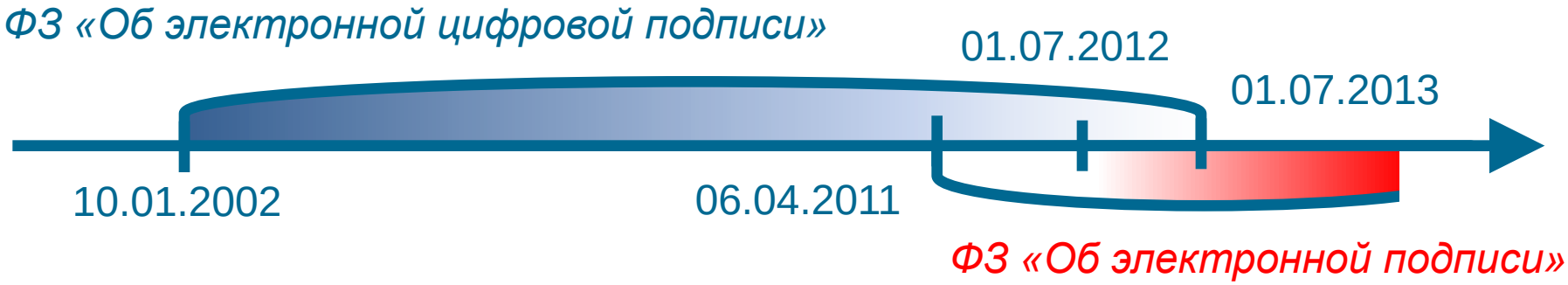
Электронная подпись как часть электронного документооборота. Рекомендации по защите систем электронного документооборота

Докладчик:
Руководитель отдела безопасности информационных систем
ООО «НТЦ «Вулкан» (лицензиат ФСБ России, ФСТЭК России и МО РФ)
Кузнецов Александр Васильевич

Обзор законодательства. Начало

- 8 апреля 2011 года вступил в силу Федеральный закон от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»
- Федеральный закон от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» определил, что Федеральный закон от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи» утратит силу 01 июля 2013 года



Обзор законодательства. Продолжение

~~Электронная цифровая подпись (ЭЦП)~~

Электронная подпись (ЭП)

Обзор законодательства. Продолжение

ФЗ № 63-ФЗ от 06.04.2011 «Об электронной подписи»

ФЗ № 65-ФЗ от 06.04.2011 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием Федерального закона «Об электронной подписи»

Распоряжение Правительства РФ № 1214-р от 12.07.2011

ПП РФ № 976 от 28.11.2011

ПП РФ № 111 от 09.02.2012

ПП РФ № 634 от 25.06.2012

ПП РФ № 852 от 25.08.2012

ПП РФ № 33 от 25.01.2013

Обзор законодательства. Продолжение

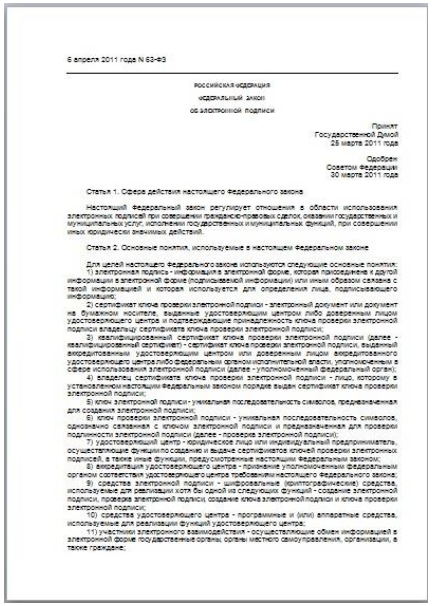
Приказ Минкомсвязи России № 250 от 05.10.2011	Приказ Минкомсвязи России № 242 от 29.09.2011	Приказ Минкомсвязи России № 108 от 13.04.2012
Приказ Минкомсвязи России № 120 от 20.04.2012	Приказ Минкомсвязи России № 320 от 23.11.2011	Приказ Минкомсвязи России № 321 от 23.11.2011
Приказ Минкомсвязи России № 360 от 28.12.2011	Приказ Минкомсвязи России № 81 от 16.03.2012	НМД ФСБ (ФАПСИ) России на СКЗИ

Приказ ФСБ России от 27.12.2011 № 795	Приказ ФСБ России от 27.12.2011 № 796

Обзор законодательства. Окончание

Федеральный закон от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» регулирует отношения в области использования ЭП при совершении юридически значимых действий и вводит:

- основные понятия;
- виды ЭП;
- условия признания ЭД, подписанных ЭП;
- обязанности участников электронного взаимодействия;
- …



6 апреля 2011 года N 63-ФЗ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

ОБ ЭЛЕКТРОННОЙ ПОДПИСИ

Принят
Государственной Думой
25 марта 2011 года

Одобрен
Советом Федерации
30 марта 2011 года

Статья 1. Сфера действия настоящего Федерального закона

Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1) 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;

2) 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;

3) квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

4) владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

5) ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

6) ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

7) удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

8) аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

9) средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

10) средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

11) участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

Свойства информации, требующие обеспечения

- **Целостность** – свойство информации, при котором ее изменение осуществляется только преднамеренно субъектами, имеющими на это право
- **Аутентичность (подлинность)** – свойство информации, гарантирующее, что субъект или ресурс идентичны заявленным
- **Неотказуемость (апеллируемость)** – способность удостоверять имевшее место действие или событие, связанное с информацией, так, что эти события или действия не могли быть позже отвергнуты

Что нам нужно?

