Управление ключами в криптографических системах защиты информации

Управление ключами (key management) - совокупность технологий и процедур, посредством которых устанавливаются и поддерживаются отношения криптографической связности между участниками криптографического протокола.

Жизненный цикл ключа - это последовательность состояний, в которых пребывает ключевая информация за время своего существования.

Жизненный цикл ключа

Генерирование ключа

↓

Распределение ключей

↓

Доставка ключа

↓

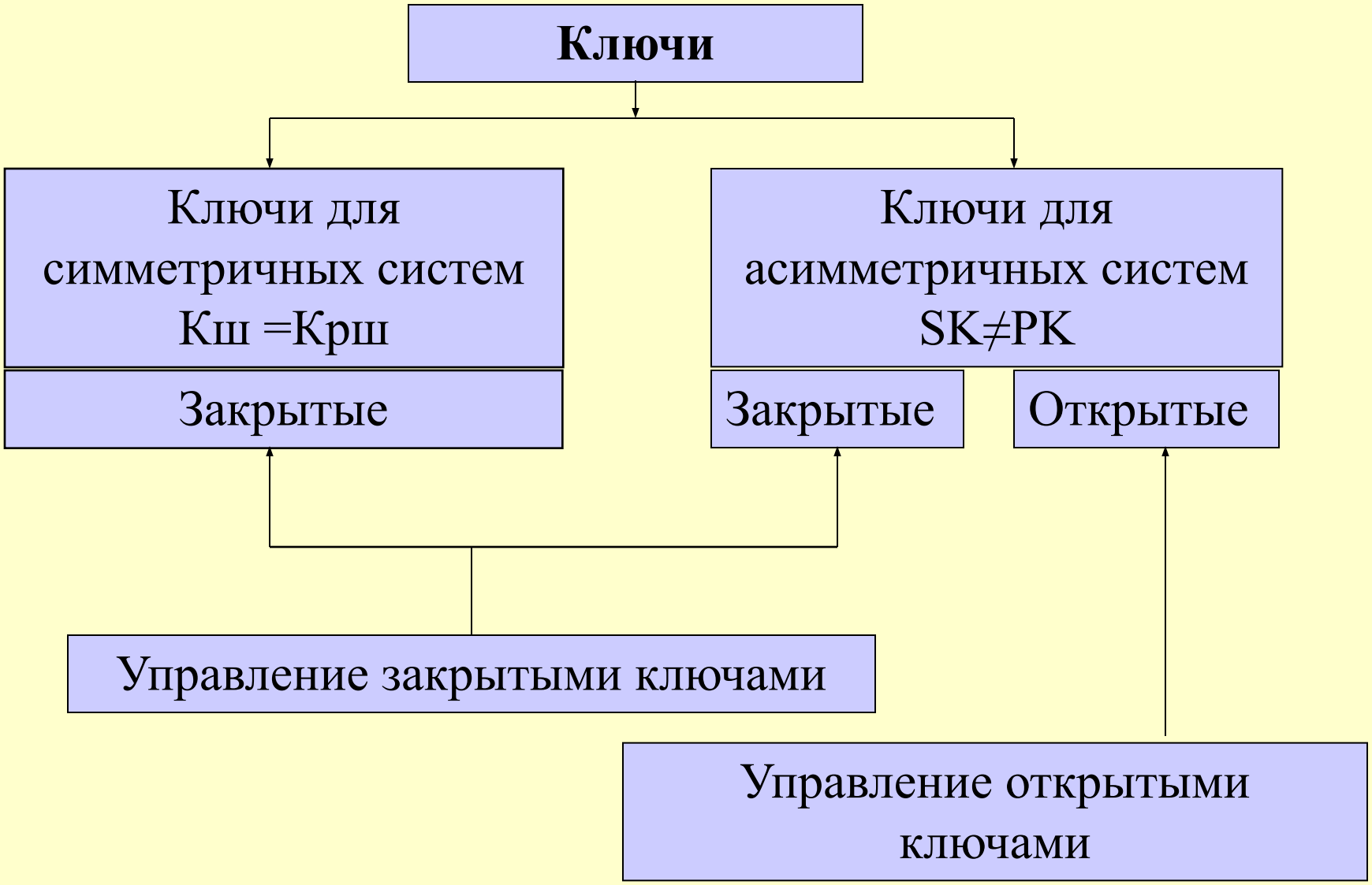
Штатное применение ключа:

- Хранение
- Учет
- Ввод в действие
- Использование в криптоалгоритме
- Копирование
- Архивирование
- Вывод из действия

↓

Уничтожение

Виды управления ключами



Требования к ШК

1. Необходимая длина ключа n;
2. Случайность и равновероятность бит ключа

$$P(K_i)=1/2^n$$

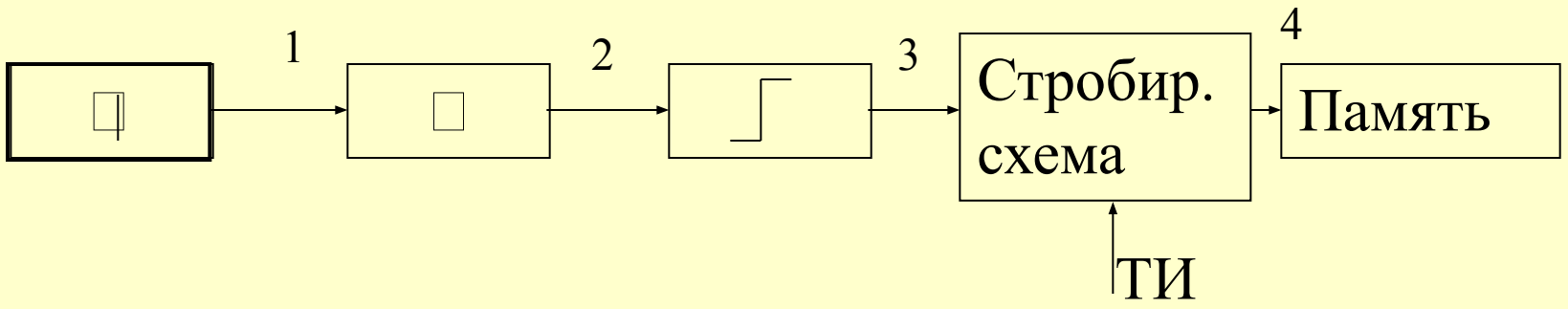
3. Секретность ключа на всех этапах жизненного цикла;
4. Целостность ключа.

Генерирование ключей

1. Программные (конгруэнтные) ДСЧ

2. Биометрические ДСЧ

3. Аппаратные ДСЧ



Программные ДСЧ

Конгруэнтный генератор

$x_{n+1}=(ax_n+b) \bmod m$,

m-модуль, $m > a,b \geq 0$. x_0- начальное заполнение.

