Иерархия удостоверяющих центров и проверка сертификатов. Продукты реализации PKI

Лекция 10

Электронная цифровая подпись по RSA

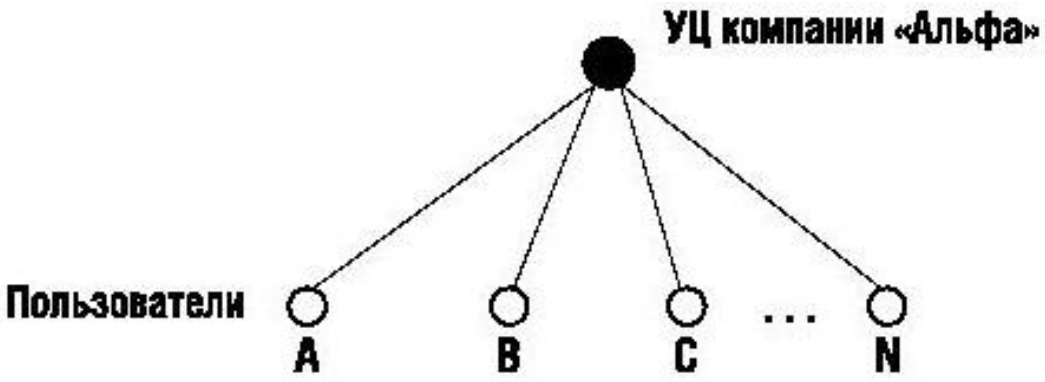
- Подписывание A:
- $SA = m^{d}_{A} \mod n$
- d_A – секретный ключ
- Проверка для B:
- A□ B: SA, M'
- B:m' = h (M')
- $m = (SA)^{e}_{A} \mod n$
- сравнивает m = m'

Архитектуры PKI

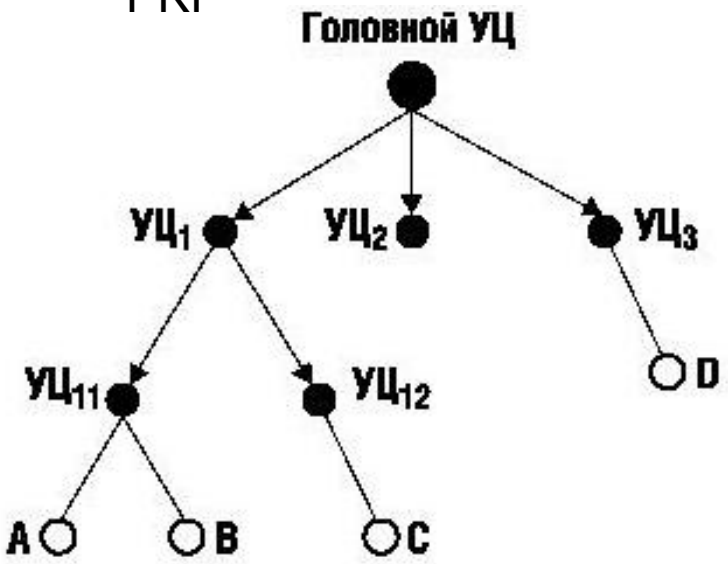
- В основном выделяют 5 видов архитектур PKI, это:
- простая PKI (одиночный УЦ)
- иерархическая PKI (подчинение нескольких УЦ вышестоящему головному УЦ)
- сетевая PKI (объединение одноранговых инфраструктур с перекрестной (кросс-) сертификацией головных УЦ)

Архитектура Public Key Infrastructure

Одиночный УЦ



Иерархическая PKI



Архитектуры PKI

- 4.Кросс-сертифицированные корпоративные PKI (смешанный вид иерархической и сетевой архитектур. Есть несколько фирм, у каждой из которых организована какая-то своя PKI, но они хотят общаться между собой
- 5.Архитектура мостового УЦ (убирает недостатки сложного процесса сертификации в кросс-сертифицированной корпоративной PKI. В данном случае все компании доверяют не какой-то одной или двум фирмам, а одному определённому мостовому УЦ, который является практически их головным УЦ)

ViPNet PKI продукты. Серверное ПО (1).

