ПРАКТИЧЕСКАЯ РАБОТА № 6.

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.

В 1977году американские математики У. Диффи и М. Э. Хеллман предложили перейти к системе, основанной на создании единого общедоступного хранилища всех открытых ключей. В несколько упрощенном и полемически заостренном варианте их предложение звучало примерно так: «Давайте издадим общедоступную книгу — справочник с открытыми ключами всех участников информационного обмена. Это полностью решит проблему хранения каждым участником большого количества ключей».

Поначалу это предложение произвело неоднозначный и даже шокирующий эффект. Однако авторы показали большое число преимуществ, которые обеспечивались его реализацией. Действительно, такая система полностью избавляла огромное число пользователей от трудоемкой работы по запоминанию, хранению и уничтожению своих открытых ключей, перекладывая эти заботы на администрацию книги-справочника. Кроме того, для пользователей значитель-но упрощалась процедура поиска открытых ключей других участ-ников обмена. Для этого пользователю достаточно найти в книге-справочнике своего адресата и извлечь хранящийся в ней его открытый ключ.

Предложение открывало и другие возможности. Например, пользователи освобождаются от необходимости самим генерировать свои открытый и закрытый ключи, это можно было делать в централизо-

ванном порядке в едином центре. За пользователем остается только священная обязанность следить, чтобы ничего неприятного не случилось с его закрытым ключом.

Осознание этих преимуществ привело к тому, что уже в начале 80-х годов прошлого века появились первые практические реализации предложенной идеи. Ядро подобной реализации составили общедоступные централизованные хранилища открытых ключей, которые получили названия *удостоверяющих центров*. Кроме собственно функции *хранения* открытых ключей, удостоверяющие центры выполняют и еще много функций. В качестве важнейших из них укажем функции *регистрации* пользователей и *формирования ключей* пользователей. Что касается самого названия, то оно связано с тем, что с самого начала одной из важнейших функций удостоверяющих центров было обеспечение инфраструктуры электронной цифровой подписи в процессе информационного обмена. Поэтому еще одной функцией удостоверяющих центров стало *удостоверение полномочий* участников обмена.

Рассмотрим, в общих чертах, как удостоверяющий центр (УЦ) осуществляет выполнение функций, связанных с обеспечением ЭЦП всех участников информационного обмена.

Обеспечивающие алгоритмы

Напомним вкратце, какими криптографическими алгоритмами обеспечивается технология использования ЭЦП в электронном документообороте. Таких алгоритмов три:

— формирование ключей клиента (алгоритм I);
— формирование ЭЦП сообщения (алгоритм G);
— проверка ЭЦП сообщения (алгоритм V).

В основу их функционирования могут быть положены различные математические методы. Если абстрагироваться от конкретных математических методов, то эти алгоритмы можно определить следующим образом.

Формирование ключей клиента A

Алгоритм

$$I \to \left(\overline{\overline{K}}_A, \overline{K}_A\right) \tag{10}$$

запускается во время регистрации клиента A в удостоверяющем центре Y. В результате клиент получает:

— $\overline{\overline{K}}_A$ — закрытый ключ, известный только ему;

— $\overline{K}_A$ — соответствующий закрытому ключу $\overline{\overline{K}}_A$ открытый ключ, который становится известен всем участникам информационной системы;
— C_A — сертификат ЭЦП клиента A — совокупность записей, содержащих различные сведения о клиенте, в частности его ФИО, полномочия, срок действия сертификата и т.п. Эта информация может быть использована в алгоритмах обмена. В разных системах структура сертификата может иметь незначительные различия. Для дальнейшего изложения удобно считать, что сертификат ЭЦП клиента A в обязательном порядке содержит открытый ключ клиента $\overline{K}_A$ и открытый ключ удостоверяющего центра $\overline{K}_Y$.

Формирование ЭЦП сообщения

Алгоритм запускается клиентом A:

$$\left(m, \overline{\overline{K}}_A\right) \xrightarrow{G} (m, s), \tag{11}$$

где m — сообщение, которое клиент A подписывает перед отправкой; s — строка, представляющая собой ЭЦП сообщения.

Говорят, что s является ЭЦП сообщения m, которая сформирована с помощью закрытого ключа $\overline{\overline{K}}_A$. Если важно указать на факт подписи сообщения с помощью данного закрытого ключа, может быть использована другая запись действия алгоритма G:

$$\left(m, \overline{\overline{K}}_A\right) \xrightarrow{G} (m)\, s/\overline{\overline{K}}_A. \tag{11'}$$

Проверка ЭЦП сообщения

Алгоритм запускается клиентом, принявшим сообщение m, подписанное с помощью ЭЦП клиентом A:

$$(m, s, \overline{K}_A) \xrightarrow{V} \{0; 1\}. \tag{12}$$

Или, используя обозначения (11):

$$\left((m)\, s/\overline{\overline{K}}_A, \overline{K}_A\right) \xrightarrow{V} \{0; 1\}, \tag{12'}$$

где m — принятое сообщение; s — подпись сообщения m, сформированная клиентом A с помощью своего закрытого ключа $\overline{\overline{K}}_A$ с использованием алгоритма G; $\overline{K}_A$ — открытый ключ клиента A.

