ПРАКТИЧЕСКАЯ РАБОТА № 8.

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ И УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ

Цель: изучить инфраструктуру открытых ключей, и принцип создания удостоверяющих центров.

Теоретические вопросы

1. Предмет и задачи удостоверяющих центров.

2. Основные понятия инфраструктуры открытых ключей.

3. Классификация удостоверяющих центров.

4.Как удостоверяющий центр (УЦ) осуществляет выполнение функций, связанных с обеспечением ЭЦП всех участников информационного обмена.

Иерархическая система удостоверяющих центров

Рассмотрим снова ситуацию двух клиентов, зарегистрированных в разных удостоверяющих центрах, и введем следующие обозначения:

Y_1, Y_2 — два разных удостоверяющих центра,

A_1, A_2 — клиенты, зарегистрированные в удостоверяющих центрах Y_1 и Y_2 соответственно,

$\bar{A}_1, \bar{A}_2$ — открытые ключи соответствующих клиентов,

$\bar{Y}_1, \bar{Y}_2$ — открытые ключи соответствующих удостоверяющих центров,

$\bar{\bar{Y}}_1, \bar{\bar{Y}}_2$ — их закрытые ключи.

Для сертификатов клиентов A_1 и A_2, содержащих открытые ключи клиентов и их удостоверяющих центров и подписанных закрытым ключом соответствующего удостоверяющего центра, введем обозначения:

$$C(A_1) = (\bar{A}_1, \bar{Y}_1)s/\bar{\bar{Y}}_1 \quad \text{и} \quad C(A_2) = (\bar{A}_2, \bar{Y}_2)s/\bar{\bar{Y}}_2$$

соответственно.

Будем считать, что удостоверяющие центры Y_1 и Y_2 являются удостоверяющими центрами нижнего уровня. С целью взаимного признания ЭЦП всех клиентов удостоверяющих центров Y_1 и Y_2 создадим в информационной системе еще один удостоверяющий центр Y, который будет по отношению к Y_1 и Y_2 удостоверяющим центром более высокого уровня.

Потребуем далее, чтобы при своем создании удостоверяющие центры Y_1 и Y_2 прошли стандартную процедуру регистрации в удостоверяющем центре Y. При этом в соответствии с протоколом регистрации удостоверяющие центры Y_1 и Y_2 получат свои сертификаты $C(Y_1)$ и $C(Y_2)$, содержащие открытый ключ регистрирующего удостоверяющего центра Y и подписанные его закрытым ключом. В соответствии с принятой системой обозначений указанные сертификаты в дальнейшем обозначим:

$$C(Y_1) = (\overline{Y}_1, \overline{Y})s/\overline{\overline{Y}} \quad \text{и} \quad C(Y_2) = (\overline{Y}_2, \overline{Y})s/\overline{\overline{Y}}$$

соответственно.

Потребуем далее, чтобы при регистрации клиентов A_1 и A_2 в соответствующих удостоверяющих центрах Y_1 и Y_2 клиенты вместе с их собственными сертификатами $C(A_1)$ и $C(A_2)$ получали также соответствующие сертификаты регистрирующих их удостоверяющих центров $C(Y_1)$ и $C(Y_2)$, которые удостоверяющие центры получили во время своей регистрации в удостоверяющем центре Y.

Общая схема взаимодействия удостоверяющих центров Y_1, Y_2 и Y представлена на рис. 4.

