

Единое пространство доверия Ожидание и реальность

**Михайлов Никита Сергеевич
Исполнительный директор
Удостоверяющего Центра Сибири**

**Научный руководитель
Шелупанов Александр Александрович
д.т.н., профессор**

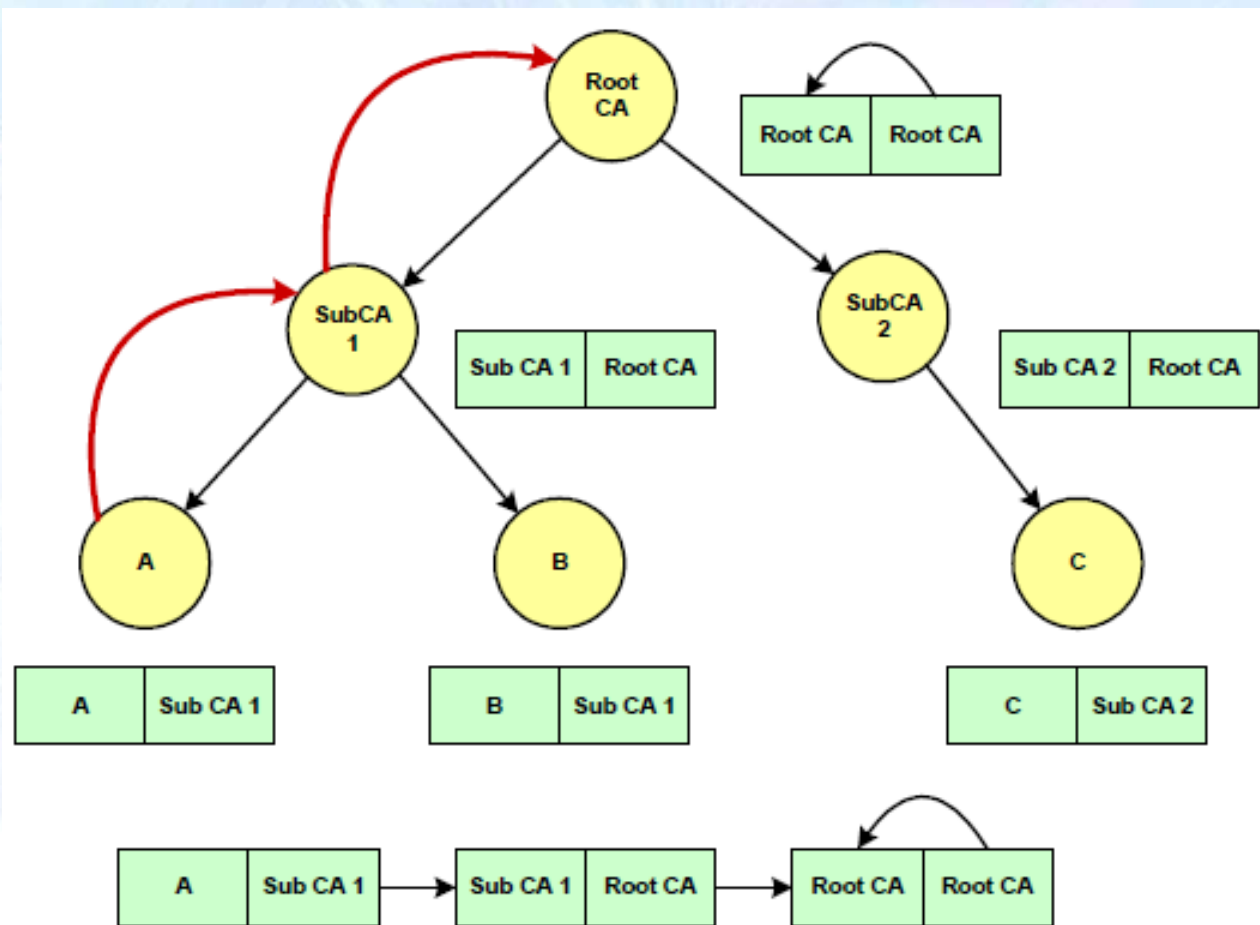
Правовые условия использования электронной цифровой подписи в электронных документах регламентируют:

- **ФЗ от 10.01.2002 №1-ФЗ «Об электронной цифровой подписи» (действовал до 1.07.2013 г., выданные сертификаты действуют до **31.12.2013**)**
- **ФЗ от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи».**

