Криптосистема ViPNet

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru

Назначение криптографических функций

Криптографические функции обеспечивают:

- конфиденциальность информации;
- идентификацию и подтверждение авторства;
- целостность передаваемой информации;
- неотказуемость от передачи электронного документа;
- неотказуемость от приема электронного документа.

Шифрование в технологии ViPNet

Особенности криптосистемы ViPNet

В ViPNet используется комбинация криптоалгоритмов:

- симметричные алгоритмы
  (алгоритмы с общим ключом);
- асимметричные алгоритмы
  (алгоритмы с открытым ключом).

Симметричные алгоритмы шифрования

Симметричный ключ – это секретная комбинация, используемая для шифрования или расшифрования.

Симметричные ключи формируются в ViPNet УКЦ.

Шифрование в технологии ViPNet

Симметричные алгоритмы шифрования

- В симметричных алгоритмах для зашифрования и расшифрования применяется один и тот же криптографический ключ.
- В ViPNet симметричные алгоритмы используются для шифрования и контроля целостности информации (шифрования IP-трафика, почтовых сообщений, прикладных и транспортных конвертов).
- Для того чтобы обмен состоялся отправитель и получатель должны знать один и тот же секретный ключ.

Шифрование в технологии ViPNet

Асимметричные алгоритмы шифрования

- В асимметричных алгоритмах шифрования используют два связанных ключа: открытый ключ и закрытый ключ.
- Закрытым ключом владеет только пользователь, который создает пару асимметричных ключей. Закрытый ключ хранится в секрете. Открытый ключ распространяется свободно.

Шифрование в технологии ViPNet

Варианты применения асимметричных ключей

Асимметричные ключи шифрования

- открытый асимметричный ключ используется для шифрования в сторонних приложениях с помощью криптопровайдера ViPNet CSP;
- секретный асимметричный ключ используется для расшифрования.

Асимметричные ключи подписи

- секретный асимметричный ключ используется для создания электронной подписи;
- открытый асимметричный ключ используется для проверки электронной подписи.

Шифрование в технологии ViPNet

Поддерживаемые криптографические стандарты

Симметричные алгоритмы	Асимметричные алгоритмы	Алгоритмы хэширования
ГОСТ 28147-89 закрытый ключ – 256 бит	**ГОСТ Р 34.10-2001** открытый ключ – 512 бит закрытый ключ – 256 бит	**ГОСТ Р 34.11-94** длина хэша – 256 бит
AES закрытый ключ – до 256 бит	**ГОСТ Р 34.10-2012** открытый ключ – 512 бит закрытый ключ – 256 бит	**ГОСТ Р 34.11-2012** длина хэша – 256 бит длина хэша – 512 бит

Шифрование в технологии ViPNet

Порядок перехода к использованию национального стандарта ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94 в средствах электронной подписи для информации, не содержащей сведений, составляющих государственную тайну, в случаях, подлежащих регулированию со стороны ФСБ России в соответствии с действующей нормативной правовой базой

(выписка из документа ФСБ России № 149/7/1/3-58 от 31.01.2014 "О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования")

Для средств ЭП, техническое задание на разработку которых утверждено после 31 декабря 2012 года, **должна быть предусмотрена реализация функций средства в соответствии с ГОСТ Р 34.10-2012** хотя бы по одному из определяемых стандартом вариантов требований к параметрам (использование варианта, соответствующего длине секретного ключа порядка 256 бит, является предпочтительным, поскольку обеспечивает достаточный уровень криптографической стойкости и лучшие эксплуатационные характеристики, в том числе при совместной реализации со схемой ГОСТ Р 34.10-2001).

Шифрование в технологии ViPNet

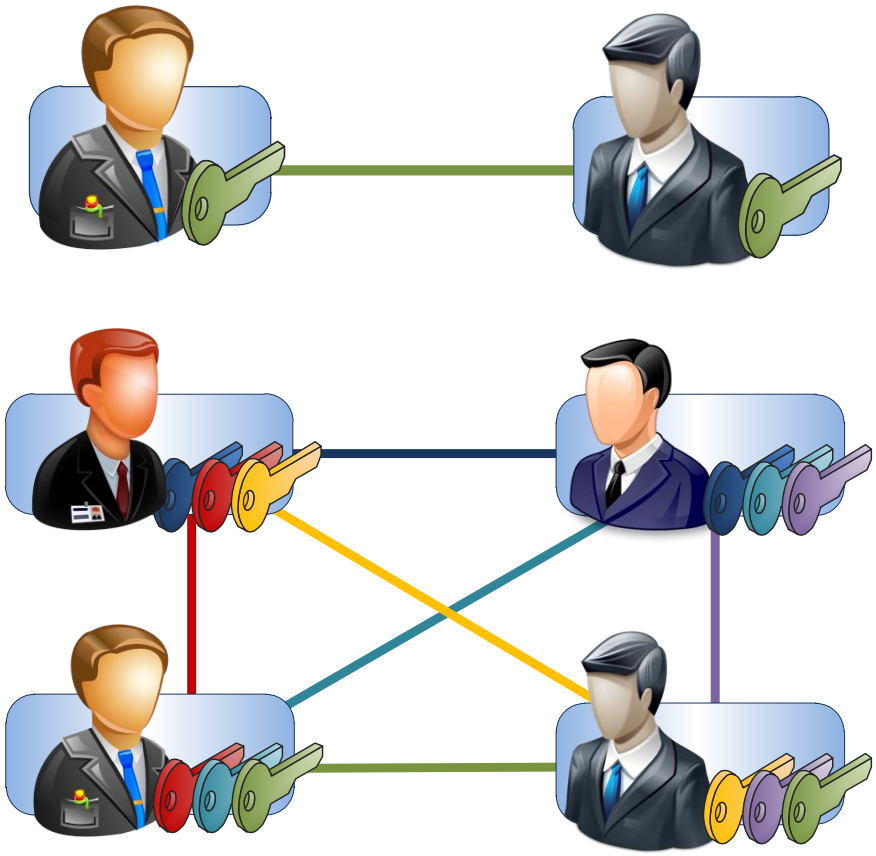
После 31 декабря 2013 года не осуществлять подтверждение соответствия средств ЭП Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27.12.2011 г. № 796, если в этих средствах не предусмотрена реализация функций средства в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94 хотя бы по одному из определяемых стандартом вариантов требований к параметрам. Исключение может быть сделано для средств ЭП, удовлетворяющих одновременно следующим условиям:

- техническое задание на разработку средства утверждено до 31 декабря 2012 года;
- в соответствии с техническим заданием разработка средства завершена после 31 декабря 2011 года;
- подтверждение соответствия средства указанным Требованиям ранее не осуществлялось.

Использование ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94 после 31 декабря 2018 года не допускается.

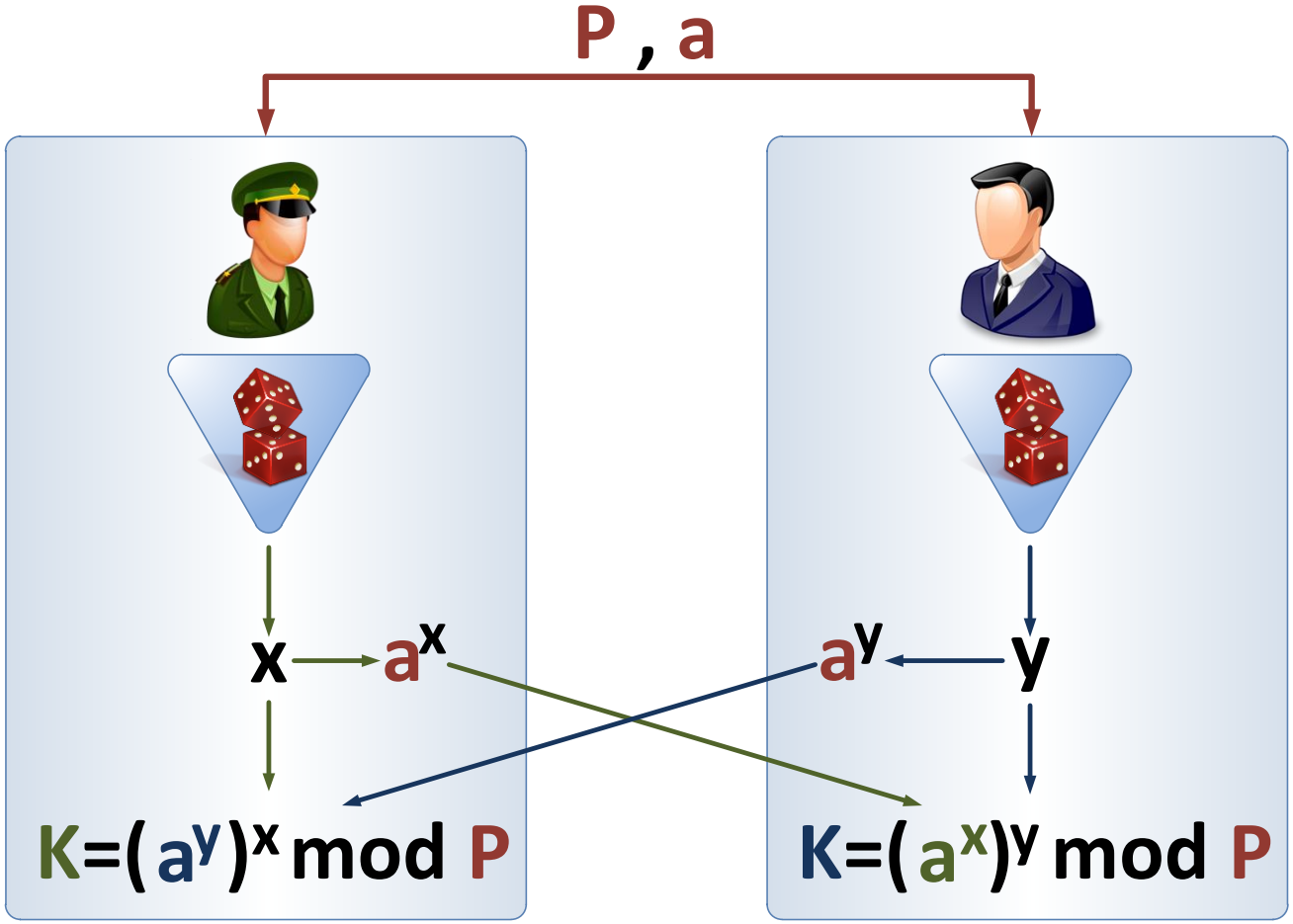
Шифрование в технологии ViPNet

Проблема распределения симметричных ключей



Шифрование в технологии ViPNet

Протокол ключевого обмена Диффи-Хеллмана



Ключевая система ViPNet

Ключевая система ViPNet

Виды шифрования в ViPNet

- **Шифрование на сетевом уровне:**
  - шифрование IP-трафика;
  - шифрование сообщений программы ViPNet Деловая почта;
  - шифрование прикладных и служебных конвертов;
- **Шифрование на прикладном уровне:**
  - создание и проверка электронной подписи;
  - шифрование в прикладных программах с помощью криптопровайдера ViPNet CSP.

Ключевая система ViPNet

Типы ключей в ViPNet

Мастер-ключи

Симметричные ключи шифрования

Асимметричные ключи шифрования

Асимметричные ключи ЭП

Ключевая система ViPNet

Мастер-ключи

Мастер-ключи своей сети ViPNet

- мастер-ключ ключей обмена
- мастер-ключ ключей защиты
- мастер-ключ персональных ключей

- формируются с помощью датчика случайных чисел;
- хранятся в программе ViPNet Удостоверяющий и ключевой центр;
- используются для формирования симметричных ключей.

Ключевая система ViPNet

Виды симметричных ключей

Ключи обмена

- формируются на основе мастер-ключа ключей обмена;
- используются для шифрования трафика между узлами ViPNet;
- шифрование выполняется на случайных ключах, сделанных на основе ключей обмена, уникальных для каждого IP-пакета;
- при хранении на сетевых узлах шифруются на специальных ключах защиты.

Ключевая система ViPNet

Применение ключей обмена

Ключевая система ViPNet

Виды симметричных ключей

Ключи защиты ключей обмена

- формируются на основе мастер-ключа ключей защиты;
- на этих ключах зашифрованы ключи обмена;
- при хранении на сетевых узлах шифруются на персональных ключах.

Виды симметричных ключей

Персональные ключи

- формируются на основе мастер-ключа персональных ключей;
- используются для разграничения доступа нескольких пользователей сетевого узла к разной ключевой информации;
- на этих ключах зашифрованы ключи защиты и другая ключевая информация, принадлежащая отдельному пользователю;
- могут храниться как на внешнем устройстве, так и на сетевом узле;
- при хранении шифруются на парольном ключе пользователя.

Ключевая система ViPNet

Виды симметричных ключей

Парольный ключ

- формируется путем вычисления значения хэш-функции пароля пользователя;
- на парольном ключе зашифрованы персональные ключи пользователя;
- может быть создан как централизованно в программе ViPNet УКЦ, так и пользователем на сетевом узле.

Ключевая система ViPNet

Защита ключевой информации

Для защиты ключей обмена применяется три уровня шифрования:

- ключи обмена зашифрованы на ключах защиты;
- ключи защиты зашифрованы на персональных ключах;
- персональные ключи зашифрованы на парольных ключах.

Пароль хранится у пользователя

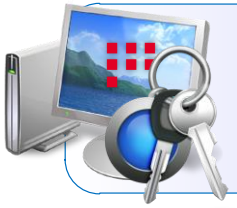
Ключи данного типа можно хранить на внешнем устройстве или сетевом узле

Ключи хранятся на сетевом узле

Ключевая система ViPNet

Ключевая информация

Дистрибутив ключей



Ключи узла

Ключи пользователя

Ключевая система ViPNet

Дистрибутив ключей

Файл с расширением **.dst**, который создается в программе ViPNet УКЦ для каждого пользователя ViPNet и содержит все необходимое для развертывания рабочего места пользователя ViPNet на сетевом узле.

Ключевая система ViPNet

Состав дистрибутива ключей

Адресные справочники

Ключи пользователя

- Хэш пароля
- Персональный ключ
- Ключ электронной подписи и сертификат ключа проверки электронной подписи
- Резервный набор персональных ключей

Ключи узла

- Ключи обмена
- Ключи защиты ключей обмена
- Справочник сертификатов ключей проверки подписи администраторов
- Списки аннулированных сертификатов своей и доверенных сетей
- Изданные кросс-сертификаты
- Служебная информация

Файл лицензии

Ключевая система ViPNet

Дистрибутив ключей

- **Необходимо создание дистрибутива ключей в случае:**
  - добавления пользователя в сеть ViPNet;
  - проблемы при функционировании узла пользователя в сети ViPNet, например, если произошла поломка компьютера и информация, хранившаяся на нем, была повреждена, и восстановить ее невозможно (в том числе справочники и ключи);
  - текущее состояние узла пользователя не позволяет выполнять отправку и прием зашифрованных писем, шифрование трафика, при этом удаленное обновление справочников и ключей по каким-либо причинам не может быть произведено.

Ключевая система ViPNet

Ключи узла ViPNet

Набор файлов, который создается в программе ViPNet УКЦ для каждого узла сети ViPNet.

Предназначены для шифрования передаваемого трафика и информации ViPNet-приложений, которой обмениваются сетевые узлы.

Ключевая система ViPNet

Состав ключей узла ViPNet

- ключи обмена
- ключи защиты ключей обмена
- справочники сертификатов администраторов своей сети
- справочники сертификатов администраторов доверенных сетей
- списки отозванных сертификатов своей сети
- списки отозванных сертификатов доверенных сетей
- изданные кросс-сертификаты
- служебная информация

Ключевая система ViPNet

Ключи узла ViPNet

- **Необходима смена ключей узла в случае:**
  - добавление или удаление связи с другим сетевым узлом вашей сети ViPNet или доверенной сети;
  - смена мастер-ключа обмена или мастер-ключа защиты;
  - смена межсетевого мастер-ключа, в случае, если текущий сетевой узел имеет связь с узлами доверенной сети;
  - компрометация текущего сетевого узла;
  - компрометация сетевого узла или пользователя, с которым установлена связь.

- **по умолчанию хранятся в каталоге ..\d_station**

Ключевая система ViPNet

Ключи пользователя ViPNet

Набор файлов, который создается в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сети ViPNet.

Содержит информацию, идентифицирующую пользователя и позволяющую ему работать с программным обеспечением ViPNet

Ключевая система ViPNet

Состав ключей пользователя ViPNet

- хэш пароля
- персональный ключ
- закрытый ключ подписи пользователя
- сертификат ключа проверки электронной подписи
- резервный набор персональных ключей

Ключевая система ViPNet

Ключи пользователя ViPNet

- **Необходима смена ключей пользователя в случае:**
  - компрометация ключей пользователя;
  - смена мастера персональных ключей;
  - выдача ключей подписи пользователю;
  - издание нового сертификата пользователя при истечении срока действия имеющегося у него закрытого ключа и соответствующего сертификата открытого ключа подписи.
- **По умолчанию хранятся в каталоге ..\key_disk**

Резервный набор персональных ключей

Резервный набор персональных ключей:

- это набор из нескольких персональных ключей, который создается в программе ViPNet УКЦ для каждого пользователя сети ViPNet;
- входит в состав первого дистрибутива ключей пользователя (dst-файла);
- файл с резервным набором ключей имеет вид **AAAA.pk** (где AAAA — идентификатор пользователя в сети ViPNet)
- по умолчанию состоит из **20** персональных ключей.

Используется при компрометации или смене мастер-ключа персональных ключей и позволяет удаленно обновить ключи пользователя и ключи узла.

Резервный набор персональных ключей

- **РНПК создается автоматически в случае:**
  - формирования самого первого дистрибутива ключей пользователя;
  - формирования ключей пользователя при добавлении пользователя на узел, на котором уже имеются другие пользователи;
  - смене мастер-ключа персональных ключей;
  - формировании ключей после компрометации пользователя, если в текущем резервном наборе пользователя были скомпрометированы все ключи.
- ***РНПК создается вручную в случае:***
  - повторного создания дистрибутива ключей для пользователя, при этом его содержание не изменяется, остается таким же, как и в предыдущих наборах, созданных автоматически.

Резервный набор персональных ключей

При передаче РНПК пользователю рекомендуется:

- сохранять резервный набор на отдельном устройстве хранения данных;
- устройство с резервным набором передавать пользователю лично в руки либо по защищенному альтернативному каналу связи;
- после получения хранить резервный набор персональных ключей в безопасном месте, отдельно от других ключей (например, в сейфе).

Компрометация ключей

Компрометация ключей

Компрометация ключей

Компрометацией ключей — утрата доверия к тому, что используемые ключи не стали известны злоумышленникам и обеспечивают безопасность информации, то есть ее

- конфиденциальность,
- целостность,
- неотрекаемость (подтверждение авторства).

Компрометация ключей

Явная компрометация

Явная компрометация — события, когда факт компрометации стал доподлинно известен:

- доступ к файлу дистрибутива ключей посторонних лиц;
- утеря ключевых носителей;
- утеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытых ключей.

Компрометация ключей

Неявная компрометация

Неявная компрометация — события, когда факт компрометации не является доподлинно установленным, однако вероятность того, что злоумышленники могли получить несанкционированный доступ к ключевой информации достаточна велика:

- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение печати на сейфе с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и не опровергнута возможность того, что это произошло в результате действий злоумышленника).

Компрометация ключей

Компрометация в сетях ViPNet

Компрометация закрытого ключа

- **Выполняется при:**
  - утрате контейнера закрытого ключа;
  - утрате дистрибутива ключей;
  - увольнении сотрудника.

Компрометация администратора сети ViPNet

- **Выполняется при:**
  - утрате пароля или любой ключевой информации администратора сети ViPNet;
  - возможности того, что посторонние лица могли получить доступ к компьютеру с установленным ViPNet УКЦ;
  - увольнении администратора УКЦ.

Компрометация ключей

Компрометация в сетях ViPNet

Компрометация пользователя

- **Выполняется при:**
  - утрате дистрибутива ключей, если дистрибутив не содержал резервного набора персональных ключей;
  - увольнении сотрудника.

Компрометация сетевого узла

- **Выполняется при:**
  - компрометации всех пользователей сетевого узла.

Компрометация пользователя при утрате доверия к РНПК

- **Выполняется при:**
  - утрате носителя с РНПК;
  - утрате дистрибутива, содержащего РНПК.

Компрометация ключей

Компрометация в сетях ViPNet

- **При компрометации ключей пользователю следует:**
  - уведомить администратора сети ViPNet о факте и обстоятельствах компрометации;
  - приостановить работу скомпрометированного узла до получения обновления при компрометации.

- **При компрометации ключей администратору сети ViPNet следует:**
  - провести процедуру компрометации ключей;
  - высылать пользователю новые ключи, защищенные с помощью очередного варианта персонального ключа;
  - провести служебное расследование.

Электронная подпись в технологии ViPNet

Электронная подпись

Электронная подпись:

- реквизит электронного документа, предназначенный для защиты данного документа от подделки;
- формируется в результате криптографического преобразования документа при помощи закрытого ключа электронной подписи;
- позволяет идентифицировать владельца сертификата открытого ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронная подпись

Электронная подпись:

- информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

(ФЗ № 63-ФЗ «Об электронной подписи»)

ЭП в технологии ViPNet

Электронная подпись

- **Электронная подпись обеспечивает:**
  - подлинность (удостоверяет личность поставившего подпись);
  - целостность (подтверждает, что документ не был изменен после подписания);
  - неотрекаемость (защищает от отказа субъекта от авторства подписанного документа).

- **Электронная подпись может использоваться:**
  - физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы.

Хэш-функция в технологии ViPNet

Хэш - функции

- **Хэш-функцией называется:**
  - криптографический алгоритм, который преобразует (сжимает) произвольный набор данных в битовую комбинацию фиксированной длины, которая называется сверткой, хэшем или цифровым отпечатком.

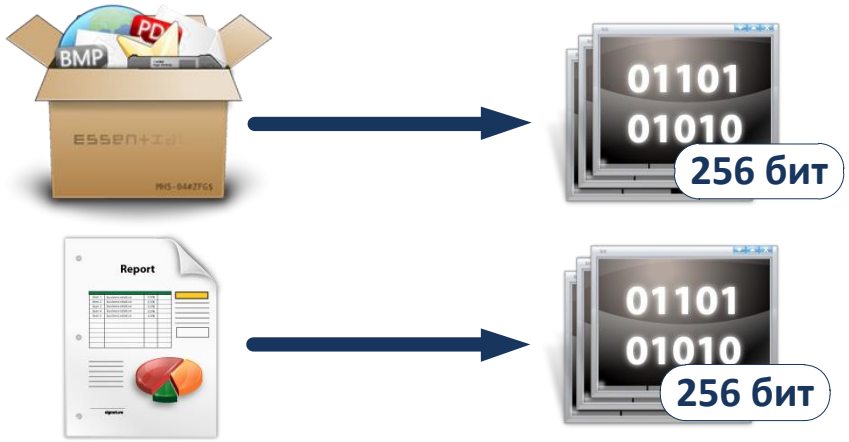
- **Хэш-функция используется:**
  - для контроля целостности сообщения;
  - для формирования контрольной суммы;
  - для формирования и проверка ЭП.

- **Алгоритмы хеширования:**
  - ГОСТ Р 34.11–94;
  - ГОСТ Р 34.11–2012 .

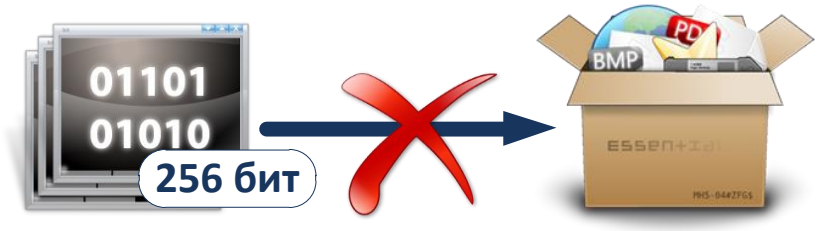
Хэш-функция в технологии ViPNet

Свойства хэш - функций

Постоянная длина значения функции:

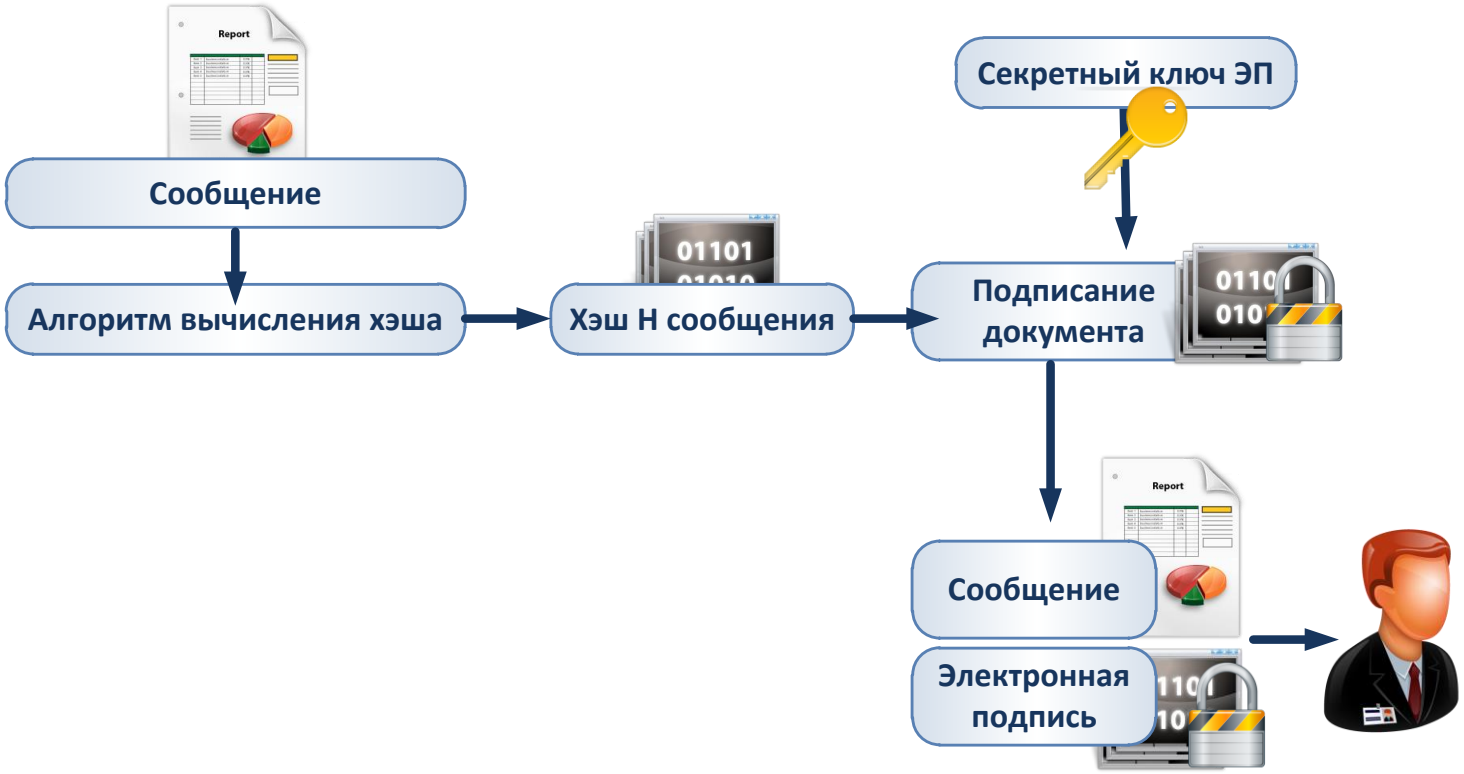


Необратимость:



ЭП в технологии ViPNet

Процедура подписания сообщения



ЭП в технологии ViPNet

Процедура проверки электронной подписи

ЭП в технологии ViPNet

Сертификат ключа проверки электронной подписи:

- электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

(ФЗ № 63-ФЗ «Об электронной подписи»)

ЭП в технологии ViPNet

Сертификат ключа проверки электронной подписи:

- это электронный документ, который связывает ключ проверки ЭП с информацией о владельце ключа (пользователе сети ViPNet).

Используется:

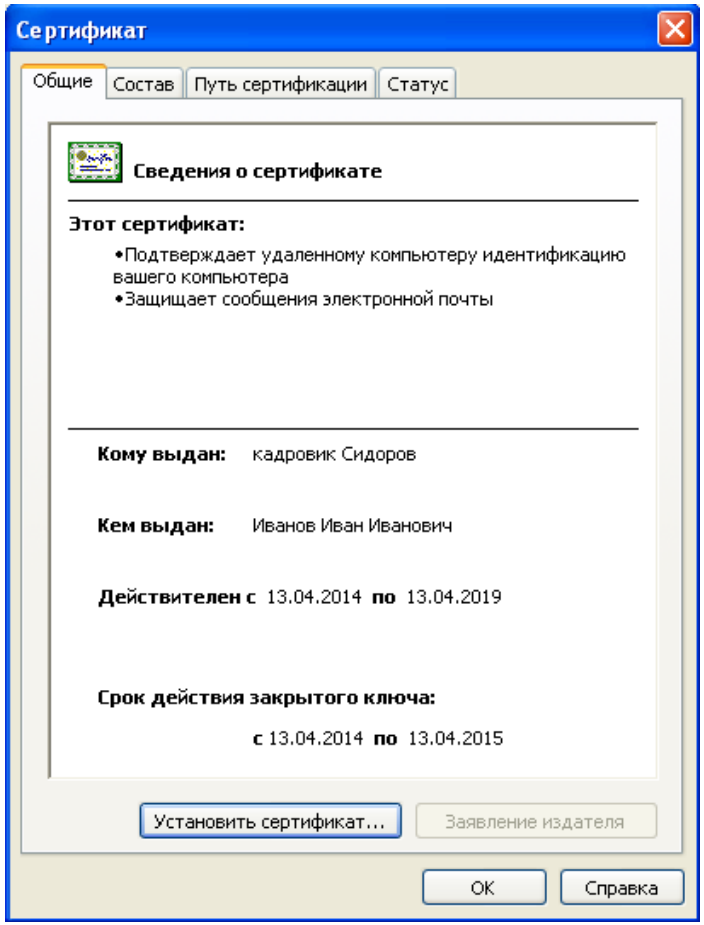
- *для проверки подписи владельца сертификата;*
- *для подтверждения того, что документ подписан именно этим пользователем.*

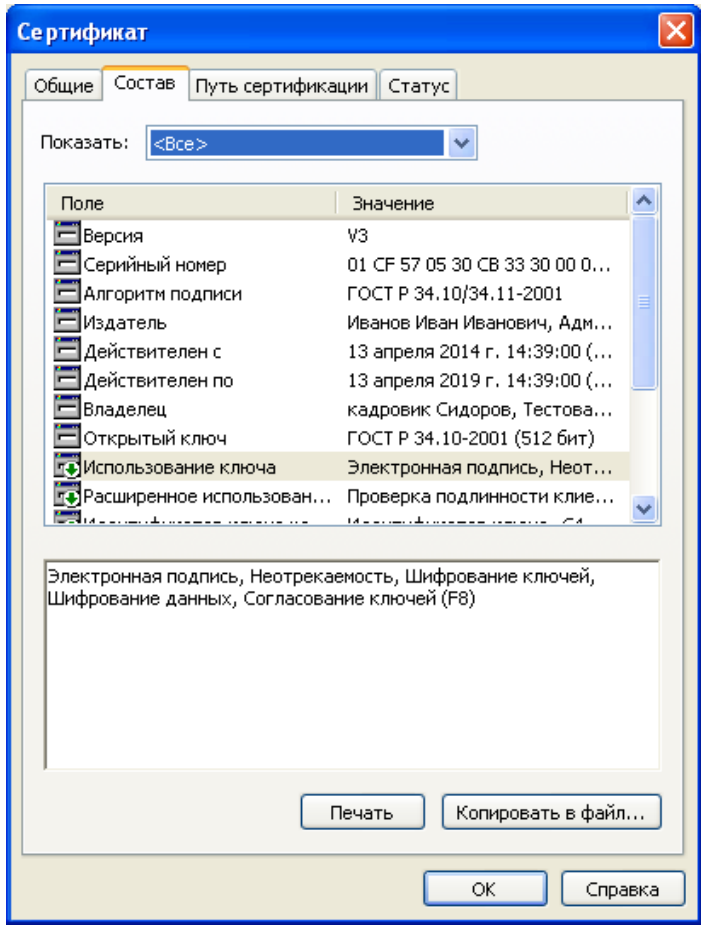
Создается в Удостоверяющем ключевом центре.

Заверяется ЭП администратора УКЦ.

