USIM-РФ

Первый этап формирования суверенного контура ИБ производства SIM-карт

Отраслевая инициатива по защите ключевой информации операторов и локализации критических этапов жизненного цикла USIM-карт в Российской Федерации.

Для обсуждения с регуляторами и представителями отрасли!



USIM-РФ — резюме

Пилотный проект отраслевого внедрения суверенного контура информационной безопасности для производства и применения USIM-карт в РФ

Что уже подтверждено

- Пилот реализован, партия введена **в коммерческую эксплуатацию**
- Отечественная ОС USIM и российский ИБ-контур охватывают **весь жизненный цикл карты**
- 2G/3G/4G/5G — Решение работает в сетях 2G/3G/4G/5G **без необходимости существенной модернизации ядра сети**
- Модель допускает **несколько российских площадок** и не создаёт зависимости от единственного поставщика

Дизайн контура ИБ (Этап 1)



Ключевой акцент для операторов

- Проект **не ломает** существующие процессы операторов
- Внедрение возможно **поэтапно** и эволюционно
- Инфраструктура оператора на 1-м этапе **сохраняется** без критических изменений
- Если себестоимость карты вырастет, то прежде всего из-за требований российского чипа, а не из-за самого **ИБ-контура**

Этап 2

1. Процедура сертификации Регулятором ОС USIM-карты
2. Российский корневой сертификат для SIM/eSIM
3. Доверенная загрузка / контроль происхождения ОС и профиля
4. Использование российской криптографии

Итог: USIM-РФ — это первая стадия эволюционного перехода к суверенному ИБ-контуру SIM/USIM без нарушения текущей инфраструктуры операторов.

Концепция проекта USIM-РФ

Создание сертифицированного и доверенного российского контура производства USIM-карт с соблюдением требований информационной безопасности.

Цель проекта

Обеспечить технологический суверенитет и защиту ключевой информации операторов при производстве SIM/USIM-карт на территории РФ.

Что создаём

Единый производственный контур с сертифицированной ОС USIM-карты, защищённой загрузкой ключей и контролем происхождения на всех этапах.

Ключевой результат

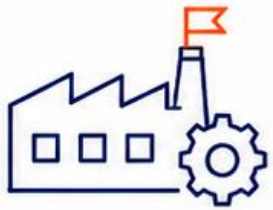
Доверенный производственный контур, соответствующий требованиям регуляторов и операторов, с возможностью масштабирования и подключения новых производителей.



Почему проект важен отрасли

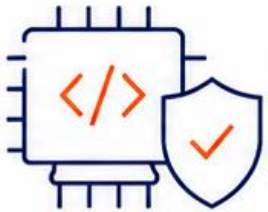
Проект USIM-РФ отвечает на ключевые отраслевые вызовы и формирует основу для доверенного контура производства SIM/USIM-карт в России.

01 Импортозамещение и технологическая независимость



- Снижение зависимости от иностранных цепочек поставок
- Локализация критических этапов производства
- Повышение устойчивости обеспечения операторов

02 Доверенное российское ПО



- Отечественная ОС USIM из реестра российского ПО
- Возможность внедрения **специализированного** функционала защиты ключей
- Контроль целостности и доверия к программной среде

03 Отсутствие зрелого российского стандарта ИБ производства SIM



- Нужен согласованный базовый набор требований
- Требуются БМУ, регламент ИБ и методические материалы
- Единые критерии оценки поставщиков

04 Необходимость отраслевого согласования с операторами и регуляторами



- Требования должны быть реализуемы в бизнес-процессах
- Важно учесть позиции операторов, производителей и регуляторов
- Совместная работа снижает риск избыточных барьеров

