Datenschutzstandardisierung im weltweiten Netz

ULD-Sommerakademie
am 1. September 2008

Jan Schallaböck
ULD62@datenschutzzentrum.de

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

- A. Einführung: Was sind Standards?
- B. Rechtliche Anknüpfungspunkte für die Einhaltung von Standards
- C. Relevante Standardisierung und Entwicklungen im Datenschutz

A. Was sind Standards?

Definition „Standard“ nach Wikipedia:

Ein **Standard** ist eine vergleichsweise einheitliche oder vereinheitlichte weithin anerkannte und meist auch angewandte (oder zumindest angestrebte) Art und Weise etwas herzustellen oder durchzuführen die sich gegenüber anderen Arten und Weisen durchgesetzt hat.

...

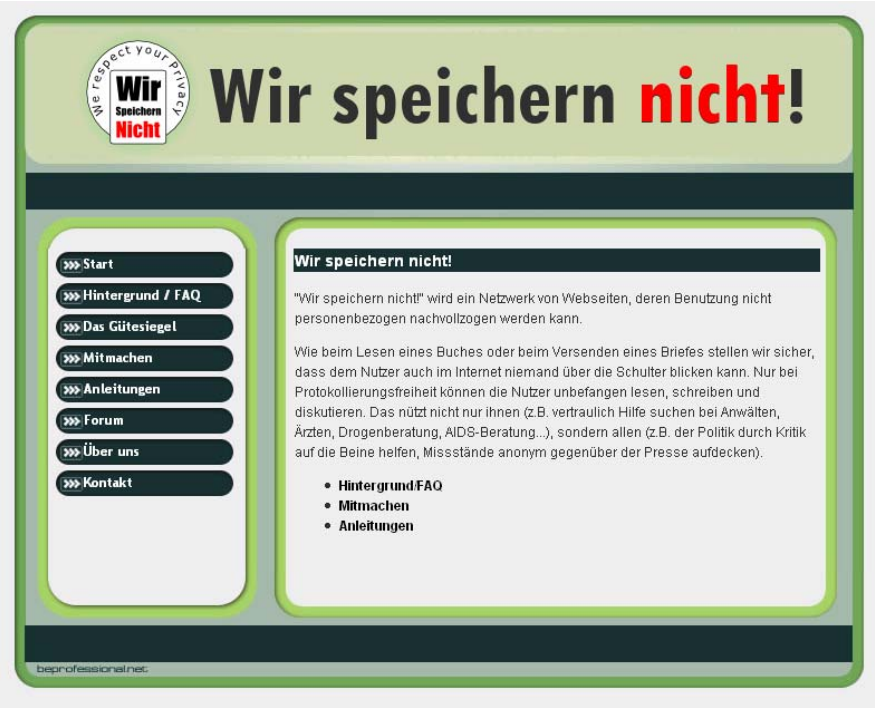
Ein *Standard* kann in einem formalisierten oder nicht-formalisierten Regelwerk bzw. in einem sich ungeplant ergebenden Regelfall bestehen beispielsweise in einer einzelnen Regel bzw. mehreren *Regeln* oder einer *Norm*.

*Standards im **engeren Sinne***

kommen von Normungsgremien

- International Telecommunications Union (ITU)
- CEN ETSI
- ICAO
- International Standardisation Organisation (ISO/IEC) als Dachverband für das
- Deutsche Institut für Normung (DIN) e.V.

- von Industriekonsortien
  - insbesondere das World Wide Web Consortium (W3C)
  - aber auch etwa OASIS die Open Group Liberty Alliance
- und als De-facto-Standards: zB. Flash, PDF, doc



„Top-Sites“
(ab Google-Page-Rank 5)

apparentbrightness.net
www.christian-hufgard.de
tracker.lotgd.de
www.henyoung.de
wir.trauen-uns.de
www.familie-hufgard.de
www.daten-speicherung.de
www.die-linke.de
www.etracker.de
jens.familie-ferner.de
fb18.de
www.filkshop.de
www.jondos.de
www.piratenpartei.de
www.ppoe.or.at
www.privacyfoundation.de
www.schokokeks.org
srbg.de
thomasmarquart.net
vorratsdatenspeicherung.de
www.wirspeichernnicht.de

„... eine vergleichsweise einheitliche oder vereinheitlichte weithin anerkannte und meist auch angewandte (oder zumindest angestrebte) Art und Weise etwas herzustellen oder durchzuführen die sich gegenüber anderen Arten und Weisen durchgesetzt hat“?