Рассмотрим последовательность операций при обмене сообщениями между клиентом A_1 и клиентом A_2, действующими в информационной системе, образованной удостоверяющими центрами Y_1, Y_2 и Y. изображенной на рис. 4. Прежде всего, будем считать, что в процессе

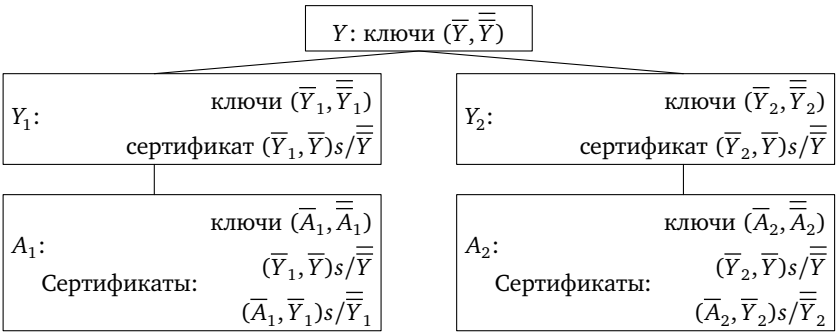

Рис. 4. Общая схема взаимодействия удостоверяющих центров Y_1, Y_2 и Y

выполнения стандартных процедур регистрации все субъекты информационной системы (удостоверяющие центры и клиенты) получили ключи и сертификаты, как это показано на рис. 4.

Тогда клиент-отправитель A_1 при отправке сообщения клиенту-получателю A_2 должен кроме трех операций, приведенных в разделе 3.2.3.4, выполнить еще одну — а именно, переслать клиенту A_2 сертификат своего удостоверяющего центра. Приведем всю последовательность операций клиента-отправителя A_1 в новых обозначениях:

$$(m, A_1) \xrightarrow{G} (m)\, s/A_1 \text{ — формирование ЭЦП сообщения } m; \quad \text{(A1.1)}$$

$$(m)\, s/A_1 \to A_2 \text{ — отправка подписанного сообщения;} \quad \text{(A1.2)}$$

$$\left(\bar{A}_1, \bar{Y}_1\right) s/\bar{\bar{Y}}_1 \to A_2 \text{ — отправка своего сертификата;} \quad \text{(A1.3)}$$

$$\left(\bar{Y}_1, \bar{Y}\right) s/\bar{\bar{Y}} \to A_2 \text{ — отправка сертификата своего удостоверяющего центра.} \quad \text{(A1.4)}$$

Клиенту-получателю необходимо выполнить дополнительные операции по сравнению с приведенными в разделе 3.2.3.5, поскольку проверка (A2.2) (см. ниже) в данной ситуации заведомо дает отрицательный результат, так как Y_1 и Y_2 — разные удостоверяющие центры. Вся последовательность операций клиента-получателя приведена ниже.

$$\left(\bar{A}_2, \bar{Y}_2\right) s/\bar{\bar{Y}}_2 \xrightarrow{E} \bar{Y}_2 \text{ — извлечение открытого ключа } Y_2 \text{ из собственного сертификата } A_2; \quad \text{(A2.1)}$$

$$\left(\left(\bar{A}_1, \bar{Y}_1\right) s/\bar{\bar{Y}}_1, \bar{Y}_2\right) \xrightarrow{V} 1 \text{ — проверка подписи присланного сертификата;} \quad \text{(A2.2)}$$

$$\left(\bar{Y}_2, \bar{Y}\right) s/\bar{\bar{Y}} \xrightarrow{E} \bar{Y} \text{ — извлечение открытого ключа } Y \text{ из имеющегося сертификата } Y_2; \quad \text{(A2.3)}$$

$$\left(\left(\bar{Y}_1, \bar{Y}\right) s/\bar{\bar{Y}}, \bar{Y}\right) \xrightarrow{V} 0 \text{ — проверка подписи присланного сертификата } Y_1; \quad \text{(A2.4)}$$

$$\left(\bar{Y}_1, \bar{Y}\right) s/\bar{\bar{Y}} \xrightarrow{E} \bar{Y}_1 \text{ — извлечение открытого ключа } Y_1 \text{ из присланного сертификата } Y_1; \quad \text{(A2.5)}$$

