

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 «ВНСryptography»

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;

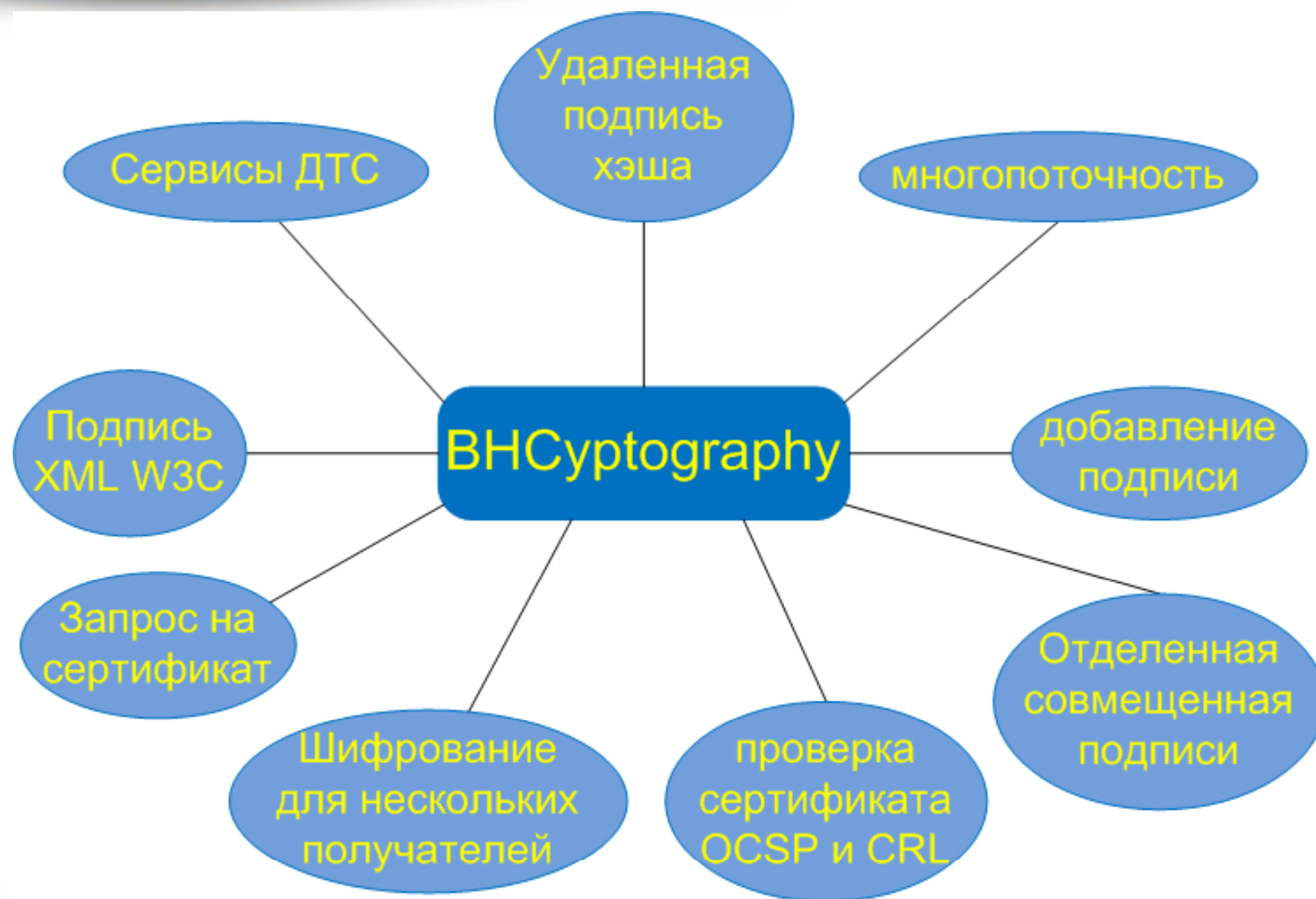
Обеспечение поддержки множества СКЗИ;

