КриптоПро eToken CSP

Персональное средство формирования квалифицированной ЭЦП для юридически значимого электронного документооборота, государственных услуг и защиты персональных данных.

Совместная разработка лидеров российского рынка информационной безопасности – компаний Крипто-Про и Aladdin

- **Аппаратная реализация российских алгоритмов ЭЦП в USB-ключах и смарт-картах**
- **Срок действия закрытого ключа пользователя – до 3-х лет!**
- **Полная совместимость и преемственность с eToken PRO и КриптоПро CSP**
- **Централизованное управление и интеграция с КриптоПро УЦ**
- **Сертификат ФСТЭК России на аппаратные ключи eToken для их использования при защите персональных данных до 2-го класса и в системах с классом защищенности до 1Г включительно**

Назначение

СКЗИ КриптоПро eToken CSP – это новое аппаратно-программное средство формирования квалифицированной ЭЦП с неизвлекаемым закрытым ключом, позволяющее увеличить срок действия закрытых ключей пользователей до 3-х лет!

Решение обеспечивает полный набор криптографических операций, реализованный в СКЗИ КриптоПро CSP 3.6 и полную интеграцию с инфраструктурой PKI на базе КриптоПро УЦ. При этом все операции с закрытыми ключами ЭЦП выполняются аппаратно, внутри чипа eToken, сами закрытые ключи никогда не покидают чип и не могут быть перехвачены.

КриптоПро eToken CSP противостоит атакам, направленным на подмену значения хэш-функции подписываемого документа, подмену значения самой подписи (например, при терминальном доступе),а так же на подбор PIN-кода.В решении реализована поддержка защищенного протокола обмена между аппаратным ключом eToken и программными компонентами КриптоПро CSP (технология работы с функциональным ключевым носителем - ФКН).

Области применения

КриптоПро eToken CSP предназначено для использования в системах юридически значимого электронного документооборота, предоставления государственных услуг в электронном виде и в других информационных системах, требующих применения технологии электронной цифровой подписи и многофакторной аутентификации.

К таким системам в первую очередь относятся:

- автоматизированные системы органов государственной власти и местного самоуправления;
- системы защищенного юридически значимого электронного документооборота системы клиент-банк, электронных торгов и пр. для подписи платежных поручений, заявок, котировок и др. документов.
- системы сдачи отчетности в электронном виде (Федеральная налоговая служба, Пенсионный Фонд РФ, Росстат, Фонд социального страхования, т.п.);
- проекты с социальной/идентификационной картой гражданина;
- системы мобильных платежей и пр.

Основные характеристики

- Поддержка полного набора криптографических операций и протоколов, реализованных в СКЗИ КриптоПро CSP 3.6 и КриптоПро УЦ.
- Аппаратная реализация российских криптографических алгоритмов и протоколов в чипе электронного ключа/смарт-карты eToken:
  - выработка ключевой пары, ЭЦП, проверка ЭЦП в соответствии с ГОСТ Р 34.10-2001;
  - вычисление хэш-функции в соответствии с ГОСТ Р 34.11-94;
  - симметричное шифрование в соответствии с ГОСТ 28147-89 в режимах простой замены и выработки имитовставки;
  - выработка ключа парной связи по алгоритму Диффи-Хелмана в соответствии с RFC 4357, п.5.
- Доступная энергонезависимая защищенная память для хранения пользовательских сертификатов, ключей, профилей и других данных.
- Уникальный неизменяемый идентификационный номер (ID) ключа, «прошитый» в чипе и напечатанный на его корпусе для удобства визуальной идентификации и учета.
- Высочайшая безопасность и защищенность от различного вида атак, подтвержденная российскими и международными сертификатами, в частности, сертификатом ФСТЭК России №1883 на соответствие заданию по безопасности по уровню ОУД2 и контролю отсутствия НДВ по 4 уровню. Данный сертификат разрешает использование продукта при создании автоматизированных систем до класса защищенности 1Г включительно и при создании информационных систем персональных данных до 2 класса включительно.

Как единый самостоятельный продукт СКЗИ КриптоПро eToken CSP находится в процессе сертификационных испытаний в ФСБ России.

