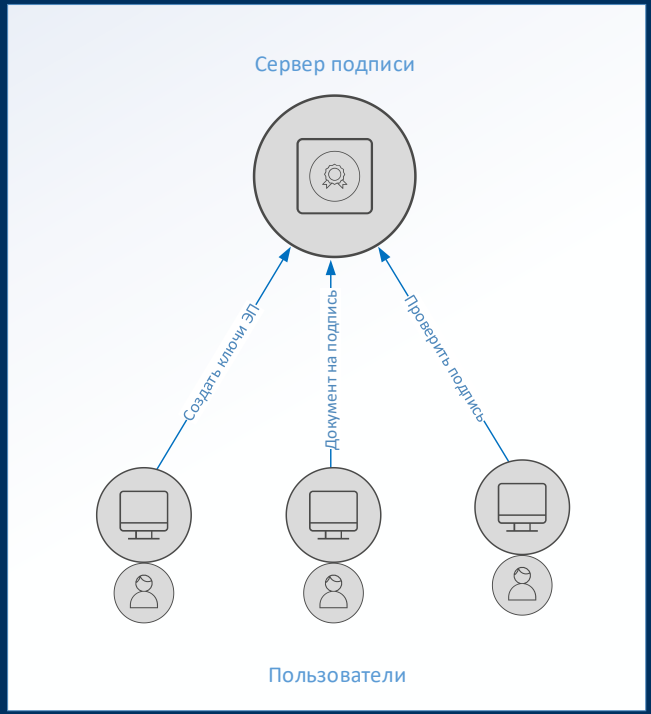
Сервер подписи ViPNet PKI Service

Что такое сервер подписи?

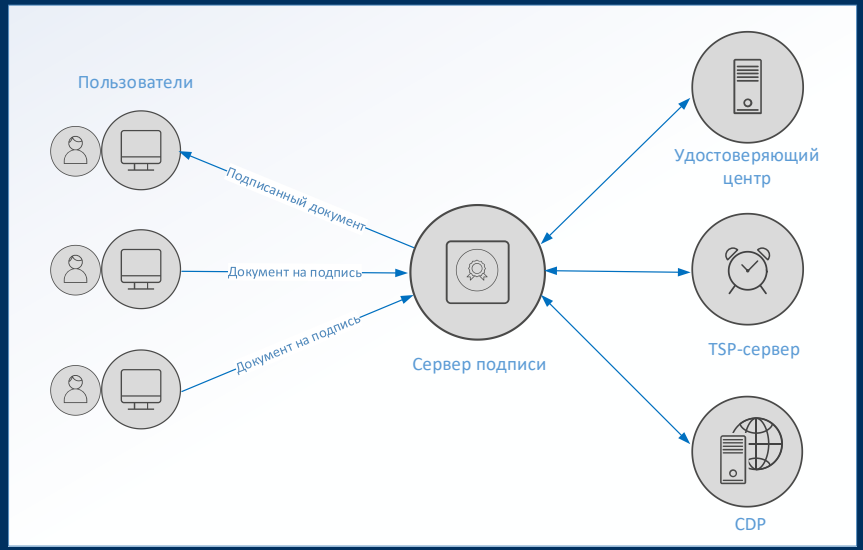
Сервер подписи обеспечивает централизованное выполнение следующих основных функций:

- ✓ генерации и хранения ключей электронной подписи;
- ✓ формирования и проверки электронной подписи.



Преимущества использования серверной подписи:

- ✓ Ключи ЭП пользователей хранятся централизованно – нельзя потерять, как токены.
- ✓ Взаимодействие с другими компонентами PKI: доступ к УЦ, серверу меток времени, к актуальным CRL.
- ✓ Аудит действий пользователей и т.п.



Доверие?

Возникают риски, связанные с доверием стороне, которой делегируются функции ИБ – оператору данных услуг.

Какие технические средства должен использовать оператор, чтобы исключить возможность компрометации и НСД к ключевой информации пользователей?

HSM - доверенные криптографические модули

ТЕХНО infotecs 2019 ФЕСТ

- ✓ Криптографическая стойкость реализуемых алгоритмов и протоколов
- ✓ Подтверждение корректности и полноты реализации мер защиты со стороны аккредитованной испытательной лаборатории, сертификация
- ✓ Гарантии сопровождения, устранения неисправностей и уязвимостей со стороны производителя на всем протяжении жизненного цикла изделия

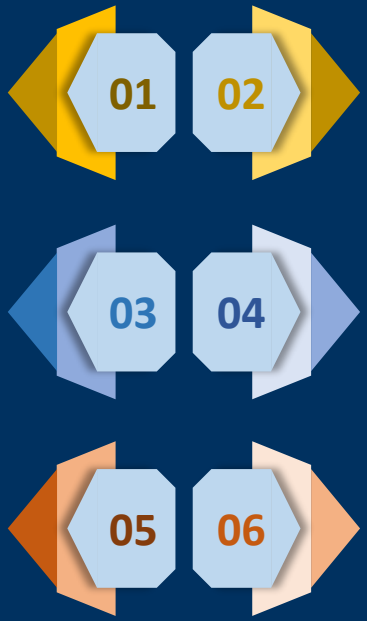
Платформа безопасности ViPNet HSM

ViPNet HSM

Программно-аппаратный модуль (HSM – Hardware Secure Module)

Повышенные меры безопасности

СКЗИ класса КВ



Выполняет криптографические операции по запросам различных сервисов («большой токен»)

Поддержка ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012

Средство ЭП класса КВ2

ViPNet HSM: повышенные меры безопастности

Встроенный аппаратный модуль:

- ✓ обнаруживает вскрытие корпуса;
- ✓ хранит и гарантированно уничтожает ключи.

Ролевая модель, обеспечивающая защиту от злонамеренных действий одного администратора:

- ✓ разделение «секрета» по схеме Шамира («2 из 3», «3 из 5»);
- ✓ сбор кворума для выполнения критичных операций.

ViPNet HSM: сертификация

ТЕХНО infotecs 2019 ФЕСТ

ViPNet HSM сертифицирован по требованиям ФСБ России:

- ✓ к СКЗИ по классу КВ;
- ✓ к средствам ЭП по классу КВ2 (приказ ФСБ России от 27.12.2011 №796).

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3746 от "04" сентября 2019 г.

Действителен до "31" октября 2021 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).
Обществу с ограниченной ответственностью «Линия защиты» (ООО «Линза»).

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс ViPNet HSM (вариант исполнения 2) в комплектации согласно формуляру ФРКЕ.00127-01 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КВ, Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КВ2, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС» сертификационных испытаний образца продукции № 818Б-001001.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00127-01 97 01 ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00127-01 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М. Ивашко

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 4 сентября 2019 г.

Первый заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России В.Н. Мартынов

ViPNet HSM: подключение прикладных сервисов

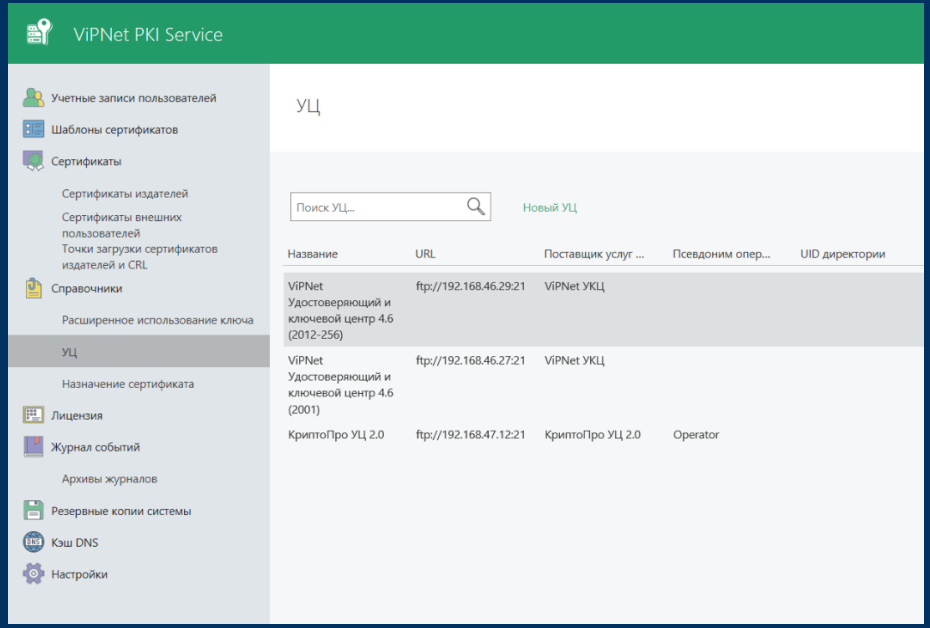
Сервер подписи ViPNet PKI Service

ViPNet PKI Service: функциональные возможности

- ✓ Генерация ключей ЭП в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012
- ✓ Формирование и проверка ЭП в соответствии с ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012.
- ✓ Поддержка форматов подписи CMS, CAdES-BES, CAdES-T, XMLDSig.
- ✓ Шифрование в соответствии с ГОСТ 28147-89.

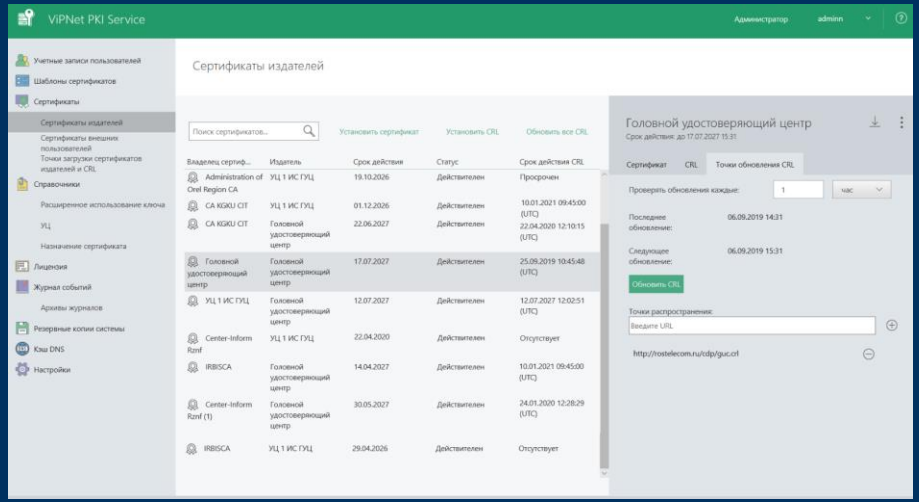
ViPNet PKI Service: взаимодействие с другими компонентами PKI

- ✓ Поддержка работы с УЦ: ViPNet Удостоверяющий центр 4 (версия 4.6), КриптоПРО УЦ 2.0.
- ✓ Формирование запросов на сертификат в формате pkcs#10.



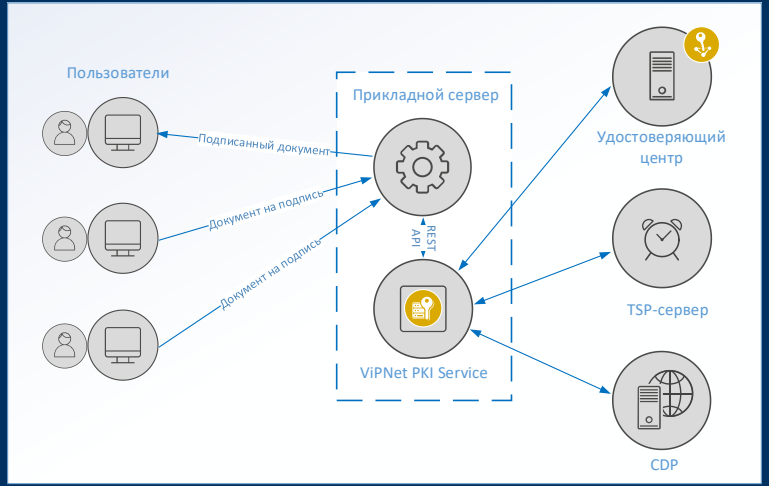
ViPNet PKI Service:
взаимодействие с другими компонентами PKI

- ✓ Поддержка меток времени в соответствии с RFC 3161.
- ✓ Возможность проверки статусов сертификатов по протоколу OCSP (RFC 2560).
- ✓ Поддержание CRL в актуальном состоянии в автоматическом режиме.



ViPNet PKI Service: дополнительные возможности

- ✓ Возможность удаленного администрирования через Web-интерфейс по защищенному каналу по протоколу TLS с использованием российских алгоритмов ГОСТ.
- ✓ Возможность встраивания в информационные системы (REST API). Потребуется оценка влияния.
- ✓ Предоставляется эмулятор в виде VA для тестирования.

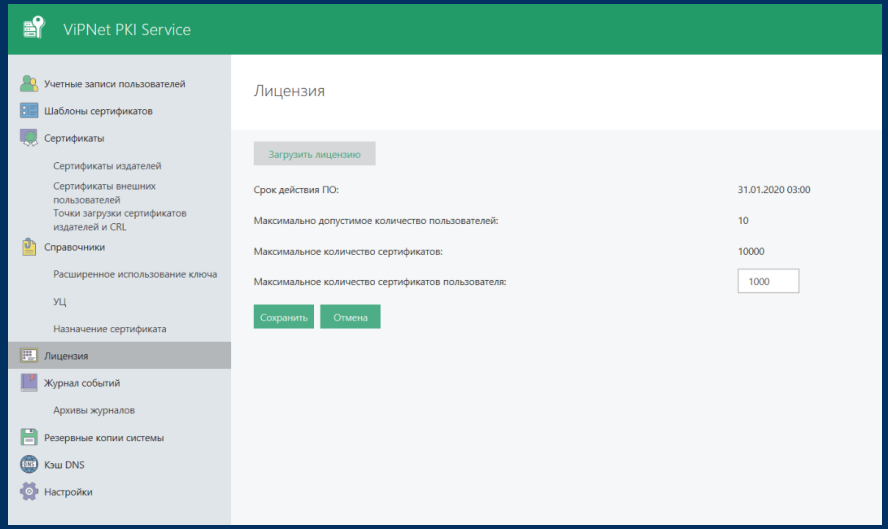


ViPNet PKI Service: лицензирование

Лицензирование:

- ✓ По количеству пользователей.
- ✓ По количеству сертификатов.

При покупке ViPNet PKI Service («Базовый продукт») в лицензию включается поддержка 10 пользователей и 100 сертификатов.



ViPNet PKI Service: сертификация

- ✓ СКЗИ КВ и средство ЭП КВ2
- ✓ Может использоваться для реализации функций ЭП в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи»

Зарегистрирован в Реестре российского ПО

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3743 от "04" сентября 2019 г.

Действителен до "04" сентября 2022 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»),
Обществу с ограниченной ответственностью «Линия защиты» (ООО «Линза»)

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс ViPNet PKI Service (на аппаратной платформе HSM 2000(2)) в комплектации согласно формуляру ФРКЕ.00184-01 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КВ, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КВ2, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС» сертификационных испытаний образца продукции № 905S-000502

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00184-01 97 01 ТУ и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00184-01 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М. Иванцов

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 4 сентября 2019 г.

Первый заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России В.Н. Мартынов

ViPNet PKI Service: пример использования

ТЕХНО 2019 infotecs ФЕСТ

ПАК ViPNet PKI Service совместно со специальным программным обеспечением (СПО) TrustGate компании «Инфотекс Интернет Траст» входят в состав Типового технического решения по обеспечению информационной безопасности при взаимодействии с Единой биометрической системой, согласованного с ФСБ России.

Банки, в соответствии с Методическими рекомендациями Банка России от 14 февраля 2019 г. № 4-МР, могут разработать собственное решение или внедрить Типовое решение на базе СПО TrustGate и ПАК ViPNet PKI Service.

ИНФОТЕКС ТРАСТ

Секция аналитических докладов:

«Решение по защите биометрических данных для ЕБС на примере сервисов Инфотекс Интернет Траст».

ТЕХНО 2019 infotecs Фест

Спасибо
за внимание!