2015 год

МЕТОДИЧЕСКОЕ РУКОВОДСТВО

для пользователей информационных систем РГП «КЦМР НБ РК» по выпуску/отзыву регистрационных свидетельств с использованием Web-центра регистрации Удостоверяющего центра

РГП «КЦМР НБ РК»

Содержание:

1. ОБЩИЕ СВЕДЕНИЯ

Перечень сокращений и терминов:

ПК – персональный компьютер пользователя;

УЦ – удостоверяющий центр;

КЦМР – РГП «Казахстанский центр межбанковских расчетов Национального банка Республики Казахстан»;

средство криптографической защиты информации (СКЗИ) «ТУМАР-CSP» – программное средство, предназначенное для выполнения криптографических операций в операционных системах Microsoft, управление которыми происходит с помощью функций интерфейса CryptoAPI;

внешний носитель – внешнее устройство для хранения ключевой информации;

профайл – набор настроек СКЗИ «ТУМАР-CSP», сохраненный под определенным именем и используемый при загрузке и создании ключевой информации;

регистрационное свидетельство – документ на бумажном носителе или электронный документ, выдаваемый УЦ для подтверждения соответствия открытого криптографического ключа законодательно установленным требованиям;

личный кабинет – функционал программного обеспечения УЦ, предназначенный для обеспечения пользователей средствами удаленного формирования и управления регистрационными свидетельствами;

офицер безопасности – работник КЦМР, осуществляющий подтверждение запросов на выпуск и отзыв регистрационных свидетельств.

1.1. Системные требования

ПК, функционирующий под управлением 32 или 64-х разрядной лицензионной операционной системы Windows 8.1, 8, 7 или VISTA.

1.2. Программное обеспечение, необходимое для работы

- ✓ Средство криптографической защиты информации (СКЗИ) «ТУМАР-CSP»
- ✓ Браузер Internet Explorer версии 6 или старше
- ✓ Программное обеспечение Adobe Flash Player актуальной версии (http://www.adobe.com/go/EN_US-H-GET-READER)
- ✓ При использовании внешних носителей требуется наличие драйвера для используемого типа устройства
- ✓ Программное обеспечение, использующее криптографические ключи и регистрационные свидетельства (Платежный терминал, VIDO и т.п.)

<u>ВНИМАНИЕ!</u> В силу особенностей архитектуры ОС Windows, для корректной работы средства криптографической защиты информации (СКЗИ) «ТУМАР-CSP» требуется отсутствие на компьютере криптопровайдеров (CSP), реализующих криптографические алгоритмы серии ГОСТ, от других производителей, а также выполнение установки СКЗИ «ТУМАР-CSP» под управлением учетной записи с правами администратора ПК.

2. НЕОБХОДИМЫЕ ДЕЙСТВИЯ

ПРИМЕЧАНИЕ: Пункты 2.1 - 2.3 выполняются только с целью переноса криптографических ключей и регистрационных свидетельств на другой компьютер. Если запрос на новый сертификат будет формироваться на том же компьютере, где установлено программное обеспечение, использующее указанные ключи, сразу перейдите к пункту 2.4.

2.1. Перенос ключевого контейнера

На компьютере с **установленными действующими криптографическими ключами и регистрационными свидетельствами**, откройте конфигуратор СКЗИ «ТУМАР-CSP» (**Пуск - Все программы – Gamma Tech – Tumar CSP v.6 – TumarCSP Конфигуратор**). В верхнем окне выберите соответствующий профайл (*для пользователей платежной системы – **FSystem**, для пользователей ФАСТИ – **FASTI2***). В столбце **«Параметр устройства хранения»** указан **каталог,** в котором хранится ключевой контейнер (файл с криптографическими ключами и регистрационными свидетельствами), в столбце **«Имя контейнера»** указано **имя файла** (Рисунок 1). Скопируйте указанный файл (*.bin) и перенесите его на компьютер, на котором будет выполняться формирование и отправка запроса на новый сертификат.

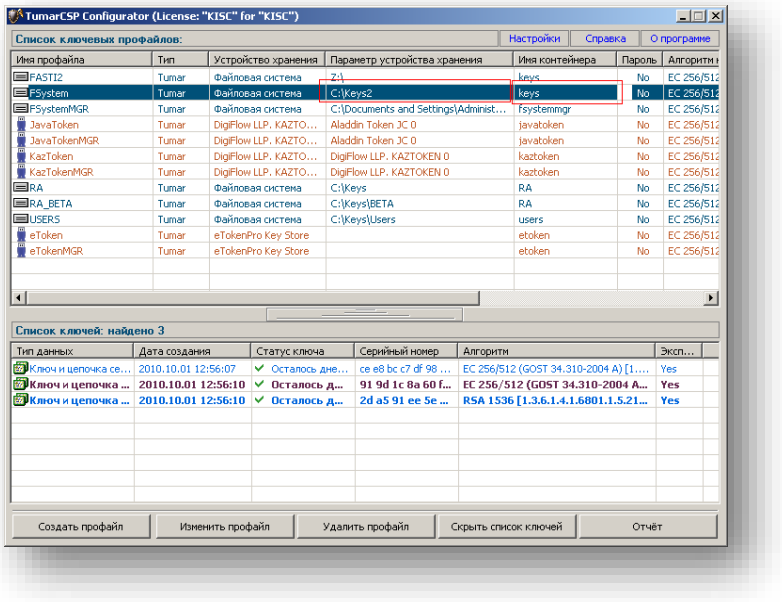

Рисунок 1.

2.2. Установка программного обеспечения «ТУМАР-CSP»

Для формирования и отправки запроса на новое регистрационное свидетельство необходимо наличие установленного СКЗИ «ТУМАР-CSP».

Для установки запустите файл TumarCSP.exe и следуйте указаниям мастера установки.

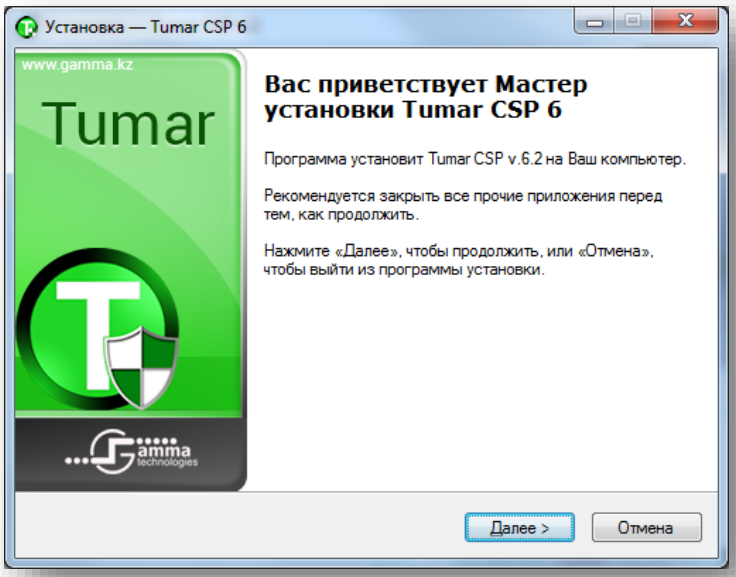

Рисунок 2.

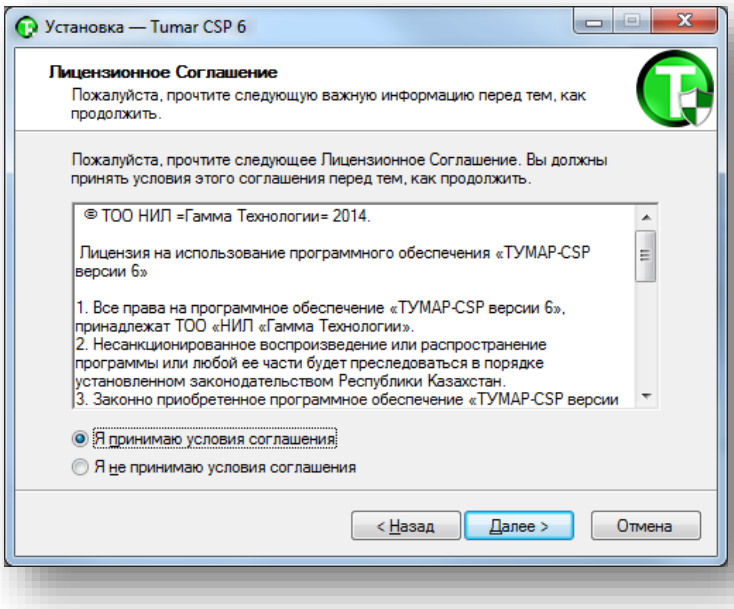

Рисунок 3.

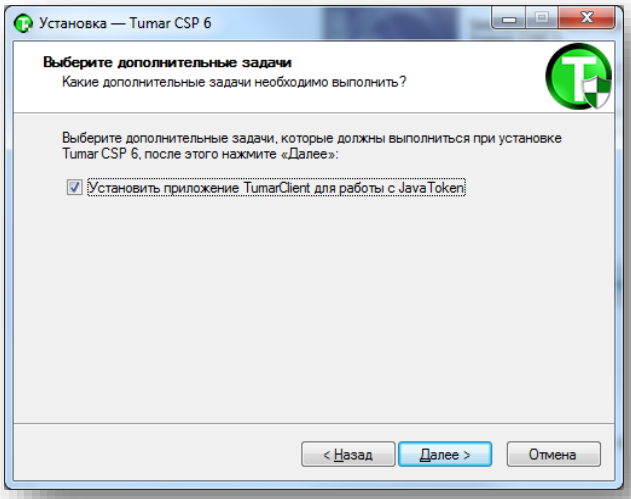

Рисунок 4.

2.3. Редактирование профайла конфигуратора программного обеспечения «ТУМАР-CSP»

Откройте конфигуратор программного обеспечения «ТУМАР-CSP» (**Пуск - Все программы – Gamma Tech – Tumar CSP v.6 – TumarCSP Конфигуратор**). Выделите правой кнопкой мыши необходимый профайл (*для пользователей платежной системы – **FSystem**, для пользователей ФАСТИ – **FASTI2**)* и выберите пункт всплывающего меню «Изменить профайл». Убедитесь, что в полях **«Параметр устройства хранения» и «Имя контейнера»** указаны верные значения, соответствующие местоположению и имени ключевого контейнера (который при необходимости был предварительно перенесен согласно п. 2.1), нажмите **«Сохранить»** (Рисунок 5).

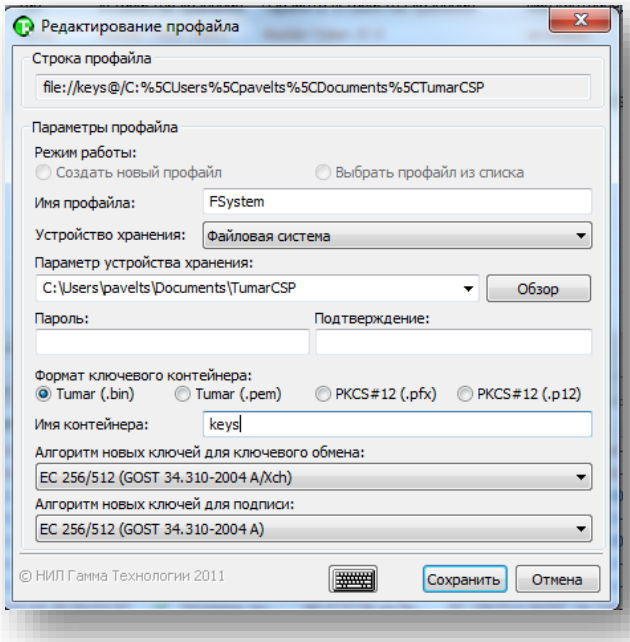

Рисунок 5.

2.4. Завершение работы приложений

Перед отправкой запроса на выпуск нового регистрационного свидетельства завершите отправку и получение всех исходящих и входящих сообщений, прекратите работу приложения, для которого выпускаются криптографические ключи и регистрационные свидетельства (Платежный терминал, VIDO и т.п.).

2.5. Вход в информационную систему Web-центра регистрации Удостоверяющего центра

Для авторизации в информационной системе удостоверяющего центра необходимо перейти по ссылке https://ca.kisc.kz/. На форме авторизации укажите название своей учетной записи и пароль, затем нажмите кнопку «Вход» (Рисунок 6).

Для входа по сертификату поставьте галочку «По сертификату», затем нажмите кнопку «Вход» (Рисунок 6) и выберите из списка соответствующий сертификат (Рисунок 7).

ПРИМЕЧАНИЕ. Если у Вас только один соответствующий сертификат для входа, то окно со списком сертификатов не выводиться.

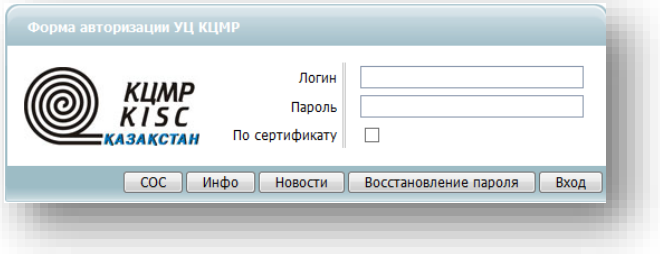

Рисунок 6.

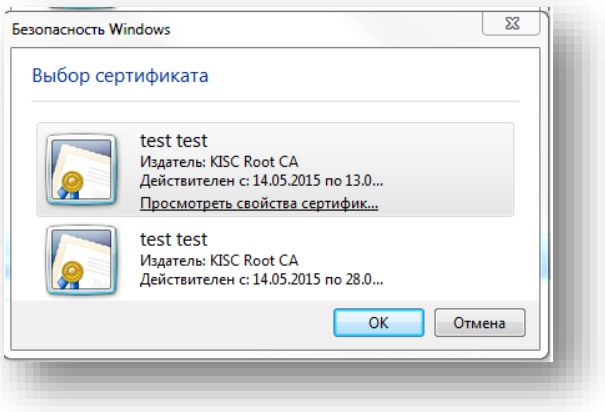

Рисунок 7.

2.6. Выпуск регистрационного свидетельства

После авторизации Вы находитесь на странице личного кабинета (Рисунок 8).

Для формирования запроса на выпуск регистрационного свидетельства нажмите кнопку **«Запрос на выпуск сертификата»**

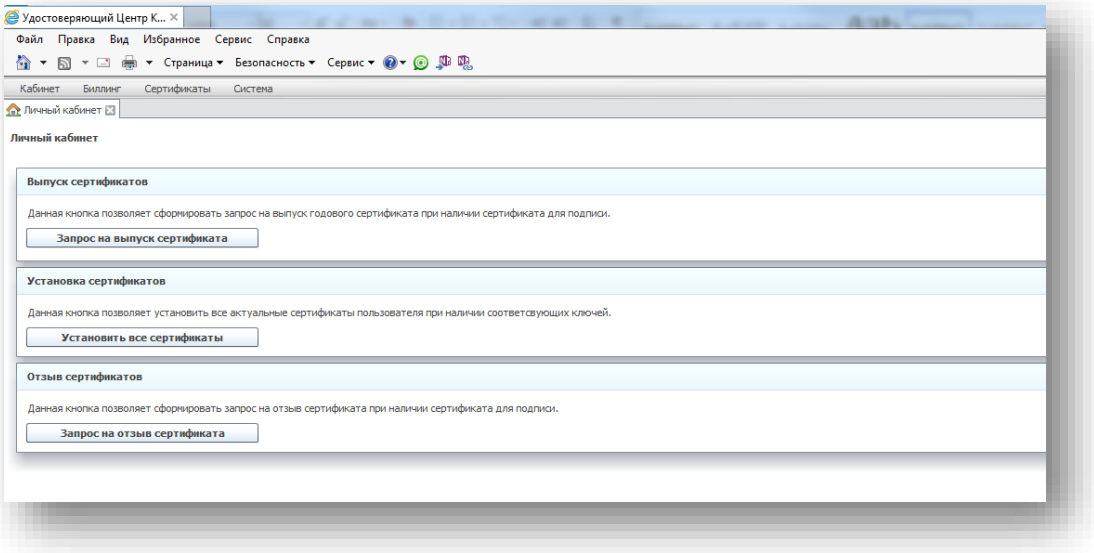

Рисунок 8.

Затем нажмите кнопку **«Отправить запрос»** (Рисунок 9).

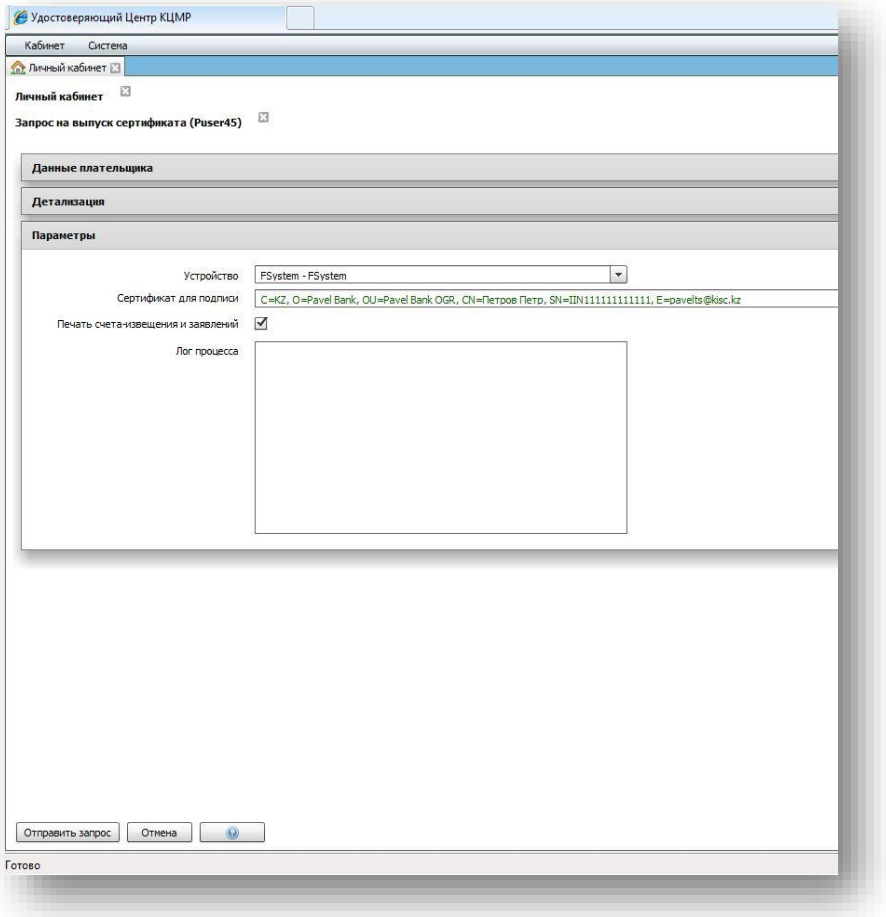

Рисунок 9.

После формирования запроса на выпуск появляется сообщение - запрос ожидает обработки (Рисунок 10).

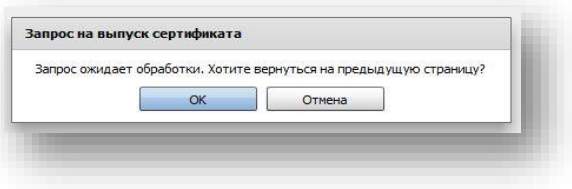

Рисунок 10.

Для подтверждения офицером безопасности КЦМР запроса на выпуск необходимо позвонить по телефонам: (727) 2506-679, 2506-664.

После подтверждения запроса необходимо установить выпущенные регистрационные свидетельства. На странице личного кабинета нажмите кнопку **«Установить все сертификаты» (Рисунок 8).**

Отображается информационное окно, сообщающее об успешной установке (Рисунок 11).

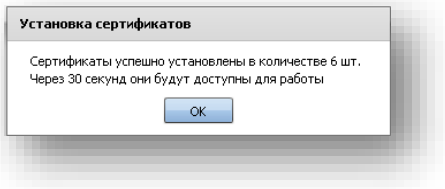

Рисунок 11.

2.7. Создание резервной копии

На компьютере, с которого отправлялись запросы на выпуск (отзыв) сертификата, откройте Конфигуратор программного обеспечения «ТУМАР-CSP» (Пуск - Все программы – Gamma Tech – Tumar CSP v.6 – TumarCSP Конфигуратор). В верхней половине выберите соответствующий профайл (для пользователей платежной системы – FSystem, для пользователей ФАСТИ – FASTI2). В столбце «Параметр устройства хранения» указан каталог, в котором хранится ключевой контейнер (файл с криптографическими ключами и регистрационными свидетельствами), в столбце «Имя контейнера» указано имя файла (Рисунок 1). Создайте копию указанного файла (*.bin) на внешнем носителе.

2.8. Отзыв регистрационного свидетельства

Внимание! Пункт 2.8 выполняется только с целью внеплановой смены криптографических ключей и регистрационных свидетельств при их компрометации. При плановой смене криптографических ключей и регистрационных свидетельств (окончание срока действия) необходимости в отзыве нет. Перейдите к пункту 2.9.

Для отправки запроса на отзыв регистрационного свидетельства необходимо нажать кнопку **«Запрос на отзыв сертификата»** (Рисунок 8), выбрать отзываемое регистрационное свидетельство и нажать кнопку **«Отозвать сертификат»** (Рисунок 12).

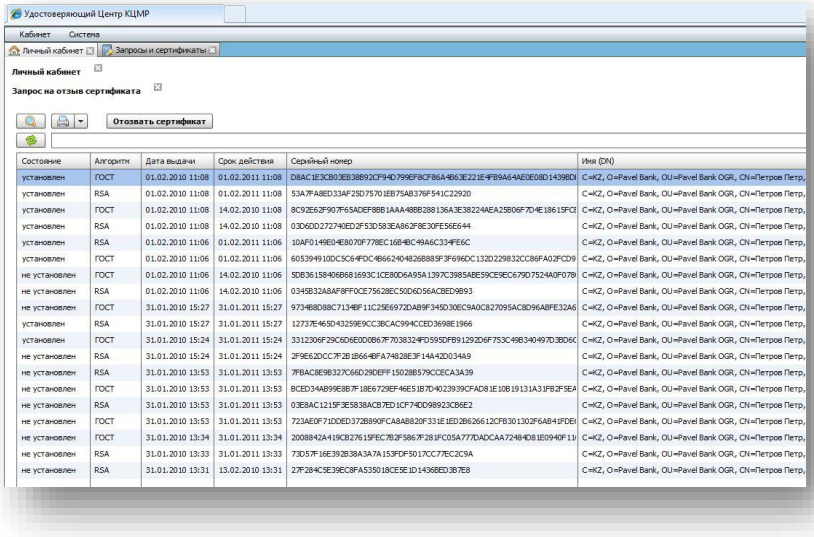

Рисунок 12.

Для отправки запроса на отзыв нажмите кнопку **«Отправить запрос»** (Рисунок 13).

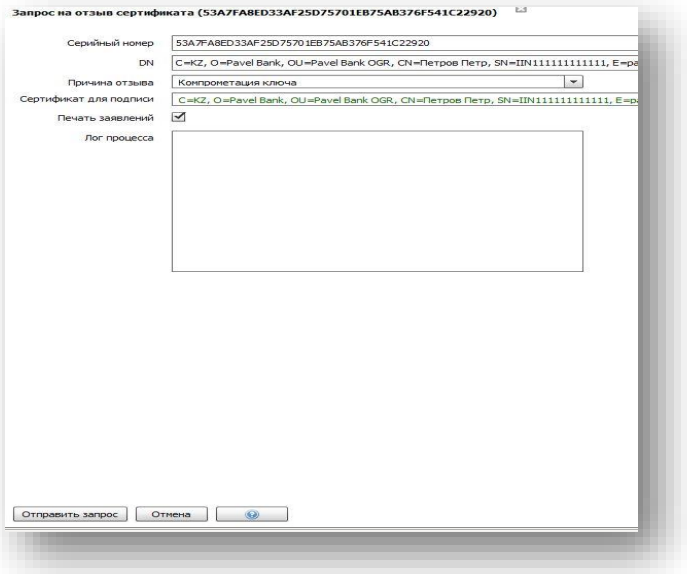

Рисунок 13.

После формирования запроса на отзыв регистрационного свидетельства появляется сообщение - запрос ожидает обработки (Рисунок 10).

Для подтверждения офицером безопасности КЦМР запроса на отзыв необходимо позвонить по телефонам: (727) 2506-679, 2506-664.

После подтверждения отзыва удалите отозванное регистрационное свидетельство. Перейдите в меню **«Кабинет - Запросы и сертификаты»,** в таблице **Запросы** выделите запрос на отзыв и нажмите кнопку **«Удалить сертификаты»** (Рисунок 14).

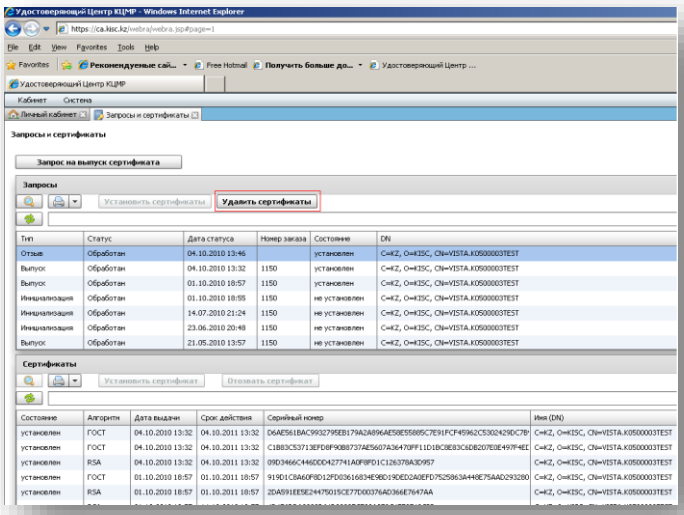

Рисунок 14.

Отображается информационное окно, сообщающее об успешном удалении регистрационного свидетельства (Рисунок 15).

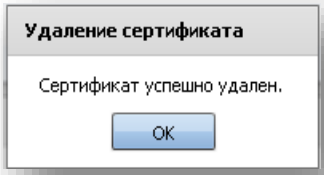

Рисунок 15.

2.9. Перенос ключевого контейнера на компьютер с прикладным ПО

Внимание! Пункт 2.9 выполняется только с целью переноса криптографических ключей и регистрационных свидетельств на другой компьютер. Если запрос на новое регистрационное свидетельство формировался на том же компьютере, где установлено программное обеспечение, использующее указанные ключи, перейдите к пункту 2.10.

Внимание! Перед выполнением Пункта 2.9 возможно потребуется выполнить дополнительные действия по перенастройке программного обеспечения,

использующего криптографические ключи и регистрационные свидетельства (Платежный терминал, VIDO и т.п.). По данному вопросу обращайтесь к специалистам сопровождения указанного ПО.

На компьютере, с **которого отправлялись запросы на выпуск (отзыв) регистрационного свидетельства**, откройте конфигуратор программного обеспечения «ТУМАР-CSP» (**Пуск - Все Программы – Gamma Tech – Tumar CSP v.6 – TumarCSP Конфигуратор**). В верхней половине выберите соответствующий профайл (*для пользователей платежной системы – **FSystem**, для пользователей ФАСТИ – **FASTI2***). В столбце **«Параметр устройства хранения»** указан **каталог,** в котором хранится ключевой контейнер (файл с криптографическими ключами и регистрационными свидетельствами), в столбце **«Имя контейнера»** указано **имя файла** (Рисунок 1). Скопируйте указанный файл (*.bin) и перенесите его на компьютер, на котором функционирует программное обеспечение, использующее криптографические ключи и регистрационные свидетельства (Платежный терминал, VIDO и т.п.). Перезапишите существующий ключевой контейнер.

2.10. Запуск приложений

Запустите приложение, для которого выпускались криптографические ключи и регистрационные свидетельства (Платежный терминал, VIDO и т.п.). Убедитесь в корректной работе приложения.