Приложение

Интерфейсный
модуль

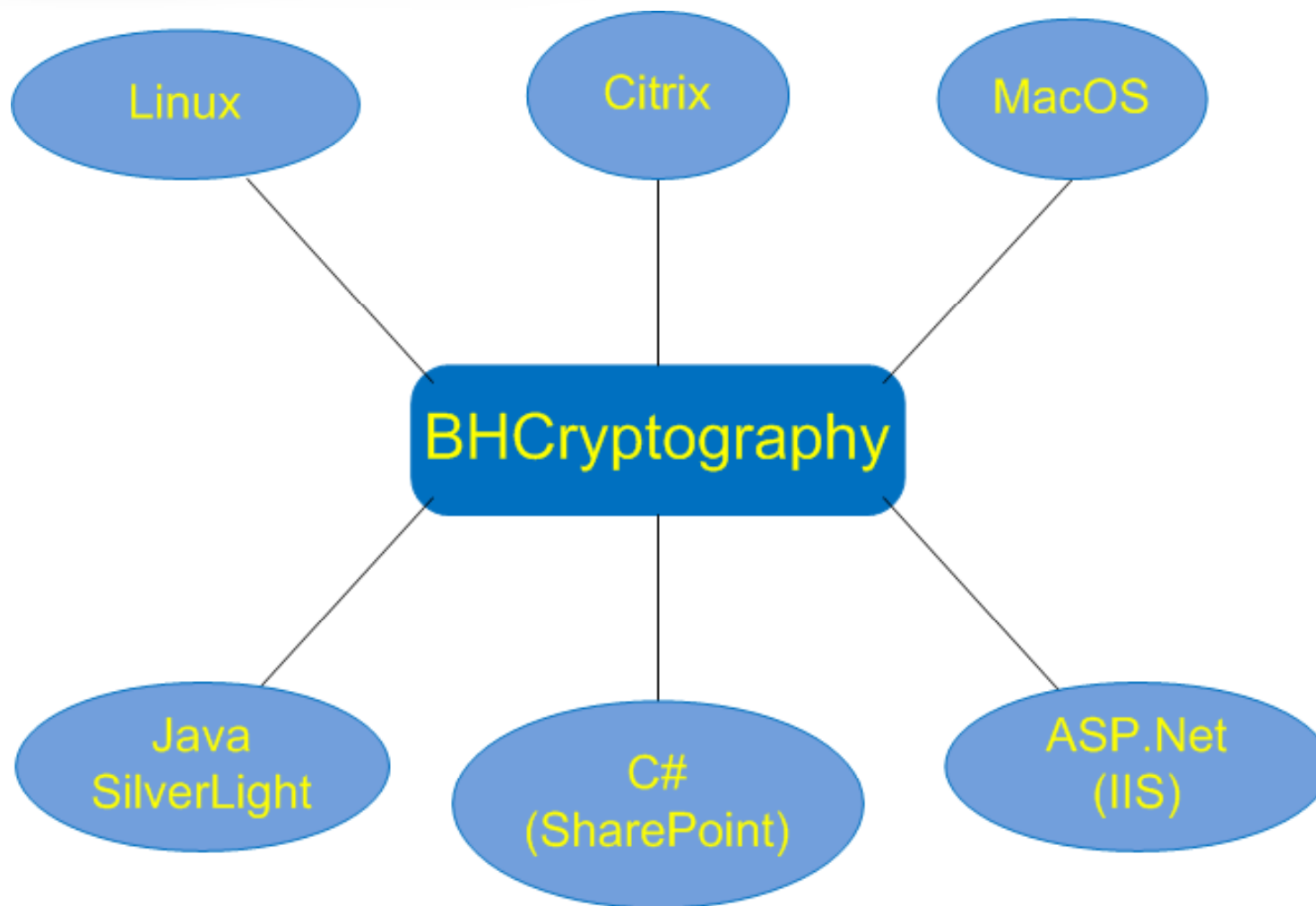
ВНСryptography

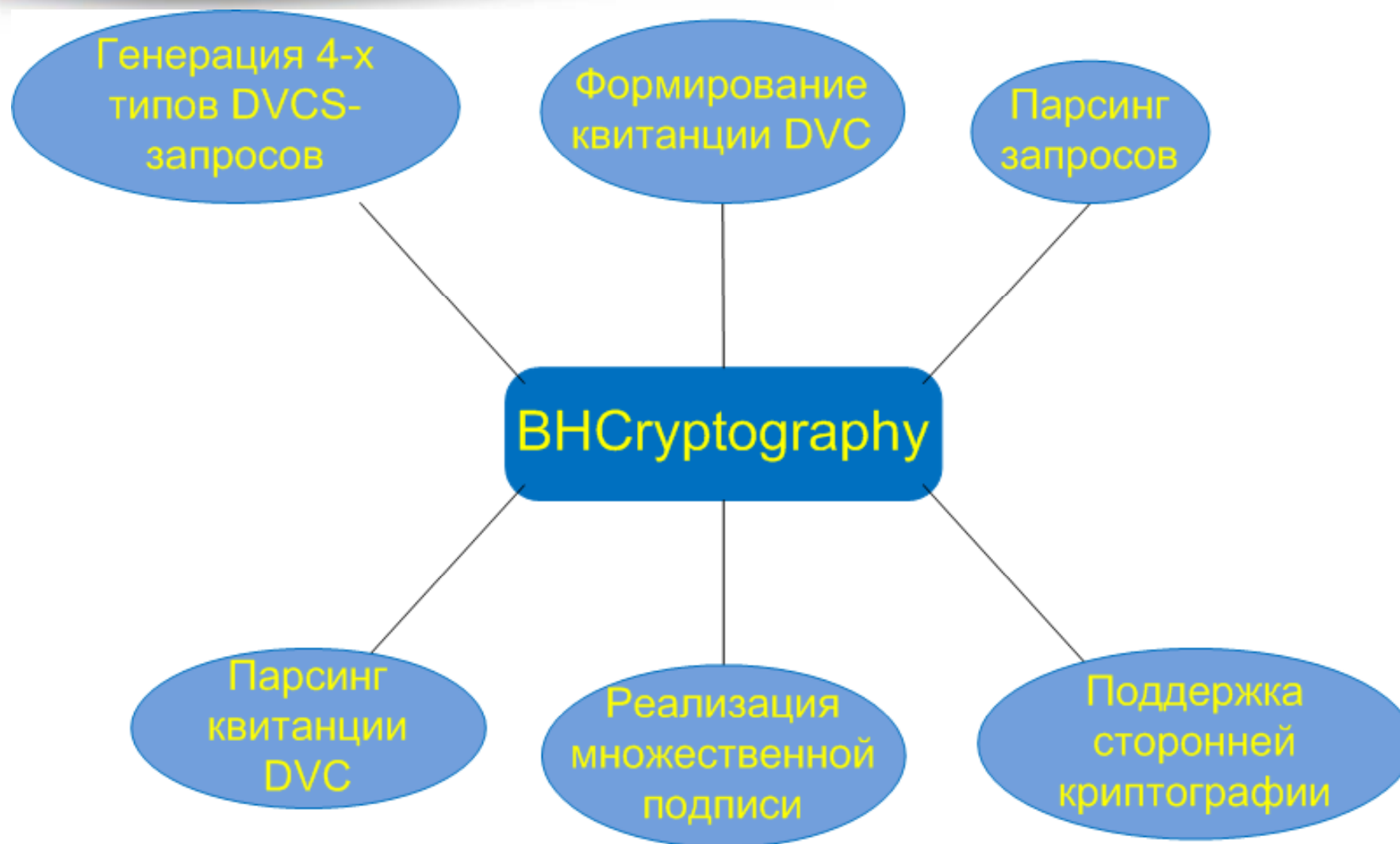
СКЗИ



Библиотека «ВНCryptography»

Возможности интеграции и совместимости





Библиотека «ВНСryptography»

Ответственность сторон в процессе встраивания

Портал
Заказчика



Интерфейс
администратора

Интерфейс
пользователя



Собственность заказчика:

- разрабатывается заказчиком;
- согласование с интерфейсными модулями;
- разрабатывается при поддержке ГИС;

Интерфейсный модуль для
взаимодействия с порталом
C#, Java

Собственность заказчика:

- разрабатывается ДРИ;
- ТЗ;
- договор;

