Copyright Notice

The International Standards listed on pages 9, 12-18 of this presentation are all draft standards currently under development. The draft standards are copyright protected. The copyright is with ISO and IEC. For the reproduction or other use of the Draft International Standards or parts thereof, as the content displayed on pages 9 and 12-18 of this presentation, permission needs to be acquired.

Permission can be acquired at:

ISO Copyright Office

Case postale 56 • *CH-1211 Geneva 20*

Tel. ***+ 41 22 749 01 11***

Fax ***+ 41 22 749 09 47***

E-mail ***copyright@iso.org***

Web ***www.iso.org***

Agenda

- Introduction
- Where privacy standardization takes place
- ISO/IEC privacy standards under development
- Participating in standardization projects

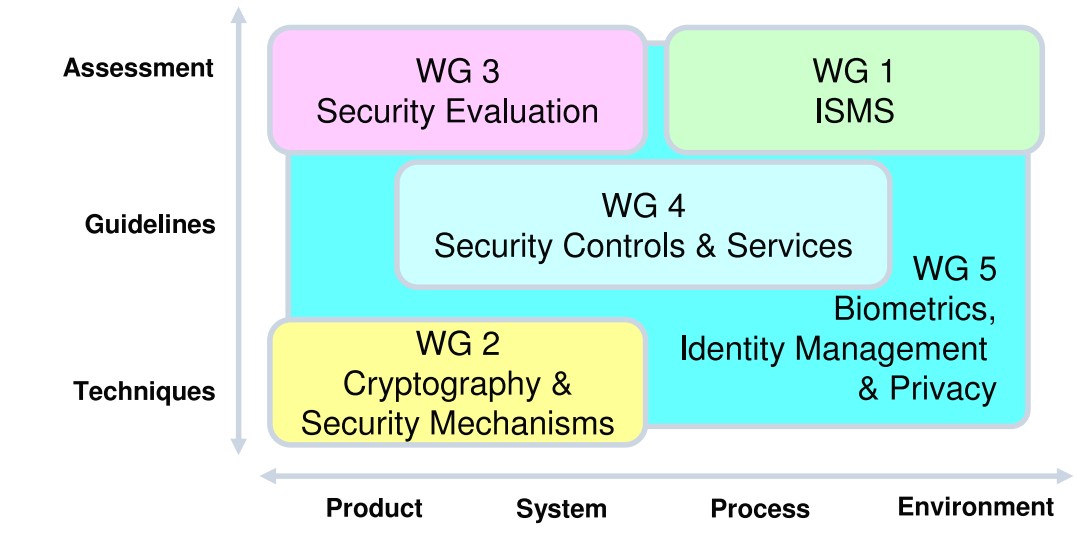
Introduction
Reasons for technical standardization

- Appropriate handling of PII
- System-independent and across national borders
- Need for a common understanding
- Addressing privacy safeguarding mechanisms

Introduction
Challenges

- **Lawyers**
- **Politicians**
- **Experts**

Where privacy standardization takes place
ISO/IEC JTC1 SC27 – Security techniques



Where privacy standardization takes place
ISO/IEC JTC1 SC27 WG5

- **Development and maintenance of standards and guidelines addressing security aspects of**
  - Identity management
  - Biometrics and
  - Privacy

Where privacy standardization takes place
WG 5 – Program of Work

Frameworks & Architectures
- A framework for identity management (ISO/IEC 24760, CD)
- Privacy framework (ISO/IEC 29100, CD)
- Privacy reference architecture (ISO/IEC 29101, CD)
- A Framework for access management (ISO/IEC 29146, WD)

