mobile business

Lecture 8

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Information & Communication Security (WS 2020/21)

Privacy Protection I

Prof. Dr. Kai Rannenberg
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

Agenda

- Data Protection and Privacy
  - Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Communication systems
  - Transaction systems
- Concepts of Privacy Protection
  - Privacy by Design (PbD)
  - Privacy Engineering
  - Transparency
  - Usability
- Integrated Privacy Protection
  - PRIME LBS
  - ABC4Trust
  - Privacy Advisor
  - Privacy Risk Communication and Mitigation

7.40 am – Making coffee

Information:

- Daily routines
- Coffee consumption

[Philipps / Saeco]

Privacy terms I

Was bringt die Zweckerfüllung mit sich?

Wenn Sie die App verwenden, zeichnen wir die **Art der Verwendung** Ihrer Saeco GranBaristo Avanti auf, um Ihnen hilfreiche Tipps, Tricks und Wartungsinformationen für Ihre Maschine bieten zu können. Wir erfassen diese Daten **zu Marktforschungszwecken** und/oder, um Ihnen hilfreiche Tipps zur Verbesserung der Leistung sowie zur Wartung Ihres Saeco Kaffeevollautomaten zu bieten.

Welche persönlichen Daten werden zu diesem Zweck verarbeitet?

Wenn Sie die App verwenden, erfasst Philips Daten zu Ihrer Verwendung der Saeco Avanti sowie **historische Daten zum Kaffeeverbrauch**. Außerdem ermittelt Philips, auf welche Art die App genutzt wird.

Die App funktioniert nicht ohne die Erfassung dieser Daten. Wenn Sie diese Daten nicht weitergeben möchten, können Sie die App nicht verwenden.

[Philipps / Saeco]

Privacy terms I (English version)

What comes with fulfilling the purpose ?

When you are using the app, we will record the **way you use** your Saeco GranBaristo Avanti to provide you with helpful tips, tricks and maintenance information for your machine. We collect this information for **market research purposes** and/or to provide you with helpful tips for improving performance and maintaining your Saeco coffee machine.

What personal data is processed for this purpose?

When you use the app, Philips collects data on your use of the Saeco Avanti and historical data on coffee consumption. In addition, Philips determines how the app is used.

The app will not work without collecting this data. If you do not want to share this information, you will not be able to use the app.

[Philipps / Saeco]

Privacy terms II

Greifen wir für den genannten Zweck auf andere Parteien zurück?
Beim Speichern der Daten sowie bei der Erfassung und Analyse statistischer Daten greifen wir auf einen **Drittanbieter** zurück.
[…]

Welche **persönlichen Daten** werden zu diesem Zweck verarbeitet?
Wir können bestimmte Registrierungsinformationen nutzen, z. B. Benutzername, Vorname, Nachname, E-Mail-Adresse, Land, Sprache, Passwort, Anrede, Alter.

Greifen wir für den genannten Zweck auf andere Parteien zurück?
Philips greift auf einen **Drittanbieter** für die Erfassung und Einbehaltung unserer Registrierungsaufzeichnungen, einschließlich der von Ihnen bereitgestellten persönlichen Daten, zurück.

[Philipps / Saeco]

Privacy terms III

Was bringt die Zweckerfüllung mit sich?

Wir erfassen und sammeln diese persönlichen Daten und **entfernen die individuelle Kennzeichnung**, um Nutzungsstatistiken zu erstellen, anhand derer wir Inhalt, Funktionen und Benutzerfreundlichkeit der App verbessern können.

Welche persönlichen Daten werden zu diesem Zweck verarbeitet?

Zu diesem Zweck verarbeiten wir Ihre **eindeutige Benutzergerätenummer**, die **IP-Adresse** Ihres Geräts, den **Typ des Internetbrowsers** für Mobilgeräte oder das **verwendete Betriebssystem** sowie **Zeiten und Daten**, zu denen die App verwendet wurde. Zudem erfassen wir **Sitzungs- und Nutzungsdaten**, also Informationen zu Ihrer Verwendung der App, z. B. Informationen zu Verbindungsanforderung, Serverkommunikation und **Datenweitergabe**, **Netzwerk-Statistiken**, Servicequalität sowie **Datum und Zeit** des Zugriffs.

[Philipps / Saeco]

Privacy terms IV

So leiten wir Ihre Informationen an Dritte weiter

Wenn Philips einem Drittanbieter die Übertragung Ihrer persönlichen Daten **außerhalb Ihrer geografischen Region** erlaubt, werden Schritte zum Schutz Ihrer Privatsphäre durch die Nutzung von vertraglichen Vereinbarungen oder anderen Mittel, die einen vergleichbaren Schutz während der Informationsverarbeitung durch vertrauenswürdige Drittanbieter bieten, eingeleitet.

[…]

Mitunter werden Geschäftsbereiche oder Teile eines Geschäftsbereichs von Philips an andere Unternehmen verkauft. Im Rahmen des zugehörigen Eigentumsübergangs können **die persönlichen Daten**, die in direkter Verbindung zu diesem Geschäftsbereich stehen, **an das erwerbende Unternehmen übergeben werden**.

[Philipps / Saeco]

Privacy terms V

Ihre persönlichen Daten können aus dem Land, in dem Sie sich befinden, an andere Unternehmen von Philips an **anderen Orten weltweit** weitergeleitet werden. Diese Länder verfügen möglicherweise nicht über ähnliche Datenschutzbestimmungen. Für den Fall, dass Ihre Daten außerhalb Ihres Landes oder Gerichtsstandes übertragen werden, werden diese möglicherweise **gemäß den Gesetzen in diesen Ländern** gehandhabt. Falls gemäß lokalem Gesetz erforderlich, werden wir Sie vorab um Ihre Zustimmung zur Weitergabe Ihrer persönlichen Daten außerhalb Ihrer geografischen Region bitten.

[…]

Sie sind jederzeit berechtigt, auf Ihre persönlichen Daten zuzugreifen oder eine Korrektur derselben zu verlangen und **gegen die Verarbeitung Ihrer persönlichen Daten Einspruch einzulegen**. Senden Sie uns hierzu eine E-Mail an privacy@philips.com, oder besuchen Sie unsere Kontaktseite.

[Philipps / Saeco]

Privacy terms VI

Änderungen an diesen Datenschutzbestimmungen

Die von Philips bereitgestellten Services entwickeln sich stetig weiter, und die Art und Form dieser Services kann sich gelegentlich ändern, **ohne** dass Sie davon **im Voraus in Kenntnis** gesetzt werden müssen. Aus diesem Grund behalten wir uns das Recht vor, **regelmäßig Änderungen an dieser Datenschutzrichtlinie** vorzunehmen. **Wir empfehlen, diese Website regelmäßig zu besuchen, um die aktuellste Version anzusehen.**

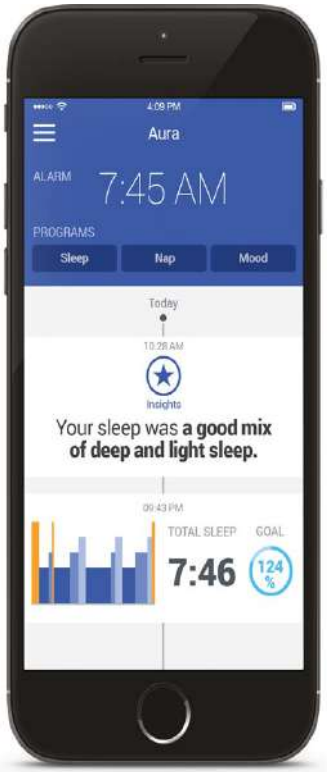
Neue Datenschutzbestimmungen sind mit ihrer Veröffentlichung wirksam. Wenn Sie geänderten Datenschutzbestimmungen nicht zustimmen, sollten Sie Ihre persönlichen Einstellungen ändern oder in Betracht ziehen, die App nicht mehr zu verwenden. Wenn Sie **nach solchen Änderungen** weiterhin auf unsere Dienste zugreifen oder sie nutzen, stellt dies eine **Annahme der geänderten Datenschutzbestimmungen** dar.

[Philipps / Saeco]

7.45 – Getting up

Information:

- Sleep rhythm
- Sleeping habits



[Withings]

7.50 – Shaving (foam running out)

Information:

- Daily routine
- Preferred products

[Amazon]

7.52 – Weighing

Information:

- Daily routine
- Weight

[Fitbit]

7.55 – Cleaning teeth

Information:

- Daily routine
- Dental health (care)

[Oral-B]

8.30 – Locking the door

Information:

- Daily routine
- Persons in household

[August]

8.35 – Turning heating down

Information:

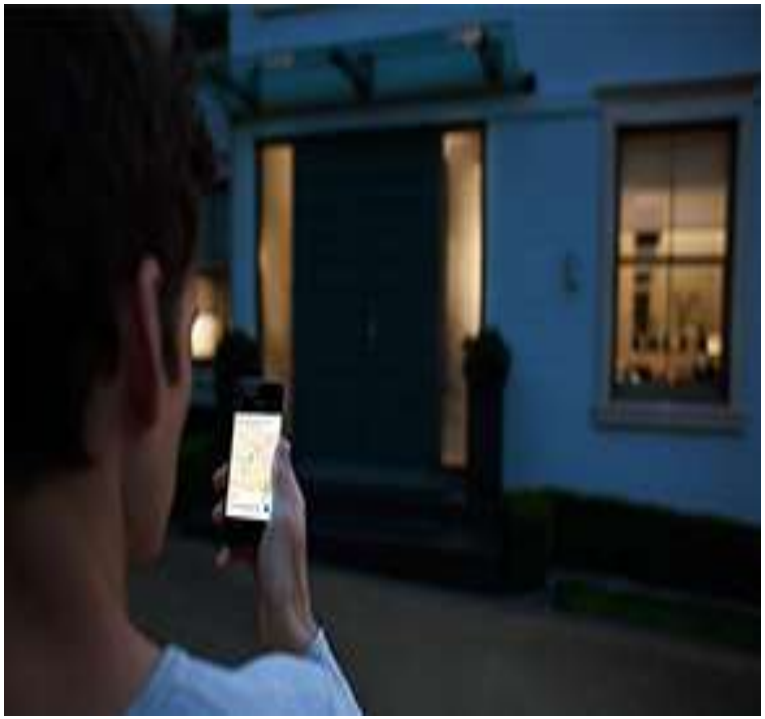
- Daily routine
- Persons in house

[Nest]

8.40 – Lights out?

