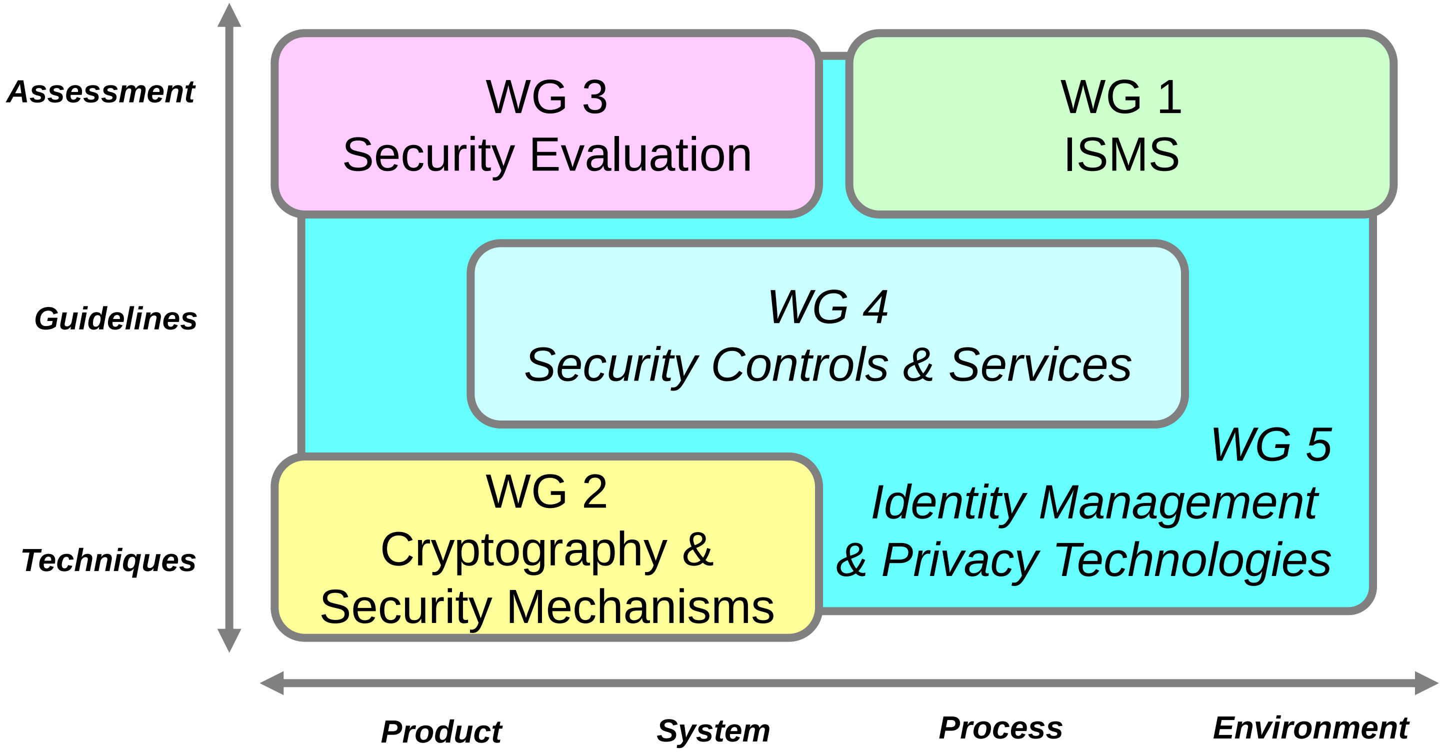
A framework for identity management (ISO/IEC 24760)

Information technology — Security techniques — **A framework for identity management**

Part 1: Terminology and concepts
Part 2: Reference architecture and requirements

Prof. Dr. Kai Rannenberg
Deutsche Telekom Chair for Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.net

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 Programme of Work

Frameworks & Architectures

- A Framework for Identity Management (ISO/IEC 24760, IS, WD, WD)
- Privacy Framework (ISO/IEC 29100, IS)
- Privacy Architecture Framework (ISO/IEC 29101, CD)
- Entity Authentication Assurance Framework (ISO/IEC 29115 / ITU-T X.1254 (formerly X.eaa), DIS)
- A Framework for Access Management (ISO/IEC 29146, WD)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X.bhsm | ISO/IEC 17922, WD)

