Средства многофакторной аутентификации

Линейка JaCarta

- USB-токены
- BIO-токены
- Смарт-карты
- Мобильные токены (OTP, Push, SMS)

- Отказ от использования ненадёжных паролей
- Двух- и трёхфакторная аутентификация пользователей
- Поддержка PKI и работа с цифровыми сертификатами
- Электронная подпись (УКЭП, УНЭП)
- Полное соответствие требованиям регуляторов и приказам РФ (63-ФЗ, №117, №796)
- Включены во все ключевые реестры Минцифры и Минпромторга
- Сертифицированы ФСТЭК России, ФСБ России

Аутентификация — что важно знать

Надёжная аутентификация — это фундамент информационной безопасности. Причиной более 70% взломов, утечек и инцидентов в информационных системах (ИС) является слабая или неправильно реализованная подсистема аутентификации пользователей.

Что такое аутентификация?

Аутентификация — это способ подтверждения личности пользователя, его идентификационных данных.

Виды аутентификации:

- Простая — логин/пароль.
- Усиленная — двухфакторная (2ФА) с использованием аппаратного устройства.
- Строгая — двух- или трёхфакторная (3ФА) с использованием аппаратного устройства, криптографии, неизвлекаемого закрытого ключа, цифровых сертификатов и технологии PKI.

Основные типы аутентификации:

- Локальная (на устройстве).
- Доменная (в сетевой инфраструктуре организации).
- Браузерная (для Web-приложений и сервисов).

Факторы аутентификации:

- Знание (пароль, PIN-код).
- Владение (устройством, аппаратным средством аутентификации).
- Биометрия (уникальные признаки человека — отпечатки пальцев).
- *Подробнее в нац. стандартах ГОСТ Р 58833-2020, ГОСТ Р 70262.1-2022, ГОСТ Р 70262.2-2025.*

Проблема использования паролей

С появлением искусственного интеллекта (ИИ) поиск и подбор паролей, используемых для защиты учётных записей в ИС, стал довольно простой задачей, занимающей, буквально, секунды.

Так выглядит таблица с оценками времени взлома/подбора пароля, если он когда-то ранее был использован кем-то, и учётная запись с этим паролем была взломана или украдена.

Количество символов пароля	Только цифры	Прописные буквы (текст)	Прописные и строчные буквы	Прописные и строчные буквы + цифры	Прописные и строчные буквы + цифры + спец. символы
4	М	М	М	М	М
5	М	М	М	М	М
...	...	...	...	...	...
17	М	М	М	М	М
18	М	М	М	М	М

М — *Мгновенно*

По материалам https://www.hivesystems.com/blog/are-your-passwords-in-the-green

Пароли, даже очень длинные и сложные, стали крайне ненадёжны. Уровень доверия к ним низкий. Это означает, что от имени пользователя в ИС организации может подключиться злоумышленник.

Организации, использующие пароли для аутентификации пользователей в своих ИС, фактически не контролируют её периметр и **становятся мишенью для атак.**

Усиленная аутентификация

Усиленная аутентификация всегда предполагает наличие у пользователя некого **уникального аппаратного устройства** *(фактор владения)*.

Подтверждением факта владения и права распоряжаться данным устройством является **пароль** (PIN-код) устройства *(фактор знания)* и/или **отпечаток пальца** пользователя *(биометрический фактор)*.

Существенные условия (для корпоративных и государственных ИС):

- Пользователь не должен иметь **административных прав** для такого устройства.

  Примеры: *личный смартфон, USB-токены, поддерживающие стандарт FIDO/FIDO-2, использовать в корпоративных ИС нельзя.*

- Устройство должно использоваться **только для целей аутентификации** (получение или генерация одноразового пароля, SMS, push-уведомления), а работа в ИС должна производиться на другом устройстве.
- Не следует путать 2ФА и двухэтапную проверку, когда код доступа (общий секрет или однократно используемый секрет) передаётся на связанный с пользователем номер его мобильного телефона.
- Недопустимо использование зарубежных сервисов (например, Google Authenticator).