КриптоПро eToken CSP

Соответствие требованиям российского законодательства

- Требования к технологиям, форматам, протоколам информационного взаимодействия, унифицированным программно-техническим средствам подсистемы удостоверяющих центров общероссийского государственного информационного центра (утвержденных Приказом №41 от 23.03.09 Министерства связи и массовых коммуникаций РФ).
- Стандарт Банка России СТО БР ИББС-1.0-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», в части обеспечения идентификации, аутентификации, авторизации, управления доступом, контроля целостности информационного обмена.

Модельный ряд

eToken выпускается в двух базовых форм-факторах – смарт-карты и USB-ключа. Для работы со смарт-картой можно использовать любой карт-ридер, в том числе встроенный в компьютер или в клавиатуру.

Дополнительно к базовой может быть добавлена функциональность, обеспечивающая совместимость с популярной на корпоративном рынке моделью eToken PRO (с западной криптографией).

USB-ключи могут выпускаться в виде комбинированных устройств:

- с дополнительной Flash-памятью объемом 1, 2, 4 ГБ (а также 8 и 16 ГБ со второго квартала 2010 г.)
- с дополнительной функцией генерации одноразовых паролей (OTP) для усиленной аутентификации пользователей при входе в ИС с использованием мобильного телефона, терминала, чужого компьютера.

Встроенная RFID-метка

В ключ eToken может быть имплантирована практически любая радиочастотная метка (RFID), используемая на предприятиях в системах контроля и управления доступом (СКУД) в помещения, учета рабочего времени сотрудников и пр.

Кастомизация

USB-ключи могут быть изготовлены на заказ в корпусах «фирменного» цвета с объемным логотипом компании или напечатанным логотипом методом тампопечати.

Смарт-карты могут поставляться как в виде «белого пластика» для самостоятельной печати на них, так и с высококачественной полноцветной полиграфией по согласованному дизайну.

По требованию заказчика могут быть разработаны и добавлены в память ключа eToken приложения, реализующие дополнительный функционал (социальная карта, транспортная карта и др.).

Технические подробности

Архитектура

Электронные ключи eToken, используемые в СКЗИ КриптоПро eToken CSP, выполнены на базе нового поколения электронных ключей eToken Java.

Основой платформы являются:

- защищенный высокоскоростной однокристальный микроконтроллер Atmel со встроенными контроллерами ISO 7816 (для смарт-карт) или USB 2.0 (для USB-ключей);
- операционная среда, соответствующая открытым спецификациям для смарт-карт Java Card Platform Specification 2.2.1 и Global Platform 2.2;
- виртуальная Java-машина для исполнения загруженных Java-апплетов.

Микроконтроллер выполнен на базе специализированной secureAVR® RISC-архитектуры и имеет эффективные встроенные средства противодействия известным физическим, логическим, переборным, стрессовым и пр. атакам в соответствии с требованиями Профиля защиты для смарт-карт (Smart Card Protection Profile – SCSUG-SCPP).

Для быстрого выполнения операций с большими числами используется специализированный 32-разрядный сопроцессор и пакет модульной арифметики и базовых операций над полем эллиптических кривых (ECC).

Микроконтроллер имеет аппаратный датчик случайных чисел (RNG), встроенные интерфейсы USB 2.0 (Full-speed, 480 Мб/сек) и контроллер ISO 7816 (со скоростью ввода-вывода 625Кб/сек), а также доступную EEPROM-память, расположенную на кристалле микроконтроллера.

Надежность

За счет использования однокристального специализированного микроконтроллера eToken имеет высочайшие эксплуатационные показатели:

- повышенные надежность и время наработки на отказ;
- пониженные энергопотребление и тепловыделение;
- повышенную защиту от пробоя статическим электричеством;
- повышенный ресурс и защищенность EEPROM-памяти (не менее 500,000 циклов чтения-записи и 10 лет хранения).

Ознакомительная версия

Для ознакомления с возможностями продукта и его тестирования доступна предварительная версия КриптоПро eToken CSP. Для ее получения обращайтесь в компании Крипто-Про и Aladdin.

ID: M03796-042010

Aladdin SECURITY SOLUTIONS
© 2010, ЗАО «Аладдин Р.Д.»
Тел.: (495) 223-0001
E-mail: aladdin@aladdin.ru
Web: www.aladdin.ru

КРИПТО ПРО
© 2010, ООО «Крипто-Про»
Тел.: (495) 780-4820
E-mail: info@cryptopro.ru
Web: www.cryptopro.ru