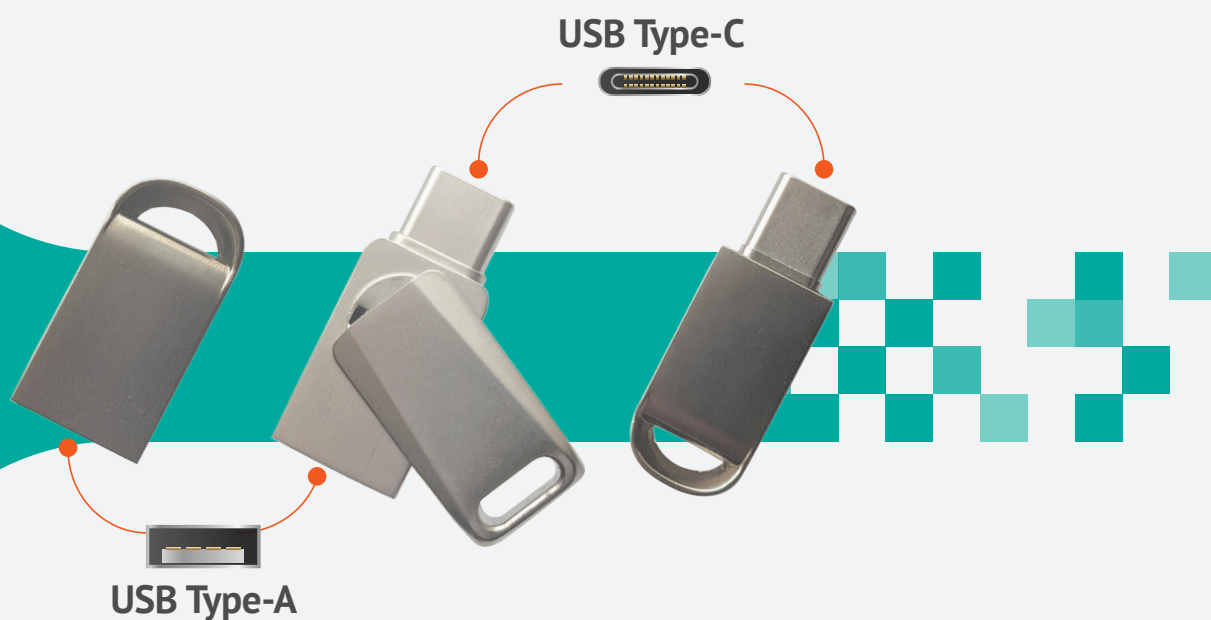


Новое поколение токенов JaCarta для строгой аутентификации и электронной подписи



JaCarta 3

- ▶ Многофункциональное СКЗИ с поддержкой всех современных криптоалгоритмов
- ▶ Универсальные форм-факторы для рабочих станций, ультрабуков, планшетов и смартфонов
- ▶ Сертификат соответствия ФСТЭК России, ФСБ России
- ▶ Спроектировано, разработано и произведено в России



Назначение

Сертифицированные USB-токены с аппаратной поддержкой российских и зарубежных криптоалгоритмов для усиленной квалифицированной электронной подписи (УКЭП) и строгой (двухфакторной) аутентификации.

Возможности



Усиленная квалифицированная электронная подпись (УКЭП)



Строгая (двухфакторная) аутентификация пользователей в информационных системах



Поддержка режима ФКН для работы с сертифицированными версиями СКЗИ КриптоПро CSP



Полное соответствие требованиям приказа ФСБ России № 171, для применения в качестве носителя в доверенных лицах ФНС в соответствии с Федеральным законом № 63-ФЗ "Об электронной подписи".



Персональный идентификатор для защиты от несанкционированного доступа для внешних модулей доверенной загрузки

Области применения



Вход в личный кабинет налогоплательщика на сайте ФНС по ЭП



Строгая двухфакторная аутентификация в корпоративные учетные записи в доменных инфраструктурах на базе Linux (ALD PRO, Samba AD, FreeIPA, OpenLDAP) и Windows



Вход по электронной подписи на Госуслуги



Ключевой носитель для ЕГАИС



Ключевой носитель для единой системы цифровой маркировки (Честный знак)



Государственные сервисы (например, Росэлторг)



Вход в учетную запись через мобильные устройства на базе Аврора и Астра мобайл

Сертификация

Согласно сертификату ФСБ № СФ/124-5060 и № СФ/124-5061 – KC1, KC2 "JaCarta-3":

- СКЗИ класса KC1/KC2 для защиты информации, не содержащей сведений, составляющих государственную тайну
- Средство электронной подписи (Приказ ФСБ России от 27 декабря 2011 г. № 796)

Согласно сертификату ФСТЭК №4446 JaCarta соответствует требованиям по безопасности информации (ФСТЭК России, 2020 г.) по 4 уровню доверия и технических условий. Разрешено использовать JaCarta в автоматизированных системах до класса защищённости 1Г, в государственных информационных системах до 1 класса защищённости, в информационных системах персональных данных до 1 уровня защищённости и в значимых объектах критической информационной инфраструктуры 1 категории.

Технические возможности

Поддержка криптографических алгоритмов на аппаратном уровне

- ГОСТ Р 34.10-2012/ГОСТ 34.10-2018 (256 и 512 бит): создание ключей ЭП, создание ключей проверки ЭП, автоматическое создание и проверка ЭП в информационной системе
- ГОСТ Р 34.11-2012/ГОСТ 34.11-2018 (256 и 512 бит): вычисление значения хеш-функции данных
- ГОСТ 34.12-2018 (Магма): генерация и импорт ключей шифрования, шифрование, расшифрование
- ГОСТ 34.13-2018 (Кузнечик): генерация и импорт ключей шифрования, шифрование, расшифрование
- RSA (длины ключей 1024, 2048, 4096)
- Криптография на эллиптических кривых ECC (ECDH, ECDSA) secp256k1, secp256r1, secp384r1, secp521r1
- AES (длины ключей 128, 192, 256 бит)
- DES (длина ключа 56 бит)
- 3DES (длины ключей 112 и 168 бит)
- Функции хеширования (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)
- Генерация последовательности случайных чисел

Применение

Аутентификация и электронная подпись для

- Электронных сервисов: портал Госуслуг, Тензор (SBIS), личный кабинет ИП и ЮЛ ФНС России, Контур (Диадок), система Честный Знак, система ЕГАИС, Такском, ИнфоТеКС Интернет Траст, Калуга-Астрал (ЭДО)
- Средств СКЗИ: КриптоПро CSP, ViPNet CSP, ViPNet OSSSL
- Программ создания ЭП: КриптоАРМ 5, ViPNet PKI Client, Jinn Client 2, SberSign 6.2
- Систем ДБО: Информационные Системы, ИНИСТ, R-Style Softlab, iSimpleLab, Юнисаб

Строгая двухфакторная аутентификация для

- Доменной 2FA: Linux (с применением ПО Aladdin SecurLogon) в доменах на базе Microsoft AD, FreeIPA, Samba DC, ALD PRO; Windows
- Зарубежных VPN: OpenVPN, Juniper, Cisco AnyConnect, Check Point Remote Access VPN, Fortigate VPN, Microsoft RRAS, GlobalProtect (PaloAlto)VPN
- Российских VPN: ViPNet Client, Континент АП\ZTN, NGate, VPN/FW "ЗАСТАВА-Клиент", С-Терра Клиент ST
- Зарубежных VDI: VMWare Horizon, Oracle VM VirtualBox, Microsoft RDP (RDS, RDG, RemoteApp, Azure), Citrix XenApp and Desktop/NetScaler
- Российских VDI: Термидеск, Basis Workplace
- SSH клиентов: Putty, OpenSSH
- При работе в тонких клиентах от HP, Dell, ICL, Тонк, Wyse

Средство персонального идентификатора для

- Средств доверенной загрузки: ПАК «Соболь», СДЗ Dallas Lock, ViPNet Safeboot 3 и выше, SafeNode System Loader
- Средств защиты информации: Secret Net Studio и Secret Net LSP, Dallas Lock 8.0, ViPNet SafePoint, Блокхост-Сеть 4

О компании

Аладдин – ведущий российский вендор – разработчик и производитель

- ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры предприятий и защиты её главных информационных активов
- средств аутентификации и электронной подписи для обеспечения информационной безопасности и защиты данных.

Компания работает на рынке с апреля 1995 г.

Многие продукты, решения и технологии компании стали лидерами в своих сегментах, во многих крупных организациях и Федеральных структурах - стандартом де-факто.

Компания имеет все необходимые лицензии ФСТЭК, ФСБ и Минобороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной, производство, поставку и поддержку продукции в рамках гособоронзаказа.

Большинство продуктов компании имеют сертификаты соответствия ФСТЭК, ФСБ, Минобороны России и могут использоваться при работе с гостайной со степенью секретности до "Совершенно Секретно". В 2012 г. в компании внедрена система менеджмента качества продукции (СМК), ежегодно проводится внешний аудит, имеются соответствующие сертификаты ГОСТ Р ИСО 9001-2015 (ISO 9001:2015) и ГОСТ РВ 0015.002-2020 на соответствие требованиям российского военного стандарта, необходимые для участия в реализации гособоронзаказа.

Основные направления деятельности

- Информационная безопасность, PKI
- Многофакторная аутентификация, обеспечение безопасного доступа к информационным ресурсам предприятия
- Организация безопасной дистанционной работы сотрудников и контрагентов организаций при использовании ими недоверенных средств вычислительной техники
- Средства электронной подписи
- Защита данных (на дисках, съёмных носителях, в базах данных)



+7 (495) 223 00 01
www.aladdin.ru
aladdin@aladdin.ru
129226, Москва, ул. Докукина, 16с1

Аладдин – ведущий российский вендор-разработчик и производитель ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры © 1995-2025, АО "Аладдин Р.Д." Все права защищены.



<https://t.me/aladdinrd>
<https://vk.com/aladdinrd>