Combating counterfeit ICT devices: a demo using Digital Object Architecture

Alexander NTOKO, Chief, Operations & Planning Department, TSB

Q8/11- 22 April 2015 (Room K)

Agenda

- Framework for Presentation
- DOA Overview & DOA Applications in ITU
- Overview of anti-counterfeiting solution
- Features of anti-counterfeit solution

- Demonstration and detailed explanation

- Handle ID, Handle record and Digital fingerprint generation
- Supply chain traceability
- ICT device authentication process
- Handle ID ICT device metadata

Framework for Presentation

- *Combating counterfeit telecommunication/information and communication technology devices* (Resolution 188)adopted by ITU Member States at the ITU Plenipotentiary Conference 2014 (PP-14) in Busan, Korea

… "*recognizing*

- *e) that Recommendation ITU-T X.1255, which is based on the digital object architecture, provides a framework for discovery of identity management information;" …*

- *"resolves to instruct the Directors of the **three Bureaux***
  1. *to assist Member States in addressing their concerns with respect to counterfeit telecommunication/ICT devices, through **information sharing** at regional or global level, including conformity assessment systems;*
  2. *to assist all the membership, **considering relevant ITU-T recommendations**, in **taking the necessary actions** to prevent or detect the tampering with and/or duplication of unique device identifiers, interacting with other* telecommunication standards-development organizations related to these matters,"

DOA - Overview

A digital object comprises of a Unique persistent identifier associated with a structured record or state information (e.g., meta-data)

"Imagine a large document or blog post with a lot of embedded URLs. After a certain amount of time those URLs will most likely become non-operational. If you replace those URLs with unique persistent digital object identifiers then, if properly administered, the links will never be lost – because the identifier is now associated with a digital object rather than a port on a machine." - **Robert E. Kahn**

Global presence

- Over 1,000 services built on DOA, in 75 countries, on 6 continents
- Today top-level DOA global root servers receive avg. 200 million resolution requests per month
- More than 16,000 assigned namespaces ("prefix")

Applications and uses in diverse domains

- Libraries and Archives
- Intellectual Property
- Distance Learning & Academic Research
- Big Data, IoT, RFID, Cloud Computing
- Entertainment Industry
- Anti-Counterfeit, Supply Chain etc.

Some Key Features

- Open architecture, Open source and cost effective to implement and use.
- **Enhanced security** based on built-in PKI with digital signature for authentication, data integrity and non-repudiation of transactions and information management.
- Powerful and sophisticated (e.g., recursive, dynamic state info) built-in **resolution system**
- **Secure record update and access** – record can be administered or seen only by the owner
- **Distributed autonomous technical management**
- **Globally interoperable** – uses Unicode 3.0 character set and UTF-8 encoding for name space. Accommodate various identifiers in all languages and scripts. Works seamlessly with existing IP-based infrastructure and applications

DOA – ITU activities and initiatives

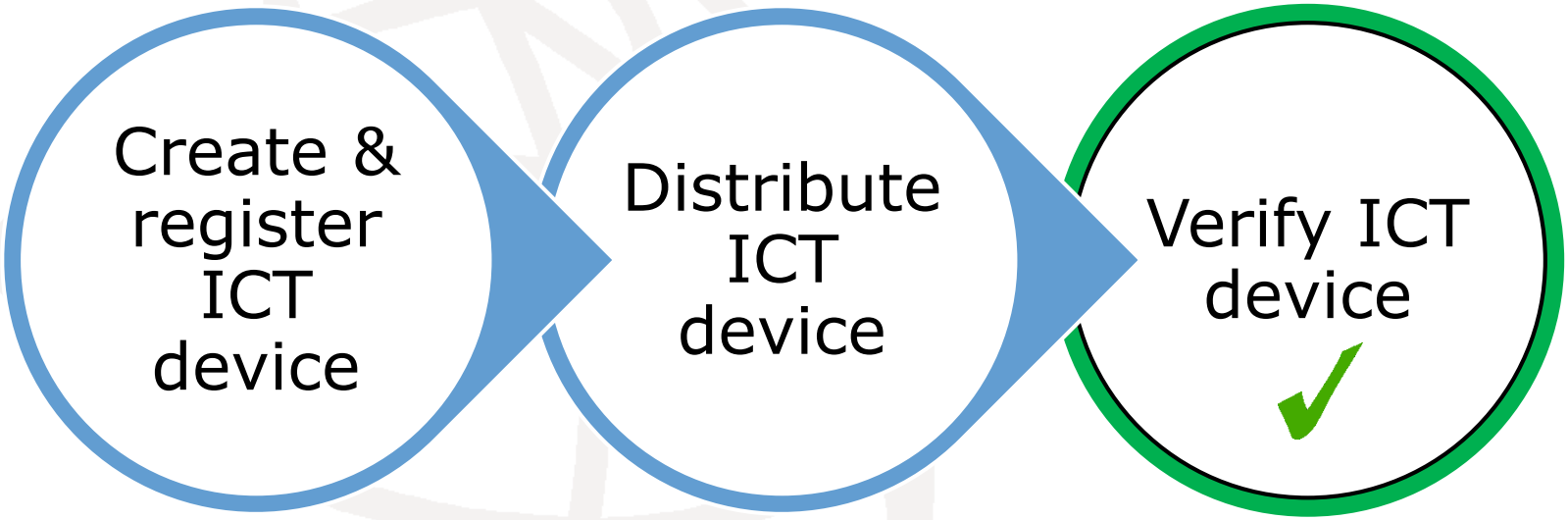
DOA supporting ITU Products and Services