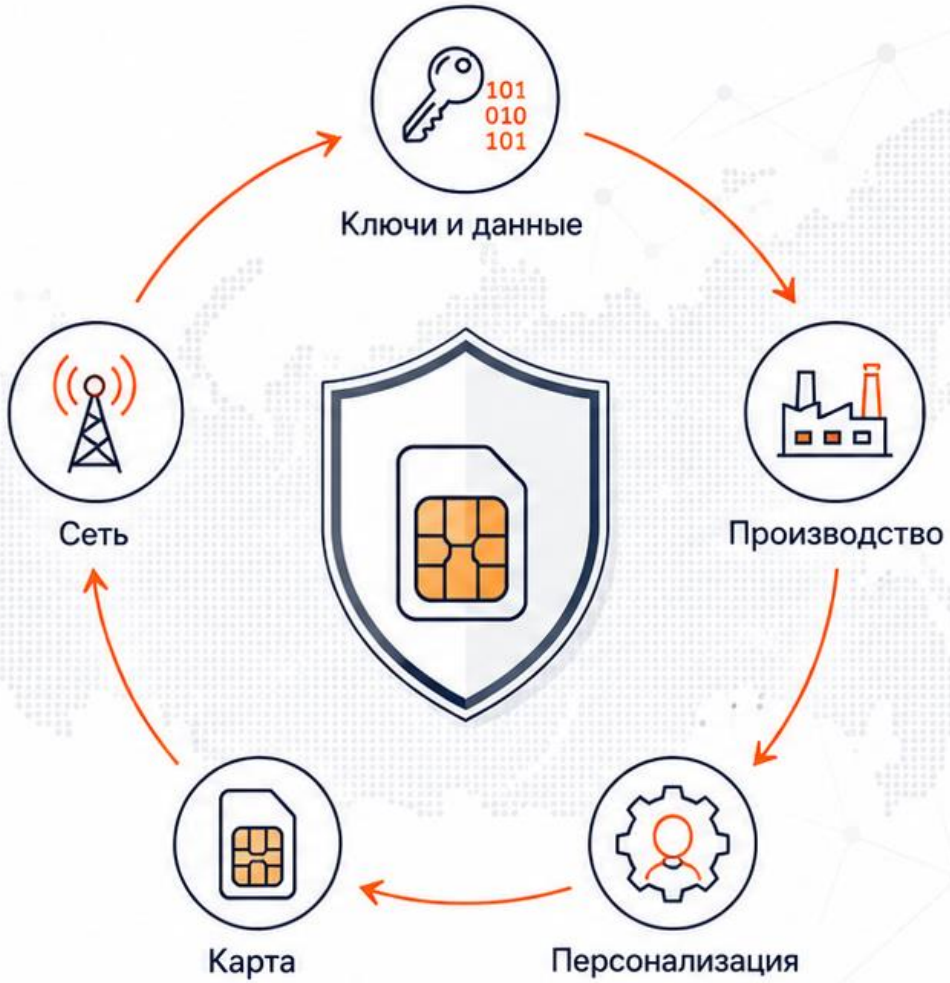
1. Проект укрепляет технологическую независимость.
2. Формирует доверенный производственный контур.
3. Создает основу для отраслевого согласования требований.

Область воздействия USIM-РФ

Проект защищает не только SIM-карту, а весь жизненный цикл: подготовка данных, производство, персонализация, загрузка ключей, эксплуатация.

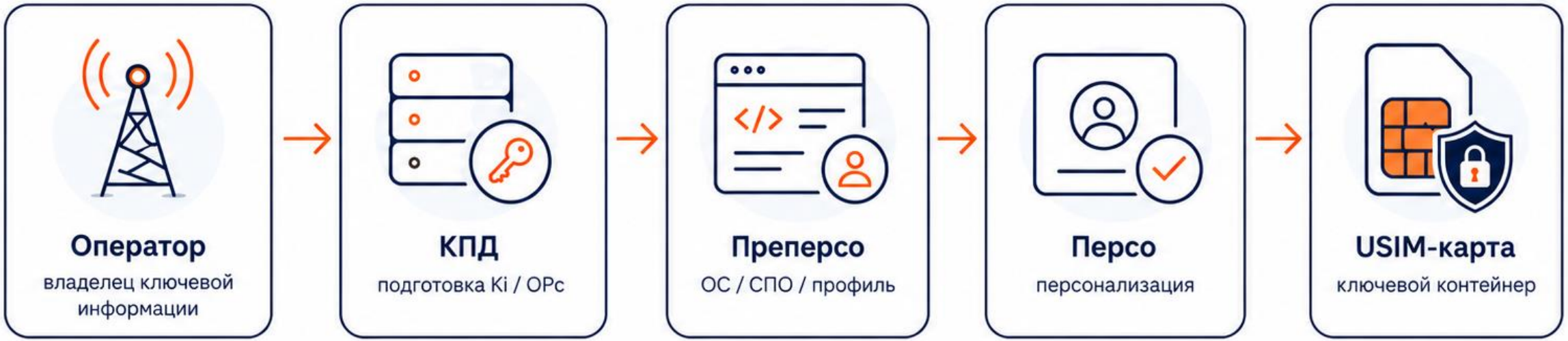


- защита ключевой информации
- локализация критических этапов
- совместимость с действующей сетью



Архитектура Этапа 1

Дизайн контура ИБ USIM-РФ



Контур разделяет ответственность и снижает риск компрометации ключевой информации на каждом этапе.