- Подтверждение того, что подписывающее лицо не случайно подписало ЭД
- Подтверждение того, что только подписывающее лицо, и только оно, подписало ЭД
- Подписывающее лицо не должно иметь возможности в последствии отказаться от факта подписания ЭД
- Зависимость ЭП от содержания подписываемого ЭД и времени его подписания (если это необходимо)

Ключевые термины и определения. Начало

- **Электронная цифровая подпись (ЭЦП)** – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе
- **Электронная подпись (ЭП)** – 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

Ключевые термины и определения. Окончание

- **Ключ ЭП (закрытый ключ)** – уникальная последовательность символов, предназначенная для создания ЭП

- **Ключ проверки ЭП (открытый ключ)** – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП

- **Сертификат ключа проверки ЭП** – электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП

- **Средства ЭП** – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП

Виды электронных подписей

Простая ЭП

Коды, пароли или иные средства, подтверждающие факт формирования ЭП определенным лицом

Усиленная ЭП

Усиленная неквалифицированная ЭП

Усиленная квалифицированная ЭП

1) Получена в результате криптографического преобразования информации с использованием ключа ЭП

2) Позволяет определить лицо, подписавшее ЭД

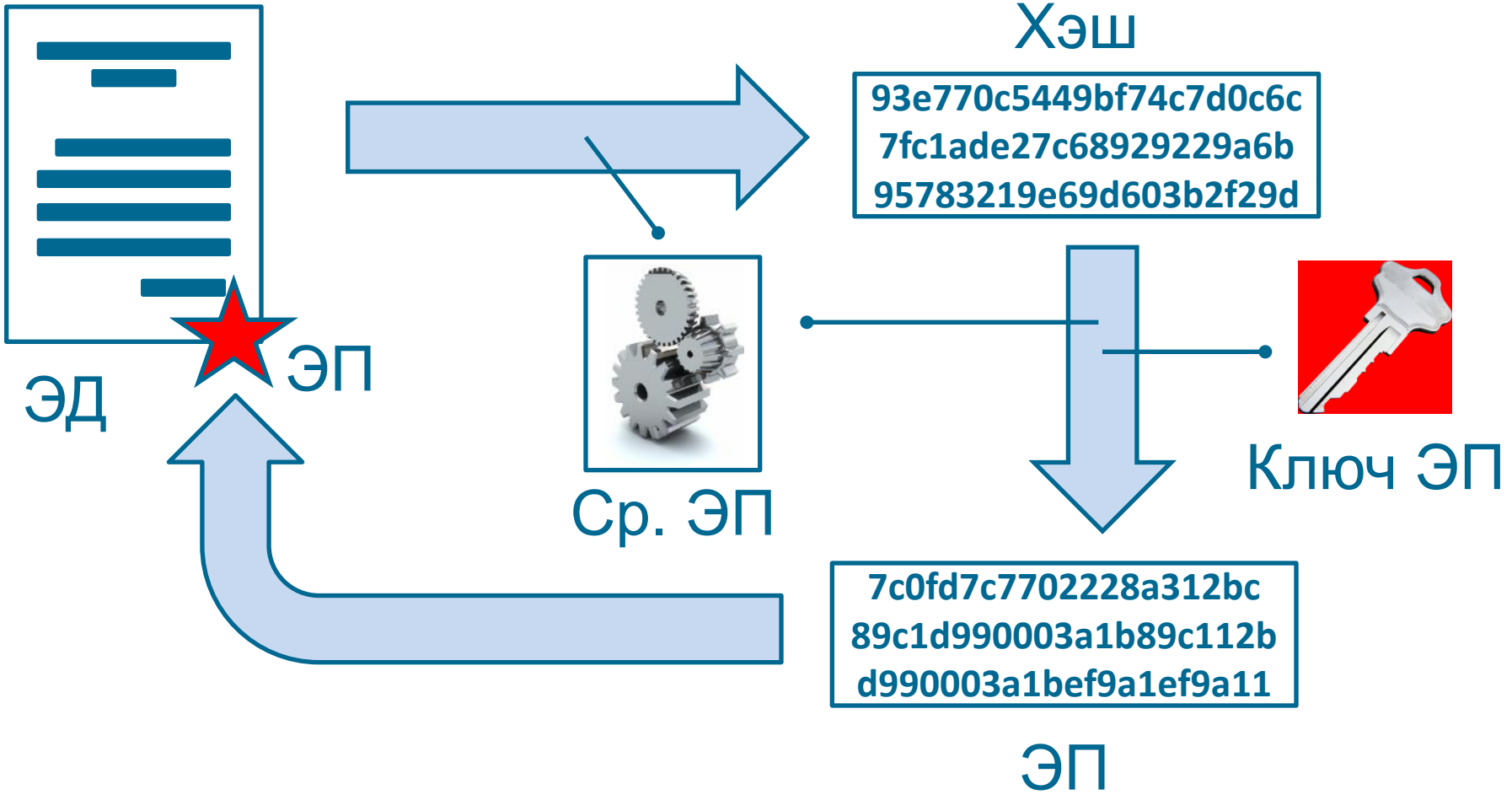
3) Позволяет обнаружить факт внесения изменений в ЭД после момента его подписания

