

## **Криптографическая система Шифр-РКІ**

### **Назначение и состав системы**

Криптографическая система Шифр-РКІ представляет собой универсальную иерархическую масштабируемую систему криптографической защиты данных и управления открытыми ключами.

Шифр-РКІ содержит набор программных средств для построения корпоративной инфраструктуры открытых ключей (Public Key Infrastructure - РКІ), которая обеспечивает доверительные взаимоотношения между корреспондентами в процессе обмена данными.

Основой доверительных отношений являются цифровые сертификаты. Сертификат однозначно связывает открытый ключ корреспондента с его именем и выдается центром сертификации ключей. Наличие сертификата, принадлежащего корреспонденту, позволяет вести с ним шифрованный обмен данными, проверять электронные цифровые подписи принятых от него сообщений и осуществлять строгую аутентификацию источника их передачи.

Шифр-РКІ позволяет создать инфраструктуру открытых ключей, включающую следующие элементы:

- главный центр сертификации ключей (ГЦСК), обладающий самоподписанным (рутовым) сертификатом и осуществляющий выдачу цифровых сертификатов для региональных (подчиненных) центров сертификации;
- региональные центры сертификации ключей (РЦСК), обладающие сертификатом ГЦСК и осуществляющие выдачу персональных цифровых сертификатов пользователям регионов;
- центры регистрации (ЦР), осуществляющие передачу запросов на сертификацию в РЦСК и прием сертификатов для пользователей, территориально удаленных от места расположения РЦСК;
- средства генерации пользовательских ключей и формирования запросов на сертификацию;
- исполнительные программные комплексы (библиотеки), выполняющие шифрование и цифровую подпись данных, которые можно использовать в различных автоматизированных системах.

В зависимости от потребностей Заказчика на базе средств системы Шифр-РКІ могут быть созданы подсистемы управления ключами и сертификатами различных конфигураций:

- *трехуровневая иерархическая (Рис. 1)*, включающая главный и несколько региональных (подчиненных главному) центров сертификации ключей, в каждом регионе - несколько центров регистрации (подчиненных своему региональному центру);

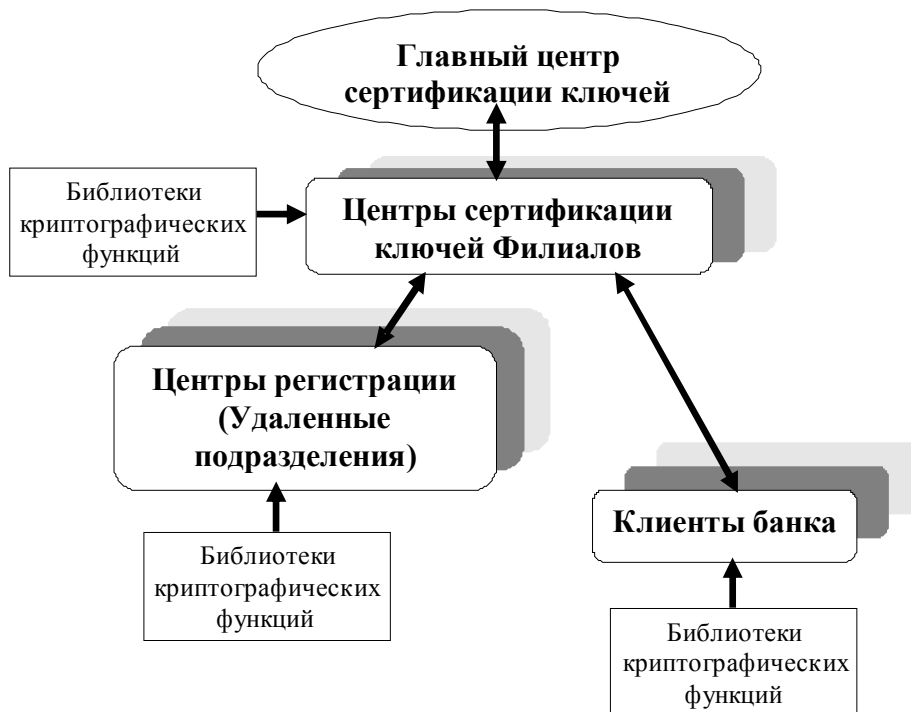


Рис. 1

- *двухуровневая иерархическая (Рис. 2)*, включающая один центр сертификации ключей и несколько центров регистрации;