Screenshot:
http://ww.wirspeichernnicht.de

B. Rechtliche Anknüpfungspunkte
für die Einhaltung von Standards

1. § 9 BDSG
2. Anlage zu § 9 BDSG
3. § 3a BDSG
4. Erwägungsgrund 46 der Datenschutzrichtlinie
5. Rechtsfolgen der Nichteinhaltung
6. Zusammenfassung

1. Anforderungen aus § 9 BDSG

- „Öffentliche und nicht-öffentliche Stellen
- die selbst oder im Auftrag
- personenbezogene Daten
- erheben verarbeiten oder nutzen

→ **haben die technischen und organisatorischen Maßnahmen zu treffen die erforderlich sind um die Ausführung der Vorschriften dieses Gesetzes** insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen **zu gewährleisten**.

- Erforderlich sind Maßnahmen nur wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

2. Anlage zu § 9 BDSG

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Datentrennungsprinzip

„Werden personenbezogene Daten automatisiert verarbeitet oder genutzt ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet oder genutzt werden zu verwehren (**Zutrittskontrolle**)
2. zu verhindern daß Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**)
3. zu gewährleisten dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung Nutzung und nach der Speicherung nicht unbefugt gelesen kopiert verändert oder entfernt werden können (**Zugriffskontrolle**)
4. zu gewährleisten dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen kopiert verändert oder entfernt werden können und dass überprüft und festgestellt werden kann an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**)
5. zu gewährleisten dass nachträglich überprüft und festgestellt werden kann ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben verändert oder entfernt worden sind (**Eingabekontrolle**)
6. zu gewährleisten dass personenbezogene Daten die im Auftrag verarbeitet werden nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**)
7. zu gewährleisten dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**)
8. zu gewährleisten dass zu unterschiedlichen Zwecken erhobene Daten **getrennt verarbeitet werden können**.“

3. § 3 a BDSG
Datenvermeidung und Datensparsamkeit

- „Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten

→ **keine oder so wenig personenbezogene Daten wie möglich zu erheben zu verarbeiten oder zu nutzen.**

- Insbesondere ist von den Möglichkeiten der **Anonymisierung und Pseudonymisierung** Gebrauch zu machen
  - soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

4. Erwägungsgrund 46 der Richtlinie 95/46/EG
(„Datenschutzrichtlinie“)

„Für den Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung personenbezogener Daten

- müssen geeignete **technische und organisatorische Maßnahmen** getroffen werden
  - und zwar sowohl zum Zeitpunkt der Planung des Verarbeitungssystems
  - als auch zum Zeitpunkt der eigentlichen Verarbeitung
    - um insbesondere deren Sicherheit zu gewährleisten und
    - somit jede unrechtmäßige Verarbeitung zu verhindern.
- Die Mitgliedstaaten haben dafür Sorge zu tragen daß der für die Verarbeitung Verantwortliche diese Maßnahmen einhält.

- Diese Maßnahmen müssen
- **unter Berücksichtigung des Standes der Technik** und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.“

5. Rechtsfolgen der Nichteinhaltung,

§ 38 BDSG

„(5) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln

- kann die Aufsichtsbehörde **anordnen**
  - dass im Rahmen der Anforderungen nach § 9 Maßnahmen zur **Beseitigung festgestellter technischer oder organisatorischer Mängel** getroffen werden.
  - Bei schwerwiegenden Mängeln dieser Art insbesondere wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind kann sie **den Einsatz einzelner Verfahren untersagen** wenn die Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines **Zwangsgeldes** nicht in angemessener Zeit beseitigt werden.
  - Sie kann die **Abberufung des Beauftragten für den Datenschutz** verlangen wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.“

6. Zusammenfassung:

Standards sind Leitlinien und ein auch mögliches Auslegungskriterium für die vorgenannten Bestimmungen

Standards können dazu dienen herauszufinden wie zB.

- geeignete technisch-organisatorische Maßnahmen (§ 9 BDSG)
- die Sicherheit des datenverarbeitenden Systems (EG 46 d. RL 95/46/EG)
- schon in der Planung (RL 95/46/EG)
- die Zugriffskontrolle (Anlage zu § 9 BDSG)
- die Datentrennung (Anlage zu § 9 BDSG)
- die Datenvermeidung und –sparsamkeit die Anonymisierung und Pseudonymisierung (§ 3a BDSG)

... nach dem Stand der Technik (RL 95/46/EG)
zu gewährleisten sind.