Protection Concepts

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

Guidance on Context and Assessment

- Authentication Context for Biometrics (ISO/IEC 24761, IS)
- Privacy Capability Assessment Model (ISO/IEC 29190, WD)
- Code of practice for data protection controls for public cloud computing services (ISO/IEC 27018, WD)
- Identity Proofing (NWIP)
- Privacy impact assessment – methodology (NWIP)

Frameworks & Architectures

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

Frameworks & Architectures

- Entity Authentication Assurance Framework (ISO/IEC 29115 / ITU-T X.1254 (formerly X.eaa), FDIS)
- A Framework for Access Management (ISO/IEC 29146, WD)
- Telebiometric authentication framework using biometric hardware security module (ITU-T X.bhsm | ISO/IEC 17922, WD)

WG 5 Identity Management & Privacy Technologies Programme of Work

- A Framework for Identity Management (ISO/IEC 24760)
  - Part 1: Terminology and concepts (IS:2011)
  - Part 2: Reference framework and requirements (WD)
  - Part 3: Practice (WD)

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

Identity Concepts
Working Definitions

- ***Identity:***
  The characteristics (attributes) representing an acting entity
- ***Partial identity:***
  A subset of the characteristics of an identity

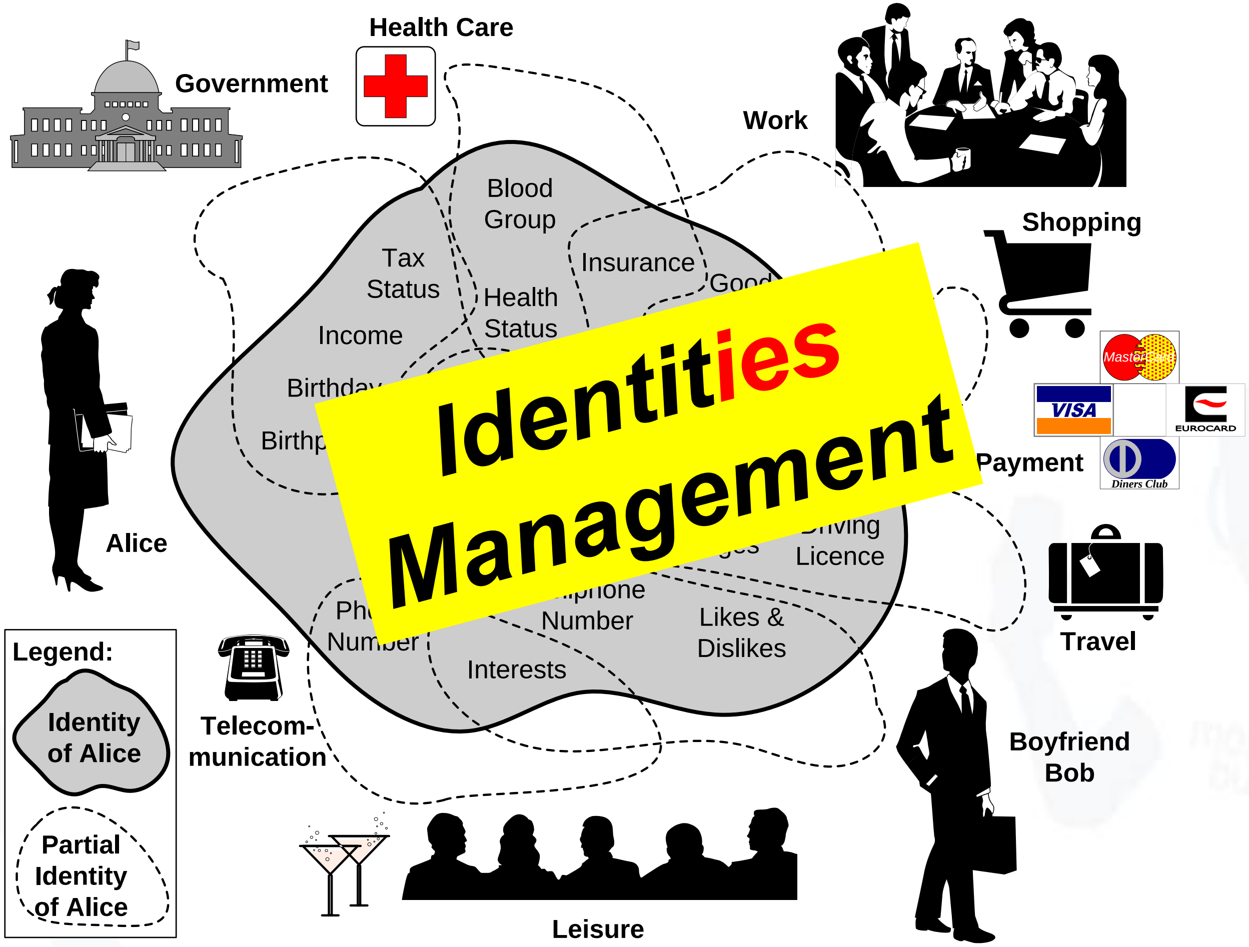
- ***ISO/IEC 24760:1 "A framework for identity management - Part 1 Terminology and concepts":***
  - **Identity** (partial identity): Set of **attributes** related to an **entity**