ПО ViPNet КС & СА (Удостоверяющий и ключевой центр, УКЦ) реализует полный набор функций по управлению сертификатами открытых ключей:

• формирование пар открытый-закрытый ключ по запросам пользователей;

• изготовление сертификатов открытых ключей;

• приостановление и возобновление действия сертификатов, отзыв (аннулирование) сертификатов;

• ведение реестра (справочника) выпущенных сертификатов и списка отозванных сертификатов;

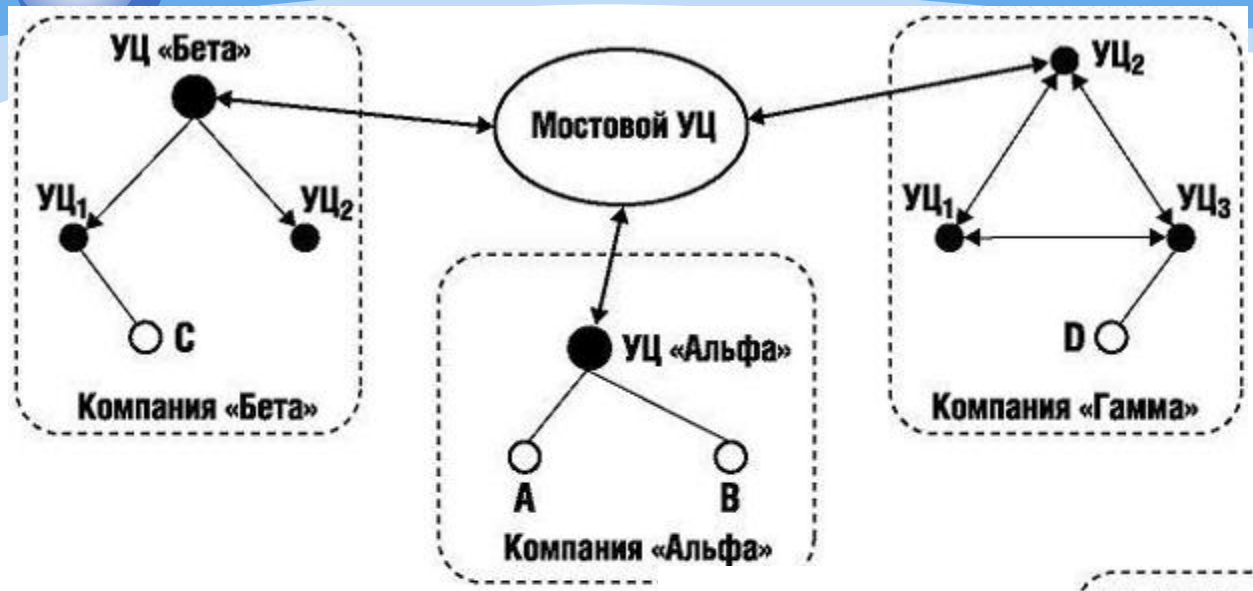
•поддерживает все архитектуры PKI.

ViPNet PKI продукты. Серверное ПО (2).

ViPNet Registration Point (пункт регистрации)

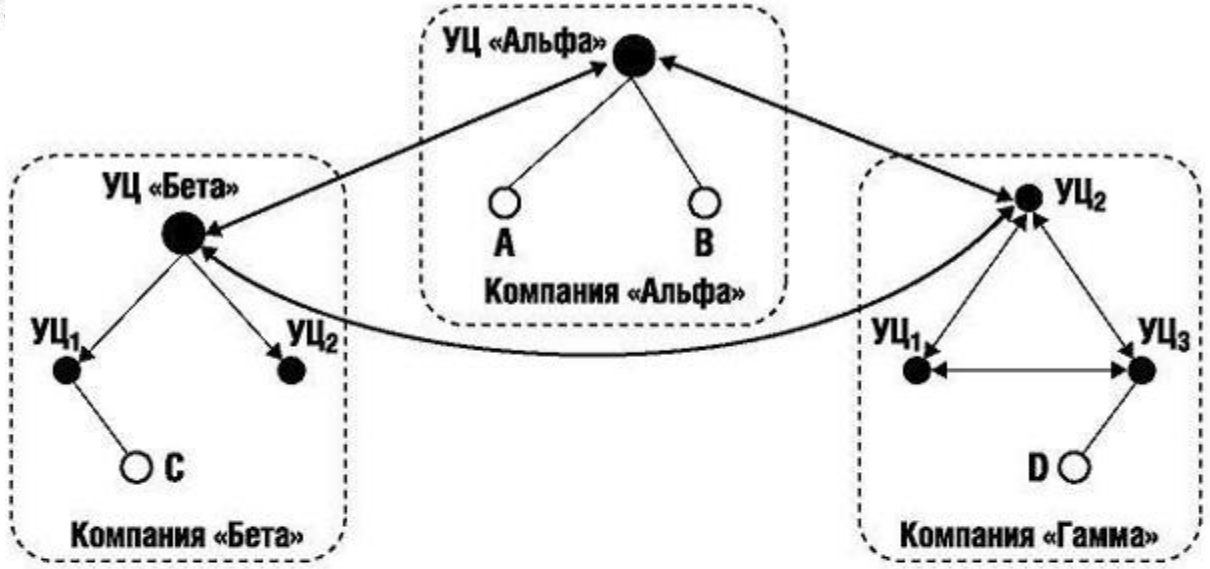
Пункт регистрации, выступая в качестве филиала УЦ, проводит идентификацию пользователей, **генерирует для них ключевые пары или устанавливает факт владения закрытым ключом по предъявленному открытому ключу**, после чего формирует и передает запрос на сертификацию в УЦ. Перенос части функций УЦ в пункт регистрации позволяет снизить требования по организационной, физической и информационной безопасности, что уменьшает расходы на создание УЦ. Пункты регистрации снижают нагрузку на УЦ по обработке запросов пользователей.

