Internationale Datenschutznormung: Identity Management, Privacy Technologies und „Privacy by Design“?

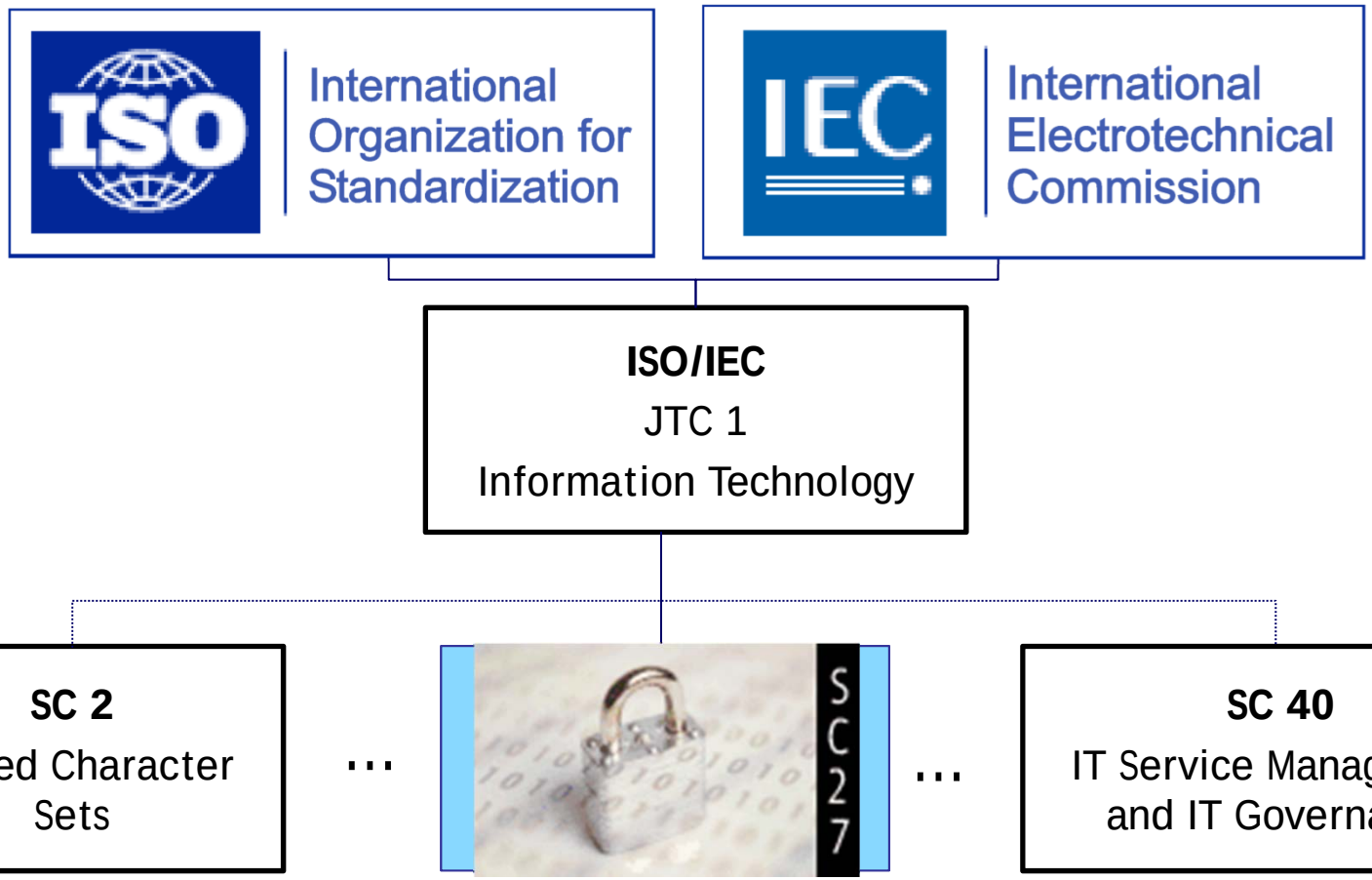
2017-01-23

[kai.rannenberg@m-chair.de]
Deutsche Telekom Chair for Mobile Business & Multilateral Security
Goethe University Frankfurt, Germany

WG 5 Identity Management & Privacy Technologies
Agenda

- **WG 5 within SC 27**
- **WG 5 standardisation projects**
- **WG 5 Standing Documents**
- **WG 5 Liaison organisations**
- **Meeting schedules**
- **Conclusions & Outlook**

SC 27 “IT Security Techniques” within ISO/IEC JTC1



SC27 Working Groups

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies

SC27
Chair: Walter Fumy (DE), Vice-chair: Marijke De Soete (BE),
Secretariat: Krystyna Passia (DIN)

WG1 *(Information security management systems)*
Convenor:
Edward Humphreys (UK)
Vice-convenor:
Dale Johnstone (AU)

WG2 *(Cryptography and security mechanisms)*
Convenor:
Takeshi Chikazawa (JP)
Vice-convenor:
Toshio Tatsuta (JP)