Теорема. *Линейная конгруэнтная последовательность имеет период длиной m тогда и только тогда, когда:*

- b и m - взаимно простые числа;

- a-1 кратно p для каждого простого p, являющегося делителем m;

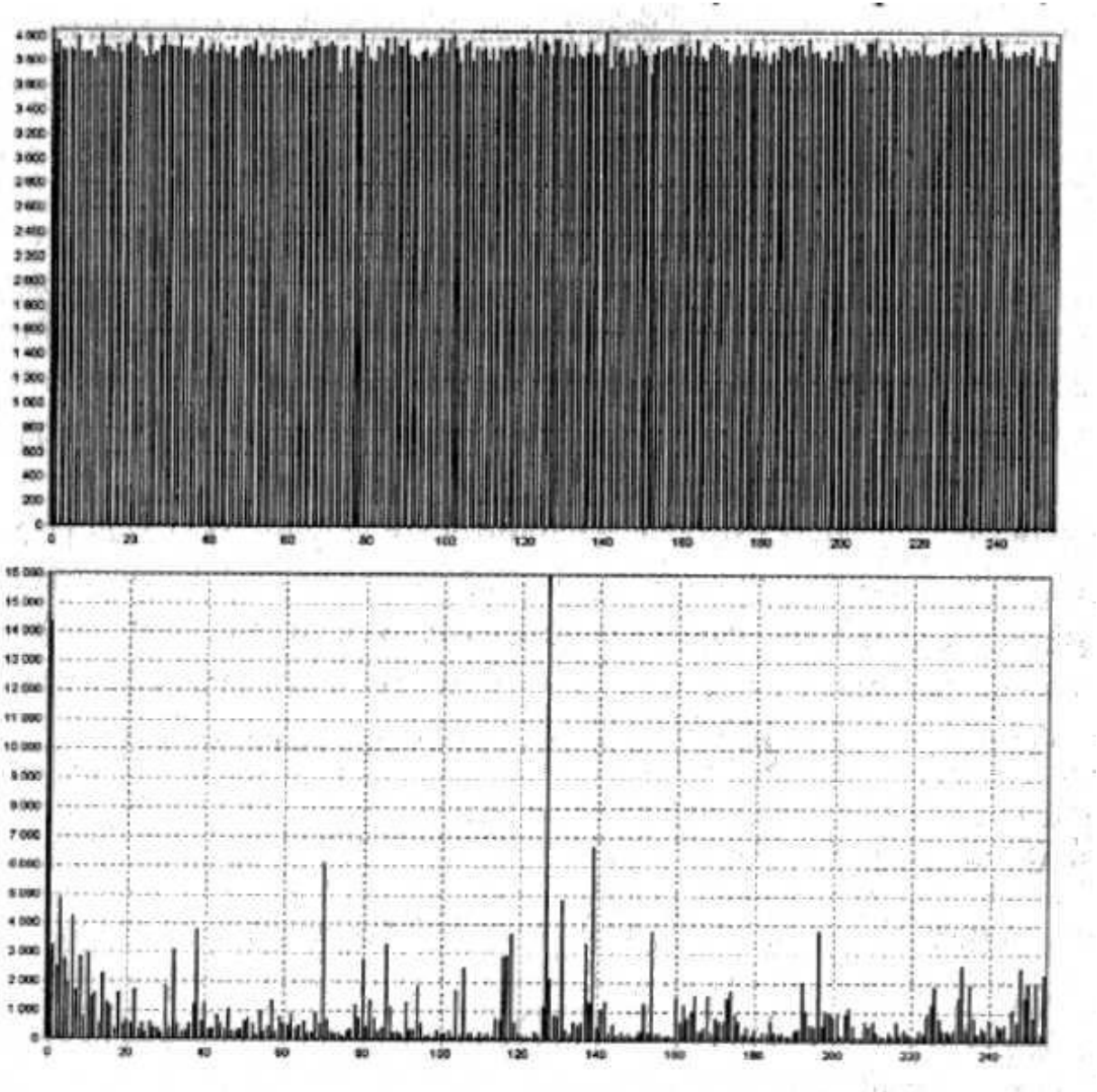
- a-1 кратно 4, если m кратно 4.

Пример: *a=106; b = 1283; m=6075.* $X_{0}=1541$.

Биометрические ГСЧ

Пример из программы PGP:
PGP все время ожидает нажатия клавиш пользователем,
Отразив в 32-битном формате момент, с которого началось ожидание. Когда пользователь нажимает клавишу записывается время нажатия и 8-битовое значение нажатой клавиши.
PGP поддерживает256 байтный буфер случайных чисел.

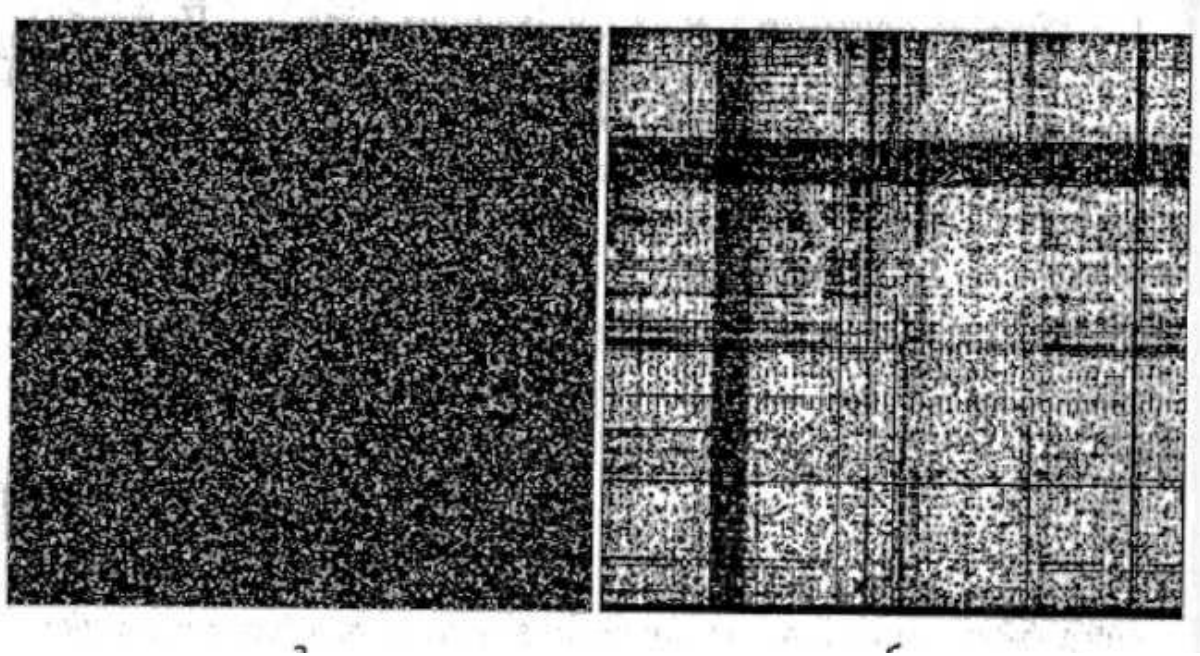
Пример гистограммы распределения элементов последовательности



Пример теста распределения на плоскости

На поле размером $(2^R-1)^*(2^R-1)$, где R- разрядность чисел последовательности, наносятся точки с координатами $(a_i;a_{i+1})$, *где* a_i – элементы последовательности, $i=1,2,\ldots,n$.