Риски, возникающие при использовании усиленной аутентификации:

- Перехват общего секрета при первичной инициализации устройства, производимой дистанционно (например, перехват QR-кода для инициализации OTP-генератора на смартфоне). Практически все решения передают общий секрет в открытом виде (кроме Aladdin 2FA).
- Извлечение из устройства секретного ключа для генерации OTP способно дискредитировать всю ИС и дать злоумышленникам доступ под видом легальных пользователей. Смартфон, как правило, имеет недоверенную среду.
- Первичная идентификация пользователей и инициализация устройств (запись общего секрета), как правило, выполняется без личной явки пользователя к администратору — удобство в ущерб безопасности.

*Усиленную аутентификацию **можно** применять в ИС среднего уровня доверия, в которых не обрабатывается информация ограниченного доступа (ДСП), персональные, биометрические, медицинские данные, служебная тайна (налоговая, банковская и др.), для внешних пользователей, имеющих учётные записи в ИС.*

Строгая аутентификация

Строгая аутентификация всегда предполагает:

- **Наличие у пользователя** уникального неклонируемого (защищённого) **устройства** с поддержкой криптографии с неизвлекаемым закрытым ключом, защитой от несанкционированного использования с помощью PIN-кода и/или контактной биометрии (например, по отпечаткам пальцев), работу с цифровыми сертификатами, разделением прав (администратор/пользователь).
- **Наличие в организации** развёрнутой PKI-инфраструктуры, собственного доверенного корпоративного Центра Сертификации (не путать с Удостоверяющим Центром), поддержку PKI и 2ФА на клиентских ОС.

Строгая аутентификация обеспечивает высокий уровень доверия ИС, является самым надёжным и удобным способом аутентификации для пользователей, сводя его действия к простой моторике — подключил своё устройство 2ФА и ввёл PIN-код. В отличие от одноразового пароля (всегда разного), PIN-код здесь постоянный (проще — помнят руки).

Альтернативой вводу PIN-кода является биометрия с использованием отпечатков пальцев. Она позволяет отказаться от запоминания и кражи PIN-кода и "привязать" используемое устройство к личности пользователя, так, что воспользоваться им для аутентификации в ИС никто кроме самого пользователя не сможет.

*Строгую аутентификацию **необходимо** применять в ИС высокого уровня доверия, в которых обрабатывается информация ограниченного доступа (ДСП), персональные, биометрические, медицинские данные, служебная тайна (налоговая, банковская и др.), **рекомендуется** применять во всех ГИС и на объектах КИИ независимо от класса защищённости.*

Как выбрать правильный вид аутентификации?

Требования законодательства

Требования к аутентификации пользователей в ИС госорганов, организаций с гос. участием, КИИ, а также для всех подрядных организаций, взаимодействующих с ними, регламентируются 117-м Приказом ФСТЭК России, вступившем в силу с 1 марта 2026 г.

Ниже приведены **минимально необходимые требования** и лучшие практики, рекомендуемые для ГИС, КИИ, а также для коммерческих компаний.

Тип пользователя	Тип доступа	Права доступа	Среда функционирования	Вид аутентификации		
				Объектовые ИС К3	Региональные ИС К2	Федеральные ИС К1
Внутренний (вкл. подрядчиков, имеющих учётные записи в ИС)	Локальный	Непривилегированный	Доверенная	П	У	У
			Недоверенная	У+	С+	С+
		Привилегированный	Доверенная	У	У	С
			Недоверенная	–	–	–
	Удалённый	Непривилегированный	Доверенная	У	У	С
			Недоверенная	С+	С+	С+
		Привилегированный	Доверенная	С	С	С
			Недоверенная	С+	С+	С+
		Непривилегированный	Доверенная (служебное мобильное устройство)	У	У	У
		Привилегированный	Недоверенная (личное мобильное устройство)	–	–	–
	Из-за пределов РФ	–	–	–	–	–
Внешний	Удалённый	Непривилегированный	Недоверенная (любая)	П	У	У

П — *пароль;* **У** — *усиленная аутентификация;* **С** — *строгая;*
+ — *с использованием специальных сертифицированных средств для безопасной дистанционной работы из недоверенной среды;*

Внутренний пользователь — *сотрудник организации или подрядчика (контрагента), имеющий в ИС учётную запись;*

Привилегированный пользователь — *пользователь с правами администратора, обладающий повышенными полномочиями (установка или обновление ПО), расширенным доступом в ИС (в т.ч. работа с критически важной информацией);*

Среда функционирования — *недоверенной считается любая среда (компьютер с установленным ПО), не соответствующая требованиям 117-го Приказа ФСТЭК России и требованиям по ИБ организации, не подтверждённая результатами гос. аттестации и/или не администрируемая самой организацией, предоставившей доступ к своей ИС.*

Достоверность результатов аутентификации зависит от ряда параметров:

- Тип пользователя (внутренний/внешний).
- Тип доступа (локальный/удалённый).
- Права доступа (непривилегированный/привилегированный).
- Среда функционирования (доверенная/недоверенная).
- Место подключения (офис, дом, территория РФ или за границей).