Information:

- Daily routine
- Persons in house



[Philipps]

More devices

[Sony]

[Mattel]

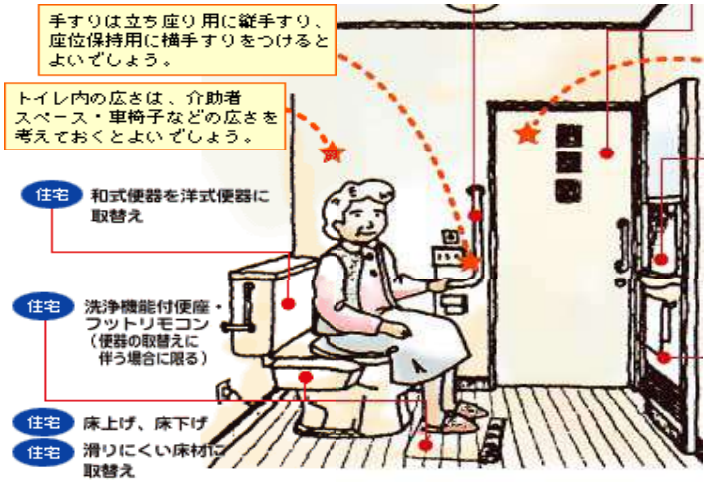
[LG]

[Beurer]

[Source: Discovergy]

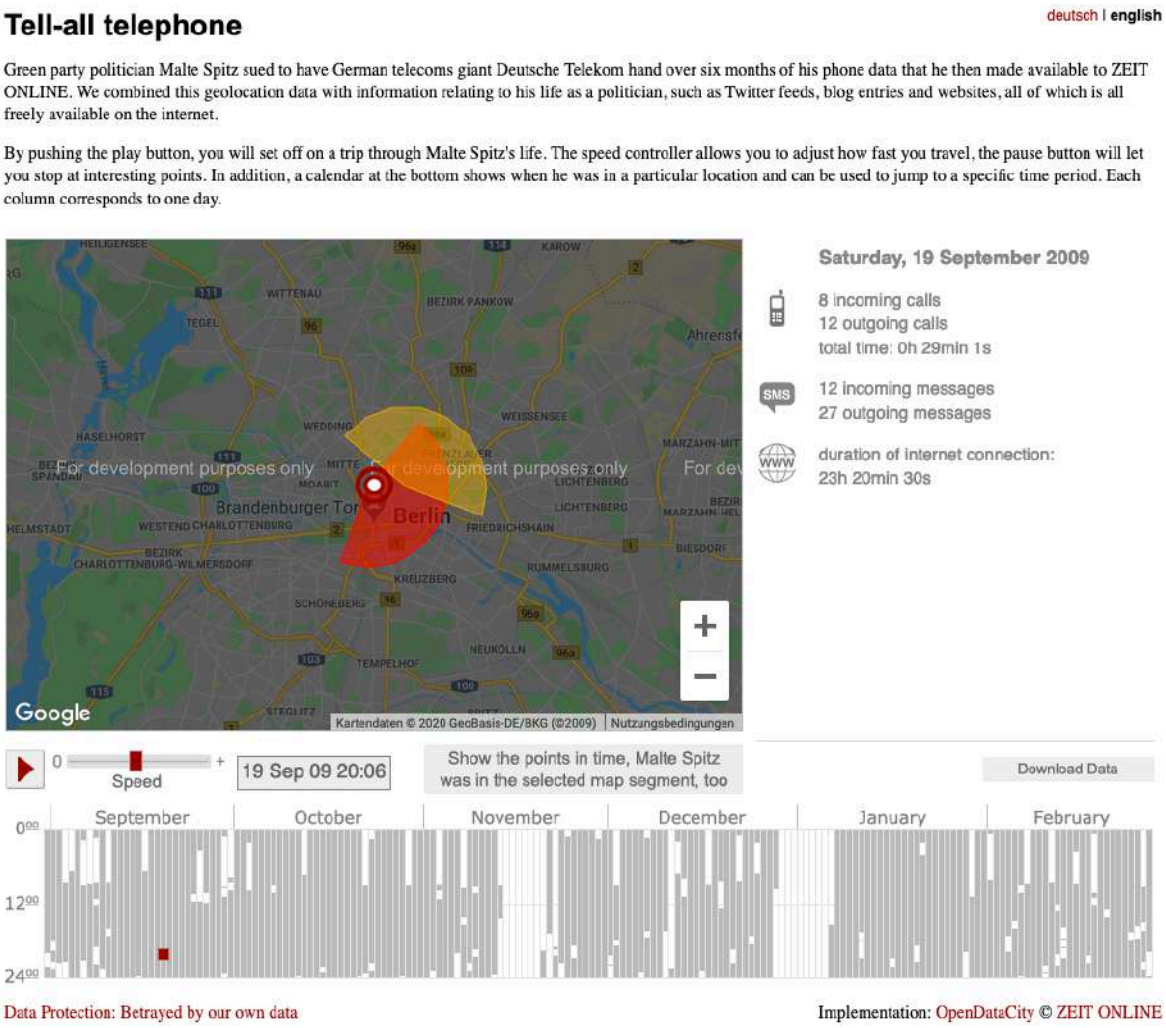
The networked washlet

- … and in Japan, Matsushita has demonstrated a health-monitoring toilet that can analyze your stool and send the information online to your doctor. [www.asiaweek.com/asiaweek/technology/article/0,8707,130495,00.html, 2001-06-22]
- " … sensors detect seven abnormal behavior patterns of the elderly in their living quarters and three abnormal patterns in the toilet area. Any abnormality that is sensed is automatically transmitted to the PHS terminals or pagers of the nursing staff. The care monitor system that uses these sensors will help provide safe and high quality nursing service." [www.mew.co.jp/e-tecrepo/73e/main02.html]



[Hitachi, Matsuhita Electric Works Limited, Panasonic, Toto]

Data retention of cell-based location data



[www.zeit.de/datenschutz/malte-spitz-data-retention] (Eng v.)

Privacy Rights Clearinghouse

Empowering Consumers. Protecting Privacy.

Chronology of Data Breaches

Custom Sort

Select your desired results. Then click "Go!"

Choose the type of breaches to display:

Click or unclick the boxes then select go.

- [x] **Unintended disclosure (DISC)** - Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.
- [x] **Hacking or malware (HACK)** - Electronic entry by an outside party, malware and spyware.
- [x] **Payment Card Fraud (CARD)** - Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
- [x] **Insider (INSD)** - Someone with legitimate access intentionally breaches information - such as an employee or contractor.
- [x] **Physical loss (PHYS)** - Lost, discarded or stolen non-electronic records, such as paper documents

Select organization type(s):

- [x] BSO - Businesses - Other
- [x] BSF - Businesses - Financial and Insurance Services
- [x] BSR - Businesses - Retail/Merchant
- [x] EDU - Educational Institutions
- [x] GOV - Government and Military
- [x] MED - Healthcare - Medical Providers

Select year(s):

- [ ] 2005
- [ ] 2006
- [ ] 2007
- [ ] 2008
- [ ] 2009
- [ ] 2010
- [ ] 2011
- [ ] 2012
- [ ] 2013
- [ ] 2014
- [ ] 2015
- [x] 2016

owasp.org

OWASP Top 10 Privacy Risks

Watch 7 Star 1

Main | Top 10 Privacy Risks | Participate | Acknowledgements | Translation | FAQs

The OWASP Top 10 Privacy Risks Project provides a top 10 list for privacy risks in web applications and related countermeasures. It covers technological and organizational aspects that focus on real-life risks, not just legal issues. The Project provides tips on how to implement privacy by design in web applications with the aim of helping developers and web application providers to better understand and improve privacy. The list uses the OECD Privacy Guidelines as a framework and can also be used to assess privacy risks associated with specific web applications.

Top 10 Privacy Risks

```
P1    Web Application Vulnerabilities
P2    Operator-sided Data Leakage
P3    Insufficient Data Breach Response
P4    Insufficient Deletion of personal data
P5    Non-transparent Policies, Terms and Conditions
P6    Collection of data not required for the primary purpose
P7    Sharing of data with third party
P8    Outdated personal data
P9    Missing or Insufficient Session Expiration
P10   Insecure Data Transfer
```

Detailed information is provided in the Top 10 Privacy Risks tab.

Quick Download

- Top 10 Privacy Risks Countermeasures v1.0 (PDF)
- Top 10 Privacy Risks Presentation (PPTX)
- Results presentation at German OWASP Day 2014
- Presentation from IAPP Global Privacy Summit 2015
- Presentation of countermeasures from IAPP Data Protection Intensive 2016

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

Project Information

Version 1.0
Lab Project
Documentation Project

Mailing List

Join Google Group

Timeline

[2014] Top 10 Privacy Risks v1.0 published
[2015] German Translation available
[2016] Countermeasures v1.0 published
[2019] Work on v2.0 started

External Links

Video from IPEN workshop at Berlin state parliament
Video from panel discussion at CPDP 2015
Video presentation from AppSec EU 2015

Agenda

- Data Protection and Privacy
  - Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Communication systems
  - Transaction systems
- Concepts of Privacy Protection
  - Privacy by Design (PbD)
  - Privacy Engineering
  - Transparency
  - Usability
- Integrated Privacy Protection
  - PRIME LBS
  - ABC4Trust
  - Privacy Advisor
  - Privacy Risk Communication and Mitigation

Data Protection and Privacy

- Both terms are related but not synonymous and have many definitions.
- 2 popular ones:
  - **Data protection** is the protection from harmful and unsolicited usage of data linked to the personal sphere of a person.
  - **Privacy** is the right to be left alone, e.g. to be unwatched or anonymous [WaBr1890].
- More work needed on a complete understanding of privacy
- Nevertheless the topic is important, as one can see from related incidents and activities to address the issue.

The Origin of Data Protection?