ВНСryptography:
TSP-клиент
OCSP-клиент

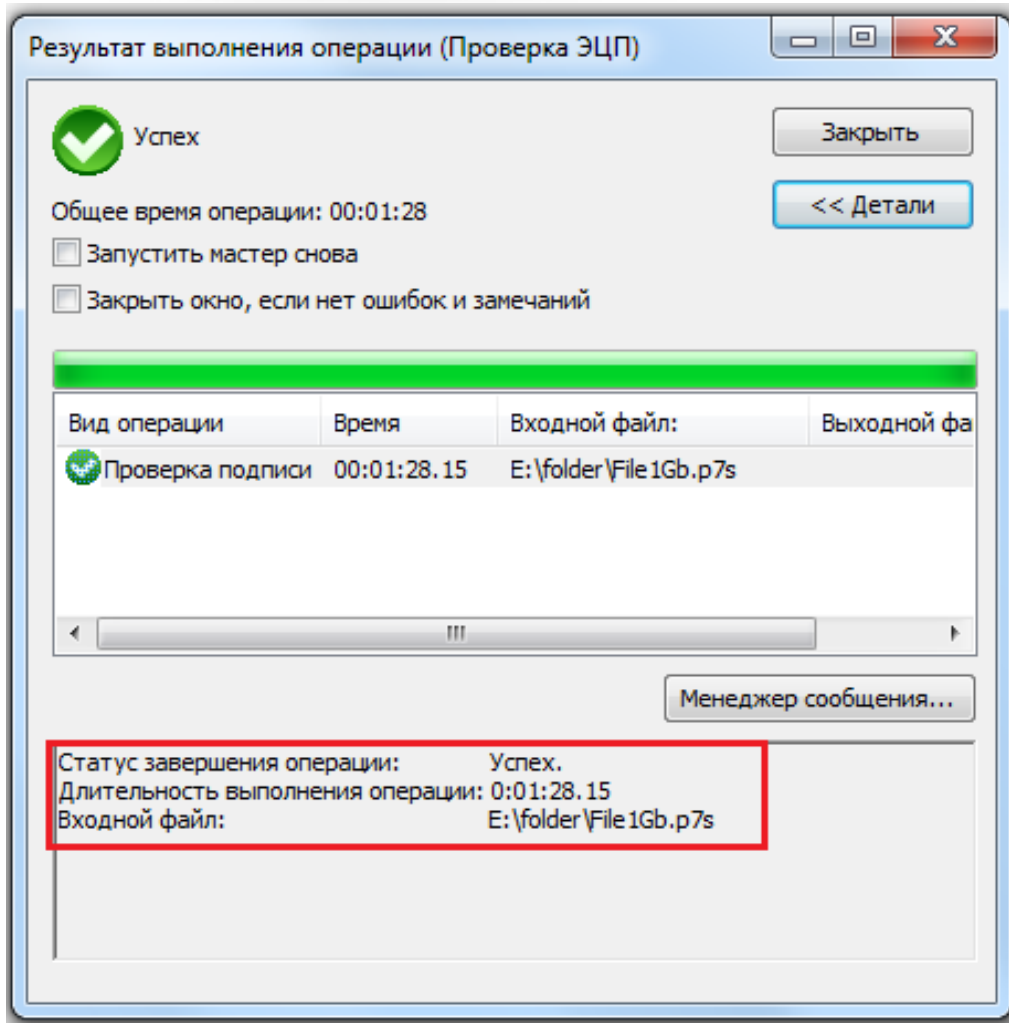
Собственность ООО
«Газинформсервис»

CryptoPro CSP

Собственность
«КриптоПро»

Библиотека «ВНСryptography»