Базовая модель угроз ИС производства USIM-карт

Модель угроз разработана в соответствии с Методикой ФСТЭК России и охватывает угрозы на всех этапах жизненного цикла ключевой информации.

Классы угроз

1. 

Нарушение конфиденциальности

Несанкционированный доступ к ключевой информации (Ki, OPe и транспортные ключи) на всех этапах жизненного цикла.

2. 

Нарушение целостности

Модификация, подмена или искажение ключевой информации, ПО, профилей и технологических данных.

3. 

Нарушение доступности

Блокирование доступа к компонентам ИС, отказ в обслуживании, уничтожение данных и средств защиты.

4. 

Специальные воздействия

Физический доступ, внедрение аппаратных закладок, считывание по побочным каналам, НСД к носителям и оборудованию.

5. 

Человеческий фактор

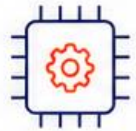
Ошибки персонала, злоупотребления полномочиями, недобросовестные действия подрядчиков.

Ключевые угрозы по этапам процесса



Утечка ключевой информации (КПД)

Перехват Ki, OPe и транспортных ключей при генерации, хранении или передаче.



Внедрение вредоносного ПО или профиля (СПП)

Загрузка недекларированных возможностей в ОС USIM-карты или профиль.



Подмена или перехват данных при персонализации (СП)

Несанкционированное изменение или загрузка ключей Ki, OPe на этапе персонализации.



Компрометация транспортных ключей (КПД + СП)

Раскрытие K4CA_batch или K4UV_batch и нарушение защищённого обмена.



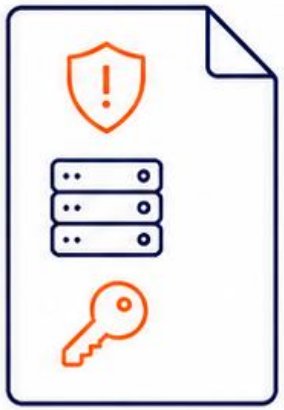
Отказ в обслуживании и уничтожение данных (Все этапы)

Нарушение доступности сервисов, уничтожение ключей и журналов, сбой производства.

БМУ + Регламент ИБ

БМУ и Регламент ИБ формируют основу суверенного допуска к производству USIM-карт: они закрепляют объекты защиты, актуальные угрозы, роли участников и обязательные меры контроля для российского производственного контура.

01 БМУ



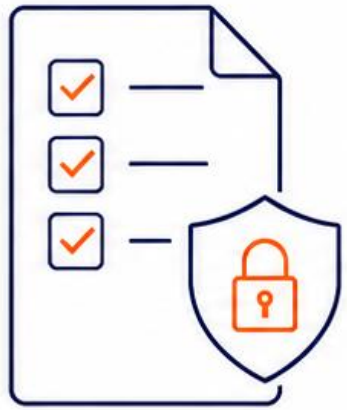
Какие угрозы актуальны?

Что такое информационная система производства карт?

Описывает структуру ИС, участников процесса, объекты защиты, источники угроз, сценарии атак и последствия нарушения безопасности.

Объекты защиты: Ki / OPc / OP • транспортные ключи • OC / профиль • КПД / Преперсо / Персо • каналы обмена

02 Регламент ИБ



Какие меры и процедуры должны быть реализованы?

Фиксирует организационные и технические требования, обязательные процедуры, этапы генерации ключей, сборки, персонализации, контроля, аудита и эксплуатации.

Меры контроля: допуск участников • аудит площадок • разграничение доступа • контроль ключей • мониторинг • инциденты

Единый «Регламент допуска производственного контура»

Почему ОС РуСим подходит для USIM-РФ

Отечественная операционная система для USIM-карт обеспечивает
защищенную загрузку ключевой информации и совместимость с массовой операторской инфраструктурой.

