Responsibilities and Certification in Cybersecurity space

Claire Loiseaux, Internet of Trust President

Inspire 5G+ Workshop, June 16th, 2021

Introduction

Created in 2014, Internet of Trust is a consulting company specialized in the security of embedded systems gathering people with over 10 and 20 years experience in certification schemes. Working regularly with **GloblalPlatform, Eurosmart, ANSSI and ENISA.** More partners and customers on www.internetoftrust.com.

Solid track record in security certification

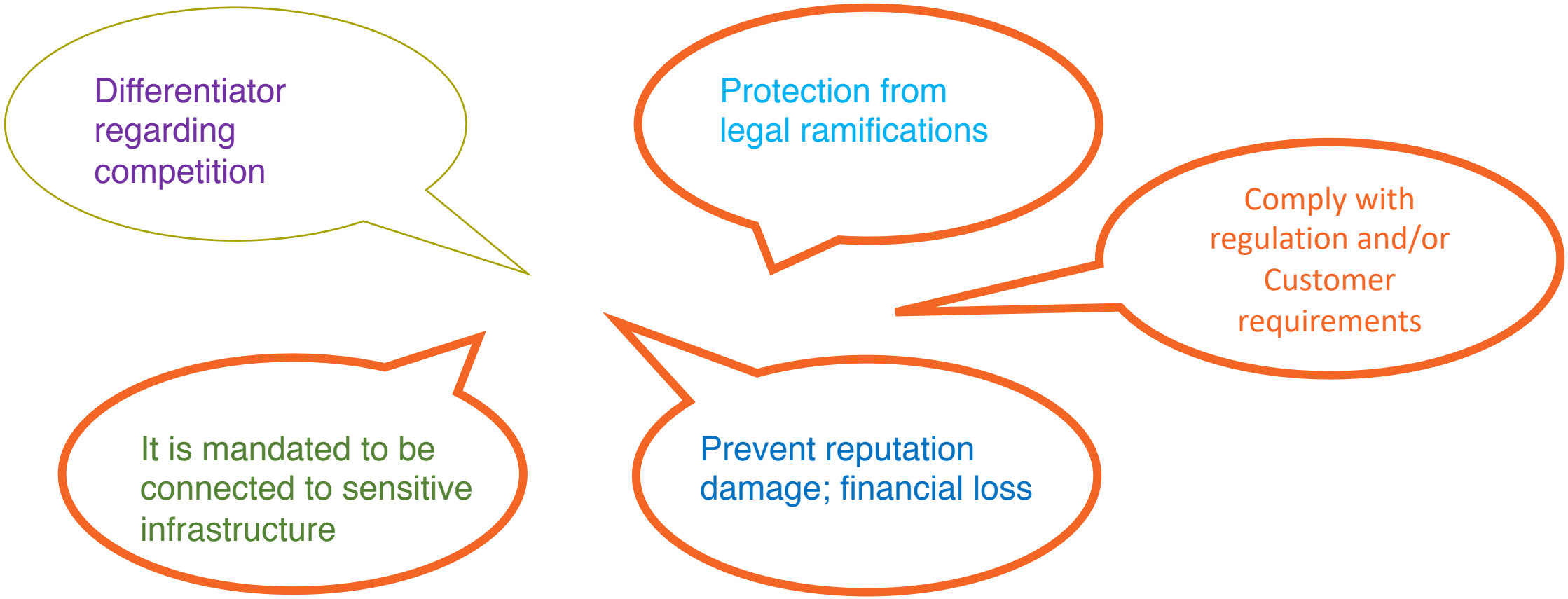
- **Security analysis** and **definition of security requirements** for 5G infrastructure, automotive and Industry 4.0 verticals including technical aspects but also Applicable standards, Regulation and evaluation schemes.
- **Scheme definition**: Common Criteria methodology and evolutions (v4) ; Edition of more than 25 Protection Profiles; Security requirements for 5G network, DRM ; Lego methodology approach designated for IoT system.
- **Training and support to prepare evaluation evidences** and follow certification in CSPN and Common Criteria framework (up to EAL7): Smart Card, Digital ID solution and Banking products**,** HSM, Mobile applications
- **Coordination of certification stakeholders**: CB (ANSSI, other European CB), Labs, product manufacturer/service providers, stakeholders, industrial associations, risk owners.
- **Operation of the security certification scheme** for the TEE and the SE for GlobalPlatform

Content

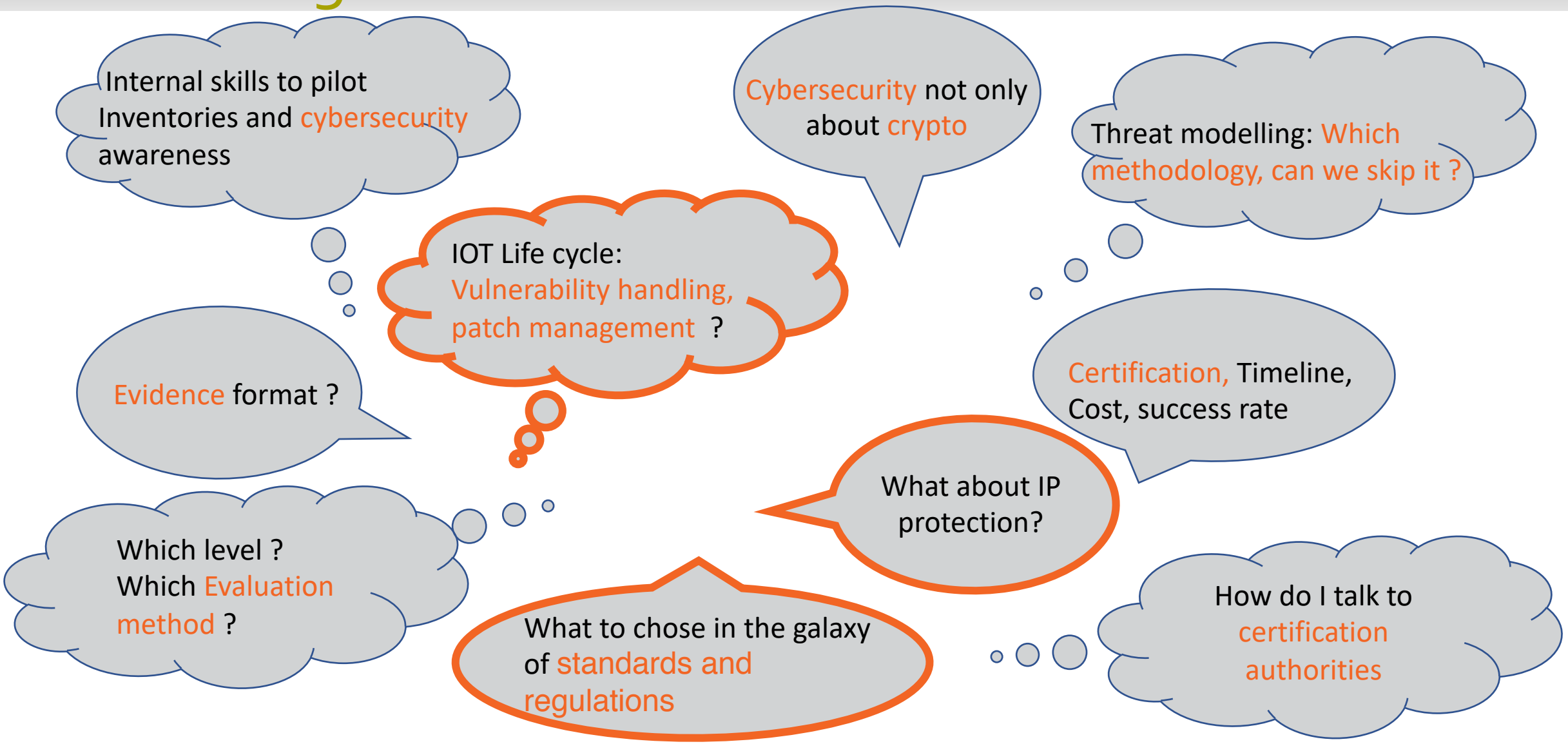
- Certification and liability aspects
  - Product
  - System

- Cybersecurity management, an interdisciplinary topic
  - Awareness
  - Common language
  - Improvement practical path ?

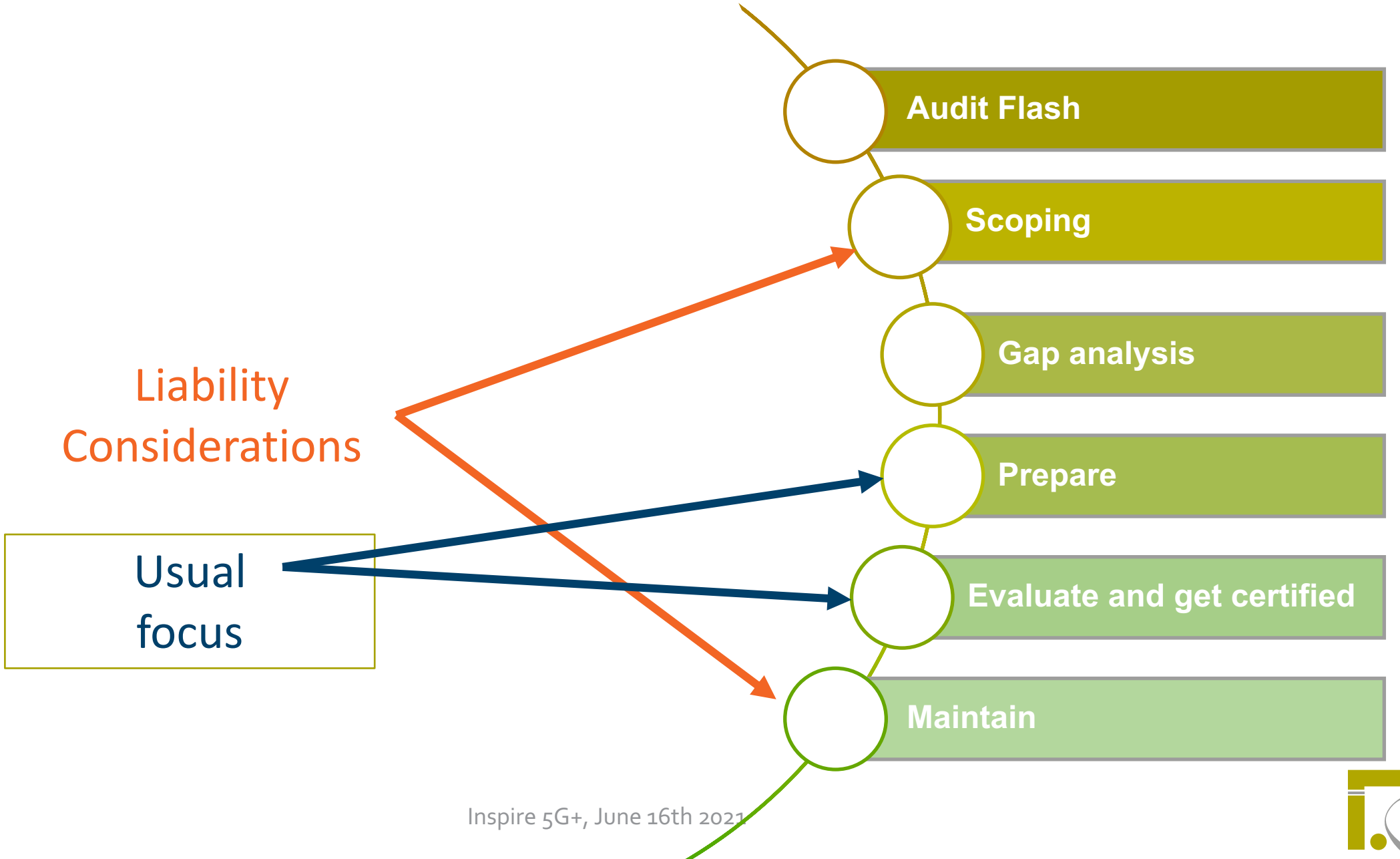
Among motivations for security « certification »



Challenges


Internal skills to pilot Inventories and cybersecurity awareness
Cybersecurity not only about crypto
Threat modelling: Which methodology, can we skip it ?
IOT Life cycle: Vulnerability handling, patch management ?
Evidence format ?
Certification, Timeline, Cost, success rate
What about IP protection?
Which level ? Which Evaluation method ?
What to chose in the galaxy of standards and regulations
How do I talk to certification authorities

Product certification compliance journey



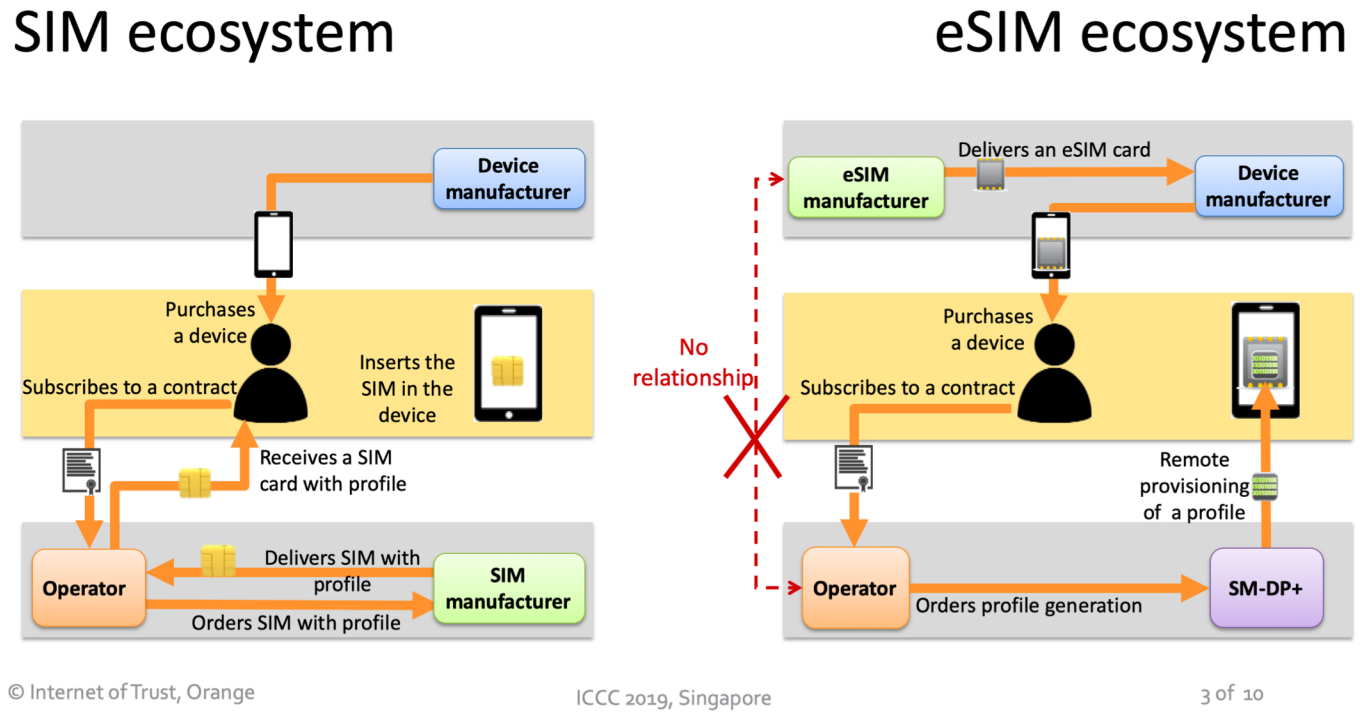
Scoping & Maintain

- Scoping (crucial to determine commitment and anticipate legal resolution)
  - Purpose and expected usage
  - Perform a risk analysis and validate it with the customer
  - Applicable security requirements
  - Applicable regulation
  - Check about applicable attack categories and level
  - Determine role and responsibility of each contractor
  - Determine evaluation scheme and level

- Maintain (mandatory under CSA certification schemes)
  - Vulnerability handling
    - Follow state of the art attacks
    - Perform impact analysis
  - Develop remediations
  - Inform about security issues and the remediations – Customers, integrators, suppliers
  - Timely remediate

Scoping: Example of responsibility transfer

eSIM & SIM ecosystem differences

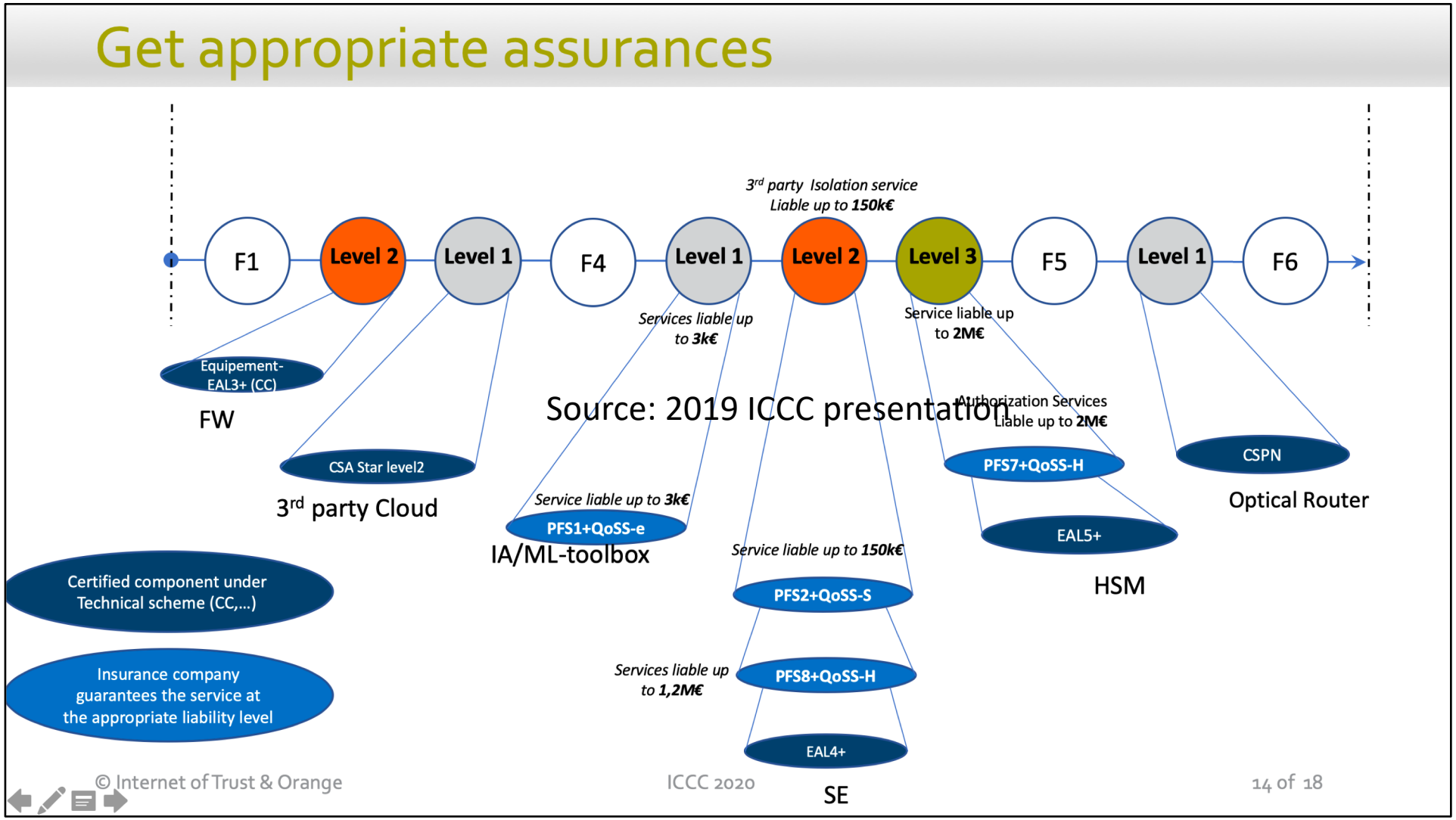


Source: 2019 ICCC presentation

Trust based on

- Operator – Sim Card Manufacturer
- One to one contracts
- eSim Certification available to any devices manufacturer and operators
- One to many contracts

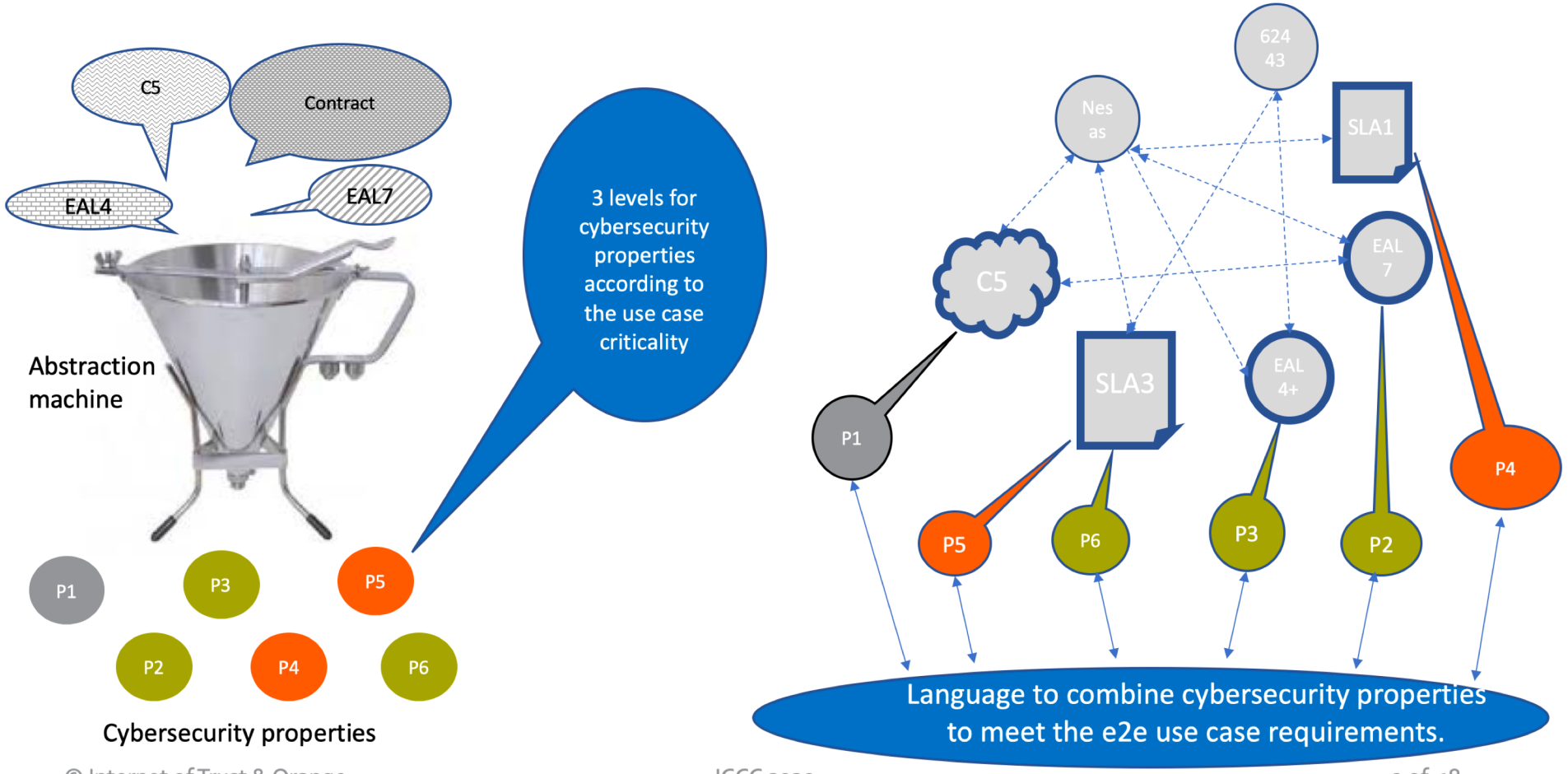
End to end – trust model



Source: 2020 ICCC presentation

Challenge

We have a dream …



ICCC 2020

9 of 18

Source: 2020 ICCC presentation

Questions to address

- Who is responsible for addressing
  - Financial loss, IP loss, Privacy breach, ransoms…
  - Safety issues
  - Paying for developing, certifying, deploy technical updates
  - Cybersecurity governance
  - Communication with involved actors

- What can we expect from
  - Design – security by design and secure update
  - Certification – Security status (up to the state of the art) at some point in time backed by recognised Certification Bodies
  - Responsibilities defined in Regulations – (Inter)national, Sectorial,…
  - Insurance – Scope and measurement methods – Prevention and Indemnification
  - Contractualisation -- Responsibility distribution in Supplier/customer Responsibility matrix ; SLA; penalties; …

INTERNET OF TRUST

Thank You!

Questions?