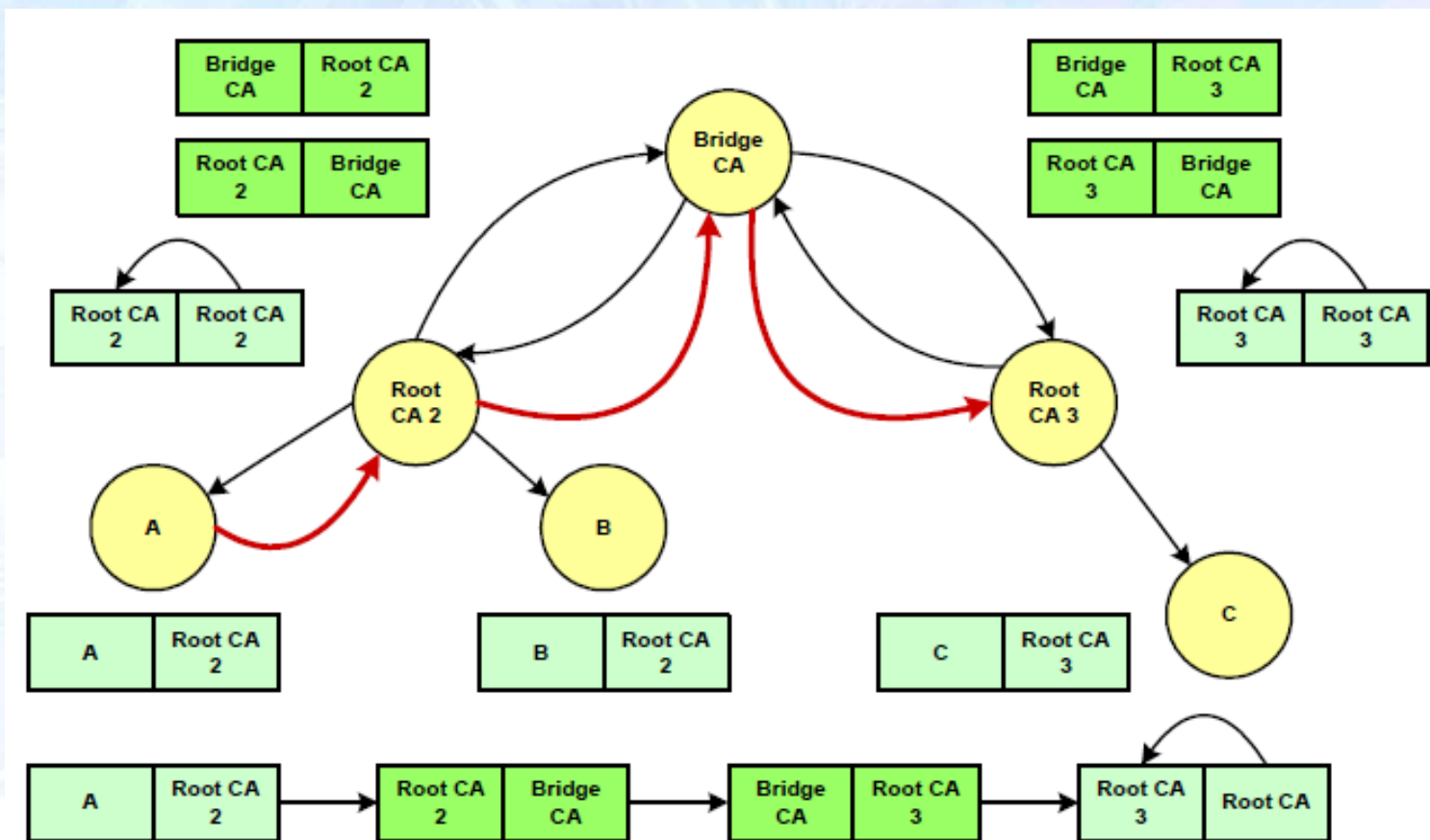
Доверие – интуитивное понятие, отражающее степень уверенности в том, что некая сущность будет вести себя предполагаемым образом.

Модели доверия являются результатом моделирования доверительных отношений, существующих в реальном мире, и отражают все их аспекты: партнерские отношения и отношения подчинения, большой или меньший уровень доверия.

Иерархическая модель



Мостовая модель



Методические рекомендации по составу квалифицированного сертификата ключа проверки электронной подписи

Версия 1.9

Настоящий документ описывает правила формирования аккредитованными УЦ квалифицированных сертификатов ключей проверки электронной подписи, которые могут использоваться в государственных информационных системах.