C. Relevante Standards für den Datenschutz im Netz

- 1. Standards für IT-Sicherheit (Exemplarisch)
  - a. ISO 2700x
  - b. Reifegradmodell
  - c. Common Criteria
- 2. Identitätsmanagement- und Policystandards
  - a. ITU-T: Focus Group on Identity Management
  - b. ISO: Working Group Privacy and Identity
  - c. W3C: Policy Language Interest Group (PLING)

1. Standards für IT-Sicherheit

(Exemplarisch)

System- oder Verfahrensbezug			
		ISO/IEC 27001 (BSI-Standards Grundschutz-Kataloge)	**ISO/IEC 2700x** (vormals British Standards) Unterstützend: **ISO/IEC 21827** (Prozess-Reifegradmodell)
Produktbezug	**ISO/IEC 15408** (Common Criteria)		
	technische Ausrichtung		**Management-ausrichtung**

a. Die ISO 27000er Normenreihe

Terminology — ISO/IEC27000 Overview and Vokabulary

Requirements — ISO/IEC 27001 ISMS Requirements; ISO/IEC 27006 Accreditiation Requirements

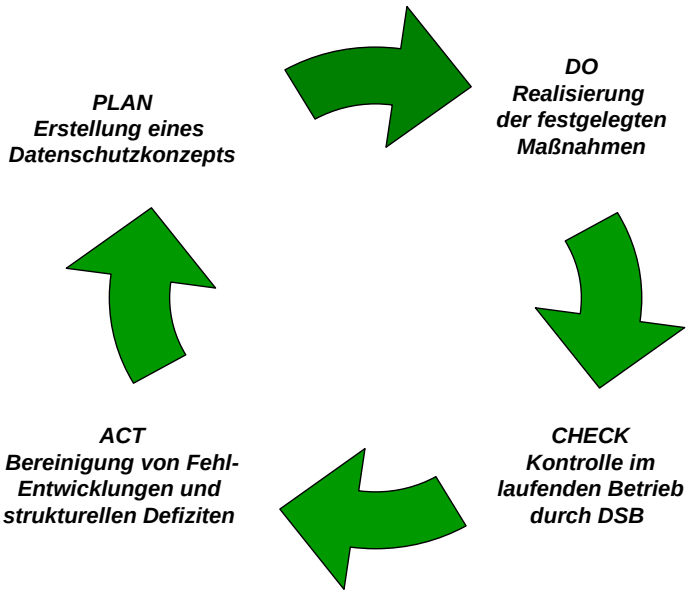
Guidance for ISMS operation and audit — ISO/IEC 27002 Code of Practice; ISO/IEC 27003 Implementation Guidance; ISO/IEC 27004 Management Measurements; 27005 Risk Management

… Und weitere derzeit noch nicht näher spezifizierte Ausführungsnormen

ISO/IEC 27001

Information Security Management Systems - Requirements

- Information Security Management System (ISMS)
  - Generelle Anforderungen
  - Errichtung und Betrieb des ISMS
  - Anforderungen an die Dokumentation
- Verantwortlichkeiten des Managements
  - Management Commitment
  - Ressourcenverwaltung
- Review des ISMS
  - Generelle Aspekte
  - Review Input
  - Review Output
  - Interne ISMS Audits
- ISMS Verbesserung
  - Kontinuierliche Verbesserung
  - Korrigierende Maßnahmen
  - Präventive Maßnahmen



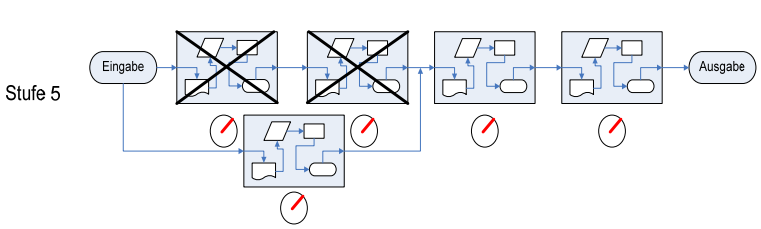
ISO/IEC 27002

Code of practice for information security management

- Klassen für die Risikoanalyse:
  - Sicherheitspolicy
  - Organisation der Informationssicherheit
  - Asset Management
  - Human Ressource Sicherheit
  - Physische und Umgebungssicherheit
  - Kommunikations- und Betriebsmanagement
  - Access Control (Zutritt Zugang Zugriff)
  - Auswahl Einführung / Entwicklung und Wartung von Systemen zur Informationsverarbeitung
  - IT-Sicherheitsvorfallmanagement
  - Business Continuity Management
  - Compliance
- Generische Sicherheitsmaßnahmen und zugehörige Sicherheitsziele

b. ISO/IEC 21827

Aufbau des Prozess Reifegradmodells



Stufe 5: Optimiert (Optimised)
Der Prozess wird unter Auswertung der KPI beständig optimiert

Stufe 4: Vorhersehbar (Predictable)
Es existieren für Arbeitsschritte und Teilprozesse Qualitätskriterien so genannte Key Performance Indikatoren (KPI)

Stufe 3: Standardisiert (Standardised)
Arbeitsschritte und Teilprozesse laufen wiederholbar ab Prozess ist dokumentiert

Stufe 2: Reproduzierbar (Managed)
auf Ebene der kleinsten Organisationseinheiten ist der Prozess organisiert; Input und Ergebnis sind definiert

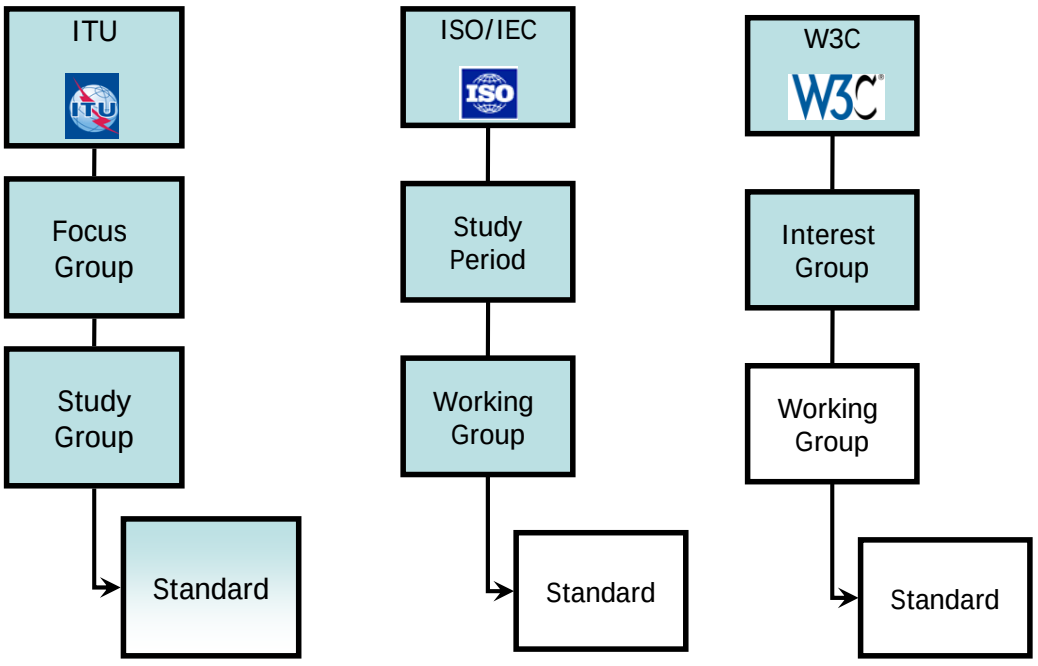
Stufe 1: Ausgangszustand (Initial)
Chaotisch eher Projekte als Prozesse; Input und Ergebnis sind nicht definiert Abläufe wiederholen sich nur selten

