КриптоПро Рутокен CSP

Программно-аппаратное средство криптографической защиты информации

КриптоПро Рутокен CSP — программно-аппаратное СКЗИ, которое объединяет возможности российского криптопровайдера КриптоПро и идентификатора Рутокен ЭЦП.

В КриптоПро Рутокен CSP криптографические операции на закрытых ключах выполняются внутри ключевого носителя и ключи не покидают USB-токен.

В продукте реализована уникальная технология ФКН, которая защищает от атак протокол обмена между программной частью и ключевым носителем, а также обеспечивает дополнительную безопасность закрытых ключей.

Возможности КриптоПро Рутокен CSP

- Поддерживается весь функционал СКЗИ КриптоПро CSP 3.6;
- Существует полная интеграция с инфраструктурой PKI, основанной на КриптоПро УЦ;
- С использованием аппаратных ресурсов Рутокен ЭЦП выполняются следующие криптографические операции:
  - Генерация ключей по ГОСТ Р 34.10-2001;
  - Формирование электронной цифровой подписи по ГОСТ Р 34.10-2001;
  - Вычисление ключа согласования Диффи-Хеллмана (RFC 4357);
- Обеспечивается безопасное хранение и использование закрытых ключей внутри ключевого носителя без возможности извлечения.

Область применения

СКЗИ КриптоПро Рутокен CSP предназначено для использования в российских системах PKI, в системах юридически значимого электронного документооборота и в других информационных системах, использующих технологии электронной цифровой подписи, например:

- в системах клиент-банк при подписи платежных поручений;
- в системах защищенного документооборота;
- в системах сбора отчетности для предоставления в электронном виде;
- в органах власти и управления на федеральном и региональном уровнях;
- во всех других случаях, где целесообразно использовать технологии ЭЦП и необходимо обеспечить повышенную защиту ключей пользователя.

Архитектура ФКН

Функциональный ключевой носитель (ФКН) реализует принципиально новый подход к обеспечению безопасного использования ключевой информации, которая хранится на аппаратном носителе. Кроме формирования ЭЦП и генерации ключей непосредственно в микропроцессоре, ключевой носитель позволяет эффективно противостоять атакам, связанным с подменой хеш-значения или подписи в канале связи.

- Повышенная конфиденциальность закрытых ключей;
- Усиленная защита данных при передаче по открытому каналу благодаря использованию взаимной аутентификации ключевого носителя и программной составляющей при помощи оригинального протокола на основе процедуры EKE (electronic key exchange). При этом передается не PIN-код, а точка на эллиптической кривой;
- Передача хэш-значения по защищенному каналу, исключающему возможность подмены;
- После создания контейнера ключ пользователя не хранится ни в ключевом контейнере, ни в памяти криптопровайдера и не используются в явном виде в криптографических преобразованиях. Соответственно даже удачная аппаратная атака на ключевой носитель не поможет узнать ключ;
- Исключена возможность подмены подписи в протоколе обмена, ЭЦП вырабатывается по частям: сначала в ключевом носителе, потом окончательно в программной части CSP

КРИПТО ПРО
www.cryptopro.ru
тел.:(495) 780-48-20
e-mail: info@cryptopro.ru

Компания АКТИВ
www.rutoken.ru
тел.:(495) 925-77-90
e-mail: info@rutoken.ru