Архитектура PKI (2)

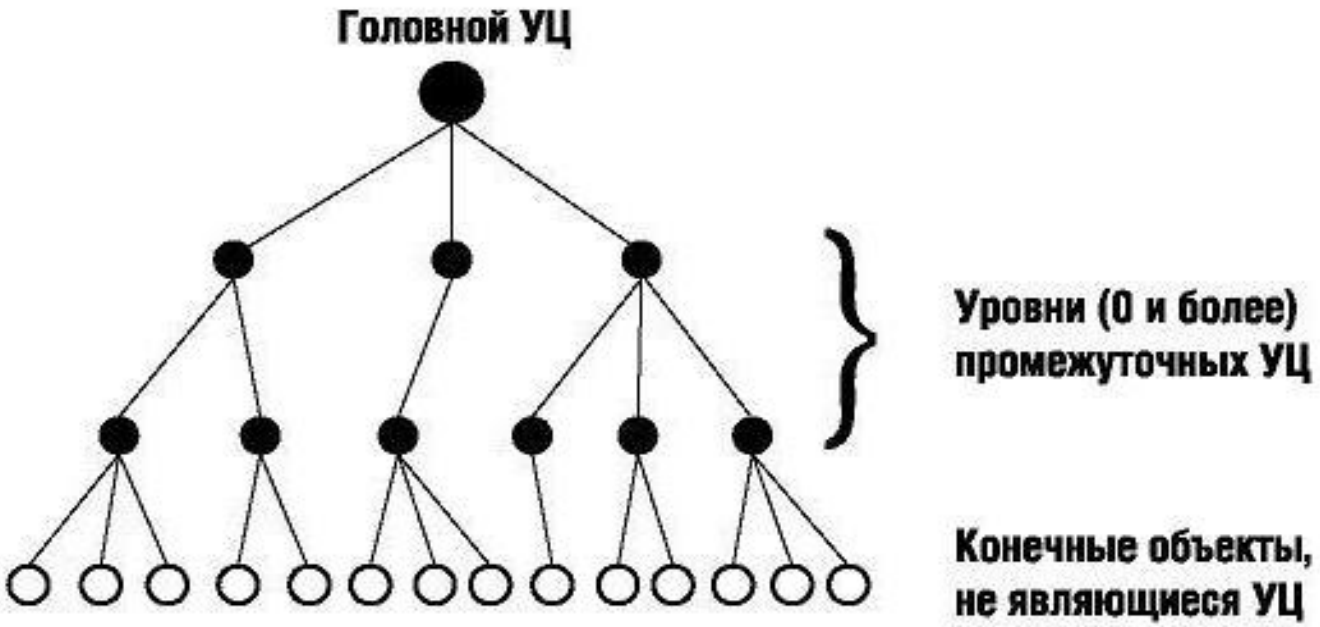


Архитектура мостового УЦ

Кросс-сертифицированные корпоративные PKI

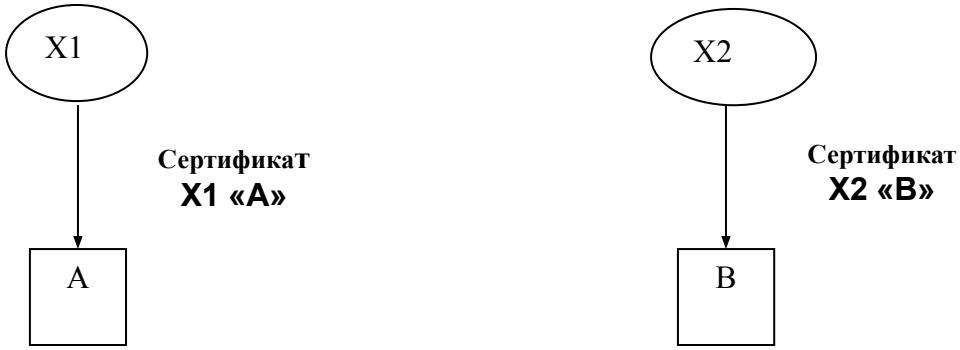


. Строгая иерархия удостоверяющих центров



Участники обслуживаются в разных ЦРК.

