Work and Projects in ISO/IEC JTC 1/SC 27/WG 5 "Identity Management & Privacy technologies"

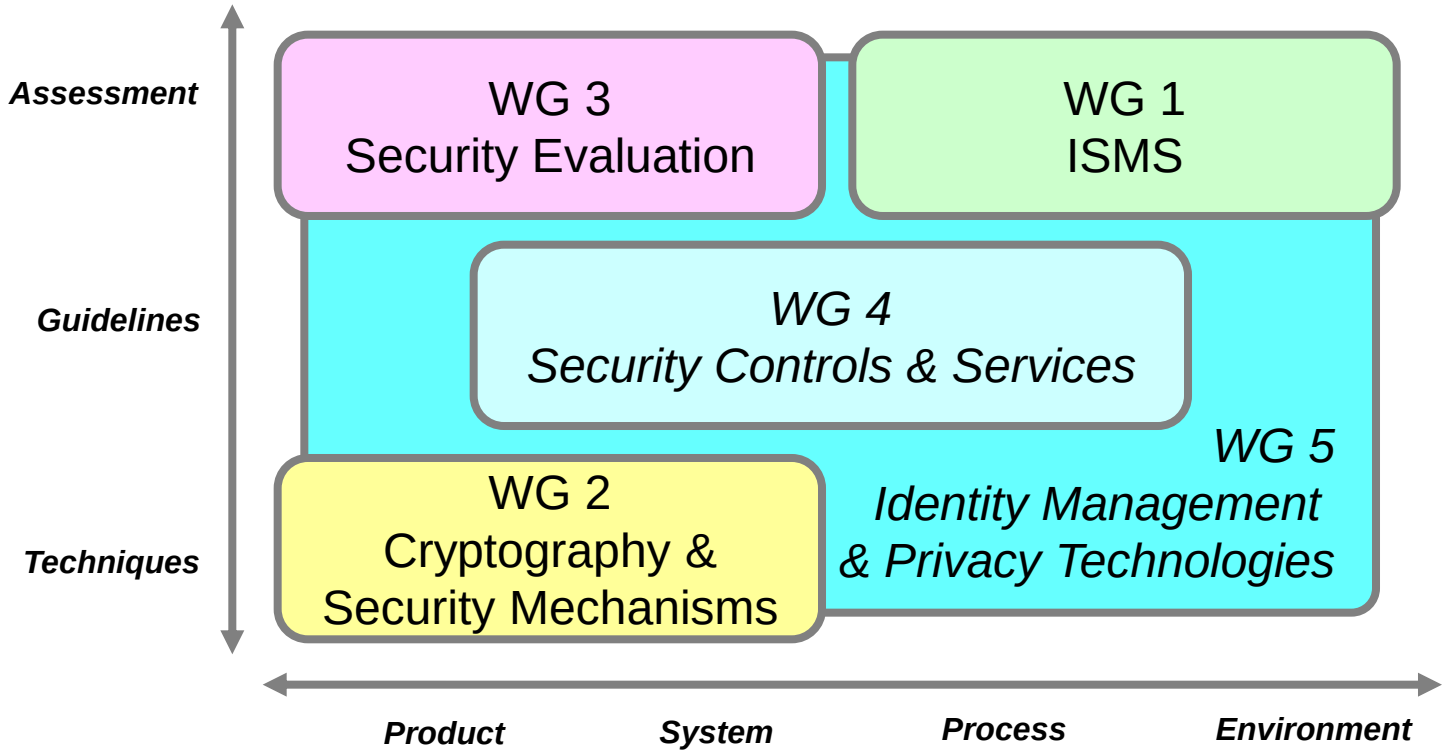
30th Plenary meeting of the Consultative Committee of the Convention for the Protection of Individuals with Regard To Automatic Processing of Personal Data
2013-10-17

Convenor WG 5
[kai.rannenberg@m-chair.net]
Deutsche Telekom Chair for
"Mobile Business & Multilateral Security"
Goethe University Frankfurt, Germany

WG 5 Identity Management & Privacy Technologies Agenda

- WG 5 within SC 27
- A bit of history pre WG 5
- Scope of WG 5
- WG 5 project overview
- ISO standards development processes
- An example for the approach of WG 5
- Projects in detail
- WG 5 Standing documents
- Liaison organisations
- Meeting schedule

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



WG 5 Identity Management & Privacy Technologies History

October 2003

JTC 1 Plenary established

- JTC 1 Study Group on Privacy Technologies (SGPT)
- for one year period of time (until October 2004) to identify standardization needs

October 2004

JTC 1 Plenary resolved to

- disband SGPT
- assign to SC 27 further activities in the Privacy Technologies area such as
  - a further inventory
  - a report back to the November 2006 JTC 1 Plenary