4) Создается с использованием средств ЭП

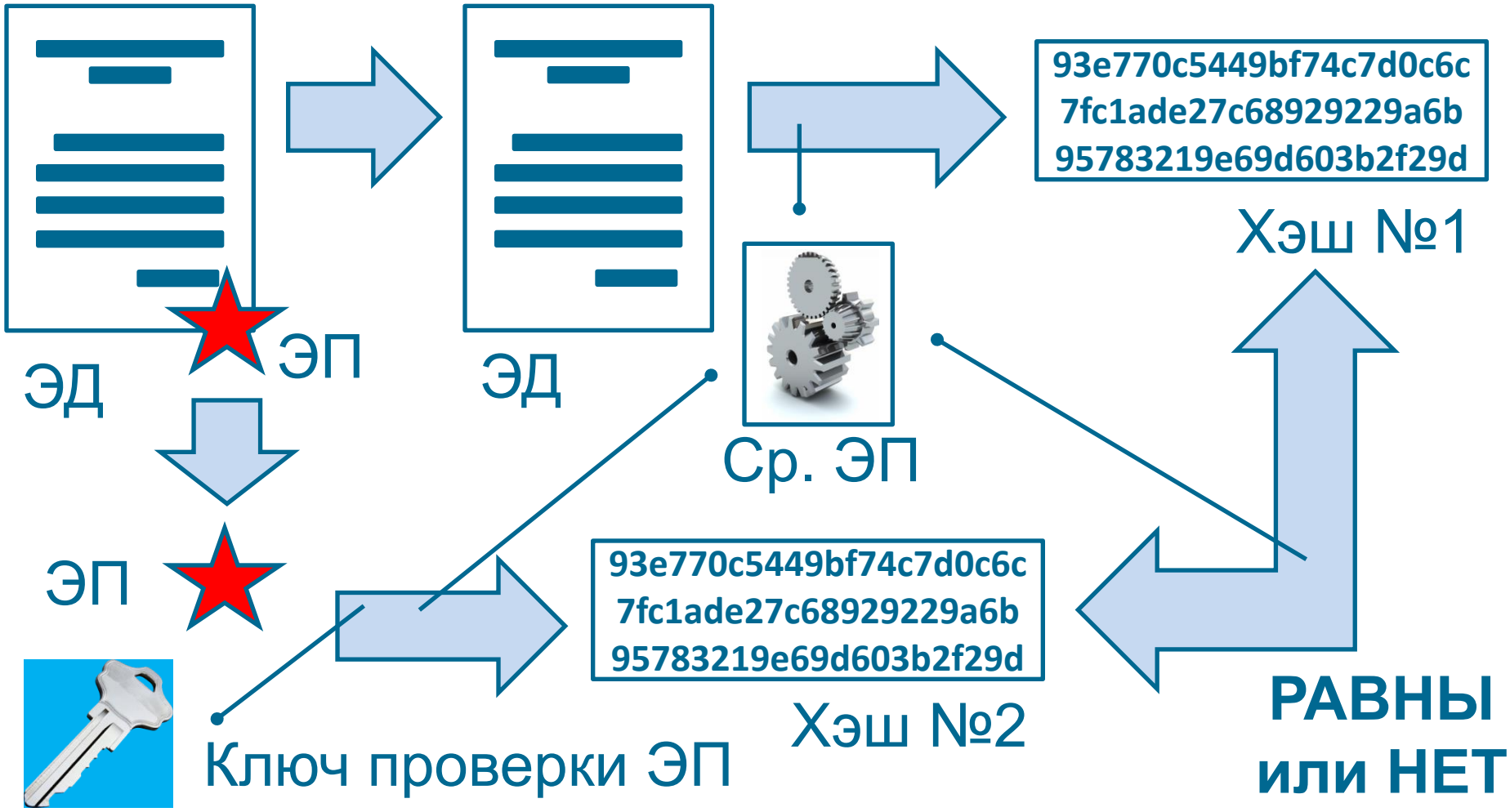
5) Ключ проверки ЭП указан в квалифицированном сертификате

