Криптосистема ViPNet

УОНЦ ДПО ПТК «Учебный центр «ИнфоТеКС»

Электронная подпись в технологии ViPNet

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:

- *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*

(п. 1 ст. 2 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

ЭП 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

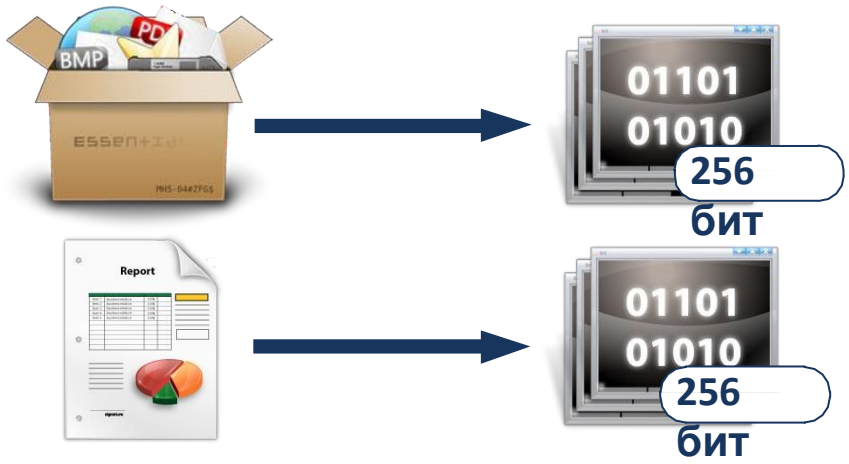
- **Хэш-функция используется:**
  - ✔ для контроля целостности сообщения
  - ✔ для формирования контрольной суммы
  - ✔ для формирования и проверка ЭП