- The term “Privacy” (‘the right to be left alone’) originates from Warren & Brandeis [WaBr1890].
- Data protection in Germany (“Datenschutz”) originates from concerns over too much information and power in the hands of large (governmental) institutions (“**Big Brother**”).
- Nowadays Data protection and Privacy in Germany are based on the right of informational self determination derived from the constitution in the “Volkszählungsurteil“ [BVG1983]).
- ***Germany has one of the most advanced infrastructures for Privacy*** but still no established German language term for Privacy beyond the (misleading) “Datenschutz”.
- Some (more or less established) related terms are:
  - Privatheit
  - Privatsphäre
  - Schutz der Privatsphäre

Agenda

- Data Protection and Privacy
  - Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Communication systems
  - Transaction systems
- Concepts of Privacy Protection
  - Privacy by Design (PbD)
  - Privacy Engineering
  - Transparency
  - Usability
- Integrated Privacy Protection
  - PRIME LBS
  - ABC4Trust
  - Privacy Advisor
  - Privacy Risk Communication and Mitigation

EU General Data Protection Regulation (GDPR)

- The EC adopted a new EU legal framework on the protection of personal data.
- The regulation entered into force on 24 May 2016. It has been applied since 25 May 2018.
- The European Commission says that the regulation “puts the citizens back in control of their data, notably through”:
  - A right to be forgotten: Users will have the right to demand that data about them be deleted if there are no "legitimate grounds" for it to be kept.
  - People will have easier access to their own data, and will find it easier to transfer it from one service provider to another.
  - Putting people in control
    - Organizations must notify the authorities about data breaches as early as possible, "if feasible within 24 hours”.
    - In cases where consent is required organizations must explicitly ask for permission to process data, rather than assume it.
  - Privacy by design and by default – privacy friendly default settings to be the norm.

[EU2016]

GDPR Principles I

- **Lawfulness, fairness and transparency:** personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation:** personal data must collected for specified explicit and legitimate purposes.
- **Data minimisation:** personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** personal data must accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

[EU2016]

GDPR Principles II

- **Storage limitation:** personal data must kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and confidentiality:** personal data must be processed in a way that ensures appropriate security of the personal data.
- **Accountability:** The controller shall be responsible for and be able to demonstrate compliance to the principles mentioned above.

[EU2016]

Principle of Accountability in the GDPR

- The controller shall be responsible for and be able to demonstrate compliance to the regulation to:
  - maintain certain documentation,
  - conduct a data protection impact assessment for more risky processing (data controllers should compile lists of what is caught), and
  - implement data protection by design and by default, e.g., data minimisation.

[EU2016] [Allen2016]

Law Alone is not Sufficient

- The increased usage of IT systems and networks leads to
  - huge amounts of data
  - easily searchable data
  - automatic analysis,
  - and knowledge extraction
- Data protection / Privacy law alone not sufficient
  - Not all processing can be controlled (e.g. every network node).
  - Deliberate breaking and bending of law (different legislations on the internet)
  - Economic pressure can force customers to give consent to almost any kind of 'privacy' policy (e.g. selling privacy for "peanuts").
- Slow pace of privacy self-regulation in the US, Focus on self-help
  - Self regulation by sustaining user ignorance
  - Enforcing norms may violate anti-trust.
  - Being a good actor (e.g. by exposing privacy practices) increases liability.
  - Legal compliance and related business processes (deemed) expensive

[Reagle1998, SelfReg1999, Bell2001, Hoofnagle2005]

⇨ Technical Privacy Protection
⇨ Standardization

Privacy principles and standardization

ISO/IEC IS 29100:2011 Privacy Framework defines the following 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

[ISO/IEC 29100:2011]

ISO/IEC JTC 1/SC 27
Information security, cybersecurity and privacy protection

ISO International Organization for Standardization

IEC International Electrotechnical Commission

ISO/IEC
JTC 1
Information Technology

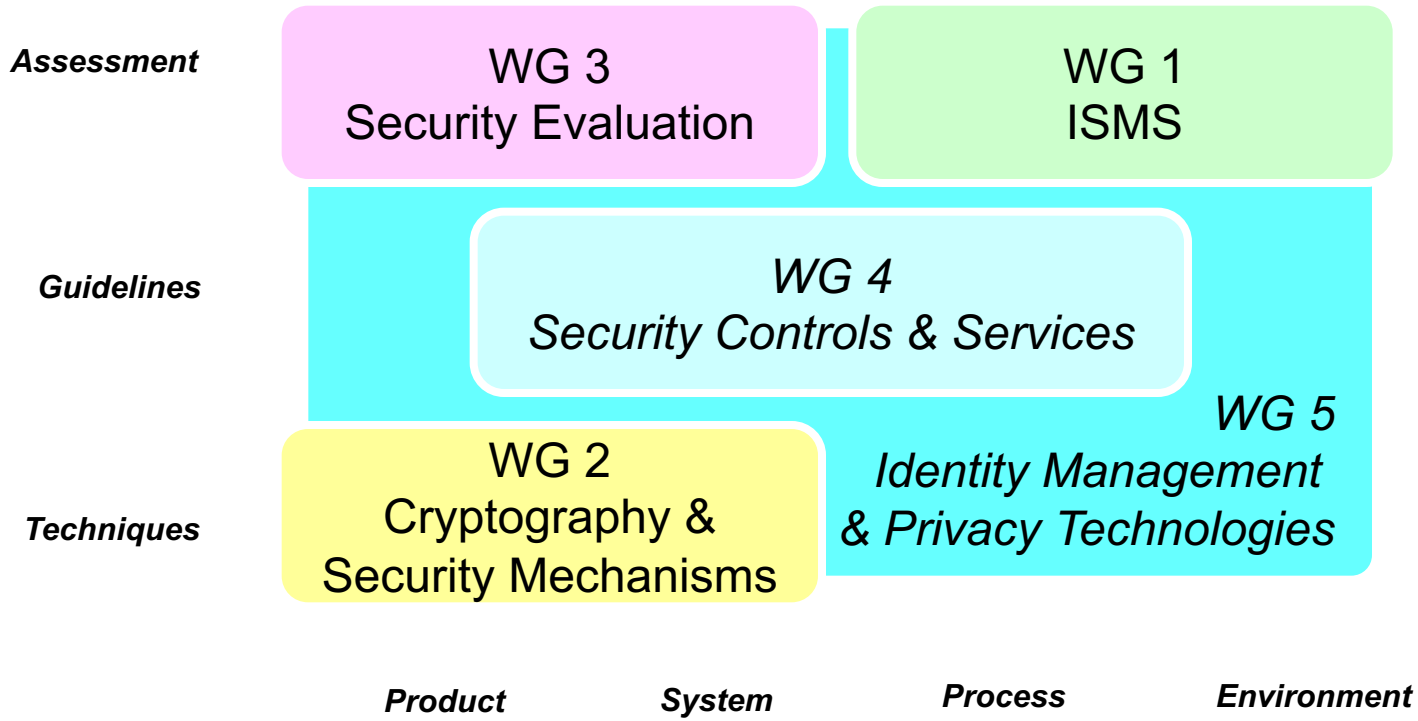
SC 2
Coded Character Sets

...

...

SC 42
Artificial intelligence

WGs within ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection



WG 5 Identity Management & Privacy Technologies Programme of Work (2008-04)

Frameworks & Architectures

- A Framework for Identity Management (ISO/IEC 24760, WD)
- A Privacy Framework (ISO/IEC 29100, WD)
- A Privacy Reference Architecture (ISO/IEC 29101, WD)
- A Framework for Access Management (ISO/IEC 29146, WD)

Protection Concepts

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

Guidance on Context and Assessment

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

WG 5 Identity Management & Privacy Technologies Programme of Work (2010-10)

Frameworks & Architectures

- A Framework for Identity Management (ISO/IEC 24760, FCD, WD, WD)
- Privacy Framework (ISO/IEC 29100, FCD)
- Privacy Reference Architecture (ISO/IEC 29101, CD)
- Entity Authentication Assurance Framework (ISO/IEC 29115 / ITU-T X.eaa, CD)
- A Framework for Access Management (ISO/IEC 29146, WD)

Protection Concepts

- Biometric information protection (ISO/IEC 24745, FDIS)
- 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)

WG 5 Identity Management & Privacy Technologies Programme of Work (2012-05)

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)

WG 5 Identity Management & Privacy Technologies Programme of Work (2014-10)

Frameworks & Architectures

- A Framework for Identity Management (ISO/IEC 24760, IS, FDIS, CD)
- 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, CD) (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, IS)
- Code of practice for PII protection in public clouds acting as PII processors (ISO/IEC 27018, IS)
- 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)

WG 5 Identity Management & Privacy Technologies Programme of Work (2016-09)

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, DIS) (formerly X.bhsm)
- Big data reference architecture – Part 4: Security and privacy fabric (ISO/IEC 20547-4, NP) (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, WD)

Guidance on Context and Assessment

- Authentication context for biometrics (ISO/IEC 24761, IS:2009/Cor 1:2013, Revision WD)
- 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, CD)
- Privacy impact assessment – methodology (ISO/IEC 29134, DIS)
- Code of practice for PII protection (ITU-T X.gpim | ISO/IEC 29151, DIS)
- Guidelines for online privacy notice and consent (ISO/IEC 29184, WD)
- Privacy engineering (ISO/IEC 27550, AWI)

WG 5 Identity Management & Privacy Technologies
Project overview (2018 – 11)

Frameworks & Architectures

- A framework for identity management (ISO/IEC 24760 (Parts 1-3, Part 1 Amendment 1), IS:2011, IS:2015, IS:2016, under publication)
- Privacy framework (ISO/IEC 29100, IS:2011)
- Privacy architecture framework (ISO/IEC 29101, IS:2013)
- Entity authentication assurance framework (ISO/IEC 29115, IS:2013, Revision WD)
- 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, IS:2017) (formerly X.bhsm)
- Big data reference architecture – Part 4: Security and privacy fabric (ISO/IEC 20547-4, CD) (together with WG 4)