$$\left(\left(\bar{A}_1, \bar{Y}_1\right) s/\bar{\bar{Y}}_1, \bar{Y}_1\right) \xrightarrow{V} 0 \text{ — проверка подписи присланного сертификата } A_1; \quad \text{(A2.6)}$$

$$\left(\bar{A}_1, \bar{Y}_1\right) s/\bar{\bar{Y}}_1 \xrightarrow{E} \bar{A}_1 \text{ — извлечение открытого ключа } A_1 \text{ из присланного сертификата } A_1; \quad \text{(A2.7)}$$

$$\left((m)\, s/\bar{\bar{A}}_1, \bar{A}_1\right) \xrightarrow{V} 0 \text{ — проверка подписи сообщения } m. \quad \text{(A2.8)}$$

Покажем, что последовательность операций (А2.1)—(А2.8) удовлетворяет всем требованиям информационной безопасности, связанным с функциями удостоверяющих центров по подтверждению полномочий всех участников информационной схемы.

Действительно, невыполнение проверки (А2.2) означает, что клиент-отправитель не зарегистрирован в том же удостоверяющем центре, в котором зарегистрирован клиент-получатель.

Убедившись в этом, клиент-получатель с помощью пары операций (А2.3)—(А2.4) приходит к выводу, что удостоверяющие центры Y_1 (где зарегистрирован клиент-отправитель) и Y_2 (где зарегистрирован клиент-получатель) оба зарегистрированы в одном удостоверяющем центре Y. Тем самым «чужой» с точки зрения клиента-получателя удостоверяющий центр Y_1 становится легитимным участником информационной схемы. И клиент-получатель может признать присланный ему отправителем по операции (А1.4) сертификат этого удостоверяющего центра.

Следующей парой операций (А2.5)—(А2.6) клиент-получатель убеждается, что присланный ему по операции (А1.3) сертификат действительно является сертификатом клиента A_1, зарегистрированного в удостоверяющем центре Y_1.

Поэтому из присланного сертификата клиент-получатель может извлечь открытый ключ клиента $\bar{A}_1$ и использовать его для проверки ЭЦП сообщения m. Что он и делает операциями (А2.7)—(А2.8).

Рассмотренная простейшая схема, содержащая лишь два удостоверяющих центра нижнего уровня, естественным образом обобщается на случай произвольного числа таких удостоверяющих центров.

Действительно, пусть в схеме уже задействовано $n-1$ удостоверяющих центров нижнего уровня. Тогда при добавлении к схеме еще одного удостоверяющего центра нижнего уровня Y_n необходимо выполнить следующие операции:

1. Зарегистрировать Y_n в удостоверяющем центре Y с выдачей ему стандартного сертификата $C(Y_n) = (\bar{Y}_n, \bar{Y})s/\bar{\bar{Y}}$.
2. При регистрации в Y_n клиентов выдавать каждому из них пару сертификатов: $C(A_n) = (\bar{A}_n, \bar{Y}_n)s/\bar{\bar{Y}}_n$ — собственный сертификат клиента A_n и $C(Y_n) = (\bar{Y}_n, \bar{Y})s/\bar{\bar{Y}}$ — сертификат удостоверяющего центра Y_n.

Выполнение действий 1 и 2, первое из которых производится только один раз при регистрации добавляемого в схему удостоверяющего центра, позволяет включить в единую информационную схему всех клиентов всех удостоверяющих центров $Y_1, Y_2, \ldots, Y_n$.

Важным преимуществом указанной схемы является то обстоятельство, что при добавлении в схему нового удостоверяющего центра вообще не нужно знать, сколько удостоверяющих центров уже задействовано в схеме. Это выгодно отличает ее от схем типа попарных обменов сертификатами между всеми удостоверяющими центрами, действующими в схеме.

Еще одним преимуществом указанной схемы является отсутствие необходимости каких-либо обменов информацией между клиентом-получателем и удостоверяющими центрами, задействованными в информационной системе.

