# Progress on Security Certification – Implementation of EU Cybersecurity Act

Jean-Pierre Quémard

DG KAT/ Alliance pour la confiance numérique

Convenor JTC1/SC27 MAG, Convenor JTC13,
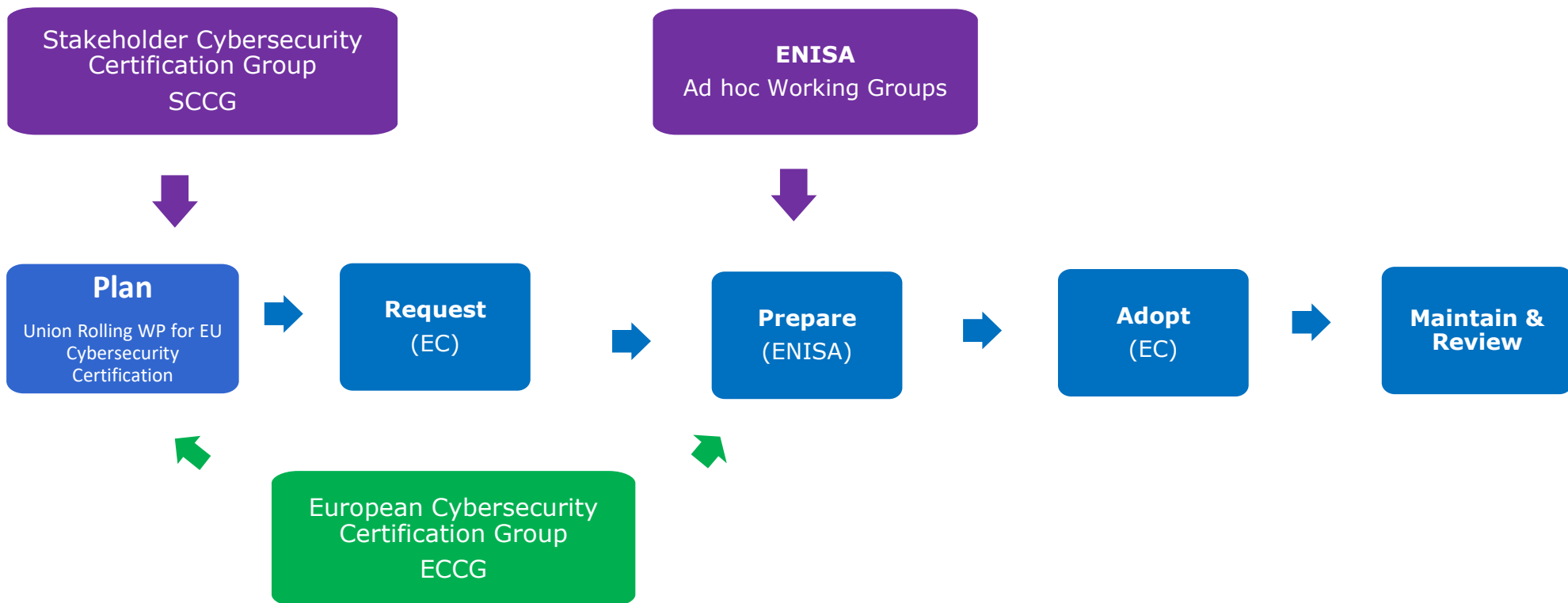
Vice Chairman ETSI TC Cybersecurity

# Agenda

- Cybersecurity Act

- Security Certification status

- Challenges for PSCE

- Rôle of standardisation

- Conclusion

# Cyber act (1)

- **One Framework**, many schemes – requirements and assessment methods tailored to the types of ICT products, services, or processes and taking into account cybersecurity risk.

- Open, inclusive and **transparent** governance processes.

- Reinforces **harmonised EU-wide** approach and building trust with peer reviews.
    - Taking into account the dynamic nature of modern software and hardware development throughout a product's lifecycle: certification processes such as secure development, vulnerability handling and disclosure, provision of updates
    - Providing additional value for users: guidance on secure configuration and use, documenting patched vulnerabilities and mitigation measures, security contact points for security researchers;

# The lifecycle of an European Cybersecurity Certification Scheme

KAT

**Stakeholder Cybersecurity Certification Group**
SCCG

**ENISA**
Ad hoc Working Groups

**Plan**
Union Rolling WP for EU Cybersecurity Certification

**Request**
(EC)

**Prepare**
(ENISA)

**Adopt**
(EC)

**Maintain & Review**

European Cybersecurity Certification Group
ECCG

# Cyber act (2) the status

➢ Entry into force June 2019

➢ European Commission first request to ENISA to prepare CC base scheme based on SOG-IS agreement ; Cloud, 5G, IOT, IACS, IOT will follow

➢ ECCG has been established; two meetings have been taken place;

➢ SCCG call for applications closed on 17 September; selection process on-going with DG CNCT;

➢ Preparation of the URWP (Union Rolling work plan) for European Cybersecurity Certification

# European Cybersecurity certification Scheme
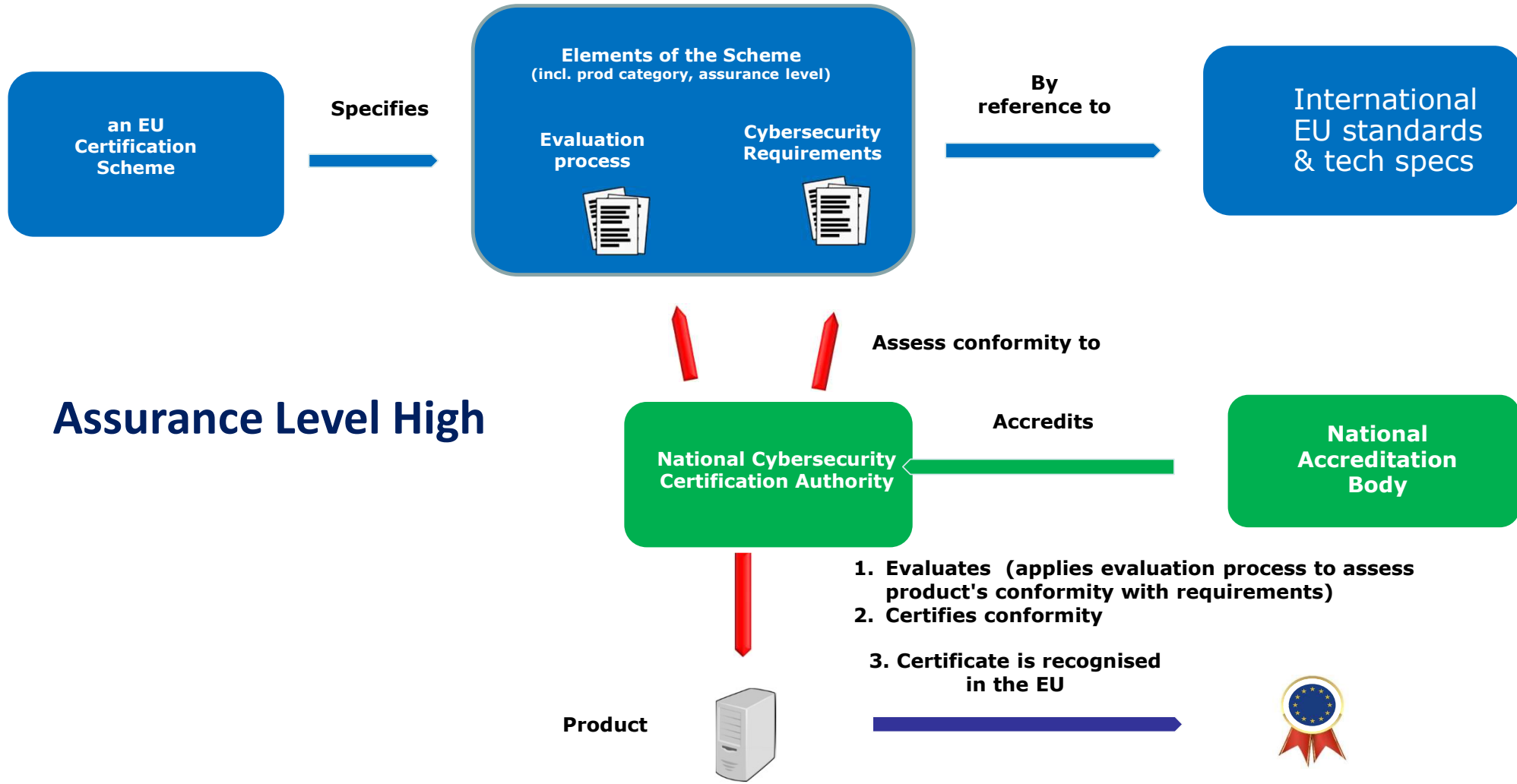
# Challenges for PSCE/Broadway

- Broadway will be in the scope of cyberact :

- For4G/5G threat management potential candidate for EUWP
  - See EU coordinated risk assessment of the cybersecurity of 5G networks Report  dated 9 October 2019

- For PPDR specificities :
  - E2E encryption (only AIE and LI are covered in 3GPP standards)
  - Key management and crypto algorithms
  - Direct Mode (Proximity services)
  - Group calls,
  - ……

# EU coordinated risk assessment of the cybersecurity of 5G networks
# Report dated 9 October 2019

- **Core network functions**                                                                      **CRITICAL**
  - User Equipment Authentication, roaming and Session Management Functions
  - User Equipment data transport functions
  - Access policy management
  - Registration and authorization of network services
  - Storage of end-user and network data
  - Link with third-party mobile networks
  - Exposure of core network functions to external applications
  - Attribution of end-user devices to network slices
- **NFV management and network orchestration (MANO)**                                **CRITICAL**
- **Management systems and supporting services (other than MANO)**       **MODERATE/HIGH**
  - Security management systems
  - Billing and other support systems such as network performance
- **Radio Access network**                                                                          **HIGH**
  - Base stations
- **Transport and transmission functions**                                              **MODERATE/HIGH**
  - Low-level network equipment (routers, switches, etc)
  - Filtering equipment (firewalls, IPS...)
- **Internetwork exchanges**                                                                **MODERATE/HIGH**
  - IP networks external to MNO premises
  - Network services provided by third parties

# Role of standardisation, the stakeholders in security evaluation and certification

- ISO/IEC JTC1 SC27 IT Security Techniques
  - 150+ Standards
  - ISMS, CC, Crypto, Privacy, Certification, biometry

- IEC TC 65 (Industrial-Process Measurement, Control & Automation)
  - IEC 62443: Industrial Automation and Control Systems Security

- CEN CENELEC JTC13
  - Transposition of ISO/IEC standards
  - Lightweight certification
  - IOT security evaluation

- ETSI TC Cyber
  - Cybersecurity for IOT
  - QSC, Middle box sceurity Critical security controls, ISI

**International SDO's**

**European SDO's**

# Role of standardisation

- In support to Cyber act
- Will guarantee :
  - Repetitability
  - Interoperability
  - Consistency at European level
  - Harmonisation of evaluation scheme
- Standards will part of the certification schemes :
  - Requirements
  - Evaluation methods
  - Evaluation of processes, companies  and people

# Conclusion

- Cyber act will have impact on Broadway

- Standardisation is a key factor of success

- Strong Need for a security evaluation Framework for PPDR networks

# Thank you
Questions ?