Protection Concepts

- Biometric information protection (ISO/IEC 24745, IS:2011, Revision CD)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, IS:2012)
- Privacy enhancing data de-identification terminology and classification of techniques (ISO/IEC 20889:2018)
- Online privacy notice and consent (ISO/IEC 29184, CD)
- Requirements for attribute-based unlinkable entity authentication (ISO/IEC 27551, WD)
- Security requirements for authentication using biometrics on mobile devices (ISO/IEC 27553, WD)
- Establishing a PII deletion concept in organizations (ISO/IEC 27555, WD)

Guidance on Context and Assessment

- Authentication context for biometrics (ISO/IEC 24761, IS:2009/Cor 1:2013, Revision DIS)
- 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, TS:2018)
- Privacy impact assessment – methodology (ISO/IEC 29134, IS:2017)
- Code of practice for PII protection (ITU-T X.1058| ISO/IEC 29151, IS:2017) (formerly X.gpim)
- Privacy engineering for system life cycle processes (ISO/IEC 27550, PDTR)
- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management – Requirements and guidelines (ISO/IEC 27552, DIS)
- Privacy guidelines for Smart Cities (ISO/IEC TS 27570, WD)
- Application of ISO 31000 for assessment of identity management-related risk (ISO/IEC 27554, WD)

WG 5 Identity Management & Privacy Technologies
Project overview (2020 – 03)

Frameworks & Architectures

- A framework for identity management (ISO/IEC 24760 (Parts 1-3), IS:2019, IS:2015, IS:2016)
- Privacy framework (ISO/IEC 29100, IS:2011; Amendment 1:2018)
- Privacy architecture framework (ISO/IEC 29101, IS:2018)
- Entity authentication assurance framework (ISO/IEC 29115, IS:2013, Revision WD)
- 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, IS:2017) (formerly X.bhsm)
- Big data reference architecture – Part 4: Security and privacy fabric (ISO/IEC 20547-4, DIS) (together with WG 4)
- User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences (ISO/IEC 27556, WD)

Protection Concepts

- Biometric information protection (ISO/IEC 24745, IS:2011, Revision CD)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, IS:2012)
- Privacy enhancing data de-identification terminology and classification of techniques (ISO/IEC 20889, IS:2018)
- Online privacy notice and consent (ISO/IEC 29184, FDIS)
- Requirements for attribute-based unlinkable entity authentication (ISO/IEC 27551, DIS)
- Security requirements for authentication using biometrics on mobile devices (ISO/IEC 27553, WD)
- Guidelines on personally identifiable information deletion (ISO/IEC 27555, CD)

Guidance on Context and Assessment

- Authentication context for biometrics (ISO/IEC 24761, IS:2009/Cor 1:2013, Revision 2019)
- 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:2019)
- Identity proofing (ISO/IEC 29003, TS:2018)
- Privacy impact assessment – methodology (ISO/IEC 29134, IS:2017)
- Code of practice for PII protection (ITU-T X.1058| ISO/IEC 29151, IS: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, IS:2019 (previously 27552))
- Privacy guidelines for Smart Cities (ISO/IEC TS 27570, DTS)
- Application of ISO 31000 for assessment of identity management-related risk (ISO/IEC 27554, WD)

WG 5 Identity Management & Privacy Technologies
Project overview (2020 – 06)

Frameworks & Architectures

- A framework for identity management (ISO/IEC 24760 (Parts 1-3), IS:2019, IS:2015, IS:2016)
- Privacy framework (ISO/IEC 29100, IS:2011; Amendment 1:2018)
- Privacy architecture framework (ISO/IEC 29101, IS:2018)
- Entity authentication assurance framework (ISO/IEC 29115, IS:2013, Revision WD)
- 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, IS:2017) (formerly X.bhsm)
- Big data reference architecture – Part 4: Security and privacy fabric (ISO/IEC 20547-4, DIS) (together with WG 4)
- User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences (ISO/IEC 27556, CD)
- Privacy enhancing data de-identification framework (ISO/IEC 27559, WD)

Protection Concepts

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

Guidance on Context and Assessment

- Authentication context for biometrics (ISO/IEC 24761, IS:2009/Cor 1:2013, Revision 2019)
- 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:2019)
- Identity proofing (ISO/IEC 29003, TS:2018)
- Privacy impact assessment – methodology (ISO/IEC 29134, IS:2017)
- Code of practice for PII protection (ITU-T X.1058| ISO/IEC 29151, IS: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, IS:2019 (formerly 27552))
- Privacy guidelines for Smart Cities (ISO/IEC TS 27570, DTS)
- Application of ISO 31000 for assessment of identity management-related risk (ISO/IEC 27554, WD)
- Organizational privacy risk management (ISO/IEC 27557, WD)
- Requirements for bodies providing audit and certification of privacy information management systems according to ISO/IEC 27701 in combination with ISO/IEC 27001 (ISO/IEC 27006-2 (27558), DTS) (together with WG 1)

WG 5 Identity Management & Privacy Technologies
Project overview (2020 – 11)

Frameworks & Architectures

- A framework for identity management (ISO/IEC 24760 (Parts 1-3), IS:2011, Revision 2019; IS:2015, Rev; IS:2016, AMD)
- 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)
- 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, CD)
- Privacy enhancing data de-identification framework (ISO/IEC 27559, WD)

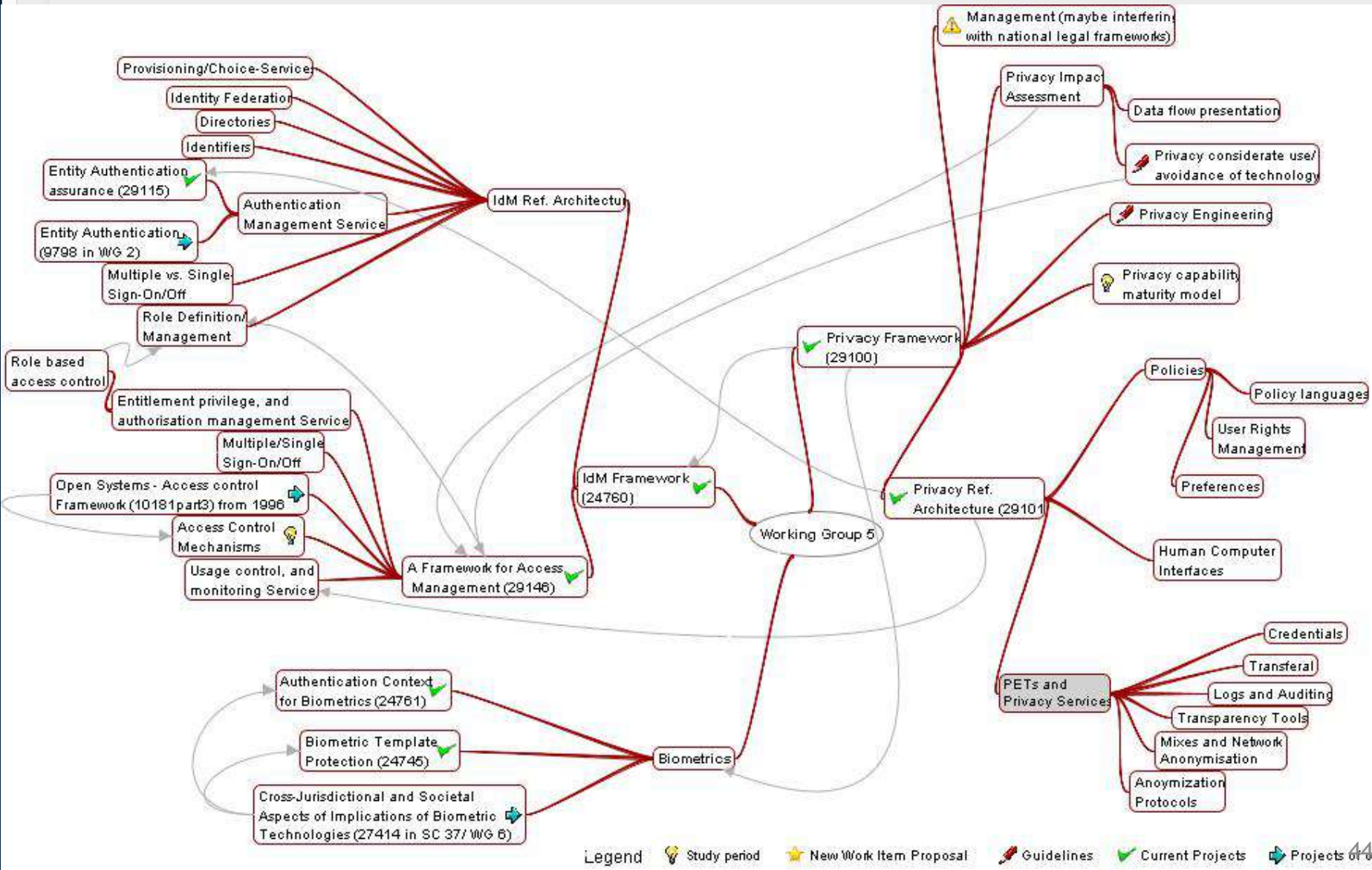
Protection Concepts

- Biometric information protection (ISO/IEC 24745:2011, Revision DIS)
- 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, DIS)
- Security requirements for authentication using biometrics on mobile devices (ISO/IEC 27553, CD)
- Guidelines on personally identifiable information deletion (ISO/IEC 27555, DIS)
- Consent record information structure (ISO/IEC TS 27560, WD)

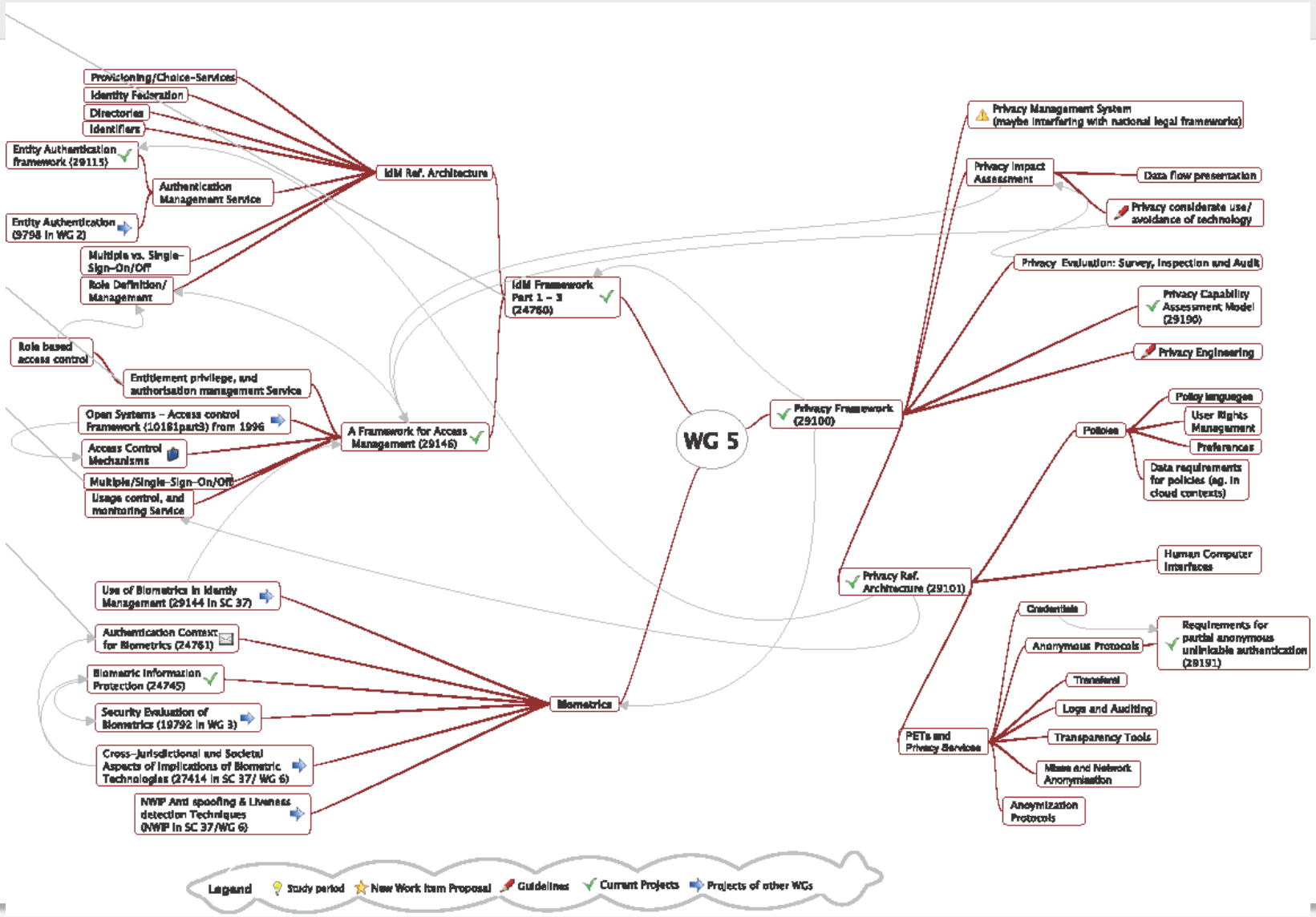
Guidance on Context and Assessment

- 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)
- 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 PRF TS 27570)
- Application of ISO 31000 for assessment of identity management-related risk (ISO/IEC 27554, WD)
- Organizational privacy risk management (ISO/IEC 27557, WD)
- Requirements for bodies providing audit and certification of information security management systems – Part 2: Privacy information management systems (ISO/IEC TS 27006-2 (27558), DTS)

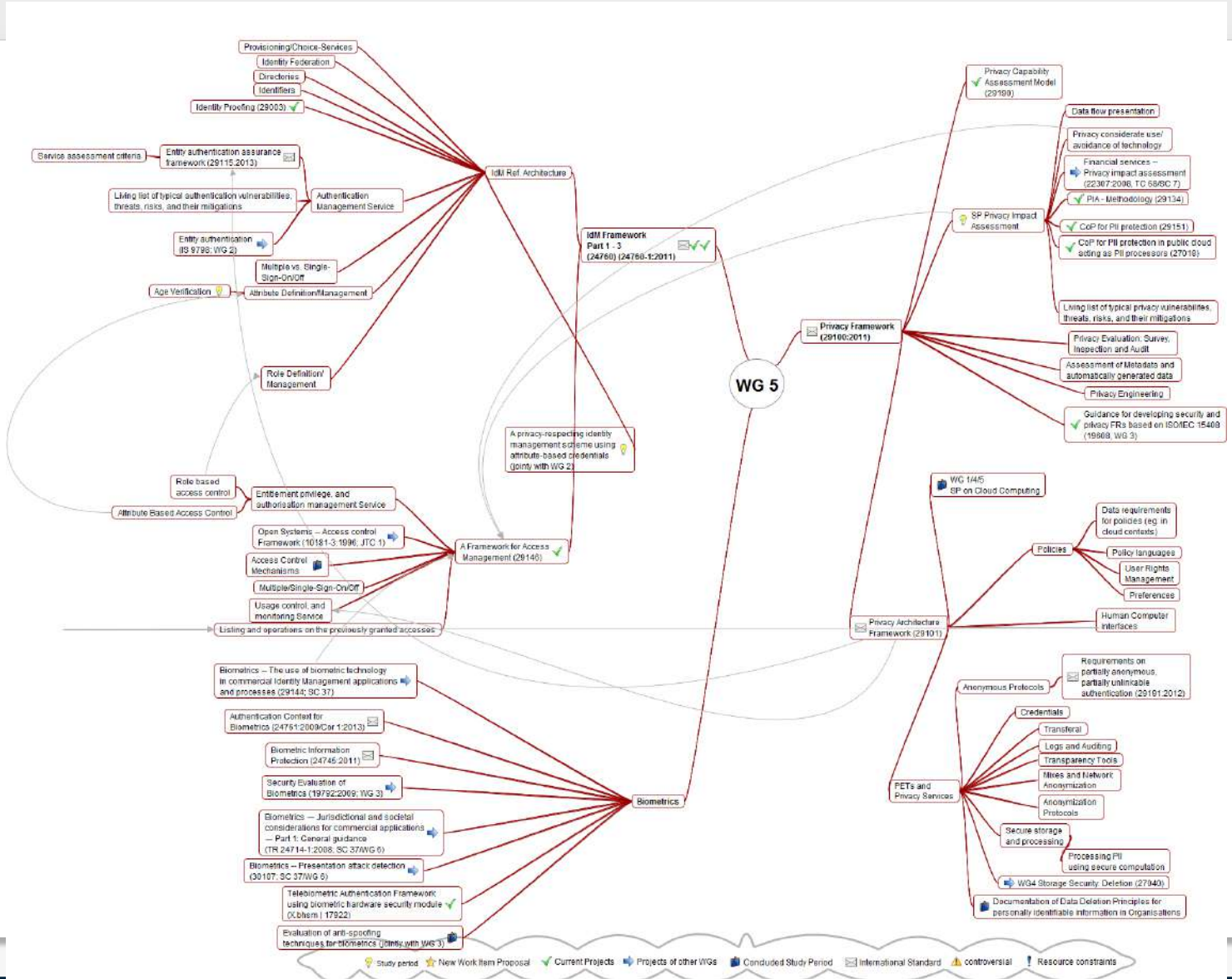
WG 5 Identity Management & Privacy Technologies Roadmap (2008-04)



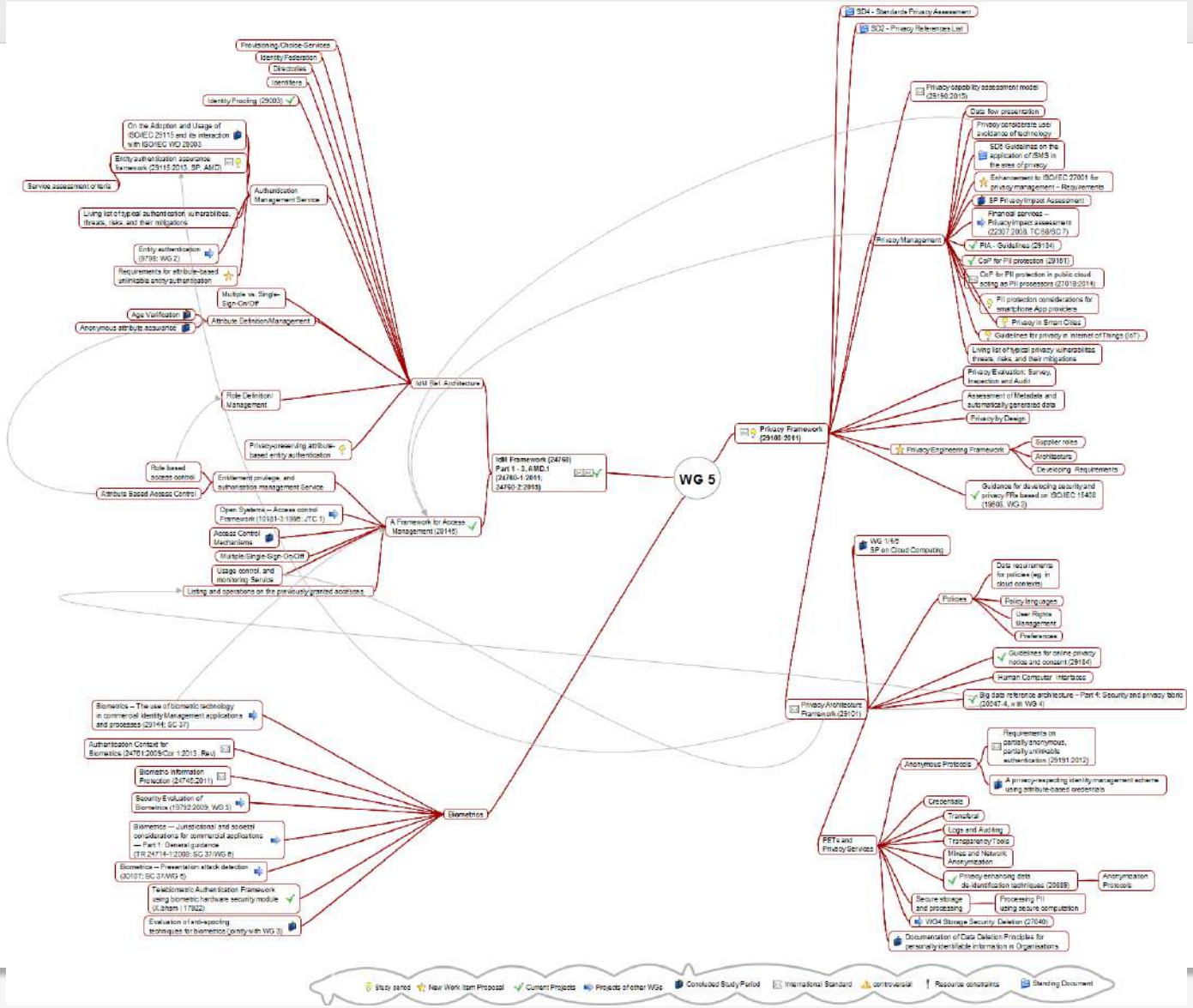
WG 5 Identity Management & Privacy Technologies Roadmap (2010-10)