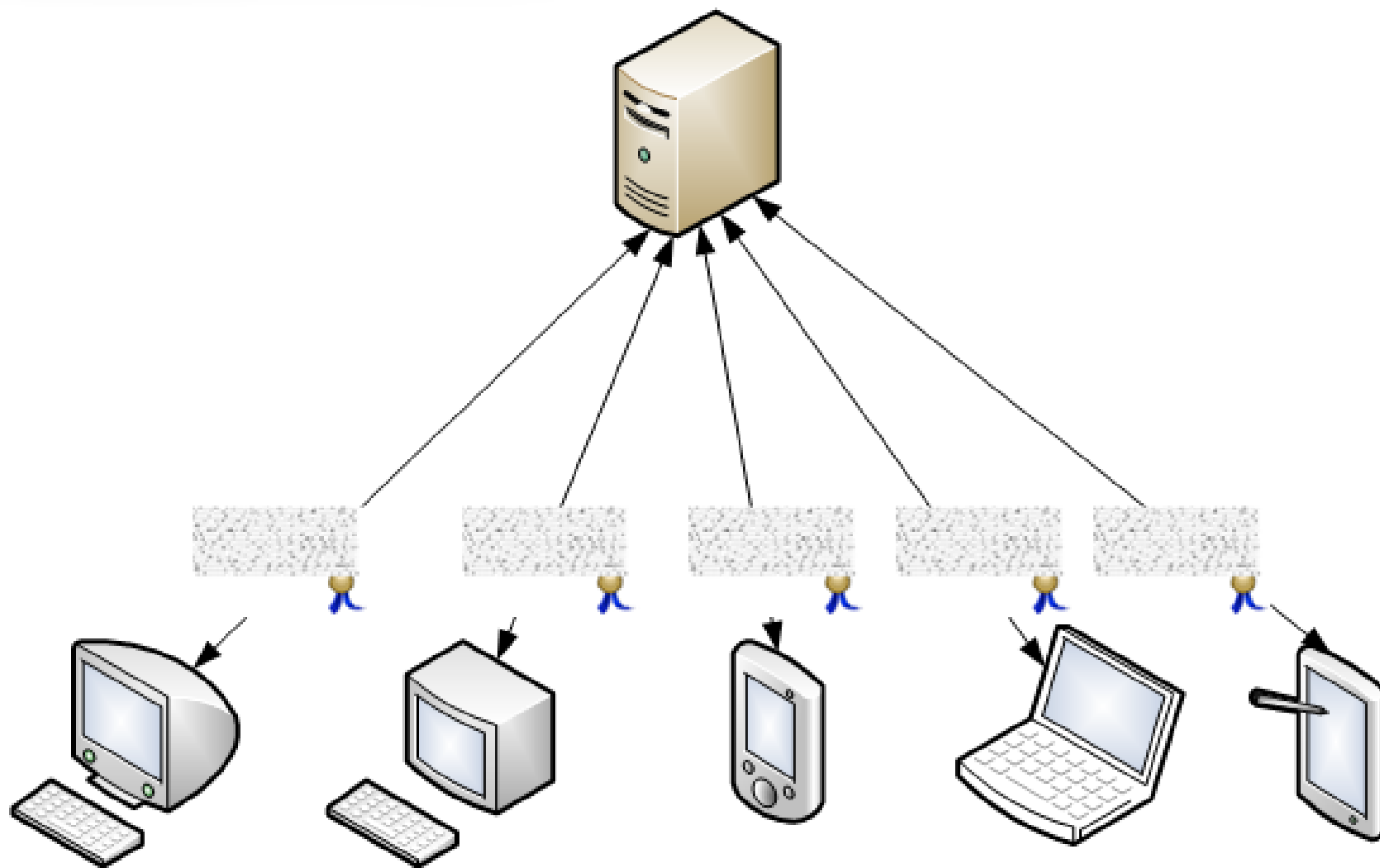
Скорость проверки подписи Файла размером 1 Гб



```
file:///D:/Users/Administrator/Desktop/LibTest/LibTest/LibTest/bin/Debug/LibTest.EXE
E:\folder\File1Gb.p7s
Press key to start verify 1 files
E:\folder\File1Gb.p7s === Подписей: 1
Operation runtime in seconds = 19
```

