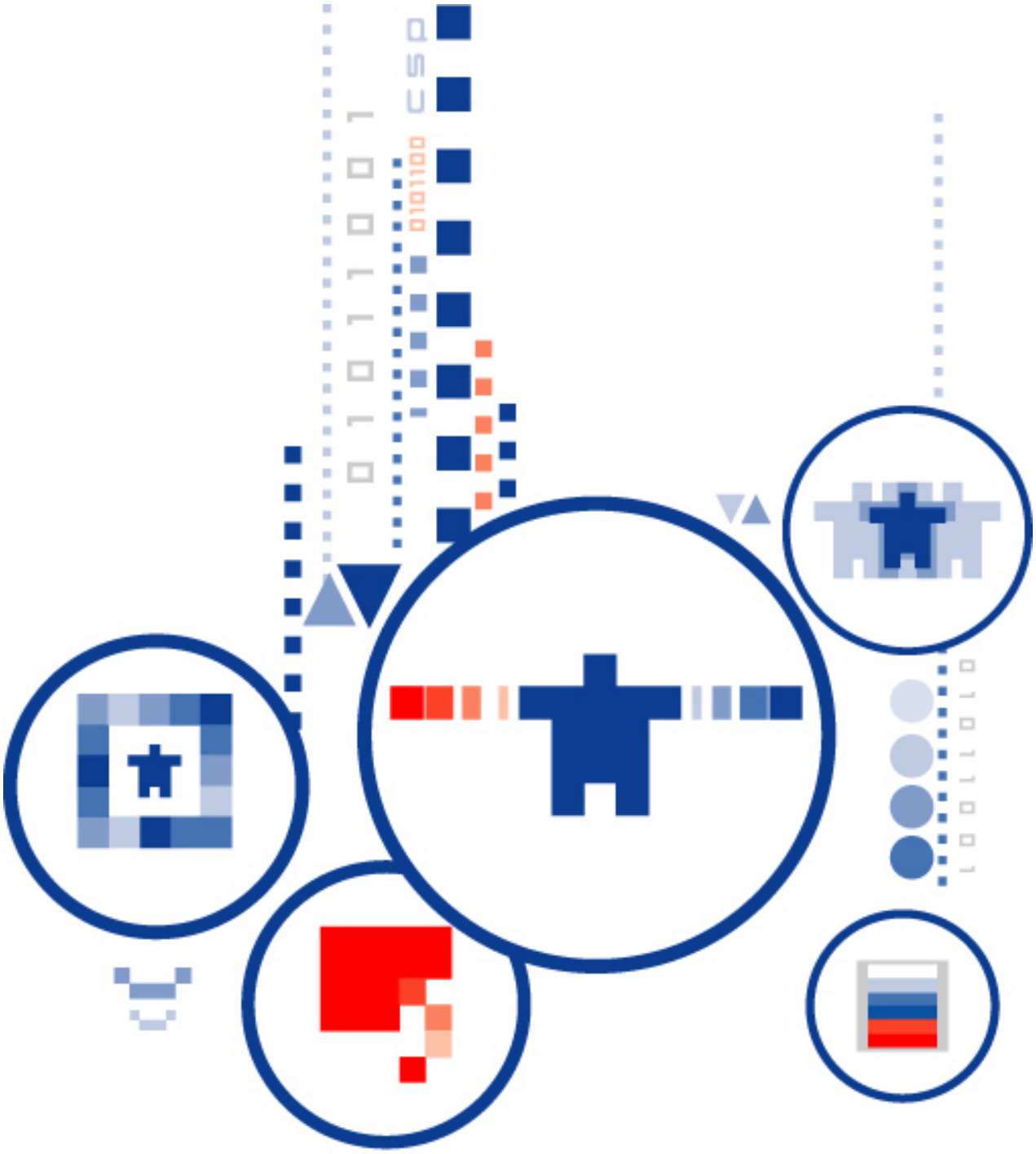
УТВЕРЖДЕН
ЖТЯИ.00035-01 90 14-ЛУ

ЖТЯИ.00035-01 90 14



КриптоПро УЦ

программно-аппаратный комплекс
удостоверяющий центр

Руководство по управлению системными ролями

АННОТАЦИЯ

Настоящий документ содержит описание настроек параметров Центра Сертификации и Центра Регистрации для управления системными ролями при эксплуатации программного комплекса «Удостоверяющий Центр «КриптоПро УЦ» (УЦ).

Существующая возможность использования ролевой модели при взаимодействии с Центром Регистрации через Интерфейс Внешних Приложений, значительно расширяет возможности построения адаптированных и гибких информационных систем с использованием сертификатов открытых ключей.

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

СОДЕРЖАНИЕ

1. Общее описание 4
2. Регистрация пользователя 6
2.1. Регистрация пользователей в централизованном режиме. 6
2.2. Регистрация пользователей в распределенном режиме. 8
3. Изготовление сертификата пользователя 9
3.1. Централизованное изготовление сертификата пользователя 9
3.2. Распределенное изготовление сертификата пользователя 9
4. Управление сертификатами пользователя. 12
5. Действия, связанные с получением данных, хранящихся в Удостоверяющем центре 13
6. Добавление новой системной роли. 14

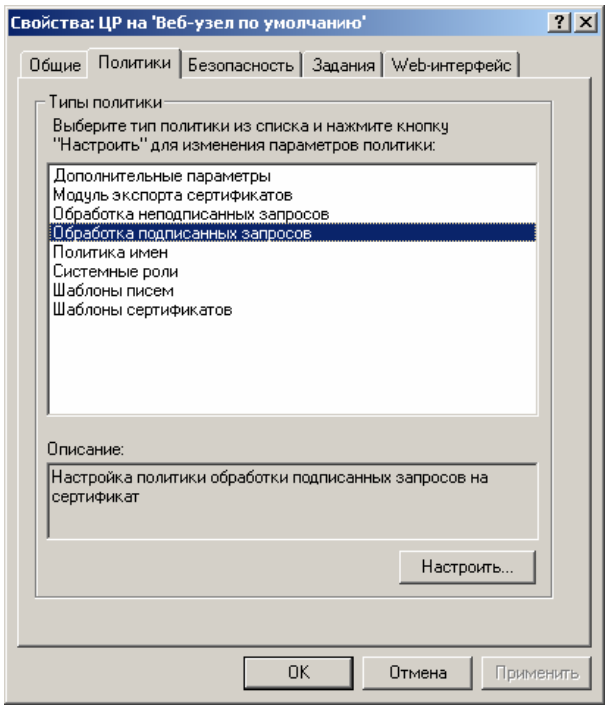
1. Общее описание

Настоящее Руководство рассматривает возможность использования реализованной в ПАК «КриптоПро УЦ» ролевой модели только с использованием компонент, входящих в состав ПАК «КриптоПро УЦ».

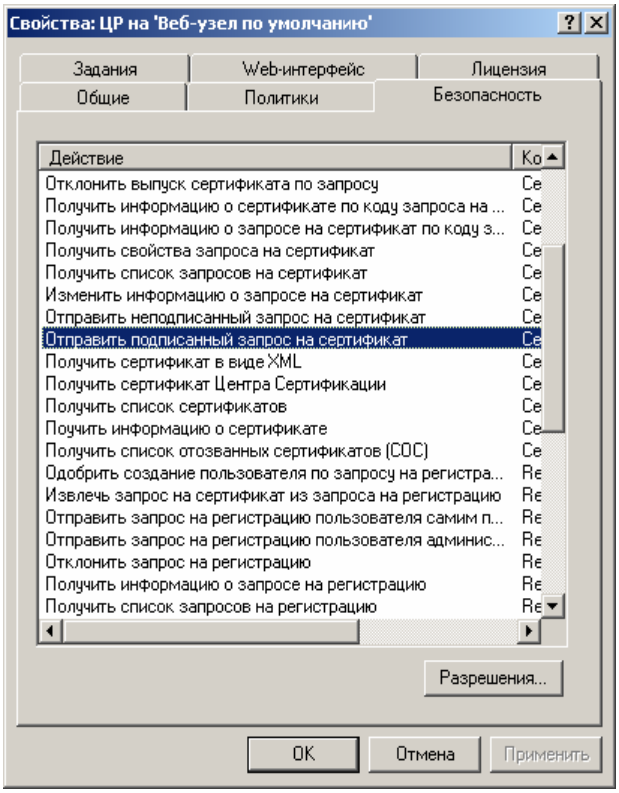
В «КриптоПро УЦ» реализована ролевая модель, и каждый пользователь Удостоверяющего Центра ассоциирован с соответствующей ролью.

Именно принадлежность пользователя к той или иной роли определяет действия, которые пользователь может осуществлять в Удостоверяющем Центре. Принадлежность пользователя к роли определяется содержанием идентификатора этой роли в области применения сертификата открытого ключа пользователя. Дополнительно введена роль, определяющие действия пользователей в Удостоверяющем центре, вообще не получивших ни одного сертификата: **Прошедший проверку**.

Возможные комбинации настроек политик Центра регистрации, прав доступа к действиям центра регистрации позволяют установить для каждой зарегистрированной роли конкретный набор действий, разрешенных/запрещенных в Удостоверяющем центре в соответствии с действующей политикой информационной безопасности.



Закладка настройки политик ЦР



Закладка настройки прав доступа к действиям ЦР

К основным действиям, осуществляемым пользователем в Удостоверяющем центре относятся:

1. Регистрация пользователя, включающая создание регистрационной записи в базе данных Центра регистрации и получение первого сертификата пользователя;
2. Изготовление сертификата пользователя;

3. Управление сертификатами пользователя;
4. Действия, связанные с получением данных, хранящихся в Удостоверяющем центре (информация о сертификатах зарегистрированных пользователей, информация о запросах, список отозванных сертификатов и т.д.).

2. Регистрация пользователя

Регистрация пользователя может быть осуществлена в двух режимах: централизованном (с использованием АРМ администратора) и распределенном (на рабочем месте пользователя с использованием АРМ регистрации).

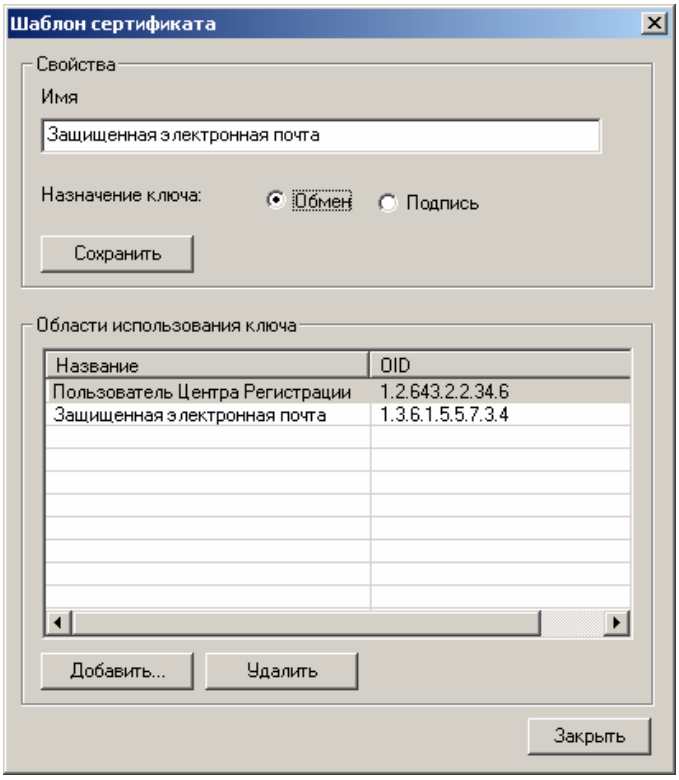
2.1. Регистрация пользователей в централизованном режиме.

Предустановленная настройка параметров Центра регистрации позволяет осуществлять централизованную регистрацию пользователя только пользователям, ассоциированным с ролью **Оператор**.

Ниже приведен список действий и установленных для них разрешений при регистрации пользователя **Оператором**:

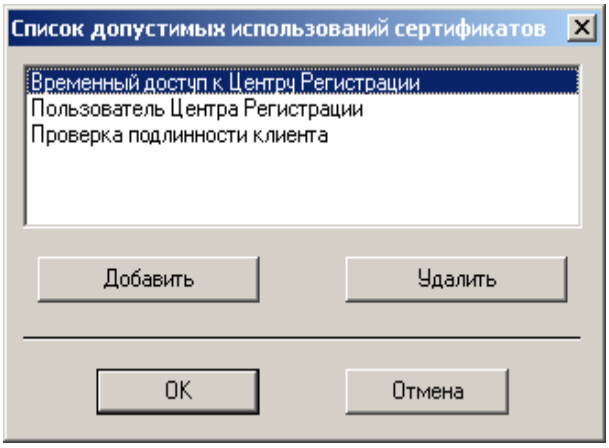
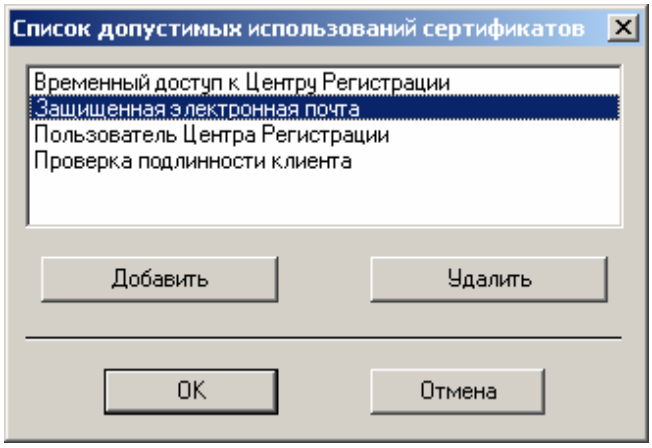
- отправить запрос на регистрацию пользователя администратором. При выполнении этого действия **Оператор** имеет право – Выполнение;
- одобрить создание пользователя по запросу на регистрацию. При выполнении этого действия **Оператор** имеет право – Делегирование, т.к. осуществляет это действие не от своего имени, а от имени другого пользователя;
- получить шаблоны сертификатов. При выполнении этого действия **Оператор** имеет право – Выполнение. **Оператор** выбирает необходимый шаблон сертификатов, содержащий области применения сертификата, которые требуется занести в сертификат.
- отправить неподписанный запрос на сертификат. При выполнении этого действия **Оператор** имеет право – Делегирование, т.к. отправляет запрос на сертификат не от своего имени, а от имени другого пользователя;
- одобрить выпуск сертификата по неподписанному запросу на сертификат. При выполнении этого действия **Оператор** имеет право – Делегирование, т.к. осуществляет одобрение не от своего имени, а от имени другого пользователя. В политике обработки неподписанных запросов для **Оператора** определяется список областей применения сертификата. Если запрос на сертификат содержал области применения, входящие в этот список (эти области определяются выбранным шаблоном сертификата), то сертификат будет издан, иначе запрос на сертификат будет отклонен и сертификат издан не будет.

  Например, **Оператор** изготавливает первый сертификат пользователя со следующими областями применения, входящими в шаблон «Защищенная электронная почта»: «Пользователь Центра регистрации», «Защищенная электронная почта».



Шаблон Защищенная электронная почта

Предустановленные настройки позволяют **Оператору** изготавливать сертификаты для пользователей только следующих областей применения: «Временный доступ к Центру регистрации», «Пользователь Центра регистрации» и «Проверка подлинности клиента», и данный запрос на сертификат будет отвергнут. Для формирования **Оператором** сертификата с областью применения «Защищенная электронная почта» необходимо добавить эту область в список допустимых использований сертификата роли **Оператор** в настройках политики обработки неподписанных запросов.

	
Предустановленные настройки обработки неподписанных запросов Оператора, не позволяющие изготовить сертификат по шаблону «Защищенная электронная почта»	Настройки обработки неподписанных запросов Оператора, позволяющие изготовить сертификат по шаблону «Защищенная электронная почта»

Если установить для этих действий аналогичные разрешения для роли Администратор, то пользователи, ассоциированные с ролью Администратор, также смогут осуществлять централизованную регистрацию пользователей с выдачей первого сертификата с областями использования, входящими в список областей использования сертификатов **Администратора** настройки политики обработки неподписанных запросов.

2.2. Регистрация пользователей в распределенном режиме.

Предустановленная настройка параметров Центра регистрации позволяет осуществлять распределенную регистрацию пользователей.

Ниже приведен список действий и установленных для них разрешений при распределенной регистрации пользователей:

- отправить запрос на регистрацию пользователя самим пользователем. При выполнении этого действия пользователь ассоциируется с ролью **Прошедший проверку**;
- одобрить создание пользователя по запросу на регистрацию. При выполнении этого действия роль **Прошедший проверку** имеет право – выполнение;
- получить шаблоны сертификатов. При выполнении этого действия роль **Прошедший проверку** имеет право – выполнение. Пользователь, ассоциированный с ролью **Прошедший проверку**, выбирает необходимый шаблон сертификатов, содержащий области применения сертификата, которые требуется занести в сертификат.
- отправить неподписанный запрос на сертификат. При выполнении этого действия роль **Прошедший проверку** имеет право – выполнение;
- одобрить выпуск сертификата по неподписанному запросу на сертификат. При выполнении этого действия роль **Прошедший проверку** имеет право – выполнение. В политике обработки неподписанных запросов для роли **Прошедший проверку** определяется список областей применения сертификата. Если запрос на сертификат имел поля, входящие в этот список, то сертификат будет издан, иначе запрос на сертификат будет отклонен и сертификат издан не будет. Предустановленные настройки позволяют роли **Прошедший проверку** изготавливать сертификаты только следующих областей применения: Временный доступ к Центру регистрации, Пользователь Центра регистрации и Проверка подлинности клиента. Например, для формирования сертификата с областью применения «Защищенная электронная почта» необходимо добавить эту область в данный список.

Предустановленная настройка параметров Центра Регистрации позволяет любому пользователю автоматически зарегистрироваться в Удостоверяющем центре и получить первый сертификат. Эту процедуру можно несколько усложнить, запретив пользователю одобрять создание пользователя и выпуск сертификата, а эти функции возложить на **Администратора**. Для этого необходимо добавить роль **Администратор** с разрешением – Делегирование для действия «одобрить создание пользователя» на регистрацию и удалить роль **Прошедший проверку** и добавить роль **Администратор** с разрешением – Делегирование для действия «одобрить выпуск сертификата по неподписанному запросу на сертификат». В этом случае пользователь не сможет зарегистрироваться в Удостоверяющем центре до тех пор, пока Администратор не одобрит регистрацию, и не сможет получить первый сертификат, пока Администратор не одобрит выпуск сертификата.

3. Изготовление сертификата пользователя

Изготовление сертификата пользователя может быть осуществлено в двух режимах: централизованном (с использованием АРМ администратора) и распределенном (на рабочем месте пользователя с использованием АРМ зарегистрированного пользователя).

3.1. Централизованное изготовление сертификата пользователя

Предустановленная настройка параметров Центра регистрации позволяет осуществлять централизованное изготовление сертификата пользователя следующим ролям: **Оператор** и **Администратор**. Отличие заключается в том, что для каждой роли определен свой список допустимых областей применения сертификатов в настройках политики неподписанных запросов. Например, администратор сможет изготовить сертификат с областью применения «Защищенная электронная почта», а Оператор нет. Эти списки можно расширить путем дополнения их необходимыми областями применения сертификатов.

Список действий и установленных для них разрешений при централизованном изготовлении сертификата пользователя:

- отправить неподписанный запрос на сертификат. При выполнении этого действия роли **Оператор** и **Администратор** имеют право – Делегирование;
- одобрить выпуск сертификата по неподписанному запросу на сертификат. При выполнении этого действия роли **Оператор** и **Администратор** имеют право – Делегирование.

Процедуру централизованного изготовления сертификата можно усложнить, запретив **Оператору** осуществлять одобрение выпуска сертификата по неподписанному запросу, исключив эту роль для данного действия. Данное действие повлечет за собой изменение предустановленного порядка централизованной регистрации пользователей, т.к. оно касается одного и того же действия, а именно – одобрить выпуск сертификата по неподписанному запросу на сертификат.

3.2. Распределенное изготовление сертификата пользователя

Предустановленная настройка параметров Центра регистрации позволяет осуществлять распределенное изготовление сертификата пользователя следующим ролям: **Пользователь ЦР**, **Оператор** и **Администратор**. Отличие заключается в том, что для каждой роли определен свой список допустимых областей применения сертификатов в настройках политики подписанных запросов.

Список действий и установленных для них разрешений при распределенном изготовлении сертификата пользователя:

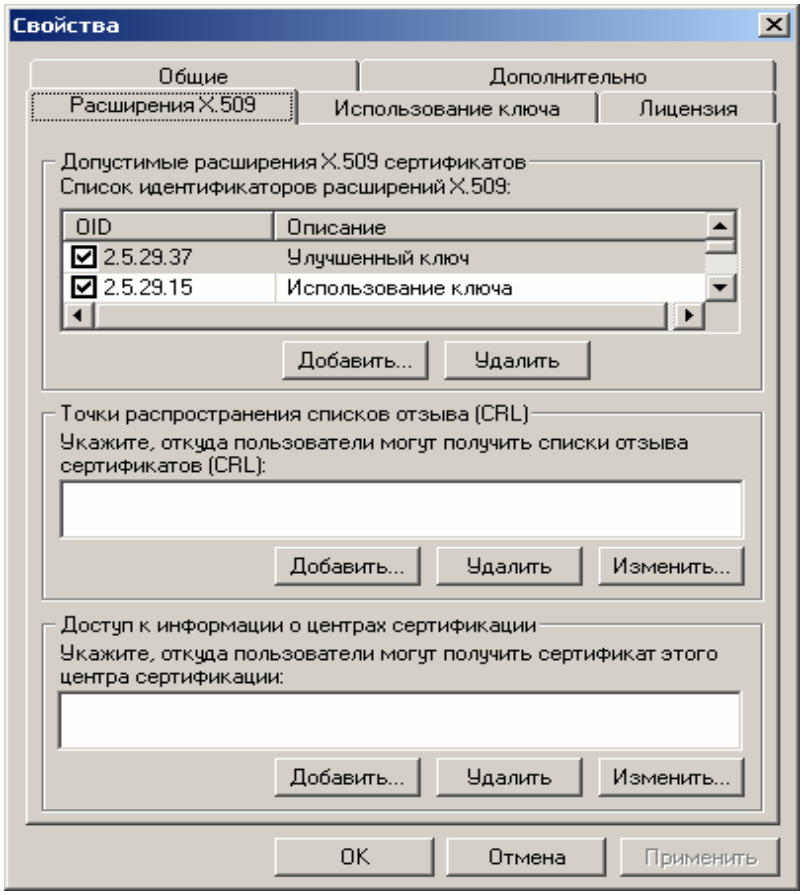
- отправить подписанный запрос на сертификат. При выполнении этого действия роли **Оператор**, **Администратор** и **Пользователь ЦР** имеют право – Выполнить;
- одобрить выпуск сертификата по подписанному запросу на сертификат. При выполнении этого действия роли **Оператор**, **Администратор** и **Пользователь** имеют право – Выполнить.

Предустановленная настройка параметров Центра Регистрации позволяет пользователю, ассоциированному с ролью **Пользователь ЦР** автоматически получать сертификат. Удалив роль **Пользователь ЦР** для действия «одобрить выпуск сертификата по подписанному запросу», пользователь, ассоциированный с этой ролью не сможет изготовить сертификат до тех пор, пока **Администратор** или **Оператор** не одобрят выпуск сертификата.

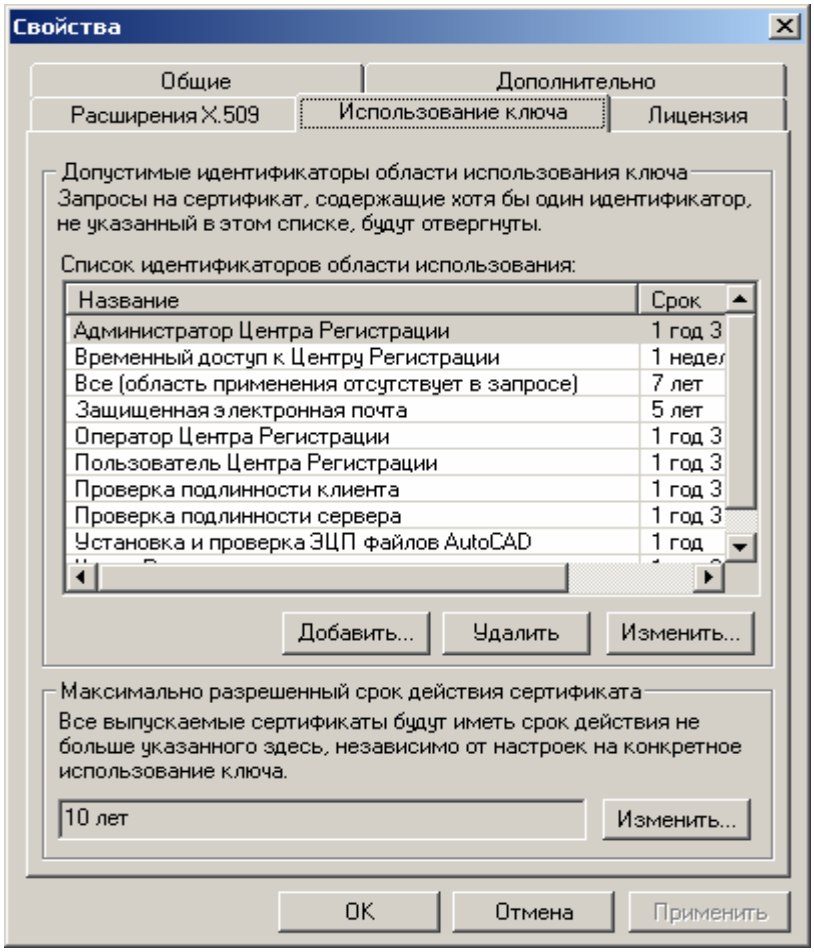
Если Регламентом Удостоверяющего центра не предусмотрено распределенное изготовление сертификатов для роли **Пользователь ЦР**, то для действия «отправить подписанный запрос на сертификат» требуется удалить эту роль.

В случае одобрения выпуска сертификата в Центре регистрации запрос поступает в Центр Сертификации Удостоверяющего центра. Сертификат будет изготовлен, если запрос удовлетворяет политике Центра Сертификации. Запрос должен содержать определенные в модуле политики расширения сертификата, и указанные в запросе на сертификат области использования ключа должны входить в список допустимых идентификаторов области использования ключа.

Например, если от Центра Регистрации поступает запрос на сертификат с областью использования - Аудит TLS трафика, а этой области использования нет в списке допустимых областей, то сертификат не будет издан.



Список допустимых расширений сертификата



Список допустимых идентификаторов области использования ключа

4. Управление сертификатами пользователя.

Под управлением сертификатами пользователя понимается возможность осуществлять отзыв, приостановление и возобновление действия сертификата. Данные действия могут быть осуществлены в двух режимах: централизованном (с использованием АРМ администратора) и распределенном (на рабочем месте пользователя с использованием АРМ зарегистрированного пользователя).

Различные варианты настройки разрешений для ролей относительно действий, связанных с осуществлением отзыва, приостановления и возобновления действия сертификата аналогичны описанным выше.

Например, для того чтобы только пользователь Удостоверяющего центра, ассоциированный с ролью **Пользователь ЦР** смог отозвать свой сертификат необходимо:

- для действия «отправить запрос на отзыв сертификата» добавить роль **Пользователь ЦР** с разрешением – Выполнение, а все оставшиеся роли исключить;
- для действия «одобрить запрос на отзыв сертификата» добавить роль **Пользователь ЦР** с разрешением – Выполнение, а все оставшиеся роли исключить;

Для того, чтобы пользователь Удостоверяющего центра (и никто другой), ассоциированный с ролью **Пользователь ЦР** имел возможность только отправлять запрос на отзыв своего сертификата, а только **Администратор** принимал решение по этому запросу необходимо:

- для действия «отправить запрос на отзыв сертификата» добавить роль **Пользователь ЦР** с разрешением – Выполнение, а все оставшиеся роли исключить;
- для действия «одобрить запрос на отзыв сертификата» добавить роль **Администратор** с разрешением – Делегирование, а все оставшиеся роли исключить;
- для действия «отклонить запрос на отзыв сертификата» добавить роль **Администратор** с разрешением – Делегирование, а все оставшиеся роли исключить.

5. Действия, связанные с получением данных, хранящихся в Удостоверяющем центре.

АРМ зарегистрированного пользователя, в отличие от АРМ администратора, менее функционален и предоставляет пользователю возможность применения только некоторых действий, предоставляемых Центром регистрации и связанных с получением данных, хранящихся в Удостоверяющем центре:

1. Получить список сертификатов;
2. Получить информацию о сертификате;
3. Получить сертификат в виде XML;
4. Получить список запросов на сертификат;
5. Получить список отозванных сертификатов;
6. Получить список запросов на отзыв сертификата;
7. Получить информацию о запросе на отзыв сертификата;
8. Получить сертификат Центра сертификации;
9. Получить шаблоны сертификатов.

Например, для того чтобы пользователь, ассоциированный с ролью **Пользователь ЦР**, мог получить список сертификатов, изготовленных Удостоверяющим центром и просматривать их, необходимо для следующих действий установить права:

- получить список сертификатов – для роли **Пользователь ЦР** – Выполнение;
- получить информацию о сертификате – для роли **Пользователь ЦР** – Выполнение и Делегирование

В приведенном примере пользователь, ассоциированный с ролью **Пользователь ЦР**, будет иметь возможность просматривать все сертификаты, включая свои и чужие. Для запрещения просмотра чужих сертификатов необходимо для действия получить информацию о сертификате для роли **Пользователь ЦР** установить только право Выполнение.

Аналогичным образом установление необходимых прав к действиям, доступным с АРМ администратора, позволяет разграничить доступ между ролями Администратора и Оператора.

6. Добавление новой системной роли.

Добавление новой системной роли УЦ выполняется в следующей последовательности:

1. Формирование объектного идентификатора системной роли
2. Регистрация объектного идентификатора системной роли в операционной системе Центра Сертификации и Центра Регистрации
3. Настройка программного обеспечения Центра Сертификации в части добавления объектного идентификатора системной роли в список допустимых областей использования ключа
4. Настройка программного обеспечения Центра Регистрации в части создания шаблона сертификата системной роли
5. Настройка программного обеспечения Центра Регистрации в части добавления объектного идентификатора системной роли в шаблон сертификата системной роли
6. Настройка политики обработки неподписанных запросов Центра Регистрации для обеспечения возможности администратору/оператору выпуска сертификата открытого ключа с данной системной ролью при его регистрации
7. Настройка политики обработки неподписанных запросов Центра Регистрации для обеспечения возможности системной роли выполнения задачи выпуска сертификата открытого ключа пользователя (при необходимости по регламенту УЦ)
8. Настройка политики обработки подписанных запросов Центра Регистрации для данной системной роли
9. Настройка прав доступа для данной системной области к задачам (методам) Центра Регистрации