WG 5 Identity Management & Privacy Technologies History

SC 27 activities (in response to JTC 1's request from October 2004)

- **October 2004**
  - Study Period on Identity Management established
- **May 2005**
  - Study Period on Privacy established
  - New Work Item Proposal: A framework for identity management (ISO/IEC 24760)
- **May 2006**
  - New Working Group 5 on Identity Management and Privacy Technologies established
  - Two new Work Item Proposals
    - A privacy framework (ISO/IEC 29100)
    - A privacy reference architecture (ISO/IEC 29101)

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, IS, CD, WD)
- Privacy Framework (ISO/IEC 29100, IS)
- Privacy Architecture Framework (ISO/IEC 29101, IS)
- Entity Authentication Assurance Framework (ISO/IEC 29115, IS)
- A Framework for Access Management (ISO/IEC 29146, CD)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X.1085 | ISO/IEC 17922, WD) (formerly X.bhsm)

Protection Concepts

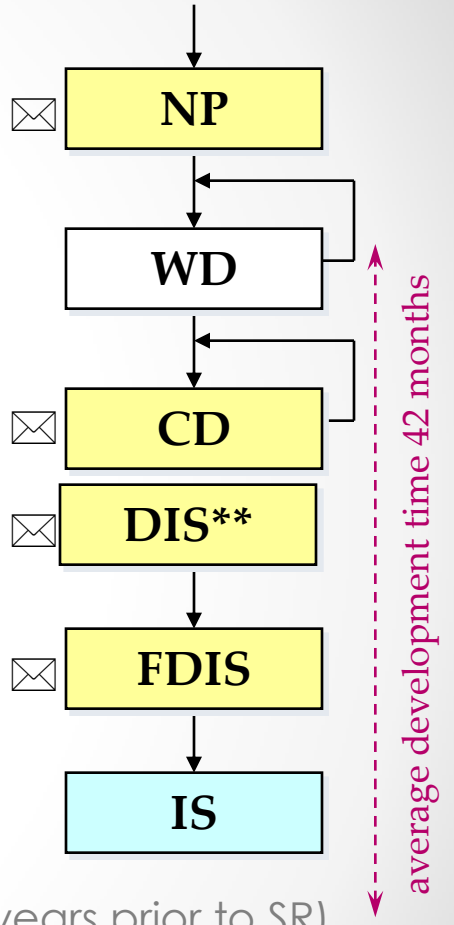
- Biometric information protection (ISO/IEC 24745, IS)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, IS)

Guidance on Context and Assessment

- Authentication Context for Biometrics (ISO/IEC 24761, IS)
- Privacy Capability Assessment Model (ISO/IEC 29190, CD)
- Code of practice for data protection controls for public cloud computing services (ISO/IEC 27018, CD) -> Code of practice for PII protection in public clouds acting as PII processors
- Identity Proofing (ISO/IEC 29003, WD)
- Privacy impact assessment – methodology (ISO/IEC 29134, WD)
- Code of practice for the protection of personally identifiable information (ISO/IEC 29151, WD)

ISO processes - Project Development

- Maturity level / state of standardization
  - Study Period / New Project (NP)
    - 3 month NP letter ballot*)
  - Working Draft (WD)
  - Committee Draft (CD)
    - 3 month CD ballot(s)
  - Draft International Standard (DIS)
    - 3 month DIS ballot (+ 2 months f. translation)
  - Final Draft International Standard (FDIS)
    - 2 month FDIS ballot
    - no more comments at this stage
  - International Standard (IS)
    - pre-review 3 years after publication (subsequent per 2 years prior to SR)
    - review every 5 years (via the Systematic Review at JTC 1 Level)
    - or after 'defect report'



✉*) one vote per P-member

**) by 100% approval ONLY (no negative votes) a FDIS LB can be skipped and a DIS text (after incorporating editorial changes) can be published.

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, …)
- **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

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
- **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

Frameworks & Architectures

- A Framework for Identity Management (ISO/IEC 24760)
  - Part 1: Terminology and concepts (IS, freely available)
  - Part 2: Reference framework and requirements (CD)
  - Part 3: Practice (WD)
- Privacy Framework (ISO/IEC 29100, IS)
- Privacy Architecture Framework (ISO/IEC 29101, IS)

Frameworks & Architectures

- Entity Authentication Assurance Framework (ISO/IEC 29115, IS)
- A Framework for Access Management (ISO/IEC 29146, CD)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X.1085 | ISO/IEC 17922, WD) (formerly X.bhsm)

WG 5 Identity Management & Privacy Technologies Programme of Work

Protection Concepts

- Biometric information protection (ISO/IEC 24745, IS)
- Requirements on partially anonymous, partially unlinkable authentication (ISO/IEC 29191, IS)

Guidance on Context and Assessment

- Authentication Context for Biometrics (ISO/IEC 24761, IS)
- Privacy Capability Assessment Model (ISO/IEC 29190, CD)
- Code of practice for data protection controls for public cloud computing services (ISO/IEC 27018, CD) -> Code of practice for PII protection in public clouds acting as PII processors
- Identity Proofing (ISO/IEC 29003, WD)
- Privacy impact assessment – methodology (ISO/IEC 29134, WD)
- Code of practice for the protection of personally identifiable information (ISO/IEC 29151, WD)

Study Periods

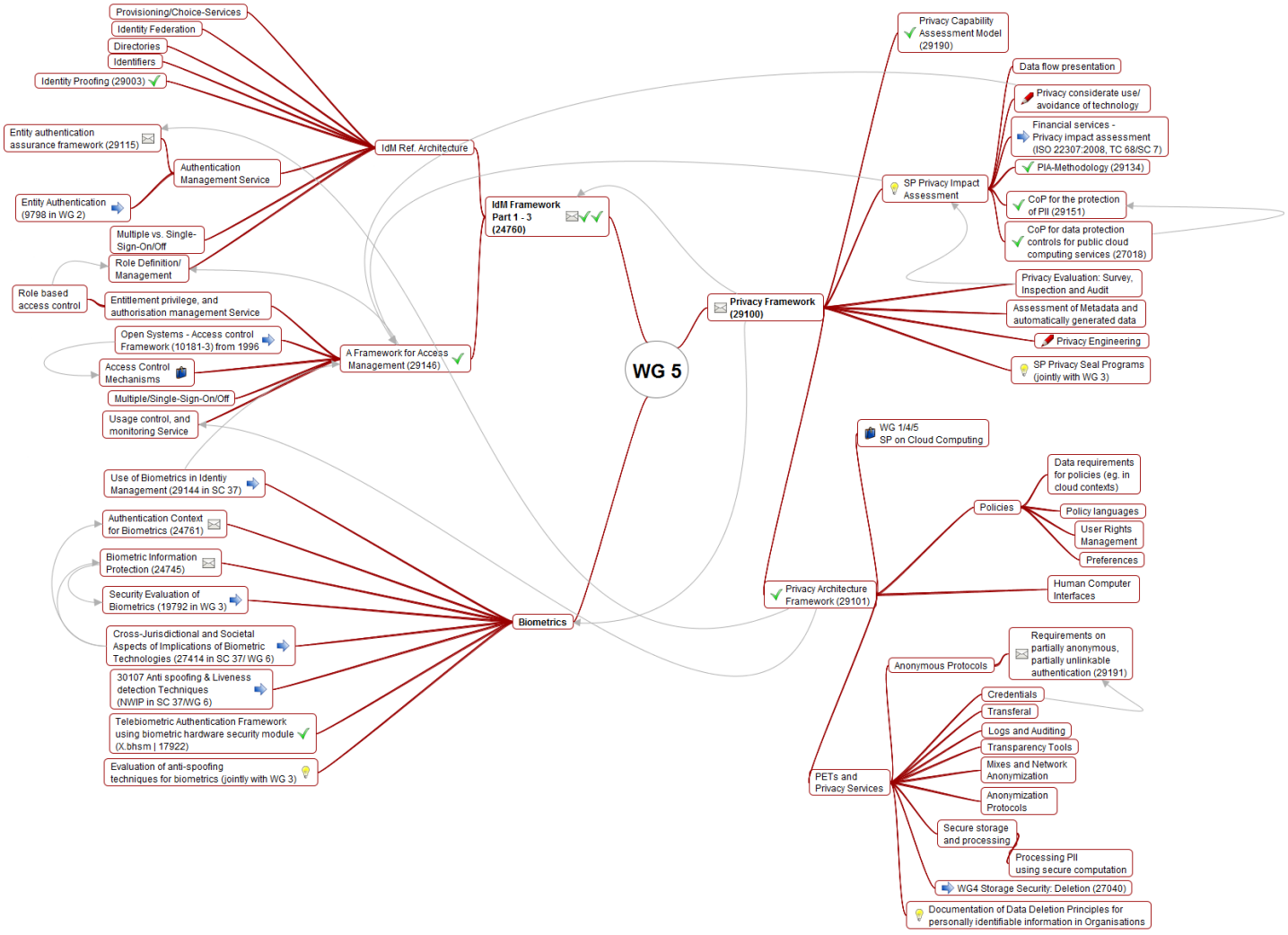
- Privacy Impact Assessment
- Security evaluation of anti-spoofing techniques for biometrics (together with WG 3)
- Privacy seal programs (together with WG 3)
- Documentation of data deletion principles for personally identifiable information in organisations