Чем больше рисков, тем больше дополнительных способов и компенсационных мер для подтверждения личности пользователя должно применяться.

Для разных сегментов ИС, условий работы пользователей, для разных сред функционирования должен быть определён РАЗНЫЙ набор факторов, дополнительных средств и способов подтверждения идентификационных данных и их связи с личностью пользователя.

Для разных сценариев рекомендуется выбирать разные типы средств аутентификации (адаптивная многофакторная аутентификация — МФА).

Подробнее об адаптивной МФА

Какое средство аутентификации выбрать?

Для строгой аутентификации

Средство аутентификации	JaCarta-3 PKI/ГОСТ	JaCarta-2 PKI/ГОСТ (SE)	JaCarta PKI	JaCarta PKI/BIO	JaCarta PKI/SecurBIO	Aladdin LiveOffice	JaCarta Virtual Token
Возможное количество факторов аутентификации	2	2	2	3	3	2	2
Форм-фактор							
USB-токен	●	●	●	○	●	●	○
Смарт-карта	○	●	●	●	○	○	○
Приложение для смартфона	○	○	○	○	○	○	●
Поддержка PKI							
Аппаратная реализация криптографии с неизвлекаемым закрытым ключом	●	●	●	●	●	●	●
Поддержка электронной подписи							
Аппаратная реализация российской криптографии с неизвлекаемым закрытым ключом	●	●	○	○	○	●	○
Хранение ключевых контейнеров программных СКЗИ (КриптоПро CSP и др.)	●	●	●	●	●	●	●
СКЗИ	JaCarta-3	JaCarta-3 (Криптотокен 2 ЭП для смарт-карт)	○	○	○	Криптотокен 2 ЭП	○
Поддержка биометрии							
С встроенным сканером отпечатков пальцев	○	○	○	○	●	○	○
С встроенным сканером отпечатков пальцев в карт-ридер	○	○	○	●	○	○	○
Сертификат соответствия							
ФСТЭК России	●	●	●	●	●	●	▸
ФСБ России	●	●	○	○	○	★	○
Для работы с гостайной	○	▸	○	○	▸	○	○
Обеспечение безопасной работы из недоверенной среды	○	○	○	○	○	●	○

▸ — *в процессе сертификации;* ★ — *имеет сертификаты на используемые компоненты*

Все модели устройств обеспечивают:

- Работу с цифровыми сертификатами, выпущенными корпоративными Центрами сертификации (**Aladdin Enterprise CA** и др.) и Удостоверяющими центрами (УЦ).
- Поддержку в системе централизованного управления жизненным циклом (**JaCarta Management System (JMS)** и др.).
- Поддержку технологии единого входа для разных приложений и сервисов — SSO (**JaCarta Identity Provider (JIP)**).
- Работу в российских ОС на базе Linux (при использовании клиентского ПО **Aladdin SecurLogon**), а также в MS Windows (при использовании **ПО "JaCarta — Единый Клиент"**).

Модели с поддержкой ЭП могут использоваться и для 2ФА, и в качестве **средства электронной подписи** (УКЭП, УНЭП), так что приобретать дополнительный эл. ключ для систем ЭДО (ФНС, ЕГАИС, Честный знак и др.) не потребуется.

Что нужно для реализации строгой аутентификации:

- Корпоративный Центр Сертификации (**Aladdin Enterprise CA**).
- Средства аутентификации.
- Клиентское ПО (для Linux — **Aladdin SecurLogon**).

Дополнительно рекомендуется:

- **Система централизованного управления жизненным циклом** цифровых сертификатов и средств аутентификации (**JaCarta Management System (JMS)**), обеспечивающая, в том числе, и автоматизацию большинства типовых рутинных операций, снижая нагрузку на администраторов.
- **Система единого входа** для разных приложений и сервисов — SSO (**JaCarta Identity Provider (JIP)**).

Для усиленной аутентификации

В качестве средства усиленной аутентификации (2ФА) могут применяться любые устройства, предназначенные для строгой аутентификации, а также средства 2ФА, указанные ниже.

Средство аутентификации	JaCarta LT*	JaCarta WebPass	Aladdin 2FA
Возможное количество факторов аутентификации	2	2	3**
Генерация/поддержка одноразовых паролей (OTP)	○	●	●
Генерация/подстановка в окно ввода сложных многоразовых паролей	○	●	○
Геолокация, возможность блокирования доступа из-за рубежа РФ	○	○	●
Сертификат соответствия ФСТЭК России	●	○	○
Поддержка ЭП			
Хранение ключевых контейнеров программных СКЗИ (КриптоПро CSP и др.)	●	○	○
Форм-фактор			
USB-токен	●	○	○
USB-токен с кнопкой подтверждения	○	●	○
Смарт-карта	○	○	○
Приложение для смартфона	○	○	●

** — рекомендуемая модель; ** — при использовании биометрии для разблокирования смартфона*

Что нужно для реализации усиленной аутентификации:

- Сервер аутентификации (**JaCarta Authentication Server (JAS)**).
- Средства аутентификации.
- Клиентское ПО (для Linux — **Aladdin SecurLogon**, для Web-приложений — **JC-WebClient**).

Дополнительно рекомендуется:

- Система централизованного управления жизненным циклом средств аутентификации (**JaCarta Management System (JMS)**).
- Система единого входа для разных приложений и сервисов — **SSO** (**JaCarta Identity Provider (JIP)**).

Для защиты личных учётных записей в онлайн-сервисах

Средство аутентификации	JaCarta WebPass	JaCarta U2F*
Количество факторов аутентификации	2	2
Аппаратная реализация криптографии с неизвлекаемым закрытым ключом	○	●
Генерация/поддержка одноразовых паролей (OTP)	●	○
Генерация/подстановка в окно ввода сложных многоразовых паролей	●	○
Один токен для множества ресурсов	●	●
Форм-фактор: USB-токен с кнопкой подтверждения	●	●

** — не для корпоративного использования! Администратором является сам пользователь*

Средства многофакторной аутентификации пользователей

USB-токены

USB-токены являются самым удобным и востребованным средством аутентификации пользователей.

Различаются исполнением (типом корпуса, USB-разъёмом, объёмом энергонезависимой памяти), сценариями использования, реализованной функциональностью.

Исполнение	Корпус	Разъём	Сценарий использования, особенности	Модели	Удобен для
	XL	Type-A	Интенсивное ежедневное использование для 2ФА и ЭП ("рабочая лошадка"): ▸ Удобный пластиковый корпус с цветной вставкой ▸ Повышенный ресурс контактной группы ▸ Позволяет встраивать RFID-метку для интеграции с корпоративной СКУД	▸ JaCarta-2 PKI/ГОСТ ▸ JaCarta-2 SE ▸ JaCarta-3 PKI/ГОСТ ▸ JaCarta PKI ▸ Aladdin LiveOffice	
	Металл	Type-A	Ежедневное использование в условиях разъездной работы для 2ФА и ЭП: ▸ Удобный прочный металлический корпус со встроенным USB-разъёмом ▸ В разъездах, в дороге его сложно будет сломать	▸ JaCarta-2 PKI/ГОСТ	
	Металл Mini	Type-A	Ежедневное использование с ноутбуком для 2ФА и ЭП: ▸ Укороченный металлический корпус (mini), объединённый с USB-разъёмом ▸ Практически не выступает за пределы корпуса ноутбука, оптимальный размер для комфортного использования	▸ JaCarta-3 PKI/ГОСТ	
	Металл	Type-C	Интенсивное ежедневное использование для 2ФА и ЭП на компьютерах и терминалах с разъёмами Type-C: ▸ Прочный металлический корпус ▸ Повышенный ресурс контактной группы	▸ JaCarta-2 PKI/ГОСТ	
	Металл Mini	Type-C	Интенсивное ежедневное использование для 2ФА и ЭП на ноутбуках, планшетах, смартфонах с разъёмами Type-C: ▸ Укороченный металлический корпус (mini) ▸ Повышенный ресурс контактной группы	▸ JaCarta-3 PKI/ГОСТ	
	Металл Dual	Type-A/C	Интенсивное использование для 2ФА и ЭП на ноутбуках, планшетах с новыми разъёмами Type-C, а также на ПК со старыми разъёмами Type-A: ▸ Укороченный дуальный металлический корпус с двумя разъёмами — Type-C и Type-A ▸ Повышенный ресурс контактной группы	▸ JaCarta-3 PKI/ГОСТ	
	Click	Type-A	Использование для 2ФА в ИС и защиты личных учётных записей: ▸ Укороченный пластиковый корпус и разъём USB ▸ Механическая кнопка с тактильным откликом для подтверждения транзакции	▸ JaCarta WebPass ▸ JaCarta U2F	
	Secur-BIO	Type-C	Интенсивное ежедневное использование для 2ФА (с отказом от ввода пароля) или 3ФА пользователей по биометрии: ▸ Встроенный сканер отпечатков пальцев ▸ Хранение шаблонов внутри устройства, а не в базе данных ▸ Возможность использования устройства только его владельцем ("привязка" к личности) ▸ Возможность крепления устройства к столу или монитору и активация его "по пальцу"	▸ JaCarta PKI/ SecurBIO	

Возможности кастомизации:

- Цвет пластикового корпуса и вставки (на заказ)

- Логотип заказчика:
  лазерная гравировка, цветная или ч/б тампопечать

Смарт-карты

Смарт-карты являются функциональным аналогом основных моделей USB-токенов и часто используются в качестве электронного удостоверения сотрудника, совмещая функции.

- Персонального средства 2ФА/3ФА (с хранением биометрических шаблонов в карте).
- Средства ЭП (УКЭП или УНЭП).
- Электронного пропуска (eID) в корпоративных СКУД и бейджа.

Возможности кастомизации:

- Может производиться печать на карте.
- Эмбоссирование.
- Встраивание NFC или RFID-метки для интеграции с корпоративной СКУД.

Ридеры для смарт-карт

Для работы со смарт-картами требуются ридеры. Аладдин выпускает целую линейку ридеров для корпоративного, мобильного (домашнего) использования, для встраивания в оборудование.

Смарт-карт ридеры для корпоративного использования:

Профессиональные доверенные смарт-карт ридеры Enterprise-класса

- Повышенный ресурс контактной группы.
- Не царапают поверхность карты.
- Усиленная защита от пробоя статическим электричеством.

JCR721

Горизонтальный

JCR731

Вертикальный

Отсоединяемый кабель разной длины с разъёмом USB Type-A/C

JCR761

Горизонтальный со сканером отпечатков пальцев

JCR781

Вертикальный со сканером отпечатков пальцев

Отсоединяемый кабель разной длины с разъёмом USB Type-A/C

Возможности кастомизации:

- Цвет корпуса
- Нанесение логотипа

Смарт-карт ридеры для портативного использования

- Очень компактные размеры, удобен для ношения с собой.
- Подключаемый кабель (разной длины, USB Type-A/C).

ASEDrive mini

Необходимое и рекомендованное ПО для работы со средствами аутентификации

ПО	Назначение
Единый Клиент JaCarta	ПО для поддержки МФА (2ФА/3ФА) и ЭП, настройки и администрирования всех моделей JaCarta
Aladdin Enterprise CA	Корпоративный Центр Сертификации (Linux)
JaCarta Identity Provider (JIP)	Корпоративный сервер SSO (в составе платформы JMS)
JaCarta Management System (JMS)	Корпоративная система централизованного управления жизненным циклом цифровых сертификатов и средств аутентификации
JaCarta SDK	Комплект разработчика для встраивания средств МФА и ЭП в прикладное ПО
Aladdin SecurLogon	Клиентское ПО для Linux с поддержкой PKI и МФА (локальной и многодоменной)
JC-WebClient	Клиент с поддержкой МФА и ЭП в любых Web-браузерах
АРМ администратора безопасности	Для настройки и администрирования СКЗИ и средств ЭП на базе JaCarta
JaCarta Authentication Server (JAS)	Высокопроизводительный сервер аутентификации Enterprise-класса (в составе платформы JMS)