Проверка подписи выполняется
быстрее в 4 раза

Параллельная обработка

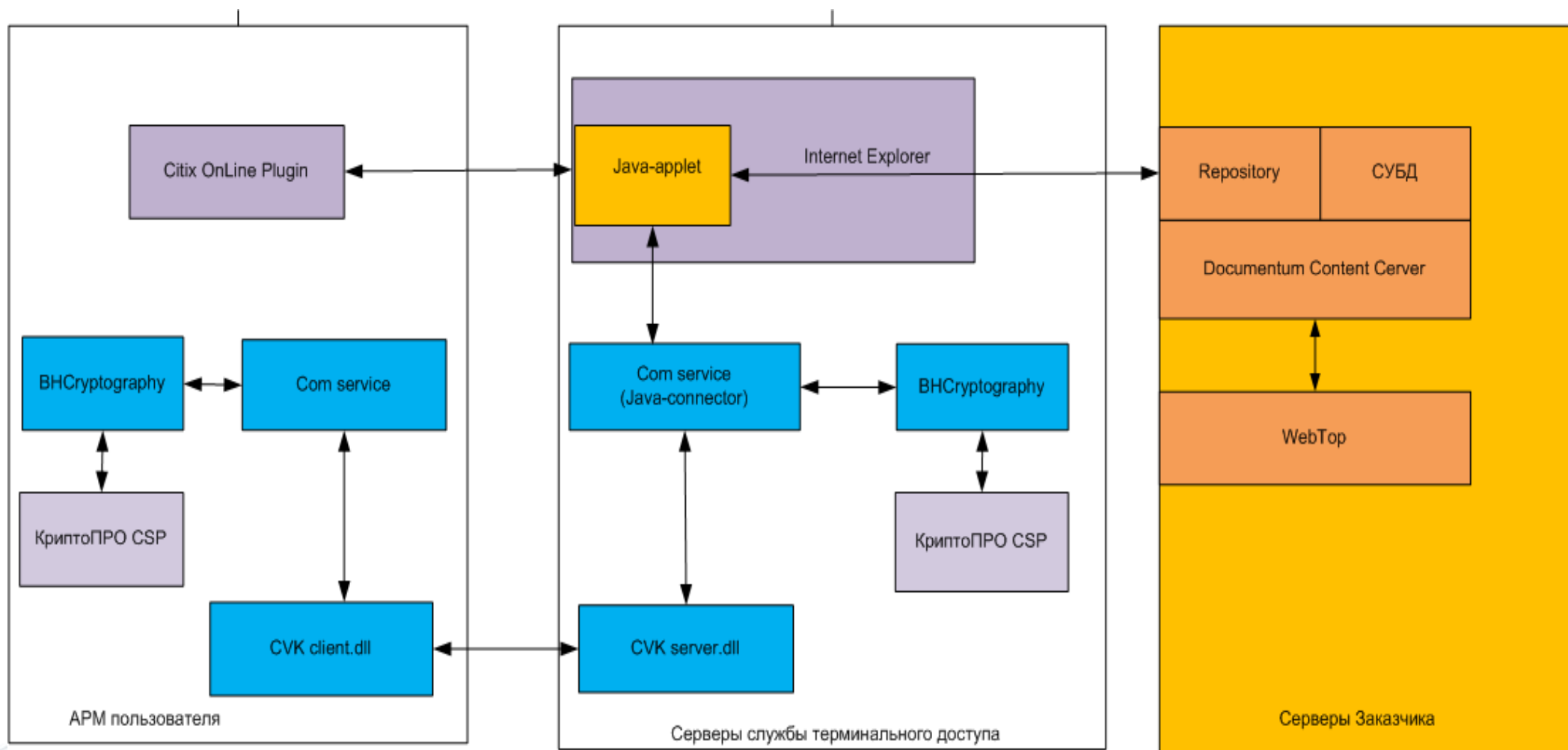


Библиотека «ВНСryptography»

