КриптоПро CSP 5.0/5.0 R2

Криптографический провайдер нового поколения

КРИПТОПРО

КриптоПро CSP 5.0 сертифицирован ФСБ России по классам КС1, КС2 и КС3. В нем преумножаются достижения предыдущих поколений криптопровайдера: шире список поддерживаемых платформ и алгоритмов, выше быстродействие, удобнее пользовательский интерфейс, единообразна работа со всеми ключевыми носителями.

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ И ОСНОВНЫЕ РЕШАЕМЫЕ ЗАДАЧИ

- Формирование и проверка электронной подписи
- Обеспечение конфиденциальности и целостности информации
- Аутентификация, шифрование и имитозащита сетевых соединений: протоколы TLS и IPsec
- Контроль целостности системного и прикладного ПО

Быстрое и безопасное использование российских криптоалгоритмов в приложениях

- Офисный пакет Microsoft Office
- Почтовый сервер Microsoft Exchange и клиент Microsoft Outlook
- Продукты Adobe
- Браузеры Яндекс.Браузер, Спутник, Internet Explorer, Chromium GOST
- Средство формирования и проверки подписи приложений Microsoft Authenticode
- Веб-серверы Microsoft IIS, nginx, Apache
- Средства удаленных рабочих столов
- Microsoft Remote Desktop Services
- Microsoft Active Directory

Поддержка современной российской и международной криптографии

Электронная подпись

ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), ECDSA, RSA

Хэш-функции

ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018), SHA-1, SHA-2

Шифрование

ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018),
ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018), ГОСТ 28147-89,
AES (128/192/256), 3DES, 3DES-112, DES, RC2, RC4

МУЛЬТИПЛАТФОРМЕННОСТЬ

Операционные системы

- Microsoft Windows
- macOS
- Linux
- FreeBSD
- Solaris
- AIX
- iOS
- Android
- Sailfish OS (Аврора)

Аппаратные платформы

- Intel / AMD
- PowerPC
- ARM
- MIPS (Байкал)
- VLIW (Эльбрус)
- Sparc

Виртуальные среды

- Microsoft Hyper-V
- VMWare
- Oracle Virtual Box
- RHEV

Функционал, появившийся в версии 5.0 R2

- Реализованы современные алгоритмы шифрования "Кузнечик" и "Магма" из ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), в т.ч. в протоколах CMS и TLS 1.2
- Класс защиты КС3 возможно реализовать не только на ОС Windows, но и на Astra Linux
- Встраивание клиентского TLS в приложения возможно без дополнительных тематических исследований
- Применение провайдера совместно с веб-серверами Apache и nginx для организации ГОСТ TLS возможно без дополнительного контроля встраивания
- Расширен список поддерживаемых ОС, платформ и ключевых носителей
- Повышена производительность

Интерфейсы встраивания в приложения

- Microsoft CryptoAPI
- PKCS#11
- OpenSSL engine
- Java CSP (Java Cryptography Architecture)
- Qt SSL

Полная совместимость с продуктами

- КриптоПро УЦ
- Службы УЦ
- КриптоПро ЭЦП
- КриптоПро IPsec
- КриптоПро EFS
- КриптоПро .NET
- КриптоПро Java CSP
- КриптоПро NGate

ПОДДЕРЖКА ПЕРЕДОВЫХ ТЕХНОЛОГИЙ ХРАНЕНИЯ КЛЮЧЕЙ

Облачный токен

Добавлена поддержка ключей, хранящихся на облачном сервисе КриптоПро DSS, через интерфейс CryptoAPI, позволяющий использовать их любыми приложениями.

Носители с неизвлекаемыми ключами и защищенным обменом сообщениями (ФКН)

Добавлена поддержка носителей с неизвлекаемыми ключами и защищенным по протоколу SESPAKE обменом сообщениями между криптопровайдером и носителем. SESPAKE реализован в некоторых носителях от Актив, ИнфоКрипт, СмартПарк и Gemalto.

Носители с неизвлекаемыми ключами

Реализована возможность работы с неизвлекаемыми ключами без обновления носителя до ФКН. Для этого добавлена поддержка таких носителей, как Рутокен ЭЦП 2.0, JaCarta-2 ГОСТ и InfoCrypt VPN-Key-TLS.

Классические пассивные USB-токены и смарт-карты

Сохранена поддержка классических носителей (без криптографических сопроцессоров) от Актив, Аладдин Р.Д., Gemalto, Multisoft, NovaCard, Rosan, Alioth, MorphoKST и СмартПарк. Также сохранена возможность хранения ключей в реестре Windows, на жестком диске и на флеш-накопителях на всех платформах.

КриптоПро CSP

@CryptoProInfoBot
info@cryptopro.ru
+7 (495) 995-48-20
https://cryptopro.ru

Единый интерфейс для работы со всеми ключевыми носителями, включая ключи в облаке

Интерфейс работы со всеми ключевыми носителями, в т.ч. с неизвлекаемыми ключами и ключами в облаке, остается единым. Переработка ПО, которое работает с КриптоПро CSP предыдущих версий, не потребуется.