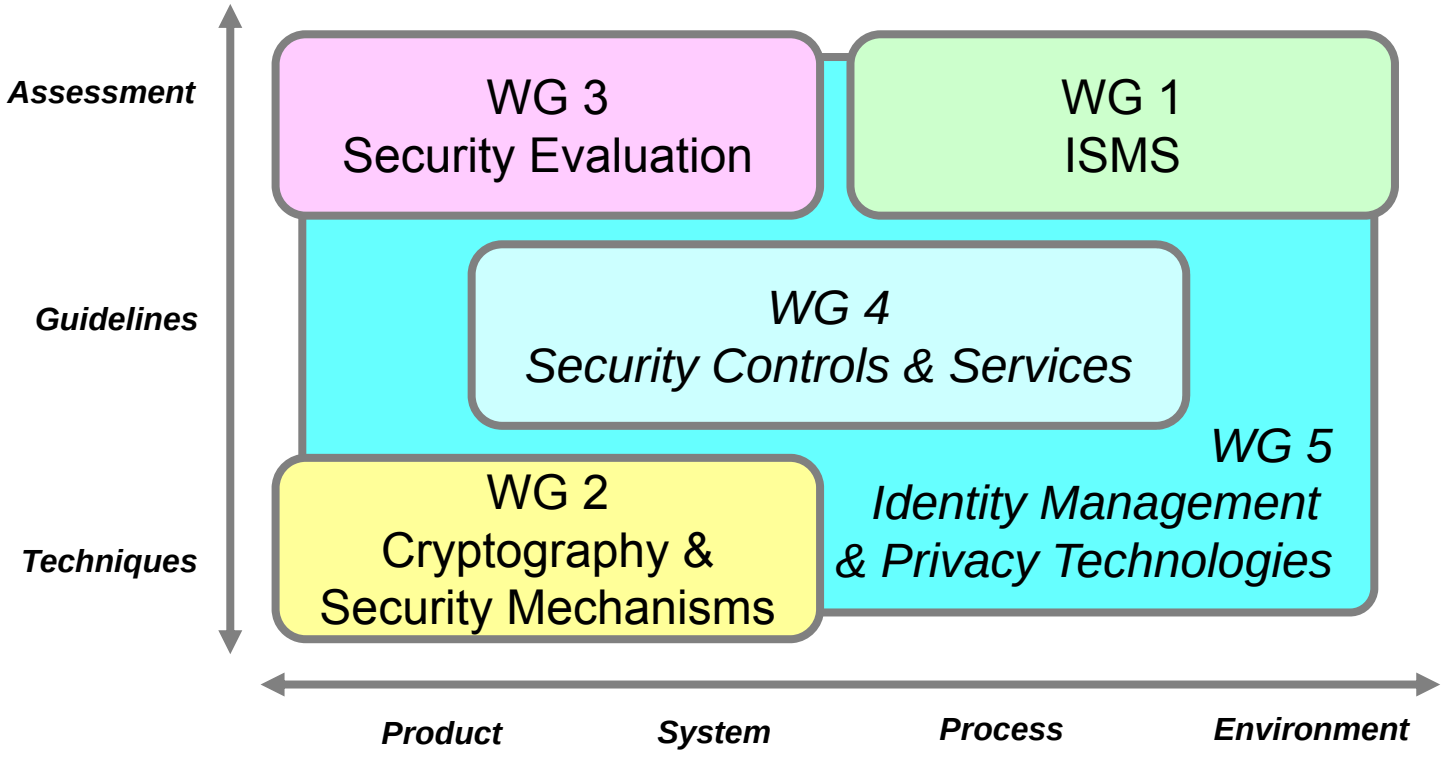
WG3 *(Security Evaluation, Testing and Specification)*
Convenor:
Miguel Bañón (ES)
Vice-convenor:
Naruki Kai (JP)

WG4 *(Security controls and services)*
Convenor:
Johann Amsenga (ZA)
Vice-convenor:
François Lorek (FR)

WG5 *(Identity management and privacy technologies)*
Convenor:
Kai Rannenberg (DE)
Vice-convenor:
Jan Schallaböck (DE)

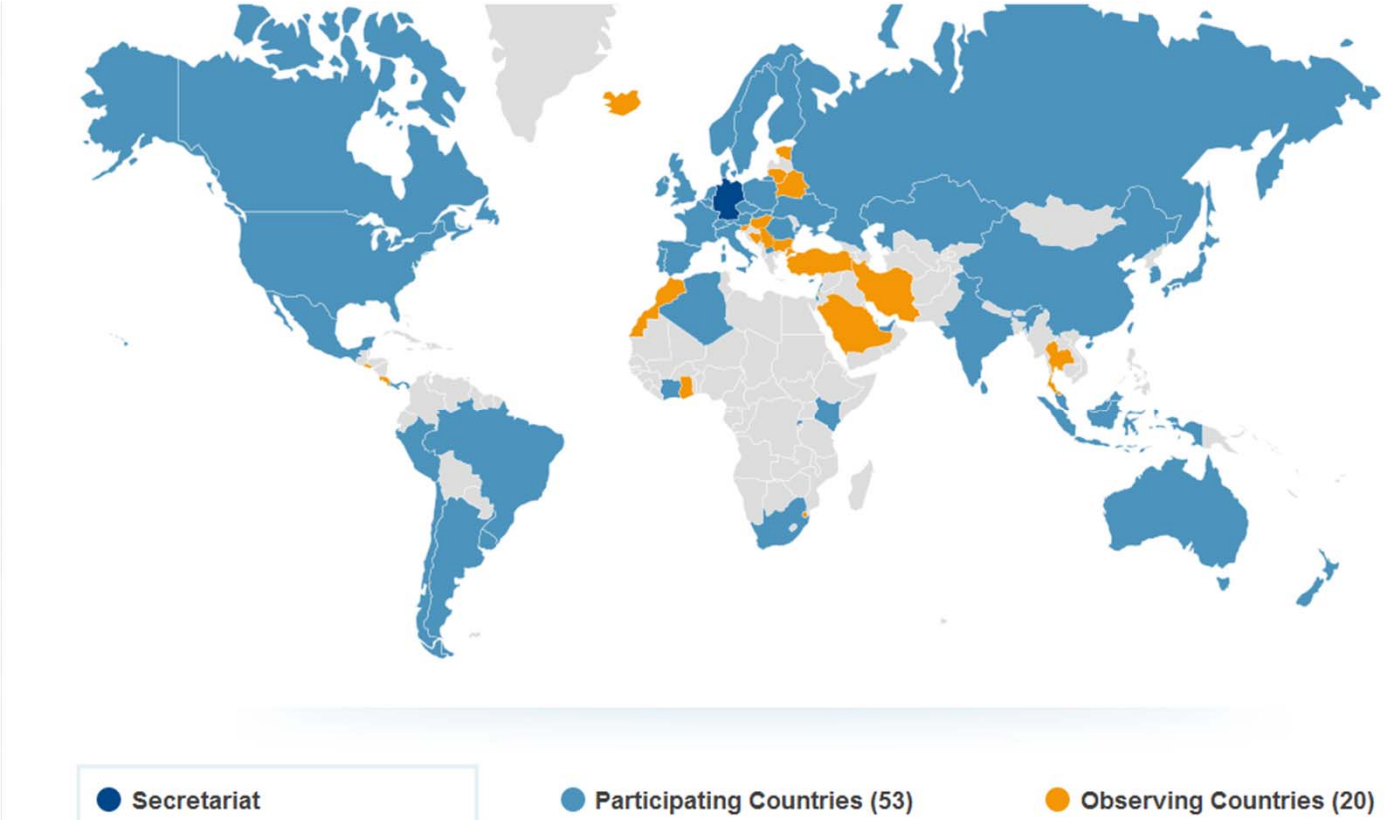
SWG-T (Transversal Items)
Convenor (acting) Andreas Fuchsberger (DE)
Vice-convenor Laura Lindsay (US)

WGs
within ISO/IEC JTC 1/SC 27 – IT Security Techniques



SC 27
Facts & Figures

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies



- Projects: 237
- Projects under development: 73
- Published standards: 164

Members:

- P-members: 53
- O-members: 20

Projects

- Projects: 237
- Projects under development: 73
- Published standards: 164

Standing Documents

- SD6 Glossary of IT Security terminology
- SD7 Catalogue of SC 27 Projects and Standards
- SD11 Overview of SC 27
- on www.din.de/en/meta/jtc1sc27/downloads

