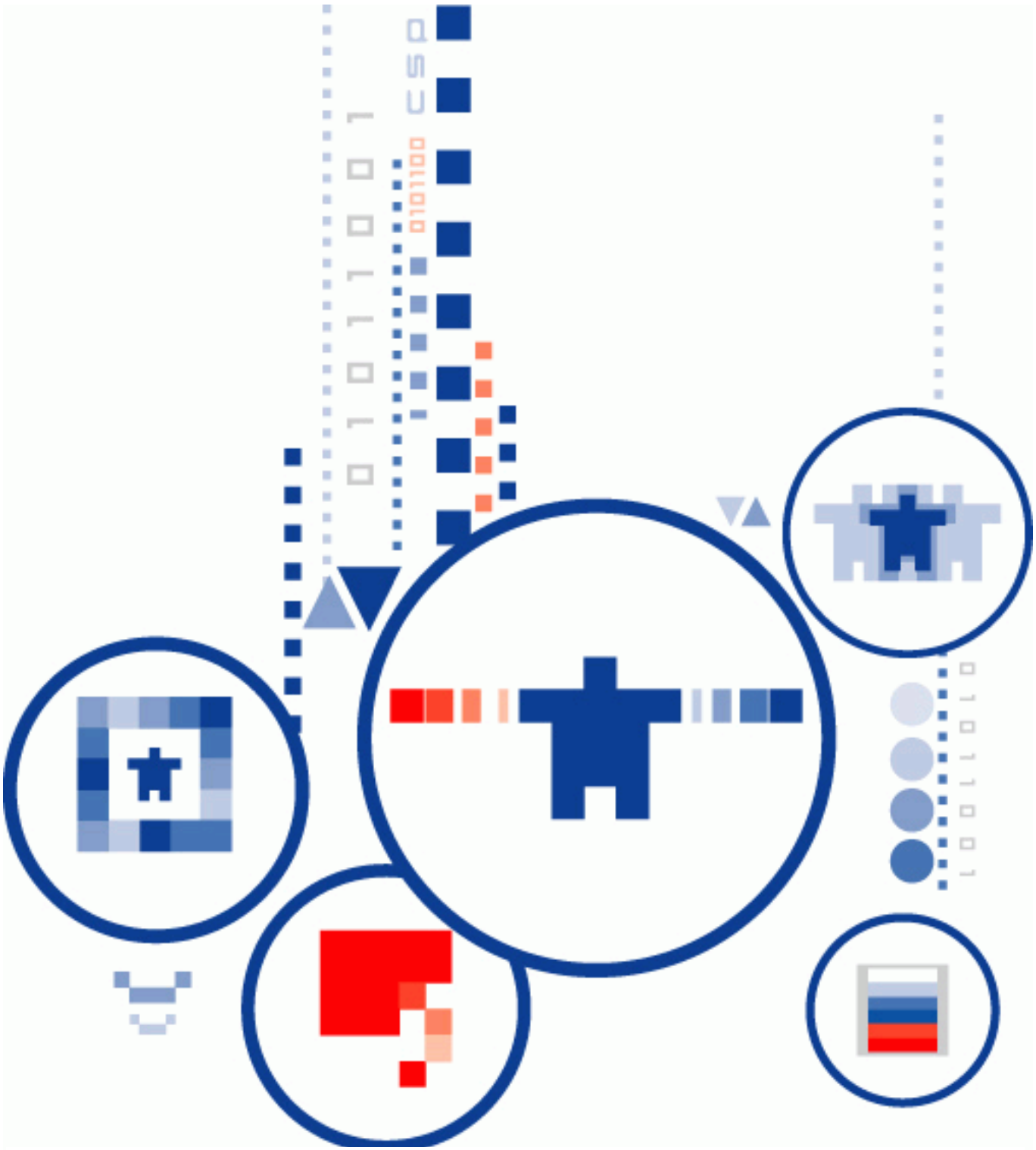


Настройка КриптоПро Winlogon в домене Windows с использованием КриптоПро УЦ

АННОТАЦИЯ

Настоящий документ содержит описание процедур настройки ПО и выпуска сертификатов с помощью **КриптоПро УЦ** для использования **КриптоПро Winlogon** в домене Windows.

Информация о разработчике:

ООО «Крипто-Про»

127 018, Москва, ул. Сущёвский вал, д. 16 строение 5

Телефон: (495) 780 4820

Факс: (495) 780 4820

http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Общие требования

Для функционирования КриптоПро Winlogon требуется, чтобы были правильно настроены рабочая станция для входа, домен и контроллеры домена. Домен должен доверять Удостоверяющему Центру (УЦ) аутентифицировать пользователей с помощью сертификатов данного УЦ. Рабочая станция для входа и контроллеры домена должны обладать правильно настроенными сертификатами.

Как и в любой реализации ИОК, все участники должны доверять корневому УЦ, который подписал сертификат выпускающего УЦ. Контроллеры домена и рабочие станции для входа должны доверять корневому УЦ.

Установка ПО и необходимые настройки для выполнения указанных требований описаны в последующих разделах.

2. Установка ПО

Для использования **КриптоПро Winlogon** на сертификатах, издаваемых **КриптоПро УЦ**, необходимо установить следующее ПО:

- на все контроллеры домена:
  - либо КриптоПро CSP 3.6 с лицензией, включающей режим KDC;
  - либо КриптоПро CSP 3.0 и КриптоПро Winlogon в режиме KDC
- на компьютеры клиентов:
  - либо КриптоПро CSP 3.6 с лицензией, включающей Winlogon клиент;
  - либо КриптоПро CSP 3.0 и КриптоПро Winlogon
- КриптоПро УЦ версии не ниже 1.4.

О требованиях к ОС и аппаратному обеспечению для перечисленного ПО см. документацию к соответствующим продуктам.

Обратите внимание, что КриптоПро Winlogon поддерживает не все виды смарт-карт (см. [CPWL]). В частности, смарт-карты Оскар, размеченные для КриптоПро CSP 1.1, не поддерживаются.

3. Настройка домена

3.1. Доверие к УЦ

Контроллеры домена и рабочие станции должны доверять УЦ для обеспечения возможности входа пользователей по сарткартам.

Если рассматриваемый УЦ, выпускающий сертификаты для входа со смарт-картой, является корневым, то его сертификат должен быть установлен в хранилища **Доверенные корневые центры сертификации** указанных компьютеров. Если же данный УЦ является подчинённым, то в это хранилище необходимо установить сертификат корневого УЦ, на котором заканчивается цепочка сертификатов выпускающего УЦ.

Описанную процедуру рекомендуется выполнить с использованием возможностей групповых политик домена Windows. Для этого в оснастке Групповые политики на контроллере домена в узле **Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Политики открытого ключа → Доверенные корневые центры сертификации** выполните импорт требуемого сертификата. Следует отметить, что файл импортируемого сертификата не должен содержать в себе цепочек сертификатов и СОС. После применения настроенной таким образом групповой политики на всех компьютерах домена данный сертификат появится в хранилище **Доверенные корневые центры сертификации**.

3.2. Разрешение аутентификации по сертификатам УЦ

Чтобы сертификаты, выпускаемые КриптоПро УЦ, могли использоваться для аутентификации в домене и входа со смарт-картой, домен должен явно доверять этому УЦ. Для этого в Active Directory в хранилище **NTAuth** должен быть прописан сертификат этого УЦ.

Чтобы поместить сертификат УЦ в это хранилище, сохраните его в файл и выполните следующую команду:

```
certutil –dspublish –f <filename> NTAuthCA
```

Здесь <filename> – имя файла с сертификатом.

Программа **certutil** устанавливается вместе со службами сертификации Microsoft на Windows 2000, а также присутствует в любой поставке Windows Server 2003. Для успешной публикации необходимо, чтобы учётная запись, под которой выполняется команда, входила в группу администраторов домена.

3.3. Обеспечение доступности сертификата УЦ второго уровня.

Если рассматриваемый УЦ, выпускающий сертификаты для входа со смарт-картой, является корневым, то его сертификат должен быть установлен в хранилища **Доверенные корневые центры сертификации** контроллеров домена и рабочих станций для входа. Если же данный УЦ является подчинённым, то возникает необходимость поиска его сертификата для подтверждения цепочки.

Для этого рекомендуется включение особого расширения **AIA (Доступ к информации о центре сертификации)** в сертификаты пользователей, выпущенные этим центром. Расширение AIA включает в себя путь к файлу сертификата данного центра сертификации, который должен быть доступен для всех пользователей.

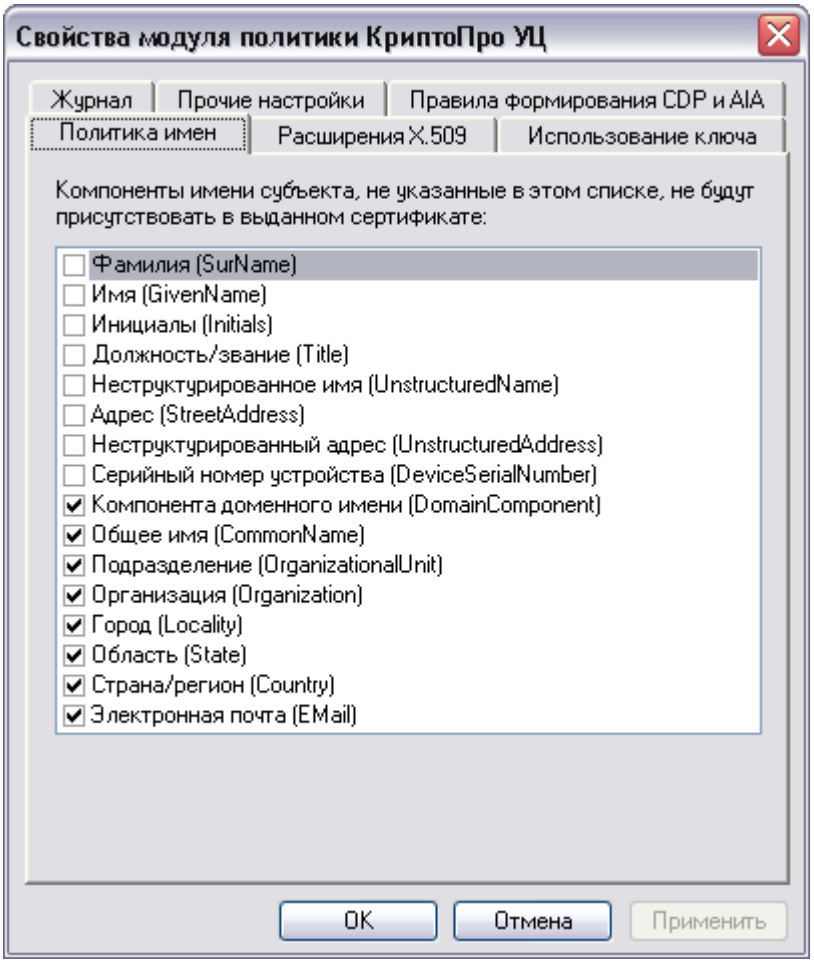
4. Настройка КриптоПро УЦ

4.1. Настройка Центра сертификации КриптоПро УЦ

Все описанные в этом разделе настройки Центра сертификации осуществляются с помощью модуля политики центра сертификации. Чтобы получить доступ к свойствам модуля политики, необходимо выполнить следующую последовательность действий:

1. Откройте оснастку **Центр сертификации** (она доступна в меню **Панель управления** → **Администрирование**).
2. Выберите настраиваемый центр сертификации и выберите пункт **Свойства** в контекстном меню.
3. Откройте вкладку **Модуль политики**, убедитесь, что выбран модуль политики КриптоПро УЦ, и нажмите кнопку **Свойства** (см. Рисунок 1).

Рисунок 1. Свойства модуля политики КриптоПро УЦ.



КриптоПро УЦ выпускает два типа сертификатов для рассматриваемого сценария:

1. Сертификаты контроллеров домена.
2. Сертификаты входа со смарт-картой.

Общим обязательным требованием к этим сертификатам является наличие в них точки распространения СОС (CDP – CRL Distribution Point). Для выполнения этого требования настройте точку CDP в модуле политики Центра Сертификации КриптоПро УЦ, если таковой ещё нет.

Для этого на вкладке **Правила формирования CDP и AIA** нажмите кнопку **Добавить** и создайте необходимое правило.

Если по каким-то причинам ваш УЦ настроен таким образом, что он не включает CDP в сертификаты, вы можете ограничиться включением CDP только в указанные выше типы сертификатов путём соответствующей настройки правил включения CDP. Критерием отличия данных сертификатов от других может служить поле EKU (Extended Key Usage): **Вход со смарт-картой** для пользователей и **КриптоПро УЦ, Контроллер домена (winlogon)** для контроллеров домена.

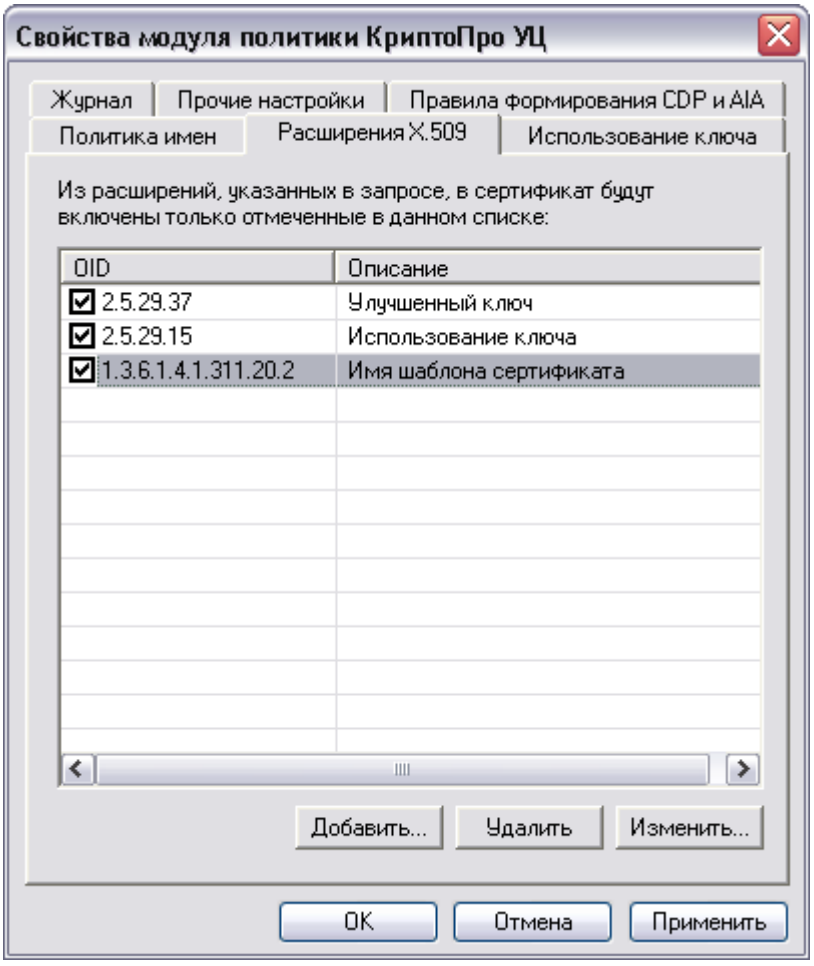
Для удобства выпуска сертификатов пользователя на АРМ Администратора, в ЦР включены шаблоны сертификатов **Сертификат входа со смарт-картой** и **Сертификат контроллера домена (winlogon)**. При создании запросов на сертификаты с использованием этих шаблонов, информация о типе запрашиваемого сертификата добавляется в расширение **Имя шаблона сертификата (CertTemplate)**.

Расширение **Имя шаблона сертификата** будет содержать значение **DomainController** для контроллера домена и значение **SmartcardUser** для пользователя.

Для корректной обработки запросов на такие сертификаты в настройках центра сертификации необходимо добавить расширение **Имя шаблона сертификата** в список расширений, включаемых в сертификат.

Для этого на вкладке **Расширения X.509** нажмите кнопку **Добавить** и добавьте расширение **OID 1.3.6.1.4.1.311.20.2 (Имя шаблона сертификата)** (см. Рисунок 2).

Рисунок 2. Список расширений, включаемых в сертификат.



Убедитесь, что на вкладке **Прочие настройки** включена опция **Добавлять расширение 2.5.29.17 ("Дополнительное имя субъекта") в сертификат входа со смарт-картой на основании информации из запроса** (настройка по умолчанию).

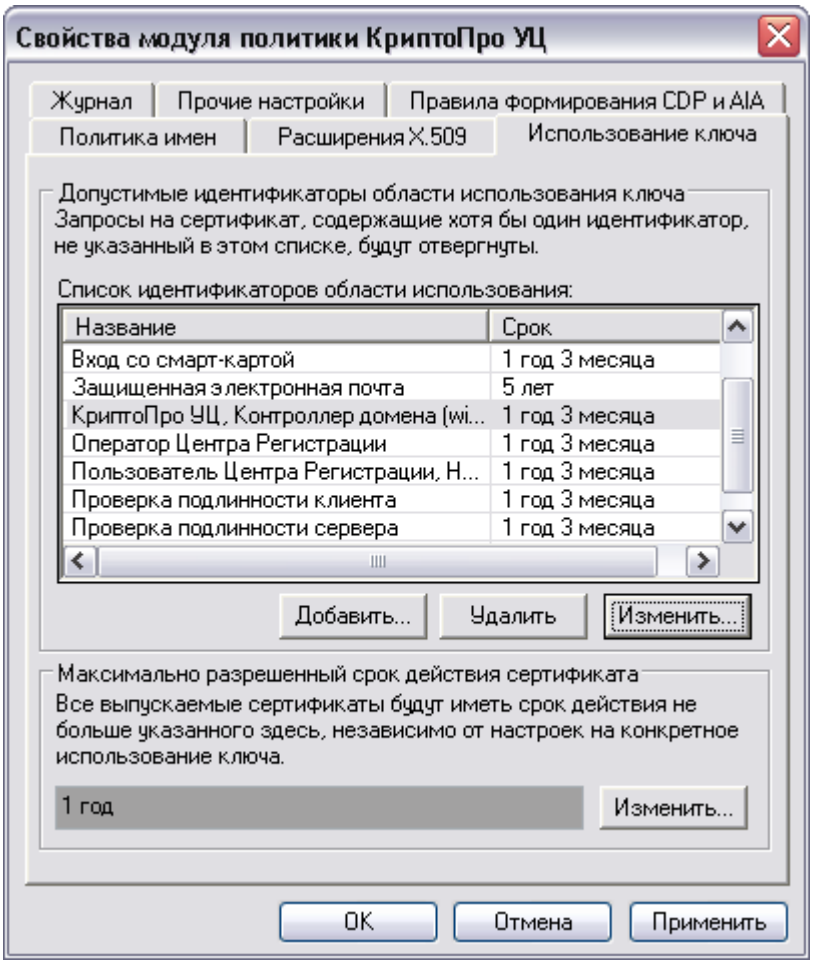
В этом случае при обработке запросов модуль политики ЦС будет перекладывать информацию из расширения **Имя шаблона сертификата** запроса в сертификат. При этом если запрошен EKU **Вход со смарт-картой**, то данное расширение должно содержать UPN, если же

запрошен EKU **КриптоПро УЦ, Контроллер домена (winlogon)**, то данное расширение должно содержать GUID и DNS-имя контроллера домена.

Кроме того, необходимо на вкладке **Использование ключа** добавить допустимые значения EKU (см. Рисунок 3):

- Вход со смарт-картой;
- КриптоПро УЦ, Контроллер домена (winlogon);
- Проверка подлинности клиента;
- Проверка подлинности сервера.

Рисунок 3. Допустимые значения EKU.

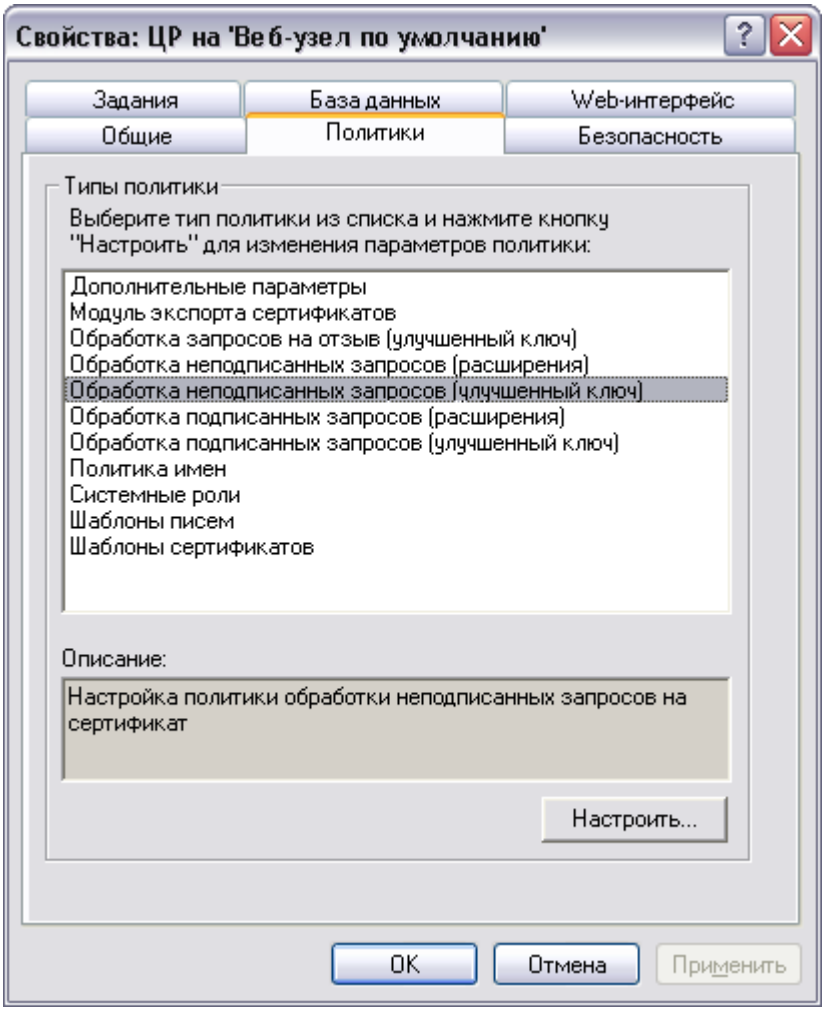


4.2. Настройка Центра регистрации КриптоПро УЦ

Все описанные в этом разделе настройки Центра регистрации осуществляются с помощью настройки соответствующих политик центра регистрации. Чтобы получить доступ к настройкам политик, необходимо выполнить следующую последовательность действий:

1. Откройте оснастку **Параметры центра регистрации** (она доступна из узла **КриптоПро**).
2. Выберите узел **Параметры центра регистрации → ЦР на "Имя веб-узла"** и выберите пункт **Свойства** в контекстном меню.
3. В диалоге свойств Центра регистрации откройте вкладку **Политики** (см. Рисунок 4), выберите нужную политику и нажмите кнопку **Настроить**.

Рисунок 4. Диалог свойств центра регистрации.



Управление расширениями сертификата осуществляется в политике **Обработка неподписанных запросов (расширения)**.

Управление EKU осуществляется в политике **Обработка неподписанных запросов (улучшенный ключ)**.

4.2.1. Шаблон сертификата "Сертификат входа со смарт-картой"

Для удобства выпуска сертификатов пользователя на АРМ Администратора, в ЦР включён шаблон сертификата **Сертификат входа со смарт-картой**. В шаблоне определены необходимые EKU: **Вход со смарт-картой** и **Проверка подлинности клиента**. Администратор Центра регистрации должен дать привилегированному пользователю ЦР, ответственному за выпуск таких сертификатов через АРМ Администратора, право выпуска сертификатов с этими значениями EKU, а также с расширением **Имя шаблона сертификата**.

Для этого необходимо:

- В политике **Обработка неподписанных запросов (расширения)** добавить в список допустимых расширений сертификата расширение
  - (OID 1.3.6.1.4.1.311.20.2) Имя шаблона сертификата.
- В политике **Обработка неподписанных запросов (улучшенный ключ)** добавить в список допустимых использований сертификатов значения:
  - (OID 1.3.6.1.4.1.311.20.2.2) Вход со смарт-картой;
  - (OID 1.3.6.1.5.5.7.3.2) Проверка подлинности клиента.

В сертификате для входа по смарт-карте должно присутствовать поле subjectAltName, где должно быть задано UPN (User Principal Name) пользователя. EKU "Вход со смарт-картой" во

всех компонентах УЦ служит признаком необходимости особой обработки запроса и сертификата.

При создании запроса UPN кладётся в запрос в расширение CertTemplate, затем ЦС перекладывает содержимое этого расширения в поле subjectAltName сертификата.

4.2.2. Шаблон сертификата "Сертификат контроллера домена (winlogon)"

Для удобства выпуска сертификатов контроллеров домена на АРМ Администратора, в ЦР включён шаблон сертификата **Сертификат контроллера домена (winlogon)**. В шаблоне определены необходимые EKU **Проверка подлинности клиента** и **Проверка подлинности сервера**. Администратор Центра регистрации должен дать привилегированному пользователю ЦР, ответственному за выпуск таких сертификатов через АРМ Администратора, право выпуска сертификатов с этими значениями EKU, а также с расширением **Имя шаблона сертификата**.

Для этого необходимо:

- В политике **Обработка неподписанных запросов (расширения)** добавить в список допустимых расширений сертификата расширение
  - (OID 1.3.6.1.4.1.311.20.2) Имя шаблона сертификата.
- В политике **Обработка неподписанных запросов (улучшенный ключ)** добавить в список допустимых использований сертификатов значения:
  - (OID 1.2.643.2.2.34.24) КриптоПро УЦ, Контроллер домена (winlogon);
  - (OID 1.3.6.1.5.5.7.3.2) Проверка подлинности клиента;
  - (OID 1.3.6.1.5.5.7.3.1) Проверка подлинности сервера.

В сертификате контроллера домена должно присутствовать поле subjectAltName, где должны быть заданы GUID контроллера домена и полное DNS-имя. Для выпуска такого сертификата в шаблон также включено особое EKU **КриптоПро УЦ, Контроллер домена (winlogon)**. Это EKU во всех компонентах УЦ служит признаком необходимости особой обработки запроса и сертификата.

При создании запроса GUID и DNS-имя кладутся в запрос в расширение CertTemplate, затем ЦС перекладывает содержимое этого расширения в поле subjectAltName сертификата.

5. Настройка контроллеров домена

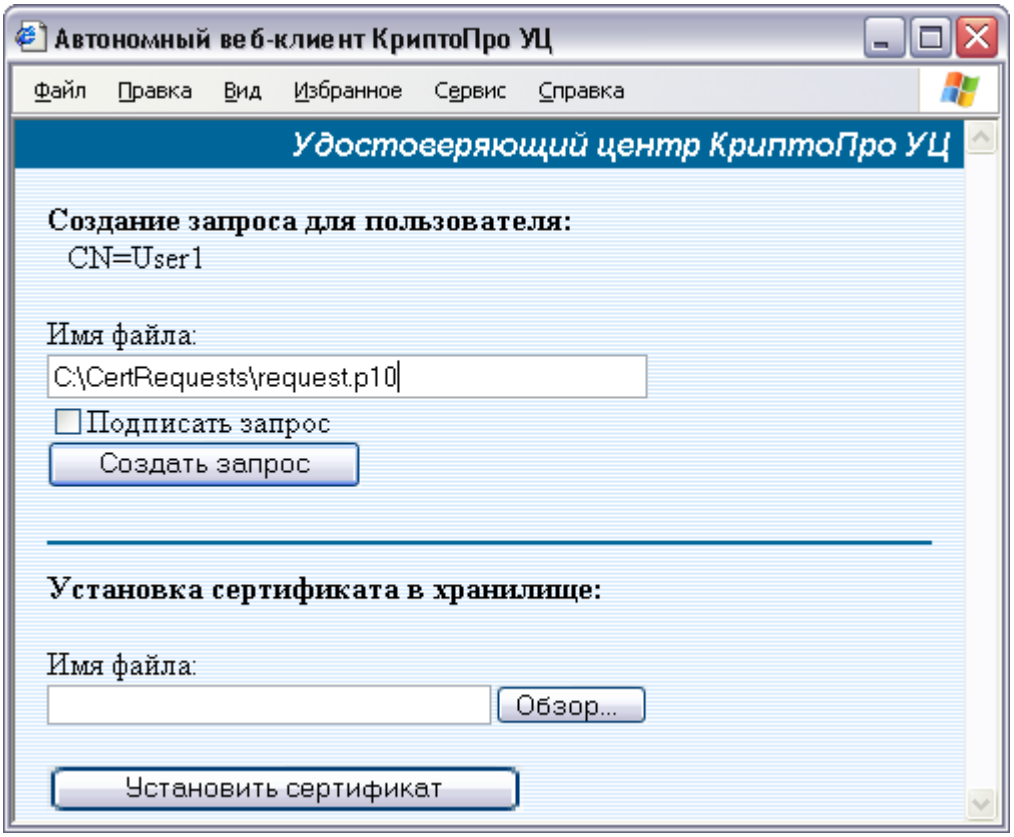
Для всех контроллеров домена необходимо выпустить сертификаты открытых ключей, которые будут использоваться контроллерами для аутентификации и защиты соединения.

Для выпуска сертификата и установки сертификата контроллера домена необходимо выполнить следующую последовательность действий:

1. Узнайте DNS-имя и идентификатор GUID контроллера домена. Для этого на контроллере домена в панели управления компьютера запустите панель **КриптоПро CSP** и на вкладке **Winlogon** нажмите кнопку **Экспортировать.** Нужная информация будет помещена в буфер обмена. Сохраните эти данные, например, в текстовый файл и перейдите на компьютер АРМ Администратора.
2. В **АРМ Администратора КриптоПро УЦ** создайте пользователя, который будет соответствовать контроллеру домена. Задайте дополнительные параметры DNS-имя и GUID для этого пользователя (узел **Свойства** в контекстном меню).
3. В **АРМ Администратора КриптоПро УЦ** создайте HTML-форму для автономной работы пользователя, соответствующего контроллеру домена (узел **Все задачи** → **Создать** → **HTML-форму для автономной работы** в контекстном меню). В качестве типа запроса на сертификат укажите **Сертификат контроллера домена (winlogon)**. Обратите внимание, что в форме должен использоваться КриптоПро CSP.
4. Перенесите созданную HTML-форму на компьютер контроллера домена и запустите её. Для корректной работы формы необходимо разрешить отображение активного содержимого в настройках Internet Explorer. Создайте в форме запрос на сертификат (см. Рисунок 5). Галочку **Подписать запрос** ставить не нужно.

Обратите внимание, что при создании запроса на сертификат с помощью HTML-формы она обязательно должна быть запущена из локального каталога компьютера, на котором планируется её заполнение. Данное требование обусловлено ограничениями безопасности Internet Explorer.

Рисунок 5. HTML-форма для автономной работы пользователя.

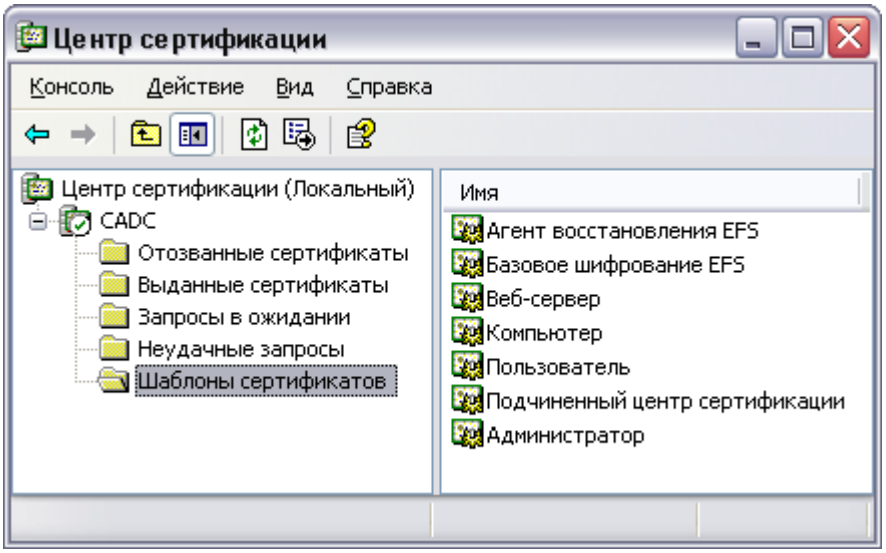


5. В приложении панели управления **КриптоПро CSP** на вкладке **Winlogon** необходимо отметить галочку **Использовать алгоритмы КриптоПро CSP на KDC**.
6. Перенесите запрос на сертификат на АРМ Администратора и выпустите для соответствующего пользователя сертификат по запросу.
7. Перенесите сертификат на компьютер контроллера домена и установите его с помощью той же HTML-формы.
8. Удалите другие сертификаты контроллера домена, если они есть, из хранилища **Личные** локального компьютера и перезагрузите его.

Описанные действия повторите для всех контроллеров вашего домена.

Если в вашем домене есть или планируется развернуть центр сертификации Microsoft в режиме ЦС предприятия (Enterprise CA), то необходимо предотвратить автоматический выпуск сертификатов контроллеров доменов, которые могут помешать работе КриптоПро Winlogon. Для этого в оснастке **Центр сертификации** удалите шаблоны сертификатов **Контроллер домена** и **Проверка подлинности контроллера домена** из списка шаблонов (см. Рисунок 6) с целью запрета автоматической выдачи сертификатов по данным шаблонам.

Рисунок 6. Список допустимых шаблонов сертификатов Центра сертификации.



6. Сертификаты пользователей

Каждый пользователь должен обладать смарт-картой (или USB токеном), содержащей закрытый ключ и сертификат для аутентификации в домене.

Требования к сертификату входа со смарт-картой и рабочей станции:

- Сертификат пользователя должен содержать правильное имя учётной записи (User Principal Name) в поле Subject Alternative Name сертификата.
- На рабочей станции для входа со смарт-картой должны быть установлены драйверы для устройства чтения смарт-карт, это устройство и используемый носитель должны быть установлены в панели управления КриптоПро CSP как считыватель и носитель, в свойствах носителя должна быть установлена галочка «Использовать для входа в операционную систему», если таковая имеется (см. [CPWLINST]).

Выпуск таких сертификатов осуществляется на **АРМ Администратора КриптоПро УЦ**. Существует два различных варианта выпуска сертификата пользователя для входа со смарт-картой:

- Создание сертификата с помощью HTML-формы, аналогично созданию сертификата контроллера домена.
- Создание сертификата непосредственно на АРМ Администратора КриптоПро УЦ.

6.1. Создание сертификата пользователя с помощью HTML-формы.

1. В **АРМ Администратора КриптоПро УЦ** создайте нового пользователя. При создании пользователя укажите дополнительный параметр UPN (User Principal Name). Этот параметр также можно задать или изменить у существующего пользователя (узел **Свойства** в контекстном меню). UPN пользователя может отличаться от имени учётной записи, используемой для входа в компьютер, но чаще всего они совпадают. UPN имеет формат user1@domain.com.
2. В АРМ Администратора КриптоПро УЦ создайте HTML-форму для автономной работы пользователя (узел **Все задачи → Создать → HTML-форму для автономной работы** в контекстном меню). В качестве типа запроса на сертификат укажите **Сертификат входа со смарт-картой**. Обратите внимание, что в форме должен использоваться КриптоПро CSP.
3. Перенесите созданную HTML-форму на рабочую станцию для входа со смарт-картой и запустите её. Для корректной работы формы необходимо разрешить отображение активного содержимого в настройках Internet Explorer. Создайте в форме запрос на сертификат.
4. Перенесите запрос на сертификат на АРМ Администратора и выпустите для соответствующего пользователя сертификат по запросу.
5. Перенесите сертификат на рабочую станцию для входа со смарт-картой и установите его с помощью HTML-формы.

Обратите внимание, что при создании запроса на сертификат с помощью HTML-формы она обязательно должна быть запущена из локального каталога компьютера, на котором планируется её заполнение. Данное требование обусловлено ограничениями безопасности Internet Explorer.

6.2. Создание сертификата пользователя на АРМ Администратора КриптоПро УЦ.

На рабочем месте привилегированного пользователя, выпускающего сертификаты для пользователей с использованием АРМ Администратора, должны быть установлены драйверы

для устройства чтения смарт-карт. Это устройство и используемый носитель должны быть установлены в панели управления КриптоПро CSP как считыватель и носитель, в свойствах носителя должна быть установлена галочка **Использовать для входа в операционную систему**, если таковая имеется (см. [CPWLINST]).

Для выпуска сертификата пользователя с использованием АРМ Администратора необходимо выполнить следующую последовательность действий:

1. В **АРМ Администратора КриптоПро УЦ** создайте нового пользователя. При создании пользователя укажите дополнительный параметр UPN (User Principal Name). Этот параметр также можно задать или изменить у существующего пользователя (узел **Свойства** в контекстном меню). UPN пользователя может отличаться от имени учётной записи, используемой для входа в компьютер, но чаще всего они совпадают. UPN имеет формат user1@domain.com.
2. Выпустите сертификат для данного пользователя, где в качестве типа запроса на сертификат укажите **Сертификат входа со смарт-картой**. Ключевую пару сгенерируйте на смарт-карте и установите сертификат в контейнер.

После этого смарт-карта может использоваться для аутентификации в домене Windows.

7. Перечень сокращений

AIA	Доступ к сведениям о центрах сертификации (Authority Information Access)
CDP	Точка распространения COC (CRL Distribution Point)
CSP	Криптопровайдер (Cryptographic Service Provider)
DNS	Доменная система именования (Domain Name System)
EKU	Расширенное использование ключа (Extended Key Usage)
GUID	Глобальный уникальный идентификатор (Globally Unique Identifier)
OID	Идентификатор объекта (Object Identifier)
UPN	Имя входа пользователя (User Principal Name)
АРМ	Автоматизированное рабочее место
ИОК	Инфраструктура открытых ключей (Public Key Infrastructure – PKI)
ОС	Операционная система
ПО	Программное обеспечение
СОС	Список отзыва сертификатов (Certificate Revocation List – CRL)
УЦ	Удостоверяющий центр

8. Перечень рисунков

9. Перечень ссылочных документов

[CPOCSP] ЖТЯИ.00023-01 90 02. “КриптоПро OCSP Server. Общее описание”.

[CPWL] ЖТЯИ.00032-01 90 01. “КриптоПро Winlogon. Описание и сценарии использования”.

[CPWLINST] ЖТЯИ.00032-01 90 02. “КриптоПро Winlogon. Установка и развёртывание”.

[PKI] Бернет, С., Пэйн, С. “Криптография. Официальное руководство RSA Security”. – М.: Бином-Пресс, 2002 г. – 384 с.: ил.

[RFC2560] Myers, M., et al., “X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP”, IETF, RFC 2560, June 1999.