JaCarta PKI/ГОСТ

JaCarta PKI/ГОСТ – PKI-токен для формирования усиленной квалифицированной электронной подписи и строгой двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам, безопасного хранения ключей, ключевых контейнеров программных СКЗИ.

- Работа с PKI в продуктах мировых вендоров обеспечивается штатными средствами.
- Усиленная квалифицированная электронная подпись с неизвлекаемым ключом ЭП для систем электронного документооборота, Web-порталов и облачных сервисов.
- Хранение ключевых контейнеров практически для всех программных СКЗИ (КриптоПро CSP, VipNet CSP и др.), а также использования в качестве отчуждаемого сертифицированного криптомодуля в составе других продуктов (в т.ч. КриптоПро CSP, VipNet CSP, Lissi CSP в режиме ЭП с неизвлекаемым ключом).
- Сертифицировано ФСБ России и ФСТЭК России.

Микроконтроллер: Защищённый смарт-карточный чип (AT90SC25672RCT), имеющий специальную сертифицированную защиту и на аппаратном, и на программном уровне (Secure by design), что позволяет успешно противостоять всем известным угрозам безопасности, методам взлома и клонирования.

Поддерживаемые криптографические алгоритмы

Для PKI-функционала: AES (длины ключей 128, 192, 256 бит); DES (длина ключа 56 бит); 3DES (длины ключей 112 и 168 бит); RSA (длины ключей 512, 1024, 2048); криптография на эллиптических кривых (длины ключей 160, 192 бит); аппаратная генерация ключей для RSA и криптографии на эллиптических кривых; алгоритмы согласования ключей: алгоритм Диффи-Хеллмана, алгоритм Диффи-Хеллмана на эллиптических кривых; функции хэширования: SHA-1, SHA-224 (эллиптические кривые), SHA-256, SHA-384, SHA-512; генератор последовательностей случайных чисел.

Для ГОСТ-функционала: ГОСТ Р 34.10-2001 (генерация ключевых пар, формирование и проверка ЭП); ГОСТ Р 34.11-94 (функция хэширования); ГОСТ 28147-89 (симметричное шифрование); реализовано только для данных, содержащихся в областях оперативной памяти изделия; алгоритм Диффи-Хеллмана (выработка ключа парной связи в соответствии с RFC 4357); генератор последовательностей случайных чисел.

Поддерживаемые операционные системы

Microsoft Windows: Windows 8.1 (32/64-бит); Windows 8 (32/64-бит); Windows 7 SP1 (32/64-бит); Windows Vista SP2 (32/64-бит); Windows XP SP3 (32-бит); Windows Server 2012 (64-бит); Windows Server 2008 R2 SP1 (64-бит); Windows Server 2008 SP2 (32/64-бит); Windows Server 2003 SP2 (32/64-бит).

Linux: Red Hat Linux Enterprise Linux 6.3 Desktop (32/64-бит); OpenSUSE 12.2 (32/64-бит); Ubuntu Desktop 12.04.1 LTS (32/64-бит); CentOS 6 (32/64-бит); Альт Линукс СПТ 6.0 (32/64-бит).

Apple Mac OS: Apple Mac OS X 10.6 x64 (Snow Leopard); Apple Mac OS X 10.7 x64 (Lion); Apple Mac OS X 10.8 x64 (Mountain Lion).

Наши контактные данные:

ул. Ленина, д.20, (четвертый этаж), каб. 422, 423. Остановка "Яблонька".
e-mail: info@ooo-skb.ru(ссылка для отправки email)
тел/факс: (3812) 53-20-18, (3812) 53-03-78