01 **Защищенная загрузка ключей**
Secure personalization, транспортные ключи, защищенная загрузка чувствительных данных.

02 **Технически реализованный механизм на карте**
Загрузка Ki / OPc и TK через APDU-команды с контролем целостности и шифрованием.

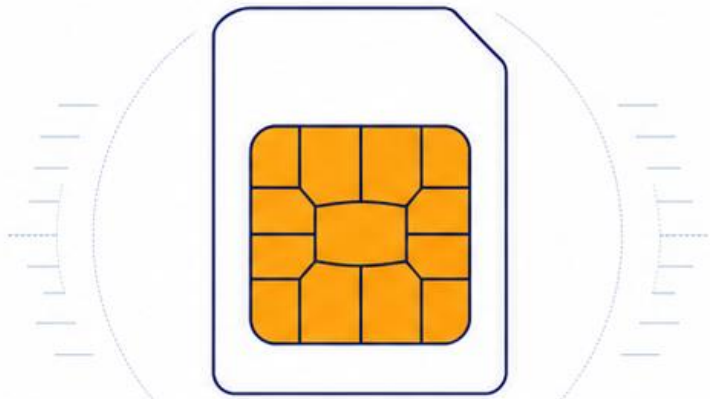
03 **Российский криптографический контур**
Поддержка MAGMA / ГОСТ и AES для совместимости с действующими процессами.

04 **Совместимость с операторами и стандартами**
ISO/IEC 7816, GSM, 3GPP, ETSI, JavaCard, GlobalPlatform, UICC / USIM / SIM API.

05 **Промышленная конфигурируемость**
Несколько конфигураций ОС под разные чипы и профили: 3G/4G/5G, EAP, TUAK, S3G и др.

ОС РуСим

ядро защиты ключевой информации



1 **Генерация ключей в КПД**
Ki и OPc генерируются в доверенном контуре (HSM). OP хранится в HSM.

2 **Защищенная передача**
Партии Ki / OPc передаются по доверенным каналам в зашифрованном виде под транспортным ключом.

3 **Персонализация карт**
Карта получает зашифрованные данные и выполняет их расшифрование и запись в защищенный контейнер внутри себя.

4 **Эксплуатация**
Ключи используются только внутри карты для аутентификации абонента. Прямой доступ к ключам невозможен.

Защита ключей на всех этапах жизненного цикла

Отечественная разработка и криптография

Совместимость с существующей инфраструктурой

Соответствие международным и российским стандартам

Готовность к промышленному массовому применению

Жизненный цикл ключевой информации при производстве USIM

Логика процесса на основе БМУ USIM-РФ, Регламента бизнес-процесса и описания ОС РуСим

1 Оператор связи

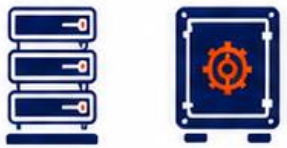
- Формирует исходную ключевую информацию OP
- Передаёт OP и параметры профиля по безопасному каналу
- Согласует правила обмена и транспортные ключи



2 КПД / Компания

Комплекс подготовки данных (КПД)

- Транспортный API: приём/передача только в зашифрованном виде
- HSM: хранение OP
- Генерация Ki и OPc
- Генерация транспортных ключей и ключей партий
- Шифрование партий (Ki, OPc)

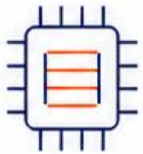


ОС / профиль карты →

3 Сегмент производства

Сборка программно-аппаратной платформы

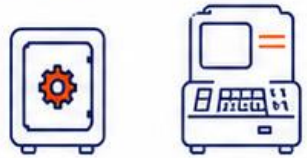
- Сборка чип-карты
- Запись ОС РуСим и профиля
- Конфиденциальные ключи в процессе ещё не обрабатываются



4 Сегмент персонализации

Персонализация USIM

- Транспортный API: обмен только в зашифрованном виде
- HSM: полностью хранит транспортные ключи
- Получение зашифрованных Ki / OPc
- Передача ключей на карту в зашифрованном виде
- Контроль качества и выпуск партий