Методические рекомендации по составу квалифицированного сертификата ключа проверки электронной подписи

Данный документ разработан в целях реализации и во исполнение:

- федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- приказа ФСБ от 27 декабря 2011 г. N 795 "ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К ФОРМЕ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ".

СН 2.5.4.3 Общее имя

Приказ ФСБ от 27 декабря 2011 г. N 795

Методические рекомендации по составу квалифицированного сертификата ключа проверки электронной подписи

В качестве значения данного атрибута имени следует использовать текстовую строку, содержащую имя, фамилию и отчество (если имеется) - для физического лица, или наименование - для юридического лица.

ЮЛ: В зависимости от типа конечного владельца СКПЭП:

- наименование организации;
- ФИО должностного лица;
- название автоматизированной системы;
- другое отображаемое имя по требованиям информационной системы.

ФЛ: ФИО

Методические рекомендации по составу квалифицированного сертификата ключа проверки электронной подписи

Приложение 14. Пример сертификата ЮЛ (должностное лицо)

■ Субъект:

- CN=Иванов Иван Иванович SN=Иванов
- G=Иван Иванович C=RU
- S=69 Тверская область L=Нижний Волочек
- O=ООО "Рога и копыта" OU=Отдел контроля
- T=Инженер-аналитик OGRN=0123456789123
- SNILS=12345678909 INN=000123456789

OGRNIP 1.2.643.100.5**ОГРНИП****Приказ ФСБ от 27 декабря 2011 г. N 795****Методические рекомендации по составу квалифицированного сертификата ключа проверки электронной подписи**

-

ОГРНИП (только для ИП)

Сертификат Головного УЦ

- **CN = Головной удостоверяющий центр**
- ИНН организации = 007710474375
- ОГРН = 1047702026701
- О = Минкомсвязь России
- STREET = 125375 г. Москва, ул. Тверская, д. 7
- L = Москва
- S = 77 г. Москва
- C = RU
- E = dit@minsvyaz.ru

Сертификат УЦ 1 ИС ГУЦ

- CN = УЦ 1 ИС ГУЦ
- C = RU
- S = 77 г. Москва
- L = Москва
- O = Минкомсвязь России
- STREET = 125375 г. Москва ул. Тверская д.7
- E = dit@minsvyaz.ru
- ОГРН = 1047702026701
- ИНН организации = 007710474375

Сертификат ТУСУР

В квалифицированном сертификате следует использовать дополнение `authorityKeyIdentifier` с занесением в поле `authorityCertSerialNumber` номера соответствующего квалифицированного сертификата аккредитованного УЦ или доверенного лица аккредитованного УЦ либо уполномоченного федерального органа, создавшего **исходный** квалифицированный сертификат. Объектный идентификатор типа дополнения `authorityKeyIdentifier` имеет вид 2.5.29.35.

Issuer : CN = УЦ 2 ИС ГУЦ С = RU S = 77 г.Москва L = Москва O = Минкомсвязь России STREET = 125375 г. Москва ул. Тверская д.7 E = dit@minsvyaz.ru ОГРН = 1047702026701 ИНН организации = 007710474375

`authorityKeyIdentifier`: CN=Головной удостоверяющий центр ИНН организации=007710474375 ОГРН=1047702026701 O=Минкомсвязь России STREET="125375 г. Москва, ул. Тверская, д. 7" L=Москва S=77 г. Москва C=RU E=dit@minsvyaz.ru

РЕГЛАМЕНТ

получения сертификатов ключей подписи и использования электронной цифровой подписи от 9 августа 2010 года.

Приказ ФСБ от 27 декабря 2011 г. N 795

CN = ФИО владельца сертификата

Неструктурированное имя

Стать поддельным аккредитованным УЦ – это просто!

1. Выбираем УЦ-«жертву».
2. Заполняем анкету с <http://reestr-pki.ru/> из раздела информация для аккредитации удостоверяющих центров с помощью информации с <http://e-trust.gosuslugi.ru/>.
3. Формируем свой самоподписанный сертификат с данными, аналогичными любого УЦ-«жертвы».
4. Пользуемся услугами любого сервиса анонимной отправки почты с подменой адреса, указав адрес из корневого сертификата УЦ-«жертвы».
5. ????????
6. PROFIT!

Почему уполномоченный федеральный орган в области использования **электронной подписи не принимает от УЦ документы по аккредитации / дополнительной аккредитации нового ПАК в электронном виде, подписанные с использованием **электронной подписи**?**

Спасибо за внимание!

Михайлов Никита Сергеевич
Исполнительный директор
Удостоверяющего Центра Сибири
e-mail: mns@udcs.ru