
# Корпоративный центр сертификации

## Aladdin Enterprise CA 2.0

- Отечественная замена Microsoft CA
- PKI уровня Enterprise на базе отечественных ОС
- Бесшовная миграция на Linux без перерыва в производстве
- Сертификация ФСТЭК
- Техническая поддержка при внедрении и эксплуатации

# Цифровая независимость в текущих условиях

Инфраструктура открытых ключей (PKI) - основа безопасной IT-среды.

Сейчас компании в России делятся на тех, кто использует PKI на базе Microsoft и тех кто «не использует PKI». И то и другое – это риск для безопасности информационной системы.

Задачи разные – решение одно.

Построить корпоративную PKI-инфраструктуру на базе отечественных решений.


Наш админ может сам сделать SSL-сертификат

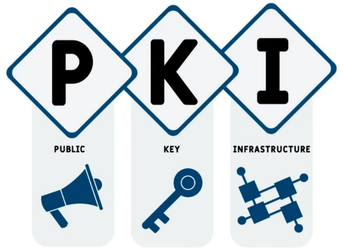
# Почему PKI для корпоративной IT-инфраструктуры?

**Строгая аутентификация пользователей в домене**

Цифровые сертификаты обеспечивают максимальный уровень доверия между серверами, пользователями и устройствами по результатам аутентификации.

**SSL-сертификаты**

Обеспечивают доверие к внутрикорпоративной инфраструктуре, службам и порталам компании, являются основой наиболее популярного в мире защищенного протокола HTTPS.




- Инфраструктура открытых ключей PKI – основа архитектуры информационной безопасности компании, её «скелет».
- Цифровые сертификаты обеспечивают надежную подпись, шифрование и аутентификацию людей, систем и устройств.
- PKI является критически важным компонентом архитектуры Zero Trust (нулевое доверие), которая лежит в основе современной кибербезопасности

**Подключение устройств по EAP802.1x**

Обеспечивает надежное подключение внешних устройств к сети предприятия, создание доверенной среды.

**АСУ ТП**

Интеграция PKI в системы управления технологическими процессами на производстве повышает уровень безопасности, обеспечивая надежную аутентификацию устройств и целостность данных.

**Сертификаты для ЭП**

Используя PKI для создания цифровых подписей, организации могут с уверенностью подтверждать подлинность электронных документов и защищаться от фальсификации.

# Чем рискуем сейчас?

## Риски использования PKI на основе Microsoft

**Более 90%** информационных систем в России построены на Microsoft Active Directory и используют Microsoft Certificate Services в качестве сервиса генерации и управления цифровыми сертификатами (сертификаты доступа, PKI инфраструктура).

- ✕ Microsoft ушел с рынка РФ, приобрести его невозможно
- ✕ Возможность полного отключения сервисов
- ✕ Отсутствие поддержки и обновлений
- ✕ Не соответствует требованиям регулятора

## Риски IT-инфраструктуры без PKI

PKI создает доверенную среду для безопасного взаимодействия пользователей и систем в сети. Это внутренний периметр безопасности, гарантирующий защиту от умышленных или непредумышленных действий внутренних нарушителей.

- ✕ Аутентификацию на основе паролей легко взломать
- ✕ Внутренняя сеть не защищена от подключения «неизвестных» устройств
- ✕ Уязвимость к фишингу (не защищена почта)
- ✕ Сложно обеспечить безопасное подключение удаленных пользователей и устройств

## А может сделать PKI на базе open-source?

Скорее нет. Для такого уровня это слишком рискованно и слишком сложно.

- ✕ Отсутствие поддержки
- ✕ Доступные компоненты не уровня Enterprise
- ✕ Недостаток экспертизы

# Импортозамещение: что важно?

Многие организации при импортозамещении ограничиваются заменой операционных систем, прикладного и офисного ПО на отечественные.

Недостаточно заместить только операционные системы и прикладное ПО. Нельзя игнорировать компоненты домена безопасности. Это сердце IT-инфраструктуры предприятия.

| Прикладное ПО | Операционная система | Доменная система | Службы сертификации |
|---|---|---|---|
| ТУРБО ERP | РЕДОС | ALD Pro | ? |
| МойОфис | АЛЬТ 8 СП | РЕДАДМ | |
| ADVANTA Система управления проектами | ASTRA LINUX | | |

## Что значит корпоративный центр сертификации

- Возможность параллельной работы в **гетерогенной среде** – как с наследием Microsoft, так и с отечественными решениями
- Реализация **строгой аутентификации** пользователей Linux – аналог встроенных сервисов Windows, включая MS Smart Card Logon
- Наличие необходимых сертификатов от отечественных **регуляторов**
- **Технологическая совместимость** с отечественными ОС и доменами
- Наличие квалифицированной технической **поддержки** и обновлений

# Aladdin Enterprise CA: основа отечественной PKI


**Aladdin Enterprise CA**

**Центр сертификации уровня Enterprise**

Для среднего и крупного бизнеса

**Полнофункциональная замена Microsoft CA**

- Глубокая интеграция в доменную инфраструктуру
- Полноценный PKI-функционал
- Автоматизация выпуска сертификатов
- Распределение ролей по разным узлам

**Бесшовная миграция**

- Параллельная работа с действующим Microsoft CA
- Импорт и использование шаблонов сертификатов Microsoft CA
- Поддержка MS Active Directory

**Для гетерогенных сред**

- Поддерживает различные архитектуры аппаратных платформ, отечественные ОС, виртуальные среды
- Одновременная работа с различными службами каталогов (Window+ Linux)
- Поддержка различных клиентских и мобильных ОС

**Совместим с отечественными и open-source службами каталогов**

- РЕД АДМ
- ALD Pro
- Альт Домен
- Samba DC
- FreeIPA

**Отвечает требованиям регулятора**

- Российское решение, в реестре отечественного ПО (№2021663130)
- Сертификат ФСТЭК УД-4 (в процессе)

**Опыт и экспертиза лидера рынка**

- Разработка плана плавного перехода на отечественные решения
- Поддержка на всех этапах
- Успешные реализованные кейсы

# Где рекомендуется использовать PKI?

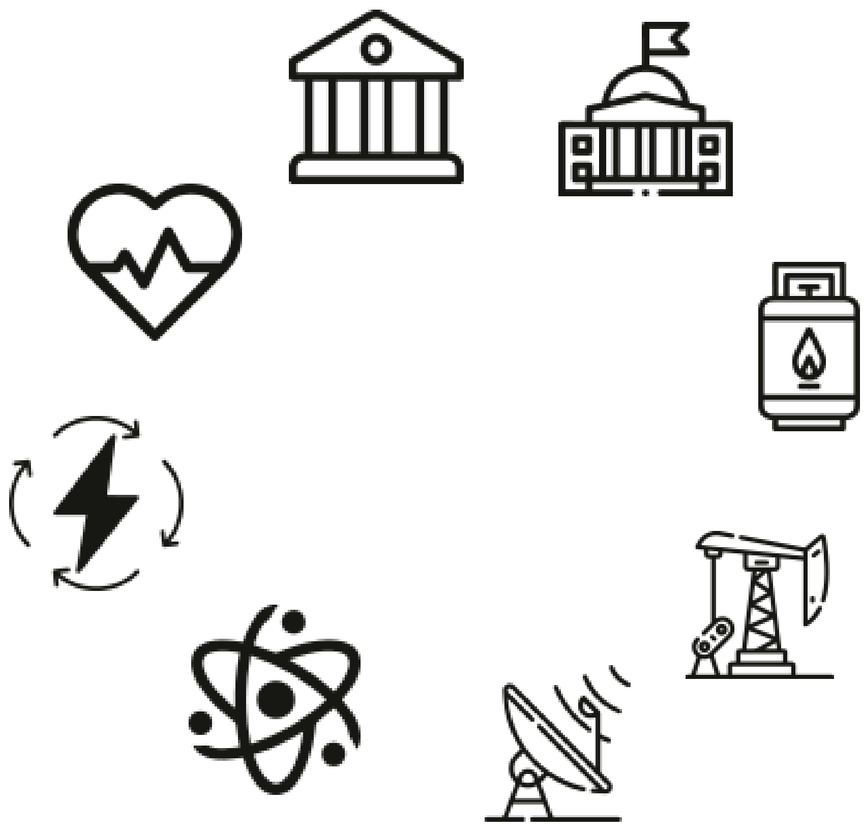
**Крупные предприятия со сложной ИТ-инфраструктурой и большой базой пользователей.** Им PKI поможет не только усилить безопасность за счет строгой аутентификации, но и облегчить управление ею.

