УТВЕРЖДЕН
ЖТЯИ.00035-01 90 13-ЛУ

ЖТЯИ.00035-01 90 13

КриптоПро УЦ

программно–аппаратный комплекс
удостоверяющий центр

Руководство по регистрации дополнительных идентификаторов областей применения сертификатов открытых ключей

СОДЕРЖАНИЕ

1. Введение 3

2. Получение и регистрация частного номера организации 3

3. Формирование объектных идентификаторов областей применения сертификатов открытых ключей 3

4. Регистрация объектных идентификаторов в операционной системе Центра Сертификации и Центра Регистрации 4

4.1. Регистрация объектных идентификаторов путем корректировки системного реестра 4

4.2. Регистрация объектных идентификаторов путем исполнения программного модуля 5

5. Настройка программного обеспечения ПК «КриптоПро УЦ» 5

5.1. Настройка программного обеспечения Центра Сертификации 5

5.2. Настройка программного обеспечения Центра Регистрации 5

5.2.1. Настройка шаблонов сертификатов 5

5.2.2. Настройка политики обработки неподписанных запросов 6

5.2.3. Настройка политики обработки подписанных запросов 6

6. Обеспечение пользователей УЦ информацией по объектным идентификаторам 7

1. Введение

Каждая область применения сертификатов открытых ключей в программном комплексе «Удостоверяющий Центр «КриптоПро УЦ» представляет собой объектный идентификатор, соответствующий рекомендациям «Simple Network Management Protocol (SNMP)» (RFC 1098).

Объектные идентификаторы областей применения сертификатов открытых ключей заносятся в качестве значений расширений типа ExtendedKeyUsage сертификата открытого ключа. На данные расширения возлагается смысловая интерпретация сведений об отношениях, при которых электронный документ имеет юридическую силу, в соответствии с требованиями Федерального закона РФ «Об электронной цифровой подписи».

Информация о разработчике ПК «КриптоПро УЦ»:

ООО "Крипто-Про"

127 018, Москва, улица Сущевский вал, 16 строение 5

Телефон: (495) 780 4820

Факс: (495) 780 4820

http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru

2. Получение и регистрация частного номера организации

Для обеспечения однозначной идентификации областей использования сертификатов необходимо выполнить процедуру получения и регистрации частного номера организации.

Получение частного номера организации может быть осуществлено из российского сегмента мирового пространства идентификаторов либо непосредственно из мирового пространства идентификаторов путем подачи заявки в Агентство по выделению имен и уникальных параметров протоколов Internet (IANA [Internet Assigned Numbers Authority]).

Данное Агентство является уполномоченным органом Общества Internet (ISOC) и Федерального Совета сети (FNC)). Получение и регистрация частного номера организации осуществляется заявительным порядком, путем заполнения и отправки прикладной формы на веб-сервере Агентства (http://www.iana.org/). Текущий список зарегистрированных номеров организаций можно получить по адресу http://www.iana.org/assignments/enterprise-numbers.

Регистрация частного номера организации в российском сегменте мирового пространства идентификаторов осуществляется Уполномоченным федеральным органом исполнительной власти РФ по применению ЭЦП. С информацией по регистрации и занесению частного номера в Реестр идентификаторов объектов российского сегмента мирового пространства идентификаторов можно ознакомиться на сайте www.reestr-pki.ru.

3. Формирование объектных идентификаторов областей применения сертификатов открытых ключей

После получения и регистрации номера организации, организация, эксплуатирующая ПК «КриптоПро УЦ» и являющаяся владельцем Удостоверяющего

Центра, самостоятельно формирует объектные идентификаторы в соответствии с RFC 1098.

Например:

Частный номер организации: 66666

1.3.6.1.4.1.66666 – ООО «Рога и копыта»

1.3.6.1.4.1.66666.1 – интернет-магазин ООО «Рога и копыта» для организаций

1.3.6.1.4.1.66666.1.1 – генеральный директор организации, являющийся покупателем в системе интернет-магазин ООО «Рога и копыта»

1.3.6.1.4.1.66666.1.2 – главный бухгалтер организации, являющийся покупателем в системе интернет-магазин ООО «Рога и копыта»

1.3.6.1.4.1.66666.1.3 – генеральный директор ООО «Рога и копыта» в системе интернет-магазин ООО «Рога и копыта»

1.3.6.1.4.1.66666.1.4 – главный бухгалтер ООО «Рога и копыта» в системе интернет-магазин ООО «Рога и копыта»

1.3.6.1.4.1.66666.1.5 – администратор системы интернет-магазин ООО «Рога и копыта»

Рекомендации:

Рекомендуется сформировать таблицу соответствия областей применения сертификатов открытых ключей объектным идентификаторам и утвердить ее установленным в организации порядком, а также включить данную таблицу в форму соглашения с пользователями Удостоверяющего Центра (например, в виде приложения).

4. Регистрация объектных идентификаторов в операционной системе Центра Сертификации и Центра Регистрации

Перед настройкой программного обеспечения Центра Сертификации и Центра Регистрации ПК «КриптоПро УЦ» на предмет использования дополнительных областей использования сертификатов открытых ключей, необходимо произвести процедуру регистрации соответствующих объектных идентификаторов в операционных системах серверов Центра Сертификации и Центра Регистрации.

4.1. Регистрация объектных идентификаторов путем корректировки системного реестра

Корректировка системного реестра Windows выполняется с использованием штатных средств Windows 2000 Server, а именно утилиты **regedit**.

Регистрация объектных идентификаторов путем корректировки системного реестра выполняется следующим образом:

1. С использованием утилиты **regedit** откройте раздел реестра с именем **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo**
2. Выполните задачу **Создать** -> **Раздел** из контекстного меню
3. Введите имя раздела соответствующее конкатенации строкового представления значения **объектного идентификатора** и строки **!7** (например: 1.3.6.1.4.1.66666.1.1!7)
4. Для созданного раздела выполните задачу **Создать** -> **Строковый параметр** из контекстного меню

5. В качестве значения имени параметра задайте значение **Name**
6. В качестве значения строкового параметра введите описание объектного идентификатора (области использования сертификата)
7. Повторите шаги с 1 по 6 для каждой дополнительной области использования сертификатов
8. Перезагрузите сервер после корректировки системного реестра

4.2. Регистрация объектных идентификаторов путем исполнения программного модуля

Для регистрации объектных идентификаторов в операционной системе можно разработать исполняемый программный модуль в виде .EXE файла.

При разработке программного модуля рекомендуется использовать функции поддержки OID из состава вспомогательных (Auxiliary) функций CryptoAPI 2.0:

- CryptRegisterOIDInfo
- CryptRegisterOIDFunction

5. Настройка программного обеспечения ПК «КриптоПро УЦ»

Настройка программного обеспечения ПК «КриптоПро УЦ» осуществляется путем последовательной настройки программных компонент Центра Сертификации и Центра Регистрации.

5.1. Настройка программного обеспечения Центра Сертификации

Настройка программного обеспечения Центра Сертификации ПК «КриптоПро УЦ» осуществляется путем настройки модуля политики КриптоПро УЦ службы сертификации Microsoft Windows 2000.

Настройка осуществляется на вкладке **Использование ключа** путем добавления дополнительных идентификаторов из числа зарегистрированных в соответствии с разделом 4 настоящего Руководства в **Список идентификаторов области использования**.

Для каждого добавляемого идентификатора необходимо задать параметр, определяющий срок действия сертификата открытого ключа. Значение данного параметра определяется, исходя из требований Регламента Удостоверяющего Центра, и не должно превышать значения параметра, определяющего максимально разрешенный срок действия сертификата открытого ключа.

5.2. Настройка программного обеспечения Центра Регистрации

Настройка программного обеспечения Центра Регистрации ПК «КриптоПро УЦ» осуществляется путем настройки параметров Центра регистрации с использованием приложения «Параметры Центра Регистрации», входящего в состав программного обеспечения ПК «КриптоПро УЦ».

Настройка параметров Центра регистрации осуществляется в окне свойств модуля доступа Центра Регистрации.

5.2.1. Настройка шаблонов сертификатов

Настройка шаблонов сертификатов осуществляется на вкладке **Политики** окна свойств модуля доступа Центра Регистрации.

Выберите тип политики **Шаблоны сертификатов** и нажмите кнопку **Настроить**.

Добавьте дополнительные объектные идентификаторы областей применения сертификатов открытых ключей в список областей применения сертификатов существующих или новых шаблонов сертификатов.

Рекомендации:

Если на Удостоверяющем Центре реализована процедура регистрации пользователей, при которой первый сертификат, издаваемый для пользователя, является служебным сертификатом, то в шаблон служебного сертификата открытого ключа дополнительные объектные идентификаторы областей применения сертификатов не добавляются.

5.2.2. Настройка политики обработки неподписанных запросов

Политика обработки неподписанных запросов применяется при постановке запроса на сертификат открытого ключа в очередь на Центре Регистрации с использованием метода **SubmitFirstCertRequest** объекта **CertRequest** Интерфейса Внешних Приложений Центра Регистрации.

Из компонентов ПК «КриптоПро УЦ» данный метод используют:

- АРМ администратора ЦР при выполнении следующих задач:
  - Создать нового пользователя;
  - Создать новый сертификат для пользователя.
- АРМ пользователя при заочной (удаленной) регистрации.

Для настройки политики обработки необходимо:

- Выбрать тип политики **Обработка неподписанных запросов** и нажать кнопку **Настроить**.
- Для каждой роли, которой нужно разрешить постановку в очередь запросов на сертификат, содержащих дополнительные области применения сертификатов, выполнить следующие действия:
  - Выбрать роль
  - Нажать кнопку **Изменить**
  - В появившемся окне нажать кнопку **Добавить**
  - Выбрать дополнительный объектный идентификатор по описанию из списка.
  - Нажать кнопку **ОК**
  - Повторить операцию **Добавить** для остальных дополнительных идентификаторов
- Нажатием кнопки ОК закрыть последовательно все окна политики **Обработка неподписанных запросов.**

Рекомендации:

Если на Удостоверяющем Центре реализована процедура заочной (удаленной) регистрации пользователей, при которой первый сертификат, издаваемый для пользователя, является служебным сертификатом, то для роли **Прошедший проверку** дополнительные объектные идентификаторы областей применения сертификатов не добавляются.

Если на Удостоверяющем Центре реализована процедура централизованной (очной) регистрации пользователей администратором, работающим под ролью **Оператор**, при которой первый сертификат, издаваемый для пользователя, является служебным сертификатом, то для роли **Оператор** дополнительные объектные идентификаторы областей применения сертификатов не добавляются.

5.2.3. Настройка политики обработки подписанных запросов

Политика обработки подписанных запросов применяется при постановке запроса на сертификат открытого ключа в очередь на Центре Регистрации с использованием метода **SubmitCertRequest** объекта **CertRequest** Интерфейса Внешних Приложений Центра Регистрации.

Из компонентов ПК «КриптоПро УЦ» данный метод используют:

- АРМ администратора ЦР при выполнении следующих задач:
  - Плановая смена сертификата администратора
- АРМ зарегистрированного пользователя.

Для настройки политики обработки необходимо:

- Выбрать тип политики **Обработка подписанных запросов** и нажать кнопку **Настроить**.
- Для каждой роли, которой нужно разрешить постановку в очередь запросов на сертификат, содержащих дополнительные области применения сертификатов, выполнить следующие действия:
  - Выбрать роль
  - Нажать кнопку **Изменить**
  - В появившемся окне нажать кнопку **Добавить**
  - Выбрать дополнительный объектный идентификатор по описанию из списка.
  - Нажать кнопку **ОК**
  - Повторить операцию **Добавить** для остальных дополнительных идентификаторов
- Нажатием кнопки ОК закрыть последовательно все окна политики **Обработка подписанных запросов.**

Рекомендации:

Если Удостоверяющий Центр не осуществляет взаимодействие с пользователя с использованием АРМов пользователя (через веб-приложения), то рекомендуется удалить разрешения в политиках обработки неподписанных и подписанных запросов для следующих ролей:

- Прошедший проверку;
- Пользователь.

6. Обеспечение пользователей УЦ информацией по объектным идентификаторам

Пользователи УЦ, как правило, являются пользователями прикладных информационных систем, в которых применяются средства и спецификации, предоставляемые Удостоверяющим Центром.

Одним из таких средств является сертификат открытого ключа.

В процессе взаимодействия пользователей прикладных информационных систем, достаточно часто возникает задача просмотра свойств сертификата открытого ключа с использованием диалоговых средств, реализованных компонентами операционной системы Windows.

При просмотре расширений ExtendedKeyUsage (оригинальный перевод Microsoft – Улучшенный ключ) в окне свойств отображаются строковые значения описания объектных идентификаторов указанных расширений.

Если объектные идентификаторы не будут зарегистрированы в операционной системе рабочего места пользователя, то в этом случае отображается непосредственно

значение объектного идентификатора, без его описательной части. Данное обстоятельство вызывает затруднение для пользователя в правильности интерпретации области использования сертификата открытого ключа, особенно при выполнении процедуры подтверждения подлинности ЭЦП в соответствии с действующим законодательством.

Техническим решением изложенной выше проблемы является:

- разработка программного модуля регистрации объектных идентификаторов областей использования сертификатов;
- предоставление свободного доступа пользователям прикладных систем к данному модулю с целью последующего его исполнения на рабочем месте пользователя.