- **ITU-T Recs in** 6 languages and various format, **+84 000** digital objects
- **Patent statements database, +2 000** digital objects
- **ITU-T active working groups**
- **ITU Library** persistent identifiers for digital docs and ITU History Portal web pages
- **ITU Publications on DVD** with DOA permanent links for enhanced client experience
- **ITU-T SGs permanent links** for liaison statements, work programme, meeting results

Ongoing DOA initiatives to address global challenges

- **Combatting proliferation of counterfeit** devices
- **Food Security** & **traceability**
- **Reconciling E-Waste** and **IoT** through DOA
- Advanced information management **s**olutions for **UN System** in the publication domain

Overview of anti-counterfeiting solution



- Manufacturer generates a Handle ID for each manufactured ICT device
- Digital fingerprint generated and assigned per ICT device

- Shipping information is added from the time the device leaves the manufacturer's plant to warehouse to distributor to retailer

- During purchase, customer retrieves the data about the device
- The customer compares the information and is able to confirm the authenticity of the device

Features of the anti-counterfeit solution

Customer verification interfaces

- Web interface
- QR code, barcode
- RFID
- IoT unit
- SMS
- Call centre
- etc.

3 distinct but combined authentication methods

1. Verification code
   - Digital fingerprint of the device generated from the properties of the device.
   - Identification mechanism of particular IoT unit

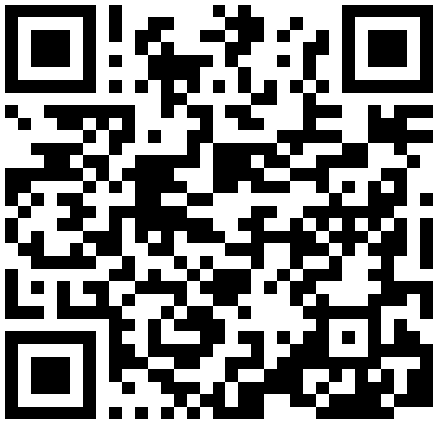
2. Unique identifiers of the device
   - IMEI number (GSMA)
   - MAC address (IEEE)
   - Product Code (GS1)
   - Serial Number (Manufacturer)

3. Supply chain traceability
   - Complete path that the device has taken from the manufacturer's plant to the retailer's store.

Demonstration

Customer verification interface

- QR code per ICT device
- QR code is visible on the ICT device's packaging



3 distinct authentication methods combined

1. Verification code
   - Digital fingerprint

   9H5N-IWQ6-BFOK-4W48-8WSG-0GC8-8

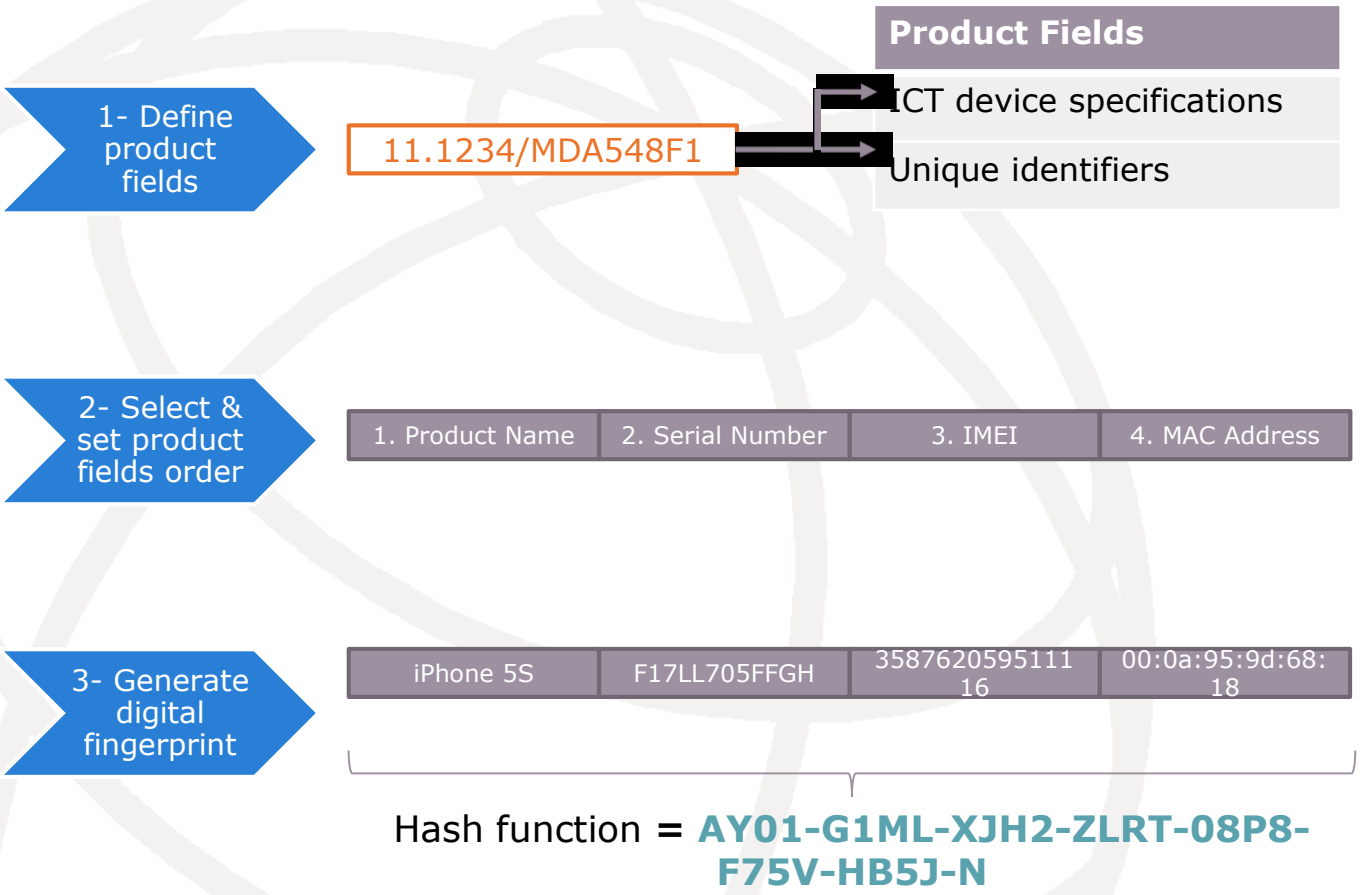
2. Unique device identifiers
   - IMEI number : **863846020122778**
   - MAC address : n/a
   - Product Code : **6 91443 004256**
   - Serial Number : **Y3Z7N143060000785**

3. Supply chain traceability
   - Complete path taken by ICT device from manufacturer's plant to retailer's store

Demonstration

This demonstration focuses on smartphones and tablets but the solution is designed to work for a wide range of ICT devices including IoT devices

Handle ID, Handle record and Digital fingerprint generation



Manufacturer

Bulk registration of ICT devices

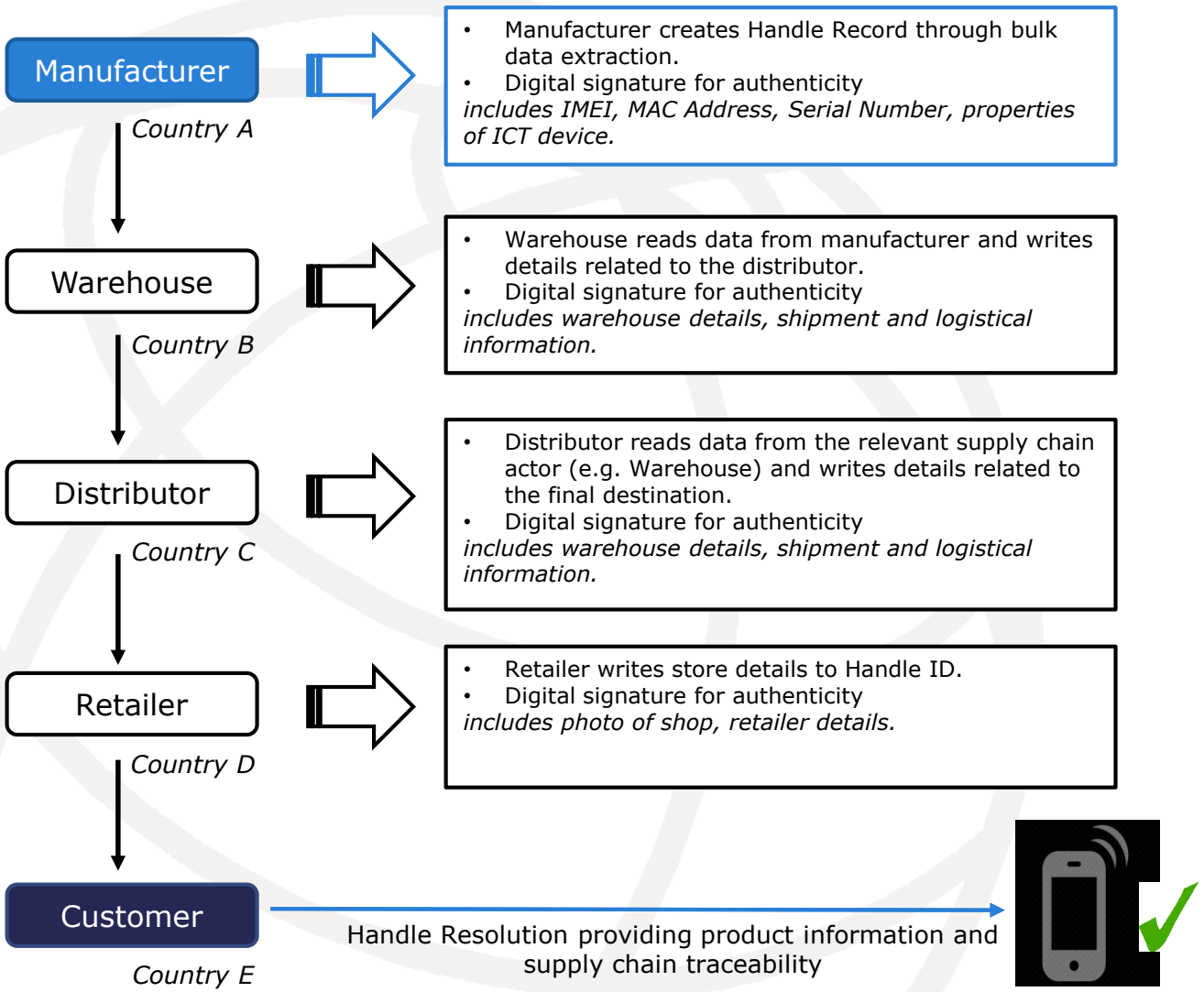
Define for each product line:

- Product field values to be taken into account in Digital fingerprint generation
- Product fields order

Generate for each device:

- Handle ID
- Digital fingerprint

Supply chain traceability

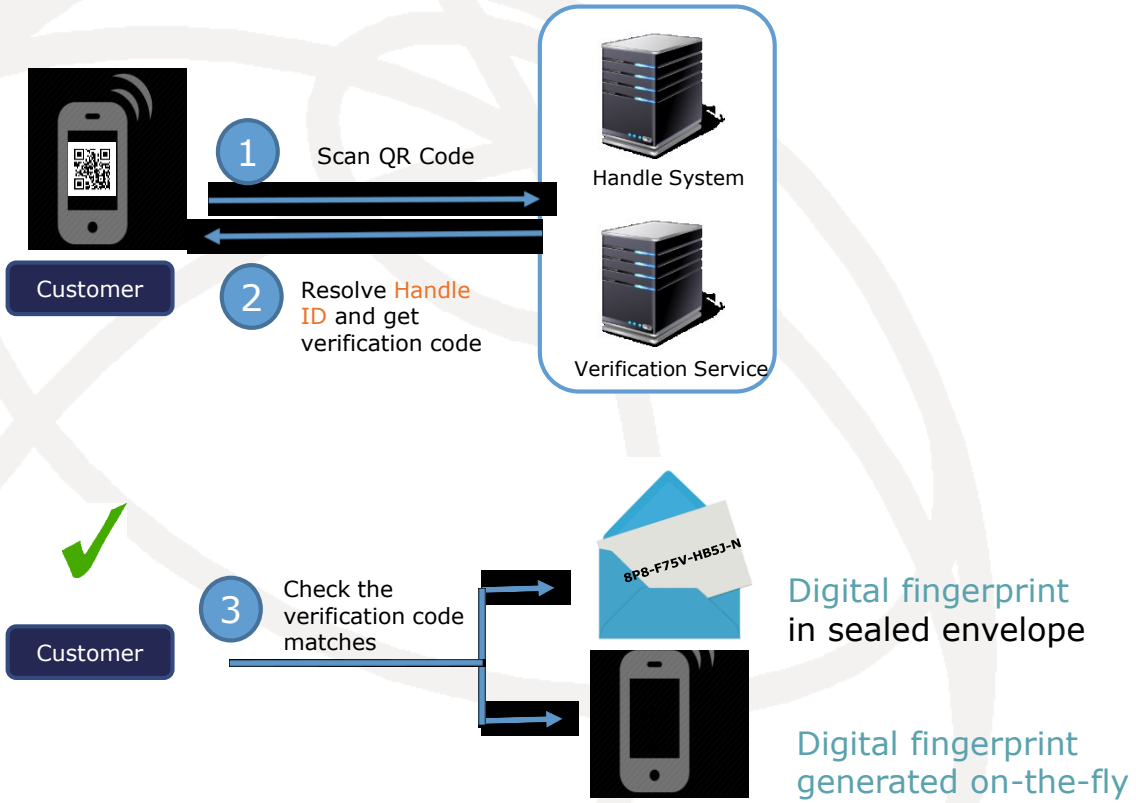


Supply chain actors

Update tracking information of the Handle ID when the product leaves the plant until it reaches the retailer's store

Built-in PKI uses digital signature for data integrity, authentication and non-repudiation

ICT device authentication process



For security reasons, the digital fingerprint is not stored on any servers.

Customer

Scans a code, or sends an SMS, or enters a code on a web interface to retrieve information about device.

Customer compares the information in the following order:

1. Digital fingerprint
2. Unique identifiers of the ICT device: IMEI, MAC address, Serial Number and Product Code
3. ICT device tracking information: retail store where this ICT device is supposed to be sold

Handle ID device metadata

Device specifications	
Brand:	Apple
Model:	IPad 2 A MC916FD/A
Manufacture Date:	01/04/2014
Color:	black
IMEI:	No information
Serial Number:	DN6GQ8LBDFJ0
Product Code:	8 85909 46497 5
MAC Address:	70:DE:E2:96:68:77
Processor:	Dual-core 1 GHz Cortex-A9
RAM:	512 MB
Other Specifications:	Wi-Fi 802.11 a/b/g/n, dual-band
Internal Storage:	64 GB
Operating System:	iOS 4, upgradable to iOS 8.3
Retail Price:	330 EUR
Message:	OS upgradable to iOS 8.3. Device available. Released 2014, April

Verification	
Handle ID:	11.1234/MDUBPCGK81 ✔
Verification Code:	401Y-P2LG-E9OG-SG00-84O8-8KO8
	Validate Verification Code

Regulators

Access to ICT devices "whitelist" based on sub-set of full device metadata and enhanced security for product ID using the verification process

Thank You

For further information:
alexander.ntoko@itu.int