

# **eToken PKI Client 5.1 SP1**

Руководство администратора

Листов: 60

Версия документа: 1.0

## Содержание

1.	Лицензионное соглашение .....	3
2.	Аннотация.....	4
2.1.	Техническая поддержка .....	4
3.	Введение .....	5
4.	Общие сведения .....	5
4.1.	Новые возможности в eToken PKI Client 5.1 SP1 .....	5
4.2.	Обзор архитектуры .....	6
5.	Системные требования.....	7
5.1.	Требования к аппаратному и программному обеспечению рабочей станции.....	7
5.2.	Требования для подключения к удаленному рабочему столу (RDP) .....	7
5.3.	Перечень задач администратора.....	8
6.	Установка .....	8
6.1.	Обновление с версии eToken PKI Client 5.1 .....	8
6.1.1	Обновление с помощью программы-мастера .....	8
6.1.2	Обновление в режиме командной строки.....	9
6.2.	Переход с более ранних версий.....	10
6.2.1	Обновление eToken PKI Client 4.0 и более поздних версий .....	10
6.2.2	Обновление eToken RTE .....	10
6.3.	Установка с помощью программы-мастера.....	10
6.4.	Установка в режиме командной строки.....	14
6.4.1	Справка по Windows Installer .....	14
6.5.	Установка параметров в режиме командной строки.....	15
6.6.	Параметры, определяемые только в процессе установки.....	15
6.7.	Установка только указанных компонентов.....	17
6.8.	Удаление компонентов из командной строки .....	18
6.9.	Установка без драйверов .....	19
6.10.	Удаление.....	19
6.10.1	Удаление стандартными средствами.....	19
6.10.2	Удаление с помощью программы-мастера .....	20
6.10.3	Удаление из командной строки .....	22
7.	Настройка eToken PKI Client .....	23
7.1.	Общие сведения об оснастке eToken PKI Client Settings.....	23
7.1.1	Как добавить административный шаблон eToken PKI Client Settings на серверной платформе Windows .....	23
7.1.2	Как добавить административный шаблон eToken PKI Client Settings в Windows XP.....	26
7.2.	Настройка параметров eToken PKI Client Settings из консоли управления Microsoft .....	29
7.3.	Как применить настройки eToken PKI Client.....	30
8.	Параметры и настройки .....	31
8.1.	Общие сведения о параметрах .....	31
8.2.	Иерархия параметров .....	31
8.3.	Настройка параметров реестра вручную .....	31
8.4.	Описание параметров реестра.....	32
8.4.1	Раздел GENERAL .....	32
8.4.2	Раздел SyncPin .....	36
8.4.3	Раздел Init.....	36
8.4.4	Раздел реестра InitApp .....	39
8.4.5	Раздел реестра CAPI .....	40
8.4.6	Раздел реестра CertStore.....	42
8.4.7	Раздел реестра Monitor.....	45
8.4.8	Раздел реестра PQ .....	45
8.4.9	Раздел реестра UI.....	50
8.4.10	Отображение и скрытие элементов интерфейса eToken PKI Client .....	51
9.	Наиболее распространенные вопросы.....	53
10.	Известные проблемы и способы их решения.....	55
11.	Изменения в API .....	59

## 1. Лицензионное соглашение

---

В процессе установки данного программного обеспечения (ПО) на ПЭВМ Вам будет предложено ознакомиться и принять (либо отказаться принять) условия лицензионного соглашения на использование ПО. Внимательно прочитайте условия лицензионного соглашения.

Выразите свое согласие принять полностью условия лицензионного соглашения, выбрав пункт «I accept the license agreement». В случае несогласия (полного или частичного) с условиями лицензионного соглашения выберите пункт «I don't accept the license agreement» и нажмите «Cancel».

Выбор пункта «I accept the license agreement» означает, что Вы принимаете условия лицензионного соглашения полностью. В случае несогласия с условиями лицензионного соглашения не используйте данное ПО.

## 2. Аннотация

---

Данный документ содержит полные сведения по установке и настройке работе ПО eToken PKI Client 5.1 SP1. Отдельный раздел документа посвящен описанию параметров реестра, которые определяют набор доступных функций и свойства компонентов eToken PKI Client.

Мы постарались наиболее полно осветить представленную тему и сделать документ удобным для практического применения. Если все же у вас возникли вопросы или пожелания по содержанию, пожалуйста, адресуйте их на [techwriters@aladdin.ru](mailto:techwriters@aladdin.ru). Мы будем благодарны за любые конструктивные замечания и с удовольствием ответим на возникшие вопросы.

### 2.1. Техническая поддержка

По вопросам технической поддержки, пожалуйста, обращайтесь в ЗАО «Аладдин Р.Д.»

по адресу: <http://www.aladdin.ru/support/index.php>. Таким способом вы всегда сможете отслеживать состояние своей заявки.

Для более оперативного разрешения вашей проблемы опишите, пожалуйста, подробно условия применения, конкретные сценарии и, по возможности снабдите свое сообщение экранными снимками и примерами исходного кода.

### 3. Введение

---

eToken PKI Client 5.1 – набор драйверов и дополнительных утилит, обеспечивающий работу с электронными ключами eToken в операционной системе Microsoft Windows.

Краткое содержание главы:

- Общие сведения
- Новые возможности eToken PKI Client 5.1 SP1

### 4. Общие сведения

---

eToken PKI Client имеет широкий спектр применения в сфере информационной безопасности. Этот пакет обеспечивает взаимодействие устройств eToken с программным обеспечением Aladdin и сторонних разработчиков для реализации самых различных решений информационной безопасности. К числу таких решений можно отнести PKI-решения на базе интерфейсов PKCS#11 или CAPI, ПО для работы с eToken, (например eToken Single Sign-On), систему централизованного управления eToken TMS и другие. eToken PKI Client позволяет построить систему строгой двухфакторной аутентификации на базе цифровых сертификатов, а также реализовать шифрование и использование электронной цифровой подписи (ЭЦП). eToken PKI Client обеспечивает возможность использования таких стандартных интерфейсов как Microsoft CAPI и PKCS#11 для доступа внешних приложений к устройствам eToken. Благодаря этому eToken может применяться для безопасного доступа в Интернет, VPN-сети, доступа к локальной сети, защиты данных, безопасного обмена электронными сообщениями, а также для работы с другими приложениями. Генерация, хранение и использование закрытых ключей RSA происходит в защищенном режиме на микросхеме смарт-карты eToken – сгенерированный закрытый ключ никогда не покидает память устройства.

Установка и обновление eToken PKI Client может осуществляться централизованно через объекты групповых политик (GPO) Active Directory, Microsoft Systems Management Server или другие подобные системы.

#### 4.1. Новые возможности в eToken PKI Client 5.1 SP1

eToken PKI Client 5.1 SP1 обладает по сравнению с более ранними версиями следующими преимуществами:

**Расширенная поддержка платформ Microsoft:** добавилась поддержка Windows 7 и Windows Server 2008 R2. Кроме того, теперь также поддерживается браузер Internet Explorer 8.0

**Поддержка новых моделей eToken:** в нынешней версии утилиты eToken имеется возможность работать с устройствами eToken NG-Flash 4.50 CardOS, eToken NG-Flash 5.30 Java и eToken NG-Flash 5.30 Java Anywhere.

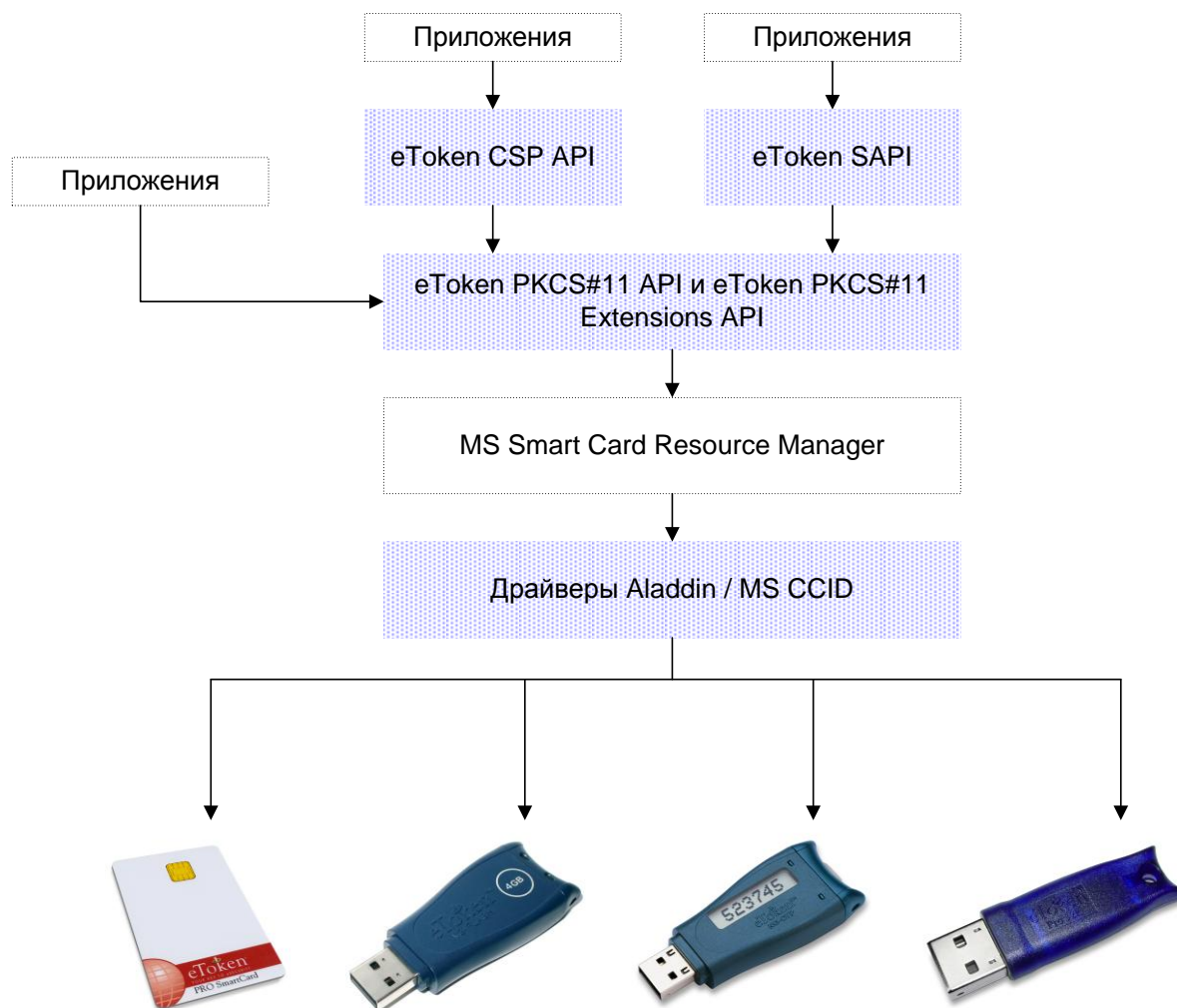
**Поддержка новых алгоритмов хэширования:** поддержка всей серии алгоритмов SHA-2.

**Поддержка по умолчанию сертификатов в кодировке, отличной от DER:** атрибут TolerantX509Attribute теперь имеет значение «Истина» по умолчанию.

При работе над этой версией помимо перечисленных усовершенствований были учтены отзывы и требования клиентов, полученные с момента выпуска предыдущих версий.

## 4.2. Обзор архитектуры

В этой главе представлена информация о составляющих компонентах eToken PKI Client и принципах их взаимодействия между собой.



Краткое содержание главы:

- Архитектура eToken PKI Client
- Компоненты eToken PKI Client

В состав eToken PKI Client 5.1 SP1 входят следующие компоненты.

**eToken PKI Monitor:** Этот сервис выполняется в фоновом режиме с момента загрузки операционной системы. Его также можно вызвать через меню Пуск.

Данный сервис отслеживает все подключенные устройства eToken, сообщает пользователю о сроке истечения пароля и позволяет получить доступ к наиболее часто используемым функциям eToken PKI Client через меню в области уведомлений.

**Утилита eToken Properties:** эта утилита открывает пользователю доступ ко всем возможным функциям eToken, включая разблокировку смены пароля, экспорт/ импорт сертификатов и прочие функции.

**Системная служба eToken:** это системный процесс (eToksrv.exe), который можно увидеть только в списке процессов в диспетчере задач. В частности он отвечает за автоматическое подключение eToken Virtual, когда он расположен в определенной папке на жестком диске или съемном устройстве.

## 5. Системные требования

Перед тем как приступить к установке eToken PKI Client необходимо в первую очередь удостовериться в том, что ваш компьютер соответствует минимальным требованиям.

### Краткое содержание

- Требования к аппаратному и программному обеспечению рабочей станции
- Требования для подключения к удаленному рабочему столу (RDP)

### 5.1. Требования к аппаратному и программному обеспечению рабочей станции

<b>Поддерживаемые операционные системы</b>	<ul style="list-style-type: none"> <li>• Windows XP SP3 (32-битные платформы), SP2 (64-битные платформы)</li> <li>• Windows Server 2003 SP2 (32/64-битные платформы)</li> <li>• Windows Server 2003 R2 (32/64-битные платформы)</li> <li>• Windows Server 2008 (32/64-битные платформы)</li> <li>• Windows Server 2008 R2</li> <li>• Windows Vista SP1/SP2 (32/64-битные платформы)</li> <li>• Windows 7 (32/64-битные платформы)</li> </ul>
<b>Поддерживаемые версии браузеров</b>	Firefox 3.0.x IE 6 / 7 / 8
<b>Поддерживаемые устройства eToken</b>	eToken PRO eToken NG-OTP eToken NG-FLASH eToken PRO Smartcard eToken PRO Anywhere eToken GT
<b>Необходимые аппаратные средства</b>	USB-порт (для аппаратных ключей eToken). Для смарт-карт необходимо наличие установленного считывателя смарт-карт.
<b>Рекомендуемое разрешение экрана</b>	Для работы утилиты eToken PKI Client Properties рекомендуется установить разрешение монитора не ниже 1024x768.

### 5.2. Требования для подключения к удаленному рабочему столу (RDP)

eToken PKI Client поддерживает следующие средства аутентификации при работе с подключением к удаленному рабочему столу.

<b>Операционная система</b>	<ul style="list-style-type: none"> <li>• Windows Server 2003</li> <li>• Windows Server 2008</li> <li>• Windows Server 2008 R2</li> </ul>
<b>Аппаратные eToken</b>	Поддерживаются
<b>Поддержка eToken Virtual на стороне клиента</b>	Нет
<b>Поддержка eToken Virtual на стороне сервера</b>	Есть

### Примечание:

Для работы с программными eToken на сервере должно быть установлено приложение eToken Network Logon.

Поддерживаемые модели программных eToken: eToken Virtual и eToken Rescue.

### 5.3. Перечень задач администратора

В качестве памятки представляем вам общий сценарий действий администратора. Более подробно все эти пункты будут рассмотрены далее в руководстве.

Если на компьютере установлена более ранняя версия eToken PKI Client, то для обновления ее до версии 5.1 SP1, прежде всего необходимо удалить все ранее созданные параметры реестра. Для этого выполните инструкции, представленные в главе Переход с более ранних версий.

Обновите или установите eToken PKI Client на каждой рабочей станции, где будут использоваться устройства eToken. Для этого руководствуйтесь инструкциями, представленными в следующих главах:

- Переход с более ранних версий;
- Установка с помощью программы-мастера;
- Установка в режиме командной строки.

Установите необходимые параметры eToken PKI Client и выполните обновление на всех пользовательских компьютерах. В этом вам помогут инструкции, изложенные в главе Настройки eToken PKI Client.

Создайте новые учетные записи пользователей. О том, как это сделать, читайте в главе Инициализация eToken.

В процессе работы с учетными записями пользователей пользуйтесь инструкциями в главе Работа с устройствами eToken.

## 6. Установка

---

В состав eToken PKI Client входят все файлы и драйверы, необходимые для работы с устройствами eToken. Вместе с ними дистрибутив включает в себя утилиту eToken Properties с удобным графическим интерфейсом, который предоставляет быстрый доступ к настройкам устройств eToken и считывателей.

Краткое содержание главы:

- Обновление с версии eToken PKI Client 5.1
- Переход с более ранних версий
- Установка с помощью программы-мастера
- Установка в режиме командной строки
- Установка без драйверов
- Удаление

### 6.1. Обновление с версии eToken PKI Client 5.1

Если на компьютере уже установлен eToken PKI Client 5.1, достаточно только установить пакет обновления (.msp).

#### Примечание:

---

Как только вы установили обновление SP1, вернуться к более ранней версии путем его удаления уже будет невозможно, то есть можно будет только удалить целиком eToken PKI Client 5.1 SP1.

---

#### 6.1.1 Обновление с помощью программы-мастера

Для того, чтобы установить пакет обновления поверх eToken PKI Client 5.1, выполните следующие действия:

1. Войдите в систему с полномочиями администратора.
2. Закройте все приложения.
3. Двойным щелчком запустите мастер установки из файла .msp (выберите 32- или 64-битную версию в зависимости от вашей операционной системы).



На экране появится приветственное окно мастера-установки.



4. Нажмите кнопку **Далее**.
5. Выполните необходимые действия, руководствуясь инструкциями в окне программы-мастера и, после того как обновление будет завершено, нажмите кнопку **Готово**.

### 6.1.2 Обновление в режиме командной строки

При обновлении eToken PKI Client используется стандартный синтаксис Windows Installer (msiexec).

#### Примечание

---

При обновлении в режиме командной строки не указывайте никаких дополнительных параметров.

---

Для того, чтобы обновить eToken PKI Client 5.1 в режиме командной строки, выполните следующие действия.

1. Войдите в систему с полномочиями администратора.
2. Закройте все приложения.
3. Откройте меню **Пуск > Программы > Стандартные > Командная строка**.

Если вы запускаете командный интерпретатор в Windows Vista, вы должны щелкнуть правой кнопкой на пункте Командная строка, выбрать Запуск от имени и учетную запись администратора.

4. Выполните команду msiexec в следующем формате:

msiexec /update PKIClient-x32-5-1-SP1.msp,

Где PKIClient-x32-5-1-SP1.msp – имя файла с обновлением. Для 64-битной платформы замените это имя на PKIClient-x64-5-1-SP1.msp. Чтобы выполнить обновление в полуавтоматическом режиме, добавьте в конце строки параметр /q.

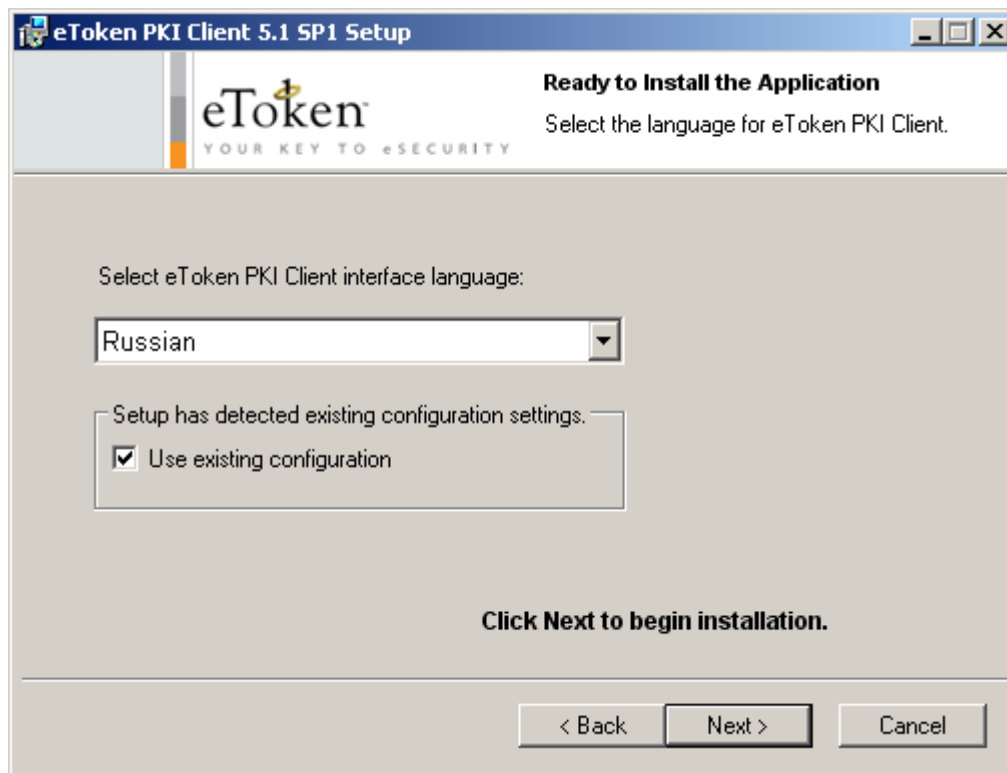
---

---

## 6.2. Переход с более ранних версий

### 6.2.1 Обновление eToken PKI Client 4.0 и более поздних версий

Если на вашем компьютере установлен eToken PKI Client 4.0 или более поздней версии, обновление будет выполнено автоматически вместе с установкой eToken PKI Client 5.1. SP1. При этом однако будут сохранены все прежние настройки реестра для данного компьютера и учетной записи пользователя.



При обнаружении таких параметров во время установки eToken PKI Client 5.1 SP1 вам необходимо будет отметить пункт **Use existing configuration** в том же окне, где вы выбираете язык интерфейса. В этом случае будут использоваться уже существующие параметры реестра.

### 6.2.2 Обновление eToken RTE

Если на компьютере установлен eToken RTE, то сначала необходимо будет удалить его, и только затем можно будет устанавливать eToken PKI Client 5.1 SP1. При удалении eToken RTE все связанные с ними параметры реестра остаются неизменными. Чтобы удалить их, выполните следующие действия.

1. Удалите eToken RTE.
2. Установите eToken PKI Client 5.1 SP1 (см. Установка с помощью программы-мастера)
3. Удалите eToken PKI Client 5.1 SP1 и в запросе на сохранение параметров реестра нажмите кнопку No (Нет). Более подробно эта процедура описана в главе Удаление.

## 6.3. Установка с помощью программы-мастера

Для установки eToken PKI Client 5.1 SP1 со стандартными настройками и компонентами используйте программу-мастер.

В процессе установки вам будет предложено изменить следующие параметры:

- Язык интерфейса, то есть тот язык, на котором будет отображаться текст в окнах утилиты eToken Properties и в меню быстрого доступа в области уведомлений.
- Путь, то есть то место, где будут располагаться все программные компоненты и прочие приложения для работы с eToken (если такие еще не были ранее установлены).

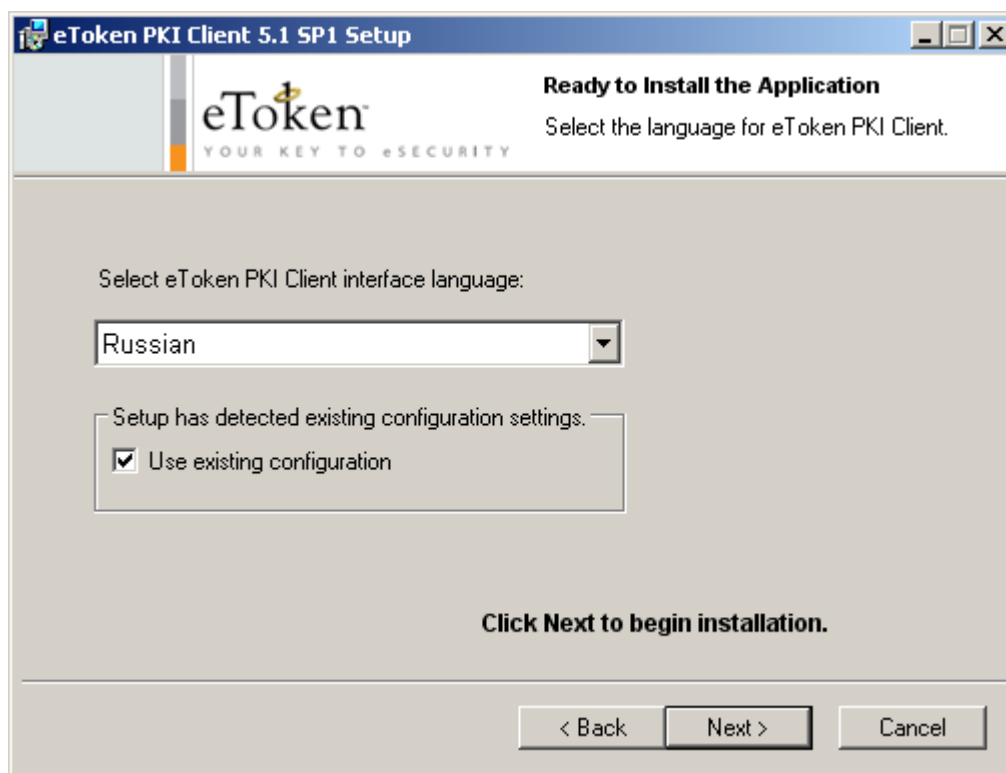
Чтобы установить eToken PKI Client 5.1 SP1 с помощью программы-мастера, выполните следующие действия:

1. Войдите в систему с полномочиями администратора.
2. Закройте все приложения.
3. Двойным щелчком запустите мастер установки из файла .msp (выберите 32- или 64-битную версию в зависимости от вашей операционной системы).

На экране появится приветственное окно мастера установки.



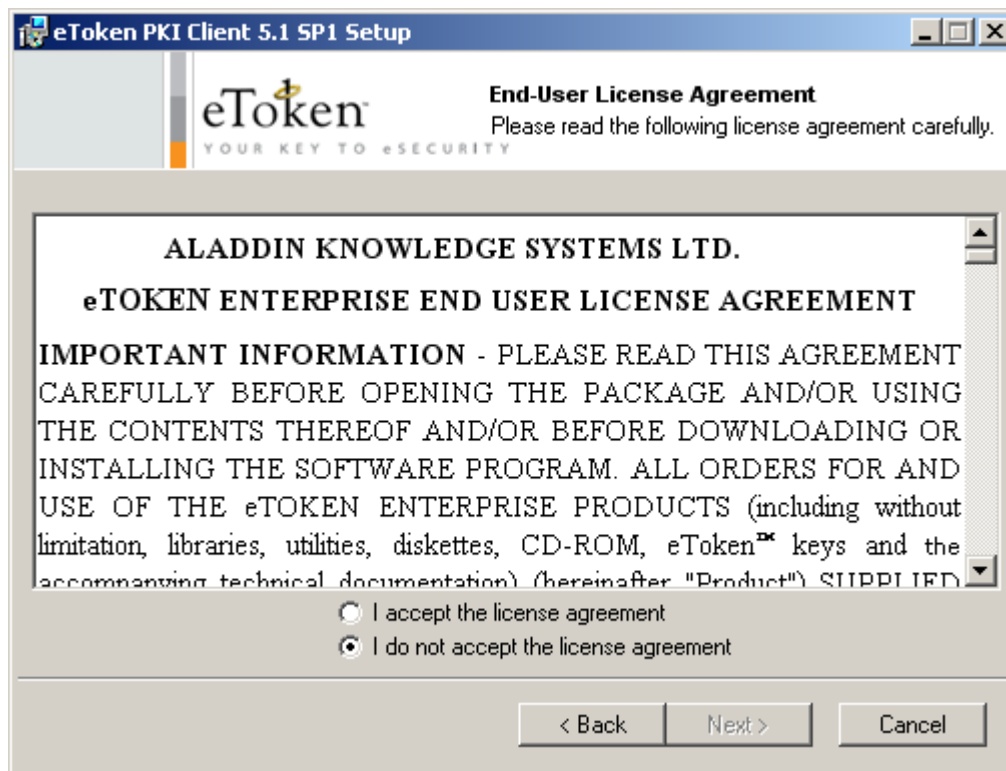
4. Нажмите кнопку **Next**. На экране появится окно, где вам будет предложено выбрать язык интерфейса.



5. В списке доступных языков интерфейса выберите **Russian** (Русский).

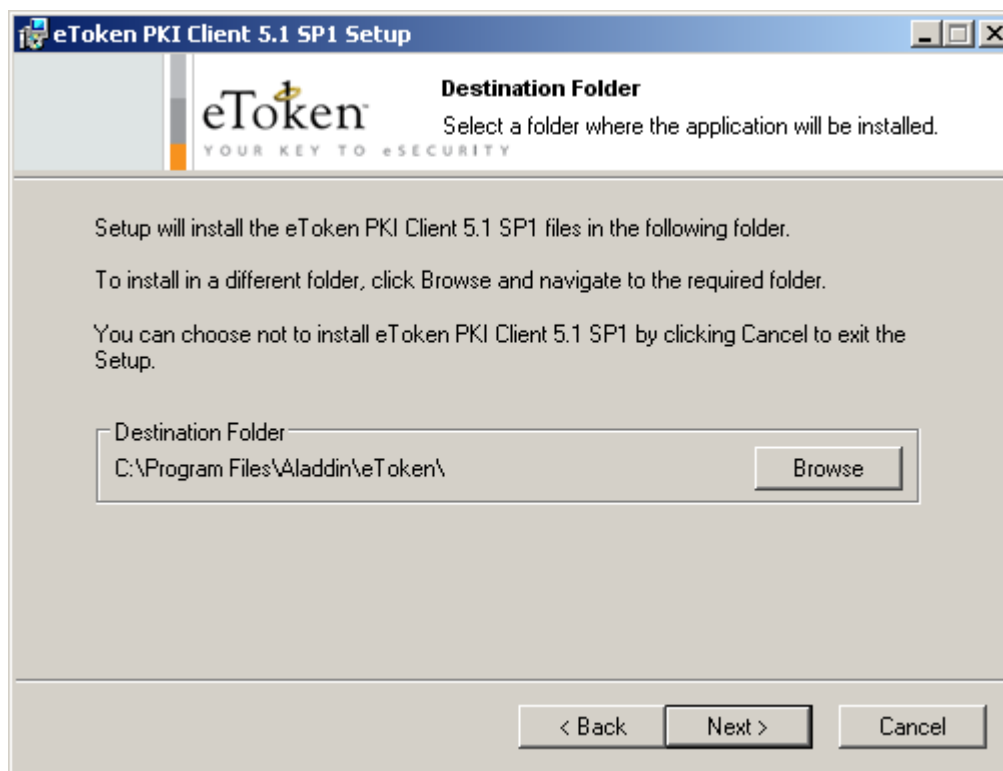
Если в этом окне вам будет предложено сохранить настройки, оставшиеся от предыдущей версии, вы можете оставить или снять флажок, тем самым сохранив эти настройки или удалив их (см. [Обновление с версии eToken PKI Client 5.1](#)).

- Нажмите кнопку **Next**. На экране появится окно с текстом лицензионного соглашения (на английском).



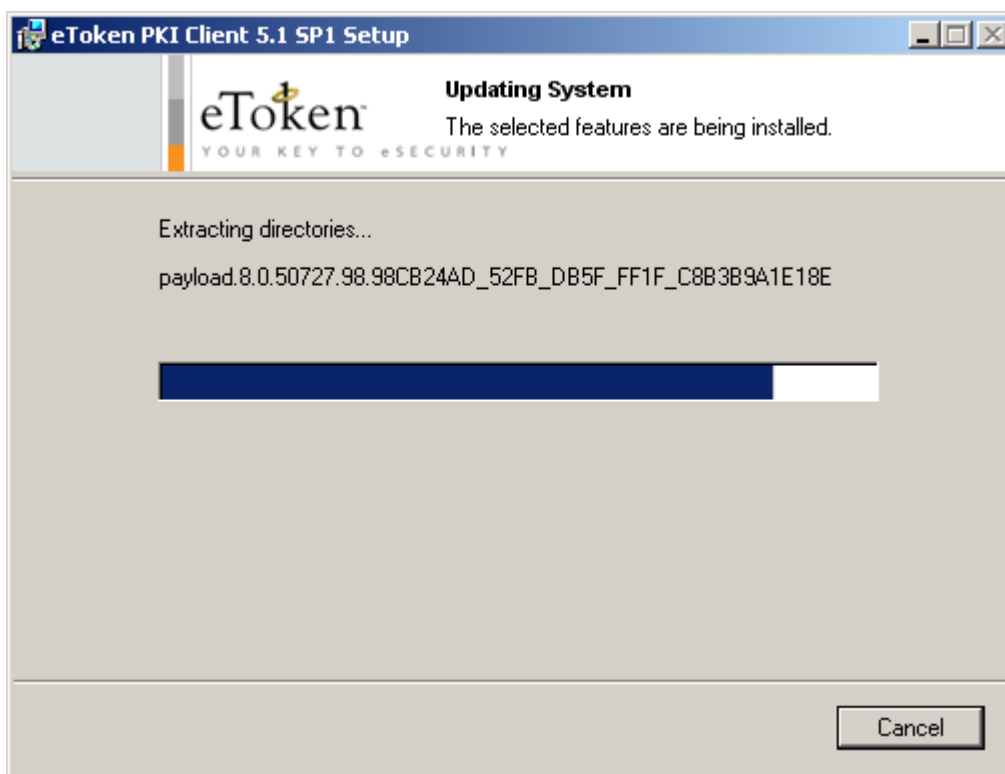
- Прочтите внимательно лицензионное соглашение и, если вы согласны со всеми его условиями, отметьте пункт **I accept the license agreement** нажмите кнопку **Next**. Если вы не понимаете или не согласны с каким-либо из положений документа, откажитесь от установки, нажав кнопку **Cancel**.

Если в предыдущем пункте вы приняли соглашение, на экране появится следующее окно:



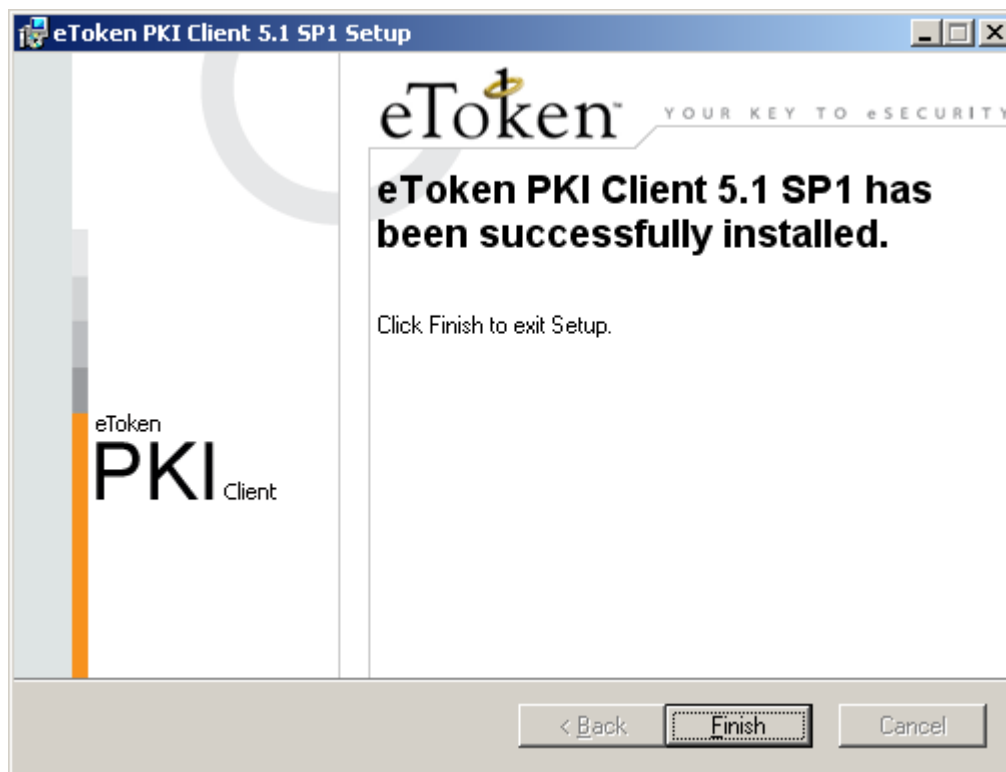
8. Укажите путь для установки, щелкнув кнопку **Browse**, или оставьте его таким, как он указан по умолчанию. Для запуска установки нажмите кнопку **Next**.

Процесс установки отображается в виде шкалы с комментариями.



После того как eToken PKI Client будет установлен, на экране появится окно с соответствующим подтверждающим сообщением.

9. Закройте окно, нажав кнопку **Finish**.



На этом установка eToken PKI Client завершена.

## 6.4. Установка в режиме командной строки

Помимо установки средствами программы-мастера есть также вариант установки из командной строки, где в качестве параметров вы можете указать необходимые для установки компоненты. В этом случае используется стандартный синтаксис Windows Installer:

```
msiexec /i PKIClient-x32-5.1-SP1.msi
```

где, PKIClient-x32-5.1-SP1.msi – это пакет установки для 32-битных платформ Windows. Для 64-битных платформ используйте файл PKIClient-x64-5.1-SP1.msi.

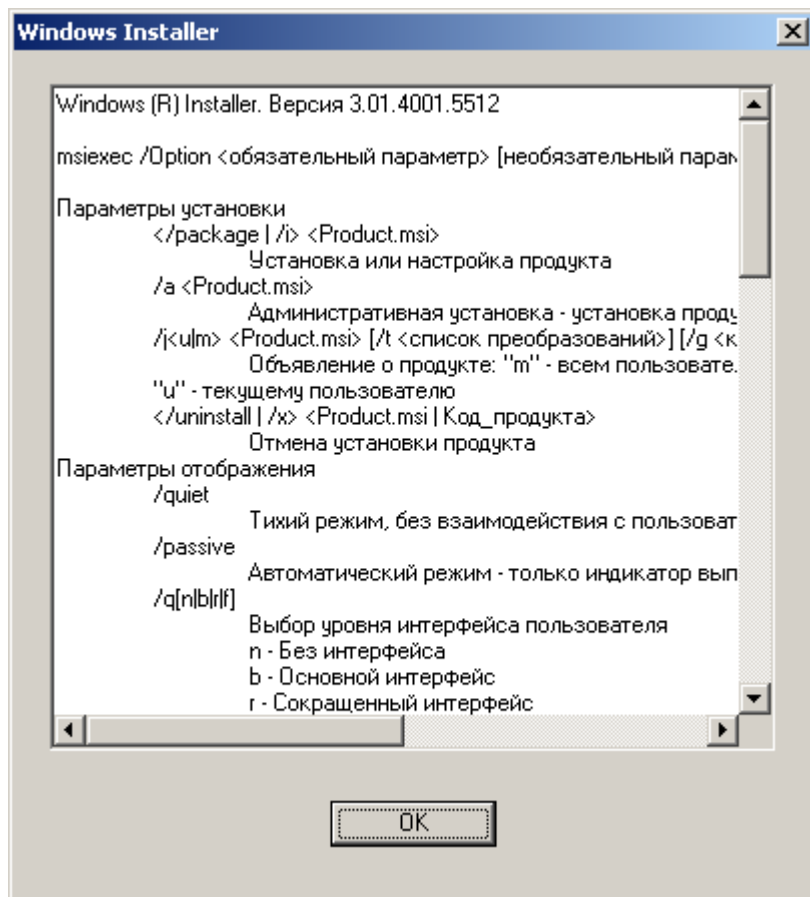
Чтобы установить eToken PKI Client в режиме командной строки, выполните следующие действия:

1. Войдите в систему под учетной записью с полномочиями администратора.
2. Закройте все приложения.
3. Откройте меню **Пуск > Программы > Стандартные > Командная строка**.
4. Если вы выполняете установку под Windows Vista, щелкните правой кнопкой в пункте Командная строка и выберите **Запуск от имени Администратора**.
5. Введите в командной строке msiexec с необходимыми параметрами.

### 6.4.1 Справка по Windows Installer

Чтобы просмотреть полный перечень возможных параметров, которые можно использовать при установке eToken PKI Client, обратитесь к встроенной справке Windows Installer. Для ее вызова выполните следующие действия:

1. Откройте меню **Пуск > Выполнить**.
2. В поле **Открыть** введите msiexec и нажмите **ОК**. На экране появится окно со списком параметров Windows Installer.



## 6.5. Установка параметров в режиме командной строки

При установке в режиме командной строки есть возможность задать особые параметры вместо тех, которые определены по умолчанию, и задать для всех таких параметров необходимые значения. Такие параметры сохраняются в реестре в разделе HKEY\_LOCAL\_MACHINE\Software\Aladdin\eToken\MIDDLEWARE. Исключением является описанный далее параметр PROP\_REG\_FILE.

Параметры можно установить только в процессе установки, но не при восстановлении уже установленного приложения.

Чтобы установить параметры установки, используйте следующий формат:

```
msiexec /i PKIClient-x32-5.1-SP1.msi ПАРАМЕТР=ЗНАЧЕНИЕ ПАРАМЕТР=ЗНАЧЕНИЕ /qb
```

Здесь:

PKIClient-x32-5.1-SP1.msi – файл дистрибутива для 32-битных платформ. Вместо него для 64-битных платформ следует использовать файл PKIClient-x64-5.1-SP1.msi.

ПАРАМЕТР – имя определяемого параметра; как правило, в его имени присутствует префикс PROP\_.

ЗНАЧЕНИЕ – значение параметра.

На следующей странице приведена таблица параметров со ссылками на более подробное их описание в данном руководстве.

Следует иметь в виду, что некоторые параметры хранятся в реестре и задаются только в процессе установки (см. [Параметры, определяемые только в процессе установки](#)), в то время как другие могут изменяться в процессе работы с eToken PKI Client.

Пример:

Чтобы установить eToken PKI Client с интерфейсом на испанском языке, отключить при этом возможность редактирования настроек в расширенном режиме, очистить в случае удаления PKI Client все связанные с ним параметры и присвоить всем прочим параметрам значения по умолчанию, необходимо выполнить команду:

```
msiexec /i PKIClient-x32-5.1-SP1.msi ET_LANG_NAME=Spanish PROP_ADVANCED_VIEW=0 PROP_CLEAR_REG=1 /qb.
```

## 6.6. Параметры, определяемые только в процессе установки

В этой главе выделены именно те параметры, которые задаются только при установке, и не подлежат дальнейшему изменению, кроме особо оговоренных случаев.

### Параметр ET\_LANG\_NAME

<b>Имя</b>	ET_LANG_NAME
<b>Описание</b>	Язык интерфейса
<b>Значения</b>	Chinese (Китайский) / English (Английский) / French (Французский) / French (Canadian) – Французский (Канада) / German (Немецкий) / Italian (Итальянский) / Japanese (Японский) / Korean (Корейский) / Polish (Польский) / Portugese (Португальский) / Russian (Русский) / Spanish (Испанский) / Thai (Тайский)
<b>По умолчанию</b>	English (Английский)

**Параметр PROP\_CLEAR\_REG**

<b>Имя</b>	PROP_CLEAR_REG
<b>Описание</b>	Удаление параметров из реестра при удалении eToken PKI Client
<b>Значения</b>	<ul style="list-style-type: none"> <li>1 (Истина): параметры удаляются из реестра.</li> <li>0 (Ложь): параметры не удаляются из реестра.</li> </ul>
<b>По умолчанию</b>	0 (Ложь)

**Параметр PROP\_FAKEREADER**

<b>Имя</b>	PROP_FAKEREADER
<b>Описание</b>	Наличие в интерфейсе ветви для виртуального считывателя
<b>Значения</b>	1 (Истина): есть. 0 (Ложь): нет. 128 – установка драйверов eToken не выполняется.
<b>По умолчанию</b>	1 (Истина)

**Примечание:**

Более подробную информацию по использованию этого параметра можно получить в службе поддержки Aladdin.

**Параметр PROP\_REG\_FILE**

<b>Имя</b>	PROP_REG_FILE
<b>Описание</b>	Импорт параметров из файла реестра в раздел HKEY_LOCAL_MACHINE на локальном компьютере.
<b>Значения</b>	Путь к файлу реестра
<b>По умолчанию</b>	-

**Примечание:**

В то время как все прочие параметры устанавливаются только в разделе HKEY\_LOCAL\_MACHINE\SOFTWARE\Aladdin\eToken\MIDDLEWARE, параметры из файла, указанного в значении PROP\_REG\_FILE записываются в раздел HKEY\_LOCAL\_MACHINE и соответствующие подразделы.

**Параметр PROP\_UPD\_INFOPATH**

<b>Имя</b>	PROP_UPD_INFOPATH
<b>Описание</b>	Путь поиска обновленных версий драйвера.
<b>Значения</b>	Путь к файлу обновленной версии драйвера.
<b>По умолчанию</b>	-

**Примечание:**

Более подробную информацию по использованию этого параметра можно получить в службе поддержки Aladdin.



**Параметр READER\_COUNT**

<b>Имя</b>	READER_COUNT
<b>Описание</b>	Количество ветвей для физических считывателей в интерфейсе утилиты «eToken Properties».
<b>Значения</b>	0-16
<b>По умолчанию</b>	2

**Примечание:**


---

Данный параметр также можно изменить после установки непосредственно в утилите eToken Properties.

---

**Параметр TARGETDIR**

<b>Имя</b>	TARGETDIR
<b>Описание</b>	Путь установки eToken PKI Client и всех прочих приложений для работы с устройствами eToken. Данный параметр задается в том случае, если на данном компьютере еще не установлено ни одного из упомянутых приложений.
<b>Значения</b>	Путь
<b>По умолчанию</b>	Значение по умолчанию отсутствует, то есть eToken PKI Client устанавливается в папку по умолчанию.

**Примечание:**


---

Этот параметр не следует использовать, если у вас на диске уже установлены какие-либо другие приложения для работы с устройствами eToken.

---

**6.7. Установка только указанных компонентов**

Чтобы установить eToken PKI Client со стандартным набором компонентов, можно использовать параметр ADDDEFAULT. По мере необходимости отсутствующие компоненты можно будет добавить позднее.

Чтобы установить только необходимые вам параметры, выполните команду в следующем формате:

```
msiexec /i PKIClient-x32-5.1-SP1.msi ADDDEFAULT=F1,F2...Fn /qb.
```

где, PKIClient-x32-5.1-SP1.msi – это пакет установки для 32-битных платформ Windows. Для 64-битных платформ используйте файл PKIClient-x64-5.1-SP1.msi.

ADDDFAULT указывает на то, что будут установлены только те компоненты, которые указаны в значении данного параметра.

F1, F2, ... - названия компонентов (см таблицу Список компонентов).

Пример: установка eToken PKI Client без утилиты «eToken Properties».

```
msiexec /i PKIClient-x32-5.1-SP1.msi ADDDEFAULT=DriverFeature,CoreFeature, UIFeature, etMonitor,etFSFeature,etVerifierFeature,NgFlashFeature /qb
```

Если впоследствии вы решите установить «eToken Properties», вам нужно будет выполнить команду в следующем формате:

```
msiexec /i PKIClient-x32-5.1-SP1.msi ADDDEFAULT=etPropsFeature /qb
```

## 6.8. Удаление компонентов из командной строки

Если вам нужно удалить какие-то из установленных компонентов, командная строка будет иметь следующий вид:

```
msiexec /i PKIClient-x32-5.1-SP1.msi REMOVE=F1, F2, ... /qb
```

где,

- PKIClient-x32-5.1-SP1.msi – это пакет установки для 32-битных платформ Windows. Для 64-битных платформ используйте файл PKIClient-x64-5.1-SP1.msi.
- Параметр REMOVE в аргументах содержит те компоненты, которые необходимо удалить
- F1, F2 - названия компонентов (см таблицу Список компонентов).

Следует помнить, что удалить можно только дополнительно устанавливаемые компоненты. Так, например, можно удалить утилиту «eToken Properties». Для этого выполните следующую команду:

```
msiexec /i PKIClient-x32-5.1-SP1.msi REMOVE=etPropsFeature /qb
```

### Список компонентов

Название	Описание	Обязательный / необязательный
<b>DriverFeature</b>	Драйверы и библиотеки	требуется для поддержки аппаратных устройств eToken
<b>CoreFeature</b>	Базовый модуль, реализующий основной функционал eToken PKI Client. Может устанавливаться без DriverFeature для работы с eToken Virtual или считывателями сторонних производителей.	Обязательный компонент
<b>UIFeature</b>	Компоненты графического интерфейса и библиотеки	Требуется для etPropsFeature и etMonitor
<b>etPropsFeature</b>	Утилита «eToken Properties»	Необязательный компонент
<b>eTMonitor</b>	Меню в области уведомлений и соответствующие дополнительные модули	Обязательный компонент
<b>eTVerifierFeature</b>	Объект eTVerifier COM	Необязательный компонент, но притом он требуется для многих Web-приложений (включая также TMS Client).
<b>NgFlashFeature</b>	Утилита eToken NG-FLASH Partition Application	Необязательный компонент. Требуется только для работы со встроенной Flash-памятью устройств eToken NG-FLASH
<b>etFSFeature</b>	При установке этого компонента в папку %systemroot%\system32 копируется библиотека etFS.dll, необходимая для работы с файловой системой eToken.	Необязательный компонент
<b>ETOKSRV</b>	Создает и активизирует службу eTSrv.exe. Данная служба отслеживает подключение/отключение Flash-устройств и осуществляет поиск eToken Virtual. Значение по умолчанию: установлен.	Необходим для приложения Single Sign-On

### Примечание:

---

Для поддержки устройств eToken без установки прочих программных компонентов eToken PKI Client в списке компонентов в командной строке достаточно указать только значение DriverFeature.

---

## 6.9. Установка без драйверов

Чтобы установить eToken PKI Client без драйверов, выполните следующие действия.

В командной строке укажите параметр PROP\_FAKEREADER=128. В этом случае установка драйверов не будет выполняться и в списке компонентов укажите все необходимые компоненты, кроме DriverFeature. Тогда формат командной строки будет следующим:

```
msiexec /i PKIClient-x32-5.1.msi PROP_FAKEREADER=128 ADDDEFAULT=CoreFeature,  
UIFeature,etMonitor,etFSFeature,etVerifierFeature,etPropsFeature /qb
```

В этом случае драйвер не будет скопирован в папку с остальными установленными компонентами. А в следующем примере он будет сохранен в папку c:\Windows\system32\setup\Aladdin\eToken\ (путь по умолчанию), но в силу того что параметр PROP\_FAKEREADER имеет значение 128, устанавливаться не будет:

```
msiexec /i PKIClient-x32-5.1.msi PROP_FAKEREADER=128.
```

## 6.10. Удаление

Для удаления eToken PKI Client 5.1 SP1 есть три способа:

- Удаление стандартными средствами Windows
- Удаление с помощью программы-мастера
- Удаление из командной строки.

Если при установке для параметра PROP\_CLEAR\_REG имеет значение «1» (Истина), то при удалении eToken PKI Clients будет одновременно удалены все соответствующие параметры реестра.

### Примечания:

---

Удаление eToken PKI Client 5.1 SP1 включает в себя все установленные компоненты, а не только пакет обновления.

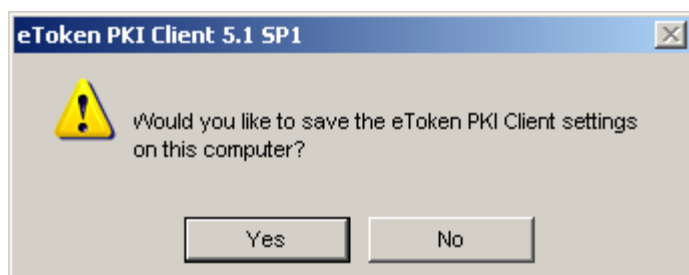
---

Если какая-либо из динамических библиотек (.dll) используется другим приложением, на экране появится окно с соответствующим сообщением. Нажмите кнопку Ignore (Пропустить) и по завершении перезагрузите компьютер.

### 6.10.1 Удаление стандартными средствами

В Windows есть стандартная схема удаления и установки программ. С ее помощью вы можете также удалить eToken PKI Client. Для этого выполните следующие действия.

1. Откройте меню **Пуск > Панель управления**.
2. Дважды щелкните на значке **Установка и удаление программ**.
3. Выберите eToken PKI Client 5.1 SP1 и нажмите кнопку **Удалить**.
4. Следуйте инструкциям, представленным в меню. Если значение параметра PROP\_CLEAR\_REG не было задано явно, то на экране появится меню следующего вида.



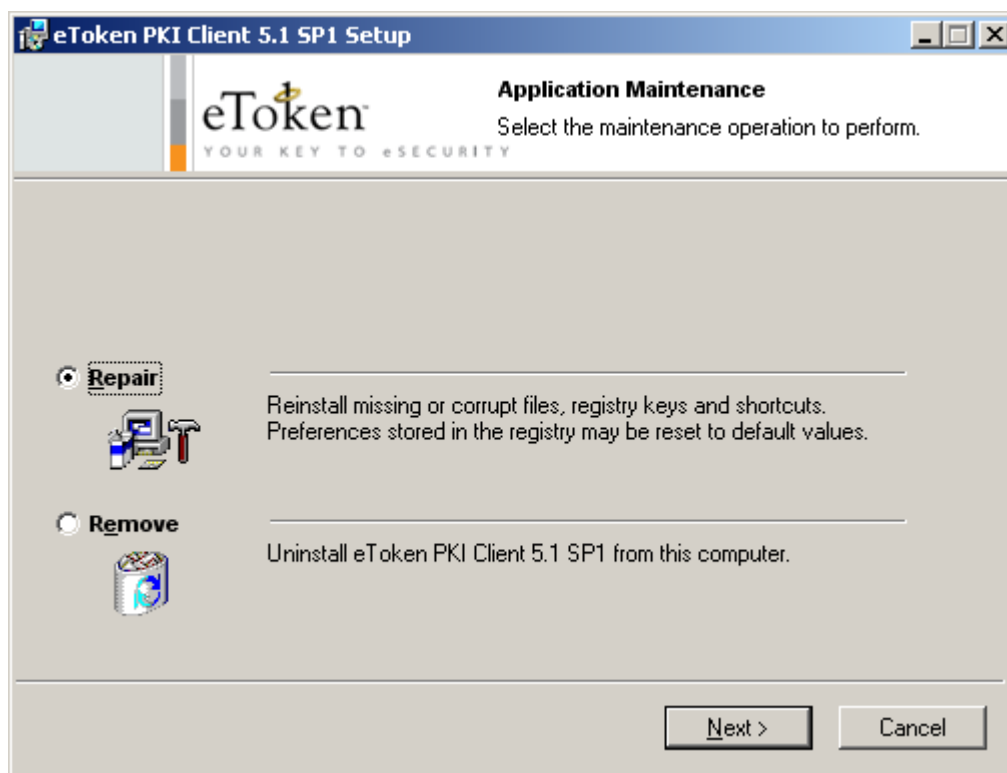
5. Нажмите **Yes**, если вы хотите оставить параметры реестра, или **No**, если вы хотите удалить их.
6. После того как eToken PKI Client будет удален, перезагрузите компьютер.

### 6.10.2 Удаление с помощью программы-мастера

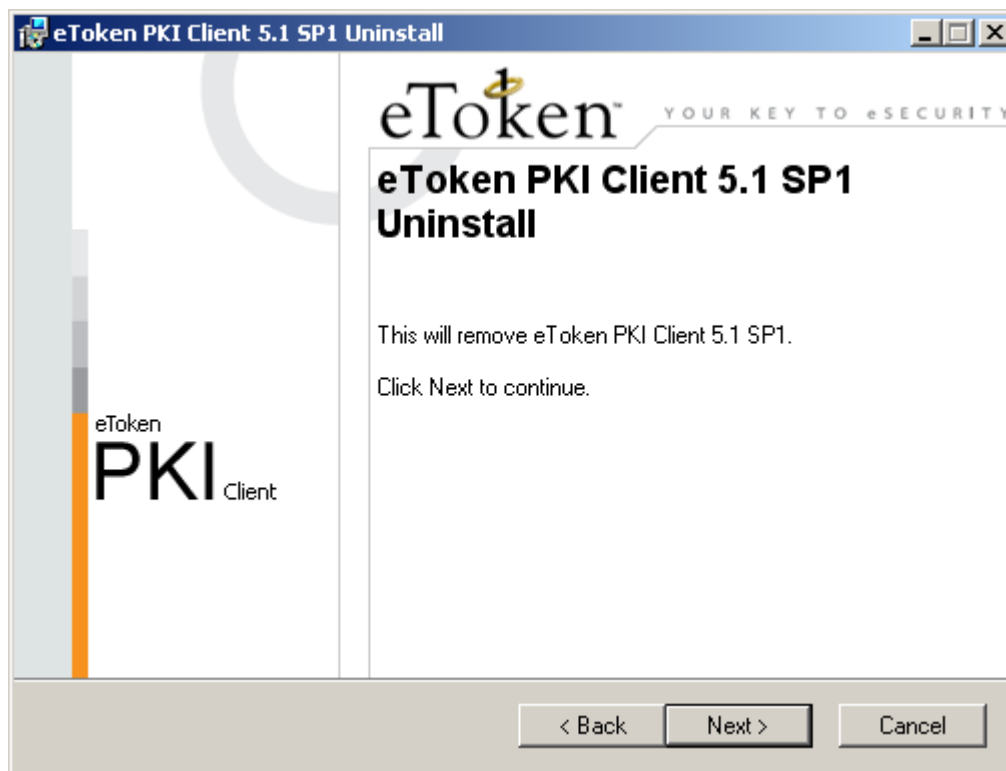
Чтобы удалить Token PKI Client с помощью программы-мастера, выполните следующие действия:

1. Войдите в систему под учетной записью с правами администратора.
2. Закройте все приложения.
3. Щелкните на файле с дистрибутивом установки PKIClient-x32-5.1-SP1.msi или PKIClient-x64-5.1-SP1.msi) в зависимости от того, какая из версий у вас уже установлена.

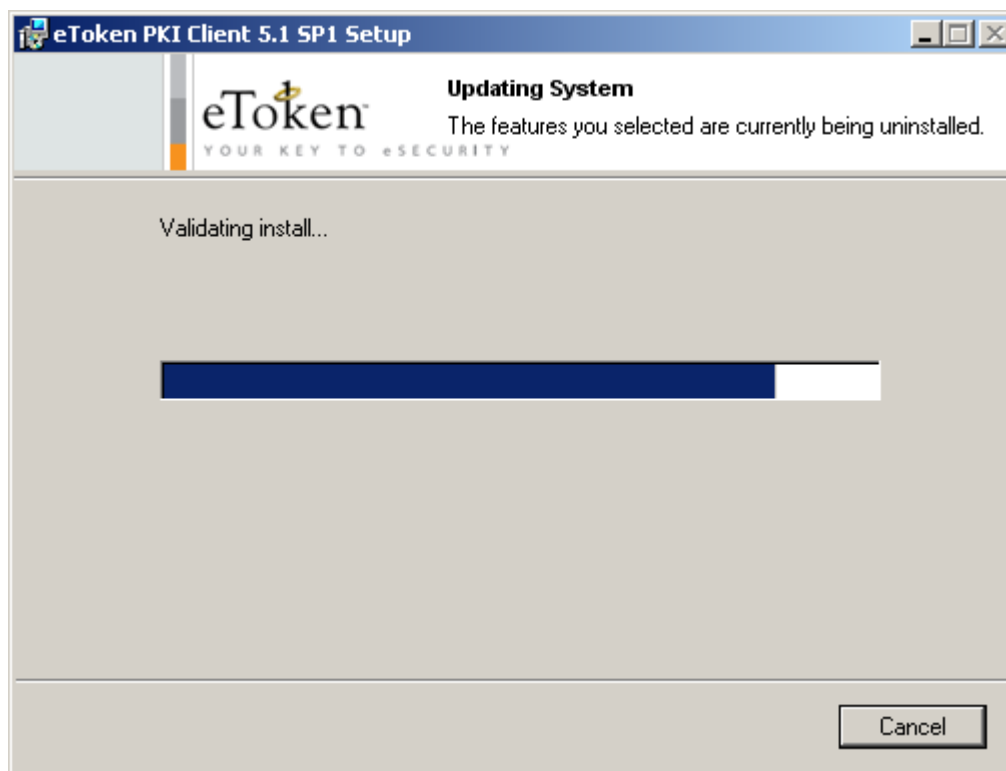
На экране появится следующее окно, где вам будет предложено либо удалить, либо восстановить приложение, если оно работает некорректно:



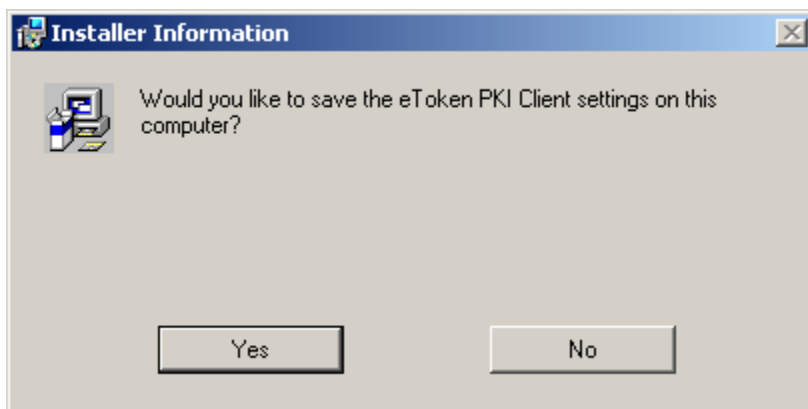
4. Выберите пункт **Remove** и нажмите **Next**. На экране появится приветственное окно программы-мастера.



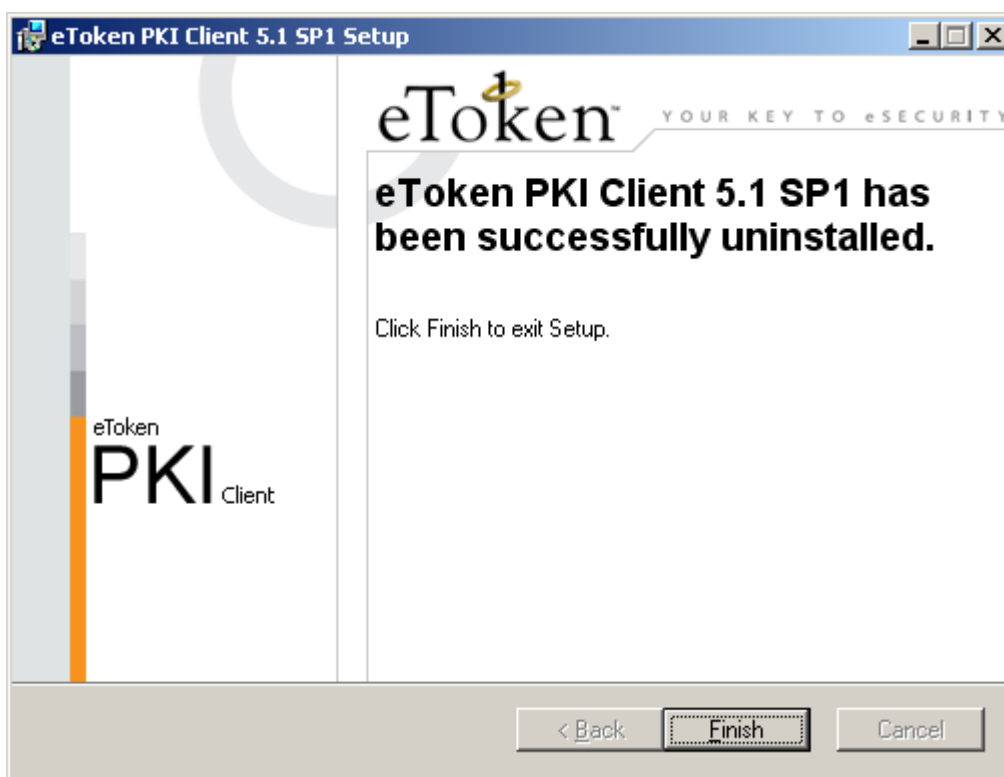
5. Нажмите кнопку **Next**, и сразу после этого начнется удаление eToken PKI Client. В следующем окне в виде шкалы с комментариями будет отображаться состояние процесса.



6. Во время удаления eToken PKI Client на экране появится окно, где вам будет предложено удалить или сохранить параметры eToken PKI Client в реестре.



7. Если вы собираетесь в дальнейшем работать с аппаратными или виртуальными ключами eToken, возможно, будет лучше, если вы оставите уже настроенные вами параметры. Тогда в этом окне нужно нажать **Yes**. Если вы уверены, что больше не собираетесь пользоваться eToken PKI Client, нажмите **No**. После этого удаление продолжится и, после того как оно будет закончено, на экране появится подтверждающее сообщение:



На этом удаление eToken PKI Client закончено. Закройте окно, нажав кнопку **Finish** и перезагрузите компьютер.

### 6.10.3 Удаление из командной строки

Чтобы удалить Token PKI Client из командной строки, выполните следующие действия:

1. Войдите в систему под учетной записью с правами администратора.
2. Закройте все приложения.
3. Откройте меню **Пуск > Программы > Стандартные > Командная строка**.
4. Если вы запускаете командный интерпретатор в Windows Vista, вы должны щелкнуть правой кнопкой на пункте Командная строка, выбрать **Запуск от имени** и учетную запись администратора.
5. Выполните команду msixec в следующем формате:

msixec /x PKIClient-x32-5.1-SP1.msi,

Где PKIClient-x32-5-1-SP1.msi – имя файла с обновлением. Для 64-битной платформы замените это имя на PKIClient-x64-5-1-SP1.msi. Чтобы выполнить обновление в полуавтоматическом режиме, добавьте в конце строки параметр /q. Вместо файла msi можно также использовать соответствующий платформе файл .msi.

Чтобы выполнить удаление в полуавтоматическом режиме, то есть без необходимости подтверждения действий, добавьте в конце строки параметр /q.

6. После того как eToken PKI Client будет удален, перезагрузите компьютер.

## 7. Настройка eToken PKI Client

---

Все настройки eToken PKI Client, за исключением тех, которые устанавливаются только в процессе установки, можно настроить в оснастке eToken PKI Client Settings. С помощью этой оснастки настраивать параметры намного удобнее, чем из стандартного редактора реестра Windows.

Краткое содержание главы:

- Общие сведения об оснастке eToken PKI Client Settings.
- Как добавить оснастку eToken PKI Client Settings на серверной платформе Windows.
- Как добавить оснастку eToken PKI Client Settings на Windows XP.
- Применение параметров, заданных в eToken PKI Client Settings.

### 7.1. Общие сведения об оснастке eToken PKI Client Settings.

Вместе с документацией в дистрибутив входит файл eTokenPKIClient 5.1.adm, в котором собраны стандартные параметры eToken PKI Client. Этот файл приведен специально как шаблон и его можно править по своему усмотрению.

- Файл можно использовать для применения параметров eToken PKI Client.
- Посредством групповых политик на серверных платформах Windows.
- Через консоль управления (MMC) в Windows XP.

Настройки, заданные в административном шаблоне eToken PKI Client Settings, отражаются в реестре системы. Эти параметры более подробно описаны далее в главе Параметры реестра.

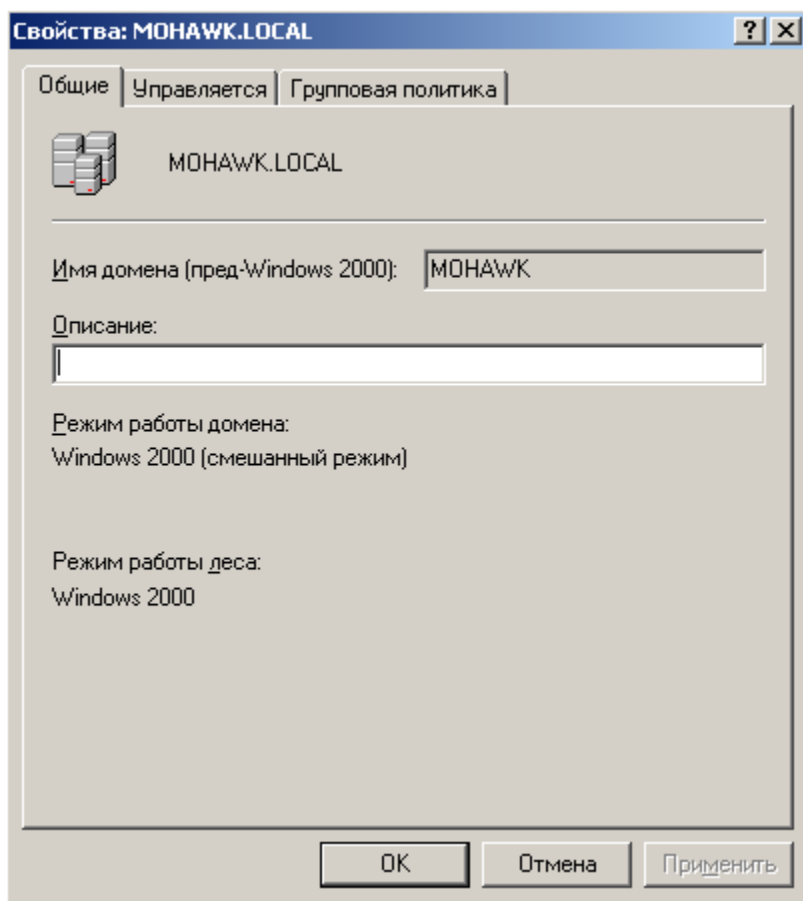
В предложенном adm-файле все параметры сохраняются в раздел HKEY\_LOCAL\_MACHINE\Software\Policies\Aladdin\eToken\MIDDLEWARE.

Параметры в этом разделе имеют наивысший приоритет по отношению к параметрам в любых других разделах. При необходимости вы можете отредактировать имеющийся adm-файл так, чтобы параметры сохранялись в другой раздел. Иерархия разделов реестра более подробно описана далее.

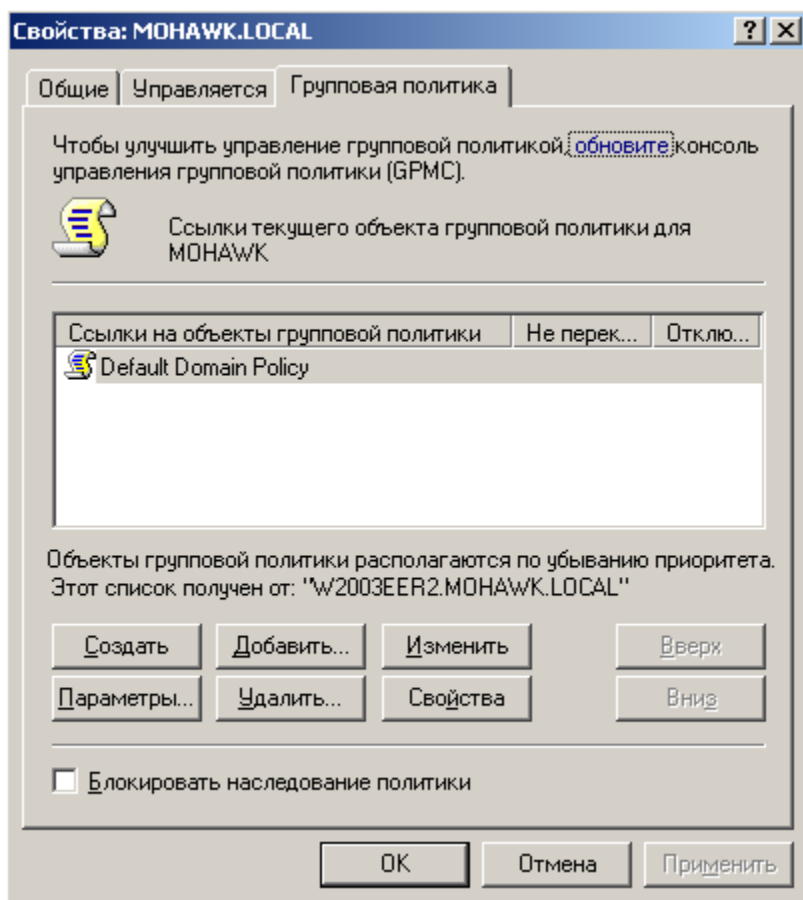
#### 7.1.1 Как добавить административный шаблон eToken PKI Client Settings на серверной платформе Windows

Прежде чем начинать работать с административным шаблоном eToken PKI Client Settings, необходимо добавить его в редакторе групповых политик. Для этого необходимо выполнить следующие действия:

1. Откройте **Пуск > Программы > Администрирование > Пользователи и компьютеры Active Directory**.
2. Щелкните правой кнопкой мыши на домене слева и в открывшемся контекстном меню выберите пункт **Свойства**. На экране откроется следующее окно.



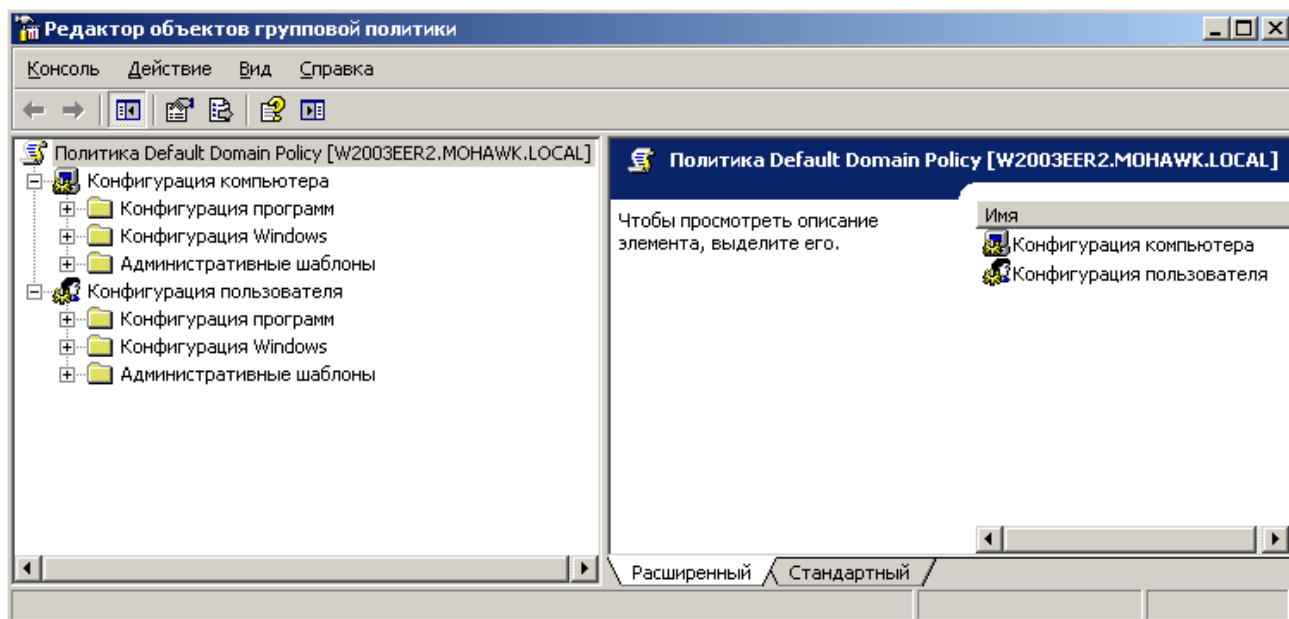
3. Раскройте вкладку **Групповые политики**.



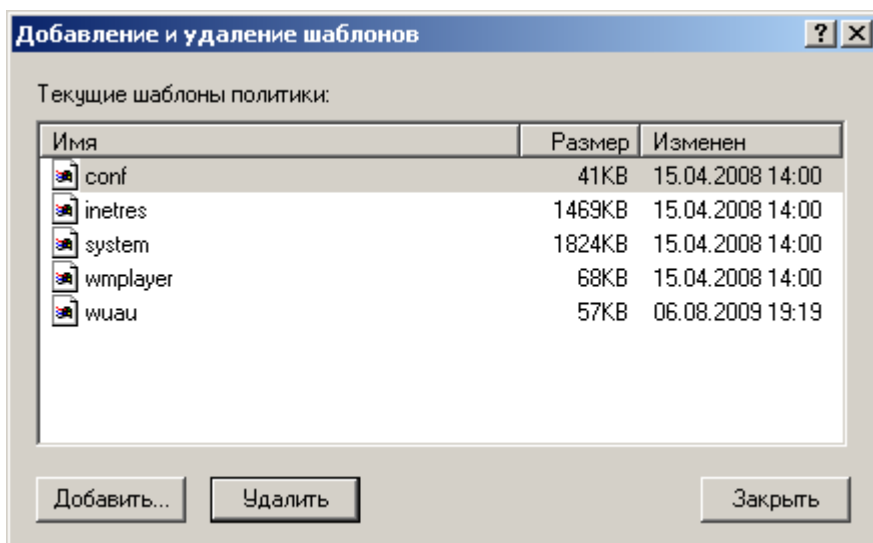
4. Выберите **Групповую политику по умолчанию** и нажмите кнопку **Изменить**.



На экране откроется окно редактора групповых политик.

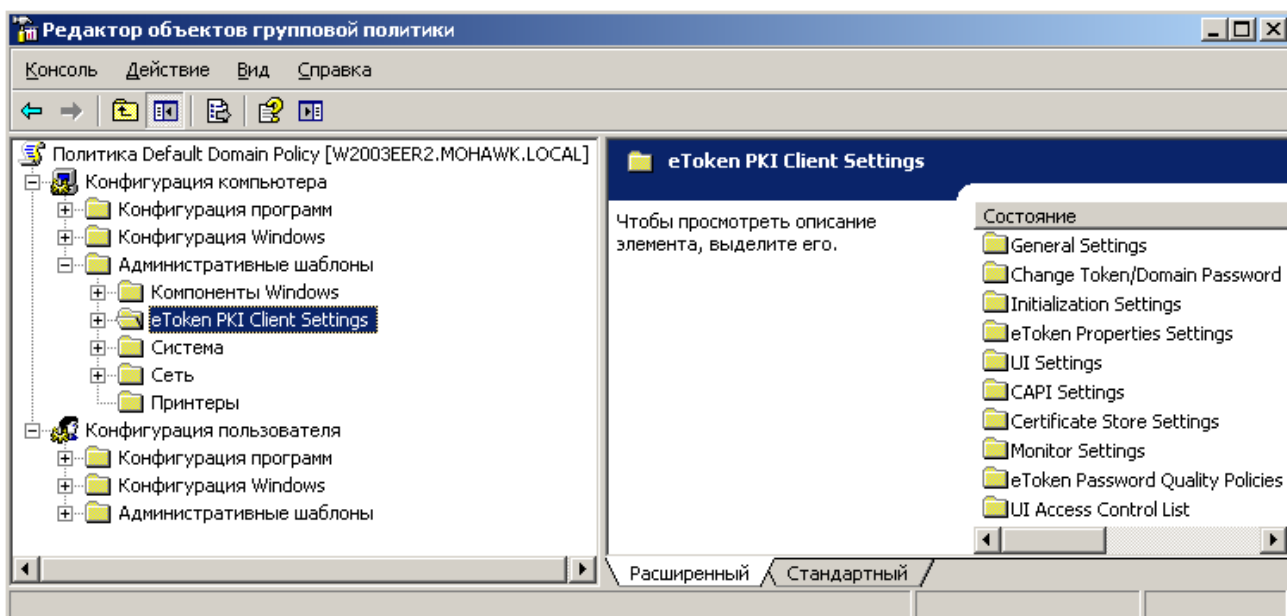


5. Раскройте ветвь **Конфигурация компьютера**, щелкните правой кнопкой мыши на пункте **Административные шаблоны**.
6. В контекстном меню выберите пункт **Добавление и удаление шаблонов**. На экране появится следующее мен.



7. Нажмите кнопку **Добавить** и укажите путь к файлу eTokenPKIClient\_5\_1.adm, который поставляется вместе с дистрибутивом. Теперь в представленном на рисунке выше списке появится шаблон с именем eTokenPKIClient\_5\_1.
8. Нажмите **Закреть**. Теперь в списке административных шаблонов появится добавленный вами шаблон **eToken PKI Client Settings**.

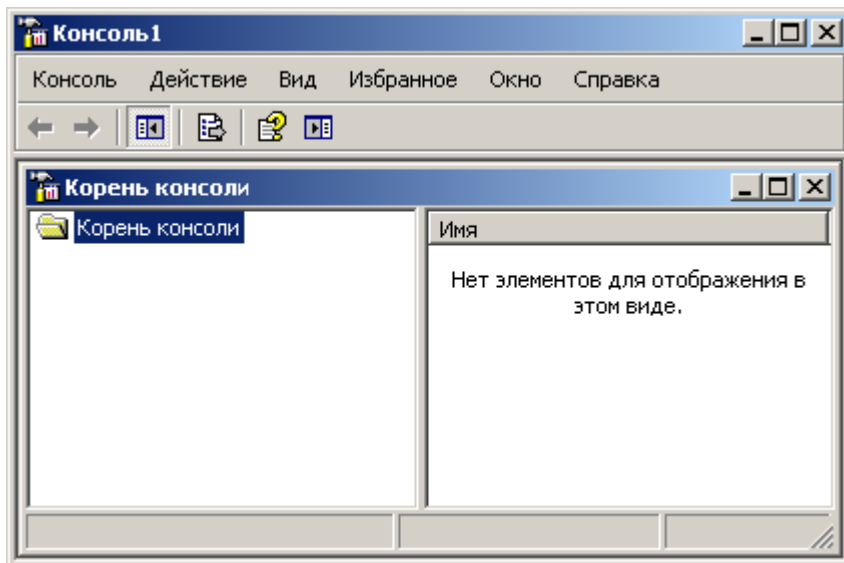
Теперь, если вы откроете ветвь eToken PKI Client Settings, вы увидите список параметров eToken PKI Client с описаниями и возможными значениями в правой части окна.



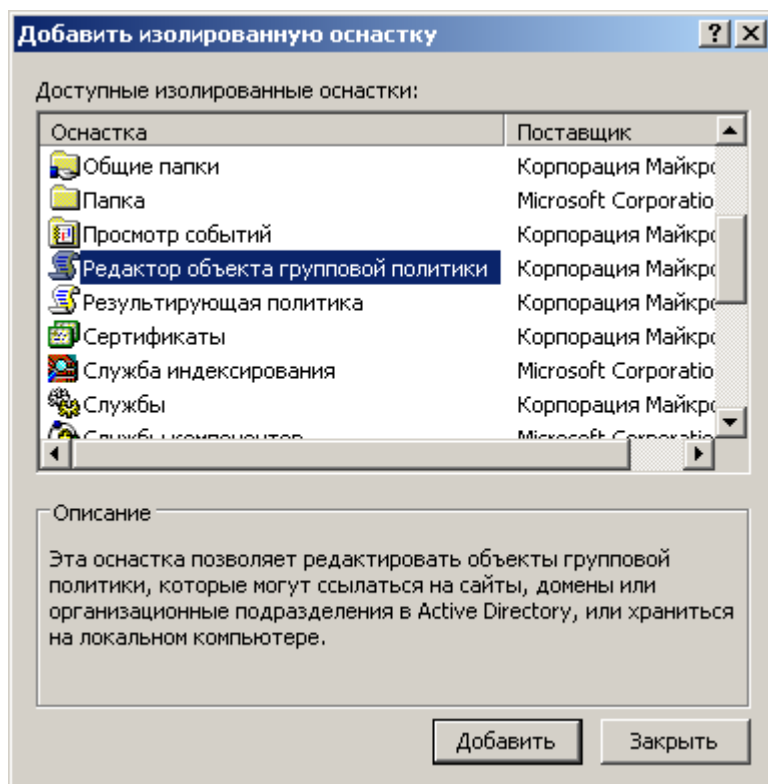
### 7.1.2 Как добавить административный шаблон eToken PKI Client Settings в Windows XP

Чтобы вам не приходилось настраивать параметры eToken PKI Clients непосредственно в реестре, вы можете добавить административный шаблон eToken PKI Client Settings. Для этого выполните следующие действия.

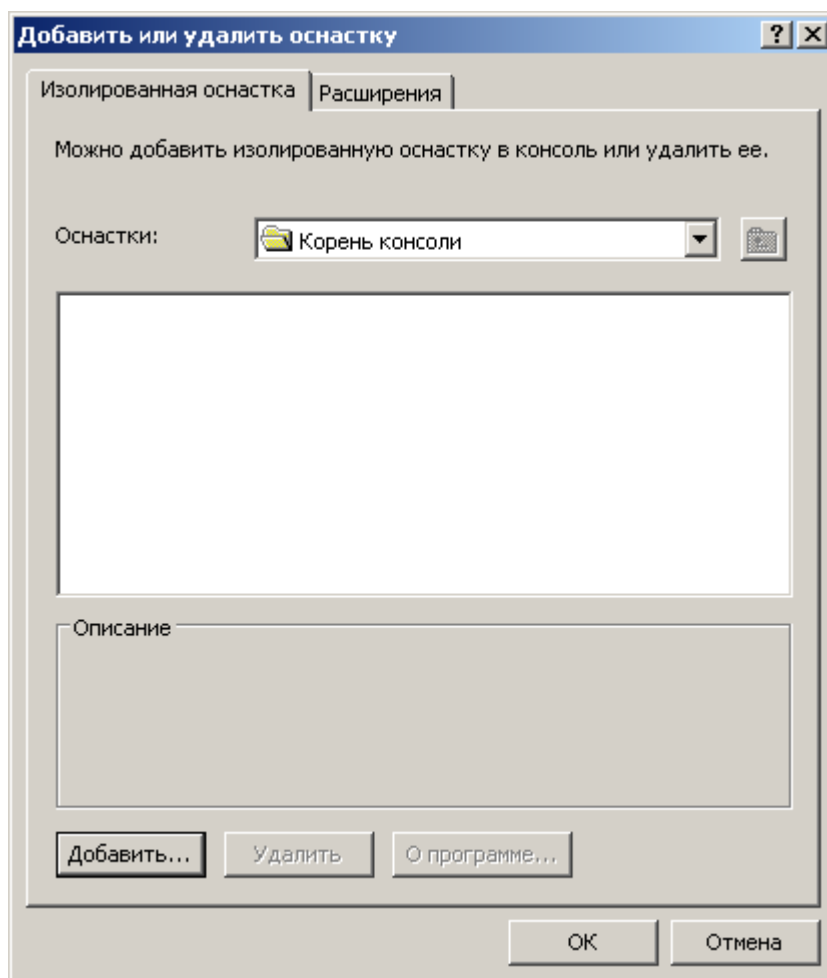
1. Откройте **Пуск > Выполнить**.
2. В поле **Открыть** введите mmc. На экране откроется окно консоли управления.



3. В верхнем меню выберите **Консоль > Добавить или удалить оснастку**.
4. В открывшемся меню нажмите кнопку **Добавить**.

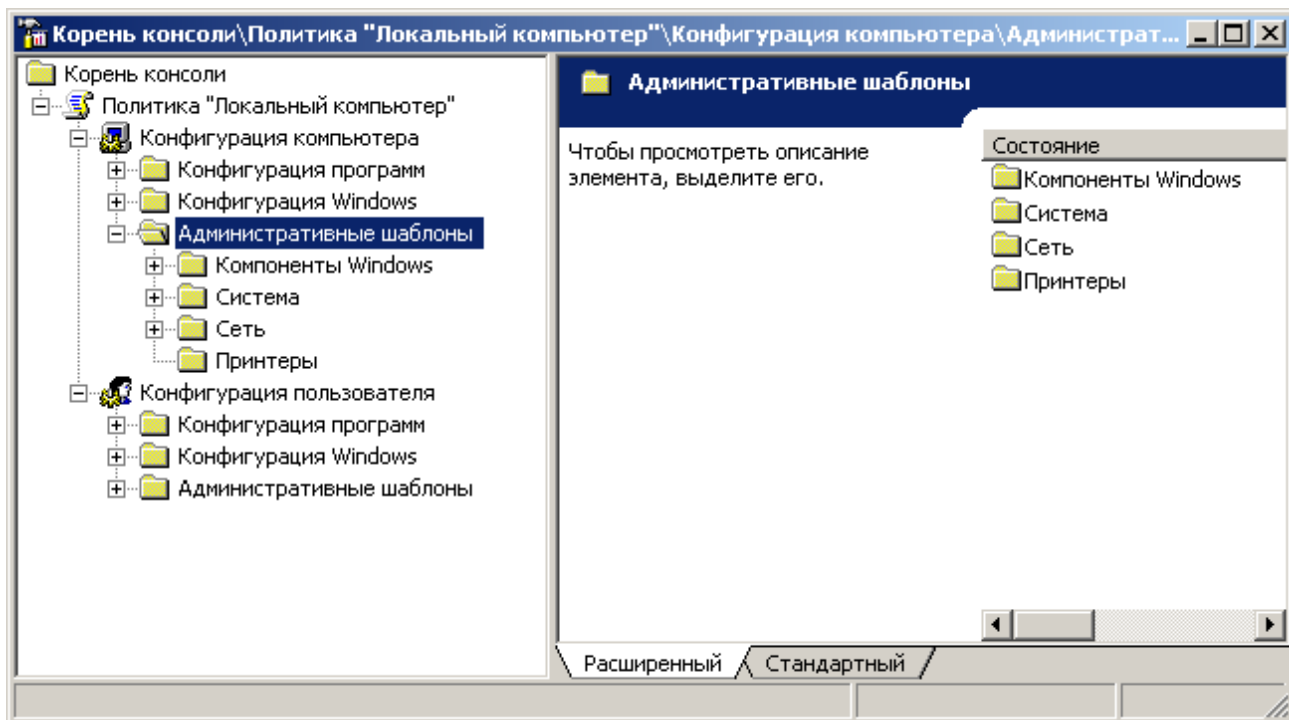


5. В списке доступных оснасток выберите **Редактор объекта групповой политики** и нажмите **ОК**. На экране появится следующее окно.



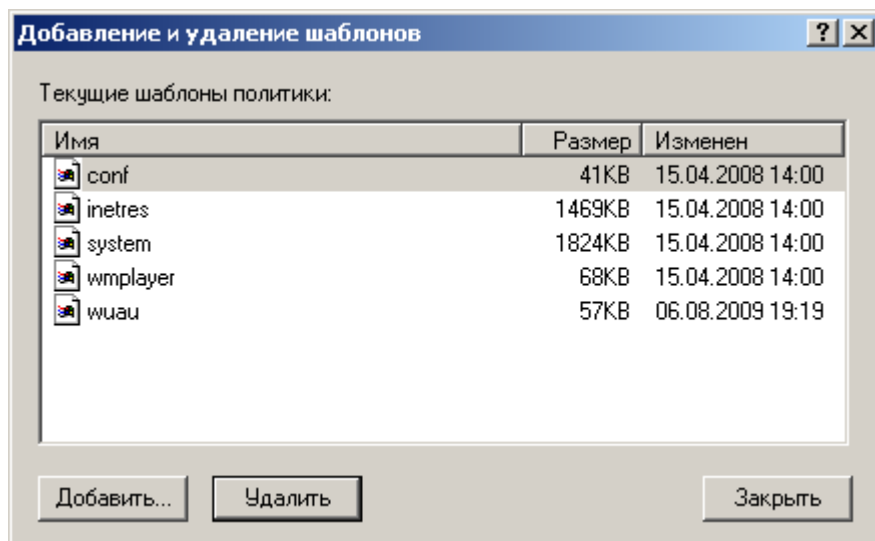
6. Оставьте установленный по умолчанию объект групповой политики (Локальный компьютер) и нажмите **Готово**.

7. Теперь в дереве консоли раскройте ветвь **Политика «Локальный компьютер» > Конфигурация** компьютера так, как показано на следующем рисунке.

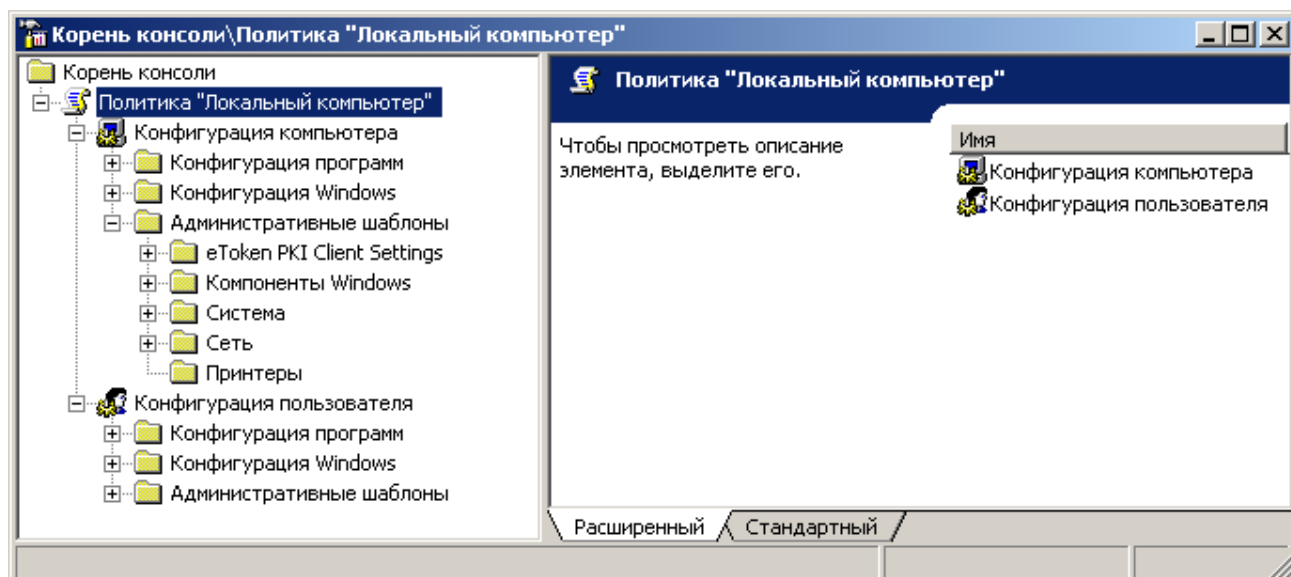


8. Щелкните правой кнопкой мыши на пункте **Административные шаблоны** и в открывшемся контекстном меню выберите **Добавление и удаление шаблонов**.

На экране появится меню следующего вида.



9. Нажмите кнопку **Добавить** и в открывшемся окне укажите путь к файлу eTokenPKIClient\_5\_1.adm.
10. В списке доступных шаблонов появится запись eTokePKIClient.
11. Закройте окно и теперь вы увидите в дереве консоли новый административный шаблон – eToken PKI Client Settings.



12. Когда вы будете закрывать консоль управления, не забудьте сохранить настройки для последующего обращения.

Если вы выполнили все описанные выше действия правильно, то для обращения к параметрам eToken PKI Client из консоли управления Microsoft вам достаточно будет открыть сохраненный вами файл с расширением msc из меню **Пуск > Выполнить**.

## 7.2. Настройка параметров eToken PKI Client Settings из консоли управления Microsoft

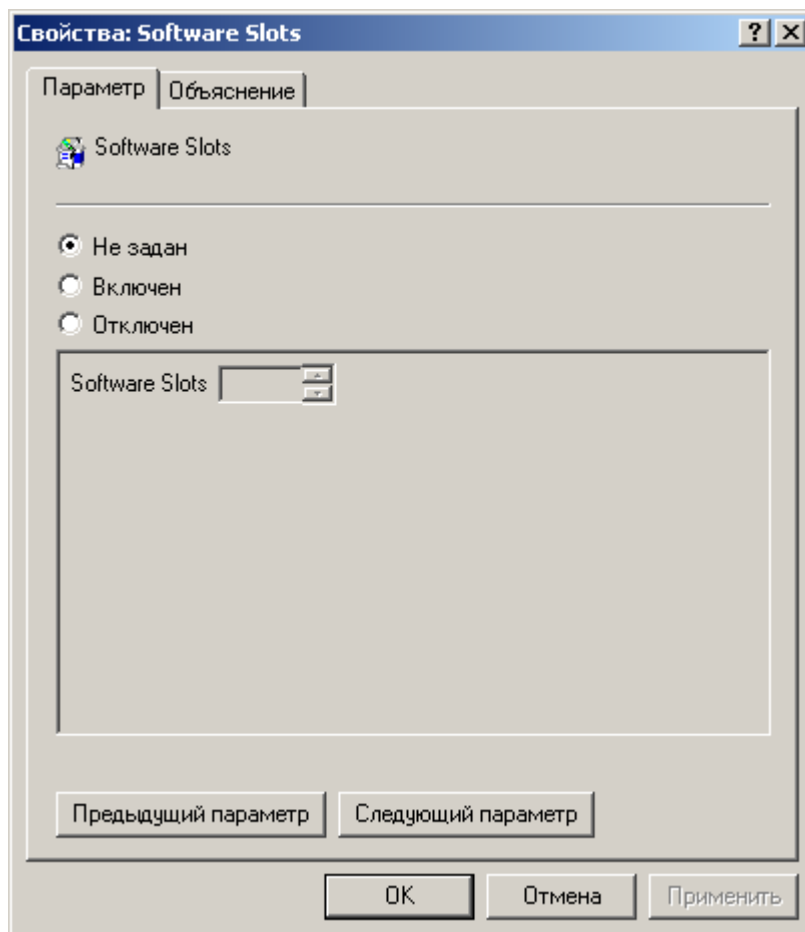
Все параметры eToken PKI Client организованы в консоли управления Microsoft по отдельным папкам. Более подробное описание каждого из параметров можно найти далее в главе Параметры

### Примечание:

Независимо от выбранного вами при установке языка интерфейса все параметры в консоли управления Microsoft отображаются только на английском. Поэтому именно так, на английском, эти параметры будут упоминаться далее в руководстве.

Чтобы изменить тот или иной параметр eToken PKI Client, [откройте административный шаблон eToken PKI Client Settings](#) на серверной платформе Windows или [откройте сохраненную консоль управления](#) так, как описано в окончании предыдущей главы.

1. Щелкните дважды на параметре. На экране откроется окно настройки выбранного параметра.
2. В данном примере открыто окно параметра, который задает количество виртуальных считывателей (для ключей eToken Virtual). Все возможные значения и переключатели представлены на вкладке Параметры, а на вкладке **Объяснение** приведено краткое пояснение по данному параметру.



3. Кроме того, на вкладке Параметр для каждого параметра имеется группа переключателей:
- **Не задан:** используется наследуемое значение политики или значение по умолчанию, если значение в политике также не заданно.
  - **Включен:** если отметить этот пункт, можно будет задать значение параметра, и это значение будет иметь силу после обновления групповой политики или после перезагрузки.
  - **Отключен:** используется значение по умолчанию.

Более подробную информацию об административных шаблонах и действии политик можно найти в официальной документации Microsoft.

Для перехода к следующему или предыдущему параметру используйте соответственно кнопки Следующий параметр и Предыдущий параметр.

### 7.3. Как применить настройки eToken PKI Client

После того как вы задали параметры в редакторе групповых политик, необходимо, во-первых, обновить параметры реестра на сервере, а во-вторых, на всех клиентских компьютерах, на которых установлен eToken PKI Client. Данная процедура включает в себя следующие шаги.

1. На сервере откройте **Пуск > Выполнить** и в командной строке введите **gpupdate**.
2. Нажмите **ОК**. После выполнения команды на сервере вступят в силу параметры, установленные в редакторе групповых политик.

Повторите те же действия на всех компьютерах, где установлен eToken PKI Client. При этом на каждом компьютере будут получены параметры с сервера.

## 8. Параметры и настройки

---

Помимо тех параметров, которые установлены в eToken PKI Client, есть также параметры объекта групповой политики, которые по усмотрению администратора могут быть заданы как более приоритетные. Большинство параметров eToken PKI Client хранятся в реестре. Их описанию как раз посвящен данный раздел.

Краткое содержание:

- Общие сведения о параметрах
- Иерархия параметров
- Настройка параметров реестра вручную
- Таблицы параметров

### 8.1. Общие сведения о параметрах

Конфигурация eToken PKI Client и связанные с ней параметры реестра определяют его интерфейс и обработку различных событий. Задать значение параметров можно несколькими способами, однако они работают не для всех параметров, и такие исключения указаны в тексте описания для каждого из таких параметров.

Итак, значения параметров устанавливаются:

- **В процессе установки из командной строки** (но не при восстановлении приложения). Эта возможность уже обсуждалась ранее в главе [Параметры, определяемые только в процессе установки](#). При этом в командной строке указывается название свойства, но не имя параметра.
- **В утилите eToken Properties**. Здесь не нужно знать имени свойства или параметров реестра. Более подробно о том, как работать с этой утилитой, читайте в руководстве пользователя.

#### Примечание:

---

Значения, заданные в приложении eToken Properties, сохраняются индивидуально для каждого пользователя (HKEY\_CURRENT\_USER), а не для всех пользователей компьютера (HKEY\_LOCAL\_MACHINE).

---

- **В административном шаблоне eToken PKI Client Settings**. Добавление шаблона и настройка параметров с его помощью описаны более подробно в главе [Как добавить административный шаблон eToken PKI Client Settings на серверной платформе Windows](#) (для Windows Server 2003/2008/2008 R2) и [Как добавить административный шаблон eToken PKI Client Settings в Windows XP](#) (для Windows XP).
- **Настройка параметров реестра вручную**. Подробнее о параметрах реестра читайте в главе [Настройка параметров реестра вручную](#). В этом случае требуется только имя параметра, но не имя изменяемого свойства.

### 8.2. Иерархия параметров

Любой параметр реестра может быть представлен в четырех разделах реестра. Если задать такой параметр в разделе, который требует административных полномочий, то его он будет иметь преимущественное значение.

Таким образом, для приложения будет иметь силу тот параметр, который находится в иерархии разделов реестра выше.

- HKEY\_LOCAL\_MACHINE\Software\Policies\Aladdin\eToken\MIDDLEWARE (требуется полномочия администратора).
- HKEY\_CURRENT\_USER\Software\Policies\Aladdin\еToken\MIDDLEWARE (требуется полномочия администратора).
- HKEY\_CURRENT\_USER\Software\Aladdin\eToken\MIDDLEWARE (полномочия администратора не требуются).
- HKEY\_LOCAL\_MACHINE\Software\Aladdin\eToken\MIDDLEWARE (полномочия администратора не требуются).
- Стандартное значение eToken PKI Client.

### 8.3. Настройка параметров реестра вручную

Чтобы настроить параметры eToken PKI Client в реестре, выполните следующие действия

1. Откройте **Пуск > Выполнить**.
2. В поле **Открыть** введите regedit и нажмите **ОК**.

На экране откроется редактор реестра, и в левой части окна вы увидите древовидную структуру разделов реестра.

3. Раскройте требуемый раздел и выберите в нем тот параметр, для которого вы хотите изменить значение. Значения параметров отображаются в правой части окна.
4. Чтобы задать значение параметра в реестре, используйте имя этого параметра, а не свойство приложения.

## 8.4. Описание параметров реестра

О том, как редактировать параметры eToken PKI Client в реестре, было сказано выше. А в этой главе будут перечислены все параметры с их описаниями и возможными значениями.

Все представленные далее параметры можно задавать при установке eToken PKI Client из командной строки. Эти параметры хранятся в разделе  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Aladdin\eToken\MIDDLEWARE.

### 8.4.1 Раздел GENERAL

Все перечисленные далее параметры сохраняются в реестре в разделе GENERAL.

Эмуляция подключенного виртуального считывателя

<b>Свойство</b>	Не указывается при установке из командной строки
<b>Параметр реестра</b>	EmulateConnectedVR
<b>Описание</b>	Последний подключенный eToken Virtual на диске отображается как смарт-карта, подключенная к считывателю «AKS VR 0»; Данный параметр присутствует только в Windows XP
<b>Значение DWORD</b>	1 (Истина) – последний подключенный eToken Virtual отображается как смарт-карта, 0 (Ложь) – последний подключенный eToken Virtual НЕ отображается как смарт-карта
<b>Значение по умолчанию</b>	0

#### Примечание

Если eToken Virtual находится не на диске, а на внешнем носителе, он отображается как смарт-карта независимо от значения данного параметра.

Кэширование закрытых данных

<b>Свойство</b>	Не указывается при установке из командной строки
<b>Параметр реестра</b>	EnablePrvCache



<b>Описание</b>	Использование кэша для хранения данных в течение сеанса. Если этот параметр имеет значение «Истина», то данные кэшируются. При этом должно удовлетворяться одно из следующих условий: <ul style="list-style-type: none"> <li>• При инициализации eToken в его параметрах должна быть установлена возможность кэширования закрытых данных.</li> <li>• Параметр PrivatedataCaching не должен иметь значения «0».</li> </ul>
<b>Значение DWORD</b>	1 (Истина) – закрытые данные кэшируются 0 (Ложь) – закрытые данные НЕ кэшируются.
<b>Значение по умолчанию</b>	1 (Истина)
<b>Как установить</b>	В утилите eToken Properties

## Количество аппаратных слотов

<b>Свойство</b>	PROP_PCSCSLOTS
<b>Параметр реестра</b>	PcscSlots
<b>Описание</b>	Количество аппаратных слотов (для подключения USB-ключей и смарт-карт eToken).
<b>Значение DWORD</b>	0-16 0 = подключение USB-ключей и смарт-карт eToken невозможно, используются только ключи eToken Virtual.
<b>Значение по умолчанию</b>	8
<b>Как установить</b>	Данный параметр можно установить как при установке в режиме командной строки, так и в утилите eToken Properties.

## Однократный запрос пароля для доступа к функциям утилиты eToken Properties

<b>Свойство</b>	PROP_SINGLE_LOGON
<b>Параметр реестра</b>	SingleLogon
<b>Описание</b>	Данный параметр указывает на необходимость (или отсутствие необходимости) повторной авторизации с паролем пользователя в рамках одного сеанса работы с утилитой eToken Properties, если это требуется для доступа к соответствующим функциям программы.
<b>Значение DWORD</b>	1 (Истина) – для доступа к функциям расширенного режима eToken Properties достаточно однократной авторизации. 0 (Ложь) – запрос на ввод пароля пользователя появляется каждый раз при попытке открыть расширенный режим утилиты eToken Properties.
<b>Значение по умолчанию</b>	0 (Ложь)
<b>Как установить</b>	Данный параметр можно установить как при установке в

	режиме командной строки, так и в утилите eToken Properties.
--	---

Если значение параметра SingleLogonTimeout больше «0», то параметр SingleLogon автоматически принимает значение «1».

#### Длительность сеанса

<b>Свойство</b>	PROP_SINGLELOGONTO
<b>Параметр реестра</b>	SingleLogonTimeout
<b>Описание</b>	Данный параметр определяет длительность сеанса в секундах, то есть то время, в течение которого для доступа к функциям расширенного режима eToken PKI Client запрос на ввод пароля пользователя eToken выводиться не будет.
<b>Значение DWORD</b>	>=0
<b>Значение по умолчанию</b>	0 (ограничение по времени отсутствует)
<b>Как установить</b>	Только при установке из командной строки.

#### Количество программных слотов

<b>Свойство</b>	PROP_SOFTWARESLOTS
<b>Параметр реестра</b>	SoftwareSlots
<b>Описание</b>	Количество программных слотов (для подключения eToken Virtual).
<b>Значение DWORD</b>	0-10  0 = подключение eToken Virtual невозможно, используются только аппаратные ключи и смарт-карты eToken.
<b>Значение по умолчанию</b>	2
<b>Как установить</b>	Данный параметр можно установить как при установке в режиме командной строки, так и в утилите eToken Properties.

#### Закрытие сеанса для работы с внешним ПО

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр реестра</b>	TolerantFinalize
<b>Описание</b>	Данный параметр определяет возможность вызова функции C_Finalize из библиотеки DllMain. Данное свойство определяется отдельно для каждого процесса.
<b>Значение DWORD</b>	1 (Истина) – закрытие сеанса работы с eToken со стороны внешнего ПО выполняется посредством вызова команды C_Finalize.  0 (Ложь) – сеанс работы между eToken и внешним ПО можно закрыть только путем отключения eToken.
<b>Значение по умолчанию</b>	0 (Ложь)

#### Примечание:

Параметр TolerantFinalize рекомендуется использовать только при работе с ПО Novell Modular Authentication Service (NMAS).

#### Поиск объектов в eToken

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр реестра</b>	TolerantFindObject
<b>Описание</b>	Если этот параметр имеет значение «Истина», то при ошибочном шаблоне функция C_Find возвращает пустой список объектов вместо ошибки.
<b>Значение DWORD</b>	1 (Истина) – функция C_Find возвращает пустой список вместо ошибки, если шаблон поиска задан неверно. 0 (Ложь) – функция C_Find возвращает ошибку, если в шаблоне поиска содержится ошибка.
<b>Значение по умолчанию</b>	0 (Ложь)

#### Атрибуты сертификатов X509

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр реестра</b>	TolerantX509Attributes
<b>Описание</b>	Данный параметр определяет допустимость различий между атрибутами CKA_SERIAL_NUMBER (серийный номер сертификата) и CKA_SUBJECT (тема) и теми же атрибутами внутри атрибута CKA_VALUE.
<b>Значение DWORD</b>	1 (Истина) – атрибуты могут не совпадать. 0 (Ложь) – атрибуты должны совпадать.
<b>Значение по умолчанию</b>	1 (Истина)

#### Примечание:

Для использования сертификатов формата x.509 в кодировке, отличной от DER, параметр TolerantX509Attributes должен иметь значение «Истина».

В некоторых более ранних версиях eToken PKI Client параметр TolerantX509Attributes по умолчанию имел значение 0 (Ложь).

#### Отключение eToken Virtual при завершении сеанса

<b>Свойство</b>	EtvLogoffUnplug
<b>Описание</b>	Если этот параметр имеет значение «Истина», то при закрытии сеанса работы в Windows происходит отключение eToken Virtual.
<b>Значение DWORD</b>	1 (Истина) – при закрытии сеанса Windows автоматически происходит отключение eToken Virtual. 0 (Ложь) – при закрытии сеанса Windows отключение eToken Virtual не происходит.
<b>Значение по умолчанию</b>	Нет

#### Защита симметричных ключей

<b>Свойство</b>	SensitiveSecret
<b>Описание</b>	Если этот параметр имеет значение «Истина», то симметричные ключи экспортировать нельзя, даже если эти ключи не имеют атрибута закрытого ключа.
<b>Значение DWORD</b>	1 (Истина) – симметричные ключи экспортировать нельзя. 0 (Ложь) – симметричные ключи можно экспортировать.
<b>Значение по умолчанию</b>	0 (Ложь)

#### 8.4.2 Раздел SyncPin

Следующий параметр хранится в реестре в разделе SyncPin.

Синхронизация пароля пользователя eToken с доменным паролем

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр реестра</b>	Domain
<b>Описание</b>	Если этот параметр имеет значение «Истина», то пароль пользователя eToken синхронизируется с паролем для доступа в домен.
<b>Строковое значение</b>	Имя домена (без суффикса), с которым выполняется синхронизация.  Если значение параметра не установлено, то синхронизация не выполняется.
<b>Значение по умолчанию</b>	Отсутствует.

#### 8.4.3 Раздел Init

Все перечисленные далее параметры сохраняются в реестре в разделе Init.

Поддержка алгоритма HMAC-SHA1 для выработки одноразовых паролей

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр реестра</b>	HMAC-SHA1
<b>Описание</b>	Отображение опции Поддержка OTP в параметрах инициализации.
<b>Значение DWORD</b>	1 (Истина) – выработка одноразовых паролей с поддержкой HMAC-SHA1 включена. 0 (Ложь) – выработка одноразовых паролей с поддержкой HMAC-SHA1 отключена.
<b>Значение по умолчанию</b>	1 (Истина) – при инициализации eToken NG-OTP (Java), eToken Java/OTP и т.п поддержка HMAC-SHA1 включена. 0 (Ложь) – все прочие модели инициализируются без поддержки алгоритма HMAC-SHA1.
<b>Как установить</b>	В утилите eToken Properties.

Поддержка более ранних версий операционных систем

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр</b>	Legacy-Format-Version

<b>реестра</b>	
<b>Описание</b>	Совместимость с более ранними версиями ОС.
<b>Значение DWORD</b>	<p>0 – при инициализации обеспечивается обратная совместимость с ранними версиями CardOS.</p> <p>4 – при инициализации обратная совместимость с более ранними версиями ОС не обеспечивается.</p> <p>5 – все сгенерированные по алгоритму RSA ключи сохраняются в отдельных папках (CardOS 4.2 FIPS и Java Card).</p>
<b>Значение по умолчанию</b>	4
<b>Как установить</b>	В утилите eToken Properties.

## Кэширование закрытых данных

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр реестра</b>	PrivateDataCaching
<b>Описание</b>	Действие данного параметра зависит от значения параметра EnablePrvCache и устанавливает возможность кэширования закрытых данных.
<b>Значение DWORD</b>	<p>0 – закрытые данные не кэшируются.</p> <p>1 – закрытые данные кэшируются только с того момента, как пользователь авторизуется со своим паролем eToken и до того момента, пока он не отключит свой eToken.</p> <p>2 – Закрытые данные кэшируются и сохраняются.</p>
<b>Значение по умолчанию</b>	2
<b>Как установить</b>	В утилите eToken Properties.

## Объем свободного пространства для хранения ключей RSA

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр реестра</b>	RSA-Area-Size
<b>Описание</b>	Объем памяти в байтах, зарезервированный для хранения ключей RSA. Данный параметр применяется для устройств eToken под управлением CardOS.
<b>Значение DWORD</b>	<p>&gt;=0</p> <p>0 = создавать ключи RSA нельзя.</p>
<b>Значение по умолчанию</b>	<p>В зависимости от модели eToken:</p> <p>В eToken с памятью 16Kб будет выделен объем, достаточный для хранения трех ключей RSA.</p>

В eToken с памятью 32Kб будет выделен объем, достаточный для хранения пяти ключей RSA.

В eToken с большим объемом памяти будет выделено пространство, достаточное для хранения семи ключей RSA.

**Примечание:**

---

Параметр RSA-Area-Size не имеет никакой силы, если параметр Legacy-Format-Version имеет значение 5.

---

## Дополнительная защита симметричных ключей RSA

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр реестра</b>	RSASecondaryAuthenticationMode
<b>Описание</b>	Метод создания ключей RSA.
<b>Значение DWORD</b>	<p>0 – ETCK_2NDAUTH_PROMPT_NEVER: Никакие новые сгенерированные ключи RSA не защищены паролем.</p> <p>1 – ETCK_2NDAUTH_PROMPT_CONDITIONAL: Если внешним приложением для параметра CKA_ALWAYS_AUTHENTICATE установлено значение «Истина», то при создании ключа будет предложено задать пароль.</p> <p>2 – ETCK_2NDAUTH_PROMPT_ALWAYS: При создании ключа появляется запрос на ввод пароля.</p> <p>3 – ETCK_2NDAUTH_MANDATORY: все ключи RSA должны быть защищены паролем.</p>
<b>Значение по умолчанию</b>	3
<b>Как установить</b>	В утилите eToken Properties.

## Создание ключей RSA длиной 2048 бит

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр реестра</b>	RSA-2048
<b>Описание</b>	Возможность создания ключей RSA длиной 2048 байт
<b>Значение DWORD</b>	<p>1 (Истина) – пункт Поддержка ключей RSA длиной 2048 бит отмечен.</p> <p>0 (Ложь) – пункт Поддержка ключей RSA длиной 2048 бит не отмечен.</p>
<b>Значение по умолчанию</b>	0 (Ложь) – пункт Поддержка ключей RSA длиной 2048 бит не отмечен, то есть создавать ключи RSA размером 2048 бит на инициализированном eToken будет невозможно.
<b>Как установить</b>	В утилите eToken Properties.

## 8.4.4 Раздел реестра InitApp

Все перечисленные далее параметры сохраняются в реестре в разделе InitApp.

## Доступ к настройкам расширенного режима

<b>Свойство</b>	PROP_ADVANCED_VIEW
<b>Параметр реестра</b>	AdvancedView
<b>Описание</b>	Отображение кнопки «Подробный вид» (значок со «звездой»)
<b>Значение DWORD</b>	<p>1 (Истина) – кнопка отображается.</p> <p>0 (Ложь) – кнопка не отображается.</p>
<b>Значение по умолчанию</b>	1 (Истина) – кнопка отображается.
<b>Как установить</b>	Только из командной строки.

## Значок в области уведомлений

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр реестра</b>	ShowInTray
<b>Описание</b>	Отображение значка в области уведомлений вместе с загрузкой eToken PKI Client.
<b>Значение DWORD</b>	1 (Истина) – значок отображается. 0 (Ложь) – значок не отображается.
<b>Значение по умолчанию</b>	1 (Истина) – значок отображается.

## 8.4.5 Раздел реестра CAPI

Все перечисленные далее параметры сохраняются в реестре в разделе CAPI.

## Повторная авторизация

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена
<b>Параметр реестра</b>	LogoutMode
<b>Описание</b>	Вывод запроса на ввод пароля пользователя eToken для каждой операции, которая требует авторизации.
<b>Значение DWORD</b>	1 (Истина) – повторная авторизация обязательна. 0 (Ложь) – запрос на авторизацию пользователя не появляется.
<b>Значение по умолчанию</b>	0 (Ложь)

## Подача заявок на выпуск сертификатов от имени другого пользователя

В eToken PKI Client предусмотрены два параметра, которые определяют возможность выдачи сертификата для другого пользователя: это параметры NoDefaultKeyContainer и DefEnrollType.

Для подачи заявки на выдачу сертификата от имени другого пользователя будут использоваться два устройства eToken:

- **eToken агента:** eToken, на котором хранится сертификат агента подачи заявок.
- **eToken пользователя:** eToken, на котором сохраняется запрошенный сертификат.

Таким образом, параметр [NoDefaultKeyContainer](#) определяет саму возможность подачи заявок от имени другого пользователя, в то время как параметр [DefEnrollType](#) устанавливает ограничение на наличие других сертификатов на eToken агента.

В зависимости от сочетания значений этих двух параметров будут возможны описанные далее [типовые сценарии](#).

## Запрос на выдачу сертификатов для другого пользователя

<b>Свойство</b>	PROP_EXPLORER_DEFENROLL
<b>Параметр реестра</b>	NoDefaultKeyContainer (в более ранних версиях – DefEnrollType)
<b>Описание</b>	Позволяет использовать отдельно два eToken: 1) eToken с сертификатом агента подачи заявок; 2) eToken пользователя, где будет сохранен запрашиваемый сертификат.



<b>Значение DWORD</b>	1 (Истина) – возможность выпуска сертификата на другой eToken НЕ допускается. 0 (Ложь) – возможность выпуска сертификата на другой eToken допускается.
<b>Значение по умолчанию</b>	1 (Истина) – в Internet Explorer. 0 (Ложь) – в остальных случаях.
<b>Как установить</b>	Только из командной строки.

Наличие других сертификатов на eToken агента

<b>Параметр реестра</b>	DefEnrollType
<b>Описание</b>	Данный параметр указывает на возможность наличия на eToken агента других сертификатов.
<b>Значение DWORD</b>	1 (Истина) – допускается возможность выпуска сертификатов для другого пользователя с использованием одного eToken, содержащего сертификат агента подачи заявок и также другие сертификаты. 0 – НЕ допускается возможность выпуска сертификатов для другого пользователя с использованием одного eToken, содержащего сертификат агента подачи заявок и также другие сертификаты.
<b>Значение по умолчанию</b>	Отсутствует

Чтобы понимать, как работают параметры NoDefaultKeyContainer и DefEnrollType и как влияют друг на друга их значения, приведем два типовых сценария:

**Сценарий 1:** На eToken хранится только сертификат агента подачи заявок, при этом сертификат выпускается на другой eToken. Этот сценарий возможен при следующем сочетании параметров NoDefaultKeyContainer и DefEnrollType.

NoDefaultKeyContainer	DefEnrollType
0	1
0	0

**Сценарий 2:** На eToken хранится сертификат агента подачи заявок и также другие сертификаты (например, для доступа в систему по смарт-карте). Сертификат создается на другом eToken. Такой сценарий возможен только при следующем сочетании параметров NoDefaultKeyContainer и DefEnrollType.

NoDefaultKeyContainer	DefEnrollType
0	1

## Длительность пользовательского сеанса

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	PasswordTimeout
<b>Описание</b>	Данный параметр указывает на длительность сеанса с момента ввода пароля пользователя eToken.
<b>Значение DWORD</b>	>=0 0 = без ограничений
<b>Значение по умолчанию</b>	0 (Ложь)

## Пароль в кодировке ASCII

eToken PKI Client использует пароли в кодировке ASCII, в то время как некоторые приложения, к числу которых относится служба авторизации по смарт-картам Microsoft, используют другие кодировки. Символы, которые не входят в набор ASCII, интерпретируются по-разному во всех кодировках. Для корректной интерпретации таких паролей необходимо, чтобы данный параметр имел истинное значение, и тогда такие пароли, которые содержат, например, букву «щ», будут интерпретироваться правильно.

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	AsciiPassword
<b>Описание</b>	Поддержка в пароле eToken символов, которые не входят в набор ASCII.
<b>Значение DWORD</b>	1 (Истина) – поддерживаются любые символы. 0 (Ложь) – поддерживаются только символы из кодировки ASCII.
<b>Значение по умолчанию</b>	0 (Ложь)

## 8.4.6 Раздел реестра CertStore

Все перечисленные далее параметры сохраняются в реестре в разделе CertStore.

## Выбор eToken для импорта сертификата

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	AddToTokenOnNewCertInStore
<b>Описание</b>	Значение данного параметра определяет доступ к пункту, указывающему на необходимость импорта сертификата не только в хранилище сертификатов, но также и в указанный eToken.
<b>Значение DWORD</b>	1 (Истина) – пункт отображается. 0 (Ложь) – пункт не отображается.
<b>Значение по умолчанию</b>	1 (Истина)

Срок до удаления сертификата из хранилища

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	CertsToRemoveStorePeriod
<b>Описание</b>	<p>Данный параметр определяет период, в течение которого eToken PKI Client будет пытаться удалить сертификат с eToken, если этот eToken не был подключен на момент удаления сертификата из хранилища.</p> <p>Данный параметр имеет силу только в том случае, если параметр RemoveFromTokenOnRemoveFromStore имеет значение 2.</p>
<b>Значение DWORD</b>	>=0
<b>Значение по умолчанию</b>	7

#### Примечание:

Данный параметр действует тогда, когда удаляемый сертификат был экспортирован в хранилище с eToken.

Экспорт сертификатов ЦС

<b>Свойство</b>	PROP_PROPAGATECACER
<b>Параметр реестра</b>	PropagateCACertificates
<b>Описание</b>	Данный параметр определяет необходимость экспорта всех сертификатов в хранилище доверенного ЦС.
<b>Значение DWORD</b>	<p>1 (Истина) – экспортировать сертификаты в хранилище доверенного ЦС.</p> <p>0 (Ложь) – НЕ экспортировать сертификаты в хранилище доверенного ЦС.</p>
<b>Значение по умолчанию</b>	1 (Истина)
<b>Как установить</b>	Данный параметр можно установить как при установке в режиме командной строки, так и в утилите eToken Properties.

Экспорт сертификатов пользователя

<b>Свойство</b>	PROP_PROPAGATEUSERCER
<b>Параметр реестра</b>	PropagateUserCertificates
<b>Описание</b>	Данный параметр определяет необходимость экспорта всех сертификатов пользователя в пользовательское хранилище.
<b>Значение DWORD</b>	<p>1 (Истина) – экспортировать сертификаты в хранилище пользователя.</p> <p>0 (Ложь) –экспортировать сертификаты в хранилище пользователя.</p>
<b>Значение по умолчанию</b>	1 (Истина)
<b>Как установить</b>	Данный параметр можно установить как при установке в режиме командной строки, так и в утилите eToken

Properties.
-------------

Удаление сертификата из хранилища при отключении eToken

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	RemoveFromStoreOnRemoveFromToken
<b>Описание</b>	Данный параметр определяет необходимость удаления сертификата из хранилища пользовательских сертификатов при отключении eToken.
<b>Значение DWORD</b>	1 (Истина) – удалять сертификат. 0 (Ложь) – не удалять сертификат.
<b>Значение по умолчанию</b>	1 (Истина)

Удаление сертификата из памяти eToken при удалении из хранилища

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	RemoveFromTokenOnRemoveFromStore
<b>Описание</b>	При истинном значении этого параметра пользователю при удалении сертификата из хранилища предлагается также удалить этот сертификат из памяти eToken.
<b>Значение DWORD</b>	0 (Никогда) – запрос на удаление сертификата никогда не появляется. 1 (Всегда) – запрос на удаление сертификата появляется. 2 – запрос появляется только в том случае, если в eToken есть сертификаты, для которых есть шаблоны, указанные в параметре RemoveFromTokenOnRemoveFromStoreTemplates.
<b>Значение по умолчанию</b>	0

Удаление сертификата из памяти eToken при удалении шаблона

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	RemoveFromTokenOnRemoveFromStoreTemplates
<b>Описание</b>	Список шаблонов, при удалении которых происходит удаление самих сертификатов из хранилища. Этот параметр имеют силу только в том случае, когда параметр RemoveFromTokenOnRemoveFromStore имеет значение 2.
<b>Строковое значение</b>	Имена шаблонов
<b>Значение по умолчанию</b>	Отсутствует

Удаление сертификатов при отключении eToken

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	RemoveUserCertsOnTokenRemove
<b>Описание</b>	При истинном значении этого параметра отключение eToken приводит к удалению сертификатов из локального хранилища, если эти сертификаты были экспортированы с eToken. Действие данного параметра распространяется на все устройства eToken.

<b>Значение DWORD</b>	1 (Истина) – пользовательские сертификаты удаляются из хранилища при отключении eToken.
	0 (Ложь) – пользовательские сертификаты НЕ удаляются из хранилища при отключении eToken.
<b>Значение по умолчанию</b>	1 (Истина)

## Синхронизация хранилища

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	SynchronizeStore
<b>Описание</b>	Синхронизация хранилища.
<b>Значение DWORD</b>	1 (Истина) – синхронизация выполняется.
	0 (Ложь) – синхронизация НЕ выполняется.
<b>Значение по умолчанию</b>	1 (Истина)

## 8.4.7 Раздел реестра Monitor

В разделе Monitor имеется только один параметр, который определяет необходимость уведомления пользователя об истечения срока действия его сертификата.

## Уведомление об истечении срока действия пароля

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	NotifyPasswordExpiration
<b>Описание</b>	Если данный параметр имеет истинное значение, то перед истечением срока действия сертификата в области уведомлений будет появляться соответствующее предупреждение.
<b>Значение DWORD</b>	1 (Истина) – показывать предупреждение.
	0 (Ложь) – НЕ показывать предупреждение
<b>Значение по умолчанию</b>	1 (Истина)

## 8.4.8 Раздел реестра PQ

Представленные данные параметры относятся к политике качества паролей и хранятся в реестре в разделе PQ.

## Объем записей в истории

<b>Свойство</b>	PROP_PQ_HISTORYSIZE
<b>Параметр реестра</b>	pqHistorySize
<b>Описание</b>	Значение данного параметра определяет количество ранее использованных паролей, с которыми не должен совпадать новый пароль eToken.
<b>Значение DWORD</b>	>=0
	10
<b>Значение по умолчанию</b>	10
<b>Как установить</b>	Данный параметр можно установить как при установке в режиме командной строки, так и в утилите eToken Properties.

## Использование символов в нижнем регистре

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	pqLowerCase
<b>Описание</b>	Возможность использования символов нижнего регистра в значении пароля.
<b>Значение DWORD</b>	0 – символы нижнего регистра разрешены; 1 – символы нижнего регистра НЕ разрешены; 2 – использование символов нижнего регистра является обязательным.
<b>Значение по умолчанию</b>	0

## Срок действия пароля

<b>Свойство</b>	PROP_PQ_MAXAGE
<b>Параметр реестра</b>	pqMaxAge
<b>Описание</b>	Срок действия пароля в днях.
<b>Значение DWORD</b>	>=0 0 = без ограничений
<b>Значение по умолчанию</b>	0
<b>Как установить</b>	Данный параметр можно установить как при установке в режиме командной строки, так и в утилите eToken Properties.

## Максимальное количество повторений одного символа в значении пароля

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	pqMaxRepeated
<b>Описание</b>	Данный параметр определяет, сколько раз один и тот же символ может повторяться в значении пароля.
<b>Значение DWORD</b>	>=0 0 = без ограничений
<b>Значение по умолчанию</b>	3

## Ограничение по частоте смены паролей

<b>Свойство</b>	PROP_PQ_MINAGE
<b>Параметр реестра</b>	pqMinAge
<b>Описание</b>	Данный параметр определяет минимальный срок (количество дней), через который можно сменить пароль.
<b>Значение DWORD</b>	>=0 0 = без ограничений
<b>Значение по умолчанию</b>	0
<b>Как установить</b>	Данный параметр можно установить как при установке в режиме командной строки, так и в утилите eToken Properties.

## Минимальная длина пароля

<b>Свойство</b>	PROP_PQ_MINLEN
<b>Параметр реестра</b>	pqMinLen
<b>Описание</b>	Данный параметр устанавливает минимальное ограничение по длине пароля (кол-во знаков).
<b>Значение DWORD</b>	>=4
<b>Значение по умолчанию</b>	6
<b>Как установить</b>	Данный параметр можно установить как при установке в режиме командной строки, так и в утилите eToken Properties.

## Использование символов разных типов в значении пароля

<b>Свойство</b>	PROP_PQ_MIXCHARS
<b>Параметр реестра</b>	pqMixChars
<b>Описание</b>	Данный параметр определяет необходимость использования в значении пароля заглавных и прописных букв, цифр и спецсимволов.
<b>Значение DWORD</b>	1 (Истина) – в значении пароля должны использоваться символы разных типов. 0 (Ложь) – ограничение на использование символов разных типов отсутствует.
<b>Значение по умолчанию</b>	1
<b>Как установить</b>	Данный параметр можно установить как при установке в режиме командной строки, так и в утилите eToken Properties.

## Права на редактирование политики паролей

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	pqModifiable
<b>Описание</b>	Данный параметр определяет возможность редактирования политики паролей (см. <a href="#">pqOwner</a> ).
<b>Значение DWORD</b>	1 (Истина) – политика паролей может изменяться только «владельцем». 0 (Ложь) – «владелец» не может менять политику паролей.
<b>Значение по умолчанию</b>	1 - для устройств eToken, принадлежащих администратору. 0 – для устройств eToken, принадлежащих пользователю.

## Использование цифр в значении пароля

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	pqNumbers
<b>Описание</b>	Возможность использование цифр в значении пароля.
<b>Значение DWORD</b>	0 – пароль может содержать цифры. 1 – пароль не может содержать цифры. 2 – пароль обязательно должен содержать цифры.
<b>Значение по умолчанию</b>	0



## Владелец политики паролей

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	pqOwner
<b>Описание</b>	Данный пароль определяет учетную запись, для которой будет возможно редактирование политики после инициализации eToken (см. <a href="#">pqModifiable</a> ).
<b>Значение DWORD</b>	0 – владельцем является администратор. 1 – владельцем является пользователь.
<b>Значение по умолчанию</b>	1 – для устройств eToken с заданным паролем администратора. 0 – для устройств eToken без пароля администратора.

## Использование спецсимволов в значении пароля

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	pqSpecial
<b>Описание</b>	Данный параметр определяет возможность использования специальных символов (например: «@», «!», «&») в значении пароля.
<b>Значение DWORD</b>	0 – пароль может содержать спецсимволы. 1 – пароль не может содержать спецсимволы. 2 – пароль обязательно должен содержать спецсимволы.
<b>Значение по умолчанию</b>	0

## Использование символов верхнего регистра

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	pqUpperCase
<b>Описание</b>	Данный параметр определяет возможность использования символов верхнего регистра.
<b>Значение DWORD</b>	0 – пароль может содержать символы верхнего регистра. 1 – пароль не может содержать символы верхнего регистра. 2 – пароль обязательно должен содержать символы верхнего регистра.
<b>Значение по умолчанию</b>	0

## Уведомление об истечении срока действия пароля

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	pqWarnPeriod
<b>Описание</b>	Данный параметр указывает, за сколько дней до истечения пароля будет отображаться соответствующее предупреждение в области уведомлений.
<b>Значение DWORD</b>	>=0 0 = уведомление не появляется
<b>Значение по умолчанию</b>	0
<b>Как установить</b>	Данный параметр можно установить как при установке в режиме командной строки, так и в утилите eToken Properties.

## Проверка качества паролей при инициализации

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	pqCheckInit
<b>Описание</b>	Проверка и применение параметров качества паролей при инициализации eToken: <ul style="list-style-type: none"> <li>Если регистрация устройств eToken выполняется средствами TMS, этот режим использовать не рекомендуется.</li> <li>При инициализации eToken в утилите eToken Properties, качество паролей не проверяется.</li> </ul>
<b>Значение DWORD</b>	1 (Истина) – выполнять контроль политики качества паролей 0 (Ложь) – не выполнять контроль политики качества паролей
<b>Значение по умолчанию</b>	0

## 8.4.9 Раздел реестра UI

Все представленные далее параметры относятся к интерфейсу пользователя и хранятся в реестре в разделе UI.

## Отображение серийного номера в десятичном формате

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	ShowDecimalSerial
<b>Описание</b>	В зависимости от значения этого параметра серийный номер в утилите eToken Properties отображается в десятичном или в шестнадцатеричном формате.
<b>Значение DWORD</b>	1 (Истина) – серийный номер отображается в десятичном формате. 0 (Ложь) – серийный номер отображается в шестнадцатеричном формате.
<b>Значение по умолчанию</b>	0 – серийный номер eToken представлен в шестнадцатеричном формате.


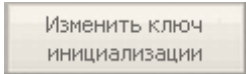








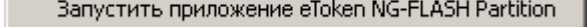


Автоподстановка стандартного значения в запросе на смену пароля

<b>Свойство</b>	Установка в режиме командной строки не предусмотрена.
<b>Параметр реестра</b>	UseDefaultPassword
<b>Описание</b>	Если данный параметр имеет значение «Истина», то при запросе на смену пароля автоматически подставляется стандартное значение («1234567890»)
<b>Значение DWORD</b>	1 (Истина) – в поле для ввода пароля автоматически подставляется значение по умолчанию. 0 (Ложь) – поле для ввода пароля остается пустым.
<b>Значение по умолчанию</b>	Отсутствует

#### 8.4.10 Отображение и скрытие элементов интерфейса eToken PKI Client

Все представленные далее параметры хранятся в реестре в разделе AccessControl. Некоторые из перечисленных элементов имеют дублирующие кнопки и пункты меню.

Все эти параметры должны иметь тип DWORD. Значение 0 указывает на то, что данный элемент будет недоступен, а значение 1 – доступен. По умолчанию все эти параметры не заданы и соответствующие им элементы меню являются доступными.

Параметр реестра	Элемент интерфейса	Описание
AddeTokenVirtual		Подключить eToken Virtual
ChangeAdministratorPassword		Изменить пароль администратора
ChangeInitializationKeyDuringInitialize		Изменить ключ инициализации
ChangePassword		Изменить пароль (пользователя)
ClearDefaultCert		Удалить сертификат по умолчанию
CopyCertificateData		Копировать в буфер обмена (сведения о сертификате)
DeleteCertificate		Удалить сертификат
DisconnectVirtual		Отключить eToken Virtual
ExportCertificate		Экспорт сертификата
ImportCertificate		Импортировать сертификат
InitializeEToken		Инициализировать eToken
LaunchNGFlashPartitionApplication		
LoginAsAdministrator		Вход с правами администратора
ManageReaders		Управление считывателями

Параметр реестра	Элемент интерфейса	Описание
OpenAdvancedModeOfInitialize		Дополнительные настройки инициализации
OpenAdvancedView		Переход в расширенный режим eToken Properties
RenameToken		Переименовать eToken
SetUserPassword		Задать пароль пользователя
Hide		Скрыть
SetCertificateAsAuxiliary	Установить как вспомогательный	
SetCertificateAsDefault	Установить по умолчанию	
OpenTokenProperties		Открыть eToken Properties
GenerateOTP		Сгенерировать OTP
SwitchToken		Устройства
SyncDomainAndTokenPass		Синхронизировать пароль
TrayIconChangePassword		Изменить пароль eToken
TrayIconClearEToken		Удалить содержимое eToken
ClearEToken		
UnlockEToken		
ViewTokenInfo		

## 9. Наиболее распространенные вопросы

---

### Какие операционные системы поддерживает eToken PKI Client 5.1 SP1?

eToken PKI Client 5.1 SP1 поддерживает следующие ОС:

- Windows XP SP3/SP2 (32-bit and 64-bit)
- Windows Vista SP2 (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows Server 2003 SP2 (32-bit and 64-bit)
- Windows Server 2008 (32-bit and 64-bit)
- Windows Server 2008 R2

### Что нового в eToken PKI Client 5.1 SP1

См. [Новые возможности в eToken PKI Client 5.1 SP1](#).

### Какие языки поддерживаются в интерфейсе eToken PKI Client 5.1 SP1?

eToken PKI Client 5.1 SP1 позволяет выбрать при установке любой из следующих языков:

- Китайский
- Английский
- Французский
- Немецкий
- Итальянский
- Японский
- Корейский
- Польский
- Португальский
- Русский
- Испанский
- Тайский

### Каковы особенности установки eToken PKI Client 5.1 SP1?

Установка состоит из следующих основных этапов:

Процесс установки можно запустить двумя способами: из файла с дистрибутивом (.msi) или из файла с обновлением (.msp). Последний может использоваться только тогда, когда у вас уже установлен eToken PKI Client 5.1 SP1. Для установки eToken PKI Client 5.1 SP1 поверх уже имеющейся ранней версии eToken PKI Client 4.0 / 4.5 / 4.55 используйте файл .msi.

В процессе установки прежние параметры реестра также имеют силу. Прочие параметры можно задать при установке в режиме командной строки. Более подробно схема установки описана выше в разделе [Установка](#).

### Какие ошибки из более ранних версии были устранены в eToken PKI Client 5.1 SP1?

- При подключении к компьютеру под управлением Windows Server 2008 через Remote Desktop и при настроенном блокировании рабочей станции по отключению eToken, открыть сеанс снова после повторного подключения eToken было невозможно.
- При обращении к генератору случайных чисел в то время как к компьютеру были подключены одновременно два устройства eToken происходила ошибка: "The operation requires a Smart Card, but no Smart Card is currently in the device" («Операция требует наличия смарт-карты, но смарт-карты не обнаружено»).
- При авторизации через RDP иногда возникали задержки.
- При подключении к компьютеру под управлением Windows Server 2008 через RDP на экране появлялось сообщение об ошибке, а значок в области уведомлений не реагировал ни на какие действия.
- При попытке создать сертификат средствами подчиненного центра сертификации MSCA периодически возникала ошибка.

- После обновления eToken PKI Client сертификат для авторизации в системе по смарт-карте переставал быть сертификатом по умолчанию. В этом случае приходилось авторизоваться в системе по имени пользователя и паролю и заново устанавливать сертификат по умолчанию.
- После авторизации на удаленном компьютере через Remote Desktop с сертификатом для доступа по смарт-карте отсоединение eToken не приводило к блокированию рабочей станции даже тогда, когда этот параметр был явно задан в настройках групповых политик.
- eToken WSO 3.0 требовал избыточное количество ресурсов ЦПУ.
- Конфликт Cisco VPN с SBL не работал с eToken PKI Client 5.1, так как не обнаруживался сертификат для доступа в сеть.
- При авторизации на сервере Citrix с eToken PRO и с установленным eToken PKI Client 5.1 происходило «зависание» терминальной сессии, а после отключения eToken она закрывалась.
- Иногда в параметрах сертификата поле **Кому выдан** оставалось пустым, если у файла .pfx было слишком длинное имя.
- Утилита eToken Properties под 32-битной ОС Windows XP иногда переставала отвечать на события.
- При импорте pfx-файла на компьютер под управлением Windows Vista происходил сбой с сообщением «Не удалось получить контекст».
- Атрибут [TolerantX509Attributes](#) по умолчанию имел значение «1» («Истина»).
- Запуск утилиты certutil.exe под Windows Vista с параметром -Scroots приводил к сбою.
- В некоторых случаях при регистрации eToken возникала ошибка с указанием на некорректные параметры качества пароля, даже если проверка сложности пароля была отключена.
- Работая одновременно с несколькими PDF-документами во время открытого сеанса Citrix ICA попытка подписать очередной документ приводила к «зависанию», и только после отключения eToken можно было продолжать работу.
- Иногда при попытке закрыть утилиту eToken Properties она переставала отвечать, а на экране появлялось сообщение об ошибке «Не удается считать данные из памяти».
- При отключении eToken на странице, защищенной сертификатом SSL, и подключении eToken после завершения сеанса SSL на экране появлялось сообщение о том, что требуемый сертификат недоступен. В таком случае пользователю необходимо было снова ввести пароль eToken.
- В модуле сопряжения PKCS#11 не поддерживались атрибуты механизмов СКА\_SHA256/SHA384/SHA512.
- Ошибки в русскоязычной локализации пользовательского интерфейса.
- Повторная попытка подключиться к Citrix ICA приводила к «зависанию». Возобновление работы происходило только после отключения eToken.
- Некорректные показания объема свободной памяти. Такое происходило иногда при выполнении операций с eToken посредством APDU-команд, и в этом случае в утилите eToken Properties отображались неактуальные данные.

## 10. Известные проблемы и способы их решения

Если в процессе работы с eToken PKI Client 5.1 SP1 у вас возникли затруднения, прежде чем обращаться в службу поддержки, попробуйте найти решение в этом разделе.

Проблема	Решение
Если попытаться установить eToken WSO 3.0 на компьютере, где уже установлен пакет eToken PKI Client 5.0 или более поздней версии, то на экране появится окно с предложением закрыть процесс eToken PKI Monitor, однако такой возможности нет.	Нажмите Пропустить и после завершения установки перезапустите компьютер.
Если на компьютере с установленным eToken PKI Client 5.0 (или более поздней версии) удалить eToken WSO 3.0, не сохранив параметры реестра, то вместе с ними будут также удалены параметры считывателей, используемые eToken PKI Client.	При удалении eToken WSO откажитесь от удаления параметров.
После обновления с версии 4.55 значок в области уведомлений не появляется, и в диспетчере задач отсутствует процесс PKI Monotor.	Перезапустите компьютер.
Если вернуться с версии eToken PKI Client 5.0/5.1/5.1 SP1 к версии 4.55, утилита eToken Properties не будет загружаться.	После удаления более новой версии удалите также вручную файл eTProps.exe и только после этого устанавливайте eToken PKI Client 4.55.
После удаления eToken eToken PKI Client 5.0/5.1/5.1 SP1 под Windows Vista файл eTFS.dll остается в папке Windows\system32.	
При удалении утилиты eToken Properties из командной строки соответствующий пункт не удаляется из меню, вызываемом из области уведомлений (при щелчке на этом пункте не происходит никаких событий).	
После обновления eToken PKI Client 5.0 или 5.1 подключенные ключи eToken Virtual могут ошибочно отображаться как эмулированные.	Решить эту проблему можно двумя способами: а) Выполните обновление без сохранения прежних параметров (eToken Virtual будет отключен). б) Отключите и подключите eToken Virtual.
Если установка eToken PKI Client на клиентском компьютере была выполнена через групповые политики, и в настройках устанавливаемого пакета был установлен параметр <b>Assign (Назначить)</b> , значок в области уведомлений не отображается даже при работающем сервисе eToken PKI Monitor.	Если закрыть сеанс и открыть снова, значок в области уведомлений появится.  Такая ошибка не возникает, если в параметрах пакета установки в GPO выбрать <b>Publish (Публиковать)</b> вместо <b>Assign (Назначить)</b> .

Проблема	Решение
При удалении eToken PKI Client 5.0 на Windows Vista процесс прерывается с ошибкой 1935.	Перезапустите компьютер и выполните установку снова.
Если на компьютере установлен eToken PKI Client 5.0 (или более поздней версии), то при добавлении вручную поставщика криптографии eToken PKCS#11 Security Provider в Mozilla Firefox получится два дублирующих объекта, так как поставщик криптографии уже устанавливается вместе с eToken PKI Client.	Удалите дублирующий поставщик криптографии.
Иногда при установке eToken PKI Client 5.0 или более поздней версии модуль PKCS#11 не добавляется в Mozilla Firefox.	Перед установкой eToken PKI Client откройте в Firefox меню <b>Инструменты &gt; Настройки</b> . В открывшемся окне раскройте вкладку <b>Дополнительно</b> и нажмите кнопку <b>Устройства защиты</b> . Затем закройте окно, нажав кнопку <b>ОК</b> . Таким образом будет добавлен файл настроек, и при установке eToken PKI Client модуль PKCS#11 будет добавлен автоматически.
Сертификат EFS не может быть создан по стандартному шаблону Microsoft.	Microsoft выпустила обновление, устраняющее эту проблему. Чтобы получить его, обратитесь в службу поддержки Aladdin.
Не удается подключиться к VPN-сети, когда одновременно подключено два или более устройств eToken.	Microsoft работает над решением проблемы (описание проблемы: SRQ080701600004).
Не удается авторизоваться в системе или в VPN-сети, когда RSA-ключ в eToken защищен дополнительным паролем.	
Не удается установить подключение с удаленной рабочей станцией через RDP по сертификату, который хранится на Flash-устройстве. Это происходит из-за того, что терминальная служба Microsoft не распознает Flash-устройства на клиентском компьютере.	
Нельзя загрузить сертификат для авторизации в системе или пользовательский сертификат из Mozilla Firefox.	
После перехода компьютера из «спящего» режима или из режима Hibernation утилита eToken Properties работает некорректно.	Щелкните на кнопке <b>Обновить</b> в верхнем меню.
В Windows Vista, даже если параметр PropagateUserCertificates имеет значение «0», то экспорт, тем не менее, периодически выполняется независимо от значения параметра.	Закройте Службу Распространения Сертификатов (Certificate Propagation Service).



Проблема	Решение
Иногда при подключении к VPN-сети фокус установлен не на окне авторизации, поэтому прежде чем ввести свои учетные данные, необходимо установить курсор в поле для ввода.	
Если в утилите eToken NG-Flash Partition попытаться открыть справку, но при этом на компьютере не будет установлено никаких приложений для просмотра pdf-файлов, то справка просто не откроется, причем сообщение об этом также не появится.	Установите Adobe Reader.
Если на 64-битной платформе Windows дважды щелкнуть на файле eToken Virtual (.etvp) или eToken Rescue (.etv), подключения eToken не произойдет.	В этом случае, чтобы подключить eToken Virtual или eToken Rescue, откройте утилиту eToken Properties, переключитесь в расширенный режим и, щелкнув правой кнопкой мыши на узле Устройства, выберите в открывшемся контекстном меню пункт <b>Подключить eToken Virtual</b> .
Если попытаться удалить из хранилища сертификат, который невозможно удалить иначе как установкой параметра RemoveFromTokenOnRemoveFromStore в «1», на экране появится сообщение о том, что сертификат удален, в то время как на самом деле он не удален.	
При работе с OWA под Windows Vista при попытке зашифровать данные или сгенерировать подпись на закрытом ключе на экране появляется сообщение "No digital ID found", при том что на самом деле сертификат присутствует. Такое поведение обусловлено ограничением OWA.	Отключите защищенный режим в Internet Explorer любым из следующих способов: <ul style="list-style-type: none"> <li>Откройте меню Сервис, выберите Свойства обозревателя, раскройте вкладку Безопасность и выберите другой режим.</li> <li>Откройте меню <b>Сервис</b>, выберите <b>Свойства обозревателя</b>, раскройте вкладку <b>Безопасность</b> и выберите пункт <b>Надежные узлы</b>. Затем нажмите кнопку <b>Узлы</b> и в открывшемся окне введите адрес OWA.</li> </ul>
Если одновременно открыты два окна – Инициализировать eToken и <b>Изменить пароль</b> , последнее перестает реагировать на события.	Закройте окно <b>Изменить пароль</b> .
При удалении eToken PKI Client под Windows Server 2008 или Windows Vista на экране появляется окно с предложением закрыть значок eToken PKI Client в области уведомлений или другое приложение.	Нажмите <b>Пропустить</b> для продолжения.

Проблема	Решение
Иногда в меню, вызываемом из области уведомлений, отображаются не все подключенные устройства eToken.	Попробуйте снова подключить нераспознанные устройства.
При установке eToken PKI Client на сервере в то время, когда к нему через RDP подключены другие пользователи, установка может быть выполнена некорректно.	Прежде чем начинать установку, проверьте, чтобы в данный момент не было никаких активных сеансов подключения по RDP.
Если на сервере Citrix установлено соединение с клиентом Citrix ICA, и сервер подключен через RDP к другому компьютеру, eToken не определяется в окне авторизации.	<p>Более подробная информация по этой проблеме представлена в базе данных Citrix (последняя обновление входит в HotFix Rollup Pack 04 для XenApp 4.5 / XenApp 5.0)</p> <p>Описание обновления для Windows Server 2003 приведено в статье CTX119060 (на английском).</p> <p>В обновлении #197595 есть поддержка нескольких языков. Перед установкой проверьте, чтобы обновление соответствовало окружению.</p>
При обновлении eToken PKI Client 5.1 SP1 появляется сообщение о том, что файл занят другим приложением. Это стандартное поведение в контексте Windows Installer.	Нажмите <b>Пропустить</b> для продолжения установки.
Окно авторизации eToken PKI Client не отвечает при авторизации в Check Point VPN.	<p>Альтернативное решение проблемы выглядит следующим образом:</p> <ol style="list-style-type: none"> <li>1. Откройте редактор реестра и в нем откройте раздел HKEY_LOCAL_MACHINE &gt; Software &gt; eToken &gt; MIDDLEWARE &gt; UI.</li> <li>2. Добавьте раздел SR_Service.exe.</li> <li>3. Добавьте новый параметр RunExternalDialog со значением «1» типа DWORD.</li> </ol>

## 11. Изменения в API

В следующей таблице приведены изменения, которые вошли в новый прикладной интерфейс eToken PKI Client 5.1 SP1.

Изменения	Описание
<b>CAPI</b> Функция CryptGetProvParam	В функции CryptGetProvParam поддерживается новый флаг Crypt_Next:  Подключение нескольких устройств eToken  CryptAcquireContext с параметрами: dwflags = CRYPT_VERIFYCONTEXT, зыяЩтефштук = Тгдд  Последовательный вызов функции CryptGetProvParam с PP_ENUMCONTAINERS: <ul style="list-style-type: none"><li>В более ранних версиях данные возвращались на произвольный eToken.</li><li>Теперь можно получить все контейнеры со всех подключенных устройств eToken.</li></ul>
<b>PKCS#11</b> Механизмы CKM_GENERIC_SECRET_KEY_GEN и CKM_RC4.	Снова добавлены эти механизмы с поддержкой ранних форматов (0 и 4).
<b>PKCS#11</b> C_GetSlotInfo и C_GetTokenInfo	Имя производителя заменено на "Aladdin Knowledge Systems Ltd."

Данный документ, а также подбор и расположение материалов в нем, является объектом авторских прав и охраняется в соответствии с законодательством РФ о защите авторских прав. Исключительным обладателем авторских и имущественных прав является ЗАО «Аладдин Р.Д.». Использование материалов любым способом без письменного разрешения ЗАО «Аладдин Р.Д.» запрещено и влечет ответственность, предусмотренную законодательством РФ.

**Аладдин** 

© 1995-2011, ЗАО «Аладдин Р.Д.»  
Все права защищены  
Тел.: +7 (495) 223-00-01  
aladdin@aladdin-rd.ru  
www.aladdin-rd.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (продлены до 18.02.13)  
Лицензии ФСБ России № 18229 от 13.10.10, № 9333Р от 03.09.10, №№ 4205П,  
4206Х от 22.06.07, № 4898П от 14.12.07  
Microsoft Certified Partner, Oracle Gold Partner  
Все товарные знаки являются собственностью их владельцев