Сертифицирующие центры – X1 и X2



X1 «A» - удостоверение пользователя A выданное центром сертификации X1
X2 «B» - удостоверение пользователя B выданное центром сертификации X2

A от B: X1 «X2» X2 «B»

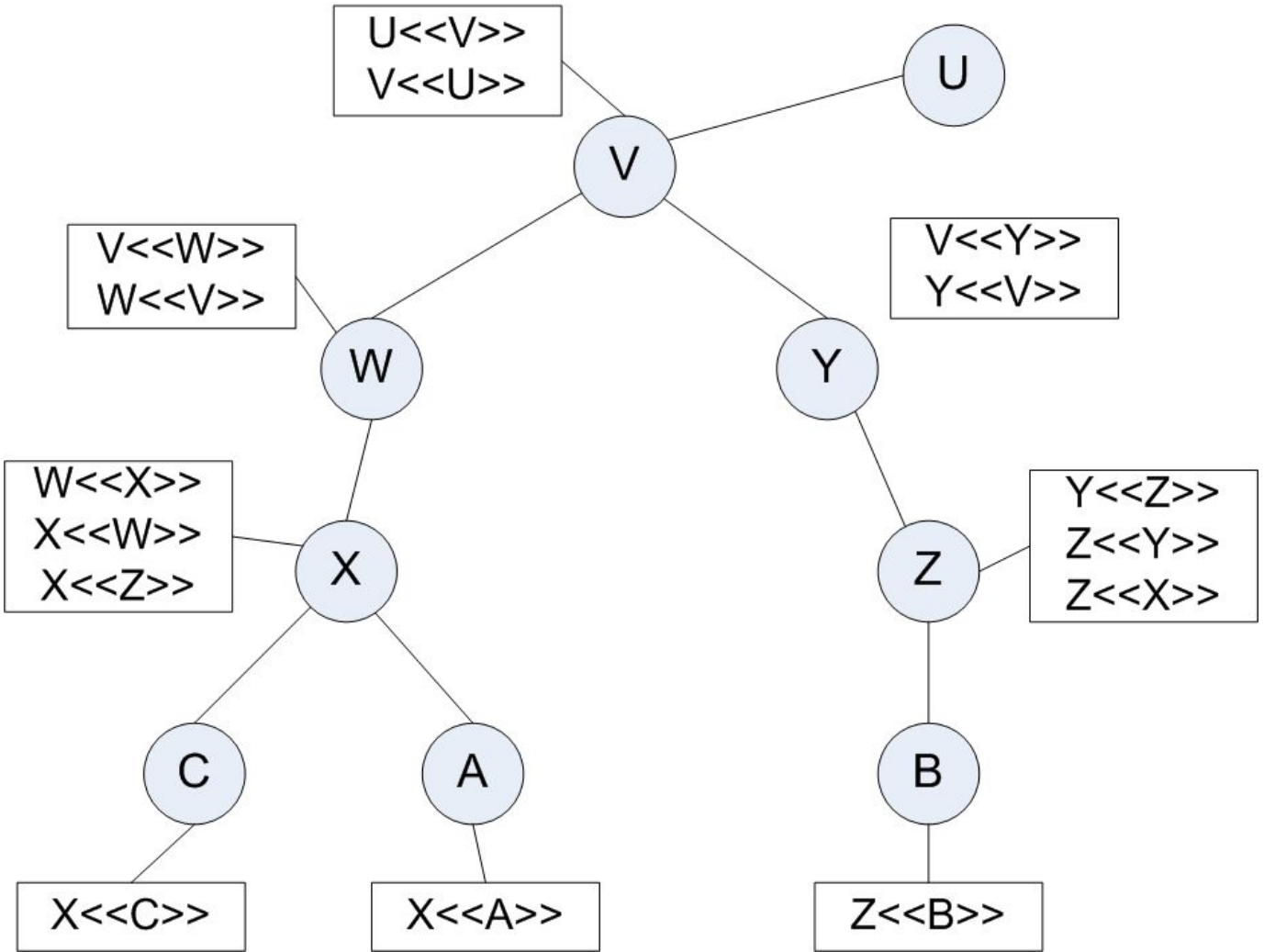
B от A X2 «X1» X1 «A»

