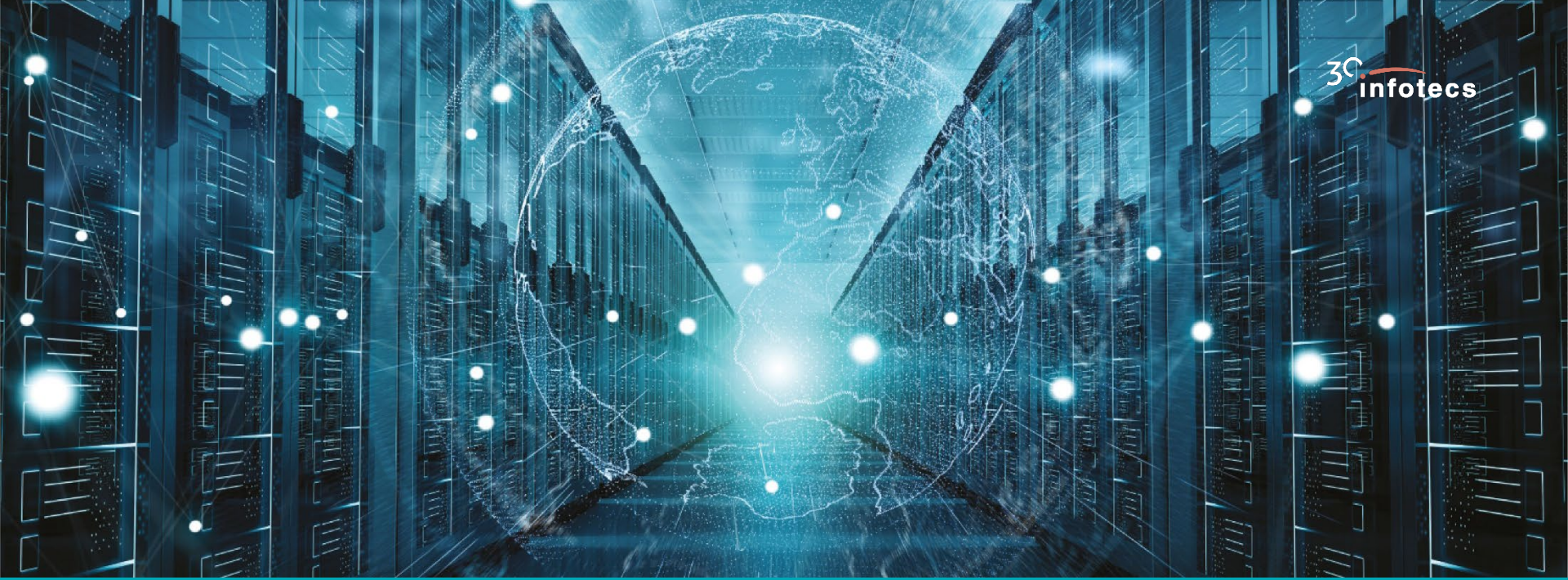
Различные форматы сертификатов ЭП Достоинства, недостатки и перспективы применения в IoT

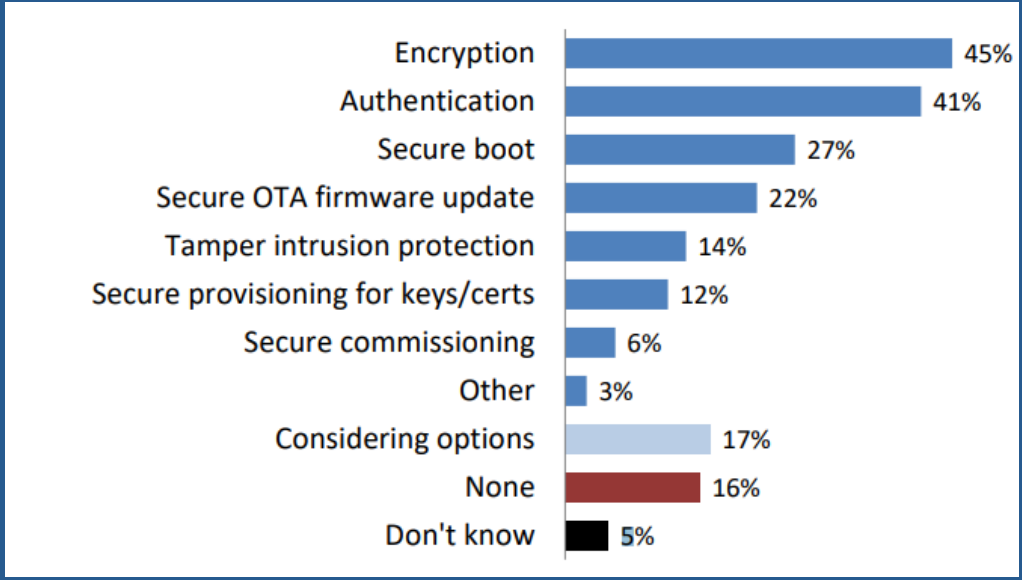
Шемякина Ольга
со-руководитель РГ «КМИС» ТК26
АО «ИнфоТеКС»



Специфика IoT/IIoT и M2M

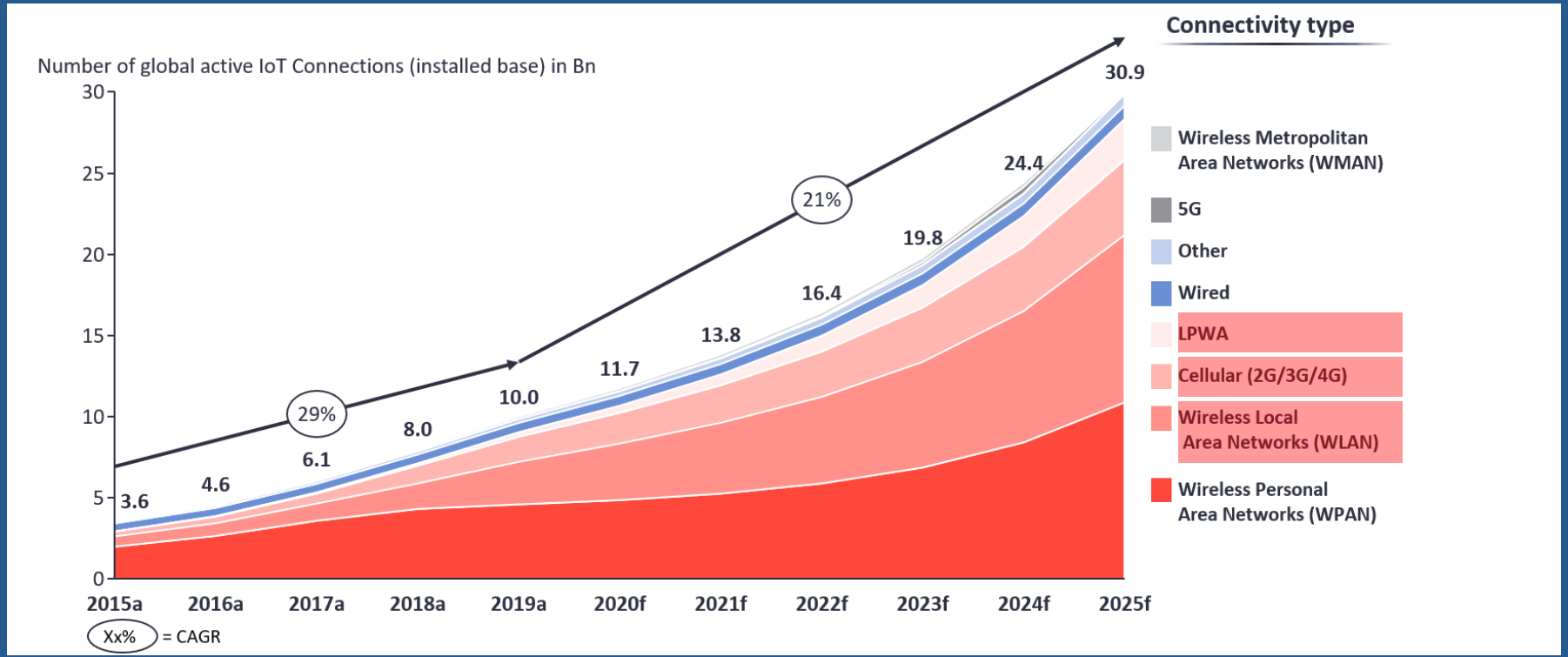
Сценарии защиты информации в IoT/IIoT-устройствах

Согласно исследованиям среди разработчиков встраиваемых систем



2019 Embedded Markets Study https://www.embedded.com/wp-content/uploads/2019/11/EETimes_Embedded_2019_Embedded_Markets_Study.pdf

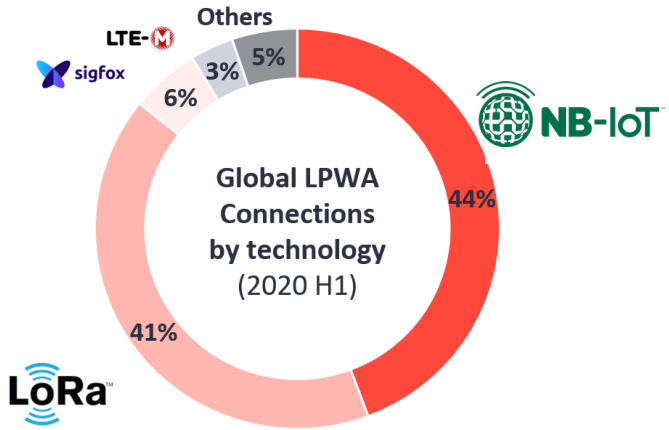
Протоколы и интерфейсы передачи данных в IoT/IIoT и M2M



SOURCE: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

Протоколы и интерфейсы передачи данных в IoT/IIoT и M2M - LPWA

Global 2020 (H1)



Russia 2020

SOURCE: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

Протоколы и интерфейсы передачи данных в IoT/IIoT и M2M

Стандарт	LoRa	UNB (Sigfox)	XNB (Стриж)	NB-Fi (WAVIoT)	NB-IoT
Частота	868 МГц	868 МГц	868 МГц	868 МГц	868 МГц
Дальность	10 км	10 км	10 км	16,6 км	15 км
Скорость передачи	0,3-50 Кбит/с	100 бит/с	100 бит/с	10-100 бит/с	200 Кбит/с
Срок работы от батареи	10 лет	10 лет	10 лет	10 лет	10 лет

Особенности протоколов

- Большое разнообразие протоколов
- Передача данных объемом в десятки-сотни байт
- Большая часть протоколов не основаны на TCP/IP
- Распространенность мультикаста и подписочной модели
- Часть протоколов чувствительны к задержкам
- «Традиционные» требования к конфиденциальности, целостности, аутентификации

Особенности каналов связи и устройств

- Разные каналы (физический, канальный, сетевой уровень)
- Каналы с низкой пропускной способностью
- Ненадежные каналы
- Малоресурсные устройства:
  - Мало памяти
  - Требуется низкое энергопотребление

Требования к криптографическим алгоритмам и протоколам

- Быстрые криптографические алгоритмы
- Алгоритмы с низким энергопотреблением
- Минимальный набор алгоритмов
- Количество добавляемых байтов должно быть небольшим
- Протоколы защиты данных должны быть независимы от протоколов транспортного и канального уровней

Зачем нужна «облегченная» PKI для M2M, IoT/IIoT?

PKI для M2M и IoT/IIoT

IoT/IIoT-системы:

- заранее неизвестные все участники системы
- постоянное изменение структуры и топологии сети

Мобильные АСУ и M2M:

- Перемещение между разной инфраструктурой

Хорошо подходят принципы PKI

PKI для M2M и IoT/IIoT

Преимущества:

- Простая инсталляция системы в целом
- Легко аутентифицировать устройства, пользователей, процессы
- Легкая масштабируемость

Недостатки «традиционной» PKI

- Большой размер сертификатов X.509:
  от 1 кб
- Большой размер добавляемых данных при подписи и шифровании (CMS):
  ≈ 300 байтов
- Большой набор криптографических примитивов для зашифрования данных
- Большой объем кода и ОЗУ для разбора форматов
- Большой объем CRL
- Сложность работы в инфраструктуре (распространение сертификатов, CRL, построение цепочек)

Плохо подходит для малоресурсных устройств

и каналов с низкой пропускной способностью

Известные в ТК 26 подходы

CV-сертификаты

CV = Card Verifiable

Особенности:

- Кодировка tag-length-value (TLV)
- Фиксированные поля

Общее упоминание:

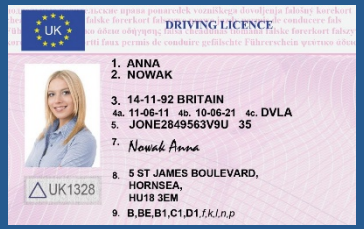
ГОСТ Р ИСО/МЭК 7816

Объект данных
CV сертификат
Тело сертификата
Идентификатор формата сертификата
Идентификатор сертификата центра, выдающего сертификат
Открытый ключ
Идентификатор сертификата владельца
Шаблон прав владельца сертификата
Дата начала действия сертификата
Дата окончания действия сертификата
Расширения
Цифровая подпись

Применение CV-сертификатов

Электронная идентификация граждан:

- Международная организация гражданской авиации (ИКАО). Doc 9303. Машиносчитываемые проездные документы
- BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token v2.21
- ISO/IEC 18013-3:2017 Information technology — Personal identification — ISO-compliant driving licence



Преимущества CV-сертификатов

- Размер существенно меньше, чем у X.509
- Разбирать проще, чем X.509
- Ведется деятельность по стандартизации в ТК 26 (с 2016):
  - Формат CV-сертификата
  - Алгоритмы взаимной аутентификации бесконтактных микросхем и взаимодействующих с ними терминалов
- Формат поддерживался (поддерживается?) в ViPNet CSP, КриптоПро CSP
- Есть открытые реализации: EJBCA, JMRTD

Недостатки CV-сертификатов

- Сценарии использования не соответствуют задачам M2M, IoT/IIoT
- Нет протоколов защищенного взаимодействия при использовании CV-сертификатов (кроме взаимодействия микросхемы карты и терминала с установлением соединения)
- Любое решение по защищенному взаимодействию будет проприетарным
- Стандартизация в РФ ведется долго
- Сертификаты издаются только РПЦ ИРКД (российский проверяющий центр инфраструктуры расширенного контроля доступа) в составе ГС МИР (Государственная система миграционного и регистрационного учёта)

Сертификаты платежных систем

Особенности:

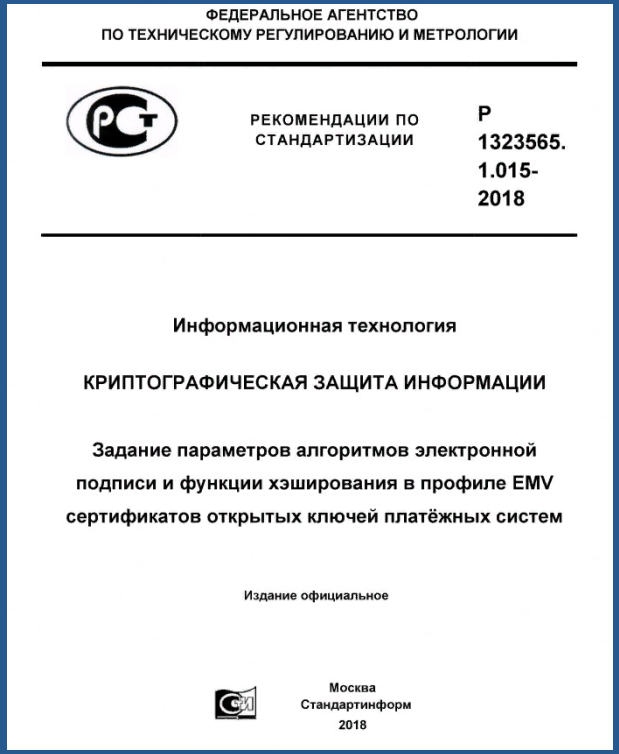
- Формат сертификатов полностью определен, не используется кодирование TLV
- Набор полей специфичен для целевого назначения
- Идентификаторы алгоритмов кодируются одним байтом

Разработаны EMV

Имя поля	Длина, байт
Header (заголовок)	1
Certificate Format (формат сертификата открытого ключа)	1
PAN	10
Certificate Expiration Date (дата истечения срока действия сертификата)	2
Certificate Serial Number (серийный номер сертификата)	3
Hash Algorithm Indicator (индикатор алгоритма вычисления хэш-функции)	1
ICC PIN Encryption Public Key Algorithm Indicator (индикатор алгоритма формирования/проверки электронной подписи карты для оффлайного шифрования PIN)	1
ICC PIN Encryption Public Key Parameters Indicator (индикатор параметров для алгоритма формирования/проверки электронной подписи карты для оффлайного шифрования PIN)	1
ICC PIN Encryption Public Key (открытый ключ карты для оффлайного шифрования PIN)	64
Signature (подпись)	64

Достоинства сертификатов платежных систем

- Компактный формат
- В РФ утверждены рекомендации по стандартизации:
  - Форматы сертификатов
  - Оффлайновая аутентификация платежного приложения



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.015-2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Задание параметров алгоритмов электронной подписи и функции хэширования в профиле EMV сертификатов открытых ключей платёжных систем

Издание официальное

Москва
Стандартинформ
2018

Недостатки сертификатов платежных систем

- Форматы и алгоритмы «заточены» под специфические для платежных систем сценарии
- Сценарии использования не соответствуют задачам M2M, IoT/IIoT
- Нет протоколов защищенного взаимодействия при использовании сертификатов (кроме оффлайновой аутентификации платежного приложения)
- Любое решение по защищенному взаимодействию будет проприетарным

Выводы

- В РФ в настоящий момент нет форматов сертификатов ЭП, подходящий для M2M, IoT/IIoT
- Сценарии использования стандартизованных решений не соответствуют задачам M2M, IoT/IIoT
- Нет протоколов защищенного взаимодействия при использовании сертификатов
(кроме оффлайновой аутентификации платежного приложения)

Есть ли границы применения PKI в M2M, IoT/IIoT

Нужны ли новые форматы и принципы взаимодействия

Нужны ли новые криптографические алгоритмы