

# Международная стандартизация ИКТ/IoT решений, используемых для борьбы с контрафактом

**Алексей Бородин**

Представитель ПАО Ростелеком в МСЭ в Женеве



# Изменения сети и услуг в эпоху Интернета Вещей

1. Чрезвычайно **большое число Интернет вещей** (до триллионов, предельное значение в соответствии с книгой *J.-B. Waldner “Nano-computers and swarm intelligence” - 50 триллионов*)
2. **Самоорганизующаяся архитектура** (вместо «тяжелой» инфраструктуры существующей сети)
3. **Сверхплотные гетерогенные сети** (включая мобильные и сенсорные сети, VANET, медицинские сети и т.д.)
4. Сети со **сверхмалыми задержками** (Тактильный Интернет, некоторые приложения медицинских сетей)

# Безопасность Интернета Вещей

1. Подмена MAC и IP адреса IoT-устройства занимает не более 1 мин → высокая вероятность клонирования IoT-устройств.
2. Повсеместное использования беспроводных технологий (WiFi, BLE, ZigBee, LoRa и др.) для подключения IoT-устройств – возросла вероятность перехвата данных «по воздуху» (например, атака «человек посередине»).
3. МСЭ–Т Х.1255 “Структура обнаружения информации по управлению определением идентичности” → разработка методов по борьбе с контрафактом продукции

# Борьба с контрафактом с использованием возможностей Интернет Вещей

Ключевые вопросы для стандартизации:

1. Безопасная и доверенная процедура идентификации Интернет Вещей с возможностью применения идентификаторов для различных отраслей промышленности (ИКТ, медицина, транспорт и т.д.)
2. Проверка подлинности идентификаторов IoT (тестирование идентификаторов IoT)
3. Системы доступа к профилям Интернет вещей по их идентификаторам

# Безопасная и доверенная процедура идентификации для IoT

В ИК20 начаты работы по новому направлению [Y.IoT-IoD-PT](#)  
*“Идентификация IoT устройств, основанных на защищенных механизмах, которые гарантируют конфиденциальность и доверие к используемым системам IoT” (январь 2016, май 2016)*

Содержание: методы и сценарии идентификации Интернет Вещей для простых Интернет Вещей на базе RFID, NFC, ПАВ и сложных Интернет Вещей на базе использования микроконтроллеров и микропроцессоров

# Тестирование идентификации Интернет Вещей

В ИК 11 начаты работы по новому направлению  
Q.39\_FW\_Test\_ID\_IoT

*“Структура тестирования систем идентификации  
используемых в Интернете Вещей” (декабрь 2015, июнь  
2016)*

Содержание: описание и сценарии тестирования процедур  
идентификации, используемых в ИВ в соответствии с  
подходом идентификации ИВ, специфицируемом в Y.IoT-  
IoD-PT

# Системы доступа к профилям Интернет вещей по их идентификаторам

В ИК20 начаты работы над проектом рекомендации [Y.IoT-DA-Counterfeit](#)

*“Information Management Digital Architecture to combat counterfeiting in IoT” (Август 2016)*

Содержание: ИКТ решения по сдерживанию распространения контрафактных IoT устройств на глобальном уровне. Рекомендация содержит описание систем, основанных на Цифровой Архитектуре (например DOA)

# Борьба с контрафактом с использованием IoT и DoA

Совместное использование систем IoT и DoA дает исключительные возможности для борьбы с контрафактом:

- Интерфейсы IoT имеют специфические особенности, которые сложно дублировать – это позволяет пользователю быть уверенным, что приобретённый продукт, оборудованный модулем IoT, является подлинным (не контрафактным)
- При использовании концепции Архитектуры цифровых объектов (Digital object Architecture – DoA) каждый продукт при использовании ИВ модуля может иметь уникальную идентификацию, которая покупателю ИКТ продукта будет привычна



## Y.IoT-DA-Counterfeit

### *“Information Management Digital Architecture to combat counterfeiting in IoT” (Август 2016)*

Рекомендация будет включать:

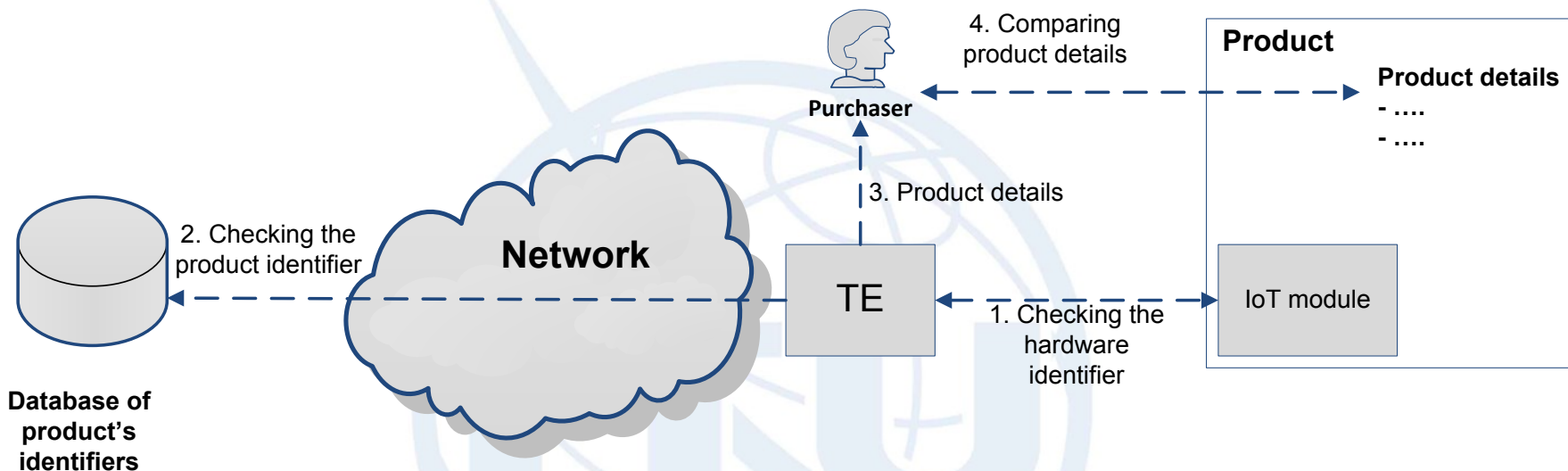
- описание системы (Digital Object Architecture – DOA - IoT) для борьбы с контрафактом
- взаимодействие с другими система «анти-контрафакта»
- принципы идентификации продукции
- описание универсальной системы идентификации
- процедура верификации идентификации продукции

Ссылки на текущие проекты рекомендаций:

[Y.IoT-IoD-PT](#) (идентификация, ИК20)

[Q.39 FW Test ID IoT](#) (тестирование, ИК11)

# Процедура верификации идентификаторов продуктов с использованием IoT и DoA (1/2)

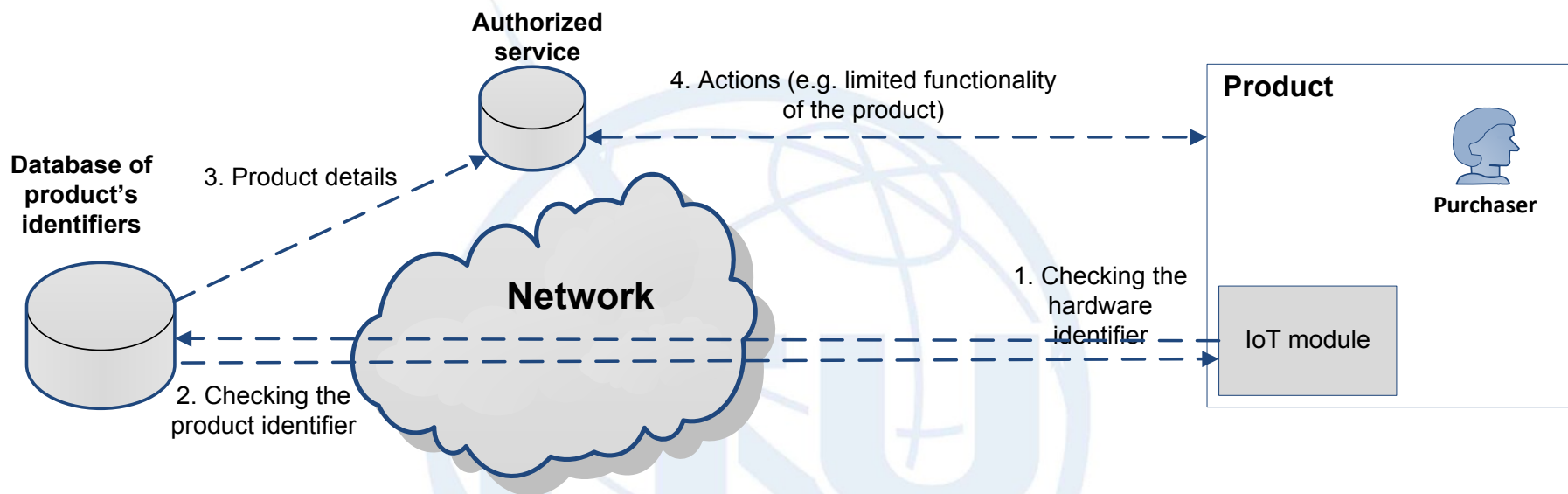


Покупатель может проверить идентификацию продукта, используя независимые технические решения, например, сканируя ВАР-код мобильным телефоном, получая код через RFID

Примечание: детальная информация доступна во вкладке [C297R1](#) (ИК 20)

(Source: Russian Federation , Jordan , Rostelecom , Saudi Arabia , SPbSUT , Sudan , Tunisia , UAE)

# Процедура верификации идентификаторов продуктов с использованием IoT и DoA (2/2)

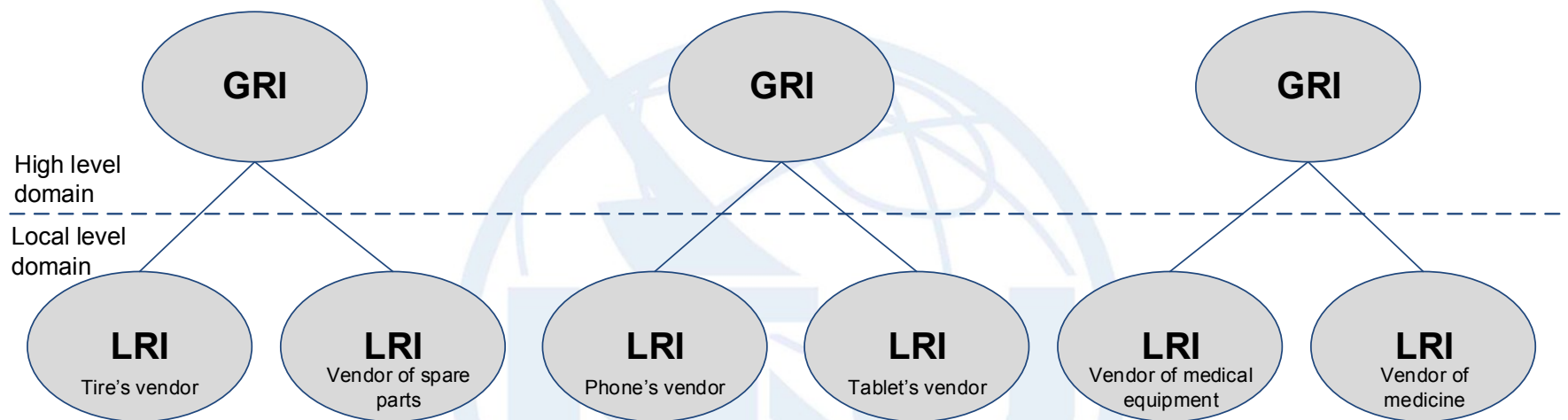


Покупатель может выбрать идентификацию продукта, используя возможности этого продукта (например, мобильный телефон, планшет, компьютер, мультимедийная система автомобиля и т.д.)

Примечание: детальная информация доступна во вкладке [C297R1](#) (ИК 20)

(Source: Russian Federation , Jordan , Rostelecom , Saudi Arabia , SPbSUT , Sudan , Tunisia , UAE)

# Глобальная система идентификации DoA/IoT



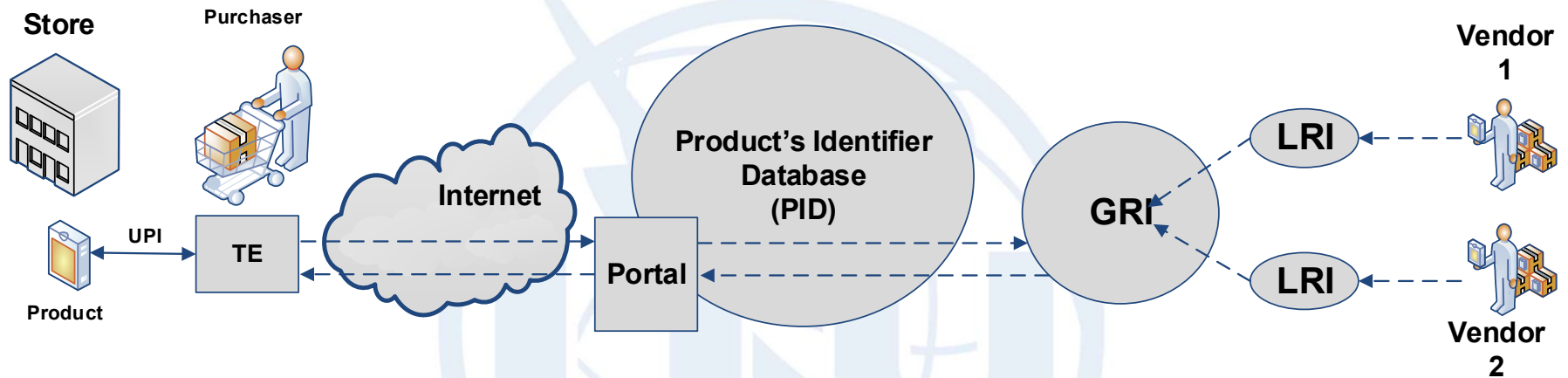
Глобальный регистр идентификаторов (GRI) расположен в странах или регионах

Локальный регистр идентификаторов (LRI) расположен у конкретных вендоров

Примечание: детальная информация доступна во вкладе [C297R1](#) (ИК 20)

(Source: Russian Federation , Jordan , Rostelecom , Saudi Arabia , SPbSUT , Sudan , Tunisia , UAE)

# Архитектура системы ИКТ идентификации, используемой для борьбы с контрафактом на базе DoA/IoT



Детальная архитектура была предложена Российской Федерацией, Иорданией, Ростелеком, Саудовской Аравией, СПбГУТ, Судан, Тунис, ОАЭ на собрание ИКТ20 в Августе 2016 года (Q.IoT-DOA\_counterfeit "IoT-DOA-based systems to be used for combating counterfeiting", [C297R1](#))

# ПРОЕКТ НОВОЙ РЕЗОЛЮЦИИ ВАСЭ-16 от Регионального Содружества в области связи (РСС)

**Исследования, касающиеся борьбы с  
контрафактом, в том числе и устройств  
электросвязи/информационно-  
коммуникационных технологий**

# Выводы

1. Эпоха Интернета Вещей ставит новые задачи в области борьбы с контрафактом
2. IoT/DoA является безопасным и универсальным решением для борьбы с контрафактом в различных отраслях (не только в ИКТ)
3. Процедура идентификации чрезвычайно важна для доверия пользователей. Необходимо разработать набор рекомендаций МСЭ-Т по верификации/тестированию процедур идентификации

# Алексей Бородин

Представитель ПАО Ростелеком в МСЭ в Женеве

E-mail: [alexey.borodin@rt.ru](mailto:alexey.borodin@rt.ru)