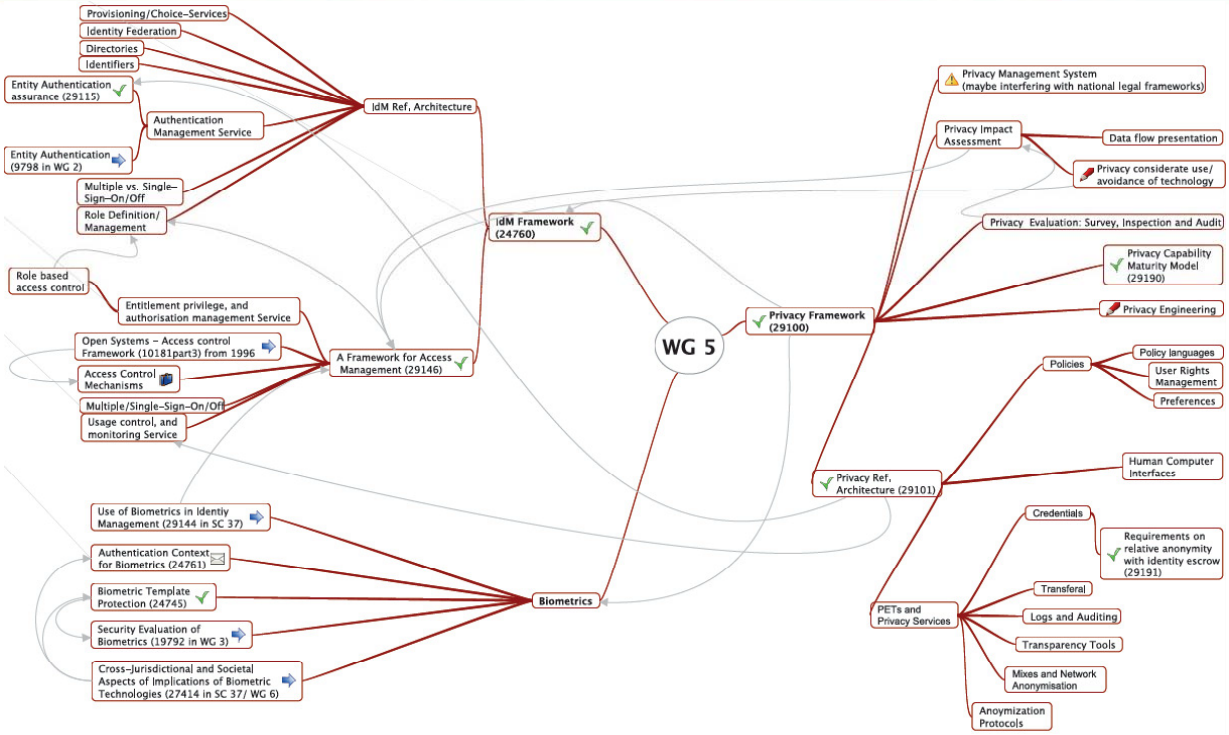
Protection Concepts
- Biometric information protection (ISO/IEC 24745, FCD)
- Requirements on relative anonymity with identity escrow – model for authentication and authorization using group signatures (WD)

Guidance on Context and Assessment
- Authentication context for biometrics (ISO/IEC 24761, FDIS)
- Entity authentication assurance (ISO/IEC 29115, CD)
- Privacy capability assessment model (ISO/IEC 29190, WD)

Where privacy standardization takes place

WG 5 – SD 1 Roadmap

Source: SC27 Document N8282 WG5 SD1 Roadmap



Where privacy standardization takes place

Ideas for future privacy standards

- **Privacy impact assessments**
- **Privacy engineering**
- **Privacy management system (?)**
- **…**

Where privacy standardization takes place
Participants in WG 5

- **National body members of ISO/IEC JTC 1 SC27**
  - Standardization organizations (e.g., DIN)
  - Data protection and privacy commissioners
  - Interested companies
  - Security and privacy experts
- **Selected liaison organizations**
  - International Conference of Data Protection and Privacy Commissioners
  - EU Data Protection Authorities through the Art. 29 Working Party
  - …

ISO/IEC Privacy standards under development
Introduction to ISO/IEC 29100 (CD4)

Source: ISO SC27 Document N8806 ISO/IEC 4th CD 29100

- **ISO/IEC 29100 – Privacy framework**
  - provides a high-level framework for the protection of personally identifiable information within information and communication technology (ICT) systems
  - is general in nature and places organizational, technical, and procedural aspects in an overall privacy framework
  - is not intended to be a global model policy, nor a legislative framework

ISO/IEC Privacy standards under development

Scope of ISO/IEC 29100 (CD 4)

Source: ISO SC27 Document N8806 ISO/IEC 4th CD 29100

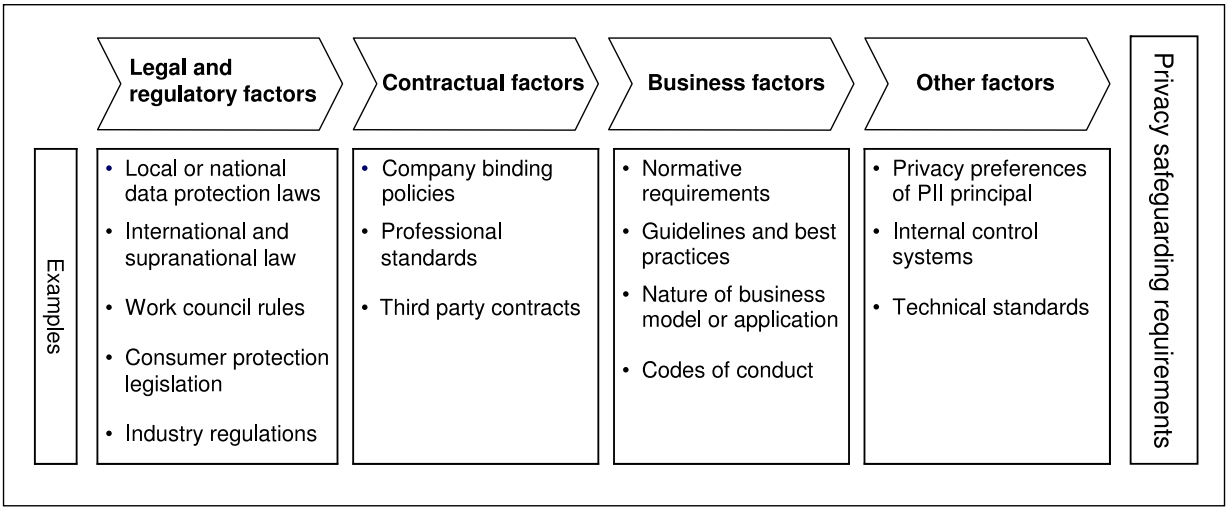
- **ISO/IEC 29100 – Privacy framework establishes**
  - a common privacy terminology;
  - a description of the actors and their roles,
  - an understanding of privacy safeguarding requirements;
  - a reference to known privacy principles.

ISO/IEC Privacy standards under development

ISO/IEC 29100 – Privacy framework

Source: ISO SC27 Document N8806 ISO/IEC 4th CD 29100

Factors influencing privacy safeguarding requirements



Source: ISO SC27 Document N8806 ISO/IEC 4th CD 29100

The privacy principles of ISO/IEC 29100

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information security controls
11. Compliance

Source: ISO SC27 Document N8808 ISO/IEC 1st CD 29101

- **ISO 29101 – Privacy reference architecture**
  - provides a consistent, high-level approach to the implementation of privacy safeguarding requirements to safeguard the processing of PII in ICT systems;
  - provides guidance for planning, designing and building ICT system architectures that more effectively facilitate the privacy of individuals by preventing inappropriate use of an individual's PII; and
  - shows how privacy enhancing technologies can be used to enhance the implementation of privacy controls.

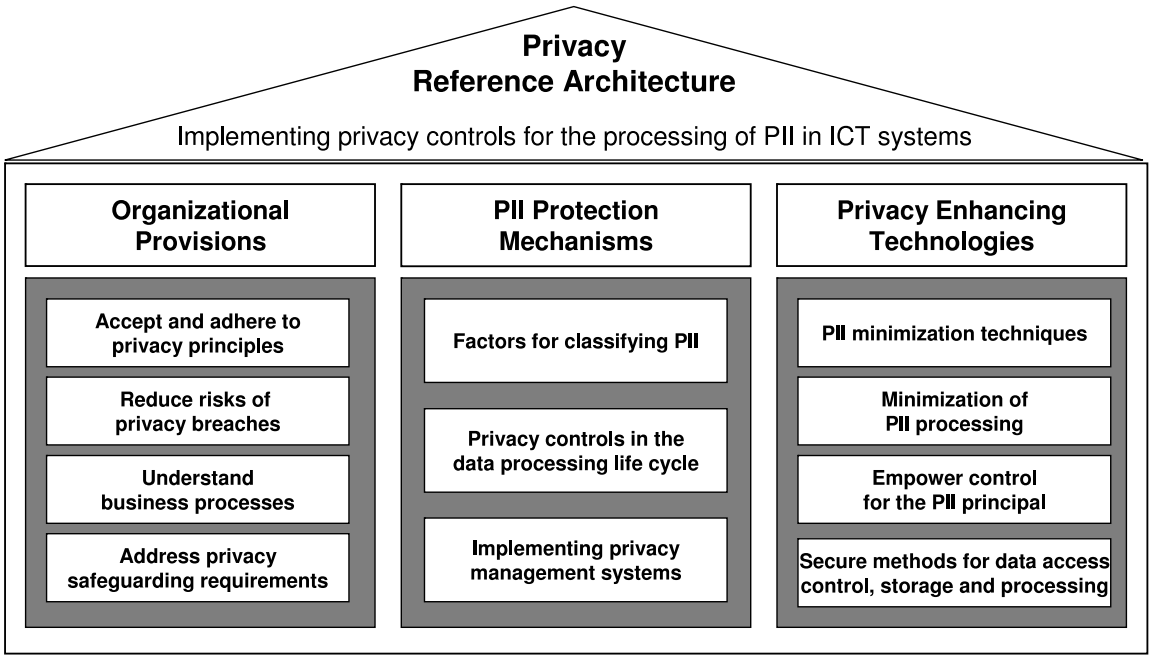
Scope of ISO/IEC 29101 (CD1)

Source: ISO SC27 Document N8808 ISO/IEC 1st CD 29101

- **ISO 29101 – Privacy reference architecture sets up**
  - organizational provisions that should be established;
  - PII protection mechanisms that should be integrated;
  - available PETs that should be used in privacy-enhanced ICT systems.

ISO/IEC 29101 – Privacy reference architecture

Source: ISO SC27 Document N8808 ISO/IEC 1st CD 29101



Contact details

- **Participation in work group meetings and providing contributions through the German standardization organization:**

  Deutsches Institut für Normung e.V.

  Gremienbetreuer: Martin Uhlherr
  martin.uhlherr@din.de

- **Technical questions on Working Group 5 and the privacy standards**

  WG 5 Convener: Prof. Dr. Kai Rannenberg
  kai.rannenberg@m-chair.net

  Project Editor: Dr. Stefan Weiss
  stefanweiss@kpmg.com

Questions and Discussion

Kontaktdaten

Dr. Stefan Weiss
Director, Advisory
Risk & Compliance

Marie-Curie-Strasse 30
60439 Frankfurt am Main
stefanweiss@kpmg.com

Tel. 49 (69) 9587 3570
Fax 49 (1802) 11991 7103
Mobile 49 (174) 3269 152

KPMG AG Wirtschaftsprüfungsgesellschaft
a subsidiary of KPMG Europe LLP