6) Для создания и проверки ЭП используются серт. средства ЭП

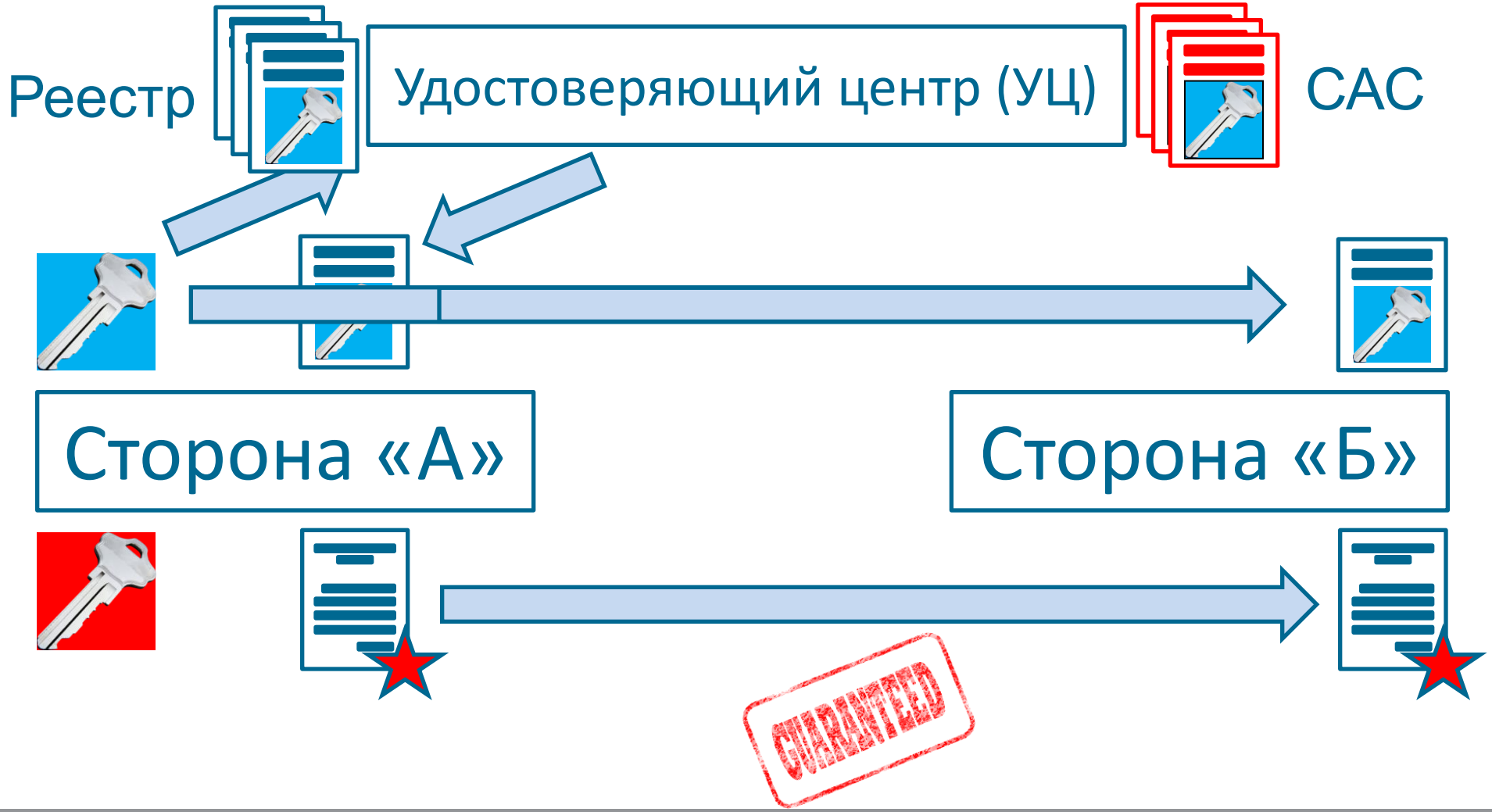
Создание электронной подписи (на стороне отправителя)



Проверка электронной подписи (на стороне получателя)



Участники электронного взаимодействия



Аккредитованные УЦ

- Перечень аккредитованных удостоверяющих центров (в формате XLS) - http://minsvyaz.ru/ru/directions/?regulator=118

- На конец января 2014 года: 338

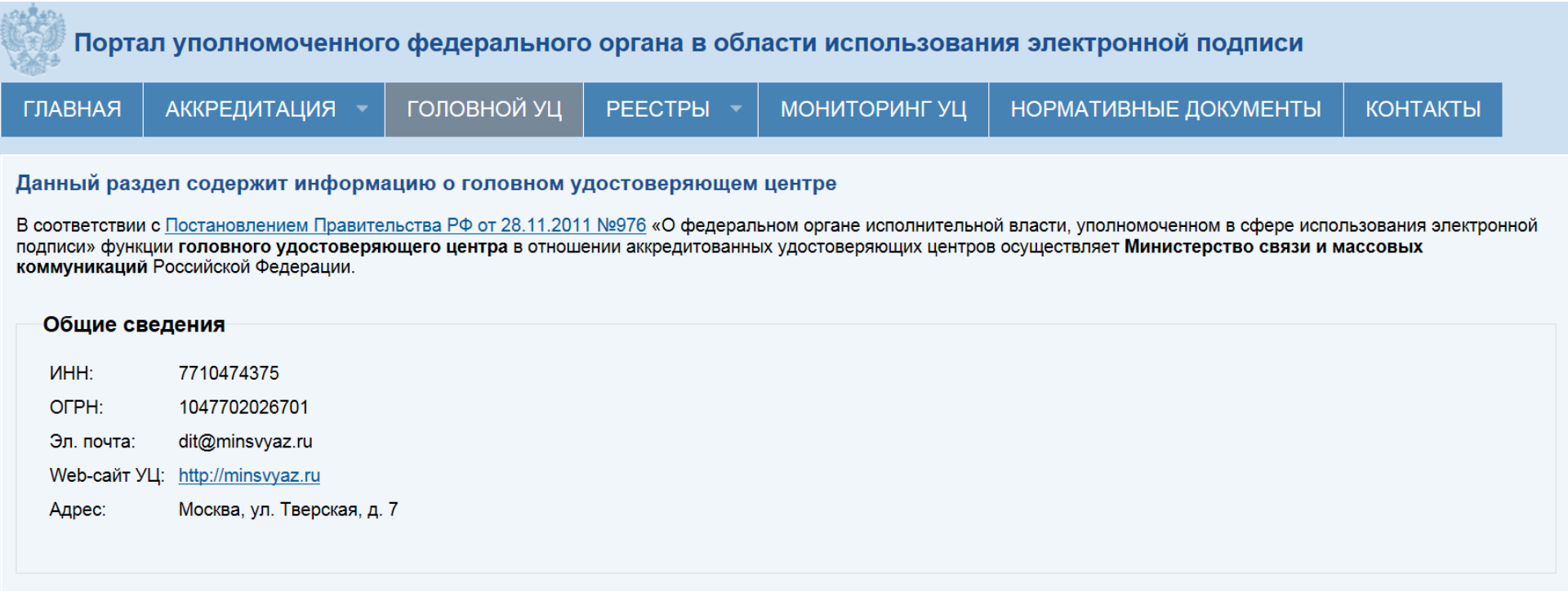
Перечень аккредитованных удостоверяющих центров

