Федеральное государственное автономное образовательное учреждение высшего образования
Национальный исследовательский ядерный университет «МИФИ»

Кафедра «Криптология и кибербезопасность»

Криптографические протоколы

курс лекций

Запечников Сергей Владимирович,
профессор кафедры «Криптология
и кибербезопасность» НИЯУ МИФИ

Москва – 2018

Криптографические протоколы

курс лекций

Лекция 3.
Протоколы аутентификации (окончание).
Управление ключами

22 февраля 2018 г.

Протоколы аутентификации, основанные на доказательствах с нулевым разглашением

Общая идея протоколов аутентификации, основанных на доказательствах с нулевым разглашением, состоит в том, что законный пользователь *P*, имеющий открытый и секретный ключи, и проверяющий *V* выполняют совместный криптографический протокол интерактивного доказательства, в процессе которого *P*, выступающий в роли претендента, должен доказать свою подлинность. Для этого он должен продемонстрировать знание секретного ключа, но не разгласить его для проверяющего *V*, т.е. из информации, полученной *V*, ему вычислительно невозможно получить секретный ключ *P*.

Все протоколы имеют два этапа: *предварительный* и *рабочий*. На предварительном, который выполняется однократно, специфицируются некоторые параметры и вырабатываются величины, участвующие в рабочем этапе протокола, в частности, открытые и секретные ключи *P*. На рабочем этапе собственно выполняется доказательство аутентичности *P*.

Протокол аутентификации Фиата – Шамира

<table>
<tr><th colspan="4">Предварительный этап</th></tr>
<tr><th colspan="2">P</th><th>Центр доверия</th><th>V</th></tr>
<tr><td colspan="2">s: $(s,n)=1,\ 1\le s\le n-1$
$v=s^2 \pmod n$</td><td>p, q – большие простые числа, $n=pq$</td><td></td></tr>
<tr><td colspan="4">n, v</td></tr>
<tr><th colspan="4">Рабочий этап</th></tr>
<tr><th></th><th>P</th><th></th><th>V</th></tr>
<tr><td>1</td><td>$r\in_R \{1,2,\ldots,n-1\}$
$x=r^2 \pmod n$</td><td>$\rightarrow$</td><td></td></tr>
<tr><td>2</td><td></td><td>$\leftarrow$</td><td>$e\in_R \{0,1\}$</td></tr>
<tr><td>3</td><td>$y=rs^e \pmod n$</td><td>$\rightarrow$</td><td></td></tr>
<tr><td>4</td><td></td><td></td><td>Если (y=0), отклоняет доказательство, так как r=0. В противном случае:
$y^2 \stackrel{?}{\equiv} xv^e \pmod n$</td></tr>
</table>

Стойкость протокола

Рассмотрим подробнее структуру этого протокола. Запрос *e* на шаге (2) требует, чтобы *P* был способен ответить на два вопроса: один из них нужен для того, чтобы продемонстрировать знание *s* и, тем самым, предотвратить обман честного проверяющего нечестным претендентом, другой – чтобы предотвратить обман честного претендента нечестным проверяющим. Соответственно запросу претендент отвечает на шаге (3) либо *y=r*, либо $x = rs \pmod n$. Ни тот, ни другой ответ не несет никакой информации об *s*: в первом случае он от *s* вообще не зависит, во втором – замаскирован случайной величиной *r*, которая известна только *P*, так как на шаге (1) тоже была замаскирована при помощи ОНФ.

Противник, пытающийся деперсонифицировать *P*, может стремиться обмануть проверяющего, выбрав произвольное *r*, вычислив $x = \frac{r^2}{v} \pmod n$ и ответив *y=r* при *e=1*, но не сможет ответить при *e=0*, так как это требует знания $\sqrt{x} \pmod n$.

Противник, выступающий в роли проверяющего, может смоделировать пары сообщений *(x,y)* самостоятельно. Действительно, можно выбирать случайные *y*, задаваться случайными битами *e={0/1}* и вычислять в зависимости от этого $x = y^2 \pmod n$ либо $x = \frac{y^2}{v} \pmod n$.

Распределение вероятностей пар *(x,y)* не будет отличаться от распределения вероятностей тех величин, что сгенерировал бы *P* в реальном протоколе. Таким образом, протокол действительно обладает свойством нулевого разглашения.

Протокол аутентификации Файге – Фиата – Шамира

Предварительный этап		
P	***Центр доверия***	***V***
s_i: $(s_i, n) = 1$, $1 \le s \le n-1$ $v_i = s_i^2 \pmod n$ $v = (v_1, v_2, ..., v_k)$ $s = (s_1, s_2, ..., s_k)$	p, q – большие простые числа, $n = pq$	
n, v_1, v_2, ... , v_k		

Рабочий этап			
	P		***V***
	for (i=1,2, ... ,t)		
1	$r_i \in_R \{1,2,...,n-1\}$, $x_i = r_i^2 \pmod n$	$\rightarrow$	
2		$\leftarrow$	$(e_{i1}, e_{i2}, ..., e_{ik}) \in_R \{0,1\}^k$
3	$y_i = r_i \left(s_1^{e_{i1}} s_2^{e_{i2}} ... s_k^{e_{ik}}\right) \pmod n$	$\rightarrow$	
4			$x_i \overset{?}{=} y_i^2 \left(v_1^{e_{i1}} v_2^{e_{i2}} ... v_k^{e_{ik}}\right) \pmod n$