WG 5 Identity Management & Privacy Technologies Scope

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

WG 5 Identity Management & Privacy Technologies Project Overview

Frameworks & Architectures

- A framework for identity management (ISO/IEC 24760 (Parts 1-3), IS:2011, IS:2015, IS:2016)
- Privacy framework (ISO/IEC 29100, IS:2011)
- Privacy architecture framework (ISO/IEC 29101, IS:2013)
- Entity authentication assurance framework (ISO/IEC 29115, IS:2013)
- A framework for access management (ISO/IEC 29146, IS:2016)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X.1085 | ISO/IEC 17922, FDIS) (formerly X.bhsm)
- Big data reference architecture – Part 4: Security and privacy fabric (ISO/IEC 20547-4, WD) (together with WG 4)

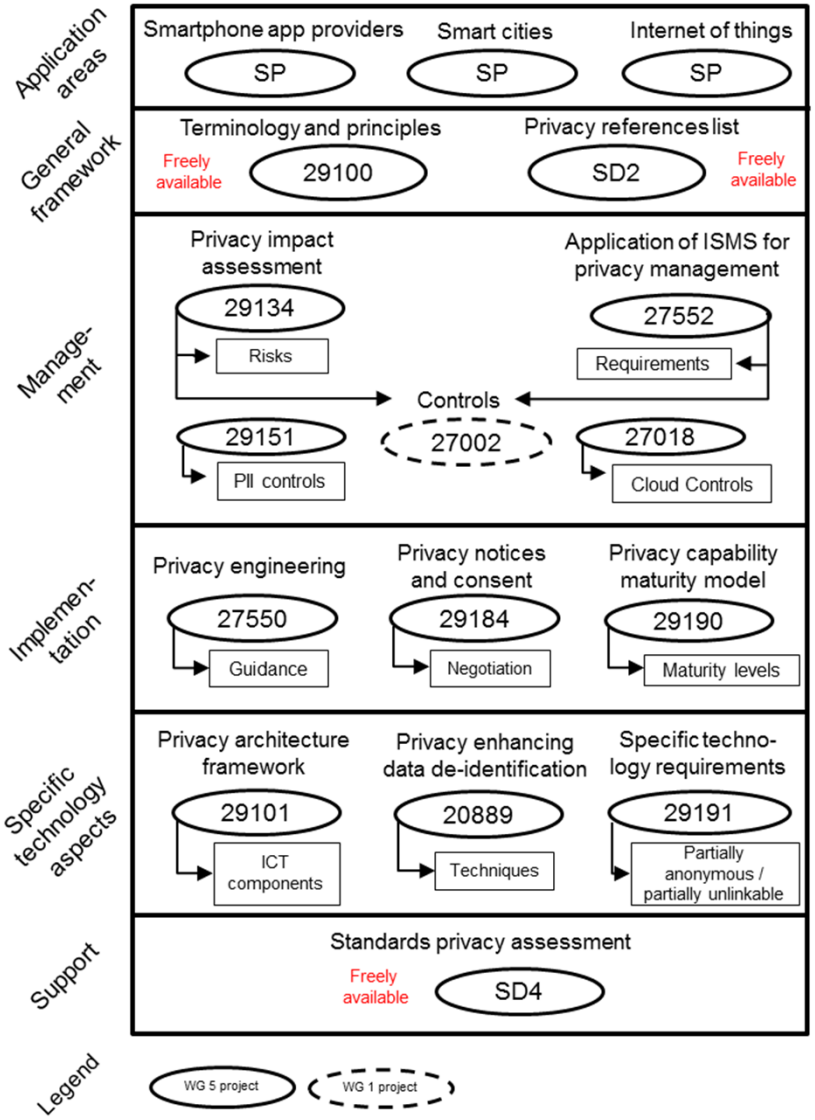
Protection Concepts

- Biometric information protection (ISO/IEC 24745, IS:2011)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, IS:2012)
- Privacy enhancing data de-identification techniques (ISO/IEC 20889, CD)
- Requirements for attribute-based unlinkable entity authentication (ISO/IEC 27551, WD)

Guidance on Context and Assessment

- Authentication context for biometrics (ISO/IEC 24761, IS:2009/Cor 1:2013, Revision CD)
- Privacy capability assessment model (ISO/IEC 29190, IS:2015)
- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018, IS:2014)
- Identity proofing (ISO/IEC 29003, DIS)
- Privacy impact assessment – methodology (ISO/IEC 29134, FDIS)
- Code of practice for PII protection (ITU-T X.1058| ISO/IEC 29151, FDIS) (formerly X.gpim)
- Guidelines for online privacy notice and consent (ISO/IEC 29184, WD)
- Privacy engineering (ISO/IEC 27550, WD)
- Enhancement to ISO/IEC 27001 for privacy management – Requirements (ISO/IEC 27552, WD)

WG 5 Identity Management & Privacy Technologies
Privacy/PII standards in SC 27/WG 5 and WG 1 (2017-01)



EU General Data Protection Regulation (GDPR) Art. 25 Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

[EU2016]

EU General Data Protection Regulation (GDPR)
Art. 25 Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

[EU2016]

EU General Data Protection Regulation (GDPR)
Art. 25 Data protection by design and by default

1. ***Taking into account the state of the art***, the ***cost*** of implementation and the ***nature, scope, context and purposes of processing*** as well as the ***risks*** of ***varying*** likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, **both at the time of the determination of the means for processing and at the time of the processing itself**, implement ***appropriate technical and organisational measures***, such as ***pseudonymisation***, which are designed to implement ***data-protection principles***, such as ***data minimisation***, in an effective manner and to ***integrate*** the necessary ***safeguards*** into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

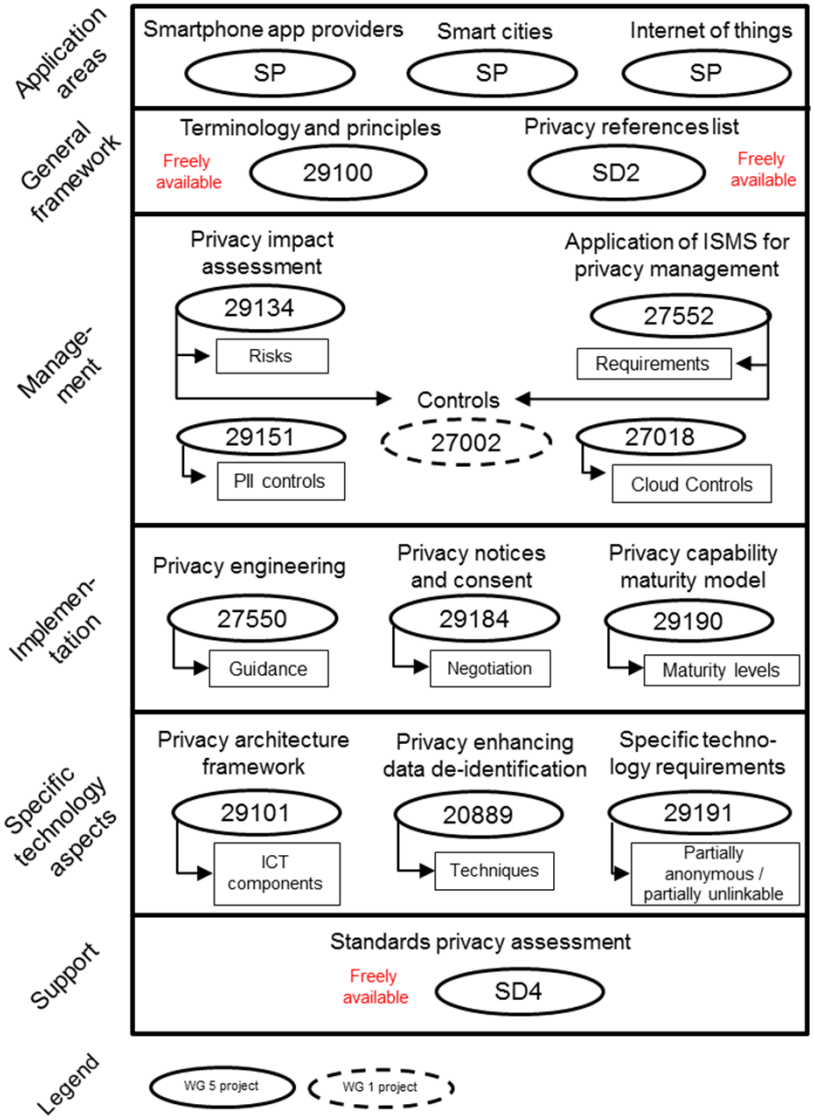
[EU2016]

EU General Data Protection Regulation (GDPR)
Art. 25 Data protection by design and by default

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An ***approved certification mechanism pursuant to Article 42*** may be used as an element to demonstrate compliance with the ***requirements set out in paragraphs 1*** and 2 of this Article.

[EU2016]

WG 5 Identity Management & Privacy Technologies
Privacy/PII standards in SC 27/WG 5 and WG 1 (2017-01)



Frameworks & Architectures (1)

- A framework for identity management (ISO/IEC 24760)
  - Part 1: Terminology and concepts (IS:2011, freely available, AMD DAM)
  - Part 2: Reference framework and requirements (IS:2015)
  - Part 3: Practice (IS:2016)
- Privacy framework (ISO/IEC 29100, IS:2011, freely available)
- Privacy architecture framework (ISO/IEC 29101, IS:2013)

Frameworks & Architectures (1)

- A framework for identity management (ISO/IEC 24760)
  - Part 1: Terminology and concepts (IS:2011, freely available, AMD DAM)
  - Part 2: Reference framework and requirements (IS:2015)
  - Part 3: Practice (IS:2016)
- **Privacy framework (ISO/IEC 29100, IS:2011, freely available)**
- Privacy architecture framework (ISO/IEC 29101, IS:2013)

ISO/IEC IS 29100:2011
Privacy principles

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
11. Privacy compliance

Frameworks & Architectures (1)

- **A framework for identity management (ISO/IEC 24760)**
  - **Part 1: Terminology and concepts (IS:2011, freely available, AMD DAM)**
  - Part 2: Reference framework and requirements (IS:2015)
  - Part 3: Practice (IS:2016)
- Privacy framework (ISO/IEC 29100, IS:2011, freely available)
- Privacy architecture framework (ISO/IEC 29101, IS:2013)

Identity Management (IdM)
An early approach

- „Fear not, for I have redeemed you;
  I have called you by name: you are mine."
  [Isaiah 43:1]

- „Μη φοβου· διοτι εγω σε ελυτρωσα,
  σε εκαλεσα με το ονομα σου· εμου εισαι"
  [Ησαιαν 43:1]

- „No temas, porque yo te he redimido,
  te he llamado por tu nombre; mío eres tú."
  [Isaías 43[1]]

- „Fürchte dich nicht, denn ich habe dich erlöst;
  ich habe dich bei deinem Namen gerufen; du bist mein!"
  [Jesaja 43,1]

Identity Management (IdM)
2 sides of a medal with enormous economic potential

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
- **Unified identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unify accounts
  - solve the problems of multiple passwords

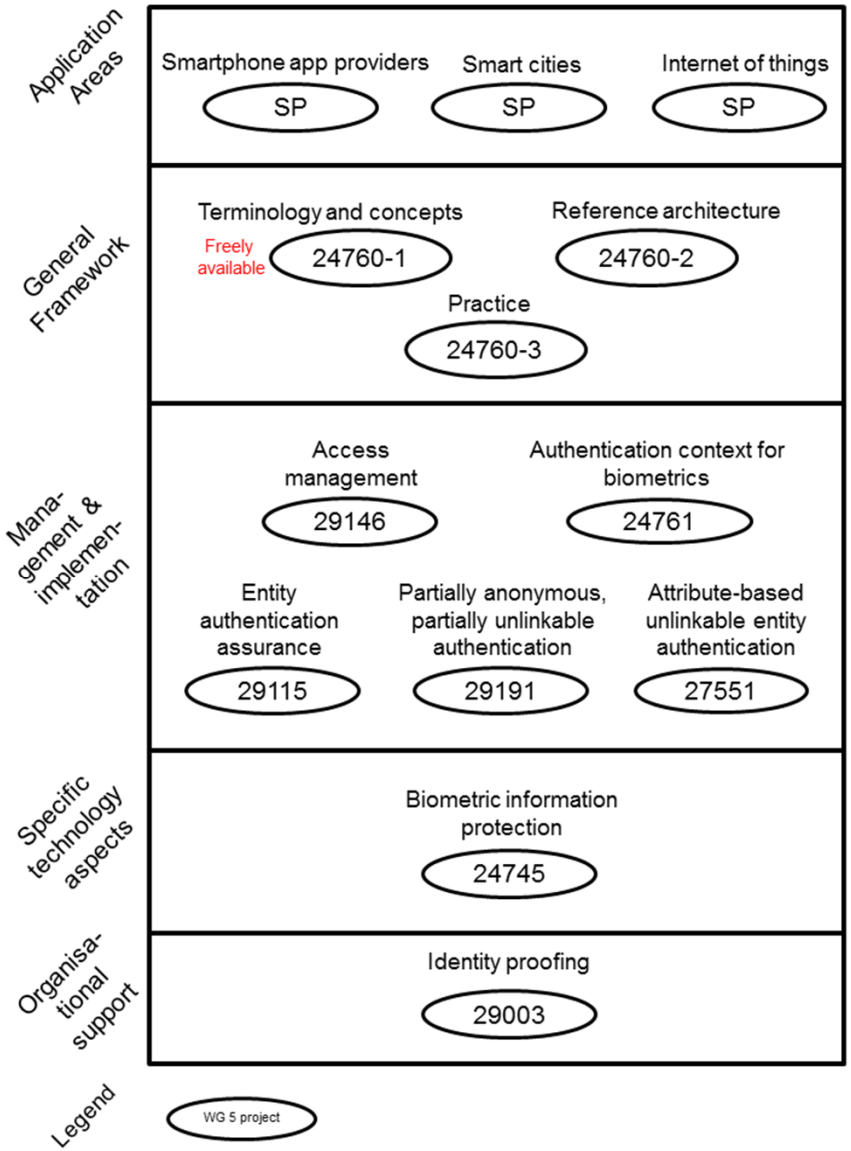
- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, 2ndLife names, …)
- **Partial identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

Identity Management (IdM)
2 sides of a medal with enormous economic potential

- **People** live their life
  - in different roles (professional, private, volunteer)
  - using different identities (pseudonyms): email accounts, SIM cards, eBay trade names, chat names, 2ndLife names, …)
- **Differentiated identities** help to
  - protect
    - privacy, especially anonymity
    - personal security/safety
  - enable reputation building at the same time
- **Identity management systems**
  - support users using role based identities
  - help to present the “right” identity in the right context

- **Organisations** aim to sort out
  - User Accounts in different IT systems
  - Authentication
  - Rights management
  - Access control
- **Partial identities** help to
  - ease administration
  - manage customer relations
- **Identity management systems**
  - ease single-sign-on by unify accounts
  - solve the problems of multiple passwords

WG 5 Identity Management & Privacy Technologies
Identity Management standards in SC 27/WG 5 (2017-01)



Frameworks & Architectures (1)

- A framework for identity management (ISO/IEC 24760)
  - Part 1: Terminology and concepts (IS:2011, freely available, AMD DAM)
  - Part 2: Reference framework and requirements (IS:2015)
  - Part 3: Practice (IS:2016)
- Privacy framework (ISO/IEC 29100, IS:2011, freely available)
- Privacy architecture framework (ISO/IEC 29101, IS:2013)

Frameworks & Architectures (2)

- Entity authentication assurance framework (ISO/IEC 29115, IS:2013, AMD DAM)
- A framework for access management (ISO/IEC 29146, IS:2016)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X.1085 | ISO/IEC 17922, FDIS) (formerly X.bhsm)
- Big data reference architecture – Part 4: Security and privacy fabric (ISO/IEC 20547-4, WD) (together with WG 4)

Protection Concepts

- Biometric information protection (ISO/IEC 24745, IS:2011)
- Requirements on partially anonymous, partially unlinkable authentication (ISO/IEC 29191, IS:2012)
- Privacy enhancing data de-identification techniques (ISO/IEC 20889, CD)
- Requirements for attribute-based unlinkable entity authentication (ISO/IEC 27551, WD)

Guidance on Context and Assessment

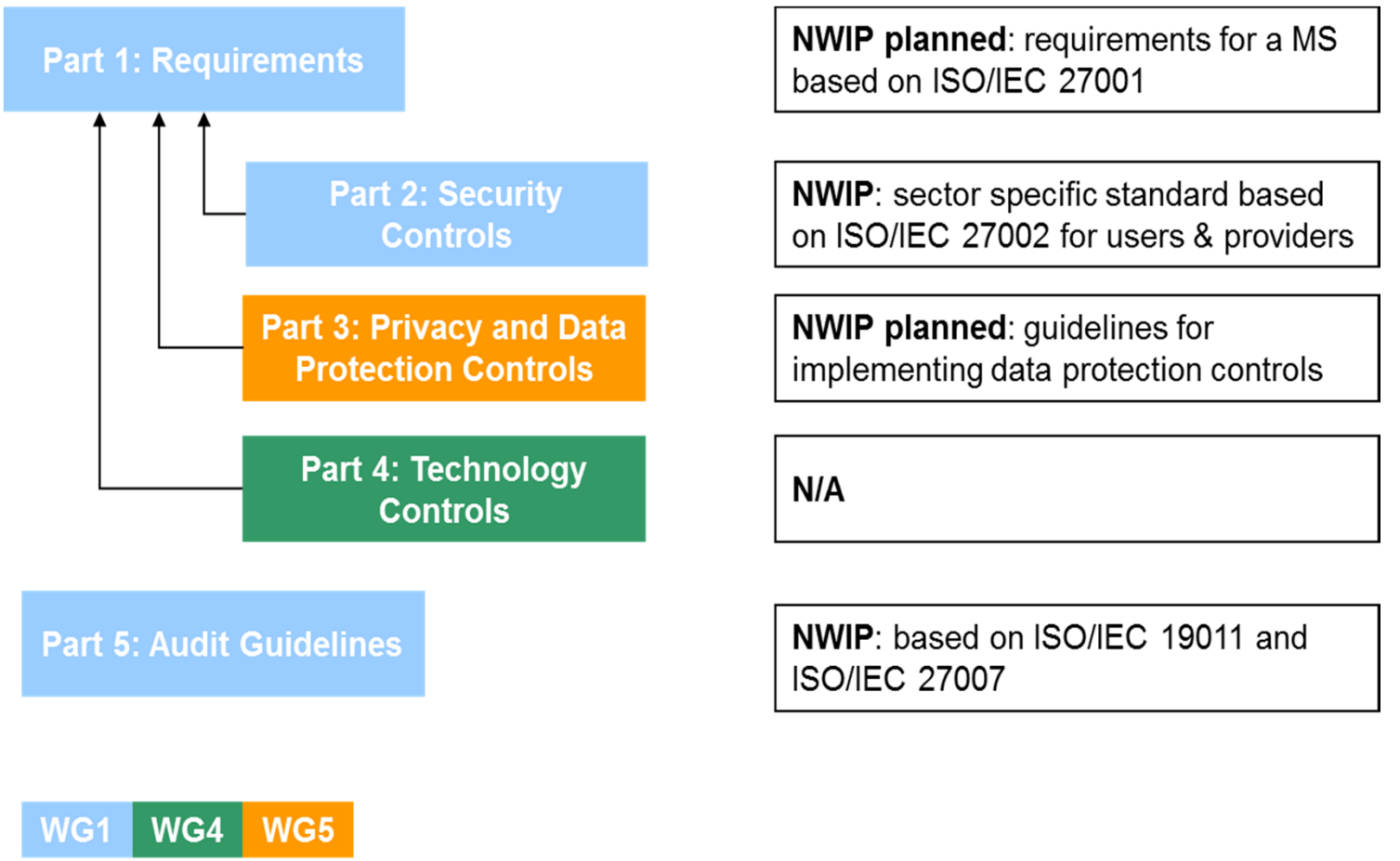
- Authentication context for biometrics
  (ISO/IEC 24761, IS:2009/Cor 1:2013, Revision CD)
- Privacy capability assessment model
  (ISO/IEC 29190, IS:2015)
- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
  (ISO/IEC 27018, IS:2014)
- Identity proofing (ISO/IEC 29003, DIS)
- Privacy impact assessment – methodology (ISO/IEC 29134, FDIS)
- Code of practice for PII protection (ITU-T X.1058 | ISO/IEC 29151, FDIS) (formerly X.gpim)
- Guidelines for online privacy notice and consent
  (ISO/IEC 29184, WD)
- Privacy engineering (ISO/IEC 27550, WD)
- Enhancement to ISO/IEC 27001 for privacy management – Requirements
  (ISO/IEC 27552, WD)

WG 5 Identity Management & Privacy Technologies Programme of Work

Guidance on Context and Assessment

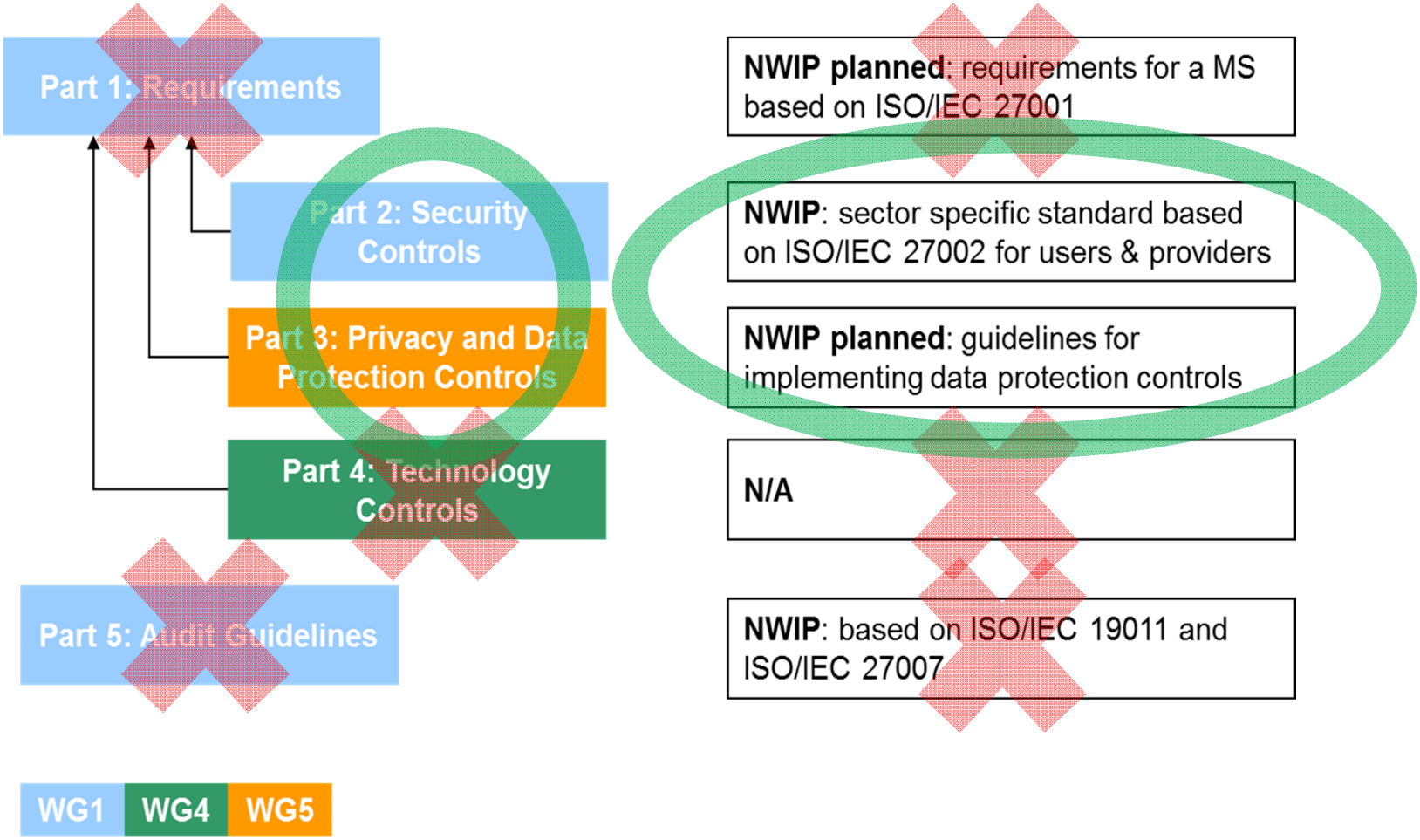
- Authentication context for biometrics (ISO/IEC 24761, IS:2009/Cor 1:2013, Revision CD)
- Privacy capability assessment model (ISO/IEC 29190, IS:2015)
- **Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018, IS:2014)**
- Identity proofing (ISO/IEC 29003, DIS)
- Privacy impact assessment – methodology (ISO/IEC 29134, FDIS)
- Code of practice for PII protection (ITU-T X.1058 | ISO/IEC 29151, FDIS) (formerly X.gpim)
- Guidelines for online privacy notice and consent (ISO/IEC 29184, WD)
- Privacy engineering (ISO/IEC 27550, WD)
- Enhancement to ISO/IEC 27001 for privacy management – Requirements (ISO/IEC 27552, WD)

ISO/IEC 27018 ”Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors “



[Figure thanks to Armin Wappenschmidt (Secunet)]

ISO/IEC 27018 ”Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors “



[Figure thanks to Armin Wappenschmidt (Secunet)]

New Work Item Proposal

- ISO/IEC 29100 Privacy framework – Amendment 1

Study Periods

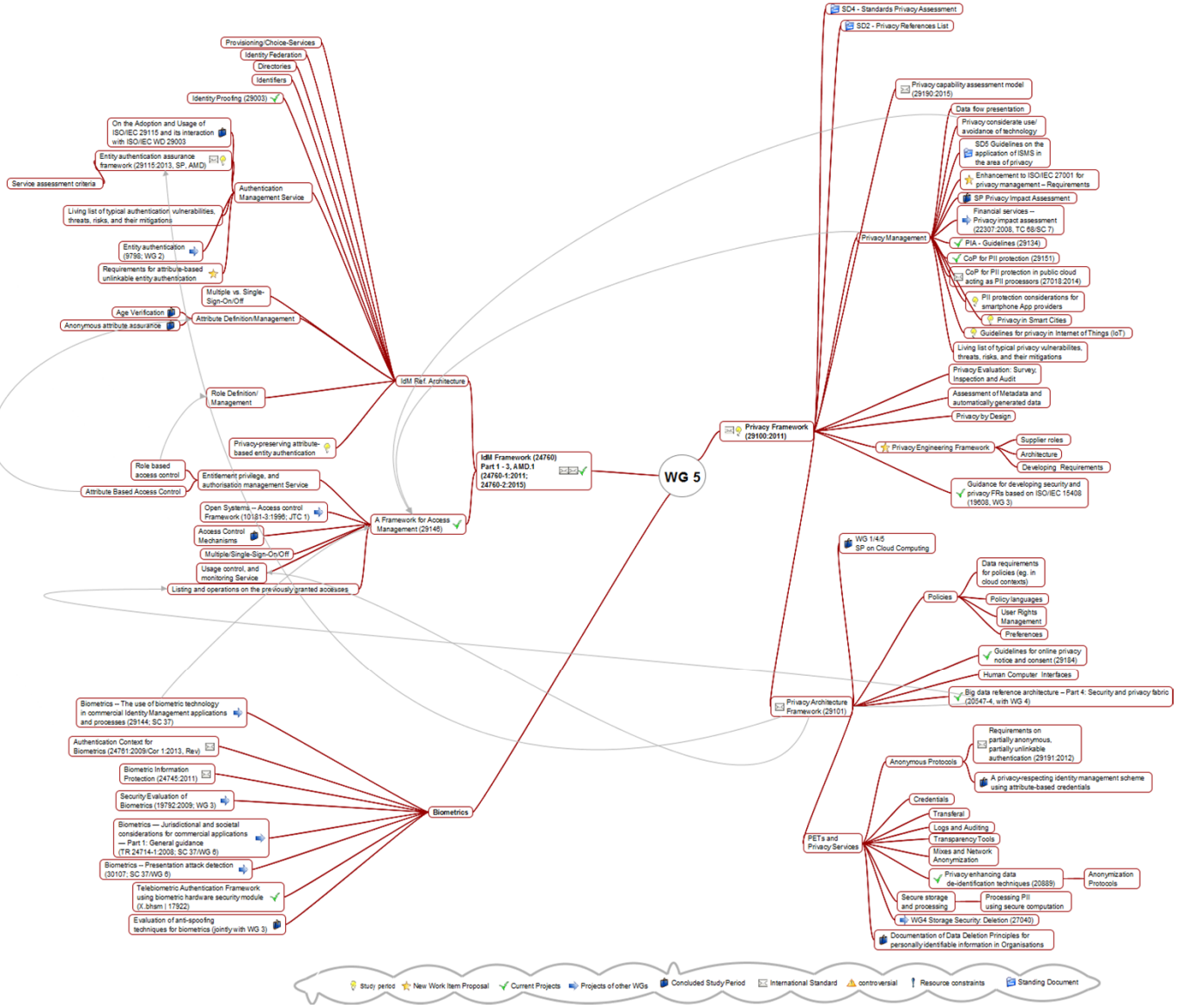
- PII protection considerations for smartphone App providers
- Privacy in smart cities
- Guidelines for privacy in Internet of Things (IoT)
- Editorial inconsistencies in ISO/IEC 29100 Information technology – Security techniques – Privacy framework
- Code of Practice solution for different types of PII processors
- Identity related standards landscape

Standing Documents

- WG 5 Roadmap
  (WG 5 SD1)
- Privacy References List
  (WG 5 SD2) (public)
- Standards Privacy Assessment (SPA)
  (WG 5 SD4) (public)

WG 5 Identity Management & Privacy Technologies Roadmap

ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies



Privacy by Design (PbD)

- PbD refers to the philosophy and approach of embedding privacy into the design specifications of various technologies.
- The concept is an example of value sensitive design, i.e., to take human values into account in a well defined matter throughout the whole process.

[Cavoukian2009]

Why Privacy by design?

- The alternative is:

Why Privacy by design?

- The alternative is:

Privacy by disaster

Why Privacy by design?

- The earlier requirements are considered ...
- ...the easier
  - They can be fulfilled
  - Fulfilment can be assessed

Adoption of Privacy by Design

- 2010: The International Conference of Data Protection and Privacy Commissioners unanimously endorsed PbD.
- 2012: The Federal Trade Commission (FTC) in the US, proposed a framework for business and policymakers with PbD as a core value.
- 2014: The European Commission announced that: ‘Privacy by Design’ and ‘privacy by default’ will become essential principles in EU data protection rules.

[CPDP2014]

Privacy-by-design
7 Foundational Principles

- Proactive not reactive
- Privacy as the Default setting
- Privacy Embedded into the Design
- Full Functionality
- End-to-End Security
- Visibility and Transparency
- Respect for User Privacy

[Cavoukian2009]

Privacy-by-design 7 Foundational Principles (in a bit more detail)

- **Proactive not Reactive**:
  - anticipates and prevents privacy invasive events before they happen
- **Privacy as the Default Setting:**
  - seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice
- **Privacy Embedded into Design:**
  - embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact
- **Full Functionality — Positive-Sum, not Zero-Sum:**
  - Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.
- **End-to-End Security — Full Lifecycle Protection:**
  - having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish.
- **Visibility and Transparency — Keep it Open:**
  - seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.
- **Respect for User Privacy — Keep it User-Centric:**
  - PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Privacy-by-design Principle 4

- **Full Functionality — Positive-Sum, not Zero-Sum:**
  - Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

Privacy-by-design Principle 4

Full Functionality — Positive-Sum, not Zero-Sum:

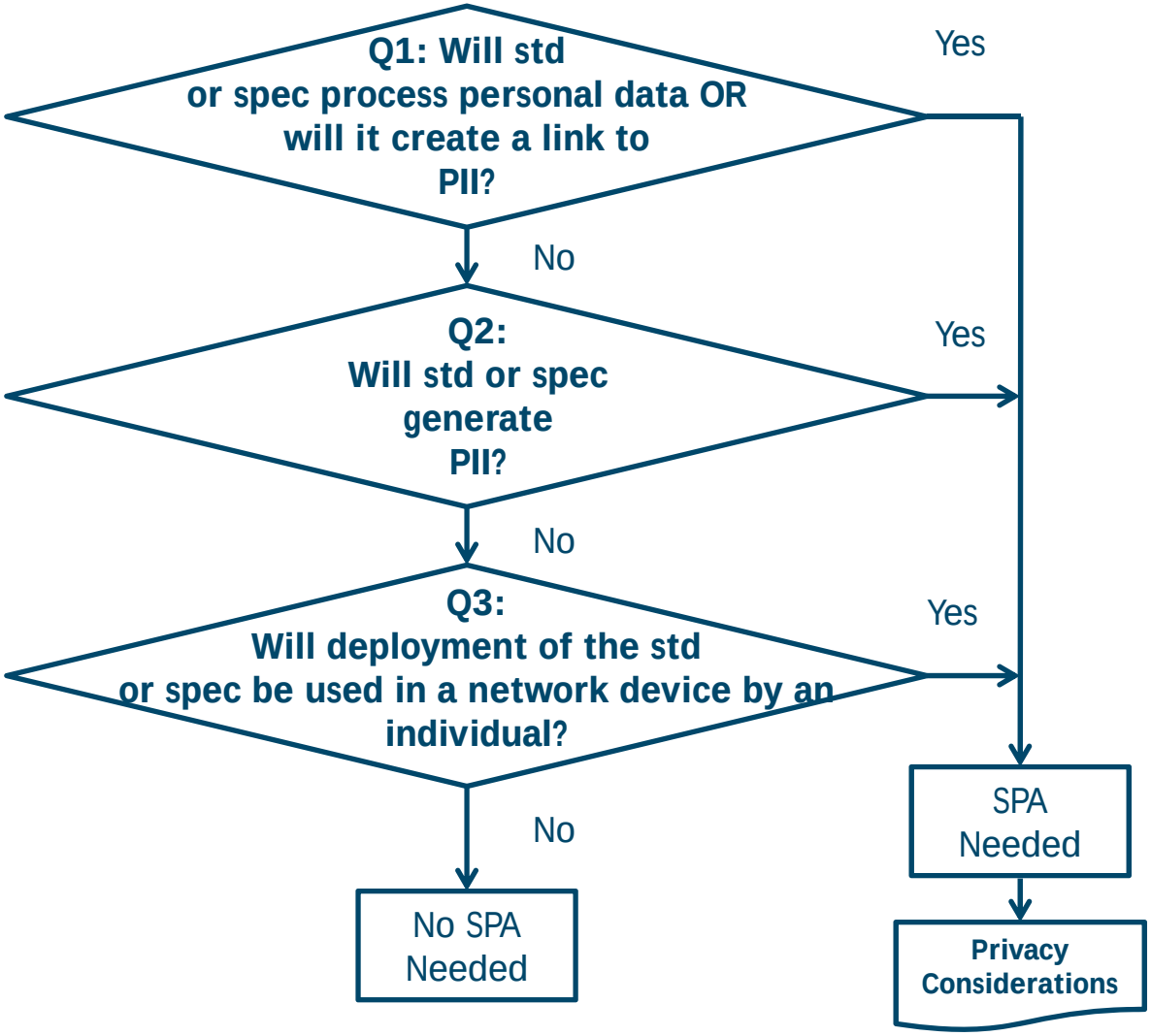
- *Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy *vs.* security, demonstrating that it *is* possible to have both.

[Cavoukian2009]

Full Functionality — Positive-Sum, not Zero-Sum:

- *Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy *vs.* security, demonstrating that it *is* often possible to have a combination of both.

Standards Privacy Assessment (SPA, SD4)
SPA or not SPA?



Standards Privacy Assessment (SPA, SD4)
Application at standards development milestones

- **Study Period and New Work Item Proposal**
  - Include an explanation of relevant privacy fundamentals, privacy goals and the SPA process
  - Identify a Privacy Champion in the project team

- **Working Draft**
  - As the project team creates functionality,
    - data flows are analyzed and categorized,
    - areas for Privacy Engineering are identified,
    - privacy requirements are identified,
    - threats are identified,
    - safeguards are defined, and
    - findings documented in SPA report.

- **Committee Draft or Proposed Draft TR**
  - The Standard or Specification Editor and project team
    - ensure that the Privacy Considerations address all issues and mitigation steps identified during the SPA process,

- **Draft International Standard/ Final Draft International Standard or Draft TR**
  - The ISO publication staff and Standard or Specification Editor
    - verify Privacy Considerations consistence with rules for International Standards

- **Maintenance of Standard/TR**
  - Deployment may lead to the reporting of privacy issues
  - To address in a timely manner through change requests

WG 5 Identity Management & Privacy Technologies
Liaisons and collaboration

- With organizations and committees dealing with specific requirements and guidelines for services and applications, e.g.:
  - ISO/IEC JTC 1
  - ISO
  - CEN
  - ETSI
  - ITU-T
  - Further organisations with specific application needs and/or expertise

WG 5 Identity Management & Privacy Technologies
Example Liaisons and collaboration – within ISO and IEC

- JTC 1/SC 17/WG 4
  - Integrated circuit card with contacts
- JTC 1/SC 37
  - Biometrics
- JTC 1/SC 38
  - Distributed application platforms and services (DAPS)
- ISO TC 215/WG 4
  - Health Informatics Security

WG 5 Identity Management & Privacy Technologies
Liaisons and collaboration – with ITU-T

- ITU-T SG 13
  - Future networks including mobile and NGN
- ITU-T SG 17
  - Security
- ETSI
  - TC Cyber

WG 5 Identity Management & Privacy Technologies
Example Liaisons and collaboration

- (ISC)2 - International Information Systems Security Certification Consortium
- ABC4Trust
- Article 29 Working Party of Data Protection Authorities in the European Union
- CSA (Cloud Security Alliance)
- ENISA (European Network and Information Security Agency)
- ISF (Information Security Forum)
- Kantara Initiative (succeeding Liberty Alliance)
- OpenID Foundation
- PRACTICE
- PRIPARE
- The International Conference of Data Protection and Privacy Commissioners

WG 5 Identity Management & Privacy Technologies
Recent and next meetings

- 2016-10-23 – 2016-10-27 Abu Dhabi (UAE) WG 5 Meeting

- 2017-04-18 – 2017-04-22 Hamilton (New Zealand) WG 5 Meeting
- 2017-04-24 – 2017-04-25 Hamilton (New Zealand) SC 27 Plenary

- 2017-10-30 – 2017-11-03 Berlin (Germany) WG 5 Meeting

- 2018-04-09 – 2018-04-13 TBD (China) WG 5 Meeting
- 2018-04-16 – 2018-04-17 TBD (China) SC 27 Plenary

WG 5 Identity Management & Privacy Technologies
Further Reading

- www.din.de/en/meta/jtc1sc27/downloads
  - SD6 Glossary of IT Security Terminology
  - SD7 Catalogue of SC 27 Standards & Projects
  - WG 5/SD2 Privacy Documents References List
  - WG 5/SD4 Standards Privacy Assessment (SPA)

- www.iso.org/obp/ui
  - ISO Online Browsing Platform (OBP)
- http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
  - Freely available standards, e.g.
    - ISO/IEC 24760-1:2011 “A framework for identity management -- Part 1: Terminology and concepts”
    - ISO/IEC 29100:2011 “Privacy framework”

Kai.Rannenberg@m-chair.de

Conclusions & Outlook

- Several projects completed
- Many more to do …
- Every new project is
  - a new challenge …
  - … and a learning (bubble-bursting) experience …
- Privacy by design is a leading paradigm, but making it a standard in itself seems difficult.

WG 5 Identity Management & Privacy Technologies

References I

[Cavoukian2009] Privacy by Design The 7 Foundational Principles, https://web.archive.org/web/*/https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf

[CPDP2014] Privacy by Design: Effective Privacy Management in the Victorian public sector, Commissioner for Privacy and Data Protection (CPDP), 2014, https://www.cpdp.vic.gov.au/pdf/background_paper.pdf

[EU2016] European Union: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); Official Journal of the European Union L 119/1, 4.5.2016, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf