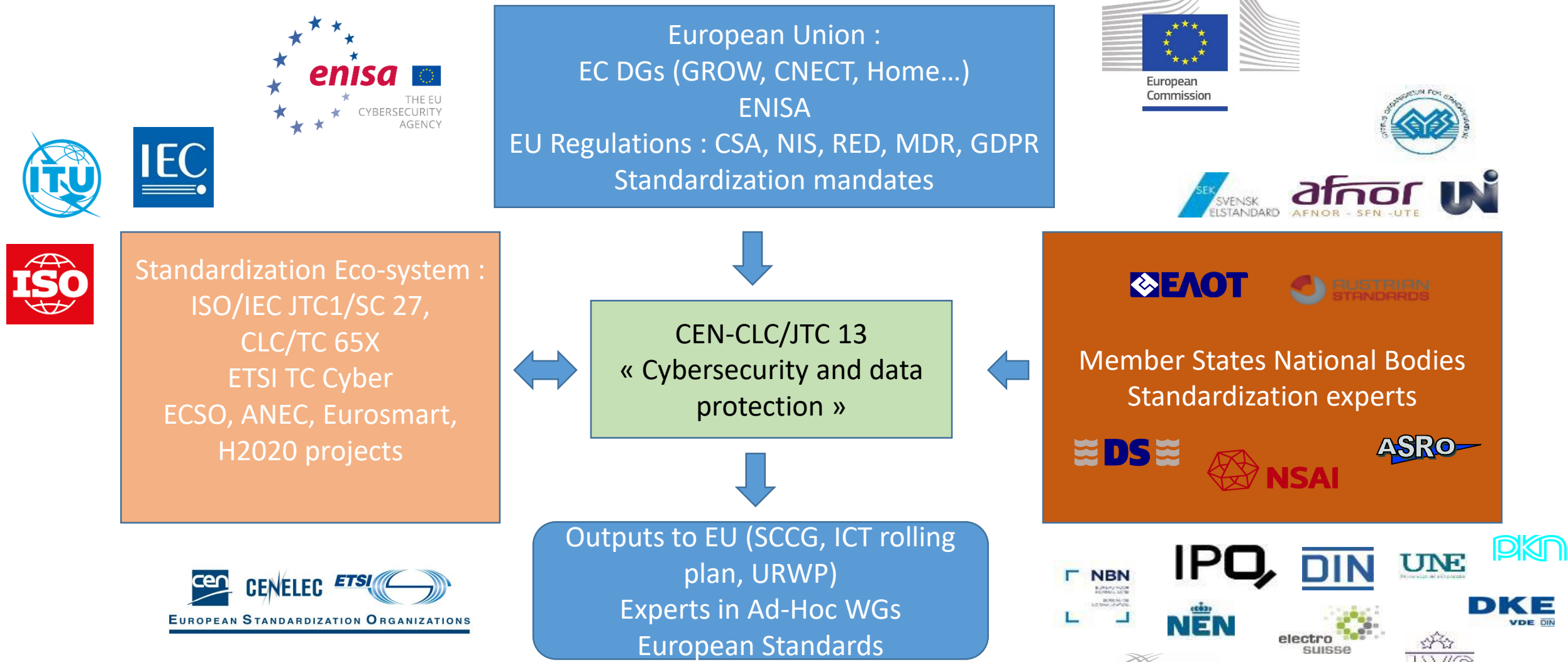**European Standardization Organizations**

Cybersecurity Standardization Conference 2021

Jean-Pierre Quémard CEN-CLC/JTC 13/WG 1 convenor

CEN-CLC/JTC 13 Introduction

European Union :
EC DGs (GROW, CNECT, Home…)
ENISA
EU Regulations : CSA, NIS, RED, MDR, GDPR
Standardization mandates

Standardization Eco-system :
ISO/IEC JTC1/SC 27,
CLC/TC 65X
ETSI TC Cyber
ECSO, ANEC, Eurosmart,
H2020 projects

CEN-CLC/JTC 13
« Cybersecurity and data protection »

Member States National Bodies
Standardization experts

Outputs to EU (SCCG, ICT rolling plan, URWP)
Experts in Ad-Hoc WGs
European Standards

CEN-CLC/JTC 13 Environment

▶ The strong digitalization of the environment implies strong cybersecurity and data protection demand

▶ More and more transversal building blocks and more and more vertical domains concerned (ICT, eHealth, transport, Energy, Domotics, Industrial systems…)

▶ Need for a strong unified European wide Market relying on Common Cybersecurity evaluation framework

▶ Standardization is a must to support this request:
  o Simplicity and openness
  o Readability and complementarity
  o Efficiency and reusability

CEN-CLC/JTC 13 Strategy

▶ Transpose all relevant standards to European standards (EN) according to international agreements :

  o ISO/IEC 270XX family
  o Common criteria ISO/IEC 15408/18045
  o Privacy standards ISO/IEC 29100/29101/29134/27701
  o Vulnerability disclosure ISO/IEC 29147/30111

▶ Cooperate with ETSI:

  o EN 303 645 'Cybersecurity for Consumer IoT'

▶ Liaise and cooperate with:

  o Other European organizations (ANEC, ECSO, SBS)
  o CEN-CLC TCs active in cybersecurity verticals

In line with the CEN and CENELEC Strategy 2030 for Digitalization & Green Transition

Some examples of JTC 13 roadmap

▶ Development of a « Fixed time evaluation method » taking into account experience coming from France, Germany, Spain and others

▶ **Cybersecurity evaluation methodology** for ICT products – **prEN 17640**
  o intended for use for all three assurance levels as defined in the Cybersecurity Act (i.e. basic, substantial and high) – addressing verticals for common framework

▶ Further projects under development:
  o **Data protection and privacy** by design and by default (under M/530)
  o Managed **Security Services Providers** Requirements (in cooperation with ECSO)
  o Requirements for **Professional Profiles** related to personal data processing and protection
  o Personal data protection requirements for **Processing Operations**

▶ Harmonization of CC and EN ISO/IEC 270XX approaches

▶ Common work with ETSI
  o IoT Cybersecurity and evaluation methods (EN 303 645, TS 103 701)
  o Standardization Request on **Servers and data storage products**
  o Protection Profiles for smart meters