c. ISO/IEC 15408 Common Criteria

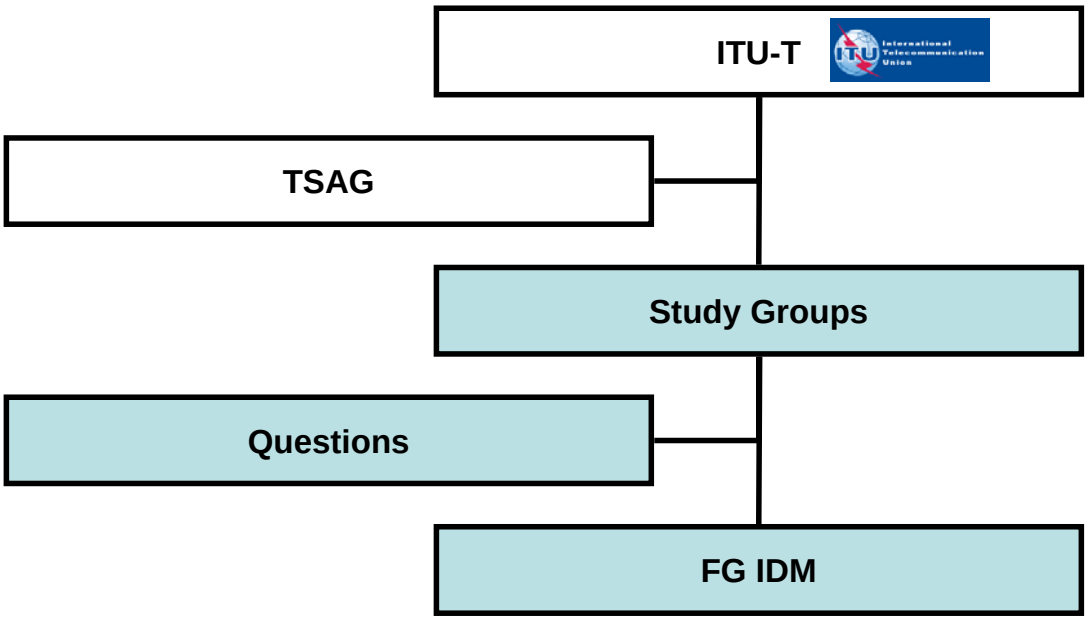
- Target Of Evaluation (TOE): Produkt
- Tests in 8 Prüfungsklassen z.B.
  - Configurations management
  - ...
  - Operational support
- Result: Evaluation Assurance Level (EAL): 7 Ebenen z.B.:
  - EAL 1: functional tested (Funktionstest)
  - ...
  - EAL 7: formal verified and tested model (Formal verifizierter und getesteter Prototyp)
- Vom Hersteller definiert:
  - Security Targets (ST): Risiken die beim Produkt betrachtet sind (Behandelt mit s.g. Security Functions SF)
  - Drei Ebenen von Security Functions (Strength of Function SOF):
    - Low
    - Medium
    - High
  - Depth of Testing: Funktionstest bis Code Evaluation; Testtiefe berücksichtigt auch die potentielle Stärke eines Angreifers
  - Besonderheit: Protection Profile (PP): Sicherheitsanforderungen die das Produkt erfüllen muss unabhängig von der Implementierung und Umgebung

Folie: nach M. Meints

2. Identitätsmanagement- und Policystandards



a. ITU-T



ITU-T Focus Group on Identity Management *(FG IdM)*

Focus Group on Identity Management

The Focus Group on Identity Management was established by Study Group 17 at its 6-15 December 2006 meeting. The objective of the Focus Group is to facilitate the development of a **generic Identity Management framework** by fostering participation of all telecommunications and ICT experts on Identity Management. The FG IdM is open to ITU Member States Sector Members and Associates as well as any individual from a country which is a member of ITU willing to contribute to the work; this includes individuals who are also members or representatives of interested Standards Development Organizations. The FG IdM will report to SG 17.

- Chairman: Abbie Barbir
- Vice-Chairman: Richard Brackney
- Vice-Chairman: Antony Nadalin

- First Meeting Geneva 13-16 Feb 2007. Proposed Scope and Means and Mechanisms were agreed and considered. The Architecture Session produced a collective vision.
- Second Meeting Geneva 23-25 Apr 2007. Followed review of its charter at the TSAG Meeting Geneva 26 Feb-1 Mar. The 2nd Meeting principal output is a synthesis of principal IdM "gap" requirements derived from submitted use cases.
- Third Meeting Mountain View California USA 17-18 May 2007 at Mountain View headquarter campus of host VeriSign Inc.
- Fourth Meeting Tokyo Japan 17-20 Jul 2007.
- Fifth Meeting in Ottawa in August 2007.

Arbeitsprogramm der FG IdM

- Ecosystem and Lexicon
- Use Cases
- Requirements
- Framework
- Privacy Guidelines

Revised Terms of Reference

(Consequences of TSAG amendments to the FG IdM ToR April 2007)

"A report on privacy guidelines and best practices; this includes identifying gaps in applicable specifications of standards bodies forums and consortia working on identity management.

Note: The above report on Privacy Guidelines and Best Practice has to indicate how existing Regulatory and Privacy requirements are implemented. **The Focus group must not define new Legal Regulatory and Privacy Requirements."**

Arbeitsprogramm der FG IdM

- Ecosystem and Lexicon
- Use Cases
- Requirements
- Framework
- ~~Privacy Guidelines~~

Aufgabenbereiche des IDM nach ITU-T

(Datenschutzrelevante Bereiche hervorgehoben)

