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

Standards for identity management and privacy

Work in ISO/IEC JTC 1/SC 27/WG 5

2022-09-28

[kai.rannenberg@m-chair.de]
Convenor WG 5

WG 5 Identity Management & Privacy Technologies
Agenda

- WG 5 within SC 27
- Standards and standardisation projects
  - Functional perspective
  - Management system perspective
  - Regulation perspective
- Meeting schedules
- Conclusions & outlook

WG 5 Identity Management & Privacy Technologies
Agenda

- **WG 5 within SC 27**
- **Standards and standardisation projects**
  - **Functional perspective**
  - **Management system perspective**
  - **Regulation perspective**
- **Meeting schedules**
- **Conclusions & outlook**

SC 27 “Security, cybersecurity and privacy protection”

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

SC 27 Plenary

Chairmanship
Chair: Andreas WOLF (DIN)
Support: Laura LINDSAY (ANSI)

Secretariat
Committee Manager: Sobhi MAHMOUD (DIN)

CAG
Convenor: Andreas WOLF (DIN)
Support: Laura LINDSAY (ANSI)

JAG IEC/TC 65 - JTC 1/SC 27
Convenor: Ingo WEBER (IEC/TC 65)
Co-Convenor: Andreas WOLF (SC 27)

WG 1 Information Security Management Systems
Convenor: Edward HUMPHREYS (BSI)
Support: Pablo CORONA (DGN)

WG 2 Cryptography and Security Mechanisms
Convenor: Takeshi CHIKAZAWA (JISC)
Support: Hirotaka YOSHIDA (JISC)

WG 3 Security Evaluation, Testing and Specification
Convenor: Miguel BAÑÓN (UNE)
Support: Naruki KAI (JISC)

WG 4 Security Controls and Services
Convenor: Johann AMSENGA (ILNAS)
Support: François LOREK (AFNOR)

WG 5 Identity Management and Privacy Technologies
Convenor: Kai RANNENBERG (DIN)
Support: Jan SCHALLABÖCK (DIN)

JWG 4 Security, privacy and identity for Blockchain and DTL
Convenor: Julien BRINGER (AFNOR) (TC 307)
Co-Convenor: Sal FRANCOMACARO (SC 27)

JWG 6 Cybersecurity requirements and evaluation activities for connected vehicle devices
Convenor: Di TANG (SC 27)
Co-Convenor: Gido SCHARFENBERGER-FABIAN (ISO/TC 22/SC 32)

AG 2 Trustworthiness
Convenor: Johann AMSENGA (ILNAS)
Support: Faud KHAN (SCC)

AG 3 Concepts and Terminology
Convenor: Elzbieta ANDRUKIEWICZ (PKN)
Support: Joanne KNIGHT (NZSO)

AG 5 Strategy
Convenor: Jean-Pierre QUEMARD (AFNOR)
Support: tbd.

AG 6 Operations
Convenor: Qin QIU (SAC)
Support: tbd.

AG 7 Communications and Outreach
Convenor: Edward HUMPHREYS (BSI)
Support: Taewan PARK (KATS)

WG 5 “ISO/IEC JTC 1/SC 27/WG 5 Identity Management & Privacy Technologies” in SC 27 “Security, cybersecurity and privacy protection”

SC 27 Plenary

Chairmanship
Chair: Andreas WOLF (DIN)
Support: Laura LINDSAY (ANSI)

Secretariat
Committee Manager: Sobhi MAHMOUD (DIN)

CAG
Convenor: Andreas WOLF (DIN)
Support: Laura LINDSAY (ANSI)

JAG IEC/TC 65 - JTC 1/SC 27
Convenor: Ingo WEBER (IEC/TC 65)
Co-Convenor: Andreas WOLF (SC 27)

WG 1 Information Security Management Systems
Convenor: Edward HUMPHREYS (BSI)
Support: Pablo CORONA (DGN)

WG 2 Cryptography and Security Mechanisms
Convenor: Takeshi CHIKAZAWA (JISC)
Support: Hirotaka YOSHIDA (JISC)

WG 3 Security Evaluation, Testing and Specification
Convenor: Miguel BAÑÓN (UNE)
Support: Naruki KAI (JISC)

WG 4 Security Controls and Services
Convenor: Johann AMSENGA (ILNAS)
Support: François LOREK (AFNOR)

WG 5 Identity Management and Privacy Technologies
Convenor: Kai RANNENBERG (DIN)
Support: Jan SCHALLABÖCK (DIN)