ЭП в технологии ViPNet

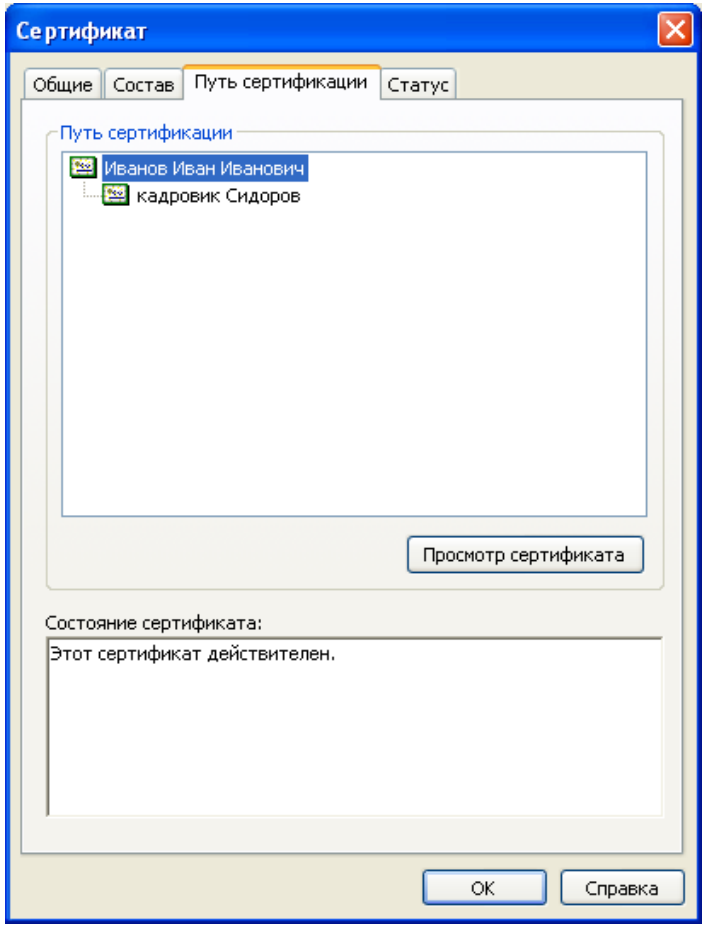
Сертификат ключа проверки ЭП

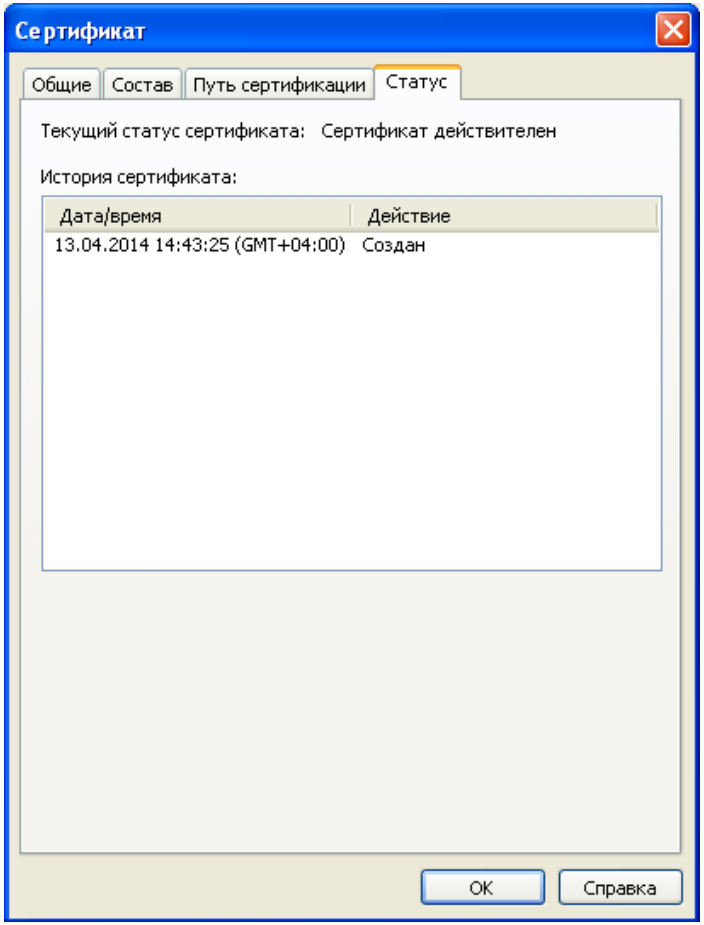




ЭП в технологии ViPNet

Сертификат ключа проверки ЭП





ЭП в технологии ViPNet

Состав полей сертификата стандарта x.509 v3

ЭП в технологии ViPNet

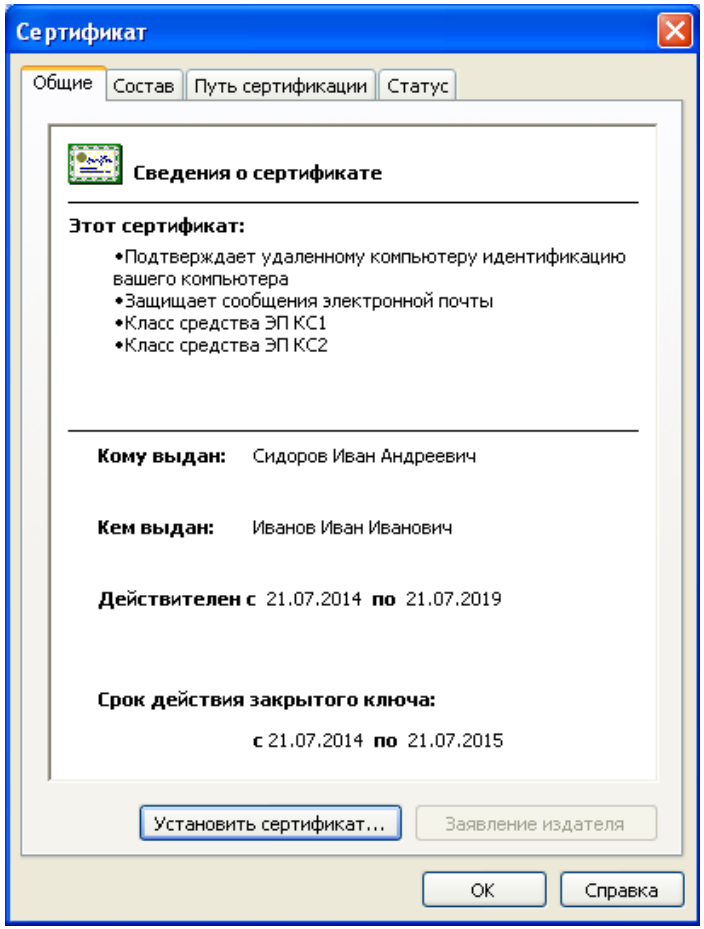
Квалифицированный сертификат ключа проверки ЭП:

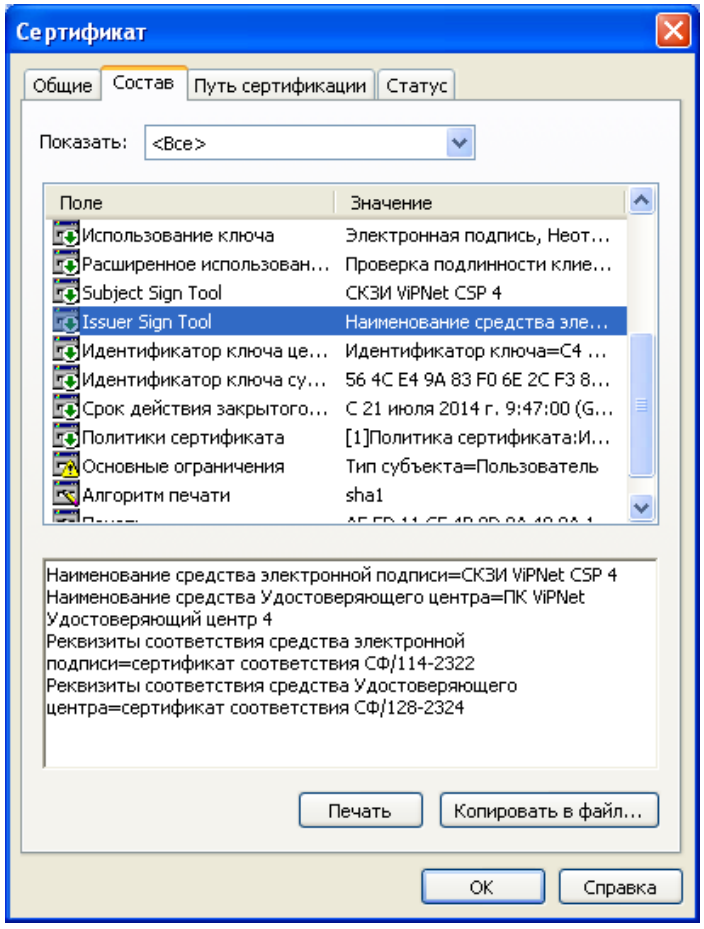
- сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган)

(ФЗ № 63-ФЗ «Об электронной подписи»)

