КРИПТОПРО

Ключевое слово
в защите информации

Классическая PKI в прокрустовом ложе IoT с примерами

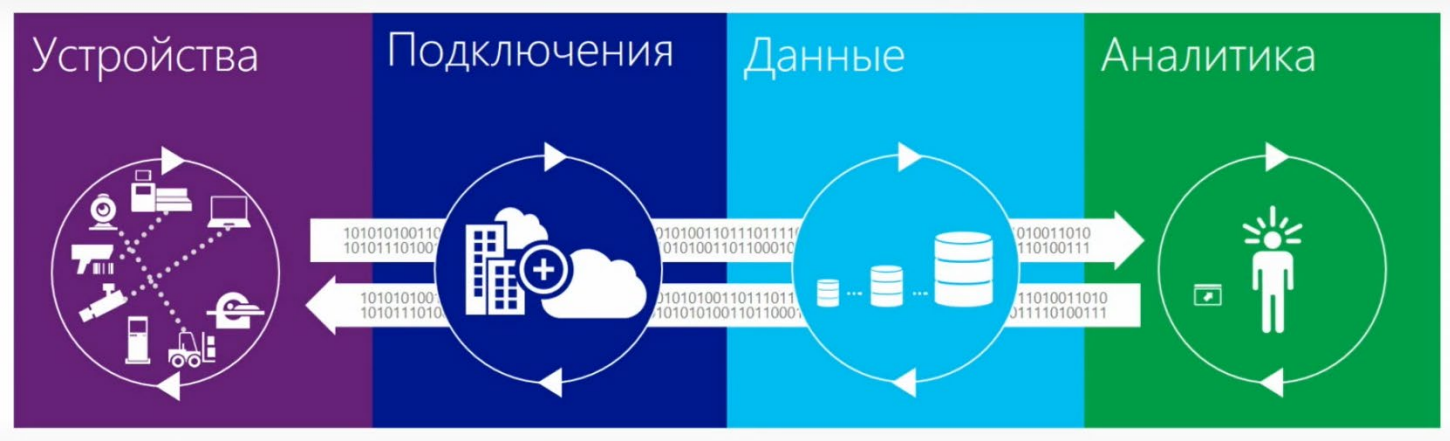
СМИРНОВ ПАВЕЛ
Директор по развитию

АЛЕКСЕЕВ ЕВГЕНИЙ
Начальник отдела криптографических исследований

АХМЕТЗЯНОВА ЛИЛИЯ
Зам. начальника отдела криптографических исследований

PKI Форум Россия 2021

Многообразие IoT

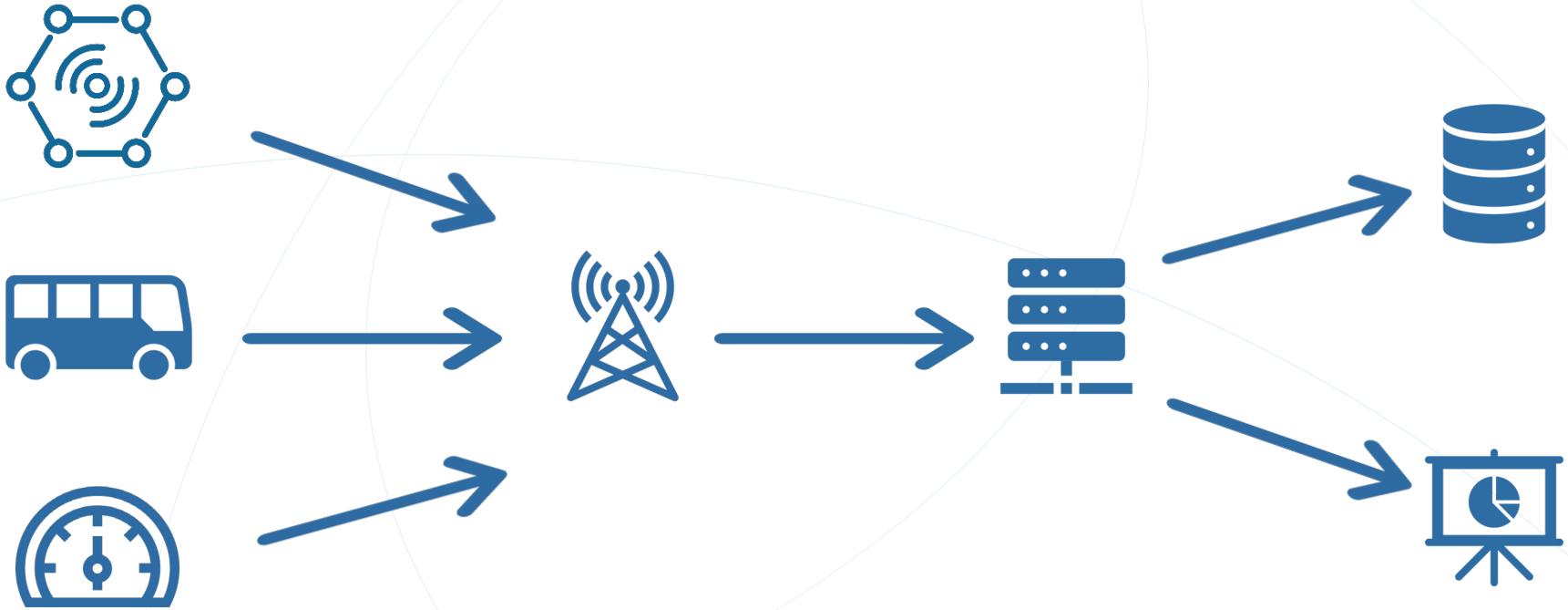


Архитектура IoT

Источник: Forrester

Различные сценарии и устройства

Сценарий «получения телеметрии»



- Односторонняя передача данных
- Требуется обеспечить некорректируемость (целостность)
- Иногда требуется конфиденциальность

Проблемы сценария

Жизненный цикл датчика

- Производство чаще всего за рубежом