- **Алгоритмы хеширования:**
  - ✔ ГОСТ Р 34.11–94
  - ✔ ГОСТ Р 34.11–2012

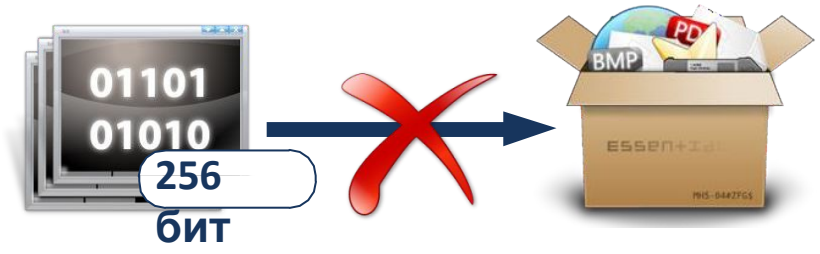
ЭП в технологии ViPNet

Свойства хэш - функций

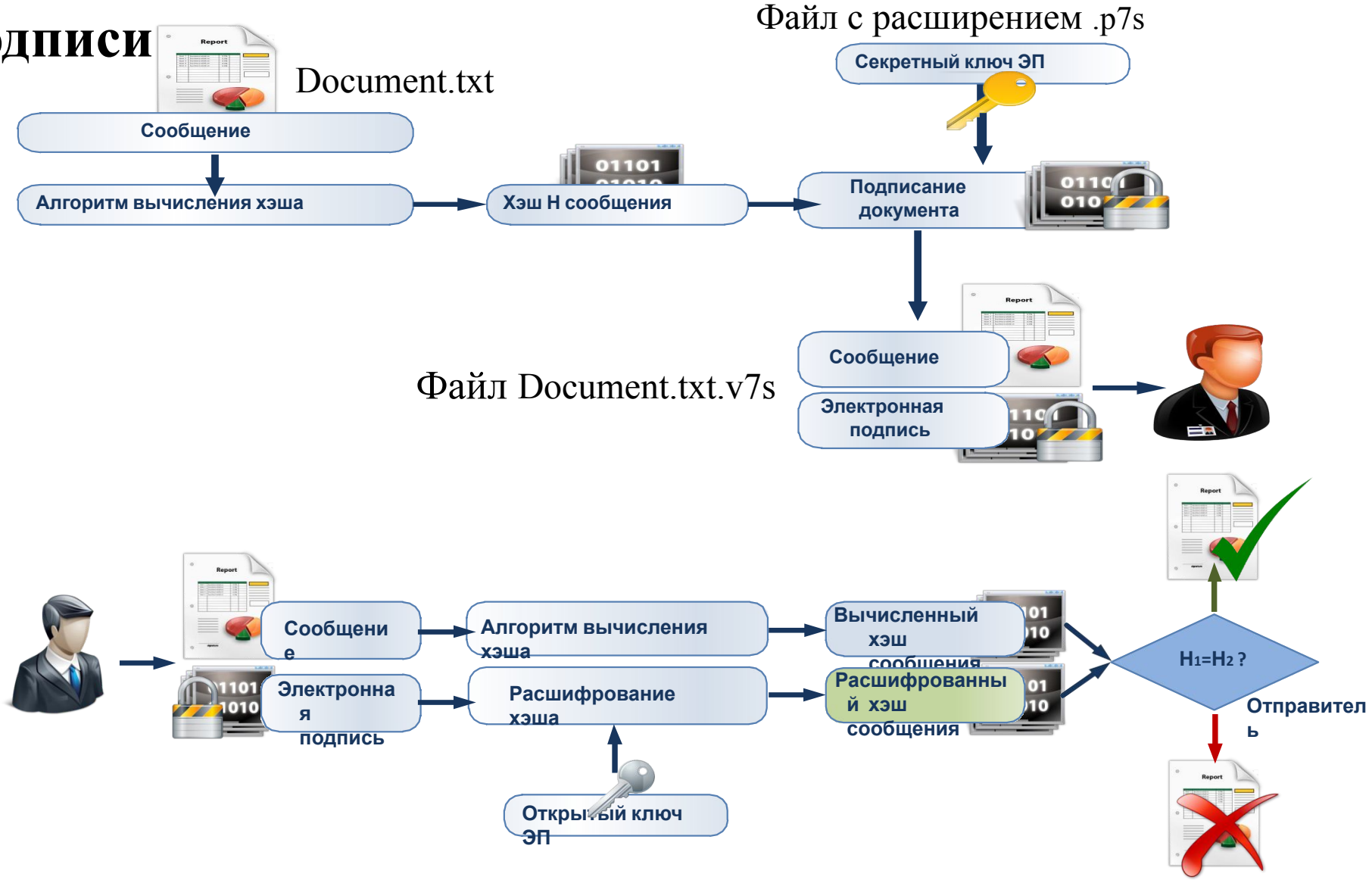
Постоянная длина значения функции:



Необратимость:



Применение хэш-функции и асимметричного алгоритма в электронной подписи



Сертификат ключа проверки электронной подписи

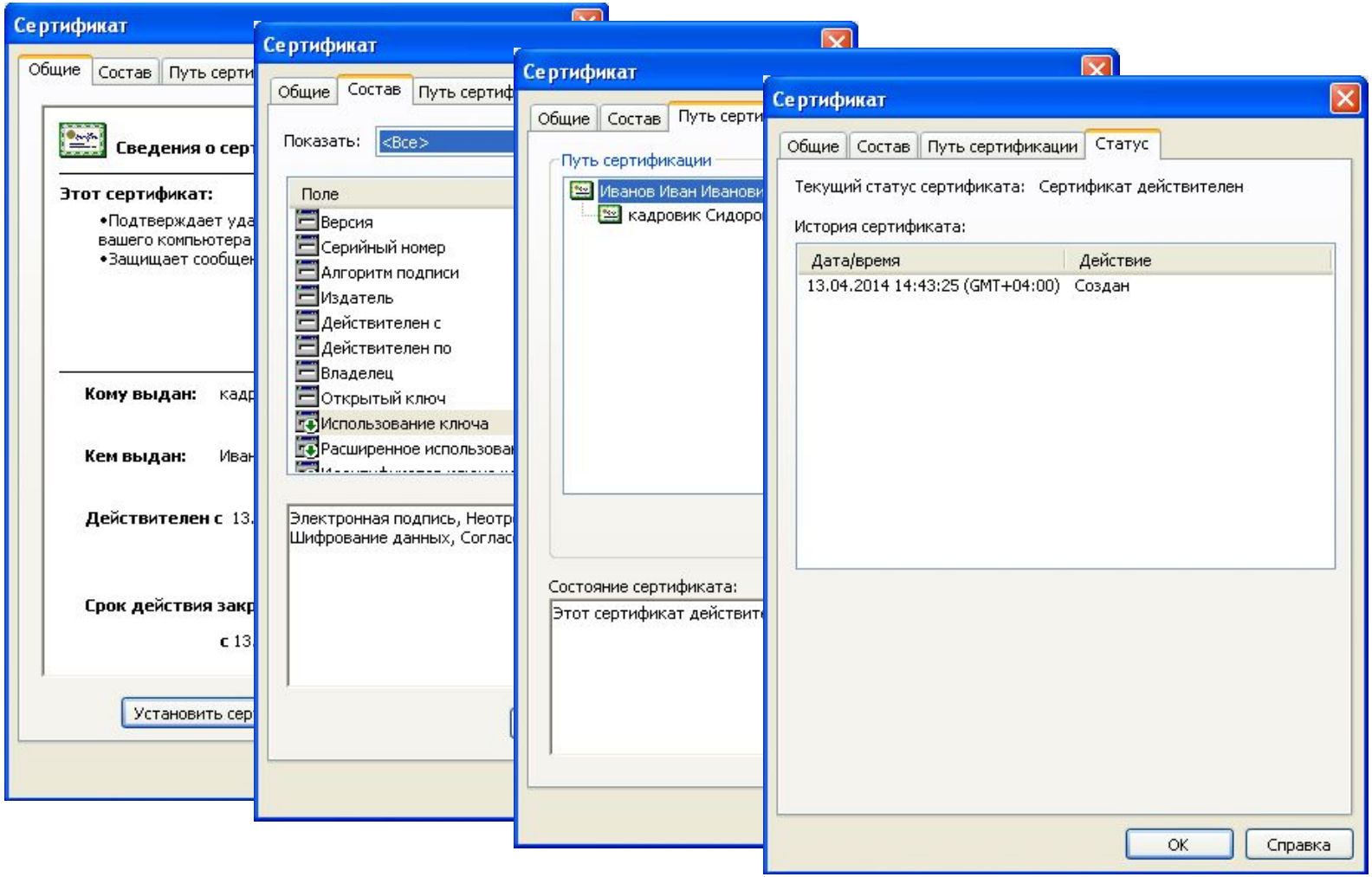
- электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи

(п. 2 ст. 2 ФЗ № 63-ФЗ «Об электронной подписи»)