Далее анализируется полученная картина. Если на поле присутствуют зависимости, наблюдаются узоры, то последовательность не является случайной.



Хранение ключей

1. Хранение ключей должно исключать доступ к ним посторонних лиц. (Сейф, печать, сигнализация, охрана,…)
2. Ключи, как правило, хранятся в зашифрованном виде:

$К_Х = К_П + ГК$

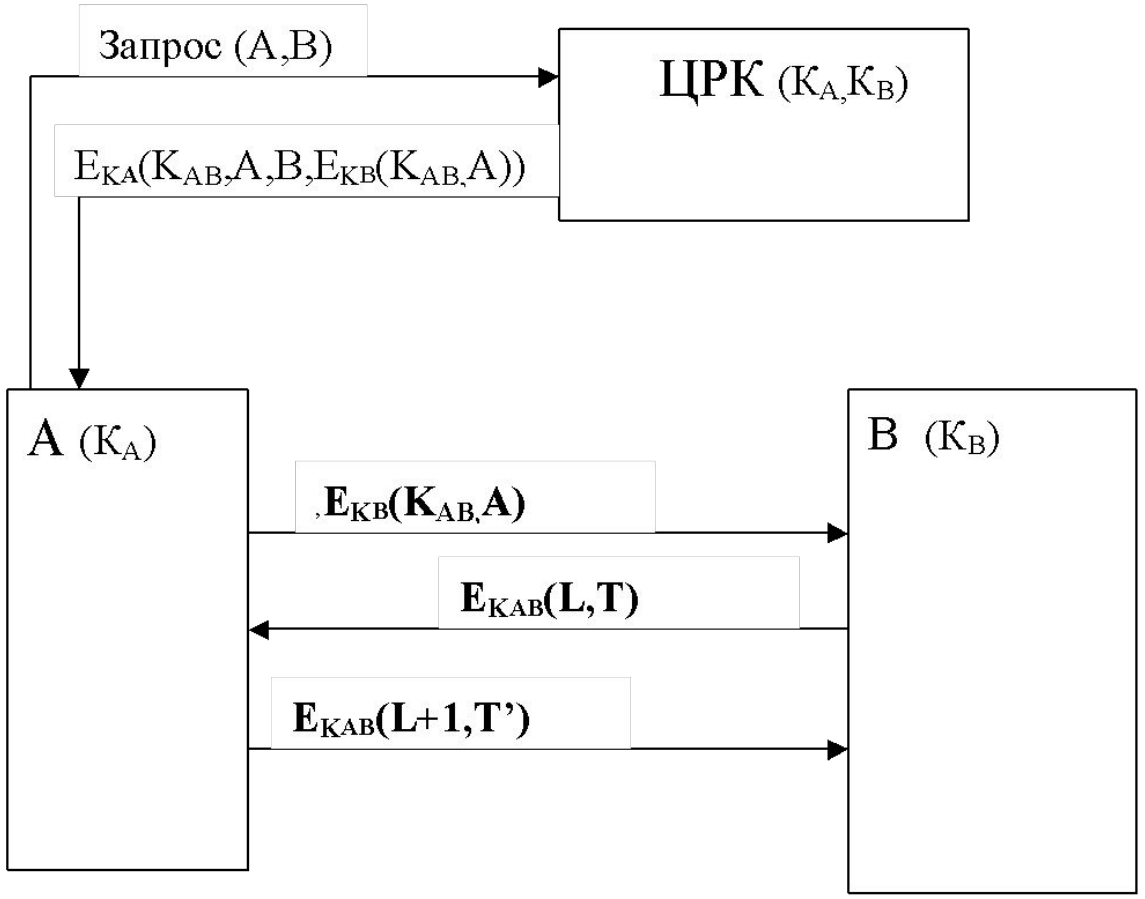
Способы распределения ключей

1. Непосредственный обмен ключами пользователями.
2. Распределение ключей с использованием ЦРК.
3. Распределение ключей с использованием ЦРК на начальном этапе.
4. Распределение ключей с использованием односторонних функции.

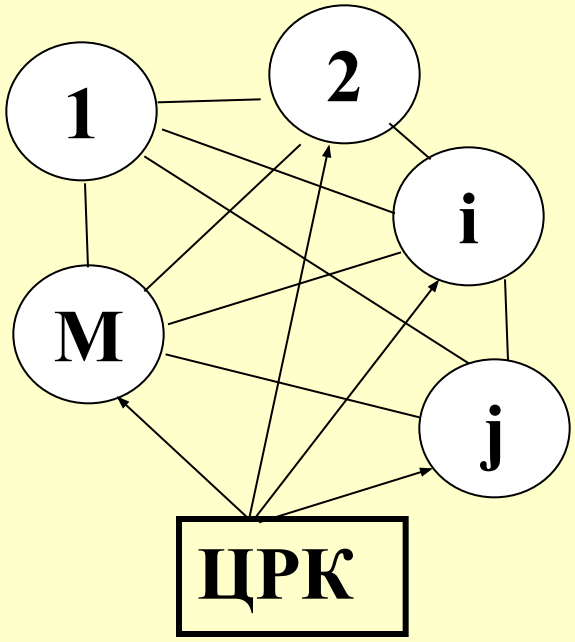
Характеристики способов распределения

- Время распределения ключей
- Объем памяти, необходимый для хранения ключей
- Объем доставляемой ключевой информации
- Устойчивость

Распределение ключей с использованием ЦРК



Распределение ключей с использованием центра распределения ключей на начальном этапе



1 этап. Распределение ключевого материала для формирования сеансовых ключей (ЦРК).
2 этап. Формирование сеансовых ключей (Узлы сети).

Требования

Объем доставляемой на узлы ключевой информации min

Устойчивость к компрометации max

Распределение ключей с использованием ЦРК на начальном этапе

Распределяемый ключевой материал должен представлять собой
некоторую структуру данных (ключевую структуру), определяющую отношения криптографической связности между узлами сети

Табл.1

Структуры ключевого материала

	Тип ключевой структуры	Объем КИ на 1 узел	Объем КИ в сети	Устойчивость
1.	Единый ключ	n	nM	Низкая
2.	Сетевой набор	n(M-1)	nM(M-1)	Высокая
3.	Базовый набор	nL	nLM	Требуемая

Параметры, характеризующие ключевую структуру:

- Время, необходимое для доставки ключевого материала (ключей)
- Объем доставляемой ключевой информации
- Объем памяти, необходимый для хранения ключевой информации
- Устойчивость к компрометациям, создаваемой ключевой структуры

Табл.1

Виды ключевых структур

	Тип ключевой структуры	**Объем КИ на 1 узел**	**Объем КИ в сети**	**Устойчивость**
1.	**Единый ключ**	**n**	**nM**	**Низкая**
2.	**Сетевой набор**	**n(M-1)**	**nM(M-1)**	**Высокая**
3.	**Базовый набор**	**nL**	**nLM**	**Требуемая (t)**

Распределение открытых ключей

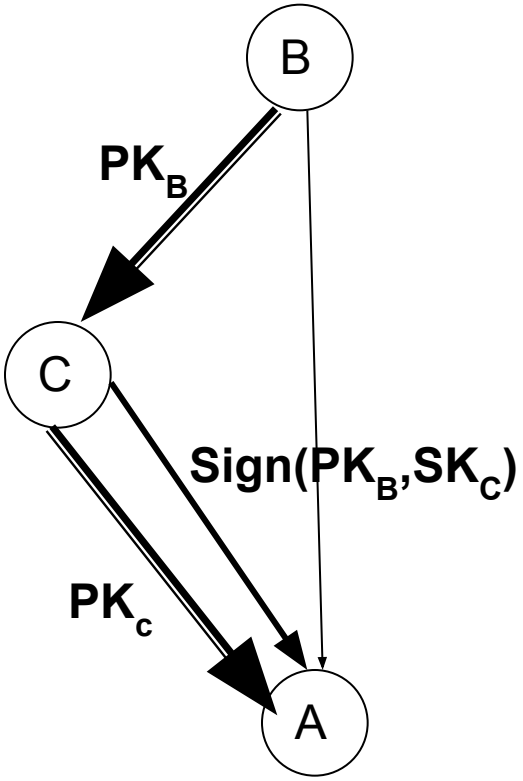
Требования к ключу:

- параметры открытого ключа определяются параметрами закрытого ключа;
-секретность ключа – требования не предъявляются;
-целостность ключа;
-гарантия принадлежности владельцу.

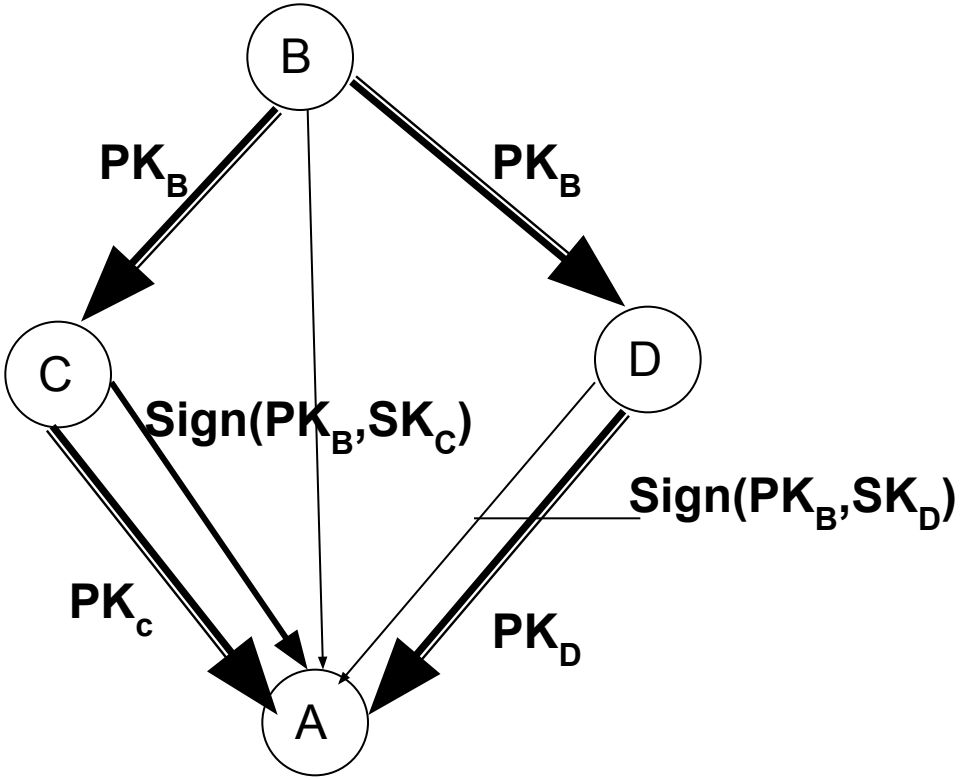
Способы распределения:

- прямой (физический) обмен между корреспондентами;
- по каналу связи с использованием дополнительного канала проверки подлинности;
-использование третьего, четвертого лица и т.д. для подтверждения подлинности (выстраивание доверительных цепочек);
- Использование сертификатов открытых ключей.