Why are partial identities important ?

- Different partial identities are assigned to and abstracted from an entity.
- The identity of an entity consists of partial identities distributed over different partners of the entity.

[BaMe05]

Partial Identities



Based on [Clauß, Köhntopp 2001]

Stages in the Identity lifecycle

- International standard ISO/IEC 24760-1:2011 defines the stages in the lifecycle of an identity in a particular domain

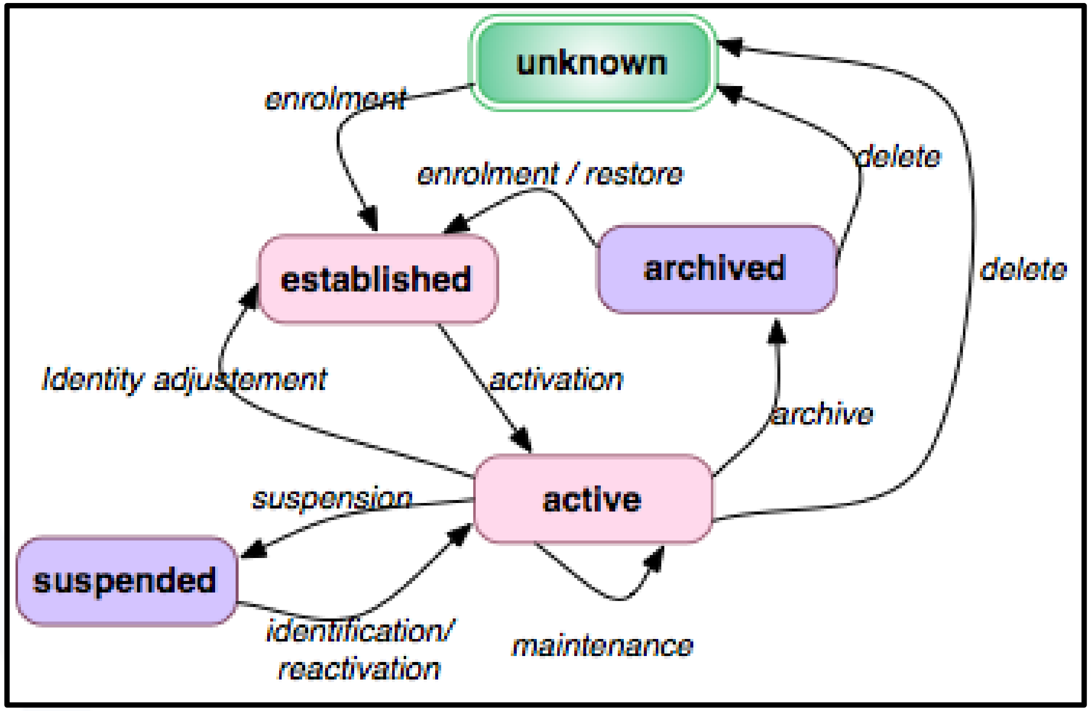


Figure 1 –Identity lifecycle.

Part 1: Table of Content

Nr.	Topic
1	Scope
2	Normative references
3	Terms and definitions
4	Symbols and abbreviated terms
5	Identity
6	Attributes
6	Managing Identity Information
7	Identification
8	Authentication
9	Maintenance
10	Implementation Aspects
11	Privacy

Part 2: Table of Content

Nr.	Topic	Page
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	2
5	Reference architecture	2
6	Requirements	10
7	Annex A Legal and regulatory aspects (Informative)	14

Clauses 5 & 6
Reference architecture & Requirements

Nr.	Topic	Page
5	Reference architecture	2
5.1	Overview	2
5.2	Actors	5
5.3	Processes	7
5.4	Components	8
6	Requirements	10
6.1	Access to identity information	10
6.2	Identity information lifecycle management	11
6.3	Quality of identity information	12
6.3.1	General	12
6.3.2	Information adjustment	12
6.4	Time reference	12
6.5	IT security	13

5.1 Overview – Possible flows of identity information (1/3)

process	actors			
	source		recipient	
	actor	action	actor	action
Identification	Principal	Presents credentials Allows capture of identity information	Verifier	Determines information to be retrieved from register and its level of assurance Performs verification
	Identity-information authority	Provides level of assurance for identity information		
	Identity register	Provide additional identity information		
Registration	Identity-information provider	Provides verified information for storage	Identity register	Stores information indexed by reference identifier.
	Reference-identifier generator	If first registration, provides new unique identifier		
Authentication	Relying party	Specifies required levels of assurance for particular identity information and the mechanism(s) to validate assertions	Identity-information authority	Associates specified levels of assurance and mechanisms with relying party.
	Identity-information authority	Provides assertion on the level of assurance of identity information	Relying party	Validates assertion
Generating reference identifier	Identity-information provider	Requests reference identifier	Reference-identifier generato	Generates reference identifier
	Principal	Provides identity information to be used as reference identifier	Reference-identifier generator	Validates suitability of provided identy information as reference identifier. Generates reference identifier.
	Reference-identifier generator	Provides generated reference identifier.	Identity-information provider	Associates reference identifier with other identity information

5.1 Overview – Possible flows of identity information (2/3)

process	actors			
	source		recipient	
	actor	action	actor	action
Revocation	Identity management authority	Decides on identity revocation	Identity register	Stores information to effect status change
	Identity-information provider	Initiates provisioning of the revocation	Relying party	Applies updated information to its service process
Activation	Identity-management authority	Activates new identity	Identity register	Stores information to effect status change
Provisioning	Relying party	Requests provisioning services	Identity management authority	Grants or denies provision service, specifies conditions.
			Identity-information provider	Records relying party as receiver of provisioning service
	Identity-information provider	Transmits identity information	Relying party	Applies updated information to its service process
	Identity-information authority	Augments identity information with assertion on the level of assurance	Relying party	Confirms the assertions meet its requirements for level of assurance
Identity adjustment	Identity management authority	Checks for identity information updates	Principal	Informs on information updates
	Principal	Notifies the availability of new or changed identity information	Identity management authority	If new information is relevant, initiates identity adjustment,
	Identity management authority	Authorizes information update	Identity register	Identity management authority
	Identity-information provider	Defines updated identity information	Identity register	Stores updated information indexed by reference identifier
		Provisions updated information.	Relying party	Applies updated information to its service process.
Identity information processing	Identity-information provider	Apply information processing operations	Identity-information provider	Retains results
			Register	Stores result of processing, possibly updating information in one or more identities.

5.1 Overview – Possible flows of identity information (3/3)

process	actors			
	source		recipient	
	actor	action	actor	action
Information-processing authorization	Identity management authority	Informs on identity information processing. Solicits authorization for processing operations	Principal	Grants or denies information processing operations
	Principal	Requests information on identity processing.	Identity management authority	Provides requested information
Auditing	Identity management authority	Defines actions to be logged, incidents to be reported.	All actors	Incorporate definitions in process implementation
	Principal	Registers complaint	Auditor	Investigates complaint
	Identity management authority	Maintains log of management actions		Reviews logs and incidents
	Identity register	Maintains log of data access operations		
	Identity-information provider	Maintains log of identity information requests and information provisioning activities		
	Identity-information authority	Maintains log of assurance assertions provided Reports on incidents		
	Auditor	Reports on findings. Recommends changes.	Identity management authority	Adjust policies and procedures to implement any recommended changes.

5.4 Identity Management system components

- Figure 1 presents the components is an identity management system.
- The figure also shows where an identity management system interfaces with actors and principals.

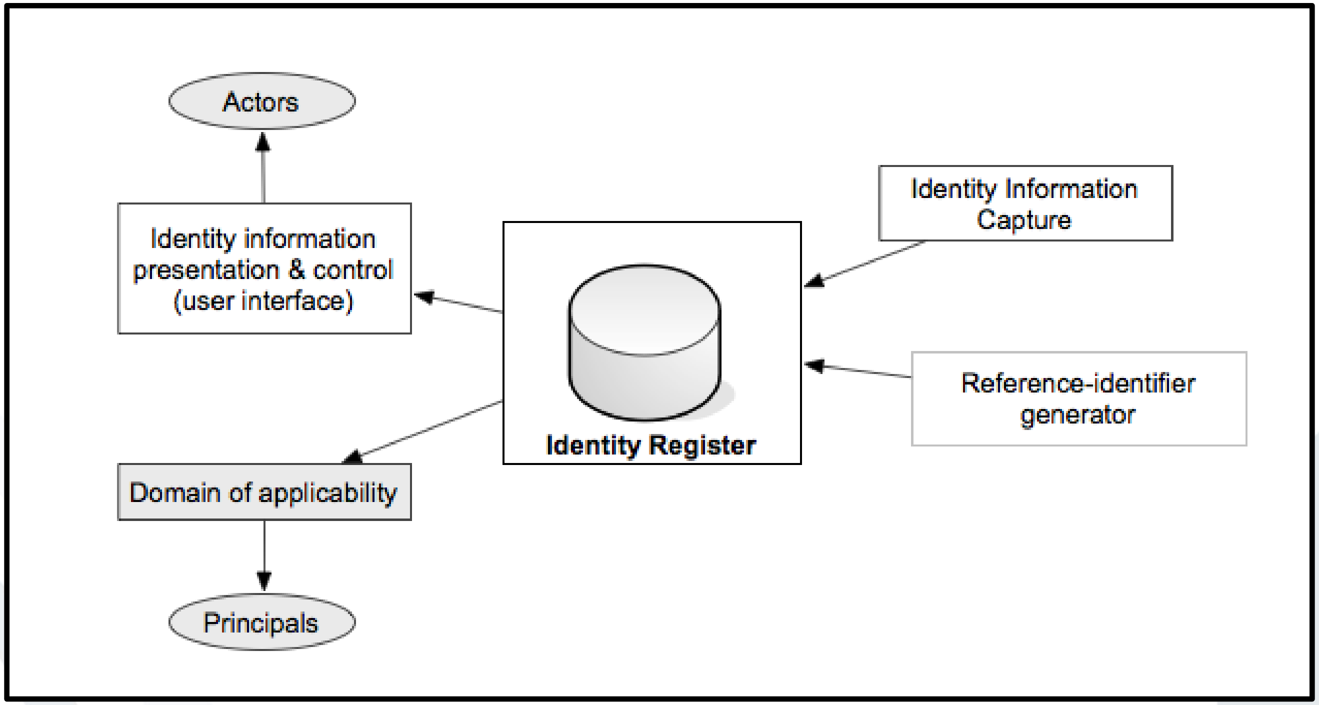
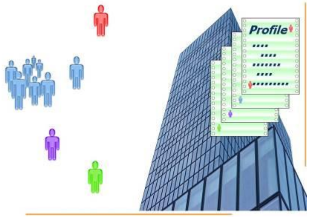

Actors
Identity information presentation & control (user interface)
Identity Register
Identity Information Capture
Reference-identifier generator
Domain of applicability
Principals

Figure 1 – Identity Management system components.

Identity Management: Types of IdM (Systems)

Type 1		Account Management: *assigned identity* *(= Tier 2)*	by organisation
Type 2		Profiling: *derived identity* *abstracted identity* *(= Tier 3)*	by organisation
Type 3	Profile Mobile	Management of *own* identities: *chosen identity* *(= Tier 1)*	by user himself supported by service providers

➲ There are hybrid systems that combine characteristics

[BaMe05]

Clauses 5 & 6
Reference architecture & Requirements

Nr.	Topic	Page
5	Reference architecture	2
5.1	Overview	2
5.2	Actors	5
5.3	Processes	7
5.4	Components	8
6	Requirements	10
6.1	Access to identity information	10
6.2	Identity information lifecycle management	11
6.3	Quality of identity information	12
6.3.1	General	12
6.3.2	Information adjustment	12
6.4	Time reference	12
6.5	IT security	13

6.2 Identity information lifecycle management

- International standard ISO/IEC 24760-1:2011 defines the stages in the lifecycle of an identity in a particular domain as reproduced in Figure 2.

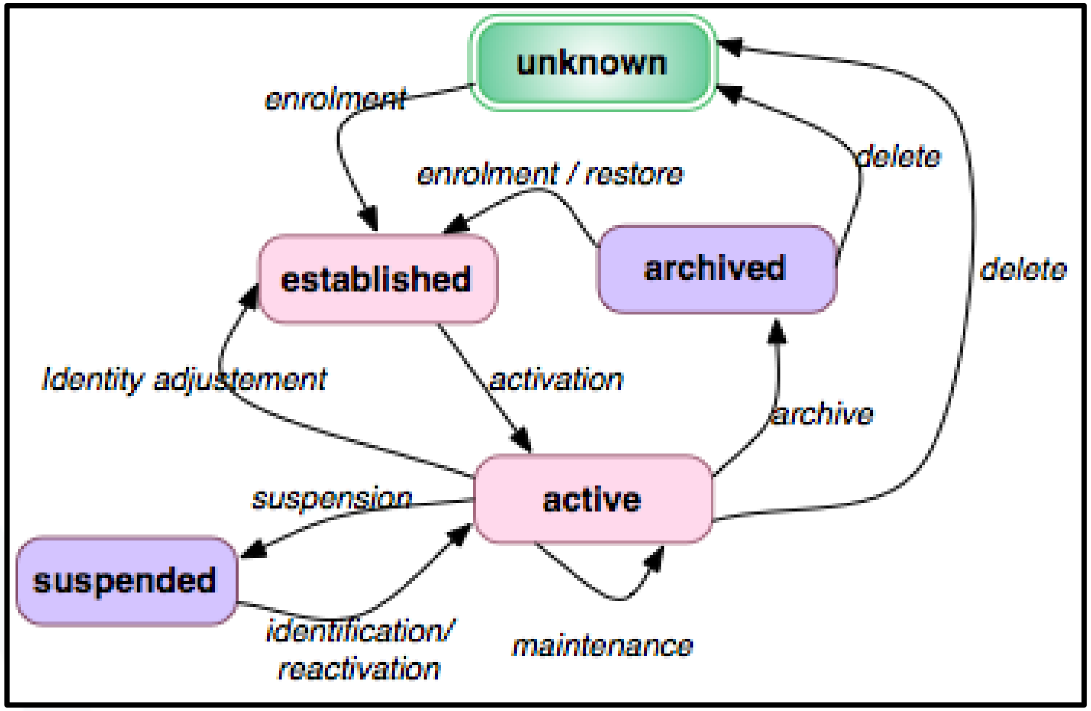


Figure 2 – Stages in the Identity lifecycle.

Part 2: Table of Content (1/3)

Nr.	Topic	Page
1	**Scope**	**1**
2	**Normative references**	**1**
3	**Terms and definitions**	**1**
4	**Symbols and abbreviated terms**	**2**
5	**Reference architecture**	**2**
5.1	**Overview**	**2**
5.1.1	Actors	2
5.1.2	Information flow	3
5.1.3	Functions	5
5.2	**Actors**	**5**
5.2.1	Identity management authority	5
5.2.2	Identity-information authority	6
5.2.3	Identity-information provider	6

Part 2: Table of Content (2/3)

Nr.	Topic	Page
5.3	**Processes**	**7**
5.3.1	General	7
5.3.2	Auditing	7
5.3.3	Generating reference identifier	7
5.3.4	Provisioning	7
5.3.5	Identity adjustment	7
5.3.6	Revocation	8
5.3.7	Identity information processing	8
5.3.8	Identity Information-processing authorization	8
5.4	**Components**	**8**
5.4.1	General	8
5.4.2	Identity register	9
5.4.3	Identity information capture	9
5.4.4	Reference-identifier generator	9
5.4.5	Identity information presentation and control	9

Part 2: Table of Content (3/3)

Nr.	Topic	Page
6	**Requirements**	**10**
6.1	**Access to identity information**	**10**
6.2	**Identity information lifecycle management**	**11**
6.2.1	General	11
6.2.2	Identity information lifecycle policies	11
6.2.3	Labelling	11
6.2.4	Archived information	11
6.2.5	Deleted information	11
6.3	**Quality of identity information**	**12**
6.3.1	General	12
6.3.2	Information adjustment	12
6.4	**Time reference**	**12**
6.5	**IT security**	**13**
Annex A	**Legal and regulatory aspects (Informative)**	**14**

Summary & Outlook

- IS 24760-1
  - completed in 2011 after several years
  - established important fundamental concepts, such as identity (partial identity) and attributes
- IS 24760-2 and IS 24760-3 will need a few more years (maybe till 2014).

- Next meeting of German mirror group of SC 27/WG 5 on August 22 with public workshop on privacy topics on August 21 in Berlin

References

- ABC4Trust: www.abc4trust.net
- Kim Cameron, Reinhard Posch, Kai Rannenberg: Proposal for a common identity framework: A User-Centric Identity Metasystem; Pp. 477 – 500 in [Rannenberg, Royer, Deuker 2009]
- Sebastian Clauß, Marit Köhntopp: Identity management and its support of multilateral security. Computer Networks, Volume 37, Issue 2, October 2001, Pages 205-219
- Deutsche Telekom Chair of Mobile Business & Multilateral Security; www.m-chair.net
- FIDIS: Future of Identity in the Information Society; www.fidis.net
- FIDIS Deliverable 3.6: Study on ID Documents; 2006; www.fidis.net
- Christian Kahl, Katja Böttcher, Markus Tschersich, Stephan Heim, Kai Rannenberg: How to enhance Privacy and Identity Management for Mobile Communities: Approach and User driven Concepts of the PICOS Project; Pp. 277-288 in: Kai Rannenberg, Vijay Varadharajan, Christian Weber: Security and Privacy – Silver Linings in the Cloud; Proceedings of 25th IFIP International Information Security Conference (IFIP SEC 2010), 20-23 September 2010, Brisbane, Australia, Springer IFIP Advances in Information and Communication Technology Series, Vol. 330, ISBN 978-3-642-15256-6
- Ioannis Krontiris, Herbert Leitold, Reinhard Posch, Kai Rannenberg: eID Interoperability; Pp. 167-186 in: Walter Fumy, Manfred Paeschke (Eds.): Handbook of eID Security – Concepts, Practical Experiences, Technologies, Publicis, ISBN 978-3-89578-379-1
- ISO Freely Available Standards; http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
- ISO Online Browsing Platform incl. Terms & Definitions; www.iso.org/obp/ui/#home
- ISO/IEC JTC 1/SC 27/WG 5: Identity Management and Privacy Technologies; www.jtc1sc27.din.de
- PICOS: Privacy and Identity Management for Community Services; www.picos-project.eu
- PRIME: Privacy and Identity Management for Europe; www.prime-project.eu
- PrimeLife: Privacy and Identity Management for Life; www.primelife.eu
- Kai Rannenberg: Multilateral Security – A concept and examples for balanced security; Pp. 151-162 in: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19-21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3
- Kai Rannenberg: CamWebSim and Friends: Steps towards Personal Security Assistants; Pp. 173 - 176 in Viktor Seige et al.: The Trends and Challenges of Modern Financial Services – Proceedings of the Information Security Summit; May 29-30, 2002, Prague; Tate International; ISBN 80-902858-5-6
- Kai Rannenberg: Identity management in mobile cellular networks and related applications; Information Security Technical Report; Vol. 9, No. 1; 2004; pp. 77 – 85; ISSN 1363-4127
- Kai Rannenberg, Denis Royer, Andre Deuker: The Future of Identity in the Information Society - Opportunities and Challenges; Springer 2009, ISBN 978-3-540-88480-4