Протокол аутентификации Гиллу - Кискатра (Guillou – Quisquater)

<table>
<tr><th colspan="4">Предварительный этап</th></tr>
<tr><th>P</th><th colspan="2">Центр доверия</th><th>V</th></tr>
<tr><td>I_P, B, J</td><td colspan="2">p, q — простые числа, $n=pq$,
I_P, $J = H(I_P)$,
$JB^v \equiv 1 \pmod n$</td><td></td></tr>
<tr><td colspan="4">n, J</td></tr>
<tr><th colspan="4">Рабочий этап</th></tr>
<tr><td></td><th>P</th><td></td><th>V</th></tr>
<tr><td>1</td><td>$r \in_R (1; n-1)$
$T = r^v \pmod n$</td><td>$\rightarrow$</td><td></td></tr>
<tr><td>2</td><td></td><td>$\leftarrow$</td><td>$d \in_R (0; v-1)$</td></tr>
<tr><td>3</td><td>$D = rB^d \pmod n$</td><td>$\rightarrow$</td><td></td></tr>
<tr><td>4</td><td></td><td></td><td>$T' = D^v J^d \bmod n$
$T \overset{?}{\equiv} T' \pmod n$</td></tr>
</table>

Протокол аутентификации Шнорра

<table>
<tr><th colspan="4">Предварительный этап</th></tr>
<tr><th colspan="2">P</th><th>Центр доверия</th><th>V</th></tr>
<tr><td colspan="2">$s \in_R \{1,\ldots,q-1\}$
$v = a^s \bmod p$</td><td>p, q — простые числа, $q \mid p-1$,
$a \in Z_p : a^q \equiv 1 (\bmod p)$</td><td></td></tr>
<tr><td colspan="4">p, q, a, v</td></tr>
<tr><th colspan="4">Рабочий этап</th></tr>
<tr><th></th><th>P</th><th></th><th>V</th></tr>
<tr><td>1</td><td>$r \in_R \{1,\ldots,q-1\}$
$x = a^r \bmod p$</td><td>$\rightarrow$</td><td></td></tr>
<tr><td>2</td><td></td><td>$\leftarrow$</td><td>$e \in_R \{0,\ldots,2^{t-1}\}$</td></tr>
<tr><td>3</td><td>$y = r + se (\bmod q)$</td><td>$\rightarrow$</td><td></td></tr>
<tr><td>4</td><td></td><td></td><td>$x \overset{?}{=} a^y v^e \bmod p$</td></tr>
</table>

Протокол аутентификации Брикелла – МакКарли

Предварительный этап		
P	***Центр доверия***	***V***
$s < p$ – секр. ключ v: $v = a^{-s} \pmod p$	p, q, w – простые числа, $qw \mid p-1; q^2 \nmid p-1; q, w \geq 2^k$ $a: a^q \equiv 1 \pmod p$	
p, a, v		

Рабочий этап			
	P		*V*
1	$r \in_R \{1,\ldots, p-1\}$ $x = a^r \pmod p$	$\rightarrow$	
2		$\leftarrow$	$e \in_R \{0,\ldots,2^t\}$
3	$y = r + se \pmod{p-1}$	$\rightarrow$	
4			$x \overset{?}{=} a^y v^e \bmod p$