JWG 4 Security, privacy and identity for Blockchain and DTL
Convenor: Julien BRINGER (AFNOR) (TC 307)
Co-Convenor: Sal FRANCOMACARO (SC 27)

JWG 6 Cybersecurity requirements and evaluation activities for connected vehicle devices
Convenor: Di TANG (SC 27)
Co-Convenor: Gido SCHARFENBERGER-FABIAN (ISO/TC 22/SC 32)

AG 2 Trustworthiness
Convenor: Johann AMSENGA (ILNAS)
Support: Faud KHAN (SCC)

AG 3 Concepts and Terminology
Convenor: Elzbieta ANDRUKIEWICZ (PKN)
Support: Joanne KNIGHT (NZSO)

AG 5 Strategy
Convenor: Jean-Pierre QUEMARD (AFNOR)
Support: tbd.

AG 6 Operations
Convenor: Qin QIU (SAC)
Support: tbd.

AG 7 Communications and Outreach
Convenor: Edward HUMPHREYS (BSI)
Support: Taewan PARK (KATS)

A legacy Information (Security) Management Paradigm …

"Collect as much information as possible – and check about a use for it later"

… which is NOT Best Practice …

"Collect as much information as possible – and check about a use for it later"

… and NOT privacy friendly

"Collect as much information as possible – and check about a use for it later"

Security & Privacy aim to address systems and their design in a holistic way

© Rumen Milkow (TaxiBerlin)

"We don't want a piece of the cake, we want the whole bakery."

„Wir wollen nicht ein Stück vom Kuchen, wir wollen die ganze Bäckerei."

[In German on the Yorck Bridges, Berlin]

WG 5 Identity Management & Privacy Technologies
Agenda

- WG 5 within SC 27
- Standards and standardisation projects
  - Functional perspective
  - Management system perspective
  - Regulation perspective
- Meeting schedules
- Conclusions & outlook

WG 5 Identity Management & Privacy Technologies
Programme of work (2008-03 – all in development)

Frameworks & Architectures

- A Framework for Identity Management (ISO/IEC 24760)
- A Privacy framework (ISO/IEC 29100)
- A Privacy Reference Architecture (ISO/IEC 29101)
- A Framework for Access Management (New Work Item Initiative)

Protection Concepts

- Biometric template protection (ISO/IEC 24745)
- Access Control Mechanisms (Study Period)

Guidance on Context and Assessment

- Authentication Context for Biometrics (ISO/IEC 24761)
- Entity Authentication Assurance (ISO/IEC 29115)
- Privacy Capability Maturity Models (Study Period)

WG 5 Identity Management & Privacy Technologies Programme of work

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

Frameworks & Architectures

- A framework for identity management (ISO/IEC 24760 (Parts 1-4); IS:2011, Revision 2019; IS:2015, Rev CD; IS:2016, DAmd; AWI)
- Privacy framework (ISO/IEC 29100:2011; Amendment 1:2018)
- Privacy architecture framework (ISO/IEC 29101:2018)
- Entity authentication assurance framework (ISO/IEC 29115:2013, Amd PWI)
- A framework for access management (ISO/IEC 29146:2016/Amd 1:2022)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X.1085 | ISO/IEC 17922:2017) (formerly X.bhsm)
- Big data reference architecture – Part 4: Security and privacy fabric (ISO/IEC 20547-4:2020) (together with WG 4)
- User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences (ISO/IEC 27556, Pub)
- Privacy enhancing data de-identification framework (ISO/IEC 27559, FDIS)

Protection Concepts

- Biometric information protection (ISO/IEC 24745:2011, Revision 2022)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191:2012)
- Privacy enhancing data de-identification terminology and classification of techniques (ISO/IEC 20889:2018)
- Online privacy notice and consent (ISO/IEC 29184:2020)
- Requirements for attribute-based unlinkable entity authentication (ISO/IEC 27551:2021)
- Security requirements for authentication using biometrics on mobile devices (ISO/IEC 27553 (Parts 1-2); Pub; AWI)
- Guidelines on personally identifiable information deletion (ISO/IEC 27555:2021)
- Consent record information structure (ISO/IEC TS 27560, WD)

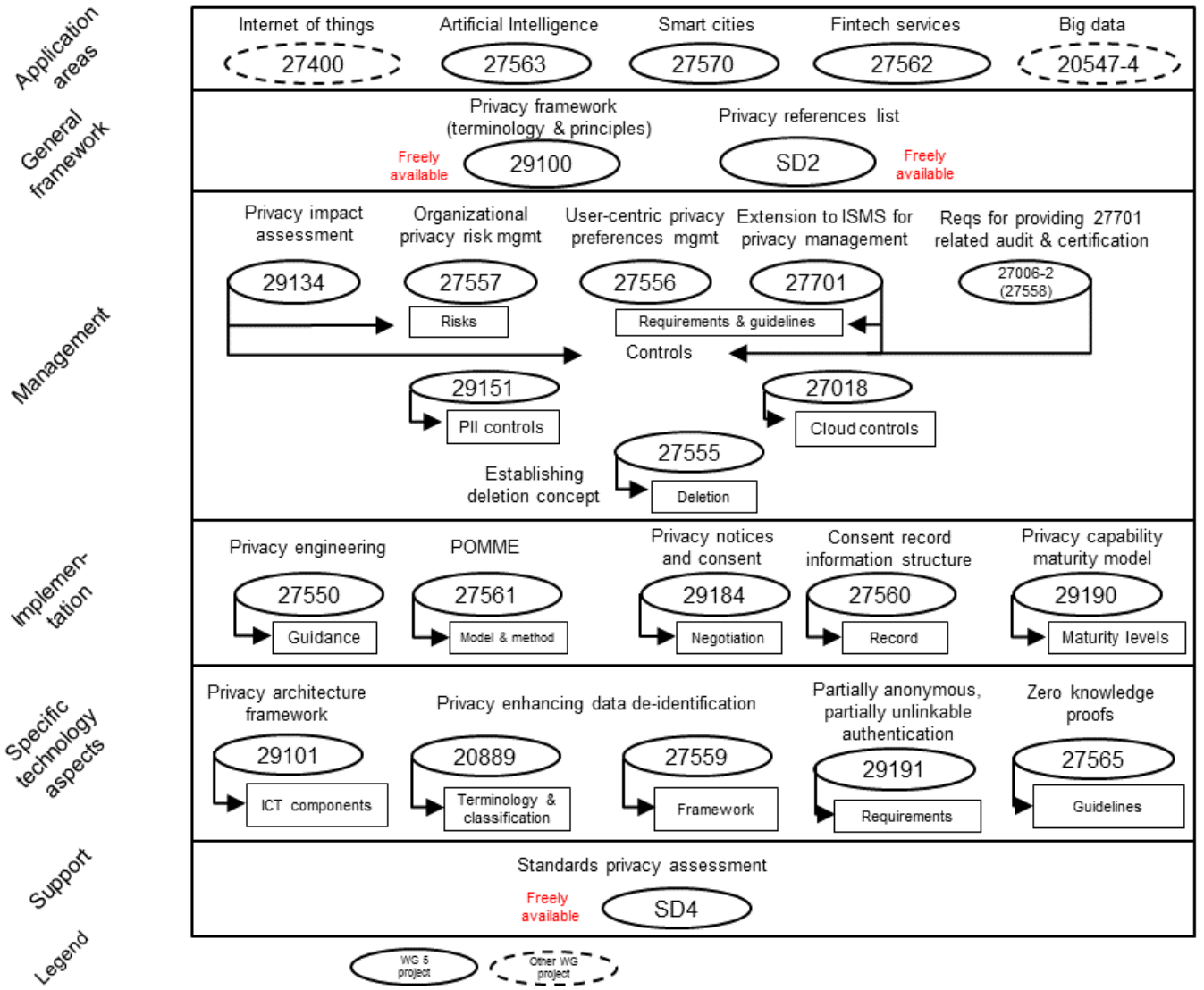
Guidance on Context and Assessment

- Authentication context for biometrics (ISO/IEC 24761:2009/Cor 1:2013, Revision 2019)
- Privacy capability assessment model (ISO/IEC 29190:2015)
- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018:2014, Revision 2019)
- Identity proofing (ISO/IEC TS 29003:2018)
- Privacy impact assessment – methodology (ISO/IEC 29134:2017, DAmd)
- Code of practice for PII protection (ITU-T X.1058| ISO/IEC 29151:2017) (formerly X.gpim)
- Privacy engineering for system life cycle processes (ISO/IEC TR 27550:2019)
- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management – Requirements and guidelines (ISO/IEC 27701:2019 (formerly 27552))
- Privacy guidelines for Smart Cities (ISO/IEC TS 27570:2021)
- Application of ISO 31000 for assessment of identity management-related risk (ISO/IEC 27554, CD)
- Organizational privacy risk management (ISO/IEC 27557, FDIS)
- Requirements for bodies providing audit and certification of information security management systems – Part 2: Privacy information management systems (ISO/IEC TS 27006-2:2021 (formerly 27558), Revision IS CD)
- Privacy operationalisation model and method for engineering (POMME) (ISO/IEC 27561, CD)
- Privacy guidelines for fintech services (ISO/IEC 27562, WD)
- Security and privacy in artificial intelligence use cases (ISO/IEC TR 27563, DTR)
- Guidelines on privacy preservation based on zero knowledge proofs (ISO/IEC 27565, WD)

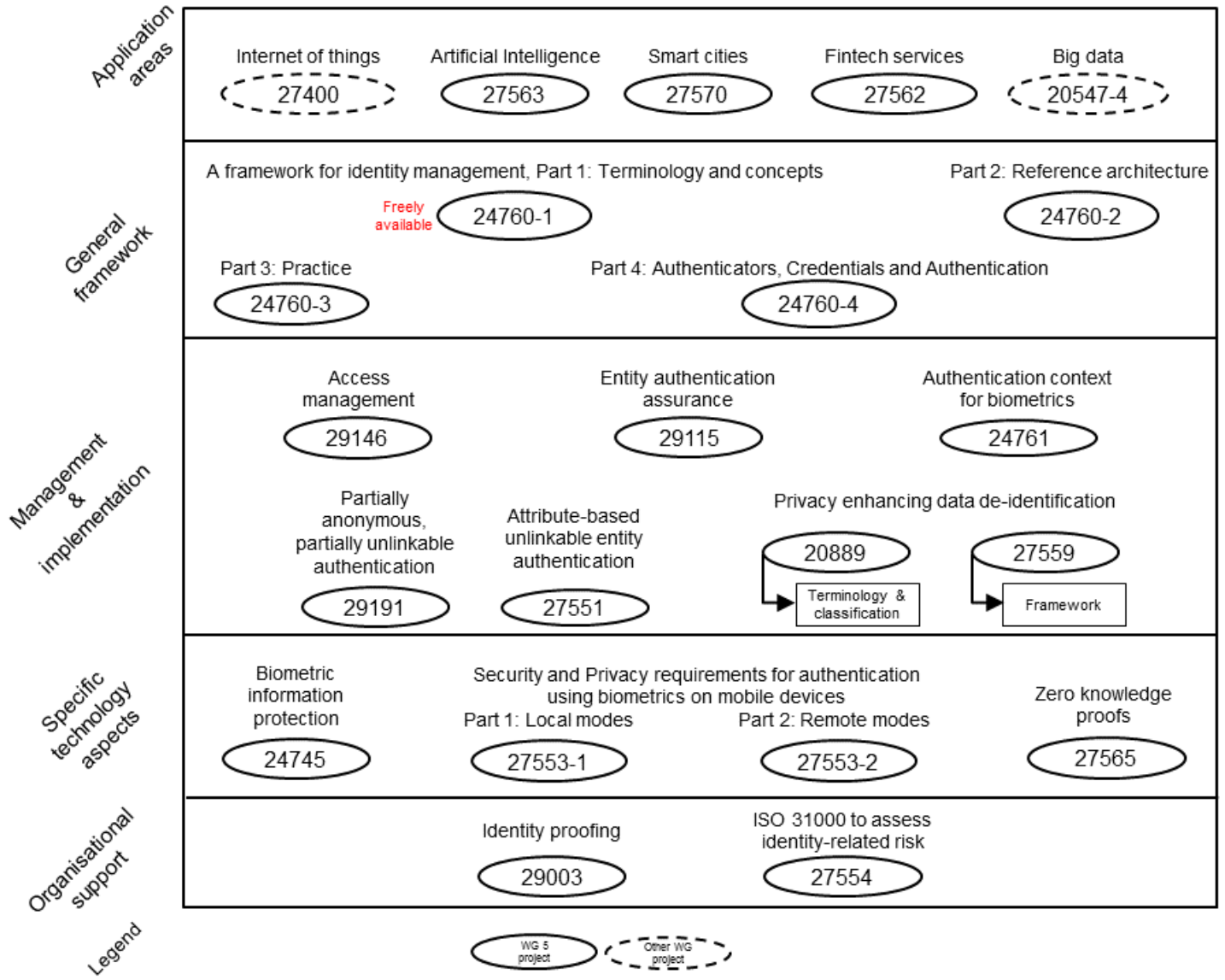
WG 5 Identity Management & Privacy Technologies
Agenda

- WG 5 within SC 27
- Standards and standardisation projects
  - Functional perspective
  - Management system perspective
  - Regulation perspective
- Meeting schedules
- Conclusions & outlook

WG 5 Identity Management & Privacy Technologies
Privacy/PII standards mainly in SC 27/WG 5 (2022-09)



WG 5 Identity Management & Privacy Technologies
Identity Management standards mainly in SC 27/WG 5 (2022-09)

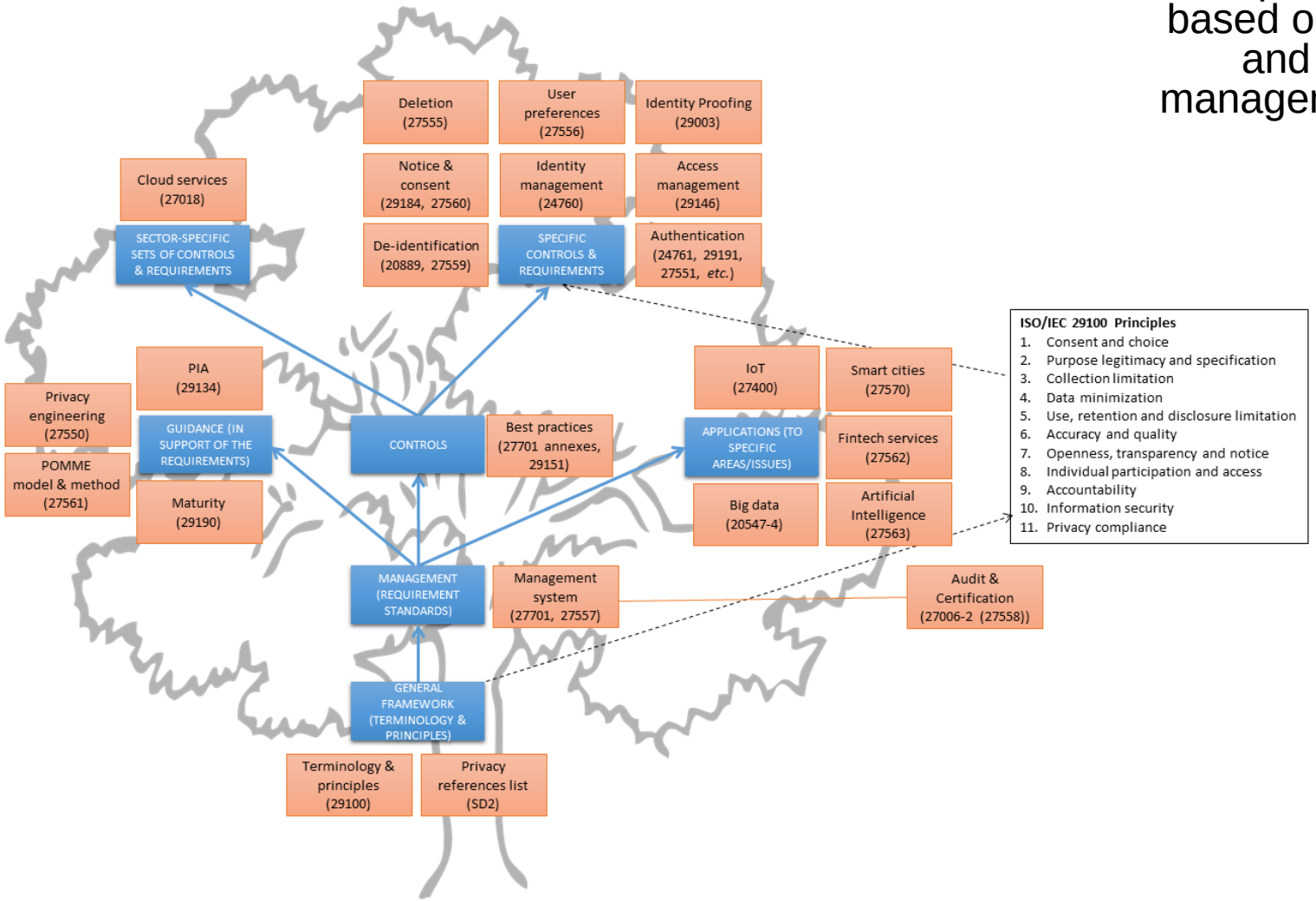


WG 5 Identity Management & Privacy Technologies
Agenda

- WG 5 within SC 27
- Standards and standardisation projects
  - Functional perspective
  - Management system perspective
  - Regulation perspective
- Meeting schedules
- Conclusions & outlook

WG 5 Identity Management & Privacy Technologies
Privacy/PII standards mainly in SC 27/WG 5 (2022-09)

A perspective based on principles and related management issues



WG 5 Identity Management & Privacy Technologies
Agenda

- WG 5 within SC 27
- Standards and standardisation projects
  - Functional perspective
  - Management system perspective
  - Regulation perspective
- Meeting schedules
- Conclusions & outlook

WG 5 projects in the context of the GDPR (preliminary assessment)

Art 4: Definition of personal data and pseudonymisation	
Art 5: Principles	
Art 6 & 7: Consent Art. 13 & 14: Information	
Art 15 & 20: Access and data portability	
Art 25: Data protection by design and by default	
Art 28: Processor	
Art 33 & 34: Breach notification	
Art 35: DPIA	
Art 40: Codes of Conduct	
Art. 42 & 43: Certification	

WG 5 projects in the context of the GDPR (preliminary assessment 2022)

Art 4: Definition of personal data and pseudonymisation	**20889:2018** Privacy enhancing data de-identification terminology and classification of techniques **27559 FDIS** Privacy-enhancing data de-identification framework
Art 5: Principles	**29100:2011** Privacy Principles (Amendment 1:2018)
Art 6 & 7: Consent Art. 13 & 14: Information	**29184:2020** Guidelines for online privacy notices and consent **AWI TS 27560** Consent record information structure
Art 15 & 20: Access and data portability	*Not yet available in WG 5*
Art 25: Data protection by design and by default	**TR 27550:2019** Privacy Engineering **WG 5 SD4** Standards Privacy Assessment (SPA) **24760**: **2011/19** A framework for identity management
Art 28: Processor	**27018:2014/19** Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
Art 33 & 34: Breach notification	Not available as such in WG 5, but related to **27701:2019** Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines **27557 FDIS** Organizational privacy risk management
Art 35: DPIA	**29134:2017, DAmd** Privacy Impact Assessment – Methodology
Art 40: Codes of Conduct	*n/a, but standards bodies can function as fora for defining these codes*
Art. 42 & 43: Certification	**27701:2019** Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines **TS 27006-2:2021** Requirements for bodies providing audit and certification of information security management systems – Part 2: Privacy information management systems (Revision towards IS ongoing)

WG 5 Identity Management & Privacy Technologies
Agenda

- WG 5 within SC 27
- Standards and standardisation projects
  - Functional perspective
  - Management system perspective
  - Regulation perspective
- Meeting schedules
- Conclusions & outlook

WG 5 Identity Management & Privacy Technologies
Recent and next meetings

2019-10-14 – 2019-10-18	Paris (France)	WG 5 Meeting
…		
2022-03-28 – 2020-04-01	virtual	WG 5 Meeting
2022-04-04 – 2020-04-08	virtual	WG 5 Meeting
2022-04-11 – 2022-04-13	virtual	SC 27 Plenary
2022-09-26 – 2022-09-30	**hybrid, Luxembourg**	**WG 5 Meeting**
2022-10-04 – 2022-10-06	**virtual**	**WG 5 Meeting**
2022-10-12 – 2022-10-13	**virtual**	**SC 27 Plenary**
2023-01-09 – 2023-01-11	if needed, virtual	WG 5 Meeting
2023-04-17 – 2023-04-21	**hybrid, Redmond (US)**	**WG 5 Meeting**
2023-04-24 – 2023-04-25	**hybrid, Redmond (US)**	**SC 27 Plenary**

WG 5 Identity Management & Privacy Technologies
Agenda

- WG 5 within SC 27
- Standards and standardisation projects
  - Functional perspective
  - Management system perspective
  - Regulation perspective
- Meeting schedules
- Conclusions & outlook

Conclusions & outlook

- Several projects completed, so a landscape is developing
- Many more projects to do …
- Every new project is a …
  - new global challenge
  - (cultural) learning experience

WG 5 Identity Management & Privacy Technologies
Further reading

- www.din.de/en/meta/jtc1sc27/downloads
  - SD6 Glossary of IT Security Terminology
  - SD11 Overview of SC 27
  - 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 24760-1:2019 “A framework for identity management -- Part 1: Terminology and concepts”
    - ISO/IEC 29100:2011 “Privacy framework”

Kai.Rannenberg@m-chair.de

Thank you very much for your attention and interest

Thanks a lot to Luxembourg for enabling this WG 5 meeting!