N п/п	Название организации/удостоверяющего центра, ИНН, ОГРН	№ Приказа	Адрес места нахождения организации	Примечание
1	Федеральное казенное учреждение «Главный центр связи и защиты информации Министерства внутренних дел Российской Федерации" (ИНН 7706752929, ОГРН 1117746217995)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	г. Москва, ул. Житная, д.16	
2	Общество с ограниченной ответственностью "Удостоверяющий центр ГАЗИНФОРМСЕРВИС" (ИНН 7805544260, ОГРН 1117847050199)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	г. Санкт-Петербург, пр. Стачек, д.47	
3	Закрытое акционерное общество "Национальный удостоверяющий центр" (ИНН 7722766598, ОГРН 1127746036494)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	г. Москва, ул. Авиамоторная, д. 8а, стр. 5	
4	Фонд «Институт фондового рынка и управления» (ИНН 7710264307, ОГРН 1027700197051)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	г. Москва, 2-й Кожевнический переулок, д.12	
5	Открытое акционерное общество "Электронная Москва" (ИНН 7707314029, ОГРН 1027707013806)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	г. Москва, Б. Сухаревский пер., д. 11, стр. 1, офис 6	
6	Общество с ограниченной ответственностью "ТехноКад" (ИНН 5009046312, ОГРН 1045002007984)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	г. Москва, ул. Минская, д. 1Г, корп. 1	
7	Общество с ограниченной ответственностью «Компания «Тензор» (ИНН 7605016030, ОГРН 1027600787994)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	г. Ярославль,Московский проспект, д. 12	
8	Общество с ограниченной ответственностью «Регистрационно-процессинговый центр «Партнер» (ИНН 6454066437, ОГРН 1036405414330)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	г. Саратов, ул.Большая Садовая, д.239, корп 42, офис 422	
9	Государственное бюджетное учреждение «Центр информационных технологий Волгоградской области» (ИНН 3444164285, ОГРН 1083444009241)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	г. Волгоград, ул. Новороссийская, д. 2к	
10	Общество с ограниченной ответственностью «Региональный сервисный центр «Инфо-Бухгалтер» (ИНН 0721009708, ОГРН 1040700231791)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	Кабардино-Балкарская Республика, г. Нальчик, ул. Идарова, 198	
11	Общество с ограниченной ответственностью «КриптоСтандарт» (ИНН 6163100972, ОГРН 1106195001494)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	Ростовская область, Ростов-на-Дону ул. Пушинская,104/32, оф. 61	
12	Общество с ограниченной ответственностью "Сбербизнес" (ИНН 7707752230, ОГРН 1117746480334)	Приказ Минкомсвязи России № 164 от 29.06.2012 г. "Об аккредитации удостоверяющих центров"	г. Москва, ул.Краснопролетарская, д.9, стр.3	
13	Общество с ограниченной ответственностью "ИнфоЦентр" (ИНН 3328430017, ОГРН 1043302000719)	Приказ Минкомсвязи России № 182 от 19.07.2012 г. "Об аккредитации удостоверяющих центров"	г. Владимир, Октябрьский проспект, д.36	
14	Областное бюджетное учреждение "Информационно-технический центр" (ИНН 4823052731, ОГРН 1114823013470)	Приказ Минкомсвязи России № 182 от 19.07.2012 г. "Об аккредитации удостоверяющих центров"	г. Липецк, ул. Крупской, д.1	
15	Общество с ограниченной ответственностью "Центр информационной безопасности" (ИНН 2225100262, ОГРН 1092225000779)	Приказ Минкомсвязи России № 182 от 19.07.2012 г. "Об аккредитации удостоверяющих центров"	г. Барнаул, ул. Северо-западная, д. 159	
16	Закрытое акционерное общество "УДОСТОВЕРЯЮЩИЙ ЦЕНТР" (ИНН 7806122720, ОГРН 1037816019647)	Приказ Минкомсвязи России № 182 от 19.07.2012 г. "Об аккредитации удостоверяющих центров"	г. Санкт-Петербург, Малоохтинский проспект, д.68	
17	Общество с ограниченной ответственностью Научно-производственное предприятие "Ижинформпроект" (ИНН 1831014533, ОГРН 1021801161140)	Приказ Минкомсвязи России № 182 от 19.07.2012 г. "Об аккредитации удостоверяющих центров"	г. Ижевск, ул. Бородина, д.21, оф. 207	

МИНКОМСВЯЗЬ РОССИИ

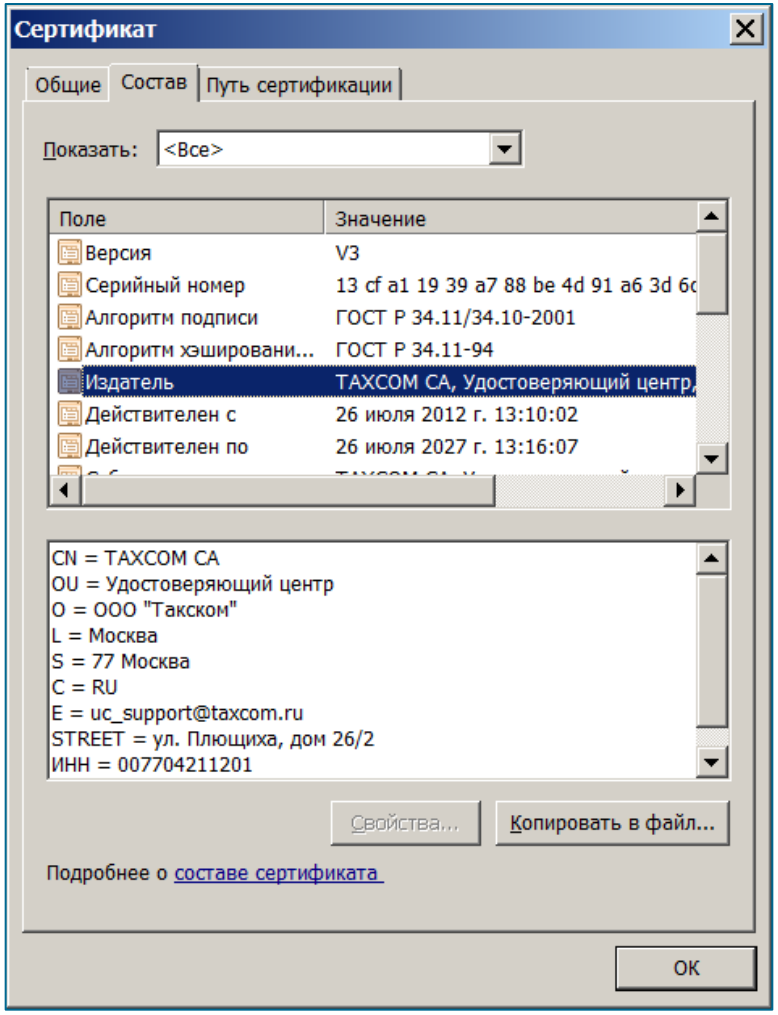
НТЦ ВУЛКАН

Головной УЦ



- Головной УЦ в отношении аккредитованных УЦ – http://e-trust.gosuslugi.ru/MainCA
- Кросс-сертификация самоподписанных сертификатов ЭП аккредитованных УЦ

Аккредитованный УЦ (пример)



Министерство связи и массовых коммуникаций
Российской Федерации

СВИДЕТЕЛЬСТВО
об аккредитации удостоверяющего центра

Регистрационный № 21 « 19 » июля 2012 г.

Настоящим Свидетельством подтверждается соответствие

Общества с ограниченной ответственностью
«Такском»
(полное наименование юридического лица, ОГРН)
ОГРН 1027700071530
г. Москва, ул. Плющиха, д.26/2
(адрес места нахождения юридического лица)

требованиям Федерального закона от 6 апреля 2011 года № 63
«Об электронной подписи».

Аккредитация предоставлена на срок до «19» июля 2017 г. включительно на основании Приказа Минкомсвязи России № 182 от « 19 » июля 2012 года «Об аккредитации удостоверяющих центров».

Министр связи и массовых коммуникаций
Российской Федерации Н.А. Никифоров

Квалифицированный сертификат

- Уникальный номер квалифицированного сертификата
- Даты начала и окончания его действия
- ФИО владельца сертификата – для физ. лица, либо наименование и место нахождения владельца сертификата – для юр. лица (ФИО уполномоченного представителя юр. лица)
- СНИЛС владельца сертификата – для физ. лица
- ОГРН владельца сертификата – для юр. лица
- ИНН владельца сертификата – для юр. лица
- Ключ проверки ЭП
- Наименование используемого средства ЭП и (или) стандарты
- Наименования средств ЭП и средств аккредитованного УЦ
- Наименование и место нахождения аккредитованного УЦ
- Номер квалифицированного сертификата аккредитованного УЦ
- Ограничения использования сертификата (если есть)

Условия признания ЭД, подписанных ЭП

- ч.1 ст.6 ФЗ «Об электронной подписи»: *Информация в электронной форме, подписанная квалифицированной ЭП, признается ЭД, равнозначным документу на бумажном носителе, подписанному собственноручной подписью …*

При одновременном соблюдении следующих условий (ст.11):

- сертификат создан и выдан аккредитованным УЦ (действующим);
- сертификат действителен на момент подписания ЭД или на день проверки, если момент подписание не определен;
- имеется положительный результат проверки принадлежности владельцу сертификата ЭП, с помощью которой подписан ЭД, и подтверждено отсутствие изменений, внесенных в этот ЭД после его подписания;
- ЭП используется в соответствии с учетом ограничений, содержащихся в сертификате (не нарушает ограничений, если они есть)

Средства ЭП

При создании ЭП средства ЭП должны:

- показывать лицу, подписывающему ЭД, содержание информации, которую он подписывает;
- создавать ЭП только после подтверждения лицом, подписывающим ЭД, операции по созданию ЭП;
- однозначно показывать, что ЭП создана

При проверке ЭП средства ЭП должны:

- показывать содержание ЭД, подписанного ЭП;
- показывать информацию о внесении изменений в подписанный ЭП ЭД;
- указывать на лицо, с использованием ключа ЭП которого подписан ЭД

НТЦ ВУЛКАН

Сертифицированные средства ЭП

- КриптоПро CSP
- Signal-COM CSP
- Верба-OW
- Сигнатура
- LISSI-CSP
- ViPNet CSP

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/114-1542 от "04" октября 2010 г.

Действителен до "04" октября 2013 г.

Выдан обществу с ограниченной ответственностью «Крипто Про»

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) «КриптоПро CSP» (версия 3.6) (исполнение 1) в составе согласно формуляру ЖТНИ.00030-02 30 01 ФО

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к СКЗИ класса КС1 и может использоваться для криптографической защиты (генерация и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти, вычисление имитовставки для данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти, вычисление электронной цифровой подписи для данных, содержащихся в областях оперативной памяти, защита TLS-соединений) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных обществом с ограниченной ответственностью «Центр сертификационных исследований» сертификационных испытаний образца продукции № 3SSK-011001

Безопасность информации обеспечивается при выполнении требований нормативных документов формуляры ЖТНИ.00030-02 30 01 ФО и сохранении в тайне ключей шифрования и закрытых ключей электронной цифровой подписи.

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

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.Н.Ковалев

ГОСУДАРСТВЕННЫЙ СТАНДАРТ СОЮЗА ССР

СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ

АЛГОРИТМ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

ГОСТ 28147—89

Издание официальное

ИПК ИЗДАТЕЛЬСТВО СТАНДАРТОВ
Москва

ГОСТ Р 34.10—2001

СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИИ
Москва

ГОСТ Р 34.11—94

СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Издание официальное

СТАНДАРТ РОССИИ
Москва

- ГОСТ 28147-89 – алгоритм криптографического преобразования
- ГОСТ Р 34.10-2001 – процессы формирования и проверки ЭЦП
- ГОСТ Р 34.11-94 – функция хэширования

НТЦ ВУЛКАН

Защита ключей ЭП

- **Обеспечение безопасности хранения ключей ЭП – одна из первоочередных задач**

Основные способы хранения ключей ЭП:

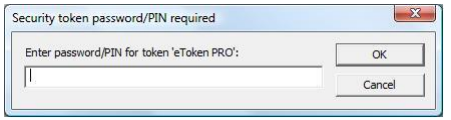
- хранение на персональном компьютере в зашифрованном виде;
- использование специальных внешних устройств

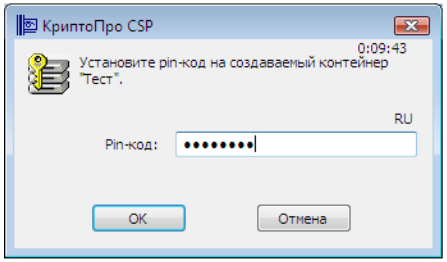
Внешние устройства хранения

Тип устройства	Достоинства	Недостатки
Флэш накопитель, дискета	Не требуется считывающие устройство	Не обеспечивают защиту информации
eToken, RuToken, MicroSD-eToken	Не требуется считывающее устройство, высокая функциональность	-
iButton	Высокая надежность, долговечность, работа в критических условиях	Требуется считывающее устройство, низкая функциональность
Смарт-карты	Высокая функциональность	Требуется считывающее устройство

Защита ключа ЭП

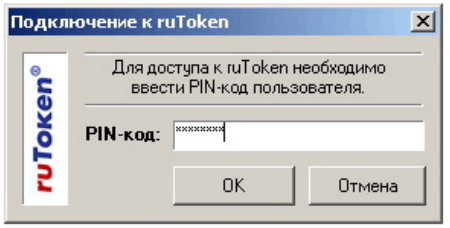
- Запрет экспорта ключа ЭП с носителя
- Защита доступа к ключу ЭП паролем или PIN-ом (смена PIN-а по умолчанию)





Не допускается:

- передавать носитель третьим лицам;
- подключать носитель к компьютерам, непредназначенным для осуществления электронного взаимодействия;



- знакомить с содержанием носителя лиц, к нему не допущенных (выводить информацию на принтер);
- записывать на носитель постороннюю информацию

НТЦ ВУЛКАН

Компрометация ключа ЭП

- Потеря носителя с ключом ЭП
- Потеря носителя с ключом ЭП с его последующим обнаружением
- Нарушение правил хранения носителя с ключом ЭП
- Возникновение подозрений на утечку информации или её искажение
- Случаи, когда нельзя достоверно установить, что произошло с носителем (в том числе случаи, когда носитель вышел из строя и не опровергнута возможность того, что данный факт произошел в результате НСД)

Аннулирование сертификата

Запрос в УЦ на аннулирование сертификата должен содержать:

- информацию, позволяющую однозначно идентифицировать сертификат;
- причину отзыва (например: *компрометация или подозрение на компрометацию, увольнение работника, организационно-штатные изменения, утеря или порча ключевого носителя, ошибка в сертификате*);
- дату и время отзыва, в случае необходимости указать «немедленно»

Дополнительные возможности в рамках ЭДО

Online Certificate Status Protocol (OCSP)

- Протокол получения статуса сертификата ЭП в реальном времени. Протокол OCSP работает по принципу «запрос-ответ»

Time-Stamp Protocol (TSP)

- Протокол представляет собой набор методов, позволяющих установить, является ли электронный документ созданным или подписанным в (или раньше) определенное время

Защита систем электронного документооборота

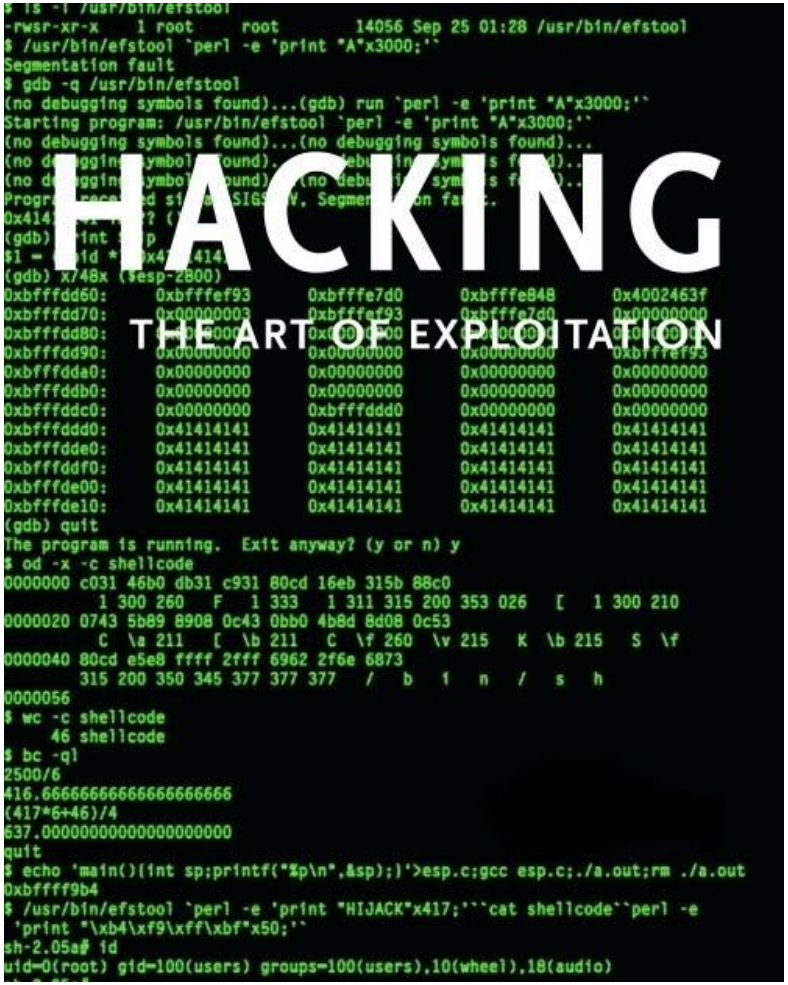
- Совокупность организационных и технических мероприятий
- Использование встроенных и дополнительных средств защиты информации

Принципы:

- актуальность;
- системность;
- комплексность;
- разумная достаточность;
- планирование и контроль;
- преемственность и совершенствование

Атаки «были, есть и будут …»

- Атаки на протокол установления связи (10 подвидов);
- Атаки на протоколы записи и протоколы данных приложений (12 подвидов);
- Атаки на инфраструктуры открытых ключей (8 подвидов);
- Прочие виды атак



Перечень атак подготовлен на основании материалов статьи «Краткий обзор SSL/TLS атак» (автор: Крис Мейер, журнал: «Безопасность ИТ-инфраструктуры № 12 (78)»)

Спасибо за внимание!

Кузнецов Александр Васильевич
Руководитель отдела безопасности
информационных систем
a.kuznetsov@ntc-vulkan.ru

ООО «НТЦ «Вулкан»
105318, г. Москва, ул. Ибрагимова, д. 31
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru