
Kiryushkin-S@gaz-is.ru

Петров Сергей Владимирович,
Начальник отдела разработки
средств защиты департамента
разработки и испытаний
Petrov-S@gaz-is.ru

www.gaz-is.ru
Тел. +7(812)305-20-50