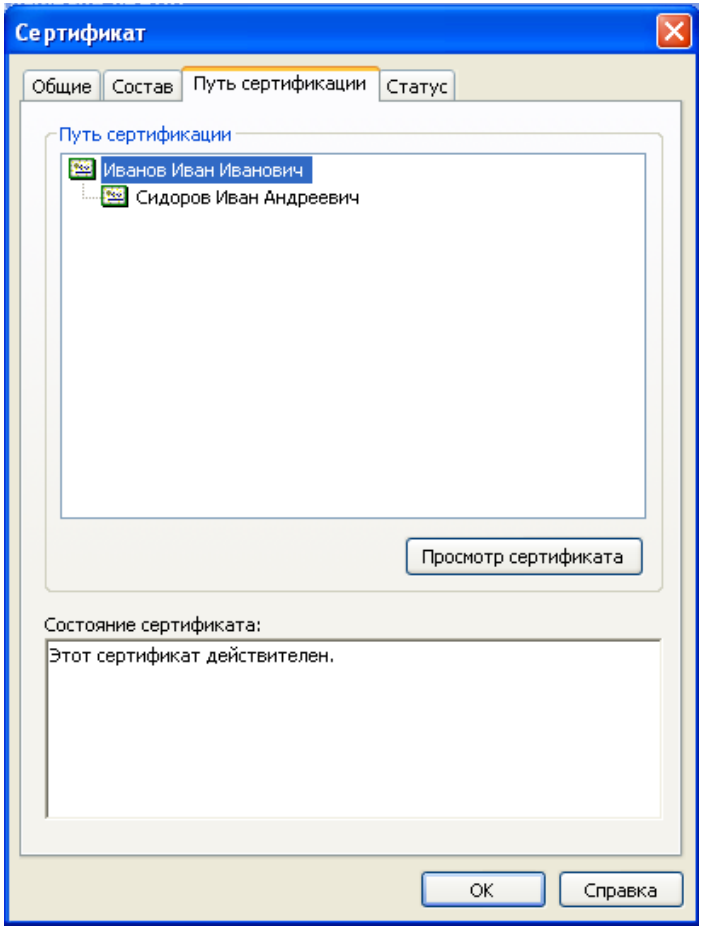
ЭП в технологии ViPNet

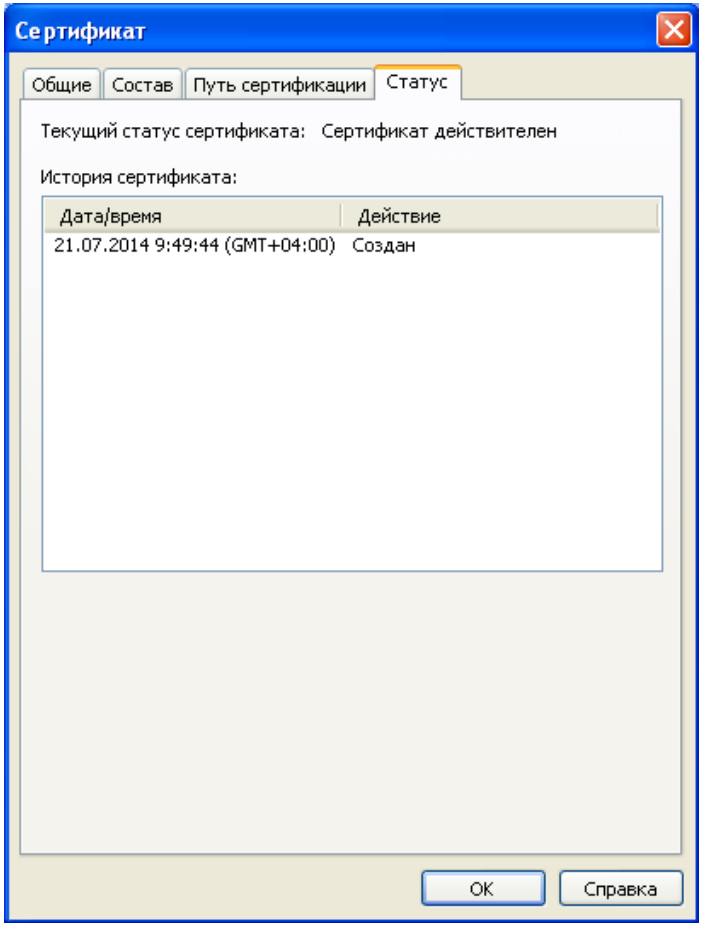
Квалифицированный сертификат ключа проверки ЭП





Квалифицированный сертификат ключа проверки ЭП





ЭП в технологии ViPNet

Список отозванных сертификатов:

- электронный документ, который содержит информацию о сертификатах, которые на определенный момент времени были отозваны, или действие которых было приостановлено.

Используется:

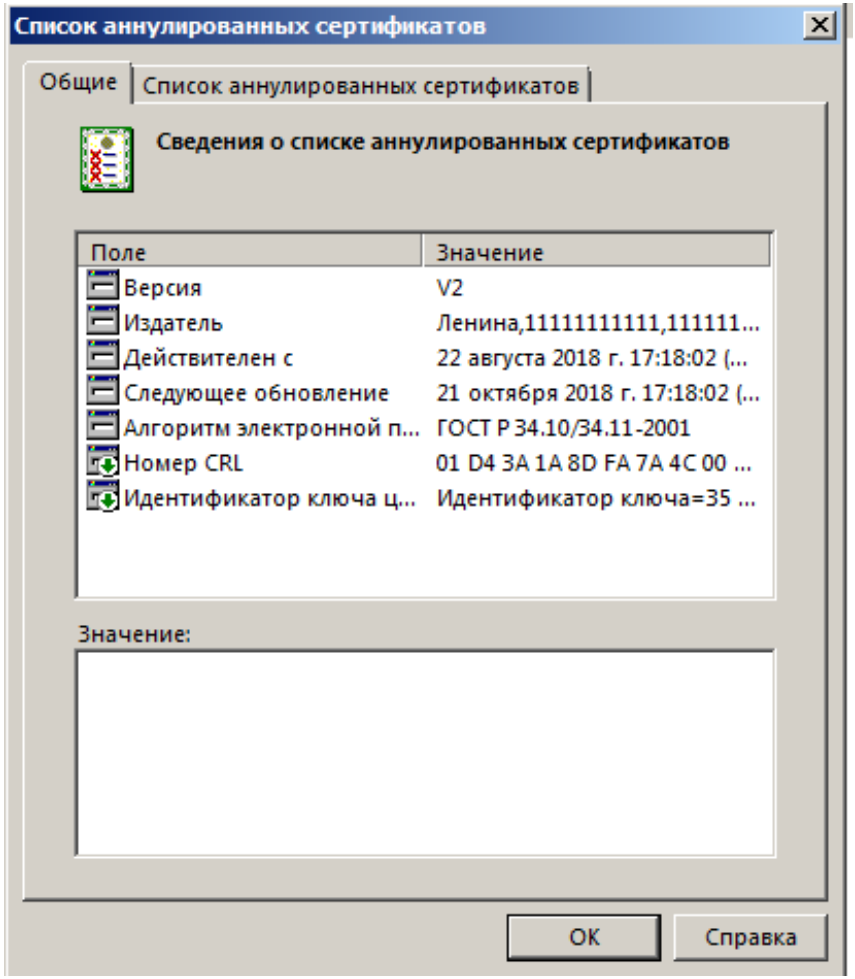
- *для определения статуса сертификата.*

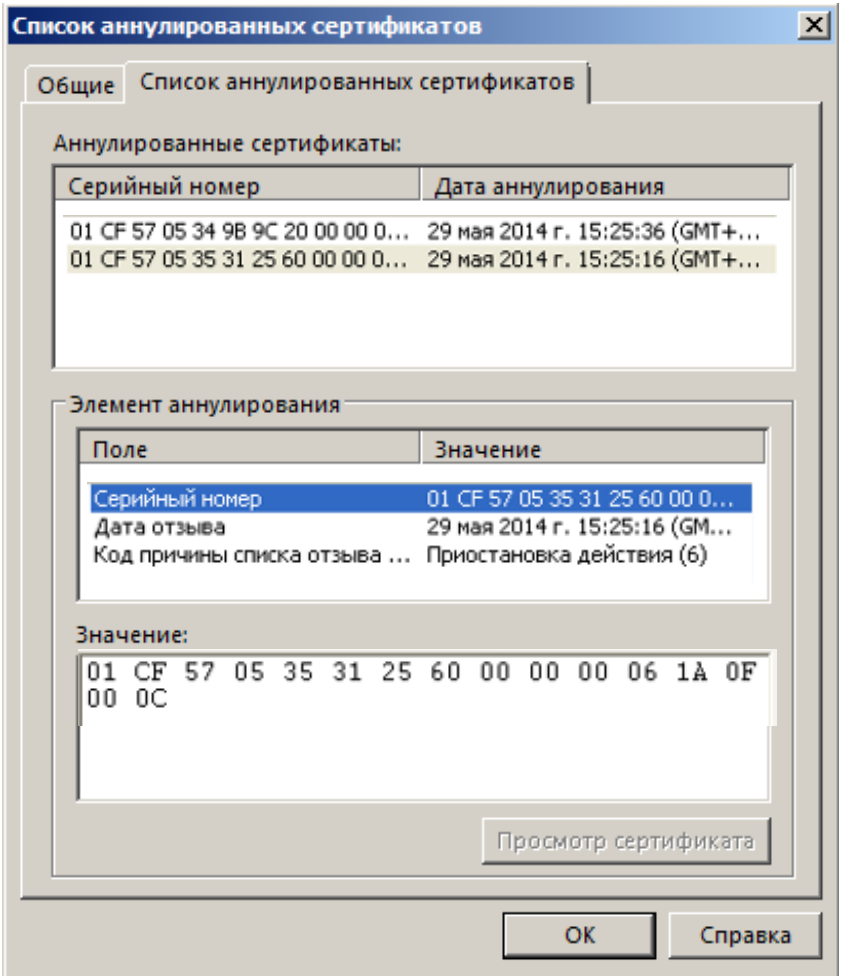
Создается в Удостоверяющем ключевом центре.

Заверяется ЭП администратора УКЦ.

ЭП в технологии ViPNet

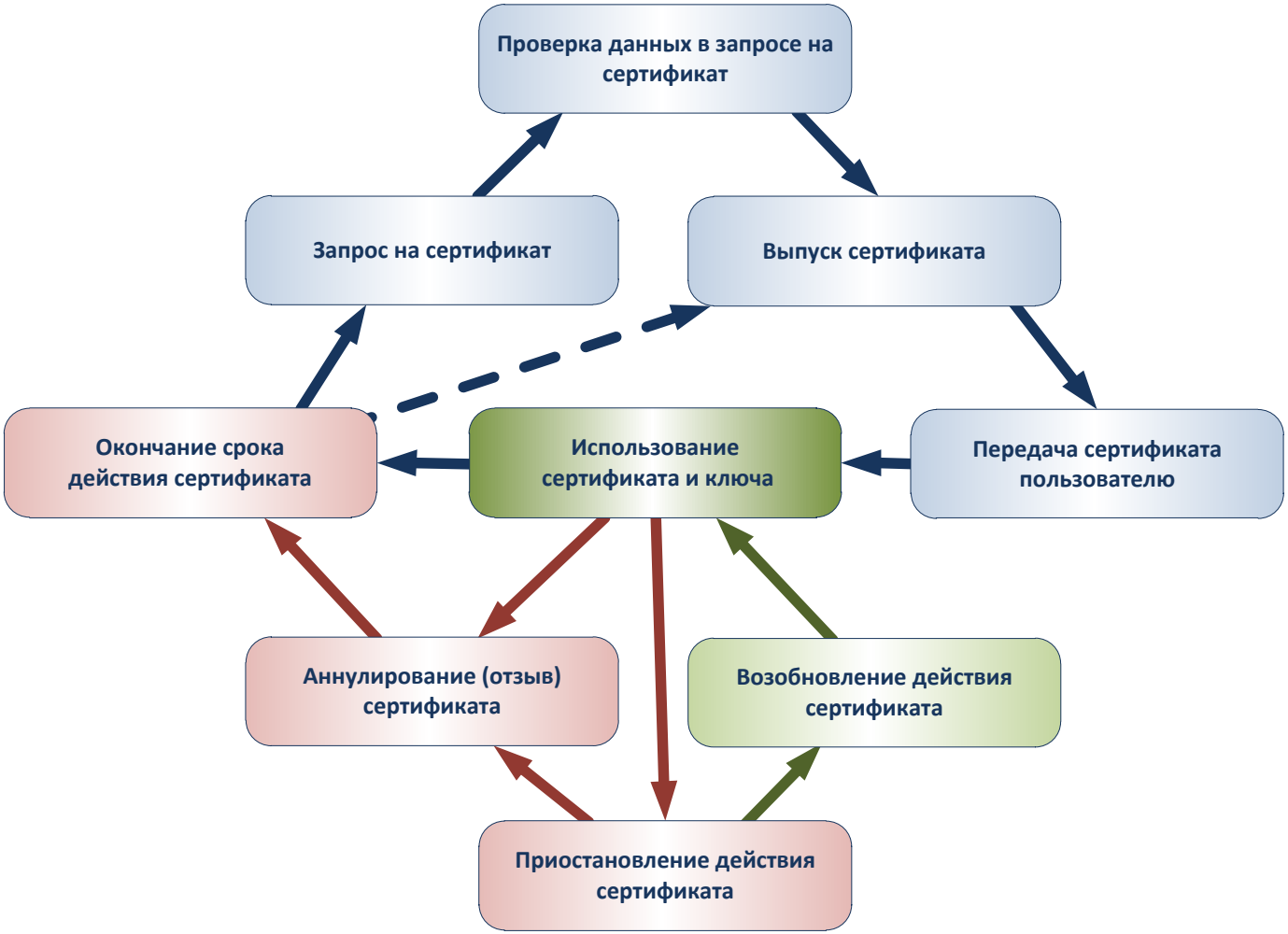
Список аннулированных сертификатов





ЭП в технологии ViPNet

Жизненный цикл сертификата



Требования регуляторов при эксплуатации СКЗИ

Основные документы, регламентирующие деятельность организации при эксплуатации СКЗИ

Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасного хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

Основные документы, регламентирующие деятельность организации при эксплуатации СКЗИ

Приказ ФСБ России от 09.02.2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005)

Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

Примерные мероприятия по организации эксплуатации СКЗИ

№ п/п	ШАГ	ОПИСАНИЕ
1	Издать Приказ об обращении с СКЗИ	1. Назначить Ответственного за организацию работ по криптографической защите информации. 2. Утвердить Инструкцию ответственного за организацию работ по криптографической защите информации. 3. Утвердить Инструкцию по обращению с СКЗИ с ознакомлением всех пользователей СКЗИ под роспись. 4. Утвердить форму Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. 5. Утвердить форму Акта об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов. 6. Утвердить форму Журнала сдачи и приема экземпляров ключей от запираемых хранилищ.
2	Организовать обучение по правилам работы с СКЗИ	Пользователям, которым необходимо получить доступ к работе с СКЗИ, организовать обучение со сдачей тестов по контролю знаний и выдачей необходимых документов
3	Издать Приказ об утверждении перечня пользователей СКЗИ	Включить в данный перечень пользователей, которые уже работают с СКЗИ, и пользователей, которые прошли обучение и получили необходимые документы.

Типовая форма журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для органа криптографической защиты)

Приложение 1
к Инструкции (пункт 26),
утвержденной приказом ФАПСИ
от 13 июня 2001 г. N 152

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении
1	2	3	4	5	6	7	8	9

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
10	11	12	13	14	15	16

Типовая форма журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)

Приложение 2
к Инструкции (пункт 26),
утвержденной приказом ФАПСИ
от 13 июня 2001 г. N 152

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Типовая форма технического (аппаратного) журнала

Приложение 3
к Инструкции (пункт 28),
утвержденной приказом ФАПСИ
от 13 июня 2001 г. N 152

N п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

Образец приказа об утверждении перечня пользователей СКЗИ

Наименование организации

ПРИКАЗ

№ _____

_____ _____ _____

дата город номер документа

Об утверждении перечня пользователей
средств криптографической защиты информации

В целях исполнения требований п.19 «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13 июня 2001г. №152 и на основании Заключений о допуске пользователя к самостоятельной работе со средствами криптографической защиты информации (далее – СКЗИ),

ПРИКАЗЫВАЮ:

1. Утвердить следующий перечень пользователей СКЗИ:

№ п/п	Фамилия Имя Отчество	Должность	Назначение СКЗИ (для работы в ГИС, бухгалтерских системах или государственных сайтах)	Наименование СКЗИ (ViPNet Client, КриптоПро, электронная подпись)

2. Контроль за исполнением настоящего приказа возложить на «Ответственное лицо».

Должность руководителя ФИО руководителя

ViPNet CSP 4.x

ViPNet CSP 4.x

ViPNet CSP

ViPNet CSP — криптопровайдер, обеспечивающий вызов криптографических функций из различных приложений, использующих интерфейс CryptoAPI 2.0

- предназначен для реализации криптографических функций;
- устанавливается как отдельная программа;
- может быть установлен как из отдельного установочного файла, так и вместе с программами ViPNet Client, ViPNet Coordinator, ViPNet CryptoService.

Назначение ViPNet CSP

- Создание ключей электронной подписи;
- Вычисление и проверка электронной подписи;
- Хэширование данных;
- Шифрование и имитозащита данных;
- Генерация случайных и псевдослучайных чисел, ключей шифрования;
- Аутентификация и выработка ключа при передаче данных по протоколам SSL/TLS;
- Хранение сертификатов открытых ключей непосредственно в контейнерах ключей;
- Поддержка различных устройств хранения электронных ключей.

Совместимость с криптопровайдерами других производителей

- Сертификаты пользователей, сформированные в УЦ КриптоПро по запросу из программы ViPNet CSP, могут использоваться для подписи с помощью криптопровайдера ViPNet CSP.
- Сертификаты, сформированные с помощью программы ViPNet УКЦ по запросу из программы КриптоПро CSP, могут использоваться в КриптоПро CSP.
- Совместимость ViPNet CSP с криптопровайдерами других производителей обеспечивается при условии реализации ими требований, содержащихся в документах RFC 4357, RFC 4490, RFC 4491.

Программный комплекс «ViPNet Удостоверяющий Центр 4.x»

Программный комплекс «ViPNet Удостоверяющий центр 4»

Программный комплекс «ViPNet Удостоверяющий центр 4.x» предназначен для реализации функций удостоверяющего центра, регистрации пользователей, создания ключей электронной подписи (ЭП), издания сертификатов ключей проверки ЭП, поддержания инфраструктуры ключей проверки ЭП.

Обязательные компоненты		
Средства удостоверяющего центра	программный комплекс **ViPNet Administrator®**	выполняет функции Центра сертификации
	программное обеспечение **ViPNet Registration Point**	выполняет функции Центра регистрации
	программное обеспечение **ViPNet CA Informing**	предоставляет функции Сервиса информирования
Вспомогательное программное обеспечение	программное обеспечение **ViPNet Publication Service**	выполняет функции Сервиса публикации
Средство криптографической защиты информации	программное обеспечение **ViPNet CSP 4.2**	используется в качестве средства ЭП

Программный комплекс «ViPNet Удостоверяющий центр 4»

Дополнительные компоненты		
	Программный комплекс **ViPNet TSP-OCSP Service**	выполняет функции службы штампов времени и сервиса проверки статуса сертификатов
	Веб-служба **ViPNet CA Web Service**	для организации взаимодействия между клиентами веб-службы и программой ViPNet УКЦ
	Программа **ViPNet CryptoFile**	для защиты файлов любых форматов с помощью шифрования

Сертификат соответствия ФСБ на программный комплекс «ViPNet Удостоверяющий центр 4»

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/118-3510 от "25" октября 2018 г.

Действителен до "05" июля 2021 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).

Настоящий сертификат удостоверяет, что изделие **«Программный комплекс «ViPNet Удостоверяющий центр 4 (версия 4.6)»** (исполнения 1, 2) в комплектации согласно формуляру ФРКЕ.00114-06 30 01 ФО

соответствует требованиям ФСБ России к информационной безопасности удостоверяющих центров класса КС2 (для исполнения 1) и класса КС3 (для исполнения 2), предназначенных для обработки информации, не содержащей сведений, составляющих государственную тайну. Требованиям к средствам удостоверяющего центра, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС2 (для исполнения 1) и класса КС3 (для исполнения 2), и Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 795, и может использоваться для реализации функций удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС»
сертификационных испытаний образца продукции № 769С-000501

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00114-06 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 25 октября 2018 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов

Удостоверяющий центр ViPNet

Удостоверяющий центр:

- юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом.

(ФЗ № 63-ФЗ «Об электронной подписи»)

Удостоверяющий центр ViPNet

Удостоверяющий центр:

- создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата (ФЗ № 63-ФЗ «Об электронной подписи»);

- является одним из главных компонентов систем юридически значимого электронного документооборота;

В сетях ViPNet сертификаты выпускаются в программе **ViPNet Удостоверяющий и ключевой центр.**

Назначение компонентов УЦ

ViPNet Administrator:

- центральный компонент программного комплекса ViPNet Удостоверяющий центр;
- предназначен для издания и обслуживания сертификатов открытого ключа;
- состоит из программ ViPNet Удостоверяющий и ключевой центр (УКЦ) и ViPNet Центр управления сетью (ЦУС).

Назначение компонентов УЦ

Состав ViPNet Administrator

Удостоверяющий и ключевой центр

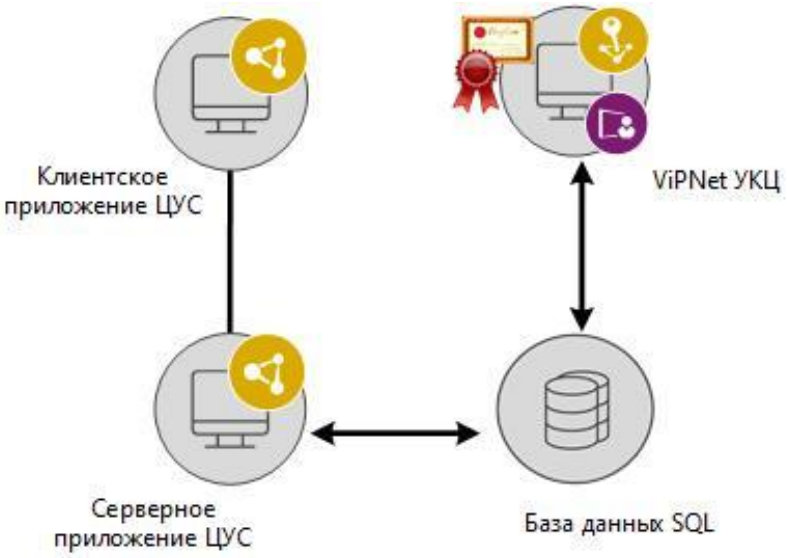
- **Отвечает за издание и управление жизненным циклом сертификатов открытого ключа:**
  - формирование сертификатов, списков отозванных сертификатов;
  - издание сертификатов пользователей;
  - отзыв, приостановление и возобновление действия выпущенных сертификатов;
- **Устанавливает доверительные отношения с другими УЦ**

Центр управления сетью

- **Предназначен для:**
  - регистрации пользователей удостоверяющего центра;
  - организации обмена служебной информацией между его различными компонентами;
- **Имеет клиент-серверную архитектуру**

Назначение компонентов УЦ

Взаимодействие компонентов ViPNet Administrator



- Управление осуществляется с помощью клиентского приложения ЦУС.
- Серверное приложение ЦУС представляет собой набор служб, которые отвечают за чтение и запись информации в базу данных SQL.
- Через базу данных происходит обмен информацией между ЦУСом и УКЦ, с программами ViPNet CA Web Service и ViPNet CA Informing.

Назначение компонентов УЦ

ViPNet Registration Point:

- предназначен для регистрации и обслуживания внешних и внутренних пользователей ViPNet и хранения их регистрационных данных.

Выполняет следующие функции:

- регистрацию пользователей;
- создание для пользователей асимметричных ключей и их сохранение в контейнерах ключей при формировании запросов на сертификаты;
- выдачу пользователям сертификатов, изданных в программе ViPNet УКЦ по запросам;
- управление жизненным циклом ранее изданных сертификатов (создание и передача в УКЦ запросов на отзыв, приостановление и возобновление действия сертификатов).