5 USIM-карта / ОС РуСим

- Приём транспортных ключей и ключей идентификации
- APDU-загрузка ключей
- Расшифрование и сохранение внутри карты
- Запись Ki и OPc в ключевой контейнер
- Временные ключи и промежуточные данные уничтожаются



Открытая обработка ключевой информации исключена

Ключевой материал передаётся только в зашищённом виде

Расшифрование Ki / OPc происходит только внутри USIM-карты

Обозначения	
OP	исходный ключ оператора
Ki	индивидуальный ключ аутентификации абонента
OPc	производный ключ оператора
TK / ключ партии	транспортный ключ для зашищённой передачи

Как ключи разворачиваются на USIM-карте

Логика загрузки ключей в ОС РуСим: APDU, KVN, CMAC, AES / MAGMA, защищённый контейнер

1 Подготовка ключевого пакета



- Персонализационная станция / HSM
- Формируется команда загрузки ключа
- Указываются тип ключа
- Присваивается версия ключа KVN
- Данные шифруются транспортным ключом

AES / MAGMA

2 Формирование APDU



DATA: key type, key index, KVN, encrypted key value, CMAC

Одна APDU-команда = один ключ

CLA	INS	P1/P2	DATA	Le

3 Передача на USIM



- Команда поступает в карту
- Ключевой материал не раскрывается на площадке
- Передача выполняется в защищённом виде

4 Проверка внутри карты

USIM / ОС РуСим



- Проверка формата APDU
- Проверка KVN
- Проверка CMAC
- Определение типа ключа

5 Внутреннее расшифрование и запись

USIM / ОС РуСим

Защищённый контейнер ключей

TK	транспортный ключ
Ki	ключ аутентификации абонента
OPc	производный ключ оператора

- Расшифрование выполняется только внутри карты
- Для TK — обновляется транспортный ключ
- Для Ki / OPc — запись в соответствующий слот

6 Завершение операции



- USIM-карта удаляет временный TK
- Временные буферы очищаются
- Промежуточные данные уничтожаются
- Ключи становятся недоступны для извлечения
- Карта готова к аутентификации абонента

Ключевые принципы безопасности

- **KVN** — версионирование ключей
- **CMAC** — контроль целостности
- **AES / MAGMA** — защита транспортного уровня
- Открытая обработка ключей исключена
- Расшифрование только внутри USIM-карты

Обозначения

- **TK** — транспортный ключ
- **Ki** — ключ аутентификации абонента
- **OPc** — производный ключ оператора
- **KVN** — версия ключа

Инфраструктура операторов — минимальное воздействие

Опасения операторов

- Риски для стабильности и доступности сети
- Сложности интеграции и изменения в ядре сети
- Высокие затраты и длительные проекты

Ответ проекта

- сети 2G/3G/4G/5G сохраняются
- логика взаимодействия с ядром сети не меняется
- оператор сохраняет контроль над ключевой информацией
- без масштабных IT-изменений и дополнительных капвложений



USIM-РФ: промышленная реализация

билайн

Реализовано

Продукт USIM-РФ создан и готов к эксплуатации

01

Пилот

Испытания в лабораторных и сетевых условиях оператора

02

Опытная эксплуатация

Стабильная работа подтверждена в реальной сети

03

Промышленная готовность

Готовность к серийным поставкам и масштабированию

04



USIM-РФ работает в действующей сети оператора

ОС «РуСИМ»

Российская программная платформа USIM-РФ

Работает в действующей сети оператора

Подтверждено в реальной эксплуатации

2G / 3G / 4G / 5G

Поддержка текущих и перспективных сетей мобильной связи

Без изменения базовой логики взаимодействия с ядром сети

Интеграция в существующую сеть и бизнес-процессы оператора

Российский периметр без монополизации

Фокус — импортозамещение при сохранении конкуренции между российскими поставщиками.
Требования к участникам открыты и не подразумевают монополизацию,
что повышает устойчивость цепочки поставок.

01



Единые требования допуска

Общие правила ИБ, БМУ, регламент, аудит площадок и требования по контролю ключевой информации.

02



Критичные операции в РФ

Подготовка данных, хранение и загрузка ключей, персонализация и контроль производственного контура.

03



Пилот → масштабирование

Модель уже апробирована на нескольких российских площадках и может тиражироваться без снижения уровня безопасности.

04



Для операторов

Снижение рисков перебоев, монопольного повышения цен, компрометации ключей и зависимости от единственного производителя.