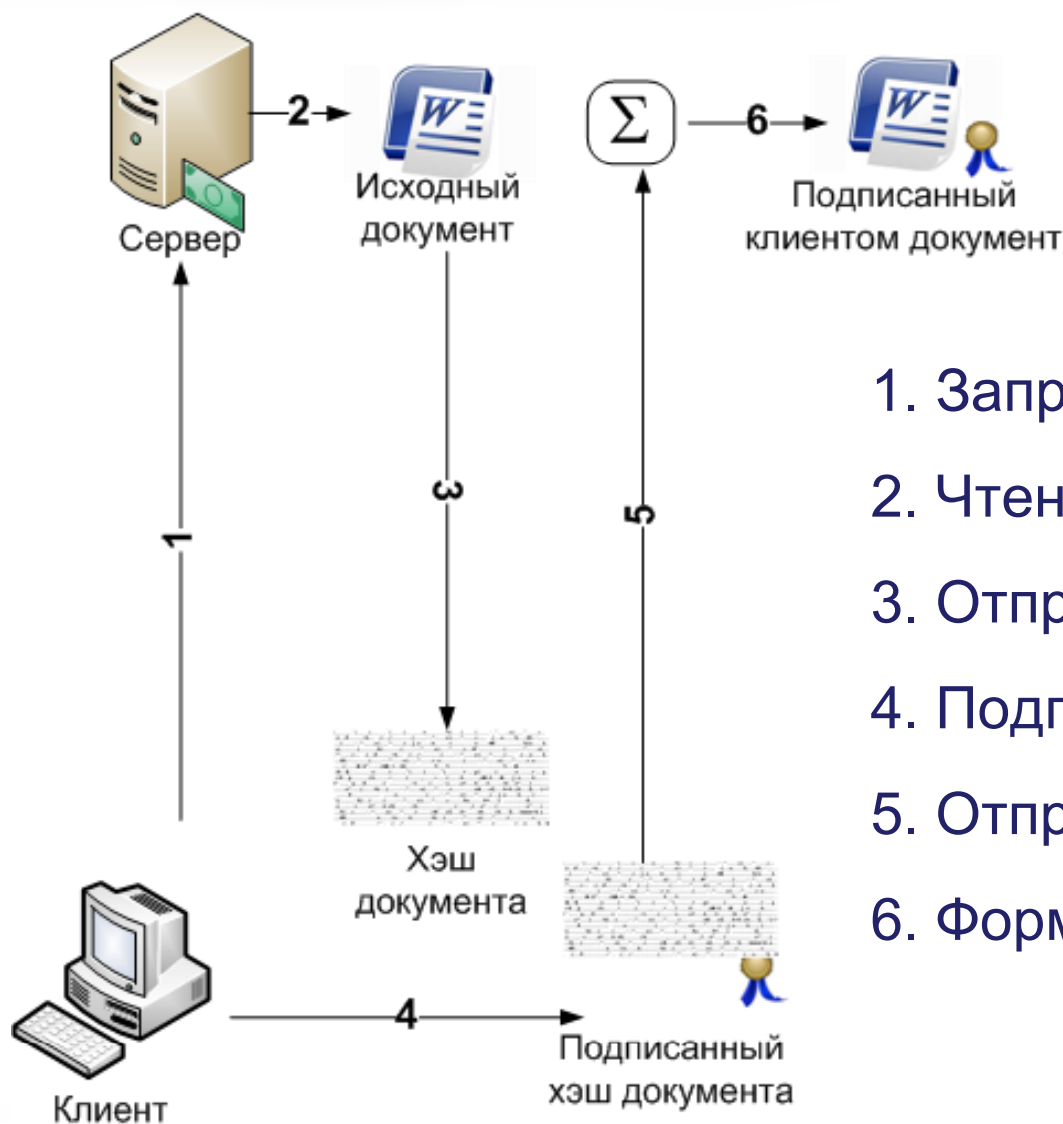
Интеграция с Citrix

Функциональная схема

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



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 «ВНCryptography»

Встраивание на Web-сервер IIS, ASP.Net

Сервер DVCS.GAZ-IS.RU

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

Библиотека «ВНСryptography»

DVC-квитанция - результат проверки множественной подписи ГОСТ, RSA, РБ



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, Т=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, Т=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""

Библиотека «ВНСryptography»

Пример встраивания: портал ООО «ТрансТелеком - Бизнес»

Портал Межкорпоративного Электронного Документооборота

Пользователь: Емельянов Егор Валерьевич

ТрансТелеКом-Бизнес

Этот список

Действия узла

Портал Межкорпоративного Электронного Документооборота > Е-документ > Компания ТТК > ТрансТелеКом-Бизнес > Архив > Входящая корреспонденция 2011