**Отрасли с высоким уровнем регулирования, объекты КИИ**. Финансы, здравоохранение, энергетика, государственное управление и оборона – там, где работают с конфиденциальными данными и предъявляют строгие требования к соблюдению нормативных требований.

**Электронная коммерция и онлайн-услуги**. Компаниям, занимающимся онлайн-транзакциями, платформами электронной коммерции и цифровыми услугами, следует использовать PKI для обеспечения безопасности данных клиентов, защиты онлайн-транзакций и установления доверия со своими пользователями.

**Транснациональные компании**. Компании, работающие в разных странах и нуждающиеся в безопасной связи и обмена данными между своими филиалами или с партнерами, как правило, используют PKI.

**Поставщики облачных услуг**. Компании, предоставляющие облачные услуги, могут повысить безопасность своих платформ, внедрив PKI для защиты данных клиентов, аутентификации пользователей и защиты каналов связи.

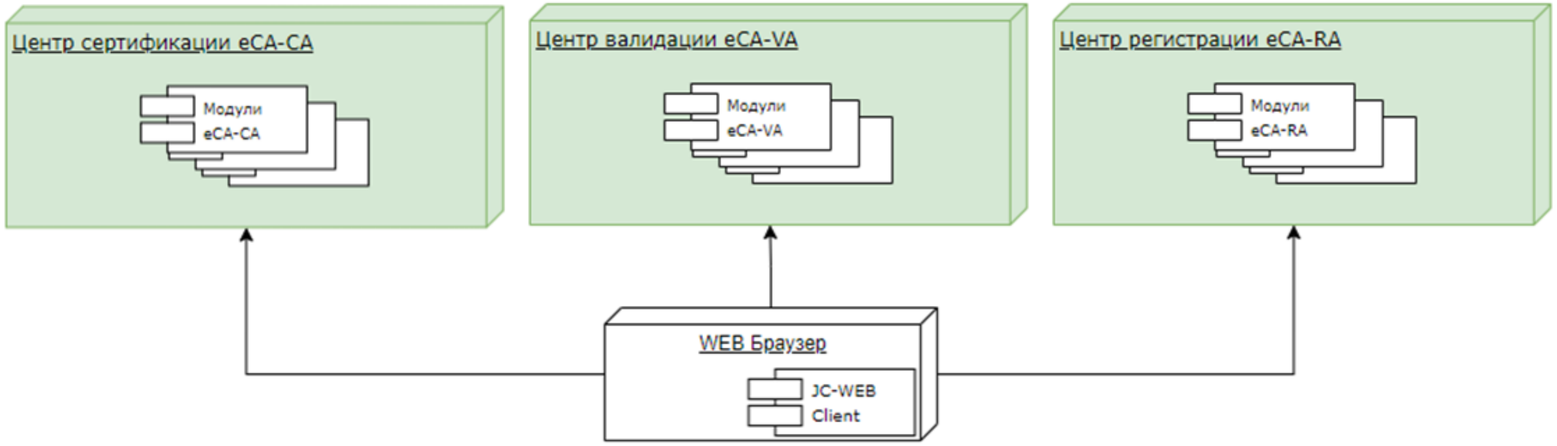


# Aladdin Enterprise CA: архитектура


## Aladdin Enterprise CA

**Центр сертификации уровня Enterprise**

Для среднего и крупного бизнеса

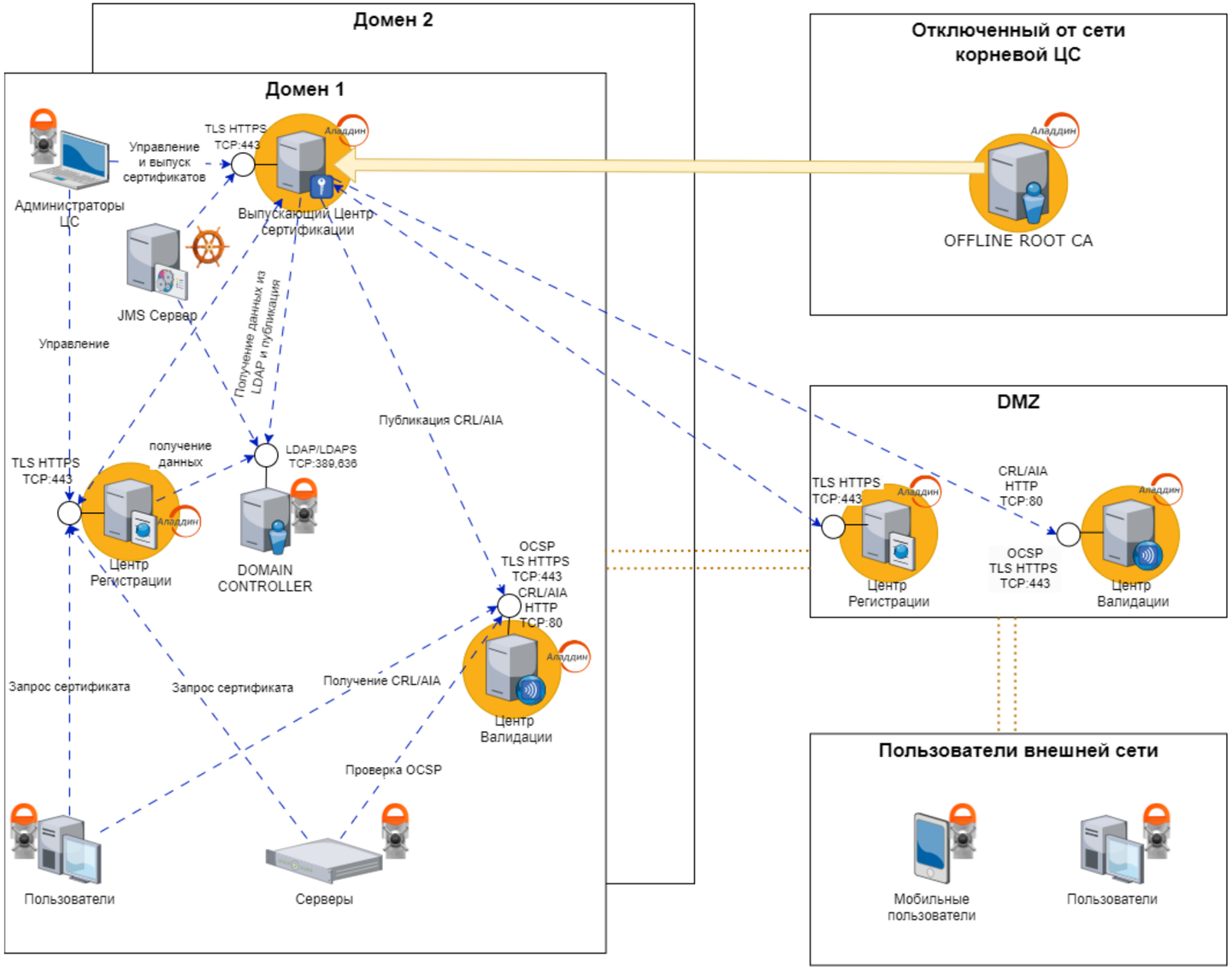



**Центр сертификации**
Ядро продукта, обеспечивает выпуск сертификатов, управление их статусами, подключение к каталогу пользователей и т.д.

**Центр валидации**
Предоставляет сведения об издателе и об отозванных сертификатах. Предоставляет точку скачивания CRL: CRL Distribution Point и службу OCSP для онлайн-проверки статусов сертификатов.

**Центр регистрации**
Компонент, предоставляющий возможность самим пользователям или техническим устройствам подключаться (аутентифицироваться) и оформлять заявку на получение сертификата. Заявка может быть обработана автоматически, с автоматической выдачей сертификата.

# Aladdin Enterprise CA: схема развертывания



# Aladdin Enterprise CA: демонстрация функционала


**Aladdin Enterprise CA**

**Центр сертификации уровня Enterprise**

Для среднего и крупного бизнеса

## Aladdin Enterprise CA 2.0

**Базовый функционал PKI**
- ✓ Возможность создания иерархии Центров сертификации
- ✓ Управление жизненным циклом сертификации
- ✓ Наличие сервисов публикации
- ✓ Наличие служб CRL DP, AIA, OCSP
- ✓ Поддержка Delta CRL
- ✓ Распределение ключевого функционала УЦ по разным узлам: Центр сертификации, Центр валидации, Центр регистрации
- ✓ Работа с шаблонами
- ✓ Алгоритмы: RSA, ECDSA

**Ролевая модель и полномочия:**
- ✓ Роль администратора
- ✓ Роль оператора для управления ЖЦ сертификатов
- ✓ Делегирование полномочий операторам и/или группам операторов

**Интеграция с доменами:**
- ✓ Загрузка объектов LDAP-каталога
- ✓ Возможность выпуска сертификатов для объектов
- ✓ Публикация сертификатов в LDAP
- ✓ Обеспечение SmartCard Logon аутентификации
- ✓ ALD Pro, РЕД АДМ, Microsoft AD, SambaDC, Free IPA

**Инфраструктурные возможности**
- ✓ Резервное копирование и восстановление
- ✓ Резервирование ключей ЦС
- ✓ Программный интерфейс (API)
- ✓ Почтовые уведомления
- ✓ Возможность мониторинга

**Миграция с Microsoft CA**
- ✓ Импорт шаблонов из Microsoft CA
- ✓ Возможность создания подчиненного от Standalone Root
- ✓ Поддержка многодоменной структуры

# Aladdin Enterprise CA: нефункциональные характеристики


**Aladdin Enterprise CA**

**Центр сертификации уровня Enterprise**

Для среднего и крупного бизнеса

**Производительность**:
Выпуск сертификатов 500 серт/мин

**Масштабируемость**:
До 500 тыс. сертификатов

**Безопасность**:
Соответствие 76 приказу ФСТЭК по УД-4
Реализация мер защиты: ИАФ, УПД, РСБ, ОЦЛ, ЗИС

**Среда функционирования**:
РЕД ОС 7.3 / Астра 1.7 / Альт СП Сервер 10
PostgreSQL (из состава ОС) / Postgres Pro / Jatoba
Open JDK 17 / Axiom JDK / Axiom JDK Certified

# Aladdin Enterprise CA: сценарии миграции


## Aladdin Enterprise CA

**Центр сертификации уровня Enterprise**

Для среднего и крупного бизнеса

# Aladdin Enterprise CA: схема лицензирования

Две основные лицензии:
1. Серверная
2. Клиентская

Серверная включает в себя PKI минимального объема:
1. Центр сертификации в роли корневого – 1 шт.
2. Центр сертификации в роли издающего – 1 шт.
3. Центр валидации с OCSP – 2 шт.
4. Возможность подключения к 1 ресурсной системе – 1 шт.
5. Возможность обновления в 2024-м году на версию с поддержкой
   - Центр регистрации – 1 шт.
   - Отказоустойчивого кластера для Центра сертификации

Клиентская лицензия
1. Субъект (максимум 3 сертификата, максимум 3 DNS-имени)

Пояснение: субъект это владелец сертификата. Например пользователь с CN, или msupn. Или семейство web-служб с одним DNS-именем. Или компьютер, соответствующий одной записи в LDAP-каталоге.