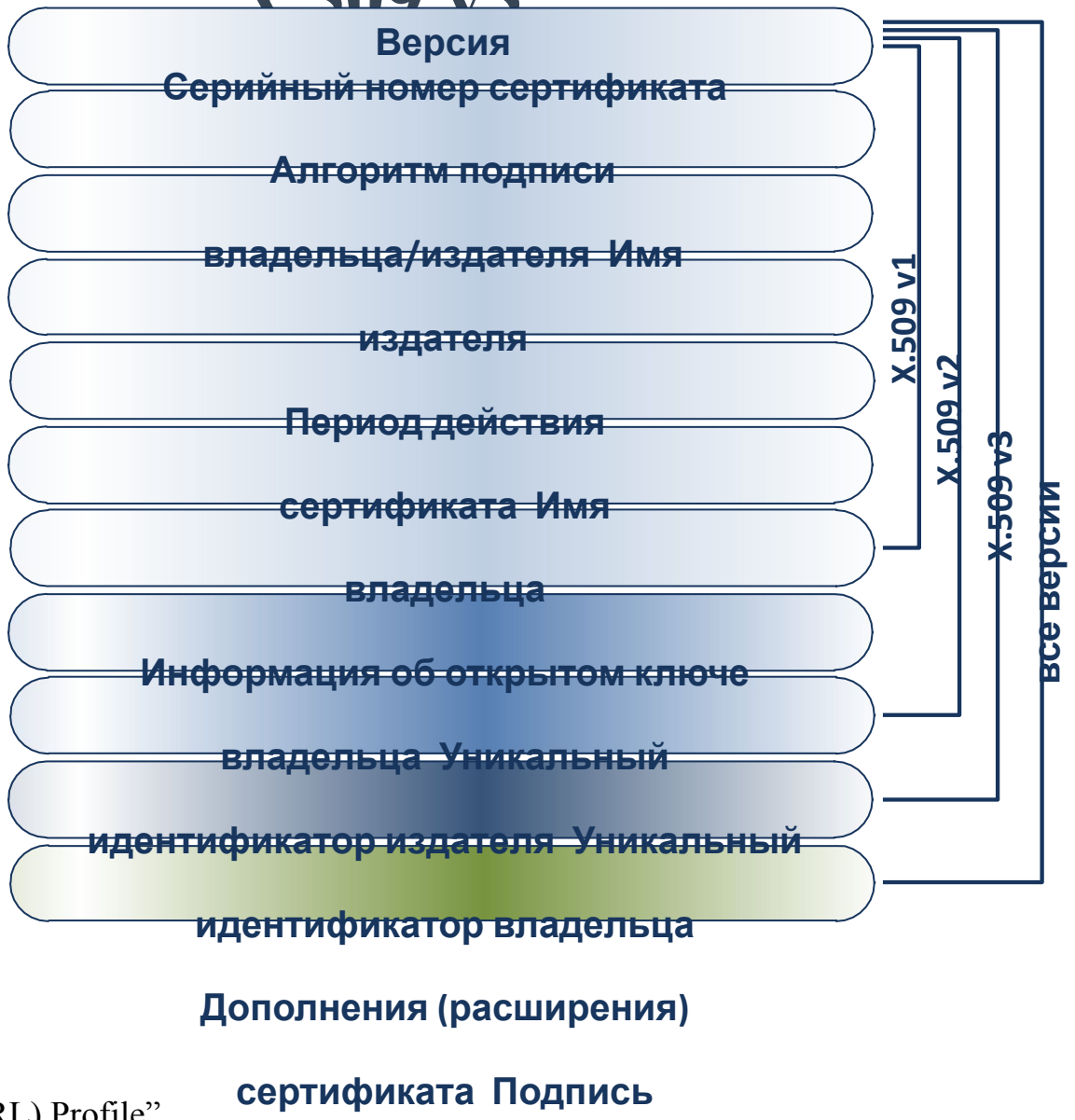
- используется:
  - *для проверки подписи владельца сертификата*
  - *для подтверждения того, что документ подписан именно этим пользователем*
- В УЦ ViPNet создается в Удостоверяющем ключевом центре
- заверяется ЭП администратора УКЦ

ЭП в технологии ViPNet

Сертификат ключа проверки ЭП



Состав полей сертификата стандарта X.509 v3



Revocation List (CRL) Profile”

ЭП в технологии ViPNet

Квалифицированный сертификат ключа проверки ЭП:

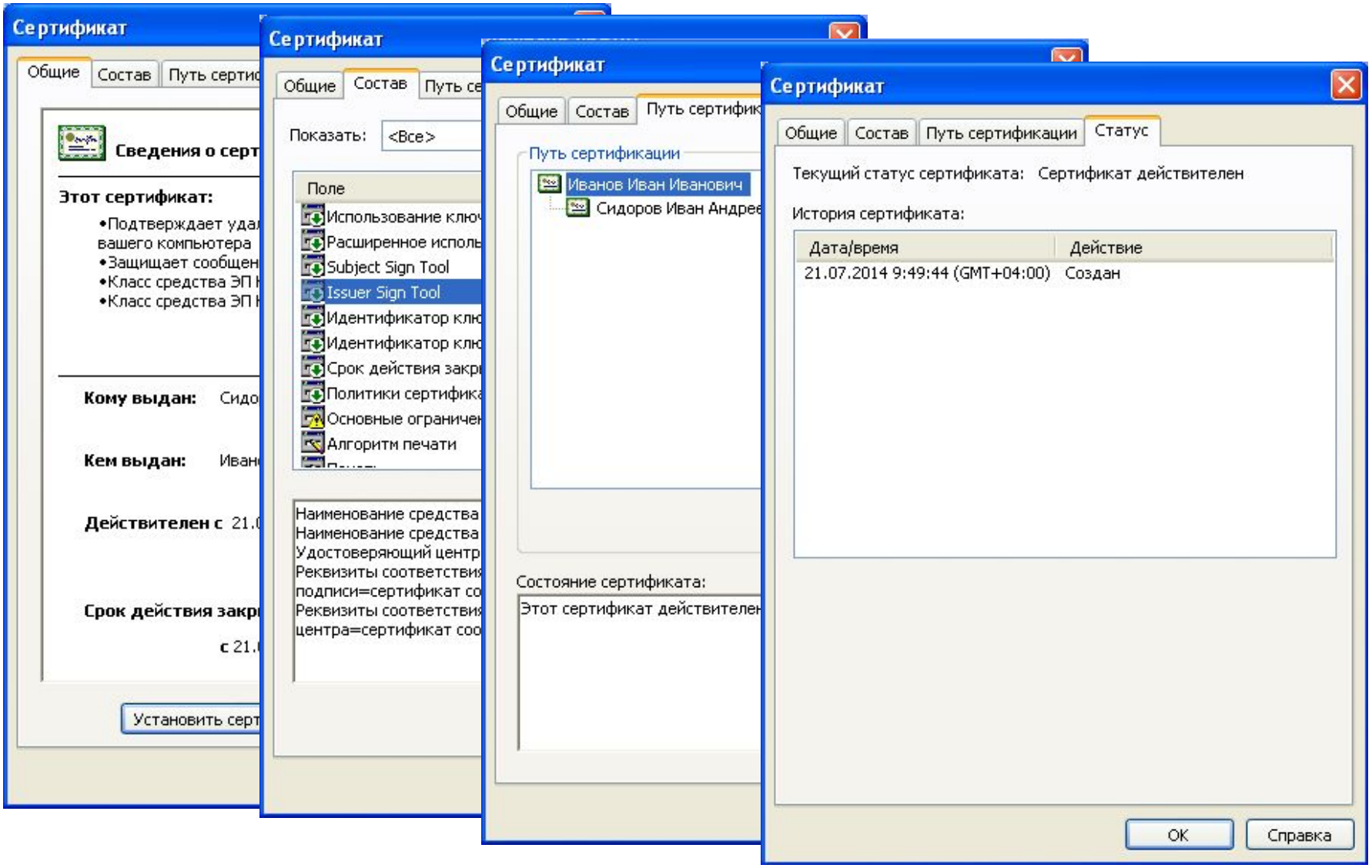
- ✔ *сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным центром удостоверяющим либо федеральным органом власти, уполномоченным в области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

(ФЗ № 63-ФЗ «Об электронной подписи»)

ЭП в технологии ViPNet

infotecs

Квалифицированный сертификат ключа проверки ЭП



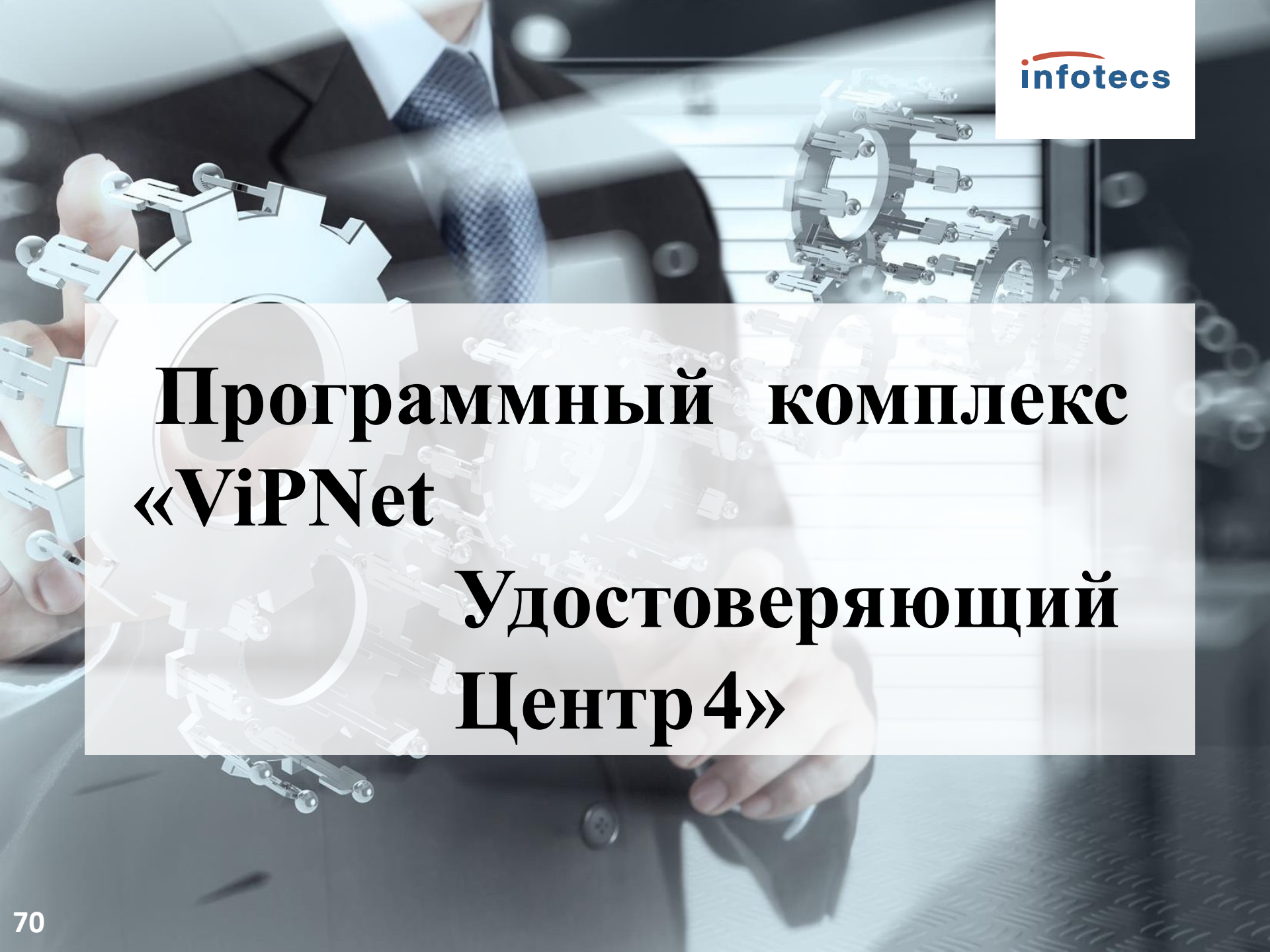
ЭП в технологии ViPNet

Список аннулированных сертификатов:

- электронный документ, который содержит информацию о сертификатах, которые на определенный момент времени аннулированы, или действие которых было приостановлено
- используется:
  - ✔ *для определения статуса сертификата*
- создается в Удостоверяющем ключевом центре
- заверяется ЭП администратора УКЦ

Жизненный цикл сертификата

Приложение № 1 к приказу ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра



Программный комплекс «ViPNet Удостоверяющий Центр 4»

Программный комплекс «ViPNet Удостоверяющий центр 4»

Программный комплекс «ViPNet Удостоверяющий центр 4» 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
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/128-2932*** от "***10***" ***августа*** 201***6*** г.

Действителен до "***10***" ***августа*** 201***9*** 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.00114-05 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 № 769В-000501.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00114-05 30 01 ФО.

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

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

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

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:

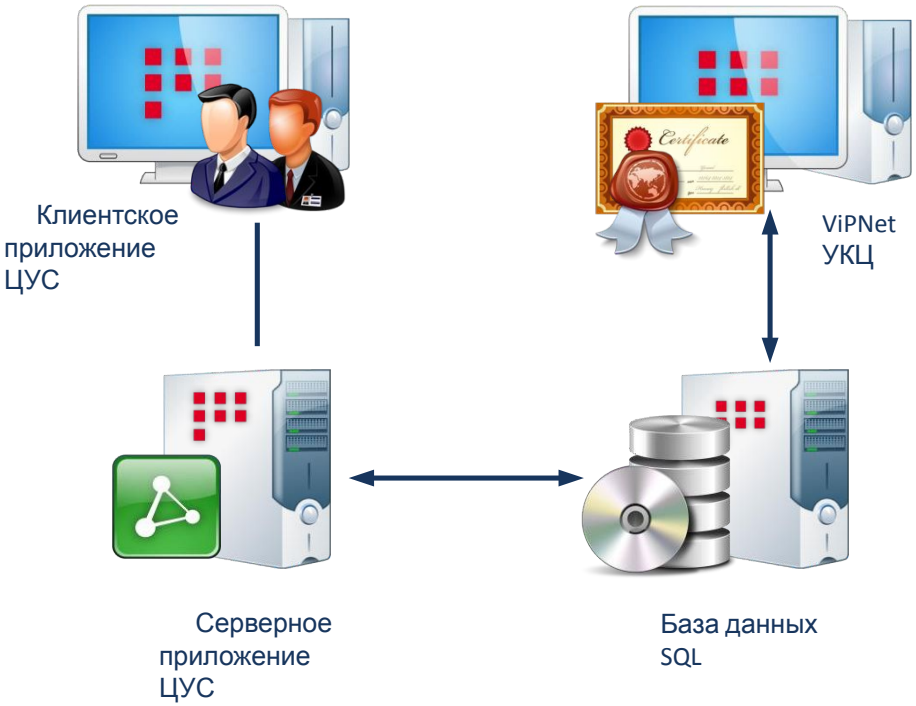
- *создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата (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

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*

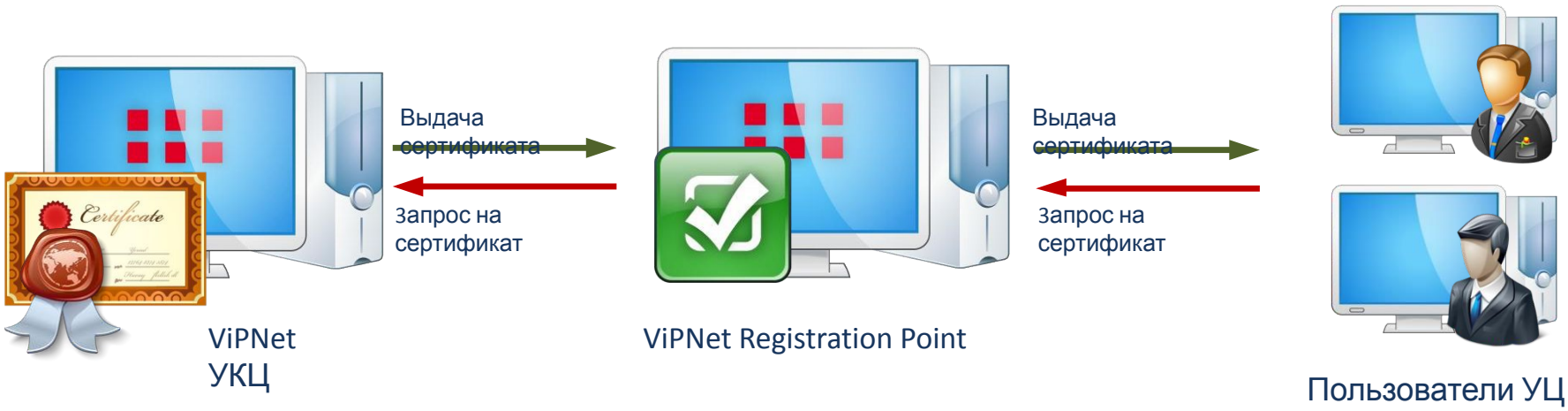
Назначение компонентов УЦ ViPNet Registration Point:

- *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, приост ие 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 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

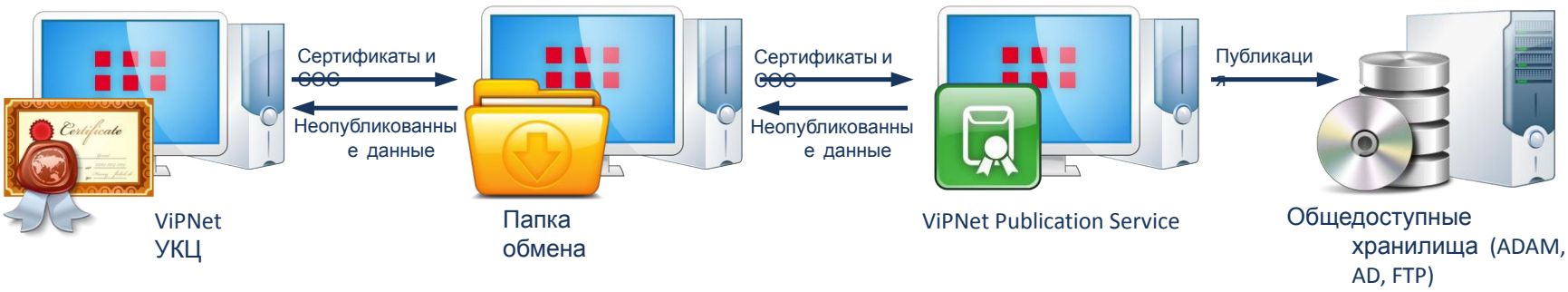
ViPNet Publication Service:

предназначен для

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

Назначение компонентов УЦ

Взаимодействие компонентов УЦ с Publication Service



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

Назначение компонентов УЦ

ViPNet CA Services:

- *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 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 для создания уведомления и настройки их рассылки, формирования отчетов и экспорта сертификатов

Назначение компонентов УЦ

Взаимодействие компонентов УЦ