European Standardization Organizations

European Standardisation for Cybersecurity and Data Protection
JTC 13 Roadmap and Achievements

Walter Fumy, Chairperson CEN-CENELEC JTC 13

Agenda

- Introduction to JTC 13
  - Scope
  - Structure
  - Cooperation
- Roadmap & Achievements
  - Pre-JTC 13
  - International Adoptions
  - Selected Project Highlights
- Annex: Additional Information

CEN-CLC/JTC 13 Cybersecurity and Data Protection

- Joint technical committee (JTC) of CEN and CENELEC
- established November 2017
- 150+ European experts on cybersecurity and data protection
- 6 dedicated working groups
- 3 plenary meetings per year
- annual outreach events

- Chairperson: Walter Fumy, Bundesdruckerei (Germany)
- Secretariat: DIN German Institute of Standardization
- Secretary: Martin Uhlherr
- CEN-CENELEC Management Centre Programme Manager: Laurens Hernalsteen

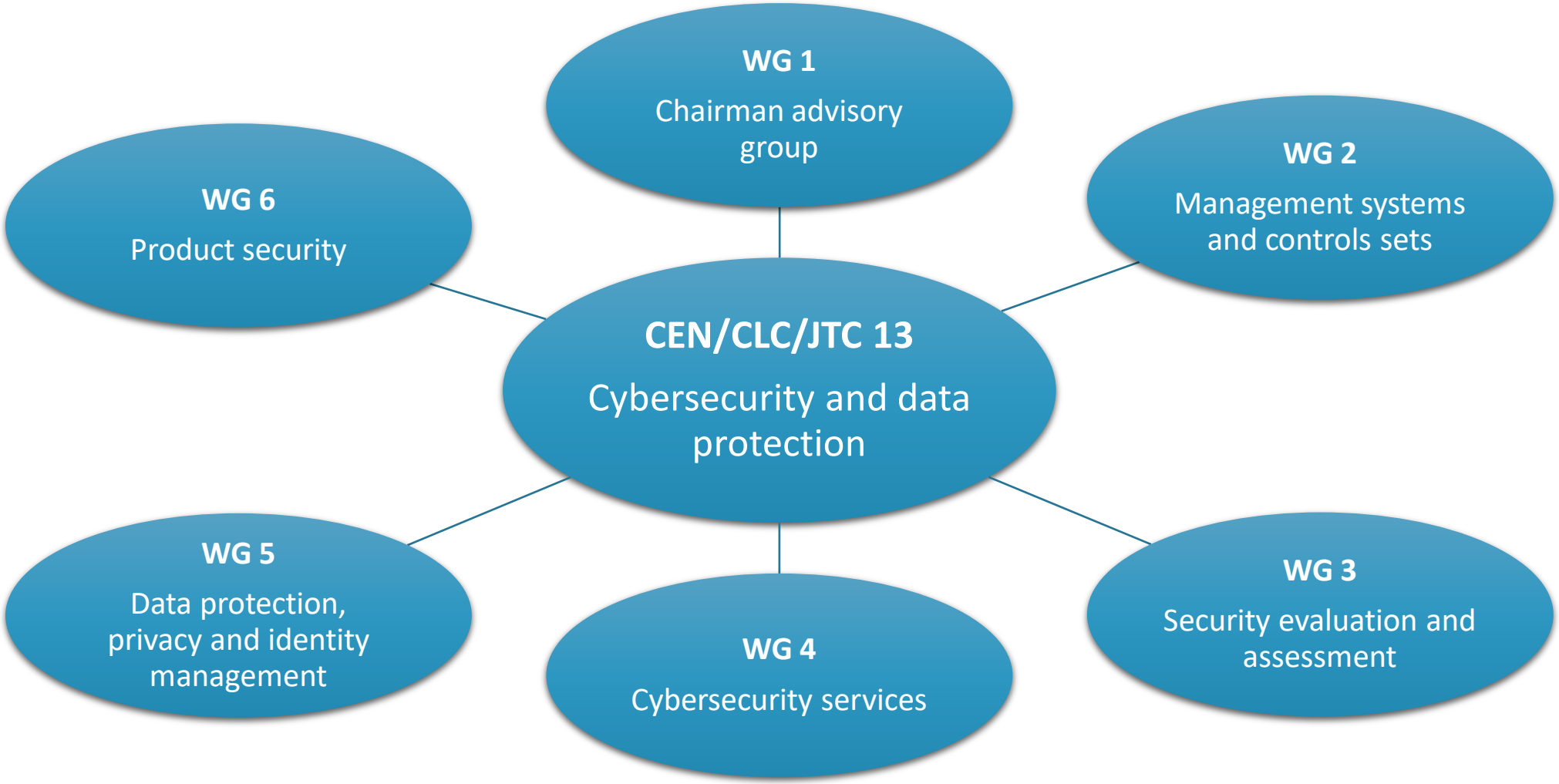
Scope (1/2)

- Development of horizontal standards in the field of cybersecurity and data protection for vertical applications domains such as ICT, eHealth, transport, smart cities, automotive, IoT, …
  - driven by European market needs
- Key areas of work
  - Security requirements, services, techniques and guidelines for ICT systems, services, networks and devices, including smart objects and distributed computing devices
  - Management systems, frameworks, methodologies
  - Data protection and privacy
  - Standards for security assessment and evaluation
  - Competence requirements in the area of cybersecurity and data protection
- Identification and adoption of documents published by ISO/IEC JTC 1, other SDOs, international bodies and industrial fora
- Development of CEN/CENELEC publications for safeguarding information

Scope (2/2)

- Partnership with international and national SDOs, industrial fora, and other stakeholders
  - International (ISO, IEC, ITU, GlobalPlatform, …)
  - Europe (ETSI, ENISA, ANEC, …)
  - National Standardization bodies relevant to our work, on international level (NIST, JISC, SAC, …)
- Contributions to ICT rolling plan, EU standardisation strategy, Union Rolling Work Programme (URWP) of the EU Cybersecurity Act (Regulation (EU) 2016/679)
- Development of standards in accordance with the EU Cybersecurity Act
  - Recital 54: International cooperation
  - Recitals 49, 66: Interoperable solutions
- … and other EU regulations such as eIDAS (Regulation (EU) 910/2014), General Data Protection Regulation (EU) 2016/679 (GDPR), NIS (Regulation (EU) 2016/1148), …

Structure



Working Groups

Working Group	Convenor	Secretariat	Secretary
JTC 13/WG 1	Jean-Pierre Quémard	DIN (Germany)	Martin Uhlherr
JTC 13/WG 2	Ralph Eckmaier	ASI (Austria)	
JTC 13/WG 3	Miguel Bañon	UNE (Spain)	Philipe Magnabosco
JTC 13/WG 4	Ralph Eckmaier (acting)	ASI (Austria)	
JTC 13/WG 5	Alessandro Guarino	UNI (Italy)	Carla Sirocchi
JTC 13/WG 6	Ben Kokx	NEN (Netherlands)	Tom Hoogendijk

Selected Liaisons and Cooperations I

European Institutional Stakeholders

- ANEC

European Association for the Coordination of Consumer Representation in Standardisation

- ETUC

European Trade Union Confederation

- ENISA

European Union Agency for Cybersecurity

Liaison and Partner Organizations

- APPLiA

Home Appliance Europe

- EADPP

European Association of Data Protection Professionals

- ECSO

European Cyber Security Organisation

- EURALARM

Association of European manufacturers, installers and service providers of the electronic Fire Safety and Security industry

- GlobalPlatform

Selected Liaisons and Cooperations II

Standardization Committees

- CEN/CLC/ETSI/SMCG
  Smart Meter Coordination Group
- CEN/CLC/JTC 19
  Blockchain and DLT
- CEN/CLC/JTC 21
  Artificial Intelligence
- CEN/TC 224
  Machine-Readable Cards
- CEN/TC 301
  Road vehicles
- CEN/TC 377/WG 1
  Information security in air traffic management
- CLC/TC 205
  Home and Building Electronic Systems
- CLC/TC 65X
  Industrial-process measurement, control and automation
- CLC/TC 79
  Alarm Systems
- ETSI TC CYBER
- ISO/IEC JTC 1/SC 27
  Information security, cybersecurity and privacy protection

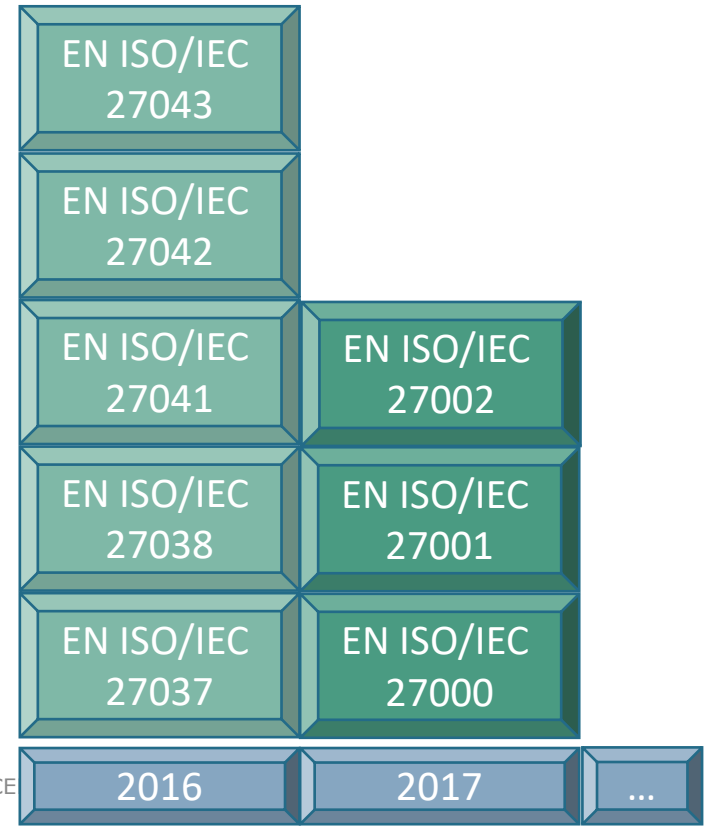
Agenda

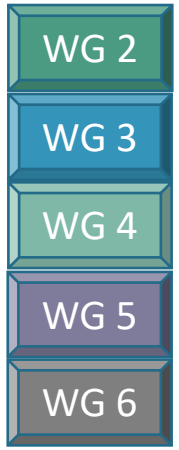
- Introduction to JTC 13
  - Scope
  - Structure
  - Cooperation

- Roadmap & Achievements
  - Pre-JTC 13
  - International Adoptions
  - Selected Project Highlights

- Annex: Additional Information

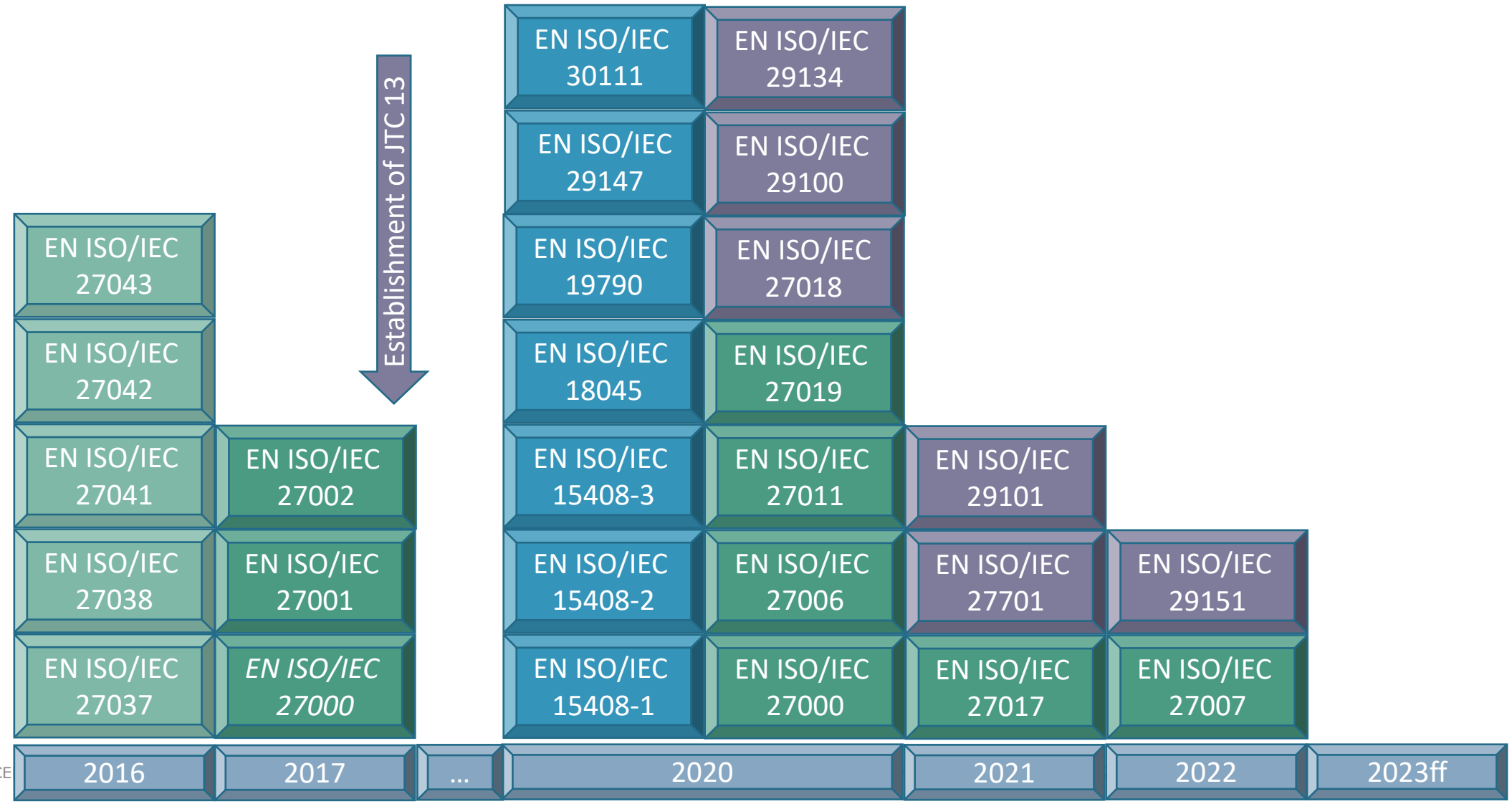
Achievements – Pre JTC 13



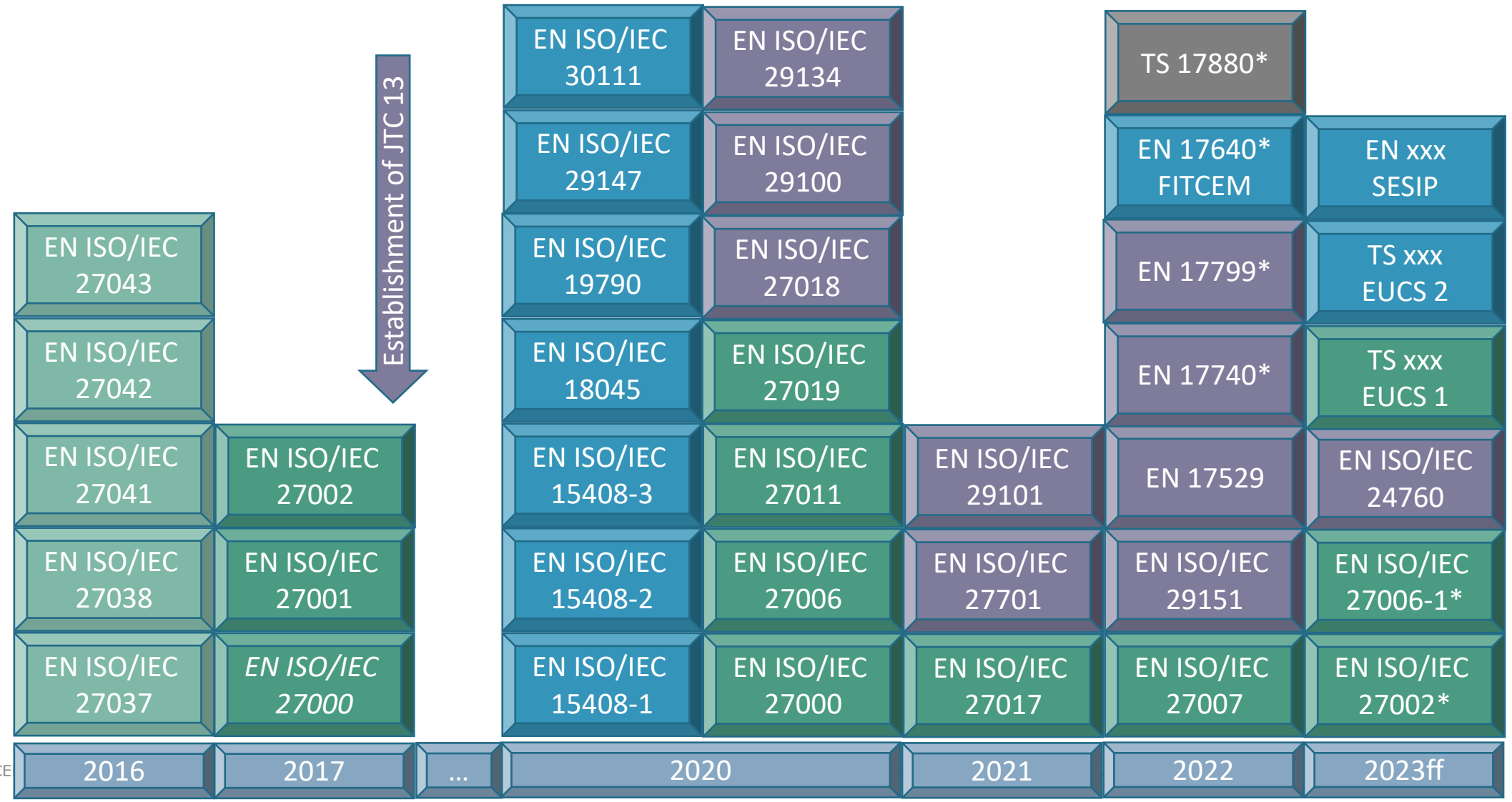


Before JTC 13 was created in November 2017, the *CEN-CENELEC Focus Group on Cybersecurity* has orchestrated the **adoption of international cybersecurity standards** for supporting the EU Digital Single Market.

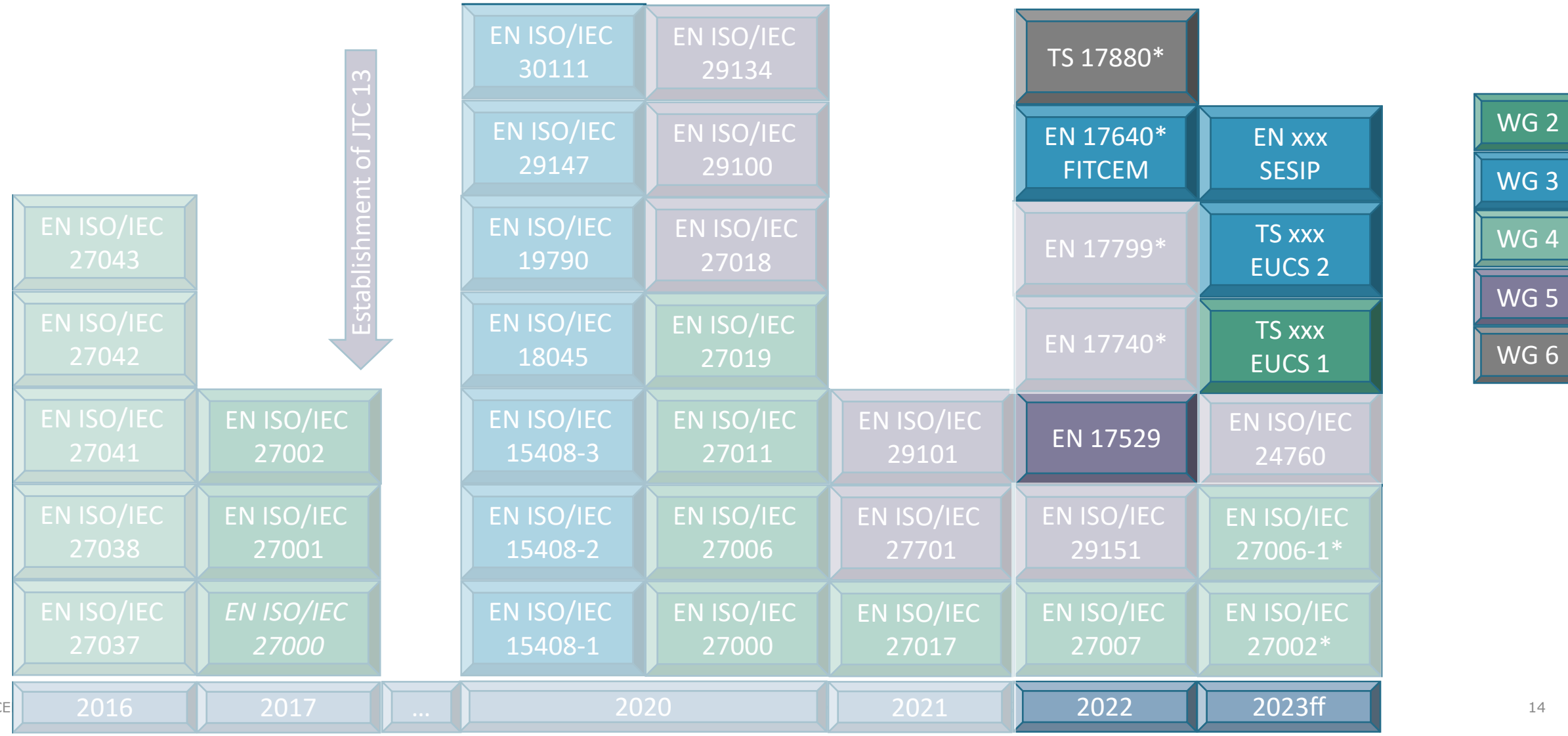
Achievements



Achievements & Roadmap



Selected Project Highlights



EN 17529:2022

Data protection and privacy by design and by default

- EN 17529 aims to ensure that data protection and privacy requirements are taken into account early on in the development of products and services.
- Developed in response to a request from the European Commission with the aim to complement international adoptions in specifically addressing European values.
- Under the same mandate, there are also two Technical Reports currently being finalised which contain recommendations on how to integrate the principle of 'data protection and privacy by design' in specific areas of application:
  - CEN/CLC/prTR xxx: Privacy management in products and services – Biometric access control products and services
  - CEN/CLC/prTR xxx: Data protection and privacy by design and by default – Technical Report on applicability to the videosurveillance industry – State of the art

prEN 17640 - FITCEM

Fixed time cybersecurity evaluation methodology for ICT products

- flexible methodology comprised of different evaluation blocks including assessment activities that comply with the evaluation requirements of the CSA
- designed for use for all three assurance levels as defined in the Cybersecurity Act (i.e. basic, substantial, high)
- methodology may be applied to both 3rd party evaluation and self-assessment

- Status: Under approval
- Expected Publication date: 2022

➢ See also: Session S22b tomorrow

WI JT013045 – prEN XXX – SESIP

Security Evaluation Standard for IoT Platforms. An effective methodology for applying cybersecurity assessment and re-use for connected products.

- Describes a cybersecurity evaluation methodology for components of connected ICT products. Security claims in SESIP are made based on the security services offered by those components (hardware or software).
- Provides a common set of requirements for the security functionality of components which apply to the foundational components of devices that are not application specific.
- Aims to support comparability between and re-use of independent security evaluations.
- Collaboration with GlobalPlatform

- Status: Under drafting (expected publication date: 2023)

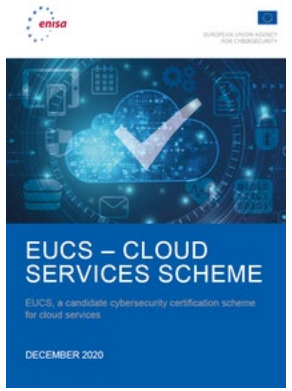
➢ See also: Session L13b tomorrow

WI JT013043 – prCEN/CLC/TS XXX

Multi-layered approach for a set of requirements for information/cyber security controls for Cloud Services (EUCS 1 project)

- Technical Specification (TS) to provide a set of information security requirements for information/cyber security controls for Cloud Services
- Requirements are labelled *basic, substantial* or *high*
- Essential component of the EUCS, as they define the technical objectives and requirements that CSPs need to fulfil in order to get a cloud service certified
- Collaboration with ENISA

- Status: Under drafting
- Expected Publication date: 2023-09

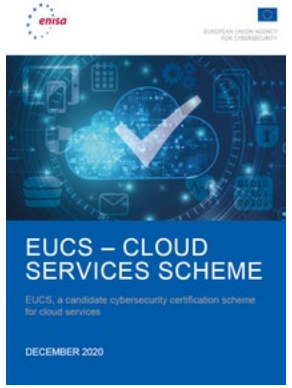


WI JT013044 – prCEN/CLC/TS XXX

Requirements for Conformity Assessment Bodies certifying Cloud Services (EUCS 2 project)

- Complements and supplements the procedures and general requirements available in ISO/IEC 17065:2012 for certification bodies performing evaluations based on EUCS or similar certification schemes of ICT services following the EU Cybersecurity Act
- Applies to all three CSA assurance levels (*basic, substantial* and *high*)
- Collaboration with ENISA

- Status: Under drafting
- Expected Publication date: 2023



prCEN/CLC/TS 17880

Protection Profile for Smart Meter - Minimum Security Requirements

- TOE: Smart supply meter that monitors, and possibly limits, the consumption of electricity, gas, thermal energy or water and communicates with users via local and network interfaces.
- The meter's basic security tasks include to ensure
  - the integrity of its content,
  - the authenticity and integrity of instructions that it acts on,
  - the confidentiality of data used to provide security functions (such as keys), and
  - the confidentiality of sensitive personal and personally identifiable information.
- Further, the meter firmware has to be protected from tampering by a firmware integrity test, and by a secure firmware update.
- Evaluation assurance level EAL3+
- *Based on TR developed and published 2019 by CEN/CENELEC/ETSI Coordination Group on Smart Meters*

- Status: Under approval (expected publication date: 2022)

Adhoc Group EU 5G CCS

- established April 2022
  - to mirror ENISA EU 5G cybersecurity certification scheme activities, and
  - to support the CEN/CENELEC representative François Zamora in the ENISA AHWG tasked to prepare the candidate EU 5G cybersecurity certification scheme

- AHG EU 5G CCS operates under the supervision of JTC 13/WG 1

JTB RED_Cyber

Joint technical Body (JTB) of CEN, CENELEC and ETSI

- to be established* for the development of three ‘generic’ standards (one for each article) in support of articles 3.3(d), (e) and (f) of the European Radio Equipment Directive (RED)
  - Common security requirements for internet-connected radio equipment
  - Common security requirements for equipment processing data (internet-connected radio equipment, childcare radio equipment, toys radio equipment, and wearable radio equipment)
  - Common security requirements for internet-connected radio equipment processing virtual money/monetary value
- very challenging timeframe (standards to be available 2023-10-01)

**) formal creation of the JTB has been put on hold within the CEN-CENELEC-ETSI Joint Presidents’ Group (JPG), waiting for the final standardization request to be made available*

Additional Information

- JTC 13 Overview and Business Plan
  - https://standards.cencenelec.eu/dyn/www/f?p=205:7:0::::FSP_ORG_ID:2307986&cs=1BFE244DDA2A68D1B5C93795034A8DD05
- Programme of Work
  - https://standards.cencenelec.eu/
- JTC 13 Secretariat
  - Martin Uhlherr
    martin.uhlherr@din.de

Thank you for your kind attention!

Contact: walter.fumy@ry-cyber.de
martin.uhlherr@din.de

International adoptions by WG2

- EN ISO/IEC 27000:2020 - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2018)
- EN ISO/IEC 27001:2017 - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)
- prEN ISO/IEC 27002 - Information security controls (ISO/IEC 27002:2022)
- EN ISO/IEC 27006:2020 - Requirements for bodies providing audit and certification of information security management systems (ISO/IEC 27006:2015, including Amd 1:2020)
- EN ISO/IEC 27007:2019 - Guidelines for information security management systems auditing (ISO/IEC 27007:2017)
- EN ISO/IEC 27011:2020 - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations (ISO/IEC 27011:2016)
- EN ISO/IEC 27017:2020 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015)
- EN ISO/IEC 27019:2020 - Information security controls for the energy utility industry (ISO/IEC 27019:2017, Corrected version 2019-08)

International adoptions by WG3

- EN ISO/IEC 15408-1:2020 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model (ISO/IEC 15408-1:2009)
- EN ISO/IEC 15408-2:2020 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components (ISO/IEC 15408-2:2008)
- EN ISO/IEC 15408-3:2020 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components (ISO/IEC 15408-3:2008)
- EN ISO/IEC 18045:2020 Information technology - Security techniques - Methodology for IT security evaluation (ISO/IEC 18045:2008)
- EN ISO/IEC 19790:2020 Information technology - Security techniques - Security requirements for cryptographic modules (ISO/IEC 19790:2012, Corrected version 2015-12)
- EN ISO/IEC 29147:2020 Information technology - Security techniques - Vulnerability disclosure (ISO/IEC 29147:2018)
- EN ISO/IEC 30111:2020 Information technology - Security techniques - Vulnerability handling processes (ISO/IEC 30111:2019)

International adoptions by WG4

- EN ISO/IEC 27037:2016 - Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012)
- EN ISO/IEC 27038:2016 - Specification for digital redaction (ISO/IEC 27038:2014)
- EN ISO/IEC 27041:2016 - Guidance on assuring suitability and adequacy of incident investigative method (ISO/IEC 27041:2015)
- EN ISO/IEC 27042:2016 - Guidelines for the analysis and interpretation of digital evidence (ISO/IEC 27042:2015)
- EN ISO/IEC 27043:2016 - Incident investigation principles and processes (ISO/IEC 27043:2015)

International adoptions by WG5

- EN ISO/IEC 27018:2020 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018:2019)
- EN ISO/IEC 27701:2021 - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines (ISO/IEC 27701:2019)
- EN ISO/IEC 29100:2020 - Privacy framework (ISO/IEC 29100:2011, including Amd 1:2018)
- EN ISO/IEC 29101:2021 - Privacy architecture framework
- EN ISO/IEC 29134:2020 - Guidelines for privacy impact assessment (ISO/IEC 29134:2017)
- prEN ISO/IEC 24760-1 - A framework for identity management - Part 1: Terminology and concepts (ISO/IEC 24760-1:2019)
- prEN ISO/IEC 24760-2 - A framework for identity management - Part 2: Reference architecture and requirements (ISO/IEC 24760-2:2015)
- prEN ISO/IEC 24760-3 - A framework for identity management - Part 3: Practice (ISO/IEC 24760-3:2016)