Приведенная схема обобщается также и на произвольную систему удостоверяющих центров, устроенную иерархическим образом. В этом случае произвольный набор удостоверяющих центров, объединенных в иерархическую информационную систему, естественно изображать в виде *графа*, то есть множества узлов (вершин), причем некоторые из них соединены связями — ребрами графа. Узлами графа будут являться удостоверяющие центры. Два удостоверяющих центра Y_i и Y_k соединены ребром графа, если Y_i зарегистрирован в удостоверяющем центре Y_k. Поскольку каждый удостоверяющий центр может быть зарегистрирован только в одном удостоверяющем центре более высокого уровня, граф, их изображающий, является *деревом* (быть может, несвязным). Один удостоверяющий центр самого высокого уровня, не зарегистрированный ни в каком другом, называется *корневым* удостоверяющим центром.

В любом удостоверяющем центре системы могут быть также зарегистрированы пользователи-клиенты.

При получении сообщения от клиента A_i, зарегистрированного в удостоверяющем центре Y_i, клиент-получатель A_j, зарегистрированный в удостоверяющем центре Y_j, должен убедиться, что отправитель A_i зарегистрирован в одном из удостоверяющих центров, входящих в общую систему с удостоверяющим центром Y_j, в котором зарегистрирован получатель A_j.

Для решения этой задачи может быть использован механизм сертификатов удостоверяющих центров.

Будем по-прежнему называть сертификатом удостоверяющего центра Y_i набор записей, содержащий открытый ключ самого удостоверяющего центра $\overline{Y}_i$, открытый ключ удостоверяющего центра $\overline{Y}_k$, в котором зарегистрирован Y_i, и подписанный закрытым ключом удостоверяющего центра $\overline{\overline{Y}}_k$. Будем обозначать сертификат удостоверяющего центра Y_i через

$$C(Y_i) = \left(\overline{Y}_i, \overline{Y}_k\right)s/\overline{\overline{Y}}_k.$$

Пусть $C(Y_i) = (\overline{Y}_i, \overline{Y}_k)s/\overline{\overline{Y}}_k$, $C(Y_j) = (\overline{Y}_j, \overline{Y}_l)s/\overline{\overline{Y}}_l$ — сертификаты двух удостоверяющих центров: Y_i — зарегистрированного в Y_k и Y_j — зарегистрированного в Y_l.

Введем две формальных операции с сертификатами.

а) *Соответствие сертификатов*

Будем говорить, что сертификаты $C(Y_i)$ и $C(Y_j)$ соответствуют друг другу, если выполнено условие

$$\left((\overline{Y}_i, \overline{Y}_k)s/\overline{\overline{Y}}_k, \overline{Y}_l\right) \xrightarrow{V} 0. \tag{14}$$

Это условие может быть выполнено только в том случае, если $\overline{Y}_l = \overline{Y}_k$, а это в свою очередь означает, что оба удостоверяющих центра Y_i и Y_j зарегистрированы в одном удостоверяющем центре, т. е. удостоверяющий центр Y_k совпадает с удостоверяющим центром Y_l.

При этом, если $C(Y_i)$ соответствует $C(Y_j)$, то и $C(Y_k)$ соответствует $C(Y_l)$, т. е. если выполнено (14), то выполняется и симметричное условие

$$\left((\overline{Y}_j, \overline{Y}_l)s/\overline{\overline{Y}}_l, \overline{Y}_k\right) \xrightarrow{V} 0. \tag{14'}$$

б) *Проверка регистрации*

Пусть по-прежнему $C(Y_i)$ и $C(Y_j)$ — сертификаты двух удостоверяющих центров. Для того чтобы проверить, действительно ли удостоверяющий центр Y_i зарегистрирован в Y_j, достаточно проверить выполнение условия

$$\left((\overline{Y}_i, \overline{Y}_k)s/\overline{\overline{Y}}_k, Y_j\right) \xrightarrow{V} 0. \tag{15}$$

Действительно, проверка (15) может быть выполнена только в случае, если $\overline{\overline{Y}}_k$ соответствует $\overline{Y}_j$, а это означает, что $Y_k = Y_j$ и сертификат $C(Y_i)$ может быть переписан в виде $(\overline{Y}_i, \overline{Y}_j)s/\overline{\overline{Y}}_j$, а это, в свою очередь, означает, что удостоверяющий центр Y_i зарегистрирован в удостоверяющем центре Y_j.

Теперь может быть сформулирован *алгоритм определения открытого ключа отправителя*.

Пусть A — клиент-отправитель, зарегистрированный в удостоверяющем центре Y_0, а A' — клиент-получатель, зарегистрированный в удостоверяющем центре Y_0' (см. рис. 5).

Здесь

$$Y_0 \to Y_1 \to \ldots \to Y_{n-1} \to Y_n \text{ — цепочка регистрации клиента } A.$$

$$Y_0' \to Y_1' \to \ldots \to Y_{m-1}' \to Y_m' = Y_{n-1} \to Y_n \text{ — цепочка регистрации клиента } A'.$$

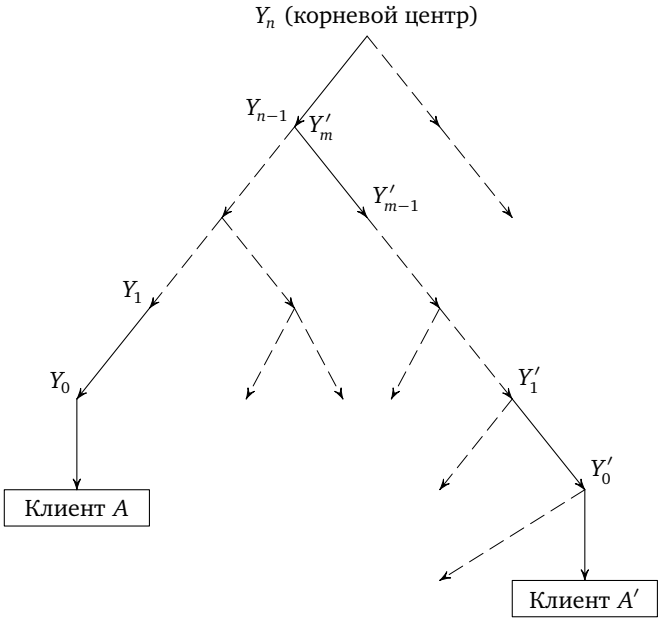

Рис. 5. Цепочки регистрации клиентов

В соответствии с соглашением при своей регистрации в Y_0 клиент A получает свой собственный сертификат $C(A)$ и всю цепочку сертификатов удостоверяющих центров вышестоящих уровней, начиная с Y_0:

$$\begin{aligned} C(A) &= (\bar{A}, \bar{Y}_0)s/\bar{\bar{Y}}_0, \\ C(Y_0) &= (\bar{Y}_0, \bar{Y}_1)s/\bar{\bar{Y}}_1, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ C(Y_{n-1}) &= (\bar{Y}_{n-1}, \bar{Y}_n)s/\bar{\bar{Y}}_n. \end{aligned} \tag{16}$$

Аналогично, клиент-получатель A' при своей регистрации в удостоверяющем центре Y'_0 получает цепочку сертификатов

$$\begin{aligned} C(A') &= (\bar{A}', \bar{Y}'_0)s/\bar{\bar{Y}}'_0 \\ C(Y'_0) &= (\bar{Y}'_0, \bar{Y}'_1)s/\bar{\bar{Y}}'_1 \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ C(Y'_{m-1}) &= (\bar{Y}'_{m-1}, \bar{Y}'_m)s/\bar{\bar{Y}}'_m \quad \text{и, учитывая, что } Y'_m = Y_{n-1}, \\ C(Y_{n-1}) &= (\bar{Y}_{n-1}, \bar{Y}_n)s/\bar{\bar{Y}}_n. \end{aligned} \tag{16'}$$

Цепочки (16) и (16′) могут быть, вообще говоря, разной длины.

Во время обмена информацией клиент A отправляет клиенту A' сообщение m, подписанное своим закрытым ключом $(m)\,s/\overline{\overline{A}}$, и всю цепочку сертификатов $C(A), C(Y_0), C(Y_1), \ldots, C(Y_{n-1})$.

Чтобы проверить правильность принятого сообщения m, клиент-получатель должен иметь открытый ключ клиента-отправителя $\overline{A}$, который ему прислан в составе сертификата $C(A)$. Для того чтобы убедиться в легитимности его использования, клиенту A' необходимо проверить, что удостоверяющие центры Y_0 и Y_0' находятся в одной информационной системе. Другими словами, что в цепочках удостоверяющих центров, имеющих сертификаты (16) и (16′), имеется общий узел. Выполнение этого условия проверяется путем попарного сравнения сертификатов из цепочек (16) и (16′) с помощью операции (14).

Если ни для одной из возможных пар сертификатов $\left(C(Y_p), C(Y_r')\right)$, где $C(Y_p)$ — сертификат из цепочки (16), $C(Y_r')$ — сертификат из цепочки (16′), операция соответствия не выполняется, то это означает, что удостоверяющий центр Y_0 не находится в одной информационной системе с удостоверяющим центром Y_0'.

Если же для какой-то пары сертификатов $\left(C(Y_p), C(Y_r')\right)$ операция соответствия (14) выполнена, то это означает, что удостоверяющий центр Y_p из цепочки (16) и Y_r' из цепочки (16′) зарегистрированы в одном удостоверяющем центре.

Для завершения процедуры проверки легитимности использования открытого ключа клиента-отправителя A, присланного в составе сертификата $C(A)$, достаточно убедиться, что все удостоверяющие центры в цепочке (16), начиная с Y_p и включая Y_0, легитимно зарегистрированы.

Для этого необходимо последовательно проверить, что для всех сертификатов, начиная с $C(Y_p)$ до $C(Y_0)$ включительно, выполняется условие

$$\left((\overline{\overline{Y}}_k, \overline{\overline{Y}}_{k+1})s/\overline{\overline{\overline{Y}}}_{k+1}, \overline{\overline{Y}}_{k+1}\right) \xrightarrow{V} 0, \tag{17}$$

где k пробегает все значения от p до 0. Если хотя бы одна из подобных проверок (17) не выполнена, цепочку регистрации Y_0 нельзя считать легитимной.

Если же выполнены все проверки (17), клиент-получатель может из присланного ему сертификата $C(A)$ извлечь открытый ключ отправителя $\overline{A}$ и проверить с его помощью правильность подписи сообщения m с использованием стандартного алгоритма проверки ЭЦП:

$$\left((m)\,s/\overline{\overline{A}}, \overline{A}\right) \xrightarrow{V} \{0; 1\}.$$

Задание.

Реализовать на любом машинном языке процесс обмена сертификатами между клиентами разных удостоверяющих центрах, которые зарегистрированы в удостоверяющем центре более высокого уровня:

1. Этапы процесса регистрации УЦ1 и УЦ2 в УЦ более высокого уровня.
2. Этапы процесса регистрации клиентов в разных УЦ (УЦ1 и УЦ2 зарегистрированных в УЦ более высокого уровня). Продемонстрировать как минимум на четырех клиентах (двух из УЦ1 и двух клиентах из УЦ2.
3. Процесс создания сертификатов УЦ1 и УЦ2.
4. Процесс создания сертификатов клиентов.
5. Осуществить пересылку сертификатов между УЦ.
6. Осуществить пересылку сертификатов между пользователями УЦ1 и УЦ2.
7. Оформить отчет о проделанной работе.