X1 «X2» X2 «X3» … XN «B» - цепочка из N элементов

Построение цепочки доверия

X<<W>>W<<V>>V<<Y>>Y<<Z>>Z<<B>> **: от A к B**

Z <<Y>> Y <<V>> V <<W>> W <<X>>X <<A>>**: от B к A**



Прямые, возвратные и самоподписанные сертификаты

- **Прямые сертификаты.** Сертификаты X, выданные другими центрами сертификации.
- **Возвратные сертификаты.** Сертификаты, выданные X для сертификации других центров сертификации.
- **Самоподписанный сертификат.** Открытый ключ для корневой подписи распространяется с автоподписью. Известен всем программным средствам.

Структура иерархической PKI (1)

Имеется главный (корневой) управляющий центр (назовем его УЦ^1). Подлинность открытого ключа УЦ^1 подтверждается соответствующим юридическим документом. УЦ^1 составляет справочники открытых ключей и выдает сертификаты пользователям второго уровня P^2_i и управляющим центрам второго уровня УЦ^2_j. Эти справочники и сертификаты УЦ^1 подписывает своим ключом.

Структура иерархической PKI (2)

Каждый управляющий центр второго уровня обслуживает свою группу пользователей и управляющих центров третьего уровня, подписывая их открытые ключи своим.

В такой системе может быть произвольное количество уровней.

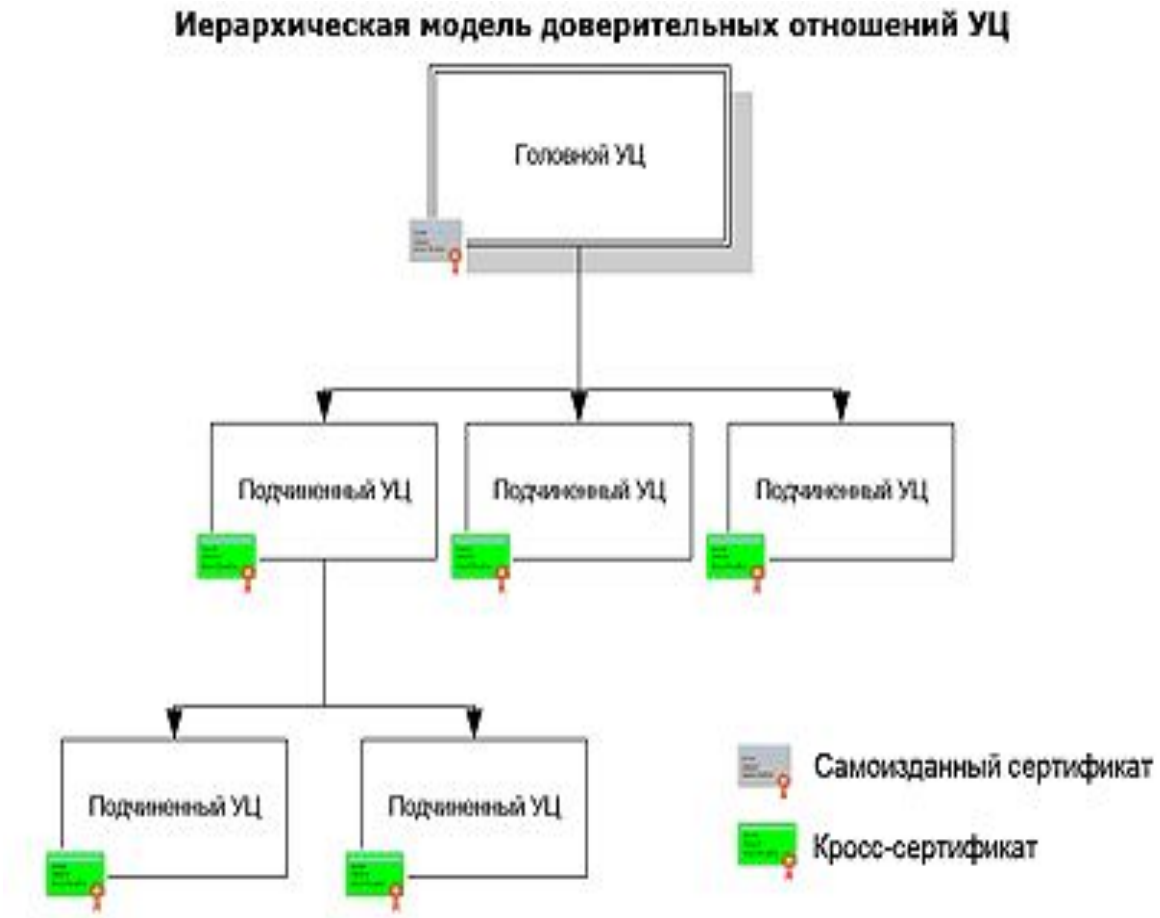
Проверка сертификатов в иерархической PKI (1)

- Для того, чтобы проверить принадлежность открытого ключа пользователя *n*-го уровня, необходимо проверить сертификат, выданный соответствующим УЦ *n*-1-го уровня. Подпись этого УЦ можно проверить по сертификату, выданному УЦ *n*-2 – го уровня, и т. д., а подлинность подписи корневого УЦ гарантируется юридическим документом.

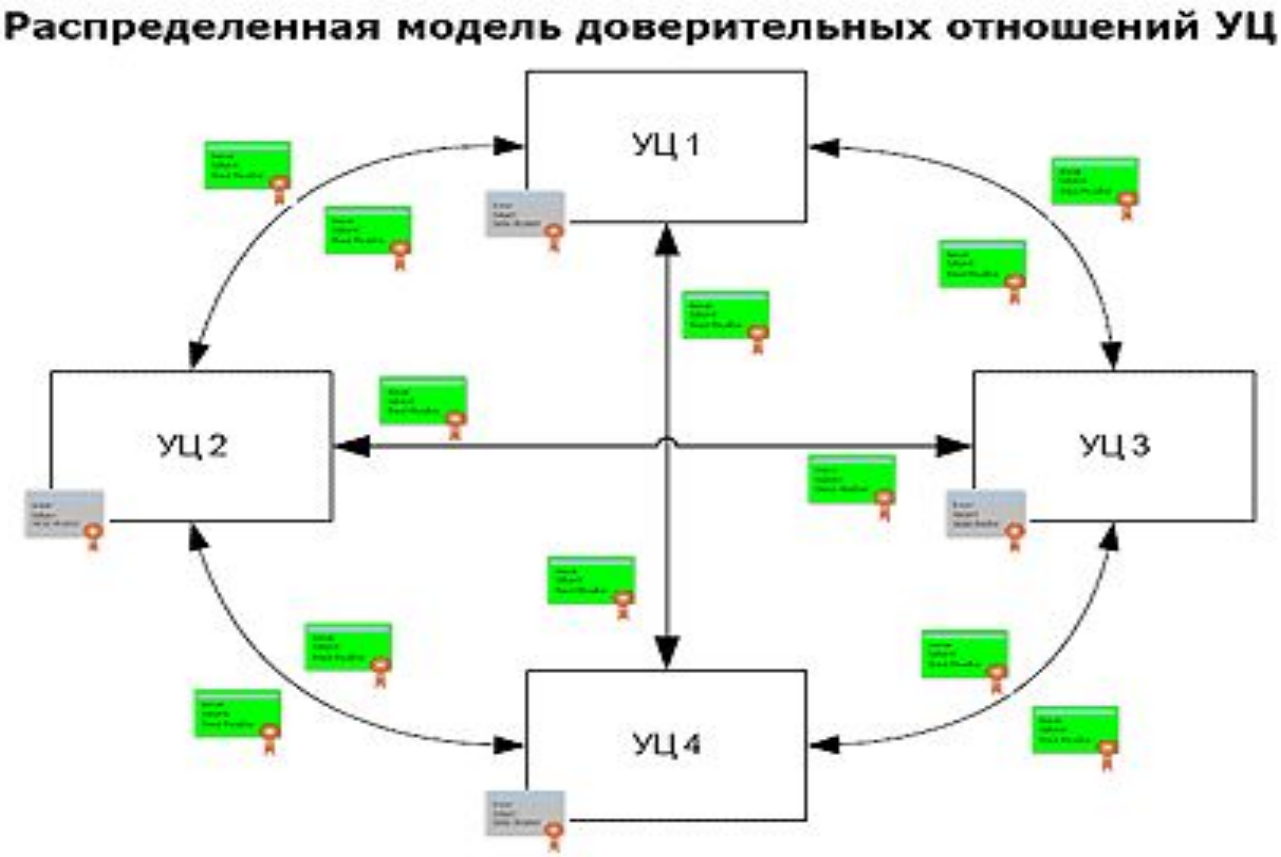
Проверка сертификатов в иерархической PKI (2)

