PDM STEP SUITE

версия 5.0

Удостоверяющий центр ЭЦП

Руководство пользователя

PDM STEP Suite v.5.0. Руководство пользователя

Удостоверяющий центр ЭЦП

АО НИЦ «Прикладная Логистика»
Москва, 5-й Донской проезд, дом 15, стр. 2
Адрес в интернет: http://www.cals.ru
Телефон/факс: +7 (495) 955 5137

Отпечатано в России

СОДЕРЖАНИЕ

1. Сокращения

ЭЦП – Электронная цифровая подпись

УЦ – Удостоверяющий Центр

Сертификат – Сертификат ключа подписи

PSS – система PDM STEP Suite

БД – База Данных

2. Термины и определения

Увеличенным шрифтом выделены наиболее важные термины.

Инфраструктура открытых ключей (Public Key Infrastructure - PKI) - интегрированный набор служб и средств администрирования для создания и развертывания приложений, использующих криптографию с открытыми ключами; обеспечивает функции управления открытыми ключами.

Удостоверяющий Центр (УЦ) – субъект инфраструктуры открытых ключей, подразделение Организатора, обладающее необходимым комплексом программно-технических средств электронной цифровой подписи, обеспечивающих изготовление и обслуживание сертификатов открытых ключей Подписчиков,

Администратора Удостоверяющего Центра и Администраторов Регистрационных Центров.

Регистрационный Центр (РЦ) – опциональный субъект инфраструктуры открытых ключей, отвечающий за идентификацию и аутентификацию Подписчиков при изготовлении сертификатов, и обладающее необходимым комплексом программно-технических средств электронной цифровой подписи и шифрования для организации защищенного канала связи, обеспечивающего достоверную передачу запросов сертификатов Подписчиков в УЦ.

2.1 *Термины Федерального закона «Об электронной цифровой подписи»*

Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Средства ЭЦП - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Сертификат средств ЭЦП - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Закрытый ключ ЭЦП (private key) - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Открытый ключ ЭЦП (open key) - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Подтверждение подлинности ЭЦП в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

2.2 *Дополнительные термины*

Контейнер – файл (или набор файлов), содержащий закрытый ключ и сертификат ключа подписи. Используется в процессе подписи электронного документа. Для доступа к информации в контейнере требуется ввести пароль.

Самоподписанный сертификат (недоверительный сертификат) (Self-Signed certificate) - сертификат сгенерированный самостоятельно, при этом подлинность сертификата подтверждается его создателем (недоверительным лицом).

Доверительный сертификат (Trusted certificate) – сертификат, выпущенный удостоверяющим центром. Выписывается на определенное имя, указывается срок действия сертификата (до 5 лет), содержит цифровые печати и подписи.

Корневой сертификат – сертификат, принадлежащий Удостоверяющему Центру, с помощью которого подписываются сертификаты, выдаваемые пользователям, и проверяется достоверность выданных ранее сертификатов.

Доверительный корневой сертификат – сертификат УЦ, все сертификаты ключей подписи которого считаются легитимными.

Отозванный сертификат – сертификат, ключ которого был выведен из обращения (аннулирован). Сертификат отзывается Удостоверяющим центром. Пользователи сертификатов

Список Отозванных Сертификатов (СОС) - перечень серийных номеров сертификатов открытых ключей, выведенных из обращения (аннулированных). Формируется Удостоверяющим Центром и заверяется электронной цифровой подписью Администратора УЦ.

Верификация открытого ключа – проверка сертификата ключа подписи с помощью сертификата удостоверяющего центра.

Стандарт X.509 ITU-T является фундаментальным стандартом, лежащим в основе всех остальных, используемых в инфраструктуре открытых ключей. Основное его назначение - определение формата электронного сертификата и списков отозванных сертификатов.

Администратор Удостоверяющего Центра (Администратор УЦ) - уполномоченный представитель Удостоверяющего Центра, ответственный за выполнение операций по изготовлению и обслуживанию сертификатов Подписчиков.