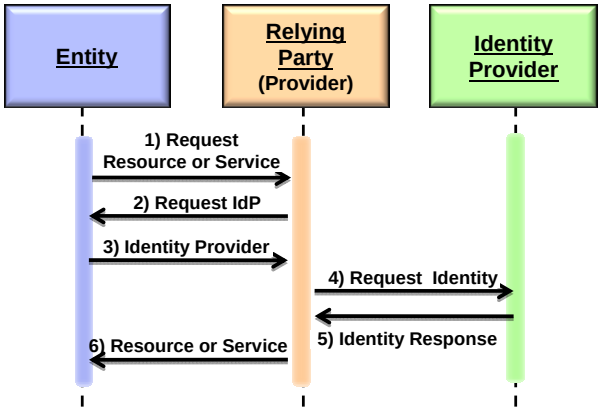
- Integration of IdM in NGN Architecture
- Discovery of Identity Resources
- Inter-Federation/Inter-CoT Interoperability
- Interoperability of Mechanisms Used to Exchange Identity Information
- **Identity Authentication Assurance**
- **Transparency and Notice**
- Integration of object management
- **IdM Security and Identity Patterns**
- Token Transformation
- **Static Trust Models and Dynamic Selections**
- Delegation
- **Meta-Data Model**

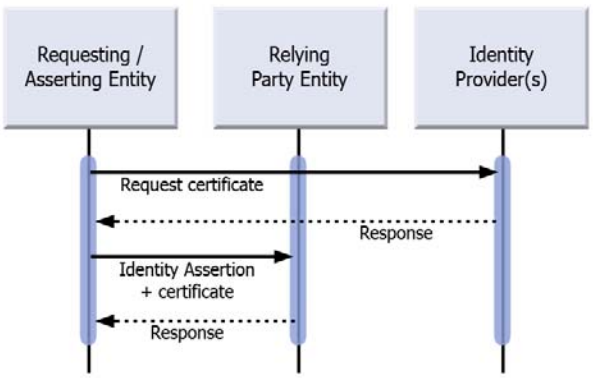
(aus den Abschlußreport der FG IdM am June 13th 2007)

Details der „Living List"

- Pseudonym
  - A fictitious identity that an Entity creates for itself whereby the Entity can remain pseudonymous or perhaps even fully anonymous in certain contexts.
- Anonymity
  - lack of any capability to ascertain identity.
  - **the quality or state of being anonymous which is the condition of having a name or identity that is unknown or concealed.**
- Credential
  - the private part of a paired Identity assertion (user-id is usually the public part). The thing(s) that an Entity relies upon in an Assertion at any particular time usually to authenticate a claimed Identity. Credentials can change over time and may be revoked. Examples include; a signature a password a drivers licence number (not the card itself) an ATM card number (not the card itself) data stored on a smart-card (not the card itself) a digital certificate a biometric template.

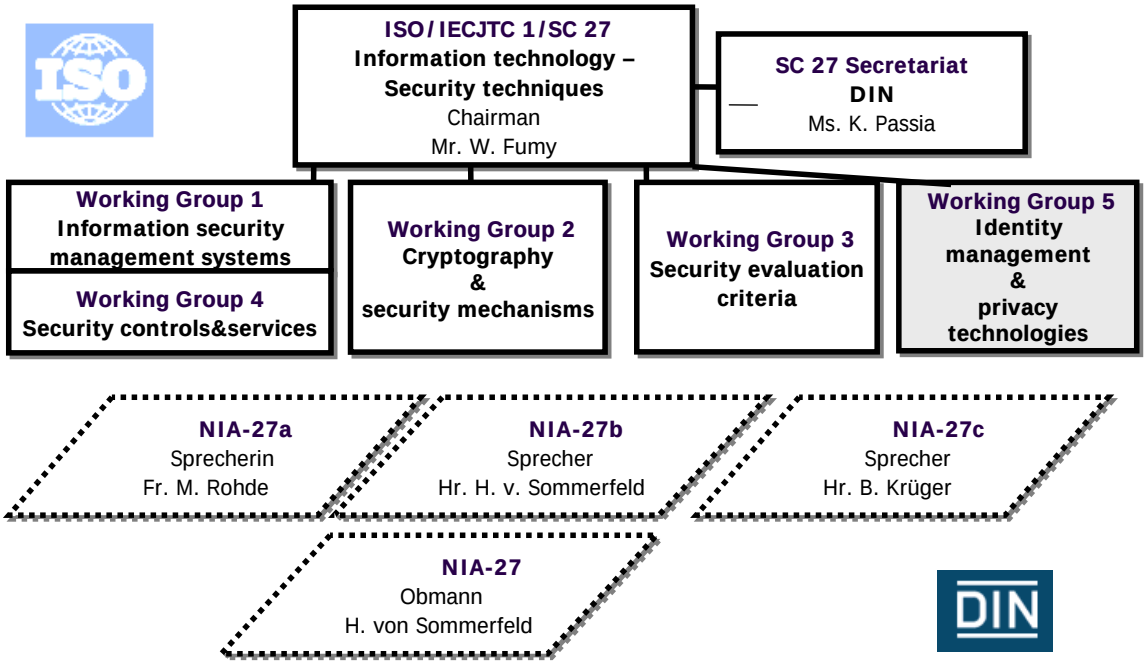
Datenflussmodell nach ITU-T FG IdM
und Alternativvorschlag der ISO (rechts)





b. ISO

(ISO/IEC JTC 1/SC 27 und DIN Spiegelgremien)



Grafik:
H. v. Sommerfeld

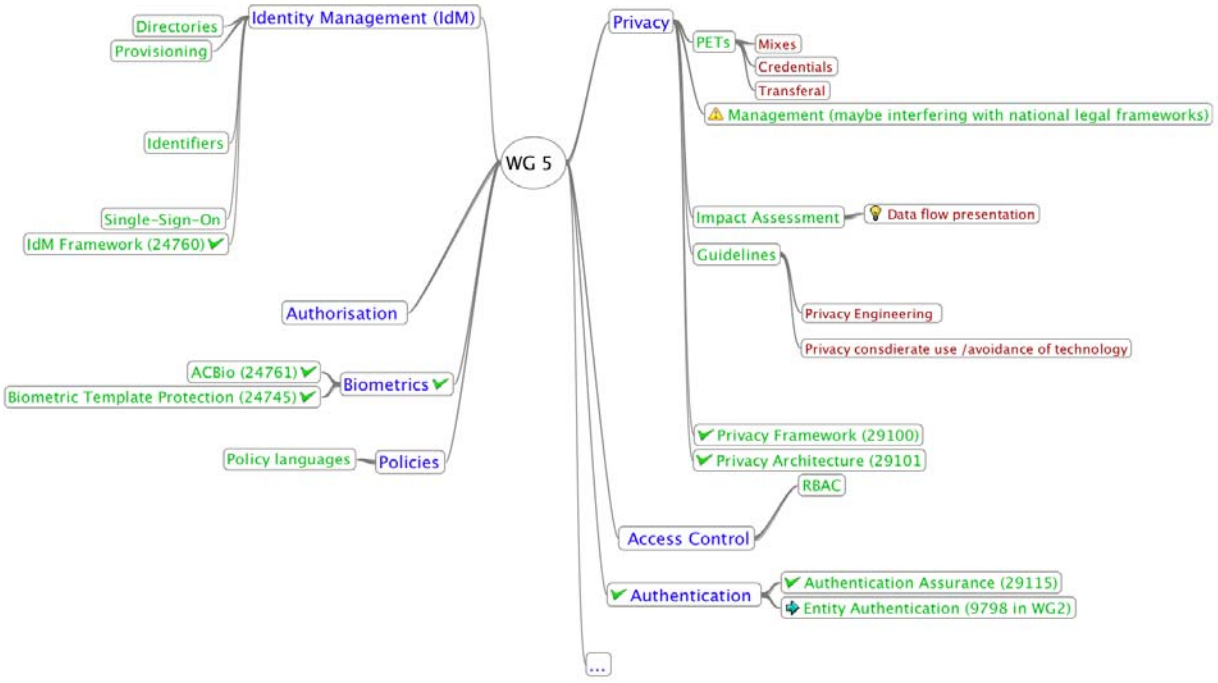
Laufende Projekte

(Auswahl)

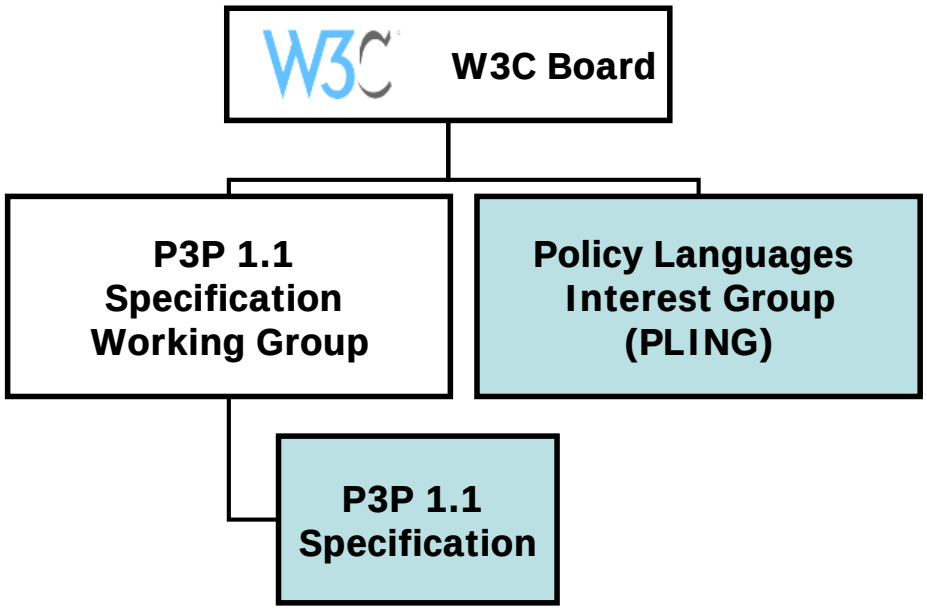
- A Framework on Identity Management
- Biometric Template Protection (24745)
- A Privacy Framework (29100)
- A Privacy Architecture (29101)
- Authentication Assurance (29115)

Roadmap:

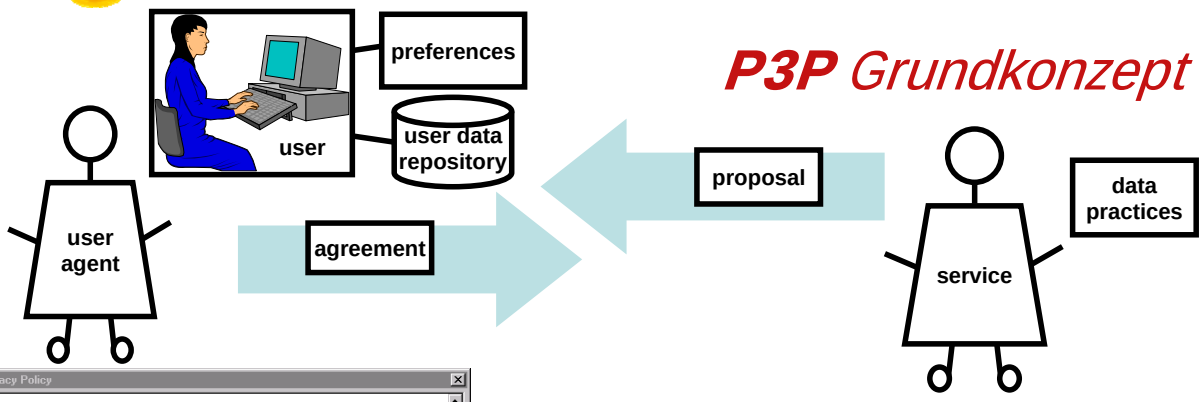
ISO/IEC/IES JTC 1/SC 27 Working Group 5

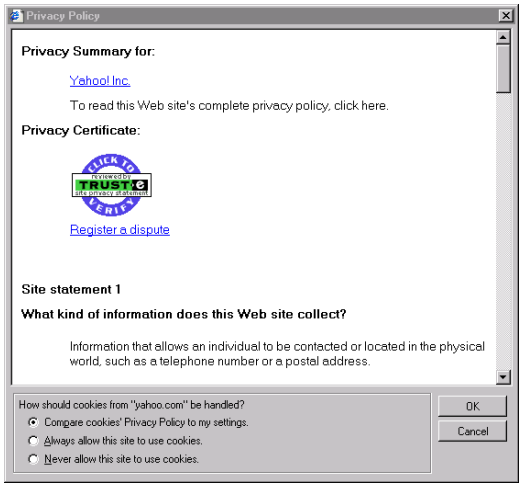


c. W3C



P3P Grundkonzept





Screenshot: wikipedia.org

- P3P ist eine formale Beschreibung von Datenschutzerklärungen
- Verbreitung stagniert
- Weiterentwicklung derzeit eingefroren
- Dennoch ein Erfolgsmodell!
- Problem die Überwachung der Einhaltung (Enforcement)

Policy Languages Interest Group (PLING)

- "Architecture and Application in particular use cases in
  - compliance
  - privacy
  - access control
  - identity management and
  - obligation management areas
- a forum to support researchers developers solution providers and users of policy languages such as
  - XACML (eXtensible Access Control Markup Language)
  - the IETF's Common Policy framework and related work and
  - P3P (W3C's Platform for Privacy Preferences Project).
- Focus on policy languages that are already specified and broadly address the privacy access control and obligation management areas; it is not expected to engage in the design of new policy or rule languages."

Herzlichen Dank!

Jan Schallaböck
Telefon +49.431.988-1285
ULD62@datenschutzzentrum.de