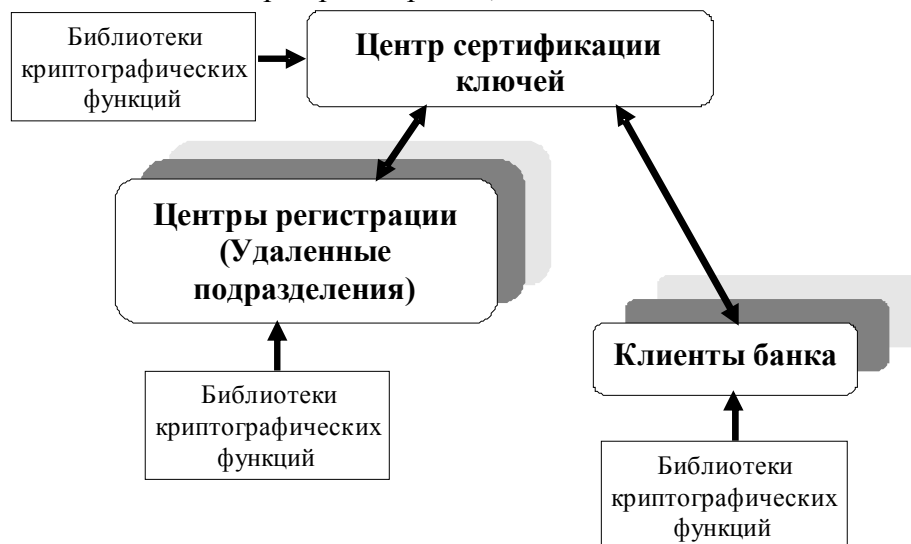


Рис. 2

- подсистема управления ключами и сертификатами для системы «Клиент-банк» (Рис. 3), состоящая из одного центра сертификации ключей.

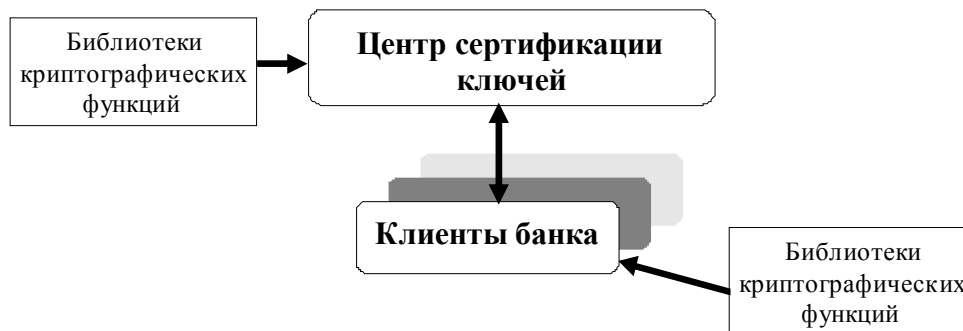


Рис. 3

Средства системы Шифр- PKI условно разделены на две части. Первая часть - базовый комплекс. В состав базового комплекса входят следующие элементы:

- АРМ главного центра сертификации ключей (ГЦСК).
- АРМ регионального центра сертификации ключей (РЦСК).
- Модуль генерации ключей.
- Модуль криптографических функций.
- Модуль интерфейса к электронной почте.

Вторая часть системы Шифр- PKI – средства расширения функциональности системы следующего состава:

- Модуль – агент регионального центра сертификации ключей (центр регистрации ключей).
- Модуль управления ключами клиента.
- Модуль – служба доступа к справочнику сертификатов.
- JAVA - модуль криптографических функций для операционных сред, отличных от Win32;
- комплекс средств защиты TSP/IP трафика (строгая аутентификация, шифрование).

### Краткая характеристика

Система обеспечивает:

- генерацию криптографических ключей;
- управление сертификатами открытых ключей пользователей и персонала автоматизированных систем и комплексов;
- криптографическую защиту данных в распределенных автоматизированных системах и комплексах различного назначения.

Система Шифр-PKI поддерживает ключи следующих типов:

- ключи цифровой подписи – секретные и открытые ключи стандарта ГОСТ 34310-95;
- ключи шифрования данных – симметричные ключи стандарта ГОСТ 28147-89.
- ключи управления - ключи шифрования данных, выработанные в соответствии с требованиями протокола Диффи-Хеллмана.

Генерацию криптографических ключей пользователей и персонала автоматизированных систем и комплексов обеспечивают:

- **Модуль генерации ключей** (для исполнителей центрального офиса, филиала, где устанавливается региональный центр сертификации ключей).
- **Модуль – агент регионального центра сертификации ключей** (для территориально-удаленных подразделений, например ТОБО банков).
- **Модуль управления ключами клиента** (для исполнителей – должностных лиц удаленного клиента).

Генерация криптографических ключей в системе выполняется по принципу «сам для себя». Средства генерации ключей позволяют осуществить выбор носителя (HDD, 3,5 ГМД, Touch Memory (iButton), смарт-карта) для сохранения секретных ключей. Секретные ключи сохраняются на носителе в зашифрованном виде. Шифрование выполняется на ключе, который вырабатывается на основе личного пароля владельца секретных ключей. Открытые ключи в виде запроса на сертификацию передаются в сертификационный центр, где вырабатывается сертификат открытых ключей пользователя.

**Управление ключами и сертификатами** пользователей обеспечивают:

- **АРМ главного центра сертификации ключей** (в центральном офисе).
- **АРМ регионального центра сертификации ключей** (в центральном офисе и филиале).
- **Модуль – агент регионального центра сертификации ключей** (в территориально-удаленных подразделениях, например ТОБО банка).
- **Модуль управления ключами клиента** (у клиентов банка).
- **Модуль интерфейса к электронной почте.**
- **Модуль – служба доступа к справочнику сертификатов.**

При управлении сертификатами открытых ключей пользователей и персонала автоматизированных систем и комплексов средства системы обеспечивают:

- подтверждение достоверности и отправку запросов на сертификацию;
- сертификацию содержащихся в запросе открытых ключей;
- адресную рассылку сертификатов;
- контроль сроков действия сертификатов (ввод в действие и вывод из действия сертификатов в соответствии с назначенным сроком);
- отзыв сертификатов;
- формирование и рассылку списков отозванных сертификатов;
- прекращение действия сертификатов на основе данных списка отозванных сертификатов;
- сервисные функции (отображение таблиц сертификатов, поиск сертификатов по различным критериям, перенос выведенных из действия сертификатов в архив, и др.).

Доставку ключевых и служебных сообщений в процессе управление сертификатами обеспечивает **Модуль интерфейса к электронной почте**, который реализует протоколы SMTP и POP3. Кроме этого, данный модуль может использоваться для раскладки ключевых сообщений по заданным каталогам, что позволяет использовать его при обмене файлами по протоколу FTP.

**Модуль – служба доступа к справочнику сертификатов** предназначен для обеспечения удаленного доступа к таблице справочника сертификатов по протоколу TCP/IP.

**Исполнительные устройства системы:**

- **Модуль криптографических функций** (динамические библиотеки для WIN32)

- *JAVA - модуль криптографических функций для операционных сред, отличных от Win32*
- *комплекс средств защиты TCP/IP трафика «EProxu»* (строгая аутентификация, шифрование).

*Модули криптографических функций* реализованы в виде динамических библиотек (\*.DLL для WIN32) или в виде JAVA-классов, которые легко встраиваются в программные средства автоматизированных систем и в процессе работы обеспечивают:

- ввод секретного ключа, его расшифрование и сохранение в памяти;
- остановку работы при несоответствии введенного секретного ключа хранящемуся в справочнике сертификату, либо если использование этого сертификата запрещено;
- поиск в справочнике и выбор сертификата, требуемого для выполнения криптопреобразований;
- проверку аутентичности и полномочности выбранного сертификата;
- хэширование данных;
- постановку и проверку электронной цифровой подписи;
- выработку ключей связи по протоколу Диффи-Хеллмана;
- генерацию ключей шифрования данных;
- выработку имитовставки и шифрование данных;
- расшифрование данных и
- контроль их целостности путем проверки имитовставки.

*Комплекс средств защиты TCP/IP трафика «EProxu»* предназначен для строгой взаимной аутентификации источника передачи и приемника данных (сторон) в процессе установления TCP/IP соединения и создания защищенного шифрованием канала связи между сторонами.

Источник передачи и приемник данных - элементы клиент – серверной системы, обмен данными между которыми выполняется по протоколу TCP/IP.

#### **Особенности реализации**

*Главной особенностью реализации системы «Шифр-РКИ» является применение механизма профилирования сертификатов.*

Профиль сертификата – это однозначно идентифицируемая, именованная совокупность общих свойств сертификатов (полномочия, назначение, срок действия, место сертификации и т.д.), позволяющая объединить сертификаты в определенную группу.

Все сертификаты, которые создаются в системе, генерируются на основе конкретного профиля. Разработчиком созданы и применяются при адаптации средств системы под конкретные требования Заказчика:

- специальные средства формирования и редактирования профилей сертификатов,
- средства настройки визуальных компонентов интерактивных программных средств, обеспечивающих диалог пользователя с программами в процессе управления сертификатами с заданным профилем (генерация ключей, формирование и обработка запросов на сертификацию, формирование сертификатов и управление ими).

Благодаря этому средства системы «Шифр-РКИ» гибко и органично вписываются практически в любые автоматизированные системы Заказчика, будучи фактически независимыми от их технологических и функциональных свойств.

*Другой, не менее важной особенностью реализации системы «Шифр-РКИ» является наличие встроенных механизмов формирования и настройки правил рассылки сертификатов и стоп-листов (списков отозванных сертификатов).* Средства системы позволяют, как Разработчику на этапе адаптации системы по требованиям Заказчика, так и

пользователям в процессе эксплуатации системы, создавать и изменять правила, по которым ГЦСК и/или РЦСК автоматически отправят выработанный сертификат (стоп-лист) заданному получателю, либо заданной группе получателей. Сертификаты (стоп-листы) рассылаются в виде *ключевых сообщений*.

Ключевые сообщения - это сообщения определенного формата, которые могут содержать запросы на сертификацию, сертификаты, либо стоп-листы. Ключевые сообщения обеспечивают обмен открытыми ключевыми данными в рамках системы «Шифр-РКІ» (между ГЦСК, РЦСК, другими получателями ключевых сообщений). Все ключевые сообщения подписываются цифровой подписью отправителя и квитируются получателем при их приеме.

Получателями ключевых сообщений являются владельцы сертификатов, имеющие полномочия получать запросы на сертификацию, сертификаты и сообщения об отмене сертификатов. Данные полномочия закрепляются в профиле, на основе которого создан сертификат владельца. В системе «Шифр-РКІ» получателями ключевых сообщений могут быть ГЦСК, РЦСК, Модуль-агент РЦСК, Модуль генерации ключей удаленного пользователя.

Доставка ключевых сообщений может выполняться *Модулем интерфейса к электронной почте*, который входит в комплект поставки системы «Шифр-РКІ», либо любыми другими транспортными средствами Заказчика.

**Третьей особенностью является порядок организации доступа к сертификатам открытых ключей.** Исполнительные устройства системы (Модуль криптографических функций, JAVA - модуль криптографических функций, комплекс средств защиты ТСП/Р трафика) при выполнении криптопреобразований используют сертификаты открытых ключей, которые хранятся в справочнике сертификатов. Доступ к сертификатам в справочнике может осуществляться двумя способами:

- первый способ – прямой (разделяемый) доступ к файлу таблицы справочника сертификатов;
- второй способ – через *Модуль – службу доступа к справочнику сертификатов* по протоколу ТСП/Р.

#### **Легитимность**

Все криптографические преобразования в системе Шифр-РКІ (генерация симметричных ключей, ключевых асимметричных пар, выработка ключей управления, цифровая подпись, шифрование, выработка имитовставки и хэш-функции) выполняются при помощи сертифицированного программного изделия «Шифр» (**сертификаты соответствия по Реестру УкрСЕПРО № UA.1.112.14243-01 от 15.06.2001г., № UA.1.112.60011-03 от 17.07.2003, АБ № 176531 от 28.10.2005г.**).