Управление ключами систем криптографической защиты информации

Понятие управления криптографическими ключами

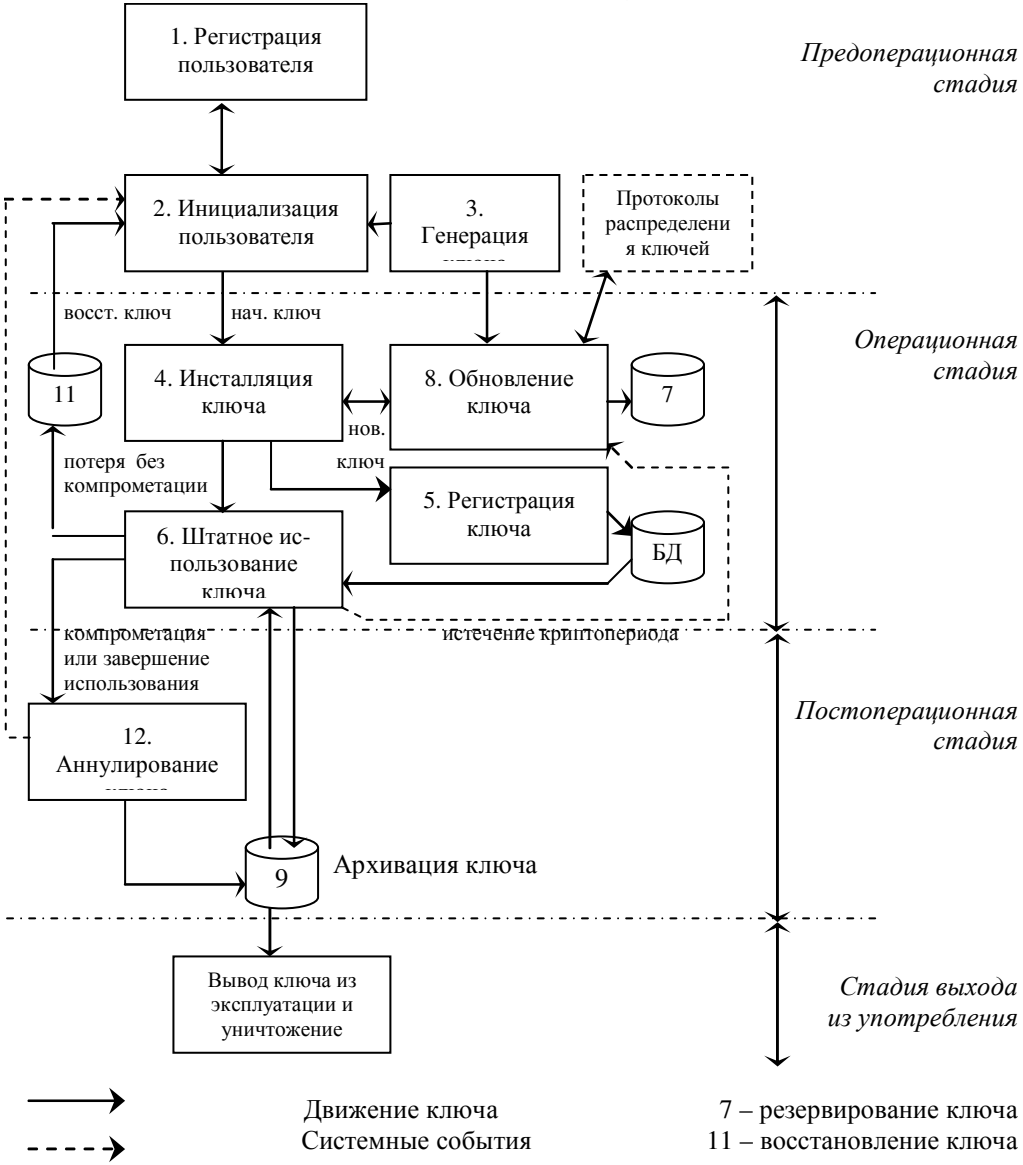
Основной международный стандарт – ISO/IEC 11770 – Key management :

- **Управление ключами - совокупность процедур и процессов, сопровождающих жизненный цикл ключей в криптосистеме.**
- **Жизненный цикл – последовательность состояний, в которых пребывает ключевой материал за время своего существования в криптосистеме:**
  - ✓ генерация
  - ✓ распространение
  - ✓ хранение
  - ✓ уничтожение и др.

Цель управления ключами – обеспечение безопасности криптографических ключей на всех этапах жизненного цикла → безопасности всей криптосистемы:

- **Секретные ключи → необходимо обеспечить секретность, подлинность, целостность:**
  - ✓ Общие секретные ключи симметричных криптосистем;
  - ✓ Частные секретные ключи асимметричных криптосистем (закрытые ключи).
- **Открытые ключи → необходимо обеспечить подлинность, целостность:**
  - ✓ Открытые ключи асимметричных криптосистем, помещаемые в общедоступные справочники.

Схема жизненного цикла ключей



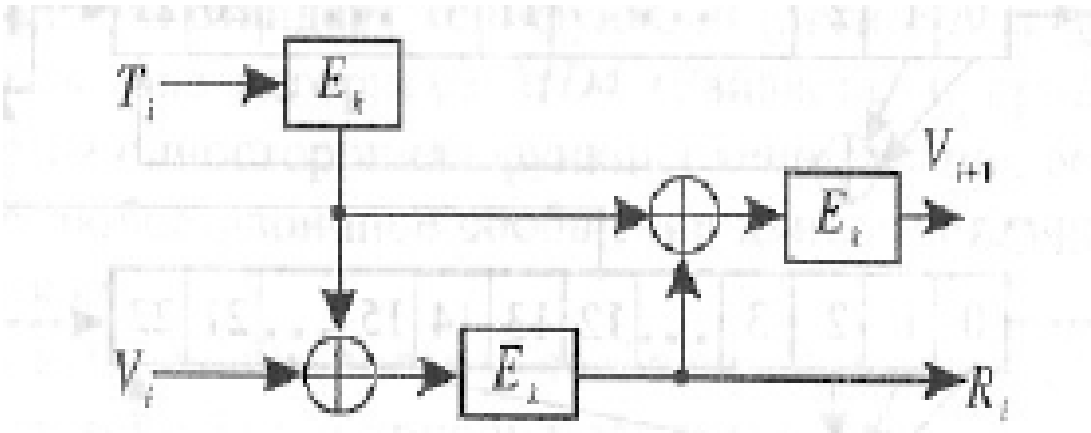
Фазы жизненного цикла ключей (1)

1. Генерация ключей:

Главная цель – сделать ключи максимально случайными, непредсказуемыми для противника:

- **Датчики случайных чисел → физические случайные величины преобразуются в цифровой вид.**
- **Генераторы псевдослучайных чисел (последовательностей) → числа вырабатываются программами по заранее заданным алгоритмам, они предсказуемы, но по своим статистическим качествам очень похожи на случайные.**

***Пример*: алгоритм генерации ключей по стандарту ANSI X9.17:**



Фазы жизненного цикла ключей (2)

2. Распространение ключей:

Транспортировка - самый опасный этап !

- **Для секретных ключей симметричных криптосистем главная цель – предотвратить попадание ключи к посторонним лицам → традиционные меры физической защиты, усиленные аппаратными и организационными мерами.**
- **Для открытых ключей главная цель – обеспечить подлинность и целостность → сложная задача, которая решается созданием Инфраструктуры открытых ключей !**
- **Инфраструктура открытых ключей (ИОК) (соотв. англ. PKI – Public Key Infrastructure) – универсальная модель организованной поддержки криптографических средств защиты информации в крупномасштабных компьютерных системах в соответствии с принятыми в них политиками безопасности, которая реализует управление криптографическими ключами на всех этапах их жизненного цикла, обеспечивая взаимодействие всех средств защиты.**

Для справки:

Инфраструктура - составные части общего устройства системы, носящие вспомогательный, подчинённый характер и обеспечивающие нормальную деятельность системы в целом.

Фазы жизненного цикла ключей (3)

3. Хранение ключей:

Главная цель – предотвращение несанкционированного доступа, обеспечение аутентичности ключей

→ Технические средства:

- **токены,**
- **смарт-карты (микропроцессорные пластиковые карты)**

– одни из самых удобных и перспективных средств:

- ✓ портативность;
- ✓ аппаратная реализация криптографических алгоритмов;
- ✓ весь ЖЦ ключи изолированы внутри физически защищённой микросхемы;
- ✓ существуют критерии оценки защищенности криптографических модулей (американский стандарт FIPS 140-3).

4. Уничтожение ключей:

Главная цель – исключить возможность попадания к посторонним лицам ранее использовавшихся ключей. → Криптографические ключи нельзя просто вывести из употребления – необходимо физически уничтожить все копии ключей из памяти аппаратных средств криптографической защиты.

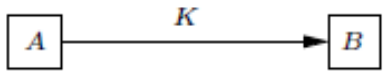
Ключевые системы симметричных криптосистем (1)

Децентрализованное и частично централизованное управление ключами

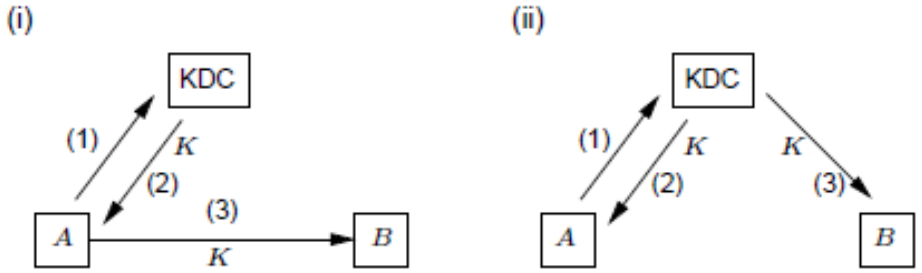
1. **Полная ключевая матрица**
2. **Один общий секретный ключ для группы участников.**
3. **Комбинированная модель (банковские карты и POS-терминалы»).**

Централизованное управление ключами

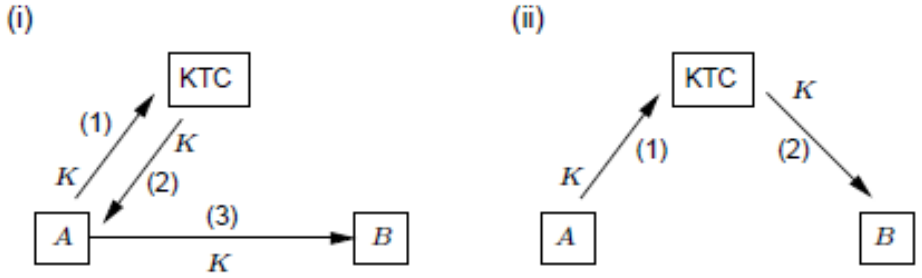
(a) Point-to-point key distribution



(b) Key distribution center (KDC)



(c) Key translation center (KTC)



Ключевые системы симметричных криптосистем (2)

Принципы функционального разделения ключей:

1.1. **Принцип целевого использования ключей.**

1.2. **Принцип иерархии ключей (ANSI X9.17).**

Мастер-ключи (МК) – ключи высшего уровня иерархии, которые сами защищаются некриптографическими средствами: физическими, аппаратными, организационными, юридическими и пр. Распределяются вручную или инсталлируются в систему на предоперационной стадии, остаются неизменными в течение всего жизненного цикла. МК защищаются мерами процедурного контроля, физической или логической изоляцией их от посторонних субъектов.

Ключи шифрования ключей (КШК) – симметричные ключи или открытые ключи шифрования, используемые для транспортировки или хранения других ключей, например, в протоколах транспортировки ключей. Безопасность КШК обеспечивается уровнем МК.

Ключи шифрования данных (КШД) – ключи, которые используются для выполнения криптографических операций над данными пользователя (шифрование, аутентификация). Обычно это кратковременные (сеансовые) ключи.

Принципы временного разделения ключей:

Криптопериод ключа – это период времени, в течение которого ключ остается действительным для санкционированного использования в системе. Введение криптопериода ключей может служить следующим целям:

- ограничению информации, связанной с определенным ключом, доступной для криптоанализа противником;
- ограничению ущерба – количества раскрытой информации – в случае компрометации ключа;
- ограничению времени, доступного для криптоаналитика противника с мощными вычислительными ресурсами.

Долговременные ключи (long-term keys) – как правило, мастер-ключи, а часто также КШК и другие ключи, способствующие обмену ключами, защищают кратковременные ключи.