Архив

Создать Действия Параметры Представление: Все документы

Тип	Имя	Кому направлено	Комментарии	Статус документа	Кем создано	Автор изменений	Ответственный исполнитель
	Письмо о логге на ЭЦП Кунину.doc	Дрылёв Александр Львович		Подписано (1 ЭЦП)	Кхан Екатерина Алексеевна	Дзителива Надежда Евгеньевна	Дзителива Надежда Евгеньевна
	Письмо В ТТК-Б по поводу системы.doc	Емельянов Егор Валерьевич		Подписано (1 ЭЦП)	Абрамов Вячеслав Михайлович	Захарова Юлия Владимировна	Дубровин Игорь Анатольевич
	ис Работа с документом	Коростелёв Игорь Алексеевич		Подписано (1 ЭЦП)	Бака Александр Иванович	Крыгина Мария Михайловна	Дубровин Игорь Анатольевич
	ри Карточка документа			Подписано (1 ЭЦП)	Михайлова Светлана Яковлевна	Крыгина Мария Михайловна	Крыгина Мария Михайловна
	11 Пересылка контрагенту			Подписано (2 ЭЦП)	Системная учётная запись	Системная учётная запись	

Корзина

- Оформление документов
- Архив

Действия:

- Работа с документом
- Карточка документа
- Уведомить и согласовать
- Пересылка контрагенту
- Назначение исполнителя
- Перенести в папку
- Переименовать
- Удалить

Портал Межкорпоративного Электронного Документооборота > ТрансТелеКом-Бизнес Пользователь: Емельянов Егор Валерьевич

ТрансТелеКом-Бизнес

Е-документ | Е-перевозка | Е-страхование | Е-таможня Действия узла

Работа с документом «Письмо В ТТК-Б по поводу системы.doc.p7s»

[Закреть](#)

Подлинность ЭЦП	ФИО	Организация
ПОДТВЕРЖДЕНА	Абрамов Вячеслав Михайлович	НУЗ Центральная поликлиника ОАО "РЖД"

[Подписать](#)

Данный документ может быть подписан

Вы можете подписать документ, нажав кнопку "Подписать" выше

Доступные действия:

- [Просмотр документа](#)
- [Просмотр протокола соответствия](#)
- [Загрузка документа](#)
- [Уведомить и согласовать](#)
- [Назначить ответственного исполнителя](#)
- [Просмотр карточки документа](#)
- [Переслать контрагенту](#)
- [Переместить в папку](#)

- Просмотр или сохранение на локальный компьютер оригинального документа
- Просмотр протокола соответствия к документу, подписанному ЭЦП
- Загрузка документа, подписанного ЭЦП, с целью дальнейшего сохранения на локальном компьютере
- Отправка уведомления пользователю кабинета с возможностью согласования
- Назначение ответственного исполнителя для документа
- Просмотр карточки документа
- Отправка документа контрагенту
- Перемещение документа в другую папку библиотеки

Портал Межкорпоративного Электронного Документоборота > ТрансТелеКом-Бизнес

ТрансТелеКом-Бизнес

Е-документ | Е-перевозка | Е-страхование | Е-таможня

Работа с документом «Письмо»

Подлинность ЭЦП
ПОДТВЕРЖДЕНА

Данный документ может быть подписан

Доступные действия:
Просмотр документа
Просмотр протокола соответствия
Загрузка документа

Уведомить и согласовать
Назначить ответственного исполнителя
Просмотр карточки документа
Переслать контрагенту
Переместить в папку

Протокол соответствия от 07.06.2011

Электронный документ «Письмо В ТТК-Б по поводу системы.doc.p7s» подписан электронно-цифровыми подписями следующих лиц:

№ п/п	Фамилия, имя, отчество	Организация	Подлинность ЭЦП
1	Абрамов Вячеслав Михайлович	НУЗ Центральная поликлиника ОАО "РЖД"	ПОДТВЕРЖДЕНА

Информация об операторе портала www.telecomtrans.com:

- телефон.: +7 (495) 500-31-58;
- факс: +7 (495) 500-31-59;
- электронная почта: info@telecomtrans.com;
- ИНН/КПП: 7709362733/771401001;
- ОГРН: 1037739163956.

Информация об Удостоверяющем центре ЗАО «Компания ТрансТелеКом»:

- телефон: +7 (495) 784-66-77, 500-31-77;
- факс: +7 (495) 784-67-29;
- электронная почта: cainfo@transtk.ru; helpdesk@transtk.ru;
- ИНН/КПП: 7709219099/997750001;
- ОГРН: 1027739598248.

Лицензии:

1. Лицензия ФСБ России № 3705П от 03 февраля 2007 года на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств

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