Результатом проверки является 0, если проверка выполнена, либо 1, если проверка не выполнена. Выполнение проверки означает одновременное выполнение двух условий:

— закрытый ключ $\overline{\overline{K}}_A$, использовавшийся при формировании подписи, соответствует открытому ключу $\overline{K}_A$, использовавшемуся при

проверке. Другими словами, пара ключей $\overline{\overline{K}}_A$ и $\overline{K}_A$ сформированы алгоритмом (10);

— сообщение m, поданное на вход алгоритма проверки (12), совпадает с сообщением m, которое было подписано с использованием алгоритма (11).

Соответственно, невыполнение проверки означает, что либо в алгоритме проверки (21) используется открытый ключ, не соответствующий закрытому ключу из алгоритма (11), либо сообщение m на входе алгоритма проверки не совпадает с сообщением, которое подписывалось при помощи алгоритма (11).

Обмен между клиентами одного удостоверяющего центра

Рассмотрим, как с использованием криптографических алгоритмов решается задача пересылки сообщения, подписанного клиентом A, клиенту B, при условии, что оба эти клиента зарегистри-рованы в одном удостоверяющем центре УЦ.

Всю совокупность операций, обеспечивающих выполнение указанной задачи, можно разбить на пять групп:

— операции, выполняемые при создании удостоверяющего центра УЦ;

— операции, выполняемые при регистрации клиента A в удостоверяющем центре УЦ;

— операции, выполняемые при регистрации клиента B в том же удостоверяющем центре УЦ;

— операции, выполняемые клиентом A при отправке сообщения;— операции, выполняемые клиентом B при получении сообщения.

Рассмотрим указанные операции по шагам.

Операции, выполняемые при создании удостоверяю-щего центра. (i) При создании удостоверяющего центра выбирается некоторая тройка криптографических алгоритмов (I, G, V), обеспечивающих технологию использования ЭЦП. (В дальнейшем все клиенты этого УЦ будут при регистрации обеспечиваться этими же алгоритмами.)

(ii) Запускается алгоритм формирования ключей I, который на выходе дает пару ключей УЦ

$$I \to \left(\overline{\overline{K}}_Y, \overline{K}_Y\right). \tag{13}$$

(iii) **Замечание.** Вообще говоря, для создания реально работающего УЦ должно быть выполнено большое количество условий, обеспе-

чивающих легитимность, в том числе и юридическую, его деятельности. Однако здесь и всюду далее мы будем останавливаться только на криптографическом обеспечении деятельности УЦ. А для этого достаточно при создании УЦ выполнить только одну операцию (31).

Операции, выполняемые при регистрации клиента. Для легитимного участия в процессе обмена информации любой участник должен пройти процедуру *регистрации* в УЦ, становясь тем самым его *клиентом*. При регистрации клиента A УЦ выполняет следующие операции.

(i) С помощью алгоритма I формируются открытый $\overline{K}_A$ и закрытый $\overline{\overline{K}}_A$ ключи клиента A.

(ii) Формируется *сертификат ЭЦП клиента A* — совокупность записей, содержащих различные сведения о клиенте, в частности, его ФИО, полномочия, срок действия сертификата и т. д. Эта информация может использоваться в алгоритмах обмена. В разных информационных системах структура и состав сертификата могут иметь незначительные различия. Для дальнейшего удобно считать, что сертификат ЭЦП клиента A в обязательном порядке содержит открытый ключ клиента $\overline{K}_A$ и открытый ключ удостоверяющего центра $\overline{K}_Y$. В дальнейшем сертификат клиента A обозначается C_A, или, если требуется подчеркнуть, какие ключи содержит сертификат клиента A, — $C_A(\overline{K}_A, \overline{K}_Y)$.

(iii) Сертификат клиента подписывается (разумеется, имеется в виду ЭЦП с выполнением алгоритма G) с использованием закрытого ключа УЦ, т. е. выполняется операция:

$$\left(C_A, \overline{\overline{K}}_Y\right) \xrightarrow{G} (C_A)\, s/\overline{\overline{K}}_Y.$$

(iv) УЦ пересылает клиенту A:

- его сертификат C_A, подписанный закрытым ключом удостоверяющего центра $(C_A)\, s/\overline{\overline{K}}_Y$ и содержащий открытый ключ удостоверяющего центра $\overline{K}_Y$, который проводил регистрацию клиента;
- его открытый и закрытый ключи $\overline{K}_A$ и $\overline{\overline{K}}_A$. При этом передаче закрытого ключа уделяется особое внимание. Физически он может быть передан по защищенному каналу связи, либо по обычному каналу в зашифрованном виде, может быть передан на «секретной» дискете или каким-либо другим способом.

(v) Клиент A, получив от УЦ перечисленные в предыдущем пункте параметры, проводит проверку правильности регистрации, для чего, используя полученный открытый ключ удостоверяющего центра $\overline{K}_Y$,

запускает алгоритм проверки V по схеме:

$$\left((C_A)\, s/\overline{\overline{K}}_Y, \overline{K}_Y\right) \xrightarrow{V} 0.$$

Если при этом результат проверки равен 0, регистрация проведена правильно.

Аналогично проводится регистрация клиента B в том же УЦ.

Операции, выполняемые клиентом A при отправке сообщения. Для отправки сообщения m, подписанного ЭЦП, клиент A выполняет следующие операции:

(i) Подписывает с использованием своего закрытого ключа сообщение m, то есть выполняет операцию

$$\left(m, \overline{\overline{K}}_A\right) \xrightarrow{G} (m)\, s/\overline{\overline{K}}_A.$$

(ii) Пересылает клиенту-получателю B сообщение m, подписанное своим закрытым ключом

$$(m)\, s/\overline{\overline{K}}_A \to B.$$

(iii) Пересылает B свой сертификат C_A, подписанный закрытым ключом УЦ, в котором клиент A зарегистрирован:

$$(C_A)\, s/\overline{\overline{K}}_Y \to B.$$

Операции, выполняемые клиентом B при получении сообщения. (i) При получении сообщения m от клиента A клиент B должен убедиться в выполнении трех условий:

— сообщение m подписано именно A;
— сообщение m дошло без искажений;
— клиент A зарегистрирован в том же УЦ, что и сам клиент B.

Мы уже отмечали, что выполнение первых двух условий обеспечивается самим механизмом использования ЭЦП. Что касается третьего условия, то его выполнение, в силу юридических функций удостоверяющих центров, обеспечивает подтверждение полномочий участников информационного обмена.

(ii) Для проверки выполнения этого условия клиент B проверяет подпись сертификата, полученного от клиента A, с использованием открытого ключа УЦ, который клиент B получил при своей регистрации. Обозначим временно этот ключ $\overline{K}_{Y_1}$ и рассмотрим результат выполнения проверки $\xrightarrow{}$

$$\left((C_A)\, s/\overline{\overline{K}}_Y, \overline{K}_{Y_1}\right) \xrightarrow{V} \{0; 1\}.$$

Выполнение указанной проверки означает, что клиент-отправитель A и клиент-получатель B зарегистрированы в одном и том же УЦ.

Действительно, клиент B извлекает открытый ключ удостоверяющего центра $\overline{K}_{Y_1}$ из *своего собственного сертификата*, о котором заведомо известно, что он выдан удостоверяющим центром УЦ во время регистрации клиента B. Затем этот ключ используется для проверки правильности подписи полученного сертификата отправителя. Однако сертификат отправителя подписан закрытым ключом удостоверяющего центра, в котором зарегистрирован отправитель. И если проверка выполнена, то это означает, что ключи $\overline{K}_{Y_1}$ и $\overline{\overline{K}}_Y$ соответствуют друг другу, а значит, ключи $\overline{K}_{Y_1}$ и $\overline{K}_Y$ совпадают и, следовательно, клиент A и клиент B зарегистрированы в одном и том же удостоверяющем центре.

(iii) Убедившись, что клиент, отправивший сообщение, зарегистрирован в том же УЦ, клиент-получатель B может проверить правильность подписи под полученным сообщением. Для этого он извлекает открытый ключ отправителя $\overline{K}_A$ из полученного вместе с сообщением сертификата отправителя C_A и использует его для проверки подписи полученного сообщения:

$$((\mathrm{m})\ \mathrm{s}/\ \ \overline{\overline{K}}_A\,\overline{K}_A) \xrightarrow{V} 0.$$

Если результат проверки равен 0, сообщение подписано правильно и, следовательно, выполнены и первые два условия.

(iv) Описанное в предыдущем пункте извлечение открытого ключа отправителя из его сертификата, полученного из удостоверяющего центра, и есть конкретное использование идеи У. Диффи и М. Э. Хеллмана о создании единого общедоступного хранилища всех открытых ключей. Все открытые ключи централизованно хранятся в удостоверяющем центре и извлекаются оттуда пользователями по мере надобности.

Задание.

Реализовать на любом машинном языке обмен сертификатами между клиентами одного удостоверяющего центра:

1. Процесс регистрации двух клиентов в УЦ.
2. Процесс создания сертификатов.
3. Осуществить пересылку сертификатов между пользователями.
4. Оформить отчет о проделанной работе.