Администратор Регистрационного Центра (Администратор РЦ) - уполномоченный представитель Регистрационного Центра, ответственный за выполнение операций по идентификации, аутентификации, проверке полномочий Подписчиков и передаче сформированных ими запросов сертификатов Администратору УЦ.

Компрометация ключа – констатация Подписчиком сертификата обстоятельств, при которых возможно несанкционированное использование его секретного ключа неуполномоченными лицами.

Плановая смена ключей - регламентируемая Администратором УЦ периодическая смена криптографических ключей Подписчиков, Администраторов РЦ и самого Администратора УЦ, не вызываемая их компрометацией.

3. Основные положения.

Работать с удостоверяющим центром имеет право администратор или сотрудник с ролью «Администратор ЭЦП».

Используемые алгоритмы ЭЦП

УЦ PSS может использовать встроенную систему ЭЦП использующую встроенные алгоритмы Microsoft Windows (AplCryptManager) и систему ЭЦП КриптоПро использующую алгоритм ГОСТ 34.10-2001 (APL КриптоПро).

Для использования системы КриптоПро на клиентском компьютере должно быть установлено и настроено средство криптографической защиты информации КриптоПро CSP. Подробнее о системе КрипроПро см. на http://www.cryptopro.ru.

Легитимность сертификатов ключа пользователя

В БД УЦ PSS могут использоваться сертификаты пользователей выданные как текущим УЦ, так и сертификаты импортированные из других УЦ.

В системе PSS легитимным считается любой сертификат ключа пользователя подписанный доверительным удостоверяющим центром.

Удостоверяющий центр считается доверительным, если его сертификат ключа находится в списке доверительных сертификатов УЦ.

Примечание: Обычно, все доверительные сертификаты (включая сертификаты ключей пользователей) задаются в хранилище сертификатов операционной системы, т.е. все доверительные сертификаты должны быть установлены на всех компьютерах, и при создании нового ключа, или отзыве ранее выданного, вся информация должна быть скопирована на все клиентские компьютеры. Для упрощения администрирования, в системе PSS все доверительные сертификаты хранятся в БД PSS.

Сертификат ключа УЦ.

При создании ключей пользователей сертификаты ключей пользователей подписываются ключом удостоверяющего центра.

Ключ удостоверяющего центра может быть получен из другого УЦ или же сформирован непосредственно в УЦ. Во втором случае ключ УЦ будет самоподписанным и его легитимность будет определяться только нормативными документами предприятия.

Удостоверяющий центр может иметь несколько сертификатов ключей УЦ. Различные ключи могут задаться, например, для различных администраторов ЭЦП.

Создание закрытого ключа подписи

Создание закрытого ключа подписи состоит из:

1. Формирования пары – закрытый и открытый ключ
2. Создания сертификата ключа подписи (включающего открытый ключ и и информацию о пользователе – владельце закрытого ключа) подписанного ключом УЦ.
3. Создание контейнера содержащего закрытый ключ и сертификат ключа подписи. (Доступ к данным контейнера защищается паролем).

4. Работа с удостоверяющим центром

4.1 *Интерфейс Удостоверяющего центра*

Интерфейс удостоверяющего центра представлен на Рис. 1. Основное окно УЦ содержит список хранящихся в БД сертификатов разделенный на 3 группы:

A – Сертификаты пользователей

B – Сертификаты удостоверяющего центра (сертификаты ключей, которыми подписываются выдаваемые центром сертификаты)

C – Доверительные корневые сертификаты (сертификаты корневых удостоверяющих центров, сертификаты выданные которыми считаются легитимными в текущей БД).

Сертификаты могут отмечаться следующими иконками:

– Действующий сертификат.

– Отозванный сертификат

– Просроченный сертификат.

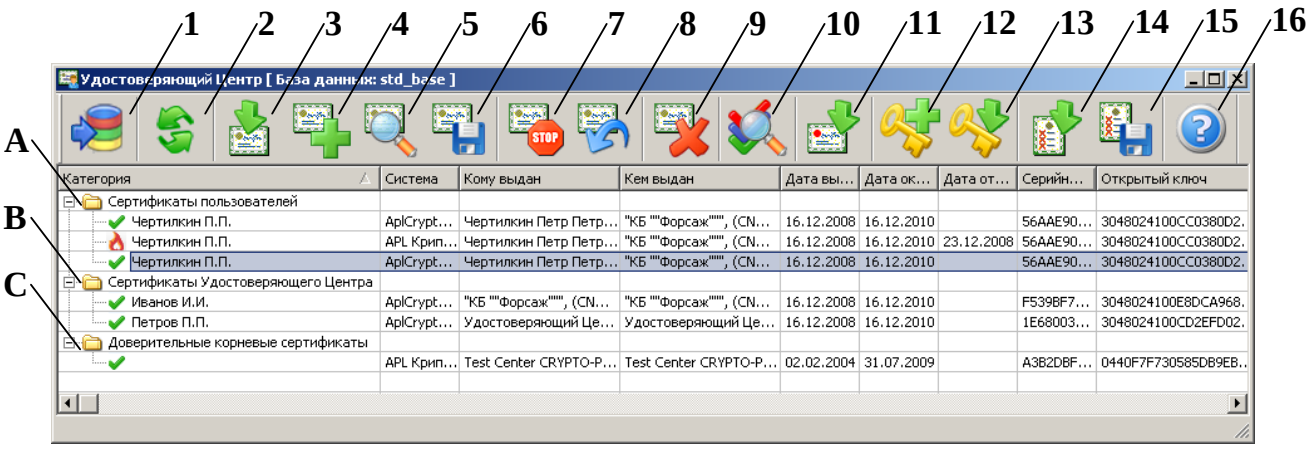

Рис. 1. Окно удостоверяющего центра

Все операции производимые в УЦ вызываются нажатием кнопок на панели инструментов:

1. Установка соединения с БД.
2. Обновление информации из БД.
3. Импорт сертификата пользователя из файла.
4. Создание нового сертификата ключа пользователя.
5. Просмотр выделенного сертификата.
6. Сохранение выделенного сертификата в файл.
7. Отзыв сертификата.
8. Отмена отзыва сертификата.
9. Удаление сертификата из БД
10. Просмотр статусов присвоенных отозванными сертификатами.
11. Импорт доверительного корневого сертификата.
12. Создание нового сертификата УЦ (самоподписанного).
13. Импорт сертификата УЦ.
14. Загрузка в БД списка отозванных ключей.
15. Создание списка отозванных сертификатов.
16. Отображение информации о программе.

4.2 *Операции удостоверяющего центра*

4.2.1 Импорт сертификата

Операция вызывается для загрузки в БД информации о сертификате сформированном в другом УЦ. Такими сертификатами могут быть:

- Сертификат пользователя (Как правило, эта операция не требуется т.к. сертификат пользователя автоматически загружается при первой же подписи выполняемой владельцем сертификата.)
- Сертификат удостоверяющего центра.

- Доверительный корневой сертификат.

Импорт того или иного сертификата вызывается нажатием соответствующей кнопки на панели управления. При выполнении операции выводится окно (Рис. 2). В нем, нажав кнопку «…», необходимо выбрать файл сертификата.

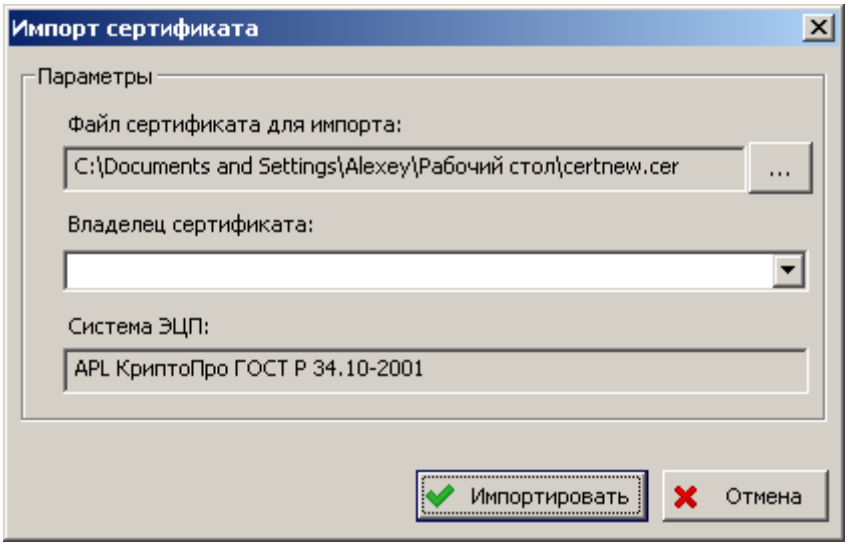

Рис. 2. Импорт сертификата

При импорте сертификата пользователя в поле «Владелец сертификата» необходимо выбрать владельца сертификата. Список возможных владельцев определяется выбором из всех сотрудников, введенных в БД, тех, данные которых совпадают с данными сертификата. Как правило, в поле «Владелец сертификата» будет только один возможный сотрудник.

При импорте сертификата УЦ или доверительного корневого сертификата поле «Владелец сертификата» не заполняется.

После нажатия кнопки «Импортировать» сертификат будет загружен в БД.

4.2.2 Создание нового сертификата ключа.

Создание нового сертификата ключа осуществляется для:

- Пользователя
- Удостоверяющего центра.

Создание нового сертификата ключа вызывается нажатием соответствующей кнопки на панели управления. При создании сертификата ключа выводится окно (Рис. 3).

Для создания сертификата ключа пользователя необходимо, нажав кнопку «  », выбрать сотрудника. Для создания сертификата ключа УЦ выбор сотрудника не требуется. После чего необходимо ввести все необходимые данные.

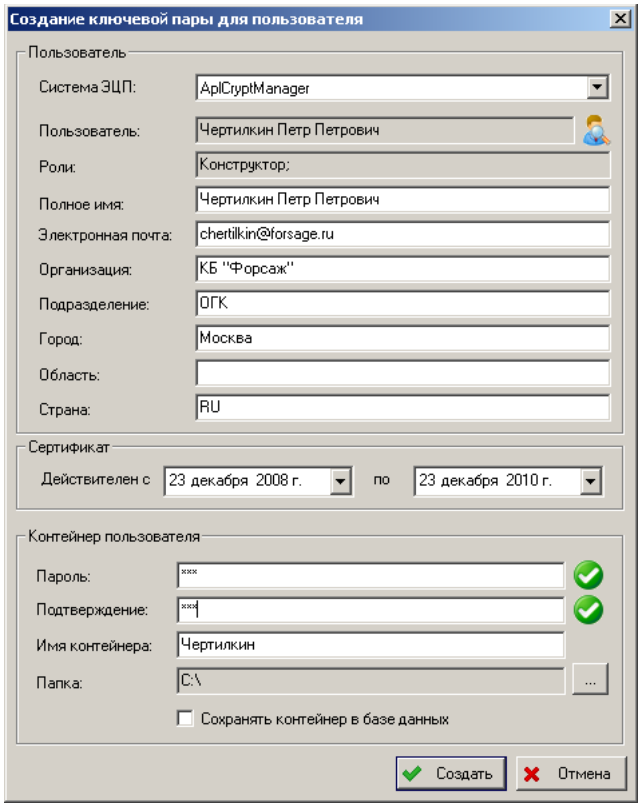

Рис. 3. Создание сертификата ключа

Если выбрана система ЭЦП «APLCryptManager»:

Контейнер с закрытым ключом сохраняется в файл, имя которого задается в поле «Имя контейнера», а путь в поле «Папка». Пароль для доступа к контейнеру задается в поле «Пароль» и подтверждается в поле «Подтверждение».

Существует возможность сохранить контейнер с закрытым ключом в БД. Если контейнер сохранен в БД, то сотрудник, при подписи может не указывать файл контейнера, а использовать контейнер из БД. Это бывает удобно, например, если на используемых компьютерах запрещено использование дисководов или USB портов.

Для сохранения контейнера в БД необходимо установить галочку «Сохранять контейнер в БД».

Для использования сохраненного в БД контейнера сотруднику также нужно будет ввести имя пользователя и пароль.

Если выбрана система ЭЦП «APL Крипто Про»:

Все действия по созданию контейнера осуществляются в соответствии с руководством по используемой версии Крипто Про.

4.2.3 Просмотр сертификата

Для просмотра сохранного в БД сертификата его необходимо выбрать в таблице сертификатов и нажать кнопку «Просмотреть сертификат». После этого сертификат будет открыт стандартным средством просмотра сертификатов MS Windows (Рис. 4).

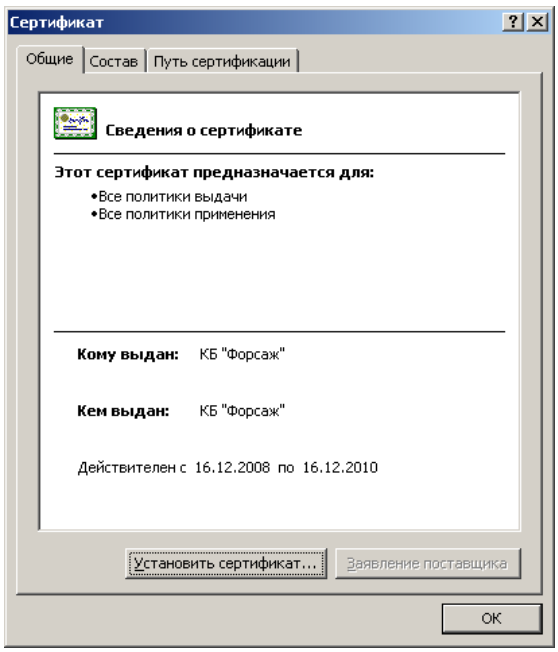

Рис. 4. Свойства сертификата

4.2.4 Сохранение сертификата на диск.

Для сохранения копии сертификата из БД на диск, сертификат необходимо выбрать в таблице сертификатов и нажать кнопку «Сохранить сертификат на диск». После этого выбрать файл, в который будет сохранен сертификат.

4.2.5 Отзыв сертификата

Для отзыва сертификата (при его дискредитации), сертификат необходимо выбрать в таблице сертификатов и нажать кнопку «Отозвать сертификат». После этого, в окне Рис. 5 указать дату и время, начиная с которого сертификат считается отозванным и нажать кнопку «Отозвать».

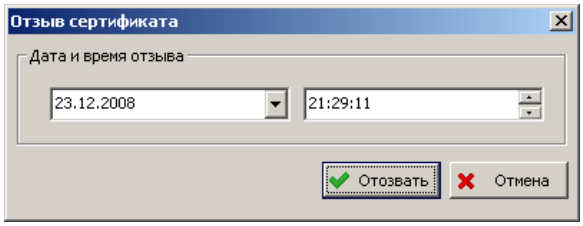

Рис. 5. Отзыв сертификата

4.2.6 Отмена отзыва сертификата

Если сертификат был отозван ошибочно, его отзыв можно отменить. Для отмены отзыва сертификата его необходимо выбрать в таблице сертификатов и нажать кнопку «Отмена отзыва сертификата». Кнопка доступна только для отозванных сертификатов.

4.2.7 Просмотр статусов присвоенных отозванными сертификатами.

Если необходимо узнать, были ли присвоены статусы с использованием отозванных сертификатов ключей, то для этого необходимо нажать кнопку «Просмотр статусов присвоенных отозванными сертификатами». При выполнении этой функции все статусы присвоенные отозванными ключами (дата отзыва раньше даты присвоения статуса) будут отображены в виде таблицы (Рис. 6).

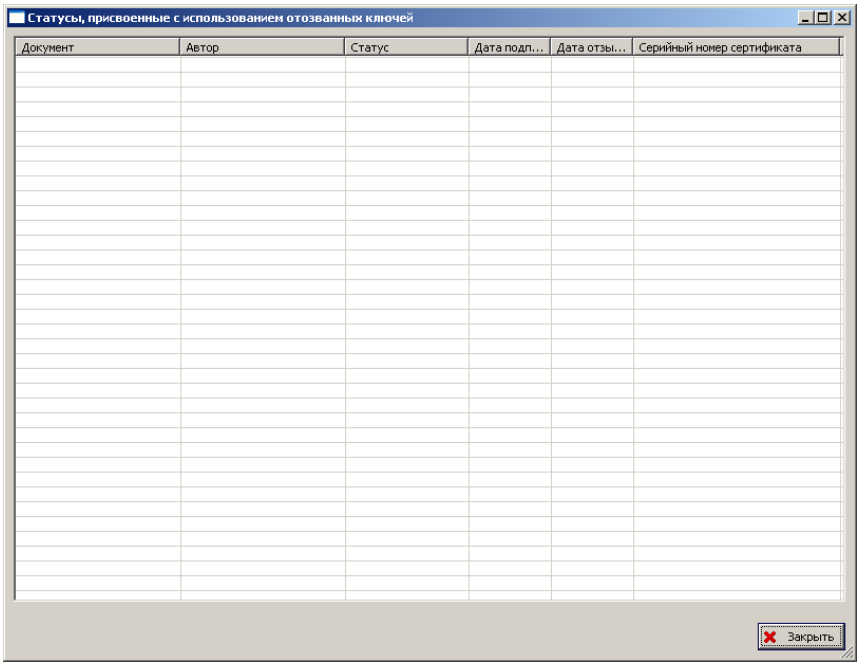

Рис. 6. Статусы, присвоенные отозванными сертификатами.

4.2.8 Список отозванных сертификатов

Если в БД используются сертификаты выданные другими УЦ, то необходимо, с заданной нормативными документами периодичностью, обновлять информацию об отзыве сертификатов. Эта информация передается в виде файлов списков отозванных сертификатов (расширение «.crl»).

Для обновления информации об отозванных сертификатах необходимо обработать файл со списком отозванных сертификатов нажав кнопку «Загрузка в БД списка отозванных ключей» и выбрав файл «.crl».

Аналогично, если в других БД используются сертификаты выданные текущим УЦ, то в эти БД, с заданной в нормативных документах периодичностью, необходимо передавать списки отозванных сертификатов текущего УЦ. Для этого необходимо нажать кнопку «Создать список отозванных сертификатов» и сохранить список в файл «.crl»

5. Настройка УЦ ЭЦП

Настройка УЦ ЭЦП состоит из:

1. Задания сертификатов ключей УЦ (импорт существующих или создание новых).
2. Импорта доверенных корневых сертификатов.

6. Совместимость с предыдущими версиями AplCryptManager.

Предыдущая версия AplCryptManager имела следующие существенные недостатки:

- Отсутствие поддержки сертификатов X5.09.
- Невозможность задания срока действия ключа.

Новая версия AplCryptManager лишена этих недостатков.

Для обеспечения совместимости старой и новой версии AplCryptManager:

- Создание сертификатов (и ключей) новой версией AplCryptManager осуществляется модулем «Удостоверяющий центр ЭЦП»
- Создание ключей старой версией AplCryptManager осуществляется в модуле «Настройка БД».

- Существующая система ЭЦП поддерживает работу как со старой, так и с новой версией AplCryptManager (как со старыми контейнерами, так и с новыми).

После окончательного перехода на новую версию AplCryptManager рекомендуется:

- **Отозвать все сертификаты выданные старой версией.**
- **Задать с помощью aplOptionsEditor.exe в БД числовой параметр «Запретить использование контейнеров AplCryptManager версии 0» и установить его значение в 1.**

7. Ссылки:

- ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
- Федеральный закон Российской Федерации от 10 января 2002 г. N 1-ФЗ.
- ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.
- RFC 3280. Housley, W. Polk, W. Ford, D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, April 2002.
- RFC 3039. S.Santesson, W. Polk, P.Barzin, M.Nystrom, “Internet X.509 Public Key Infrastructure Qualified Certificates Profile”, January 2001.
- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459)
- Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510)
- Internet X.509 Certificate Request Message Format (RFC 2511)
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527)
- Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates (RFC 2528)
- Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2 (RFC 2559)
- Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP (RFC 2585)
- Internet X.509 Public Key Infrastructure LDAPv2 Schema (RFC 2587)
- X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560)