Техническая спецификация

Критерий	Характеристики
Надежность и безопасность	**Все устройства линейки JaCarta:** ▸ Сконструированы как безопасные и для целей безопасности (Secure By Design) – Производятся на базе защищённых микроконтроллеров, сертифицированных по требованиям EMV и CAST – Процесс разработки соответствует требованиям разработки безопасного ПО (ГОСТ Р 56939-2024), менеджмента качества (ГОСТ Р ИСО 9001-2015) и военного стандарта и ГОСТ РВ 0015.002-2020. ▸ Имеют повышенную защиту от статического электричества, электромагнитного излучения и помех (ГОСТ Р 30805.22-2013, FCC) ▸ Имеют повышенную степень пыле- и влагозащищённости (до IP68)
Эксплуатационные характеристики	▸ Не менее 5 000 подключений к USB-порту ▸ Срок хранения данных в памяти: не менее 10 лет ▸ Рекомендуемый срок полезного использования: 3 года
Поддерживаемые криптографические алгоритмы	**Модели для PKI аппаратно реализуют зарубежные криптографические алгоритмы:** ▸ RSA: аппаратная генерация ключей длиной 1024, 2048, 4096 бит ▸ AES: длины ключей 128, 192, 256 бит ▸ DES: длина ключа 56 бит ▸ 3DES: длины ключей 112 и 168 бит ▸ SHA-1, SHA-224, SHA-256, SHA-384, SHA-512: вычисление значения хеш-функции ▸ Криптография на эллиптических кривых ECC (ECDSA, ECDH) **Модели для работы с ЭП аппаратно реализуют российские криптографические алгоритмы:** ▸ ГОСТ Р 34.10-2012/ГОСТ 34.10-2018 (256 и 512 бит): генерация ключевых пар, формирование и проверка электронной подписи ▸ ГОСТ Р 34.11-2012/ГОСТ 34.11-2018 (256 и 512 бит): вычисление значения хеш-функции ▸ ГОСТ Р 34.12-2015/ГОСТ 34.12-2018, ГОСТ Р 34.13-2015/ГОСТ 34.13-2018 (Магма, Кузнечик): генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ) ▸ ГОСТ 28147-89: генерация ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ)
Поддерживаемые интерфейсы, стандарты и технологии	▸ USB 2.0 ▸ CCID (Circuit Card Interface Device) ▸ PC/CS ▸ Cryptographic Service Provider (CSP) ▸ Microsoft Smartcard Minidriver ▸ Microsoft Crypto API ▸ Сертификаты X.509 v3 ▸ PKCS #11 v2.40 ▸ ISO/IEC 7816.
Поддерживаемые ОС	▸ Microsoft Windows 7 и выше ▸ Семейство GNU/Linux, включая все актуальные российские ОС ▸ Apple macOS 10 и выше

О компании

"Аладдин" — ведущий российский разработчик и производитель ключевых компонентов для построения доверенной безопасной ИТ-инфраструктуры предприятий и защиты её главных информационных активов.

Компания работает на рынке с апреля 1995 г. (31 год).

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 России, ФСБ России 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".

С 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 требованиями российского военного стандарта, необходимые для участия в реализации гособоронзаказа.

Ключевые компетенции:

- Аутентификация.
  - Подготовлено 13 национальных стандартов по идентификации и аутентификации.
  - Выпущено учебное пособие "Аутентификация — теория и практика".
  - Защищена докторская диссертация.
- Доверенная загрузка и "стерилизация" импортных ARM-процессоров с TrustZone.
- Разработка встраиваемых (embedded) Secure OS и криптографии для микроконтроллеров, JavaCard.
- Биометрическая идентификация и аутентификация по отпечаткам пальцев (Match On Card/Device).
- PKI для Linux и российских ОС.
- Прозрачное шифрование на дисках, флеш-накопителях.
- Защита баз данных.
- Аутентификация и электронная подпись для Secure Element (SE), USB-токенов, смарт-карт, IIoT-устройств, Web-порталов и электронных сервисов.
- Для всех, кто пользуется системами юридически значимого документооборота, массовыми онлайн сервисами с применением электронной подписи ЭП (УКЭП).

Аладдин

+7 (495) 223 00 01
aladdin@aladdin.ru
Москва, ул. Докукина, 16с1
www.aladdin-rd.ru
t.me/aladdinrd
vk.com/aladdin

Каталог компании

© 1995–2026, АО "Аладдин Р.Д."
Все права защищены