Назначение компонентов УЦ

Взаимодействие компонентов УЦ с Registration Point

ViPNet Registration Point является посредником между внешними пользователями и удостоверяющим центром и обеспечивает взаимодействие между ними.

Назначение компонентов УЦ

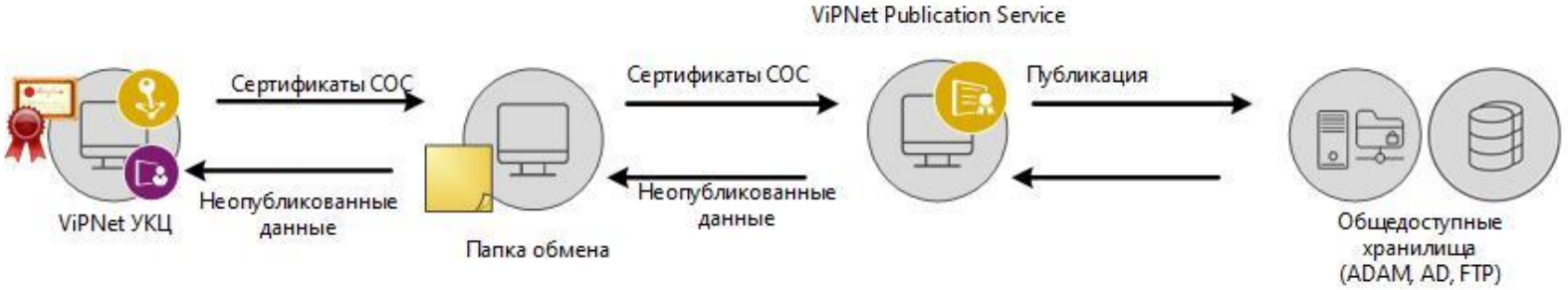
ViPNet Publication Service

Предназначен для

- публикации автоматически или вручную следующих данных:
  - сертификатов пользователей;
  - сертификатов издателей (в том числе корневых и кросс-сертификатов);
  - СОС, выпущенные своим УЦ;
  - СОС, выпущенные сторонними УЦ.
- поиска и просмотра опубликованных данных;
- экспорта опубликованных сертификатов;
- опроса точек распространения СОС сторонних удостоверяющих центров.

Назначение компонентов УЦ

Взаимодействие компонентов УЦ с Publication Service



- Взаимодействие осуществляется через специальную папку обмена.
- УКЦ формирует сертификаты и СОС и помещает их в папку обмена.
- ViPNet Publication Service следит за содержимым папки обмена и публикует сертификаты и СОС в соответствии с заданными правилами и в заданных общедоступных хранилищах (ADAM, AD LDS, Active Directory, FTP-сервер).
- Сертификаты и СОС, опубликованные в хранилищах, доступны пользовательским приложениям.

Назначение компонентов УЦ

ViPNet CA Informing

Предназначен для выполнения следующих функций:

- информирования администраторов программы ViPNet УКЦ;
- информирования пользователей УКЦ об истечении срока действия их сертификатов;
- формирования отчетов о сертификатах, изданных удостоверяющим центром, для учета всех изданных в организации сертификатов;
- экспорта сертификатов из базы данных ViPNet Administrator.

Состоит из:

- **службы уведомлений,** отвечающей за рассылку уведомлений пользователям и администраторам удостоверяющего центра;
- **клиентского компонента** — графического интерфейса, с помощью которого создаются уведомления и настройки их рассылки, а также формирования отчетов и экспорта сертификатов

Назначение компонентов УЦ

ViPNet CA Informing

Принцип работы программы ViPNet CA Informing основан на взаимодействии компонентов программы с базой данных настроек ViPNet CA Informing и с базой данных программы ViPNet Удостоверяющий и ключевой центр.

Назначение компонентов УЦ

ViPNet CA Web Service:

Веб-служба, предназначенная для передачи в программу ViPNet УКЦ запросов от пользователей стороннего программного обеспечения или от сторонних центров регистрации, а также для передачи ответов на запросы пользователям и в центры регистрации;

Получает от пользователей и передает в УКЦ:

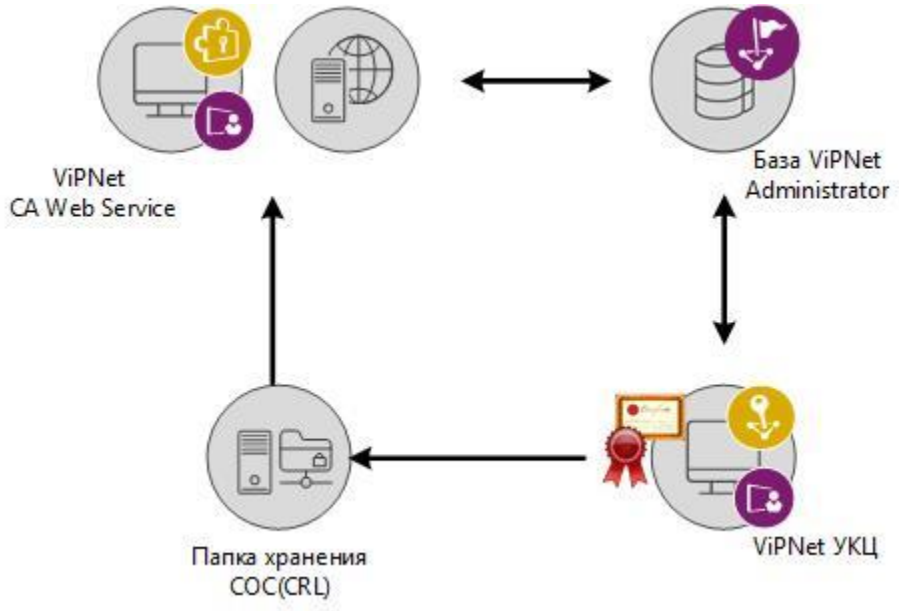
- запросы на выдачу сертификатов в форматах PKCS#10 и CMS;
- запросы на отзыв, приостановление и возобновление действия сертификатов;
- запросы актуальных списков отозванных сертификатов.

Передает пользователям:

- изданные по запросам сертификаты;
- актуальные СОС.

Назначение компонентов УЦ

Взаимодействие компонентов УЦ с CA Web Service



- Передача запросов в УКЦ и ответов пользователям и в ЦР производится автоматически.
- Взаимодействие с УКЦ осуществляется через базу данных ViPNet Administrator и папку хранения COC.
- Пользователи взаимодействуют с CA Web Service с помощью специального ПО.

Назначение компонентов УЦ

ViPNet TSP-OCSP Service

- позволяет обеспечить выполнение следующих функций:
  - выдачу штампов времени по TSP-запросам для удостоверения точного времени создания или подписи электронных документов;
  - предоставление информации о статусах сертификатов в реальном времени по OCSP-запросам.
- может использовать источники точного времени следующих типов:
  - системное время компьютера, на котором установлен;
  - специализированная аппаратура (измерители времени и частоты);
  - NTP-сервер;
- состоит из:
  - службы Infotecs TSP/OCSP Server;
  - клиентского компонента;
  - «Настройка параметров ViPNet TSP/OCSP Server».

Назначение компонентов УЦ

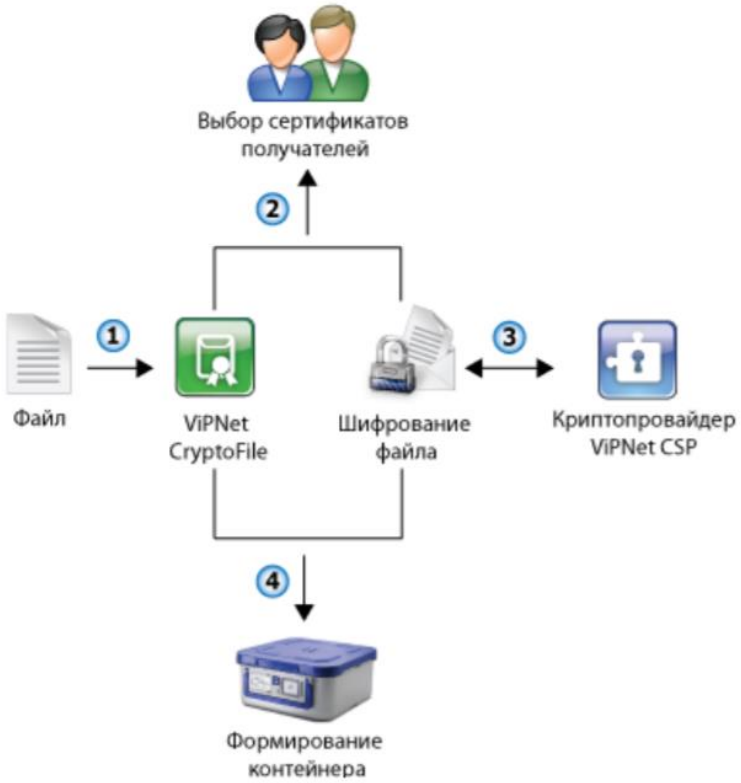
ViPNet CryptoFile

Предназначен для

- проверки электронной подписи и определения авторства пользователей, подписавших документы:
  - при проведении технической экспертизы при разборе конфликтных ситуаций;
  - по обращениям пользователей в удостоверяющий центр;
- заверения файлов электронной подписью;
- шифрования файлов;
- формирования TSP-запросов на получение штампов времени и добавление полученных штампов в электронную подпись файлов.

Назначение компонентов УЦ

ViPNet CryptoFile

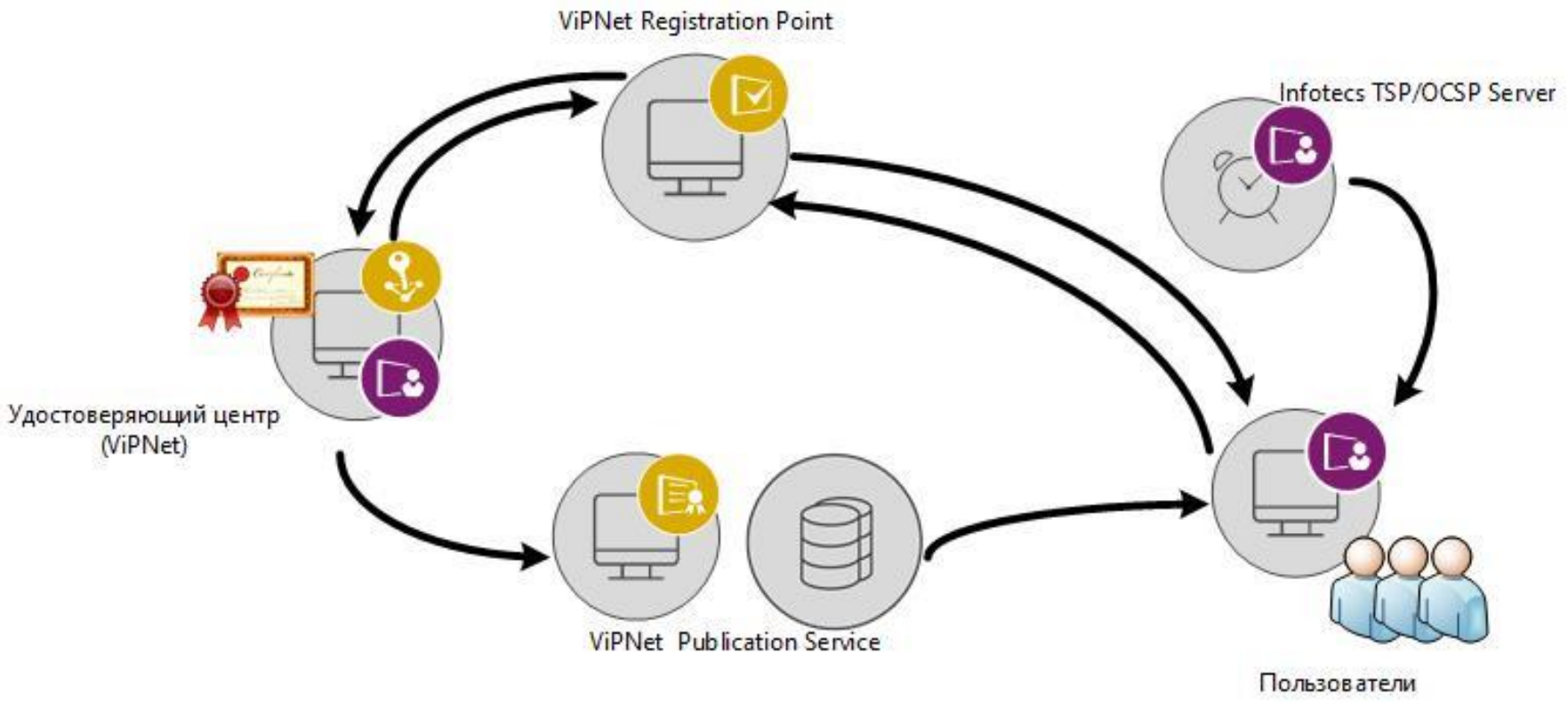


Подписание данных файла с помощью ViPNet CryptoFile.

Шифрование данных файла с помощью ViPNet CryptoFile.

Назначение компонентов УЦ

Взаимодействие компонентов УЦ



Отношения доверия

Кросс-сертификация

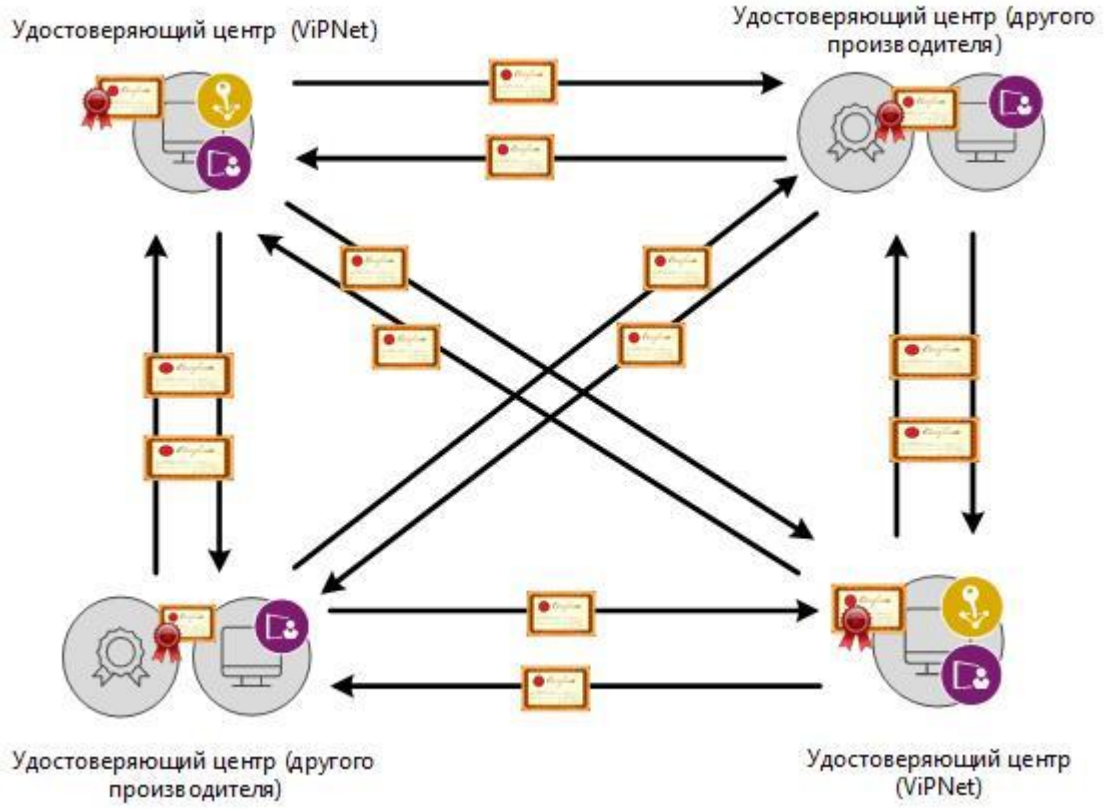
Кросс-сертификация:

- механизм установления доверительных отношений между удостоверяющими центрами, осуществляемый через выпуск кросс-сертификатов одним УЦ для другого УЦ;
- используется при создании сетевой, иерархической и мостовой моделей архитектуры PKI.

Доверительные отношения могут быть установлены как с УЦ, построенными на базе технологии ViPNet, так и с УЦ других производителей.

Отношения доверия

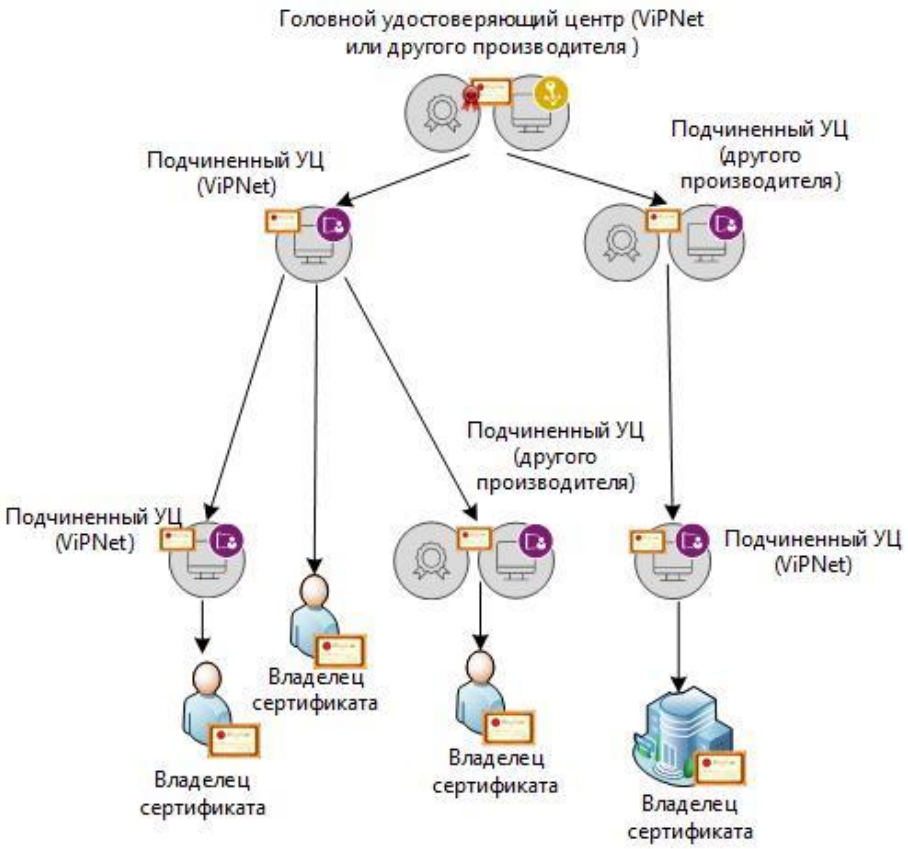
Распределенная модель доверия



- Все УЦ равноправны.
- Каждый УЦ имеет свой корневой сертификат.
- Обычно используется в PKI при установлении доверительных отношений между УЦ разных организаций.

Отношения доверия

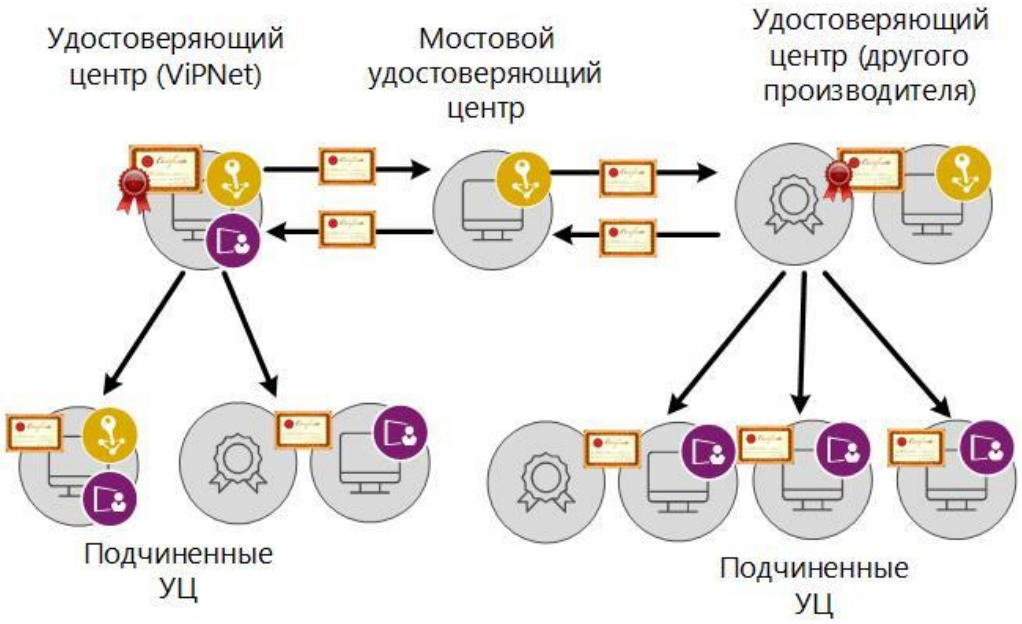
Иерархическая модель доверия



- УЦ объединены в древовидную структуру и связаны отношениями «вышестоящий — подчиненный».
- Головной УЦ выдает сертификаты подчиненным ему УЦ.
- Сертификат головного УЦ является корневым (самоподписанным).
- Подчиненные УЦ могут выдавать сертификаты УЦ более низкого уровня и пользователям.

Отношения доверия

Мостовая модель доверия



- Выделенный УЦ выступает в роли посредника («моста») между остальными УЦ, связывая их между собой.
- Не является головным удостоверяющим центром.
- Не выпускает сертификаты непосредственно для конечных пользователей.
- Через «мостовой» УЦ могут быть связаны системы УЦ.

infotecs

Спасибо за внимание!

Вопросы?

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru