ESMART PKI Client

Описание изменений версии 4.4

Исправления, улучшения

- *Исправлено отображение атрибутов в утилите PKIClientCli*
- *Исправлен вызов C_Digest с возможностью передавать все данные единой посылкой без использования C_DigestUpdate*
- *Доработано окно ввода ПИН-кода для карт/токенов ESMART Token ГОСТ, исправлено появление окна ввода ПИН на заднем плане*
- *Исправлено появление окна ввода ПИН-кода для карт/токенов ESMART Token ГОСТ при входе в систему или при выходе из сеанса.*

Драйвера

- *Обновлены драйвера для устройств ESMART Token 64K в пластиковом корпусе для работы в Windows 10*

ESMART PKI Client

- *Работа приложения ESMART PKI Client в ОС Linux стала более стабильной*
- *В приложении добавлен выбор типа генерируемого ключа ГОСТ*
- *В Windows 10/Windows Server 2016 по умолчанию отключена служба смарт-карт. Инсталлятор изменяет состояние данной службы по умолчанию и позволяет перевести службу в автоматический режим запуска*

Совместимость с УТМ ЕГАИС

- *Улучшена работа с транспортным модулем системы ЕГАИС для носителей ESMART Token ГОСТ и MSKEY «Ангара»*
- *Исправлена проблема создания сертификата RSA в личном кабинете*
- *Добавлена возможность расшифровки пакета обновления при работе с УТМ ЕГАИС*

Описание изменений версии 4.3

Новые компоненты

- ***Утилита командной строки esmart_firmware_checker** для проверки целостности прошивки USB-токенов и считывателей смарт-карт с использованием CRC128 или имитовставки по ГОСТ 28147-89.*
- ***Утилита командной строки ESMART PKIClientCli** под ОС Windows, Linux, macOS. Утилита позволяет выполнить все основные операции с картами и токенами ESMART.*
- ***Плагин для браузера Mozilla Firefox**, позволяющий выполнить все основные операции с картами и токенами ESMART по интерфейсу PKCS#11 с использованием JavaScript. Плагин, демонстрационная страница и документация доступны по адресу demo.esmart.ru.*

Общие обновления

- *Обновлены драйвера для ОС Linux и macOS.*
- *Добавлена возможность устанавливать CCID-драйвер в ОС Linux при наличии любой из двух версий библиотек-зависимостей: libusb 0.1 libusb 1.0.*
- *Обновлены модули поддержки носителей ESMART Token 64k и ESMART Token ГОСТ для СКЗИ CryptoPro CSP, добавлена возможность управления размерами контейнеров.*
- *Исправлен импорт файлов PKCS#12 с ключами ГОСТ Р 34.10-2012.*
- *Улучшена поддержка сертификатов с ключами нового стандарта ГОСТ Р 34.10-2012 в 256-битном режиме, в том числе обработка полей квалифицированных сертификатов в соответствии с приказом ФСБ №795 от 27 декабря 2011 г.*

Библиотеки, реализующие API PKCS#11

- *Улучшены функции работы с подписями C_ISBC_pkcs7Sign, C_ISBC_pkcs7Verify, C_ISBC_ pkcs7VerifyEx.*
- *Функция C_ISBC_pkcs7Sign возвращает ошибку CKR_VENDOR_CERT_EXPIRED при попытке подписи сертификатом с истекшим сроком действия.*
- *Добавлена поддержка нового типа объектов — доверенных корневых сертификатов, которые используются при проверке цепочки сертификатов. Для добавления и удаления доверенного корневого сертификата требуется ввод SO PIN.*
- *Добавлена функция C_ISBC_CertVerify для проверки сертификата по следующим параметрам: срок действия, отзыв по списку CRL (опционально) и проверку цепочки до доверенного корневого сертификата.*
- *В запрос на сертификат добавлена поддержка параметра «ОГРНИП» (OID 1.2.643.100.5).*
- *В запрос на сертификат добавлена поддержка параметра «Сведения о шаблоне сертификата» (OID 1.3.6.1.4.1.311.21.7).*
- *В функцию C_GetTokenInfo добавлен возврат версии ПО криптографического чипа.*
- *Исправлен экспорт функций из библиотек.*
- *Функция C_DeriveKey доработана на соответствие требованиям ТК26: параметры механизма CKM_GOSTR3410_2012_DERIVE задаются массивом байт.*
- *Поддержана работа с VKO, добавлена возможность использовать ключ, выработанный в результате VKO, поддержано свойство CKA_EXTRACTABLE.*
- *Для механизмов GOSTR3410_DERIVE и GOSTR3410_2012_DERIVE возвращается доступная функция CKF_DERIVE.*
- *Снято требование обязательного присутствия атрибута CKA_GOST28147_PARAMS в шаблоне объекта симметричного ключа.*
- *Добавлена возможность получения списка механизмов и информации по каждому механизму.*
- *Осуществлена доработка возможности использования сессионных объектов.*
- *Изменен способ работы со отметками времени в журнале событий на ESMART Token ГОСТ.*
- *Исправлена работа библиотек с процессорами архитектуры ARMv7.*

- *Ускорено выполнение функции завершения сессии C_Finalize.*
- *Исправлено внутреннее исключение при работе с функцией C_CloseAllSessions.*
- *Решена проблема загрузки контейнеров CryptoPro CSP с ключевой парой ГОСТ Р 34.10-2012 в 256-битном режиме.*
- *Расширен набор поддерживаемых криптопараметров ГОСТ Р 34.10, добавлена поддержка параметров CryptoPro XA, CryptoPro XB.*

C++ SDK

- *Добавлен пример для вычисления имитовставки на данные.*
- *Добавлен пример для выработки VKO.*
- *Добавлен пример чтения журнала ESMART Token ГОСТ.*
- *Добавлен пример работы с функцией проверки цепочки сертификатов.*
- *Добавлен пример загрузки доверенных сертификатов.*
- *Примеры скорректированы в соответствии с новым способом работы со отметками времени в журнале событий.*

Java SDK

- *В Java API добавлены функции: генерация ключевой пары, запрос сертификата, просмотр списка объектов.*
- *В запросе сертификата добавлена возможность работы с необязательными полями через параметры --ext и --attr.*
- *В библиотеке-обертке поддержан функционал проверки цепочки сертификатов с использованием функции C_ISBC_CertVerify.*
- *Обновлены примеры скриптов для вызова новых функций.*

ESMART PKI Client

- *Добавлена возможность загрузки доверенных корневых сертификатов только при предъявлении ПИН-кода администратора (SO PIN).*
- *В окне заполнения формы для создания запроса на сертификат при генерации запроса для ключей ГОСТ добавлена возможность выбрать тип ключа ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012 в 256-битном режиме.*
- *Добавлено поле «Сведения о шаблоне сертификата» (OID 1.3.6.1.4.1.311.21.7) в окно запроса на сертификат.*
- *Добавлено поле «ОГРНИП» (OID 1.2.643.100.5) в окно запроса на сертификат.*
- *В окне подтверждения подписи в поле отображение параметра label заменено на значение «Субъект сертификата».*
- *Во вкладке с параметрами токена добавлено отображение версии программного и аппаратного обеспечения.*
- *Реализована возможность опциональной проверки цепочки сертификатов и списка отзыва при проверке подписи.*
- *Добавлено уведомление об ошибке при попытке использовать для подписи недействительный по сроку действия сертификат.*
- *Исправлена отображение типа закрытых ключей.*
- *Изменен расчёт времени в журнале событий.*
- *Добавлена поддержка параметров CryptoPro XA, CryptoPro XB.*
- *Исправлена работа с объектами, не имеющими значений параметров id и label.*

ESMART PKI Client

Описание изменений версии 4.2

Новые возможности:

- *Добавлен журнал основных событий безопасности на ESMART Token ГОСТ. Для использования данной функции может потребоваться инициализировать карту. Журнал хранит события, связанные с инициализацией, сменой ПИН-кодов и вводом неверного ПИН-кода.*
- *Расширена поддержка сессионных объектов для объектов типа CKO_PUBLIC_KEY для функций C_Verify и C_VerifyInit и CKO_SECRET_KEY для импорта закрытого ключа из контейнера PKCS12 или закрытого ключа PKCS5 для функции C_UnwrapKey.*
- *Реализована поддержка блокирующего режима (без флага CKF_DONT_BLOCK) для функции C_WaitForSlotEvent.*
- *Реализована поддержка атрибута TRUSTED для сертификата удостоверяющего центра при предъявлении пароля администратора карты (загрузить сертификат с атрибутом TRUSTED возможно только по предъявлению SO-PIN).*
- *Реализована поддержка атрибутов CKA_START_DATE, CKA_END_DATE и CKA_VENDOR_CPRO_KP_NOTAFTER для объекта CKO_PRIVATE_KEY.*
- *Реализована поддержка функции C_UnwrapKey для ESMART Token ГОСТ.*
- *Добавлена возможность просматривать просматривать список контейнеров КриптоПро на ESMART Token ГОСТ.*
- *Добавлена реализация алгоритма хеширования ГОСТ Р 34.11-2012 в 256-битном режиме.*
- *Форма генерации запроса на сертификат дополнена в соответствии с требованиями 63-ФЗ «Об электронной подписи».*
- *В форму генерации запроса на сертификат добавлен выпадающий список для выбора страны.*
- *Добавлена поддержка возможности входа в личный кабинет системы ЕГАИС для ESMART Token ГОСТ и ESMART Token MS_KEY.*

Внесены изменения:

- *Изменен путь для Mono .Net Framework 4.4.1 и выше в macOS: /Library/Frameworks/Mono.framework/Versions/Current/bin/*
- *Исправлено обнаружение библиотек в системных директориях при работе со сканером отпечатка пальца Futronic FS82.*
- *Доработано получение запроса сертификата "Error:pkcswrapper::createcsr:C_ISBC_CreateCSR(0x6)" при работе с ключевой парой RSA в системе ЕГАИС.*
- *Исправлена возможность смены ПИН-кода пользователя в ESMART PKI Client для алфавитных ПИН-кодов.*
- *Исправлена работа с удалением контейнеров CryptoPro CSP*
- *Изменена настройка модуля CryptoPro CSP, позволяющая создавать на карте более 9 контейнеров*
- *Изменен способ создания записей в реестре при установке и восстановлении ESMART PKI Client*