- Ограниченные возможности технического обслуживания
- Срок жизни без обслуживания больше стандартного срока жизни ключа
- Нет возможности дистанционно обновлять ключи

Ограниченные возможности датчика

- Ограниченные вычислительные ресурсы
- Потенциально большой объём собираемой информации
- Трудность создания надёжного источника случайности

- *В совокупности могут сделать невозможным применение «классического» PKI-ного алгоритма подписи*

Решение 1: Распределенное формирование подписи

Когда подходит:

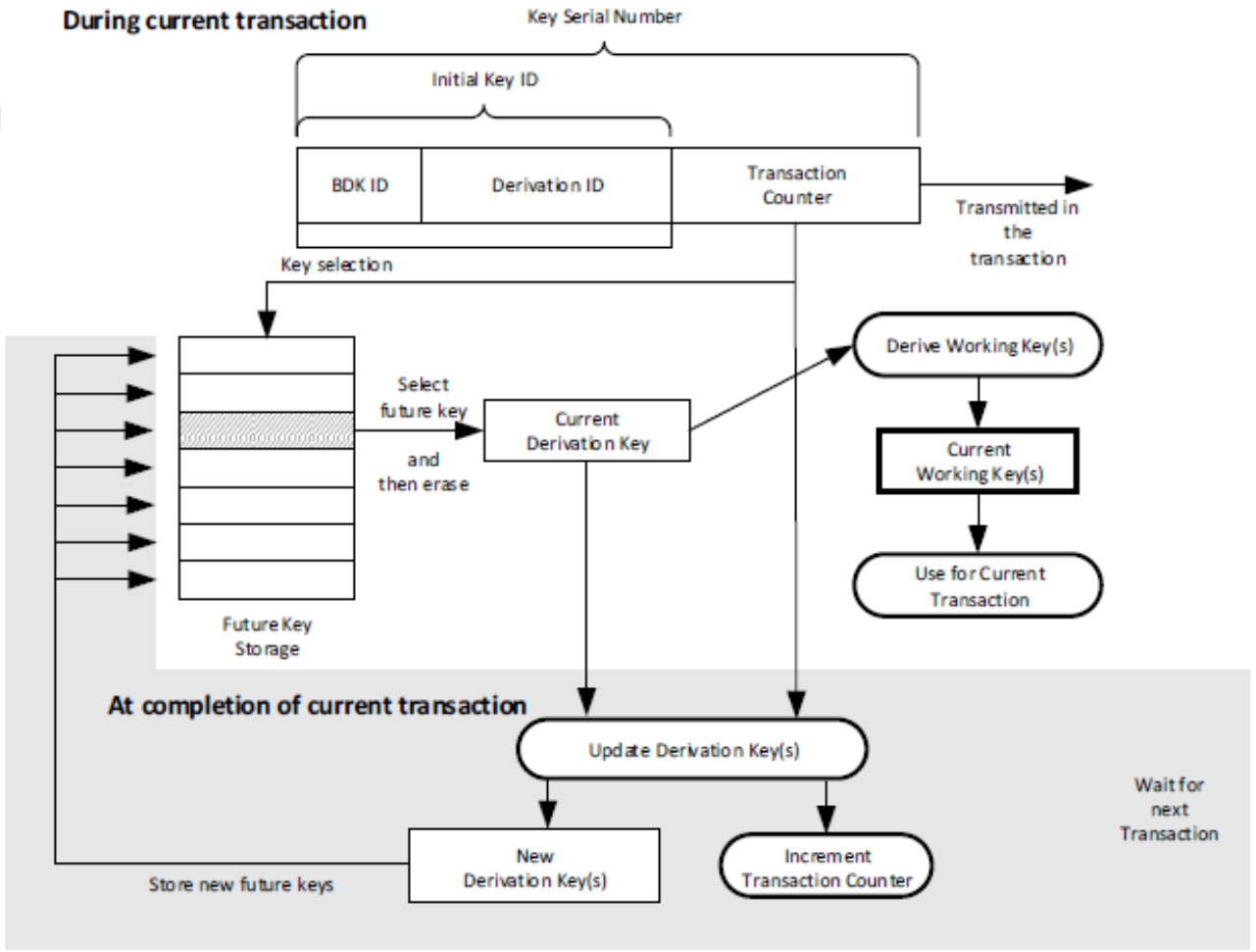
- Требуется обеспечить некорректируемость (целостность)
- Необходима симметричная криптография на датчике
- Необходима выгрузка юридически значимых записей телеметрии

Решение 2: DUKPT для управления симметричными ключами

- Ключи устройств порождаются из мастер-ключа по идентификатору устройства
- Начальный ключ устройства записывается при инициализации
- Из начального ключа последовательно вырабатываются следующие
- Уникальный ключ для каждой передачи вырабатывается из текущего ключевого состояния, которое после этого обновляется

Достигаемые свойства:

- Уменьшение нагрузки на ключ
- При компрометации одного ключа передачи остальные ключи не компрометируются
- При компрометации устройства предыдущие ключи не компрометируются



Источник: ANSI X9.24

Решение 3: хэш-код будущего ключа в сертификате

При инициализации устройства

- В устройстве создаются две ключевые пары – исходная и будущая
- Хэш-код «будущего» открытого ключа заносится в сертификат исходного (или хранится в центре)

Для смены ключа

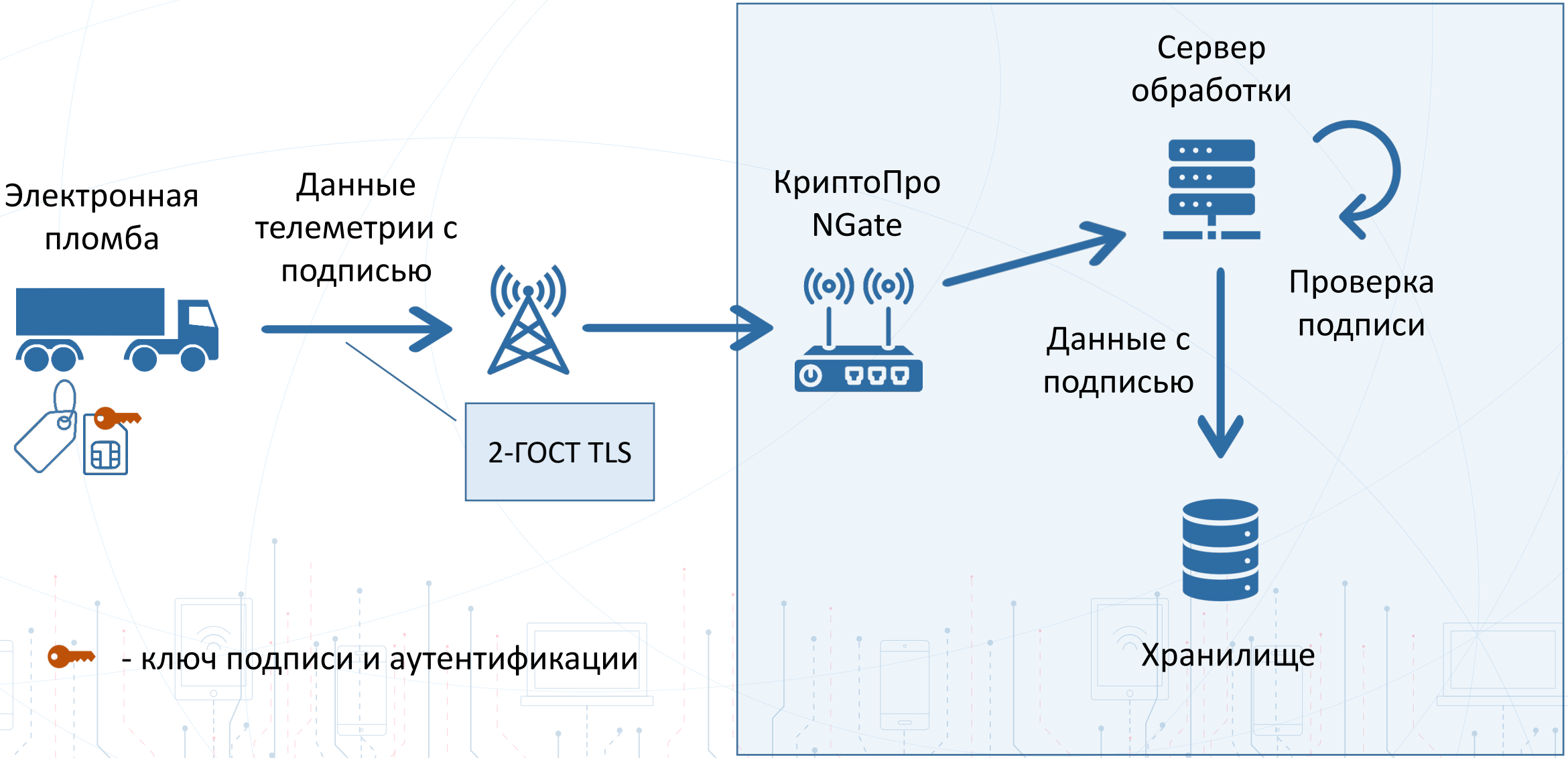
- Создаётся «будущая» ключевая пара
- Создаётся запрос на сертификат «следующего» ключа, в который помещается хэш-код «будущего» открытого ключа
- Запрос подписывается «текущим» ключом

Достигаемые свойства

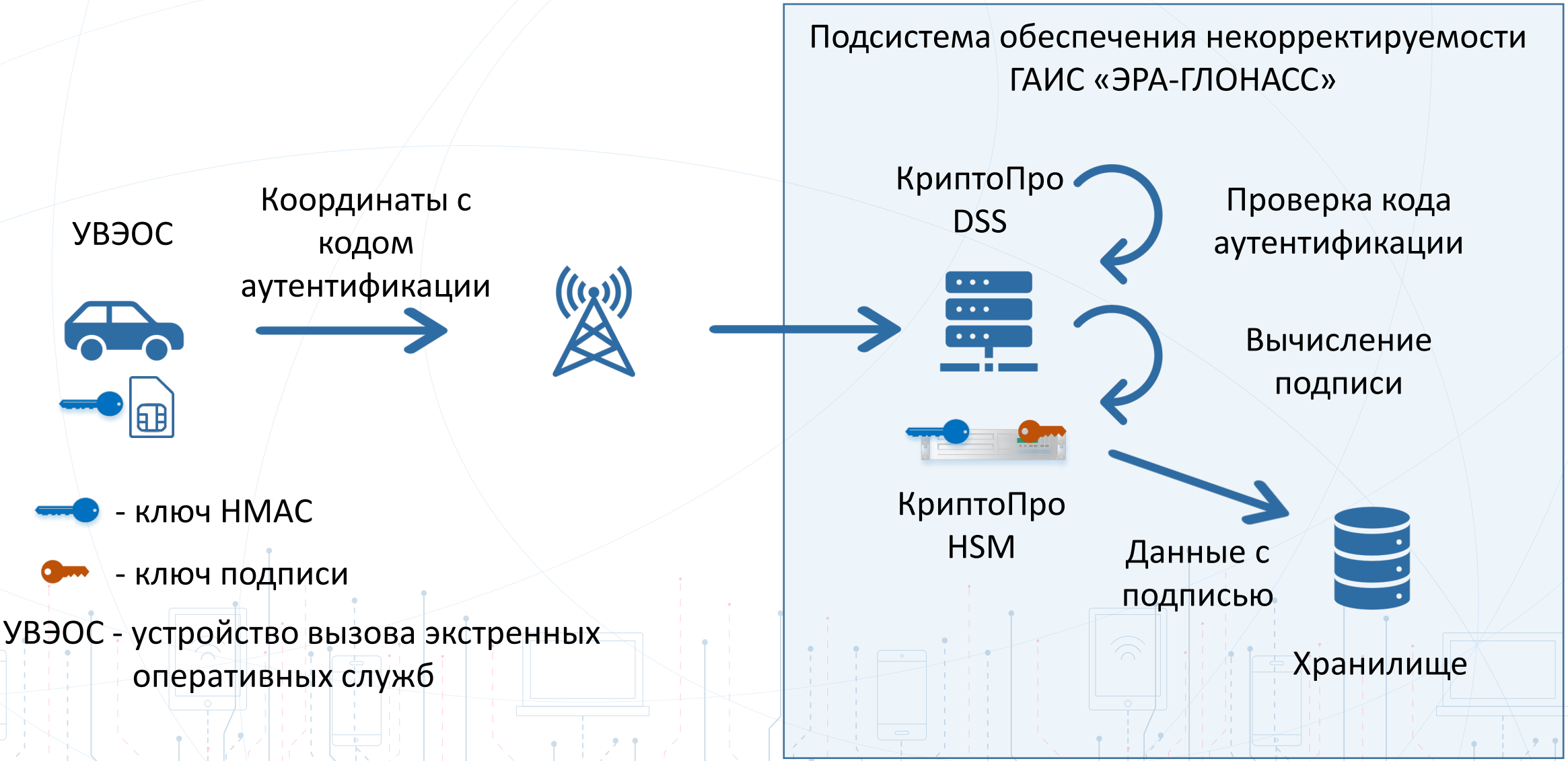
- При неявной компрометации текущего ключа следующие ключи не компрометируются

Источник: IETF RFC 8649

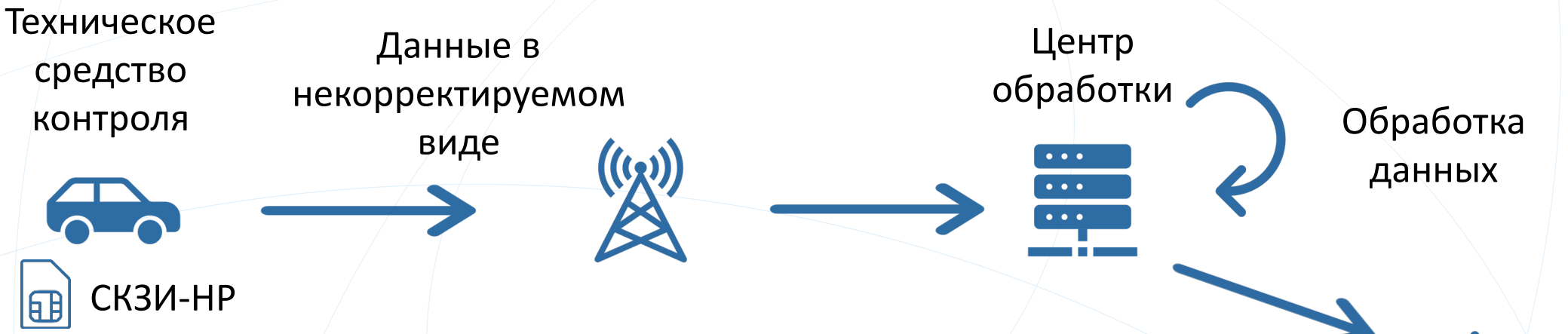
Пример: электронная пломба при перевозке груза



Пример: экстренный вызов с автомобиля



Пример: страховая телематика с автомобиля



- Требуется высокий уровень защищенности – КС3?
- Срок жизни без обслуживания более 10 лет
- Сертификация по требованиям к СКЗИ-НР

Возможные подходы:

- Симметричные ключи в СКЗИ-НР + DUKPT + распределенное формирование подписи
- Асимметричные ключи в СКЗИ-НР, автоматическая смена с использованием и проверкой хэш-кода будущего ключа

КРИПТОПРО

Ключевое слово
в защите информации

СПАСИБО ЗА ВНИМАНИЕ!

127018, г. Москва, ул. Сущевский Вал, д.18
Тел./факс: +7 (495) 995-48-20

https://cryptopro.ru

Общие вопросы: **info@cryptopro.ru**
Контрактный отдел: **kpo@cryptopro.ru**
Для дилеров: **dealer@cryptopro.ru**