Дополнение к серверной лицензии:
1. Подключение к ресурсной системе
2. Wildcard
3. Дополнительный Центр валидации
4. Служба OCSP на Центре валидации
5. Дополнительный Центр регистрации

Дополнение к клиентской лицензии:
1. Увеличение количества сертификатов
2. Увеличение количества DNS-имен

Две схемы лицензирования – подписочная и неограниченная по времени, с возможностью продления технической поддержки.

# Центр компетенций Аладдин

Разработаем план импортозамещения и поможем его реализовать

**Помощь в построении системы 2ФА на базе отечественных ОС**

+ Инфраструктура открытых ключей (PKI)
+ Удалённое подключение сотрудников
+ Централизованное управление защищёнными носителями информации

**Интеграция системы 2ФА в ИТ-инфраструктуру заказчика**

+ Обеспечение связи с доменами на базе РЕД АДМ, ALD Pro и др.
+ Обеспечение связи с системами IdM

**Помощь в миграции инфраструктуры с Windows на Linux**

+ Разработка плана миграции на базе готовых отработанных методик

# План действий


**Aladdin Enterprise CA (Aladdin eCA)**

**Центр сертификации под Linux для организации инфраструктуры открытых ключей в ИС**

1. Узнать стоимость и необходимые контакты http://promo.aladdin.ru/eca
2. Получить демо и провести пилот
3. Узнать о специальных условиях

Программа по **импортозамещению** Аладдин

# Спасибо за внимание. Вопросы?


## Aladdin Enterprise CA

**Центр сертификации уровня Enterprise**

Для среднего и крупного бизнеса

**Полнофункциональная замена Microsoft CA**

- Глубокая интеграция в доменную инфраструктуру
- Полноценный PKI-функционал
- Автоматизация выпуска сертификатов
- Распределение ролей по разным узлам

**Бесшовная миграция**

- Параллельная работа с действующим Microsoft CA
- Импорт и использование шаблонов сертификатов Microsoft CA
- Поддержка MS Active Directory

**Для гетерогенных сред**

- Поддерживает различные архитектуры аппаратных платформ, отечественные ОС, виртуальные среды
- Одновременная работа с различными службами каталогов (Window+ Linux)
- Поддержка различных клиентских и мобильных ОС

**Совместим с отечественными и open-source службами каталогов**

- РЕД АДМ
- ALD Pro
- Альт Домен
- Samba DC
- FreeIPA

**Отвечает требованиям регулятора**

- Российское решение, в реестре отечественного ПО (№2021663130)
- Сертификат ФСТЭК (в процессе)

**Опыт и экспертиза лидера рынка**

- Разработка плана плавного перехода на отечественные решения
- Поддержка на всех этапах
- Успешные реализованные кейсы

Денис Полушин

АО "Аладдин Р.Д."

d.Polushin@aladdin.ru

linux@aladdin.ru

# 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.

Многие продукты, решения и технологии компании стали лидерами в своих сегментах, а 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".

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 7 национальных стандартов по идентификации и аутентификации (ГОСТ 58833-2020, ГОСТ Р 70262-2022)
  - Выпущено учебное пособие "Аутентификация – теория и практика"
  - Защищена докторская диссертация
- Доверенная загрузка и технология "стерилизации" импортных ARM-процессоров с TrustZone
- Разработка встраиваемых (embedded) Secure OS и криптографии для микроконтроллеров, смарт-карт, 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 и технология "опровославливания" зарубежных СУБД
- Аутентификация и электронная подпись для Secure Element (SE), USB-токенов, смарт-карт, IIoT-устройств, Web-порталов и эл. сервисов.