Standardization of Knowledge and Skills for IT Security

Milan

Friday, October 28th 2016

UNINFO

Veronica Salsano

Overview

- Standardization in general
- Legislation
- Technical foundations
- Actors
- Current situation
- Security
- The way forward
- Conclusions

UNINFO

Standardization in General (1)

According to Regulation UE 1025/2012

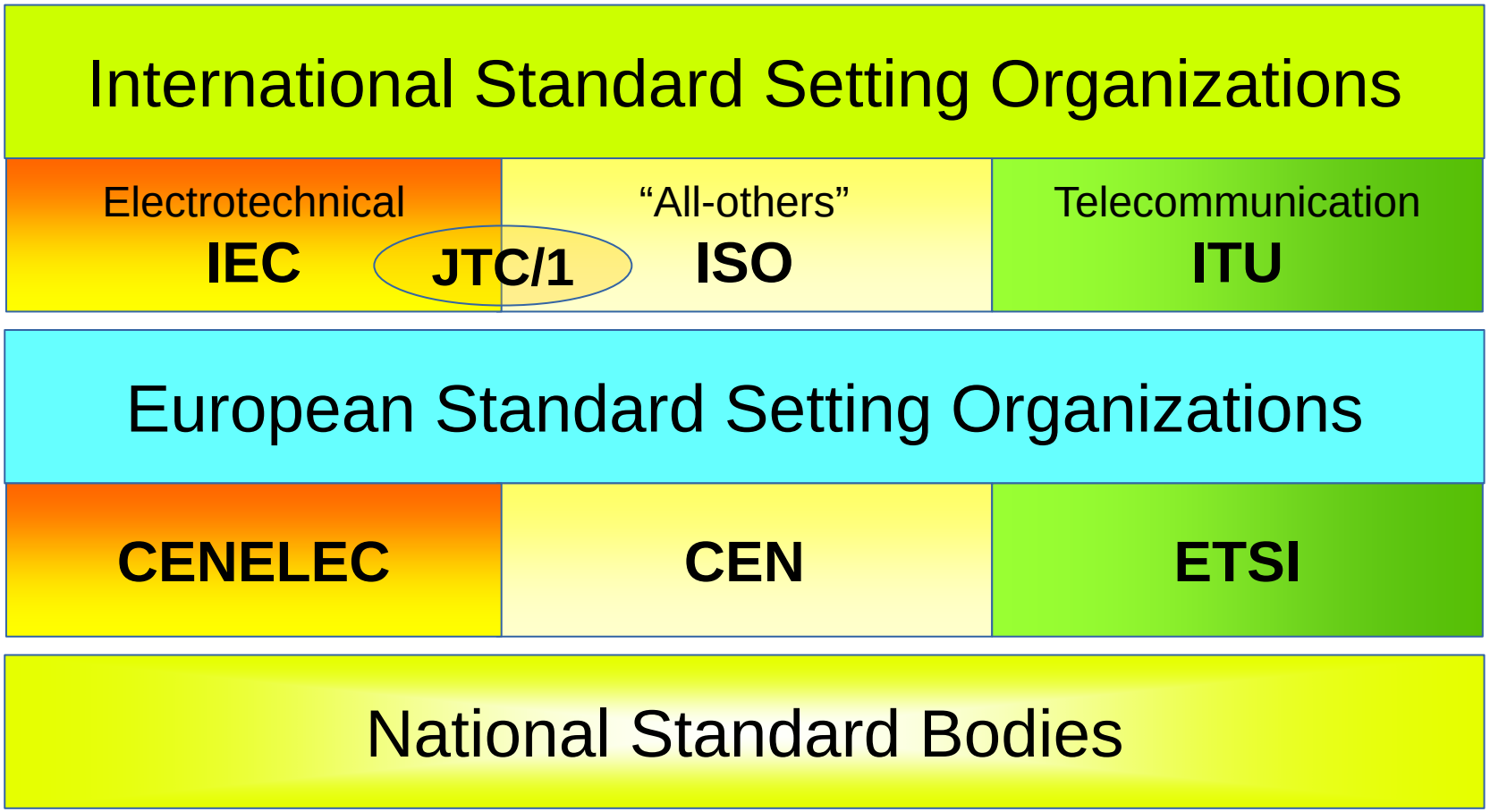
"The primary objective of standardization is the definition of voluntary technical or quality specifications with which current or future products, production processes or services may comply"

Standards

- Promote interoperability of products and services
- Improve safety, reliability and in general quality of products
- Allow scale economies
- Foster competition
- Facilitate trade and commerce by removing barriers
- Promote the sharing of knowledge

UNINFO

Standardization in General (2)



Standardization in General (3)

Technical Committees

- Managed by NBs (National Bodies)
- Produce EN, CEN/TS (Technical Specification), CEN/TR (Technical Report); ISO IS (ISO Standard)
  - EN and CEN/TS cogent when published

Workshops

- Private agreement among participants
- Produce CWA (CEN/CENELEC Workshop Agreement)

UNINFO

Legislation

Italy

In Italy two national laws have been issued, reinforcing the role of technical standards for regulating professionalism matters:

- Law n°4, January 14th 2013
- Legislative Decree n°13, January 16th 2013

"The qualification of professional performance is based on its conformity with the technical standards UNI ISO, UNI EN ISO, UNI EN e UNI, in the next sections called « UNI technical standards», following Directive 98/34/CE of the European Parlament and of the Council of 22nd June 1998, and on the basis on the guidelines CEN 14 of 2010"

Europe

- Annual Union Work Programme (AUWP)
- the EU Rolling plan for ICT Standardization (Rolling Plan in short)
- The Communication on the Digital Single Market (DSM) Strategy of 6 May 2015

UNINFO

Technical foundations (1)

Overall Model

- A horizontal framework standard (i.e. the CEN/CWA e-CF «European Competence Framework»)
- Sectorial profiles (vertical, based on the framework)
- Support tools

UNINFO

Technical foundations (2)

Framework e-CF

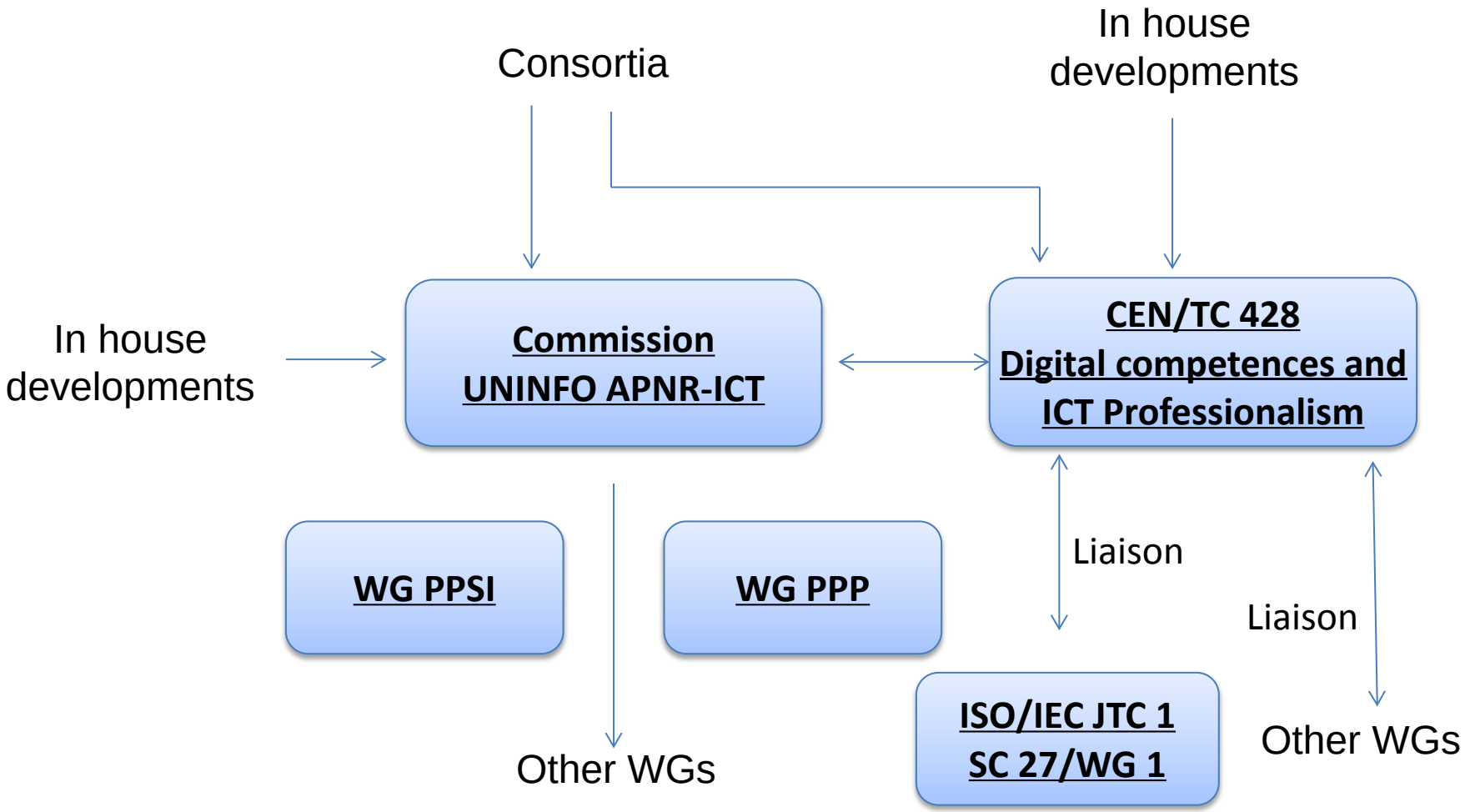
- COMPETENCE is “demonstrated ability to apply knowledge, skills and attitudes for achieving observable results”
- SKILL is the “ability to carry out managerial or technical tasks”
- KNOWLEDGE represents the “set of know-what” and can be described by operational descriptions (e.g. programming languages, design tools...)
- ATTITUDE means in this context the “cognitive and relational capacity” (e.g. analysis capacity, synthesis capacity, flexibility, pragmatism...) [incorporated in Competences]

UNINFO

Technical foundations (3)

- Competences from a library are selected, when appropriate completed with ad hoc definitions, and combined to define professional profiles.
- Professional profiles are the subject of certification.
- Profiles are classified in levels of generality (generations) by providing increasing refinements an details inheritance.

Actors


Consortia
In house developments
In house developments
Commission UNINFO APNR-ICT
CEN/TC 428 Digital competences and ICT Professionalism
WG PPSI
WG PPP
Liaison
Liaison
Other WGs
ISO/IEC JTC 1 SC 27/WG 1
Other WGs

Current Situation (1)

- Framework (e-CF v3) and methodology are European Standards, and consequently they are also national standards Europewide
- The security profile (as well as the Web Manager profile) is an Italian national standards. Italy intends to present them to CEN for adoption as European standards
- Work is ongoing in Italy on privacy and several other profiles
- Work in ISO/JTC1 is ongoing in security profiles independently of the CEN endeavours, some form of light collaboration is in place through liaisons.

UNINFO

Current Situation (2)

Italian Standards

- UNI 11506:2013 – Unregulated professional activities- Professions in the ICT sector. Definition of the rerquirements of knowledge, ability and competences.
- UNI 11621 «Unregulated professional activities- Professions in the ICT sector.
  - Part 1 Methodology for the construction of professional profiles based on eCF - published
  - Part 2 “Second generation” professional profiles - published.
  - Part 3 Professional profiles for professions operating in the web – published.
  - Part 4 Professional profiles for information security - published
  - Part 5 Professional profiles for privacy - ongoing
  - Part 6 Professional profiles for geographical information - ongoing
  - Other parts (Communicator, Project manager, Legacy manager) – onging

UNINFO

Current Situation (3)

CEN standards

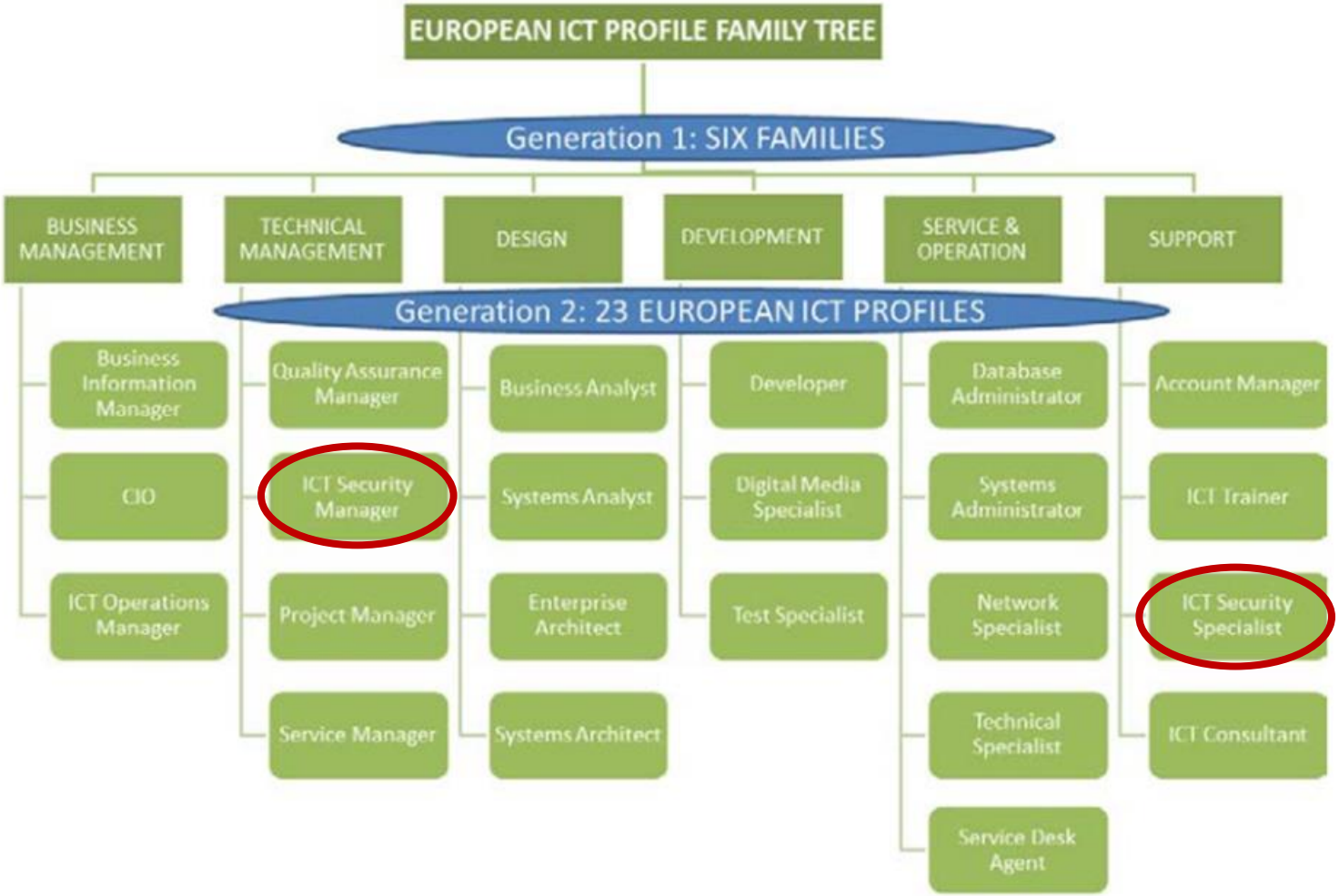
- EN 16234-1:2016 – e e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework
- CEN/TR 16234-2:2016 – e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 2: User Guide
- WI TR 16234-3 – e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 3: Methodology.

ISO standards

- ISO/IEC 27021 - “Competence requirements for information security management systems professionals”.

UNINFO

Security (1)
UNI 11621-2 1°& 2° generation profiles



Security (2)
UNI 11621-4 IS professional profiles

CONTEXT	ACTIVITY: MANAGEMENT	ACTIVITY: CONTROL
DIRECTION	Information security top manager (CISO)	Information security process analyst
ORGANIZATION	Information security manager	
PROCESSES	Information security process specialist	
APPLICATIONS	Information security application specialist	Information security technical analyst
INFRASTRUCTURES	Information security infrastructures specialist	
INCIDENTS	Incident response specialist	Forensics analyst

UNINFO

UNI 11621-4 IS professional profiles

Relationships between second (right) and new third generation profiles (left)

Third generation profile	*Related second generation profile*
Information security top manager (CISO)	ICT Security Manager
Information security manager	ICT Security Manager
Information security process analyst	ICT Security Specialist
Information security technical analyst	ICT Security Specialist
Forensics analyst	ICT Security Specialist
Information security process specialist	ICT Security Specialist
Information security infrastructures specialist	ICT Security Specialist
Information security applications specialist	ICT Security Specialist
Incident response specialist	ICT Security Specialist

UNINFO

Other professional profiles

Defined in other national or international standards

Third generation profile	*Related second generation profile*
ICT Security manager	ICT Security Manager
Digital data conservation manager	ICT Security Manager
Specialist for coninuing operations	ICT Security Specialist

UNINFO

Hot topics

- Profiles
  - Breack even between detail and breadth of applicability
  - Multi part standards?
  - Multidisciplinarity
  - Certifiers as final customers

- EN 16234-1 revision
- Quality evaluation Methods (Quality Label)
- CEN/TC 428 Work plan

UNINFO

Strategy

- Complete the offer
- Methodology
- Quality
- Dissemination

Areas of envisaged activity

- Profiles
- Quality
- Other standard bodies
- Best practice
- Curricula
- Quality assurance
- Other areas (robotics, health care..)

UNINFO

UNINFO's contacts

http://www.uninfo.it

uninfo@uninfo.it

Veronica Salsano - salsano@uninfo.it


https://www.facebook.com/UNINFO.it


https://twitter.com/uninfo_it


http://www.slideshare.net/uninfoit

UNINFO