Standing Documents

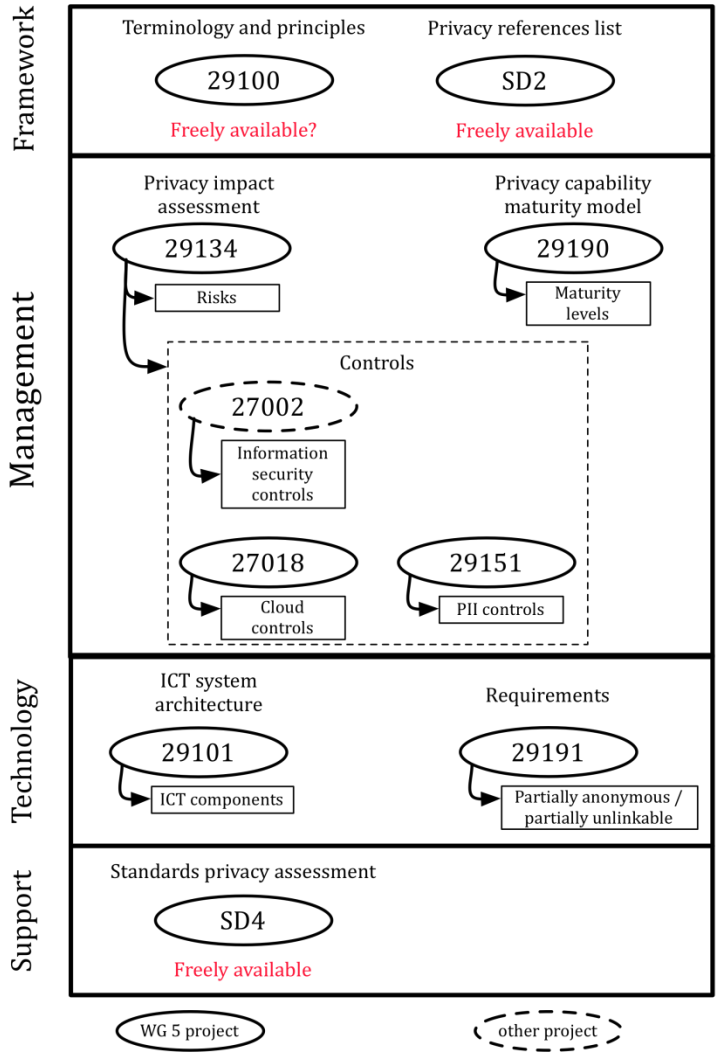
- WG 5 Roadmap (WG 5 SD1)
- Privacy References List (WG 5 SD2) (public)
- Harmonized Vocabulary Effort (WG 5 SD3)
- Standards Privacy Assessment (SPA) (WG 5 SD4)

WG 5 Identity Management & Privacy Technologies Roadmap

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



WG 5 Identity Management & Privacy Technologies
Privacy/PII standards in SC 27/WG 5 and elsewhere



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

- CEN TC 225
  - AIDC Technologies
- ITU-T SG 13
  - Future networks including mobile and NGN
- ITU-T SG 17
  - Security
- ITU-T JCA Cloud
  - Cloud Computing Privacy Aspects

WG 5 Identity Management & Privacy Technologies Liaisons and collaboration

- ABC4Trust
- Article 29 Working Party of Data Protection Authorities in the European Union
- Cloud Security Alliance (CSA)
- ENISA (European Network and Information Security Agency)
- EUDCA (European Data Centre Association)
- FIDIS (Future of Identity in the Information Society)
- Kantara Initiative (succeeding Liberty Alliance)
- PICOS (Privacy in Community Services)
- The International Conference of Data Protection and Privacy Commissioners

WG 5 Identity Management & Privacy Technologies
Next Meetings

- 2013-10-21 – 2013-10-25 Songdo (Korea): WG 5 Meeting

- 2014-04-07 – 2014-04-11 Hong Kong: WG 5 Meeting
- 2014-04-14 – 2014-04-15 Hong Kong: SC 27 Plenary

- 2014-10-13 – 2014-10-17 Ottawa (Canada): WG 5 Meeting

- Probably 2015-05-04 – 2015-05-08 TBD (Malaysia): WG 5 Meeting
- Probably 2015-05-11 – 2015-05-12 TBD (Malaysia): SC 27 Plenary

WG 5 Identity Management & Privacy Technologies Further Reading

- www.jtc1sc27.din.de/en
  - SD6 Glossary of IT Security Terminology
  - SD7 Catalogue of SC 27 Standards & Projects
  - WG 5/SD2 Privacy Documents References List
- 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”

Kai.Rannenberg@m-chair.net

WG 5 Identity Management & Privacy Technologies