Распределение открытых ключей с помощью доверителей

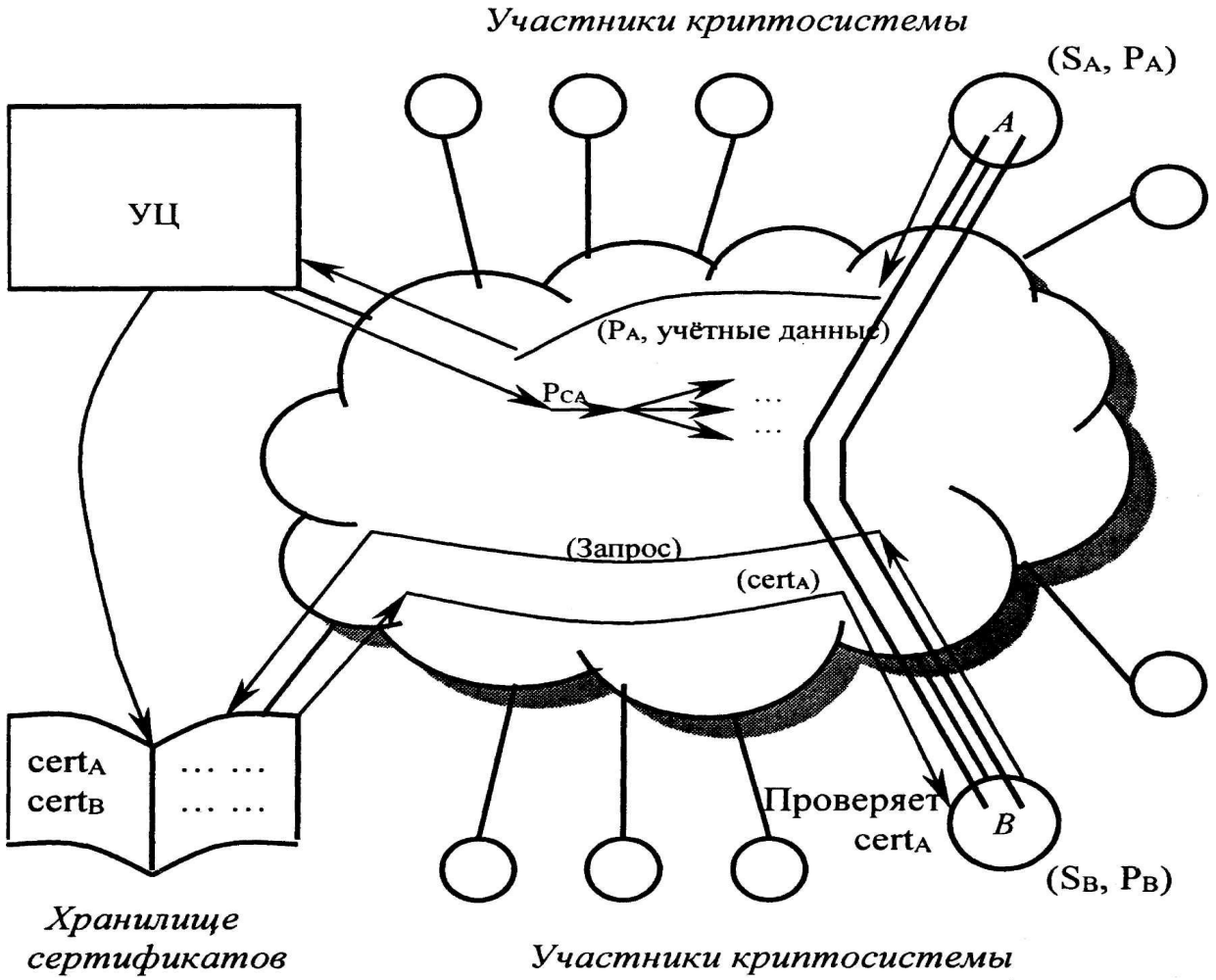


Уровень доверия - полный



Уровень доверия - частичный

Распределение открытых ключей с использованием сертификатов



Инфраструктура открытых ключей
Public Key Infractructure (PKI)

Инфрастуктура открытых ключей - комплексная система, обеспечивающая все необходимые сервисы для использования открытых ключей.

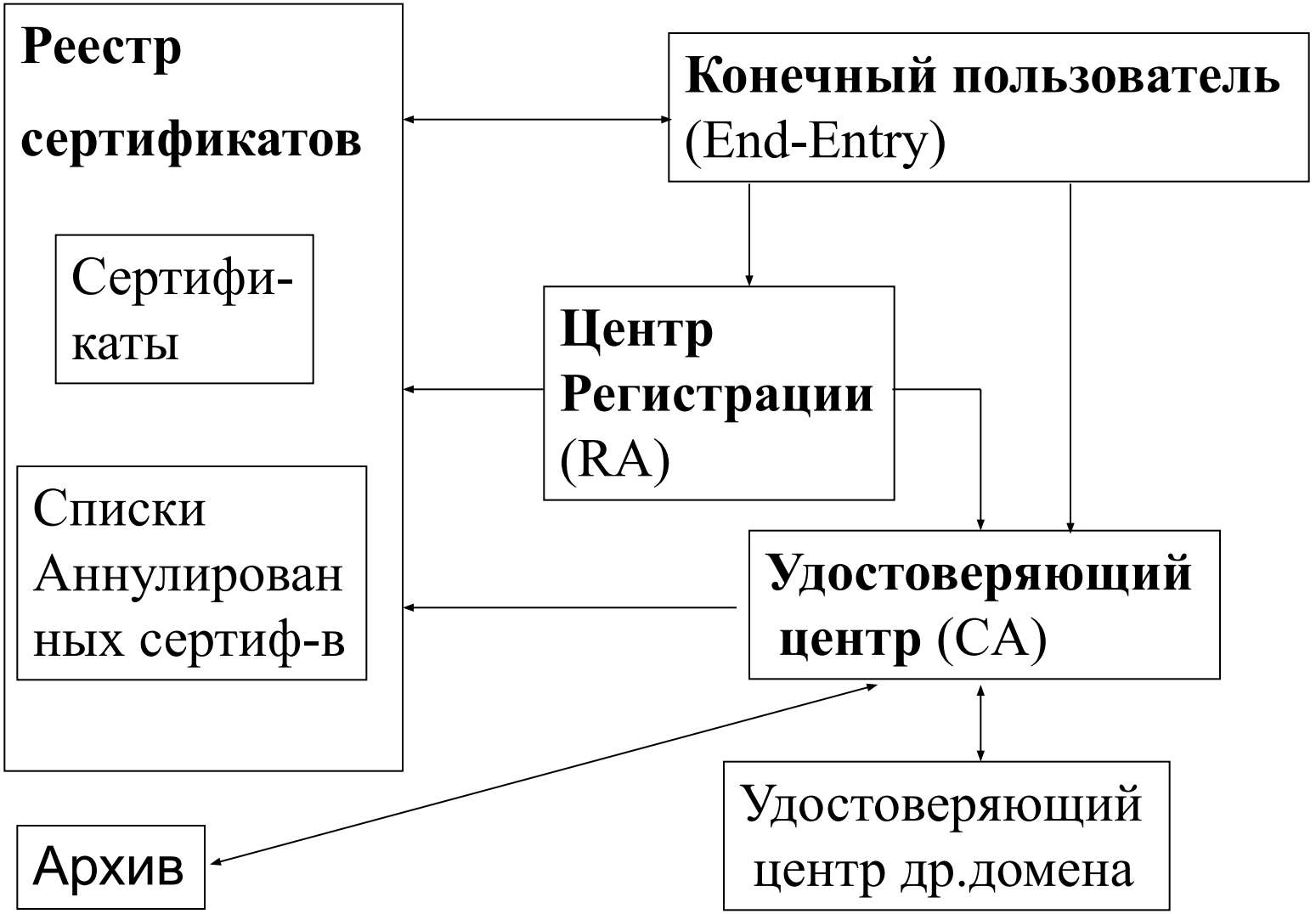
Физически PKI состоит из программ, форматов данных, коммуникационных протоколов, политик и процедур, необходимых для создания, управления, хранения, распространения и аннулирования сертификатов открытых ключей.

PKIX - PKI для формата сертификатов стандарта X.509.

Основные компоненты PKI

-удостоверяющий центр;
-регистрационный центр;
-реестр сертификатов;
-архив сертификатов;
-пользователи.

Архитектура PKIX



Архитектура PKI

Конечный субъект – пользователь, использующий сервисы PKI
Удостоверяющий центр – выпускает сертификаты и управляет ими
Сертификат открытого ключа – специальная структура данных, содержащее признаки владельца, открытый ключ и их подпись УЦ (Виды сертификатов: серт. пользователей, серт. УЦ, кросс-сертификаты – серт. УЦ других доменов безопасности.
Центр регистрации –отвечает за идентификацию субъектов.
Репозитарий сертификатов – хранилище, выпущенных в обращение сертификатов и списков аннулированных сертификатов. Метод доступа в репозитарий протокол LDAP v2.
Списки аннулированных сертификатов – включает серийные номера серт., метки времени, подписи УЦ. Выпускается периодически.
Потоколы: RFC 2510(CMP), RFC 2510, RFC 2559 (LDAP), RFC 2585, RFC 2560(OCSP)

Сервисы PKI

Криптографические сервисы:

-генерация ключей;

-выработка ЭЦП;

-верификация (проверка) ЭЦП;

-шифрование (расшифрование) данных

Сервисы управления сертификатами:

-выпуск сертификата;

-управление жизненным циклом сертификатов ключей;

-поддержка реестра;

-хранение сертификатов и CAC в архиве.

Вспомогательные сервисы:

-регистрация;

-создание резервных копий и восстановление ключей;

-авторизация;

-корректировка ключей и управление историями ключей

Жизненный цикл сертификата

Формат сертификата открытого ключа по стандарту ITU X.509

Образец сертификата

Удостоверяющий Центр ФГУП НИИ "Вектор"-СЦПС "Спектр"
Бланк сертификата открытого ключа

Сведения о сертификате:
Этот сертификат:
Подтверждает удаленному компьютеру идентификацию вашего компьютера
Защищает сообщения электронной почты
Кому выдан:
Петрова Татьяна Вячеславовна
Кем выдан:
SPECTRUDC
Действителен с 16 марта 2007г. 9:09:00 UTC по 16 марта 2008г. 9:18:00 UTC
Версия:3 (0x2)
Серийный номер: 6160 FCCB 0000 0000 0111
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10.-2001
Идентификатор: 1.2.643.2.2.3
Параметры 0500
Издатель сертификата: CN = SPECTRUDC, O = Special Center of Program Systems SPECTR, L = Saint - Petersburg, C = RU, E = udc@spectrudc.ru
Срок действия:
Действителен с: 16 марта 2007 г. 9:09:00 UTC
Действителен по: 16 марта 2008 г. 9:18:00 UTC

Владелец сертификата: CN = Петрова Татьяна Вячеславовна, O = ООО Объединённое Бюро кредитных историй, L = Санкт-Петербург, S = Санкт-Петербург, C = RU, E = petrova@obkl.ru

Открытый ключ:

Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19
Параметры: 3012_0607 2A85 0302 0224 0006 072A 8503 0202 1E01
Значение: 0440 0468 FA69 1CBA D10E 878B F649 DCCB 39A6 9577 2Q92 C419 57E6 8C89 3B88 103D A0B4 6E39 1390 E239 9874 7423 B8C5 6DCA 03OA F1CA F90B C687 2114 9AC3 2CE8 A6C6 32FF

Расширения сертификата X.509

1. Расширение 2.5.29.15 (критическое)

Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость , Шифрование ключей , Шифрование данных(FO)

2. Расширение 2.5.29.37

Название: Улучшенный ключ
Значение: Администратор ОБКИ(1.2.6431)1.1.1) Защищенная электронная почта(1.3.6.1.5.5.7.3.4) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)

3. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта
Значение: 3164 A901 5A85 9A5Ь 188A 0D6F 2617 46C0 8AC3 3A95

Образец сертификата

4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа = B9B9 4A1C 753A D189 A8D6 AF90 902F FB29 D2C5 5416
5. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя:
U RL=http: // www. spectrudc. ru/spectrudc. crt
6. Расширение 1.3.6.1.5.5.7.1.1
Название: Доступ к информации о центрах сертификации
Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя:
URL=http://www.spectrudc;.ru/spectrudc.crt

Подпись Удостоверяющего центра:

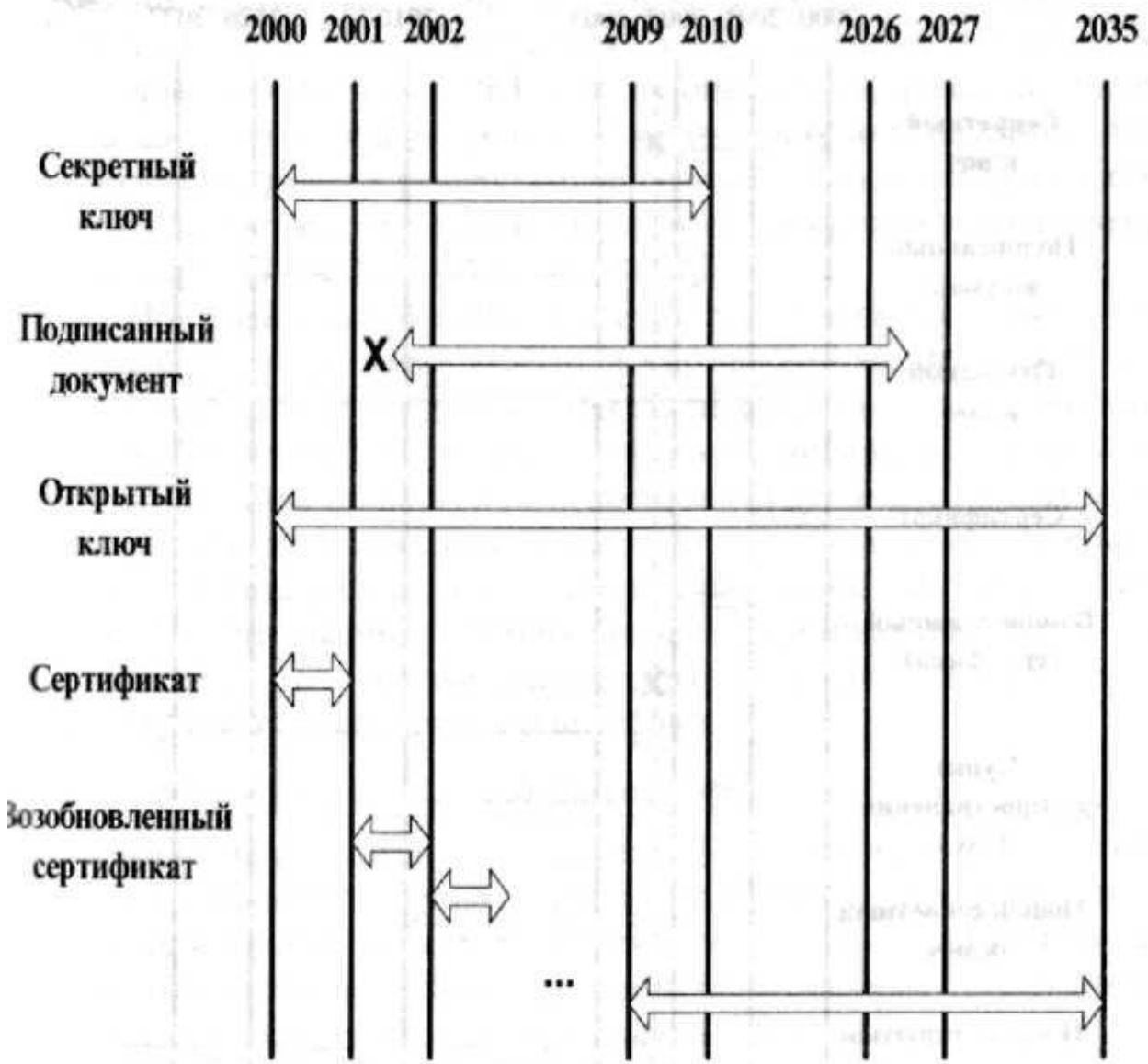
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001 Идентификатор: 1.2.643.2.2.3 Параметры: 0500
Значение: B80A 4D2B 1936 OFDD 28C9 C7F9 3D8A AD22 7E8F FAB6 39BD 3815 DEOC 47FA 72B3 3F8F 263A DA58 2D73 8D97 CB3C A523 E4EF 2826 AFDA C949 763A F38A 5A7D 2FF0 78CA 87A7

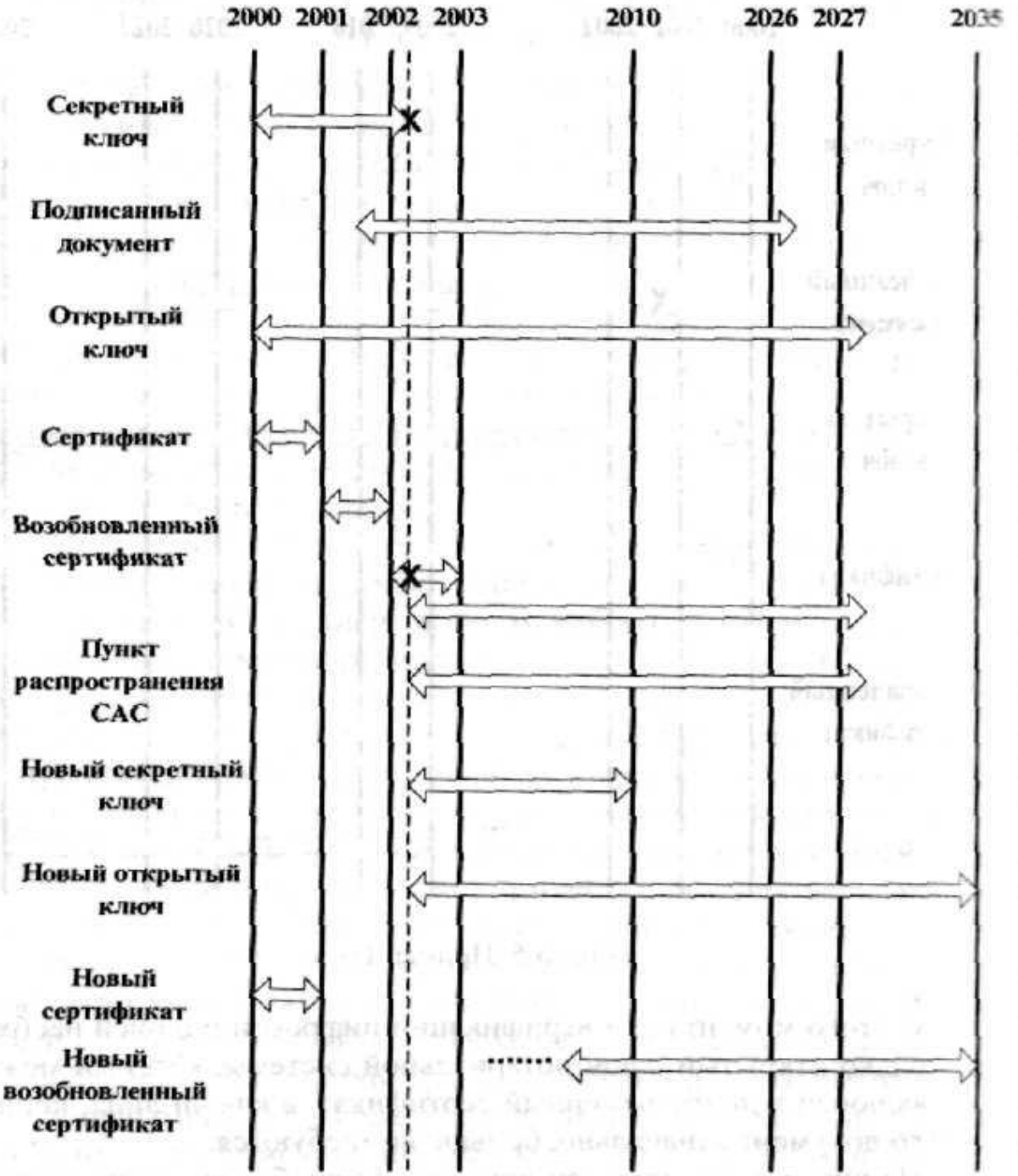
Уполномоченное лицо Удостоверяющего центра
ФГУП НИИ "Вектор"-СЦПС "Спектр": _____/_____
" _____ 20__г.

Примерная политика использования сертификатов

Срок действия сертификата открытого ключа - 1 год;
Срок действия закрытого ключа -10 лет;
Срок действия ЭЦП с момента подписания -25 лет.

Секретный ключ используется для подписания деловых контрактов.


2000
2001
2002
2009
2010
2026
2027
2035
Секретный ключ
Подписанный документ
X
Открытый ключ
Сертификат
Возобновленный сертификат
...


2000
2001
2002
2003
2010
2026
2027
2035
Секретный ключ
Подписанный документ
Открытый ключ
Сертификат
Возобновленный сертификат
Пункт распространения CAC
Новый секретный ключ
Новый открытый ключ
Новый сертификат
Новый возобновленный сертификат

Программные средства поддержки PKI

Программные обеспечение PKI мировых производителей

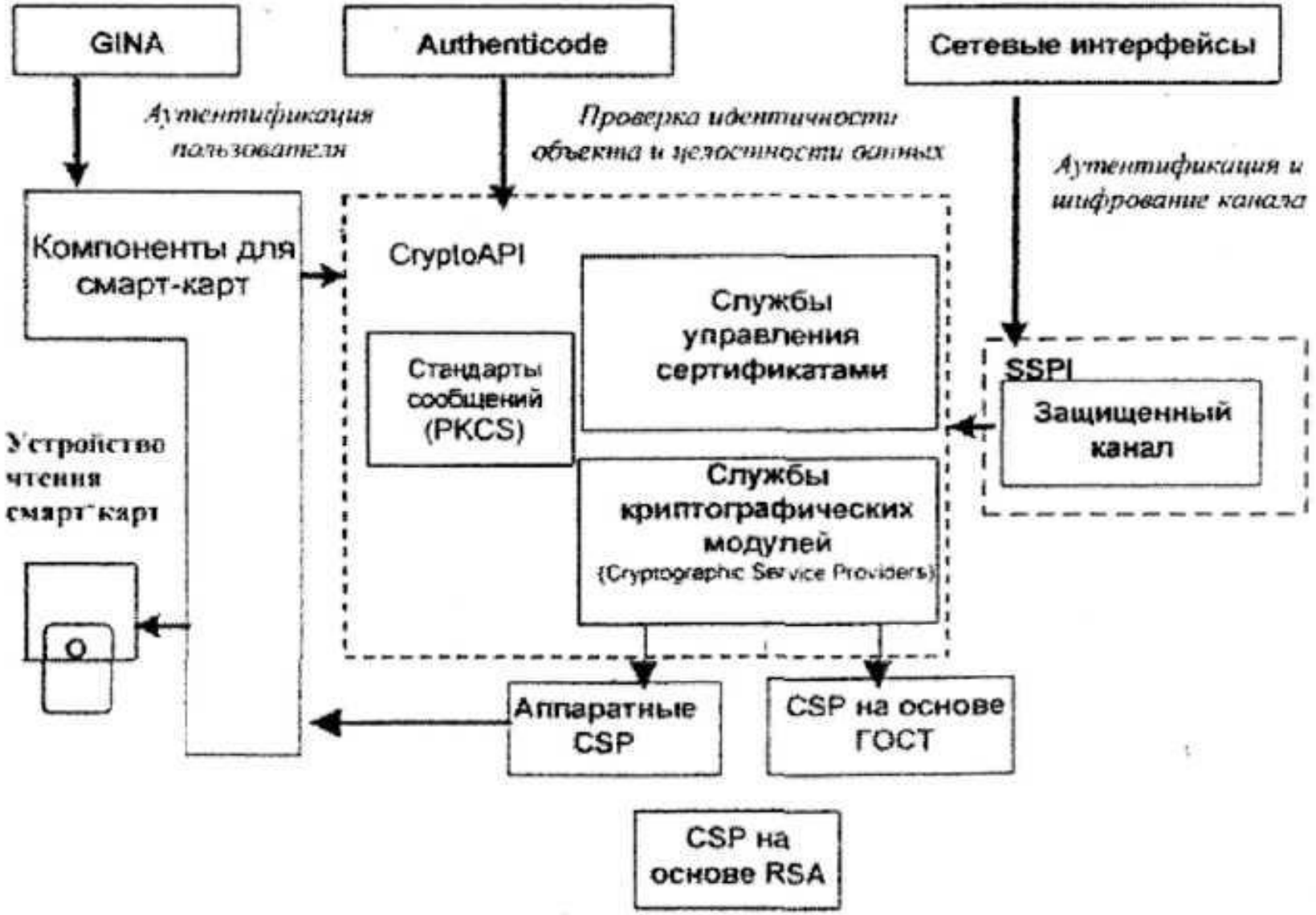
- Entrust/PKI 5.0
- Baltimore UniCERT 5.0
- BT TrustWise`Onsite 4.5
- IBM Trust Authority 3.1
- RSA Kenon certification Authority 6.5

PKI, интегрированные в операционные системы:
Novell: Public key Infrastructure Services (PKIS)
Microsoft: Microsoft Certificate Services

Программное обеспечение PKI российских компаний:

- Программный комплекс VCERT PKI;
- Средство криптографической защиты КриптоПро CSP;
- Программный комплекс «Вепрь»

Служба управления сертификатами в Windows 2000/XP поддержка криптографических приложений



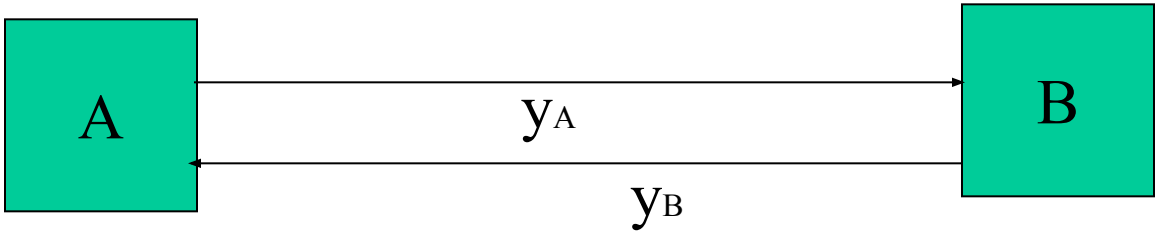
Применение сертификатов в Win/XP

1. Защищенная электронная почта:
-ЭП электронных документов;
-Шифрование данных.
2. Безопасное сетевое взаимодействие:
-Проверка подлинности сервера;
-Проверка подлинности клиента.
3. Осуществление VPN соединений (протокол IPSec).
4. ЭП программных компонент и их прверка (модуль Authenicode).
5.Шифрующая файловая система (EFS).
6. Аутентификация пользователей с помощью смарт-карт.

Иерархия центров сертификации


Центр сертификации
КриптоПро TLS
Двусторонняя аутентификация
Шифрование трафика
Центр регистрации
Центр регистрации
Администратор
Администратор
Программный интерфейс
Двусторонняя аутентификация
Шифрование трафика
Регистрация
Взаимодействие с Центром Регистрации
Внешние приложения
Пользователи

Система распределения ключей Диффи-Хеллмана



A генерирует большое случайное число x_A, $1 \le x_A \le p-1$, p - **простое число.**

x_A **сохраняется в секрете.** **вычисляет** $y_A = \alpha^{x_A} (\mathrm{mod}\ p)$.

B: генерирует x_B, **вычисляет число** y_B.

A, приняв от B y_B, **вычисляет**

$$K_A = (y_B)^{x_A} \bmod p = (\alpha^{x_B})^{x_A} \bmod p = \alpha^{x_B x_A} \bmod p.$$

B, приняв от A y_A, **вычисляет**

$$K_B = (y_A)^{x_B} \bmod p = (\alpha^{x_A})^{x_B} \bmod p = \alpha^{x_A x_B} \bmod p.$$

Видим, что $K_A = K_B = K$.

Далее ключ K **может быть использован в симметричной системе шифрования.**