Кратковременные ключи (short-term keys) – ключи, выработанные посредством протоколов обмена ключами или транспортировки, которые используются как КШД или сеансовые ключи для одного сеанса связи между абонентами криптосистемы.

Модели и стандарты инфраструктуры открытых ключей (ИОК)

Инфраструктура открытых ключей (ИОК) (соотв. англ. PKI – Public Key Infrastructure) – универсальная модель организованной поддержки криптографических средств защиты информации в крупномасштабных компьютерных системах в соответствии с принятыми в них политиками безопасности, которая реализует управление криптографическими ключами на всех этапах их жизненного цикла, обеспечивая взаимодействие всех средств защиты.

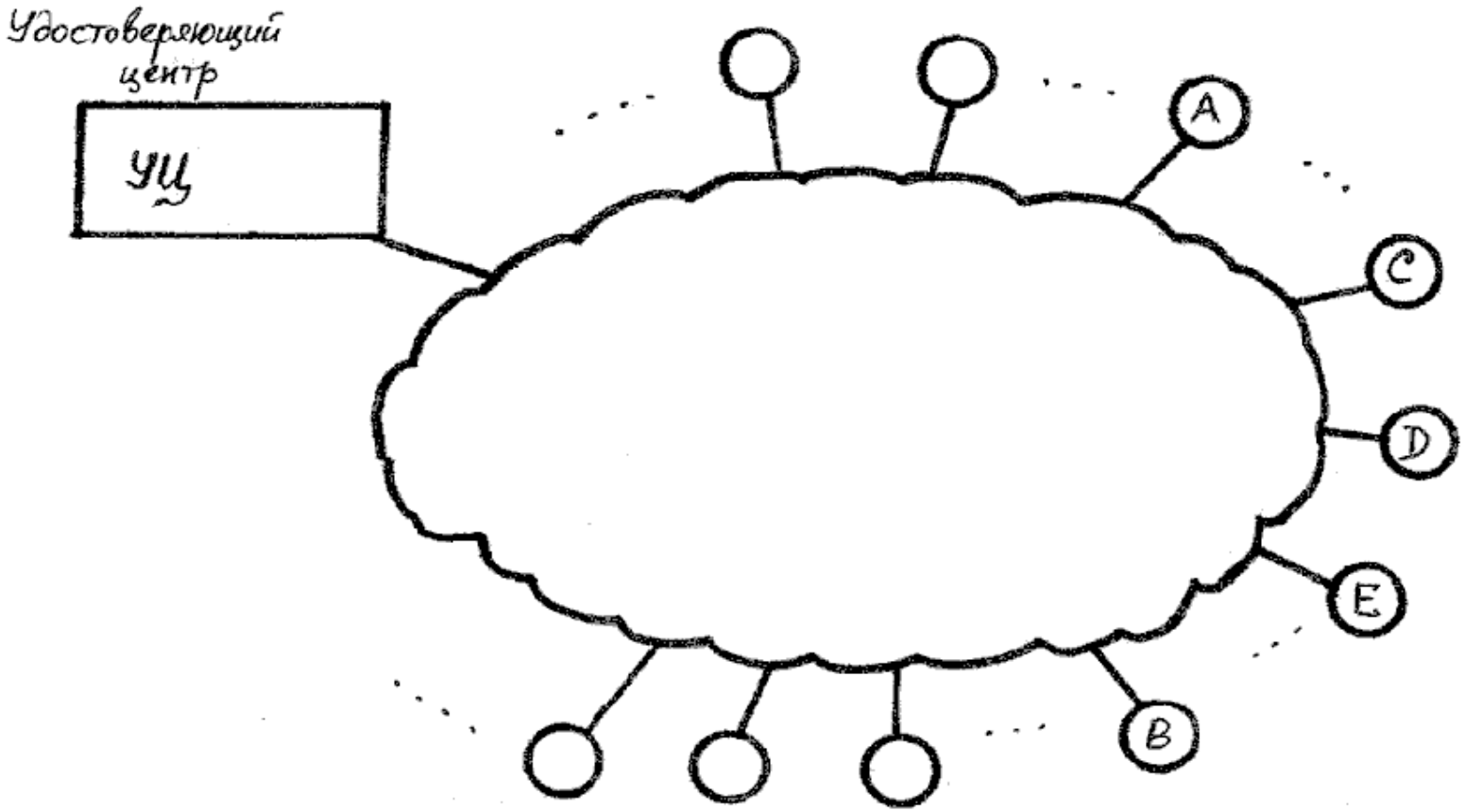
Разрабатываются рядом международных организаций: ISO совместно с IEC, ITU, IEEE, IETF, The Open Group, …

Наибольшее значение имеют следующие модели:

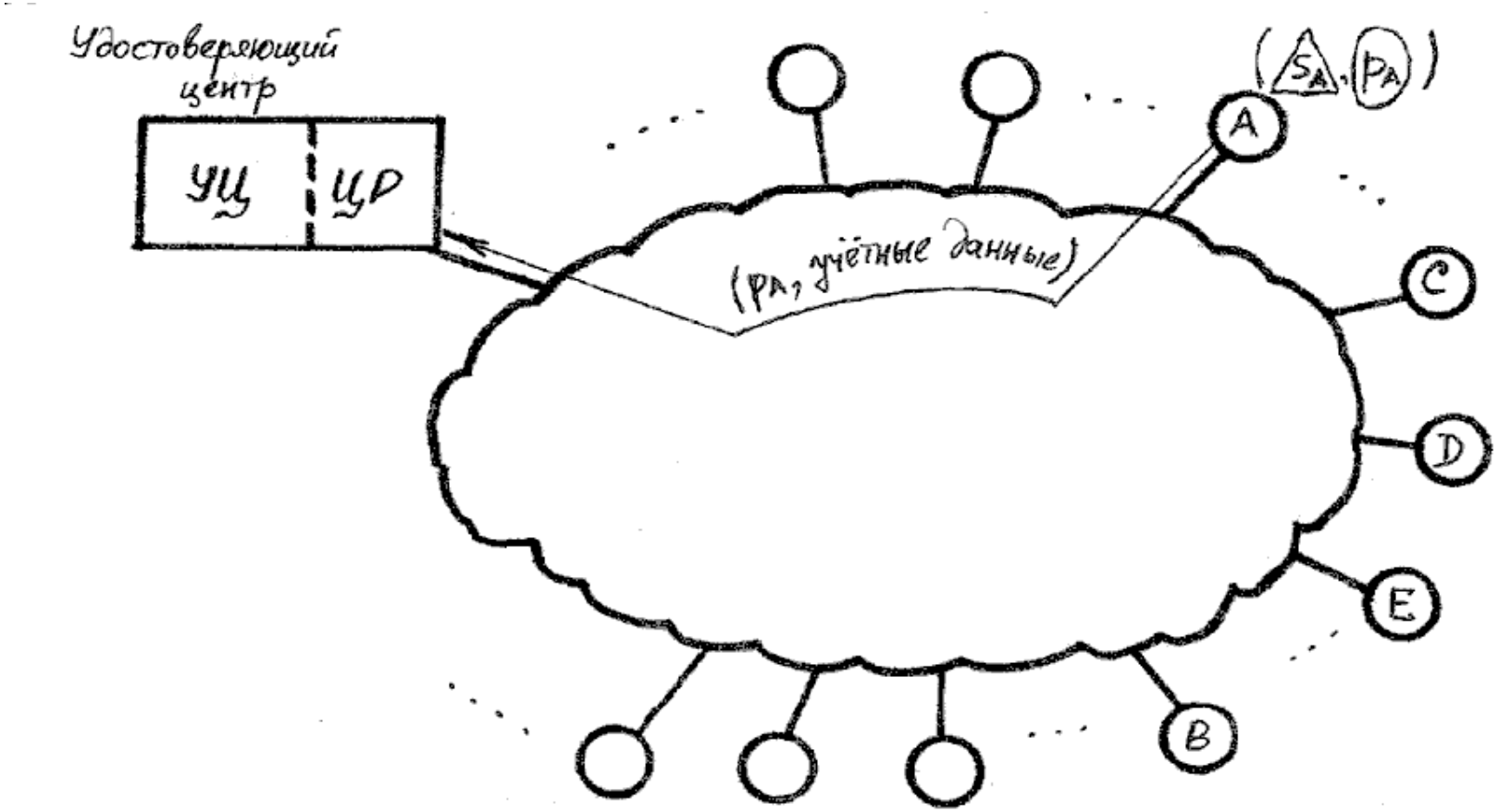
PKIX (Public Key Infrastructure for X.509) – модель IETF на базе X.509 – рекомендации Международного телекоммуникационного союза ITU

SPKI (Simple Public Key Infrastructure) – модель IETF

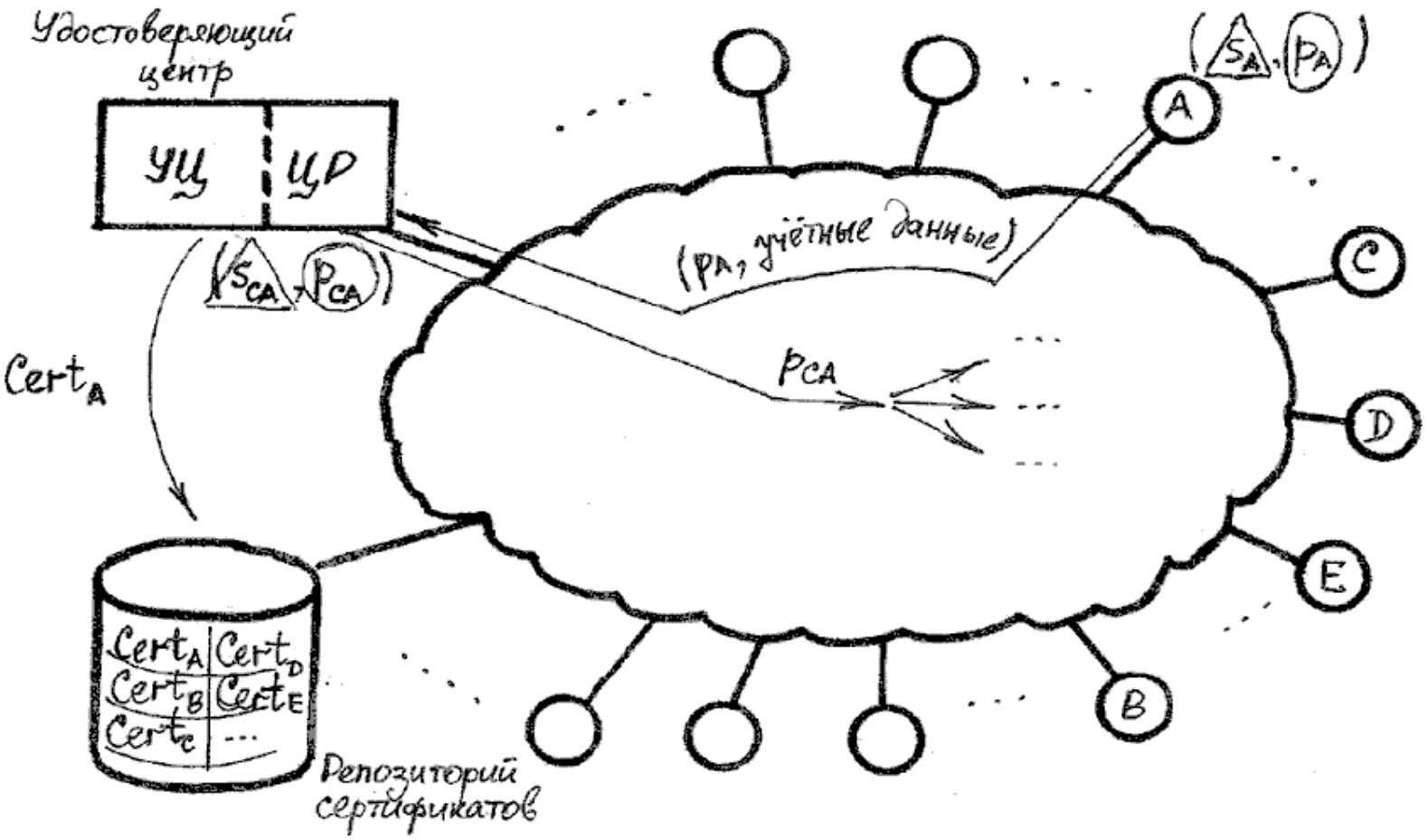
Обобщенная модель ИОК (1)



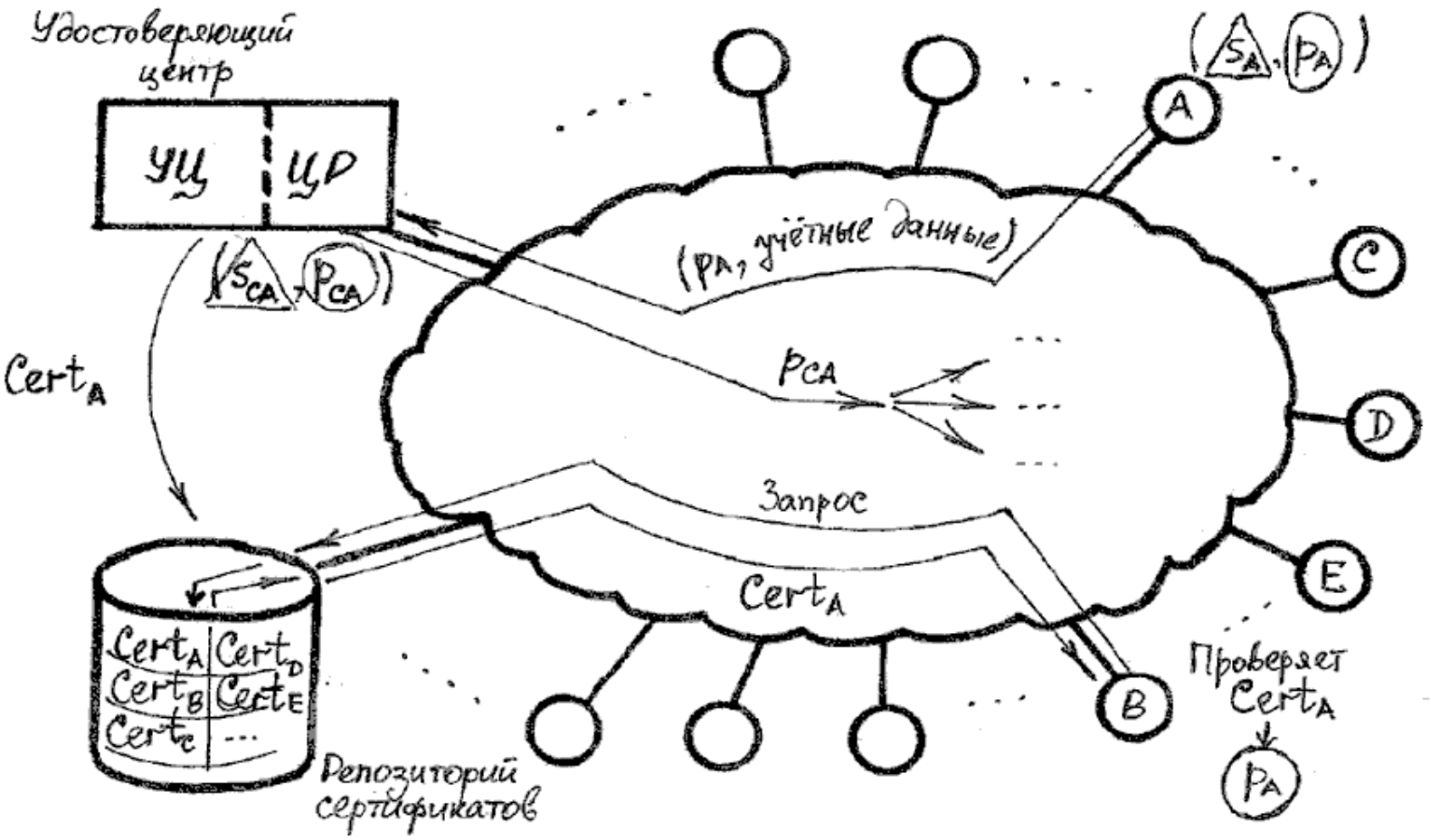
Обобщенная модель ИОК (2)



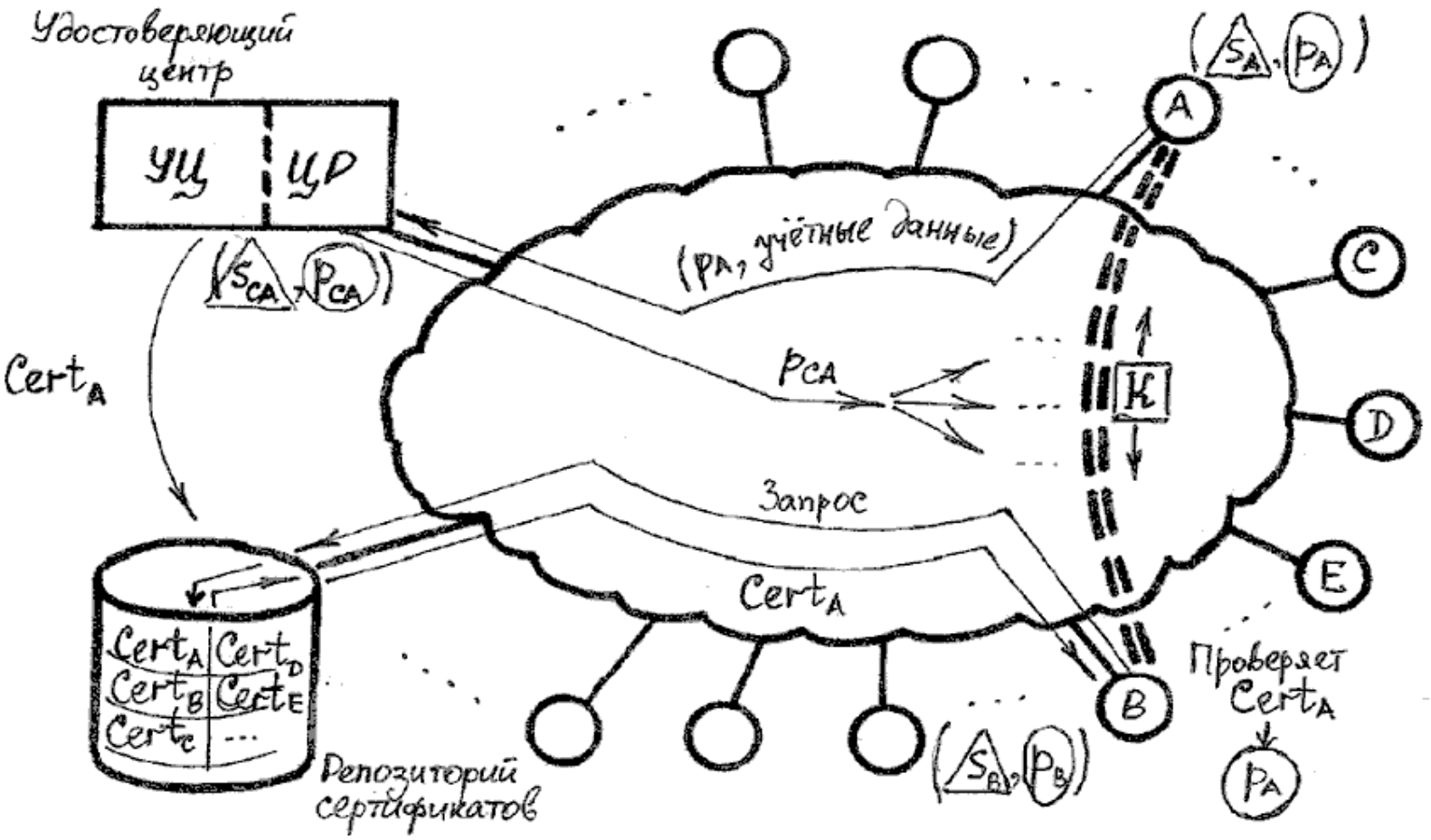
Обобщенная модель ИОК (3)



Обобщенная модель ИОК (4)



Обобщенная модель ИОК (5)



Формат сертификатов открытых ключей (по ITU X.509)

Версия сертификата
Серийный номер сертификата
Идентификатор алгоритма цифровой подписи, используемого удостоверяющим центром
Имя удостоверяющего центра (директориальное имя по стандарту X.500)
Период действия сертификата
Имя владельца открытого ключа (директориальное имя по стандарту X.500)
Информация об открытом ключе владельца: • идентификатор алгоритма; • значение открытого ключа.
Уникальный идентификатор удостоверяющего центра, выпустившего сертификат (v2)
Уникальный идентификатор владельца открытого ключа (v2)
Поле расширения (v3): содержание не определено.
Цифровая подпись удостоверяющего центра под всеми предыдущими полями

Формат списка аннулированных сертификатов (по ITU X.509)