- Для того чтобы все пользователи системы могли проверить подлинность сертификатов друг друга, каждый из УЦ, к которому они принадлежат, распределяет между пользователями подписанный этим УЦ справочник открытых ключей, в котором указаны открытые ключи главного УЦ и всех подчиненных УЦ, через которые проходит путь от данного пользователя к главному УЦ

Иерархическая модель доверительных отношений УЦ



Распределенная модель доверительных отношений УЦ



Кросс-сертификаты

В распределенной модели доверительных отношений, все Центры Сертификации удостоверяющих центров имеют самоизданные сертификаты. Удостоверяющие центры устанавливают между собой доверительные отношения попарно, путем выпуска кросс-сертификатов Центров Сертификации. Таким образом, каждый Центр Сертификации помимо самоизданного сертификата является владельцем кросс-сертификатов, в количестве, равном числу Центров Сертификации, с кем были установлены доверительные отношения.

ViPNet PKI продукты. Серверное ПО (3).

ViPNet Publication Service (Сервис публикации). Осуществляет ведение открытого справочника, куда помещаются выпущенные сертификаты и списки отозванных сертификатов. Публикует выпущенные УЦ сертификаты, кросс-сертификаты и списки отозванных сертификатов в хранилищах, осуществляет загрузку списков отозванных сертификатов внешних УЦ из хранилищ при интеграции в масштабных PKI

ViPNet PKI продукты. Клиентское ПО (1).

ViPNet CryptoService предоставляет пользователю возможность управлять своими криптографическими ключами: генерировать пары открытый-закрытый ключ, записывать ключи в защищенные контейнеры и внешние электронные носители и считывать ключи из них, обновлять сертификаты. Обмен ключевой и служебной информацией с компонентами PKI, созданными на базе ПО ViPNet, полностью автоматизирован и производится криптографически защищенным способом.

ViPNet PKI продукты. Клиентское ПО (2).

ViPNet Client (Клиент) — это программный комплекс для ОС Windows 2000/Windows XP/Vista/Windows 7/Server 2003/Server 2008 (32 бит), ОС Vista/Windows 7/Server 2008/Server 2008 R2 (64 бит), выполняющий на рабочем месте пользователя или сервере с прикладным ПО функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования.

КриптоПро УЦ

- **ПАК «КриптоПро УЦ»** обеспечивает организационно-техническую реализацию Удостоверяющего центра, предоставляя пользователям все необходимые средства и спецификации для использования сертификатов открытых ключей.

КриптоПро УЦ

Предназначен для:

- автоматизации деятельности Удостоверяющего Центра при выполнении им своих целевых функций согласно действующего законодательства РФ;
- автоматизации деятельности по управлению сертификатами открытых ключей, применяемых для шифрования, аутентификации и обеспечения достоверности информации.

Обеспечивает:

- Реализацию инфраструктуры Удостоверяющих Центров, построенных как по иерархической так и по сетевой (распределенной) модели.
- Генерацию ключей подписи и шифрования.
- Выполнение процедуры подтверждения подлинности ЭЦП.
- Ведения реестра зарегистрированных пользователей.
- Приостановление/возобновление действия сертификатов открытых ключей.

Основные составляющие

- **Основные составляющие Удостоверяющего центра на базе «КриптоПро УЦ»:**
- Центр Сертификации «КриптоПро УЦ»;
- Центр Регистрации «КриптоПро УЦ»;
- АРМ пользователя в составе Центра Регистрации;
- АРМ администратора Центра Регистрации;
- АРМ разбора конфликтных ситуаций.

Технические характеристики

- **Создание и проверка электронной цифровой подписи (ЭЦП)**
- ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94
- **Шифрование и имитозащита**
- ГОСТ 28147-89 с использованием СКЗИ «КриптоПро CSP» версии 3.6, СКЗИ «КриптоПро CSP» версии 3.6.1. и ПАКМ «Атликс HSM»
- **Формирование электронных сертификатов открытых ключей**
- x.509v3 (согласно RFC 3280 и RFC 5280 с учётом RFC 4491)

Атликс HSM

- **Атликс HSM** - аппаратный криптографический модуль (hardware security module), совместимый с КриптоПро CSP.
- **Атликс HSM** в первую очередь предназначен для обеспечения безопасного хранения и использования закрытого ключа уполномоченного лица удостоверяющего центра, что обеспечивается выполнением всех криптографических операций, в том числе по генерации ключа уполномоченного лица в криптомодуле. Защита ключа уполномоченного лица удостоверяющего центра обеспечивается в том числе с использованием "раздельных секретов"

Атликс HSM - аппаратный криптографический модуль (hardware security module)

Для активизации закрытого ключа одновременно необходимы три из пяти дополнительных закрытых ключей, хранящихся на процессорных картах РИК (российская интеллектуальная карта). Кроме этого, взаимодействие центра сертификации с криптомодулем возможно только после двусторонней аутентификации

Криптографические алгоритмы, реализуемые криптомодулем Атликс HSM

- генерация ключей, используемых в алгоритмах ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001;
- шифрование/расшифрование данных по ГОСТ 28147-89;
- контроль целостности данных посредством вычисления имитовставки по ГОСТ 28147-89;
- вычисление значения хэш-функции в соответствии с ГОСТ Р 34.11-94;

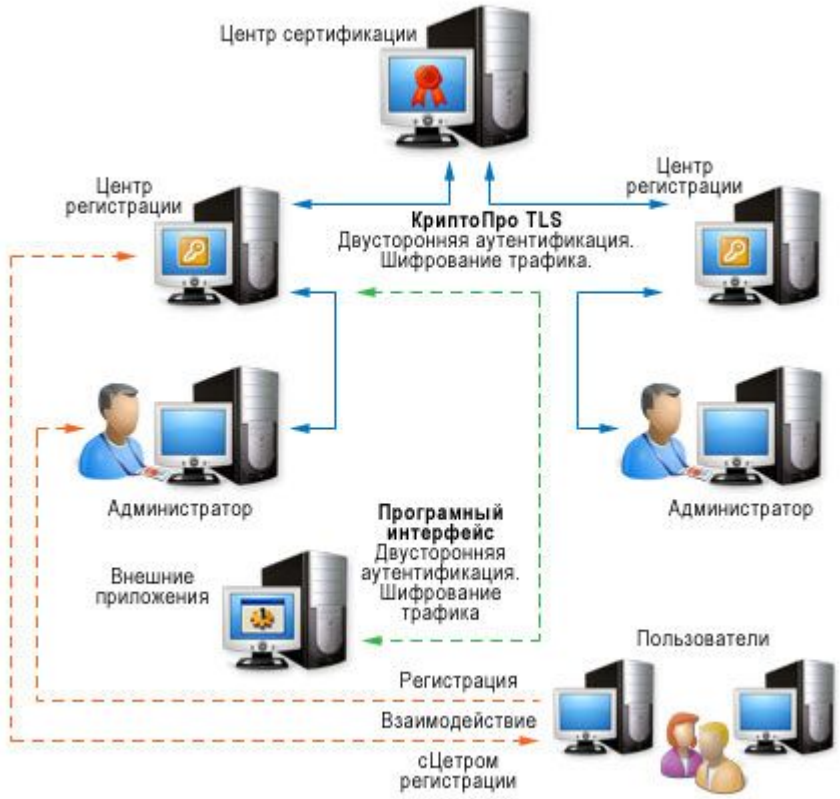
Криптографические алгоритмы, реализуемые криптомодулем Атликс HSM

- вычисление и проверку электронной цифровой подписи (ЭЦП) в соответствии с ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001.
- выработка ключа парной связи по Диффи-Хеллману на базе ключей по алгоритмам ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001.

Сроки действия ключей при использовании криптомодуля Атликс HSM:

- максимальный срок действия закрытых ключей ЭЦП - 5 лет;
- максимальный срок действия открытых ключей ЭЦП при использовании алгоритма ГОСТ Р 34.10-2001 - 30 лет.

Использование PKI



КриптоПро УЦ