Суверенность ≠ монополизация. Цель — единые требования, конкуренция и масштабируемость.

Этап 2 — Российская криптография



Переход от подтвержденного производственного ИБ-контура к сертифицированной криптографической модели SIM/eSIM.

2026

01

Сертификационный трек у регулятора для ОС USIM-карты

2027

02

Российский корневой сертификат для SIM/eSIM

2027

03

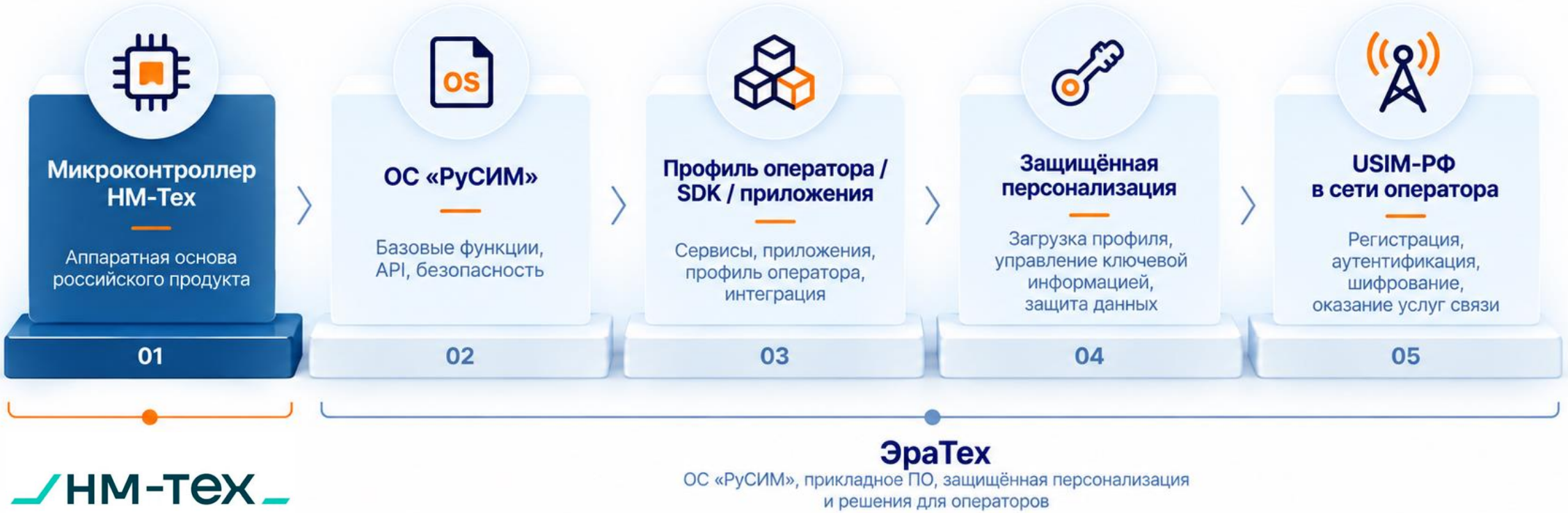
Доверенная загрузка и контроль происхождения ОС и профиля

2028

04

Российская криптография на алгоритмах S3G, Кузнечик и другие, введение компонентной базы

Этап 3 – Переход на российские микроконтроллеры



Российский микроконтроллер НМ-Тех **завершает** уже существующий продуктовый стек

Локализация и 719ПП – SIM-карта как конечный продукт

ЭраТех

Российский микроконтроллер

Отечественная аппаратная основа SIM/USIM



01

ОС «РуСИМ»

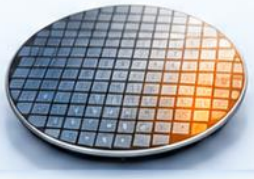
Российская ОС для SIM/USIM. Контроль программной платформы



02

Производство

Сборка и тестирование на российских площадках партнёров



03

Защищённая персонализация

Загрузка профиля, ключевой и сервисной информации в защищённой среде в РФ



04

Контроль жизненного цикла

Контроль процессов, обновлений и информационной безопасности на всех этапах



05

Оценивать нужно конечный продукт SIM/USIM,
а не отдельный компонент.

Российская ОС — один из **ключевых элементов локализации.**

Дорожная карта