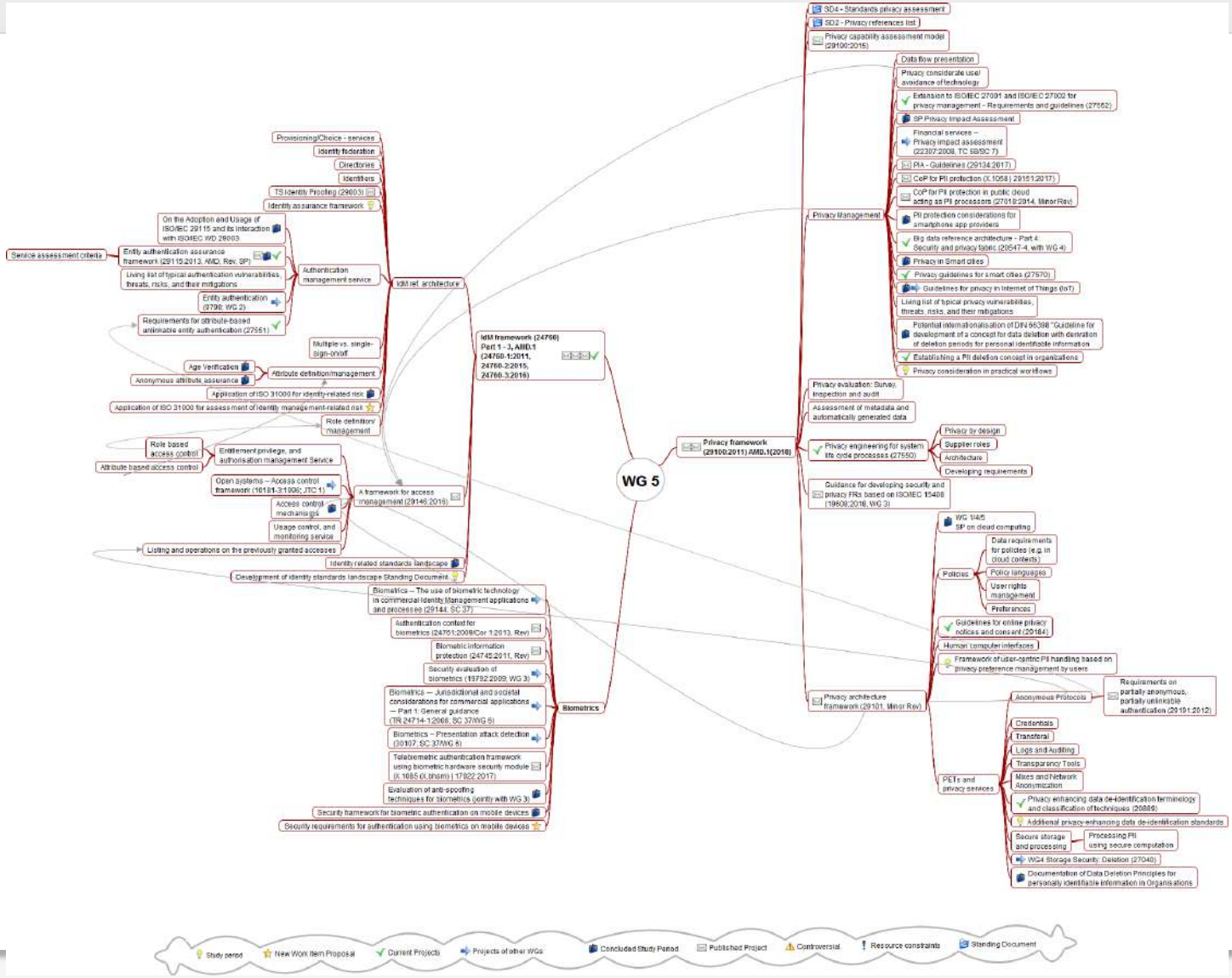
WG 5 Identity Management & Privacy Technologies Roadmap (2014-09)



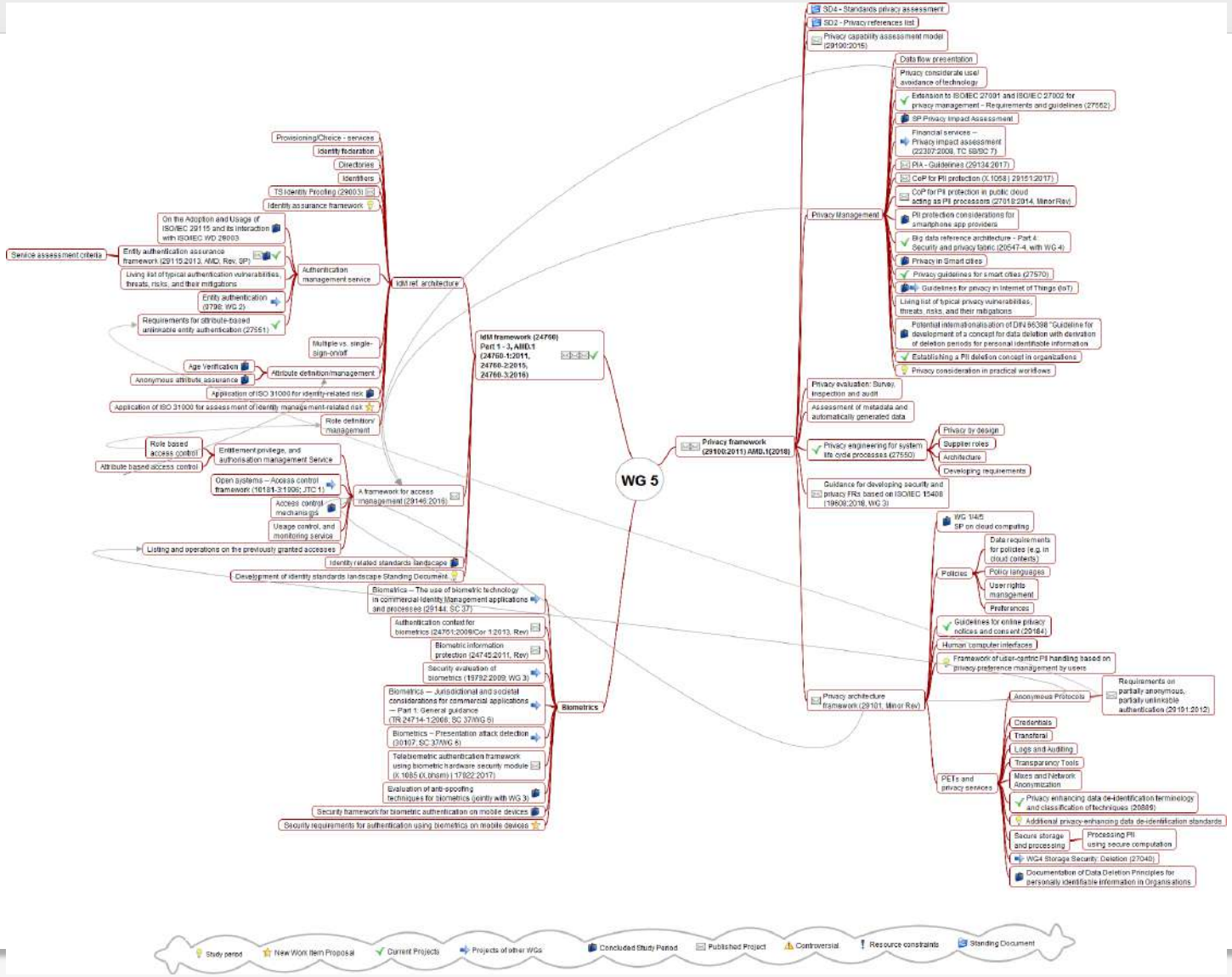
WG 5 Identity Management & Privacy Technologies Roadmap (2016-05)



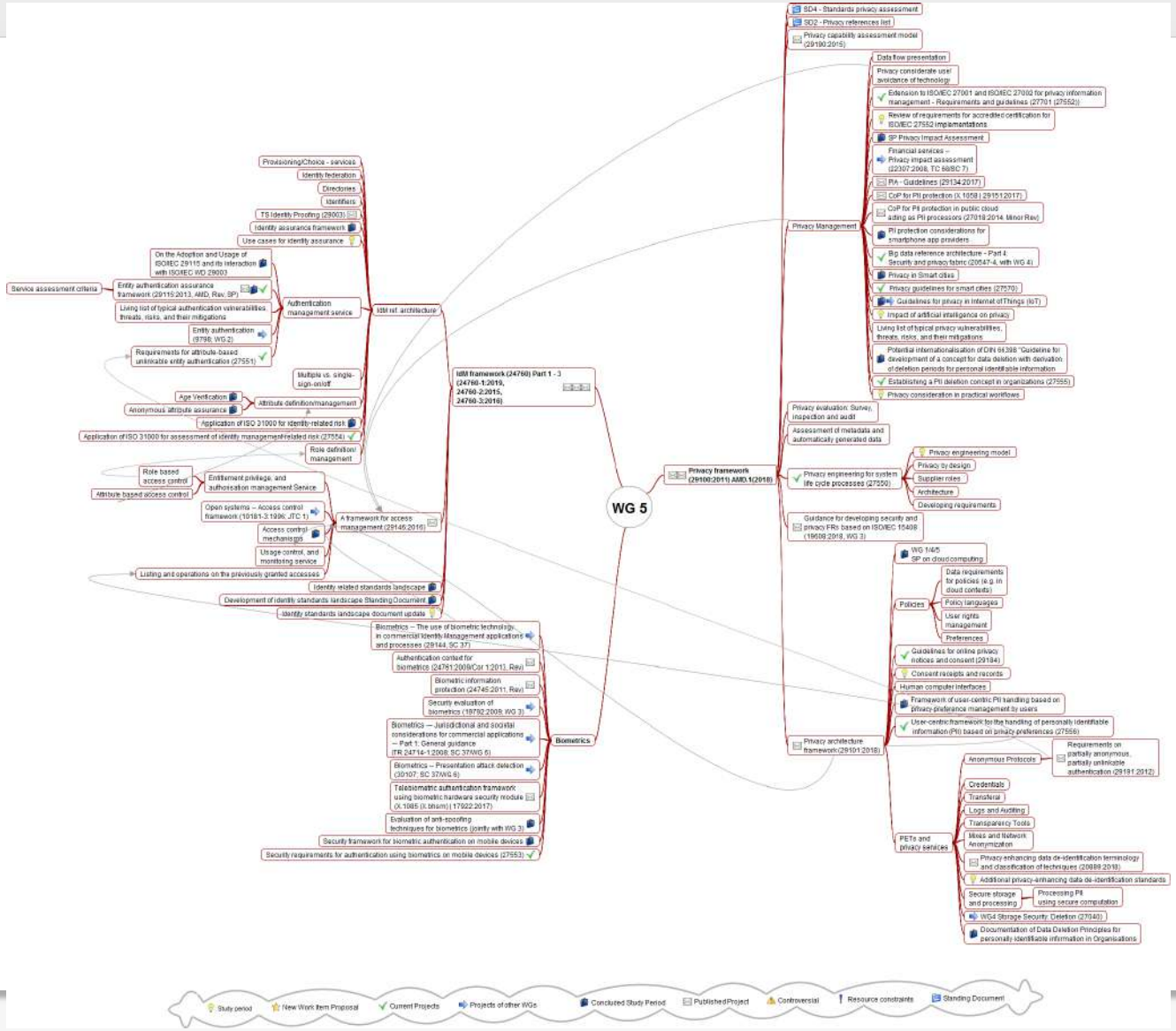
WG 5 Identity Management & Privacy Technologies Roadmap (2018 – 10)



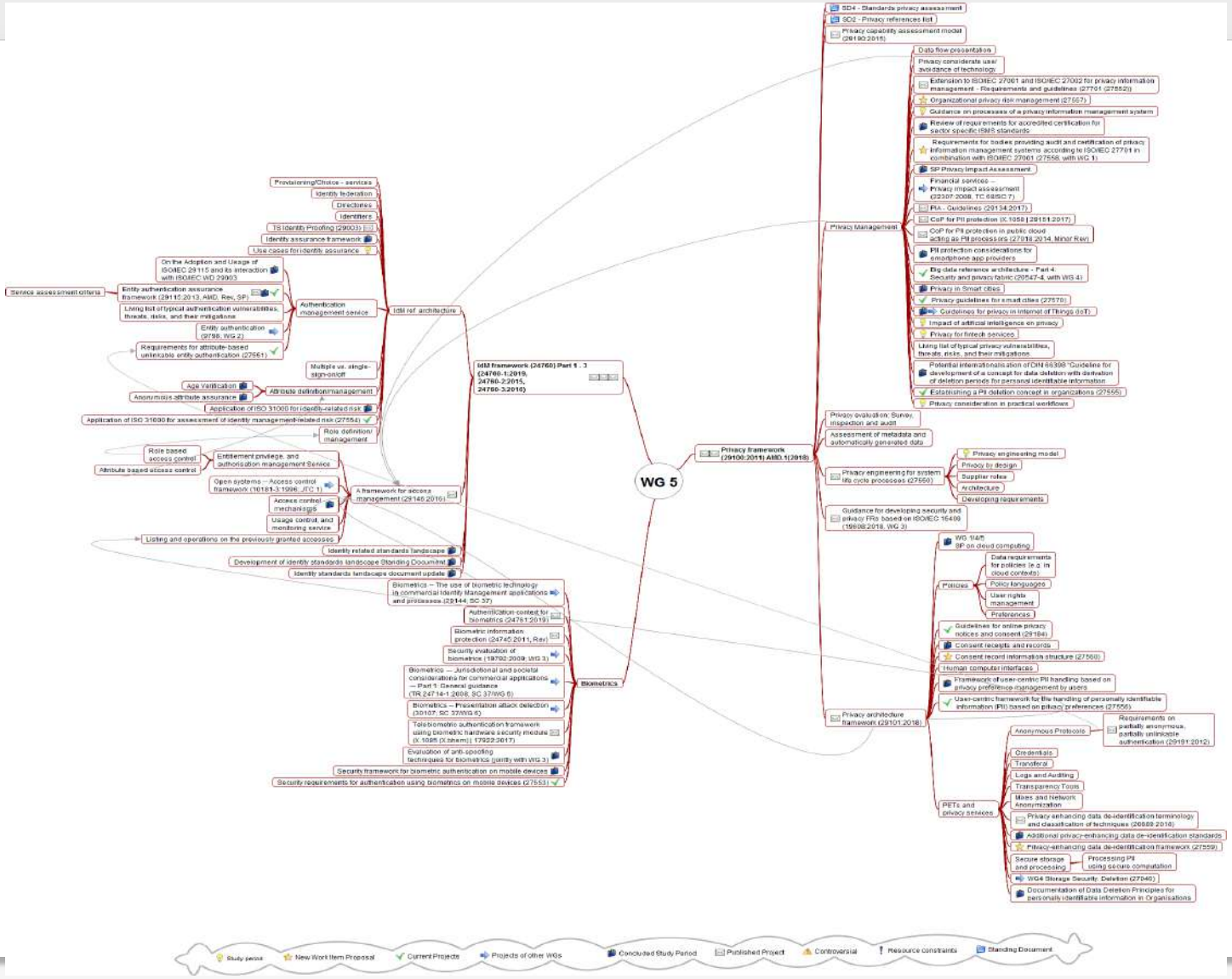
WG 5 Identity Management & Privacy Technologies Roadmap (2018 – 10)



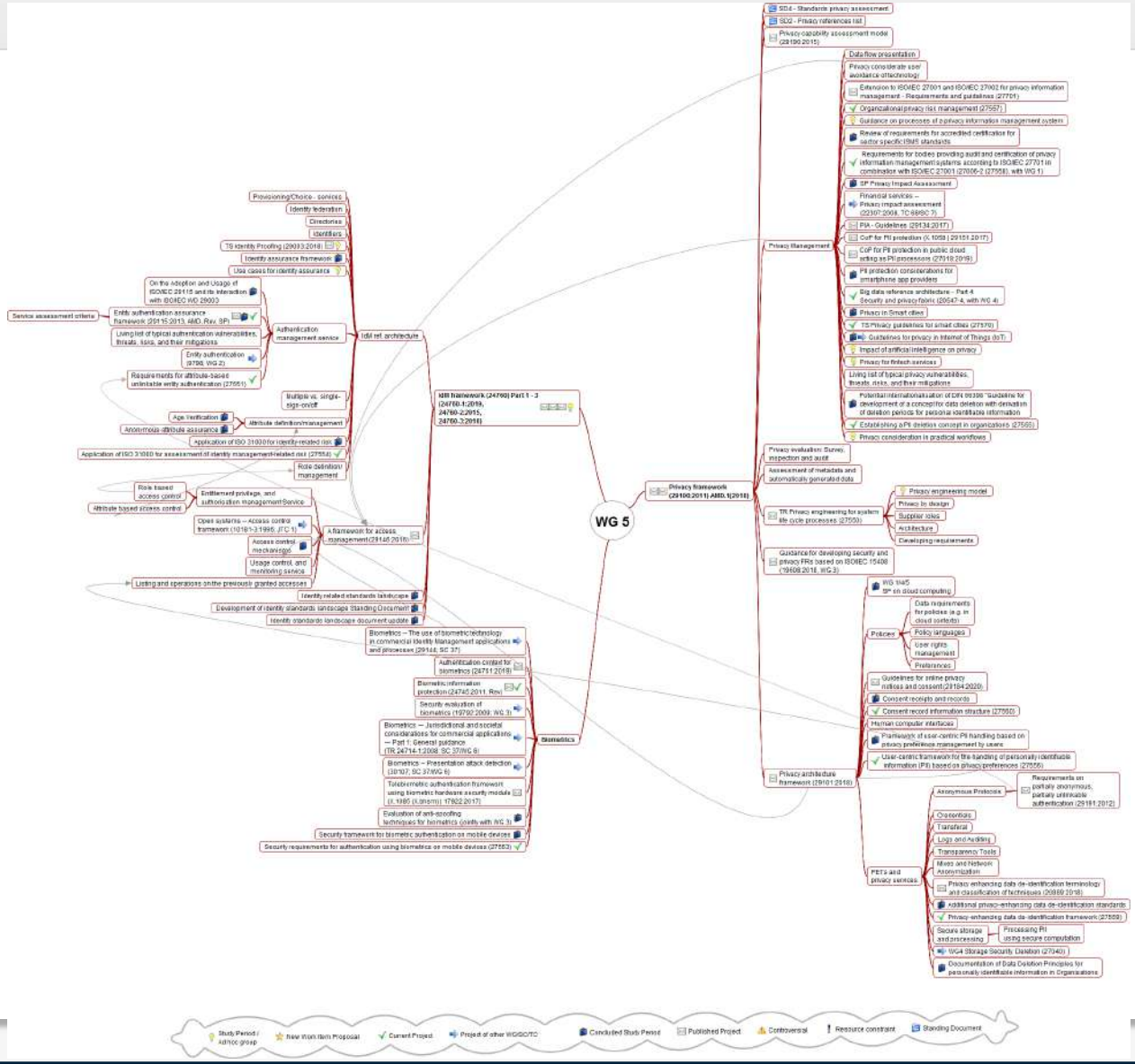
WG 5 Identity Management & Privacy Technologies Roadmap (2019 –07)



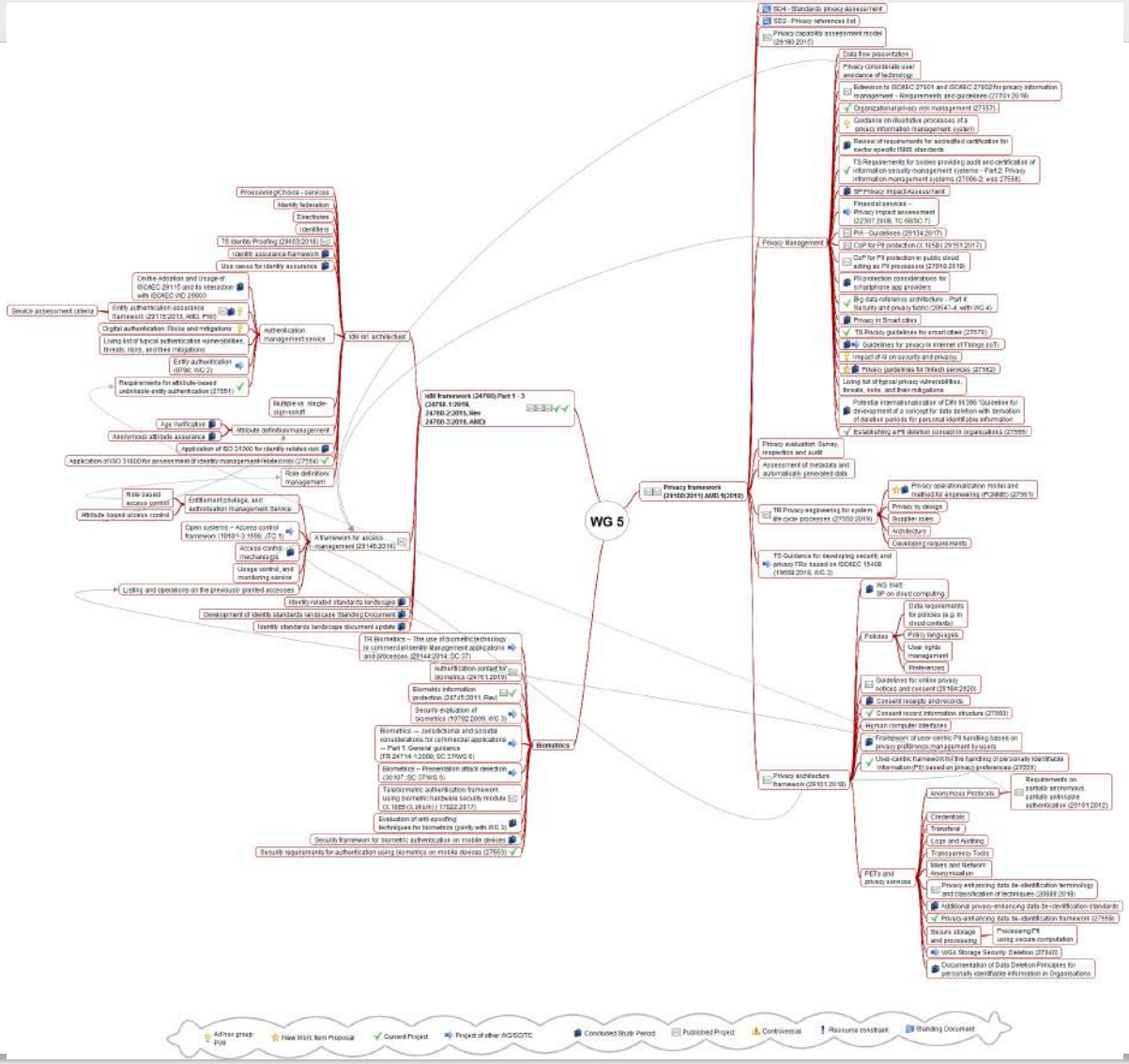
WG 5 Identity Management & Privacy Technologies Roadmap (2020 – 01)



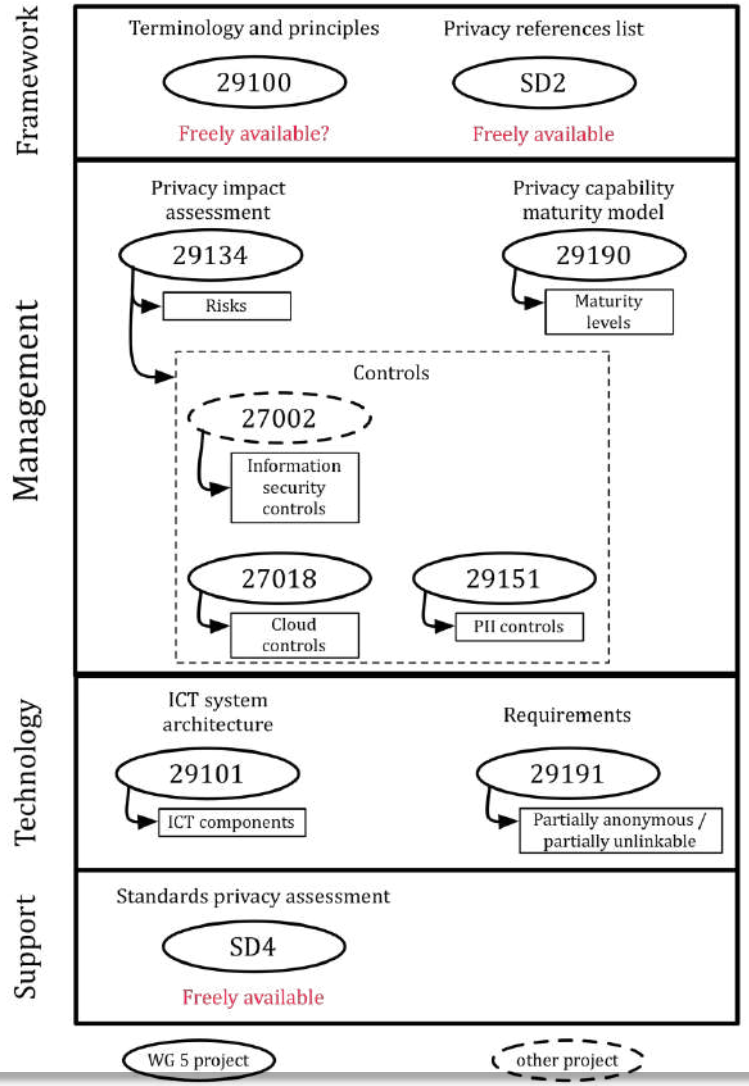
WG 5 Identity Management & Privacy Technologies Roadmap (2020 – 06)



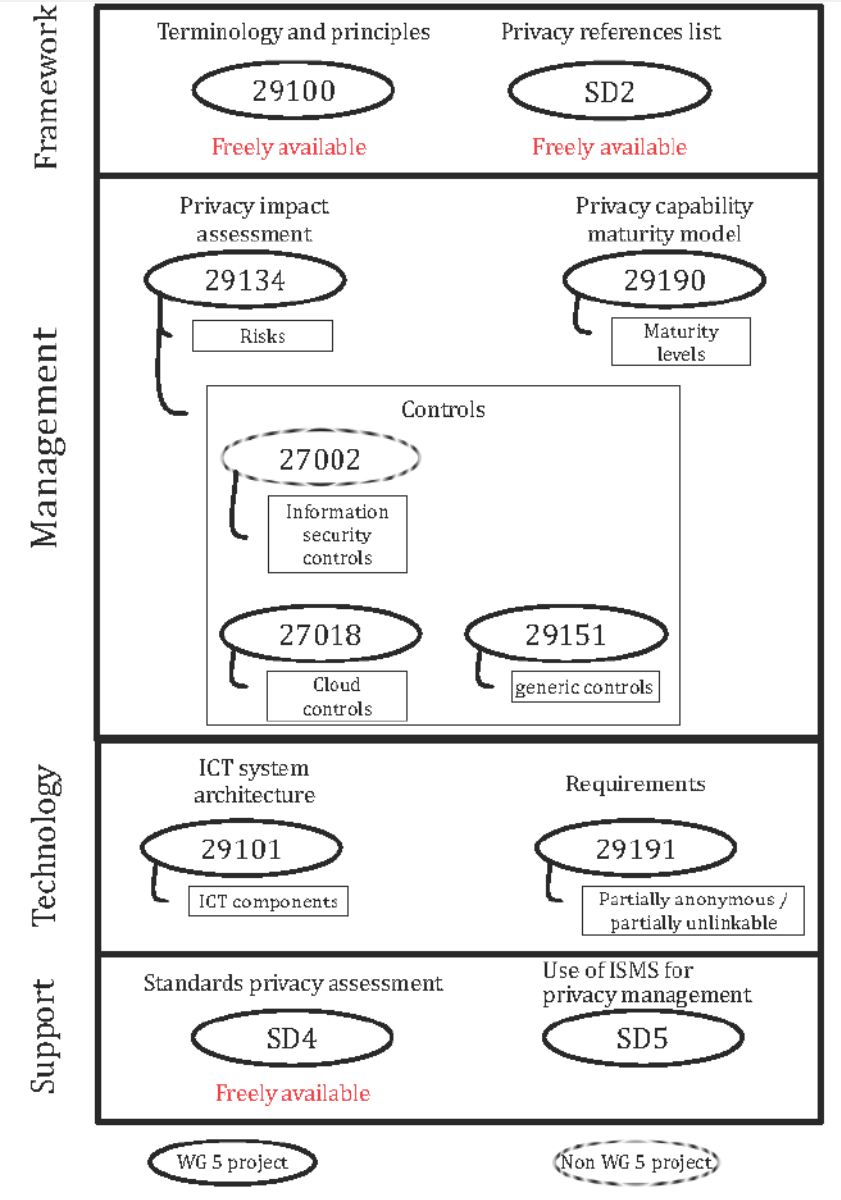
WG 5 Identity Management & Privacy Technologies Roadmap (2020 – 11)



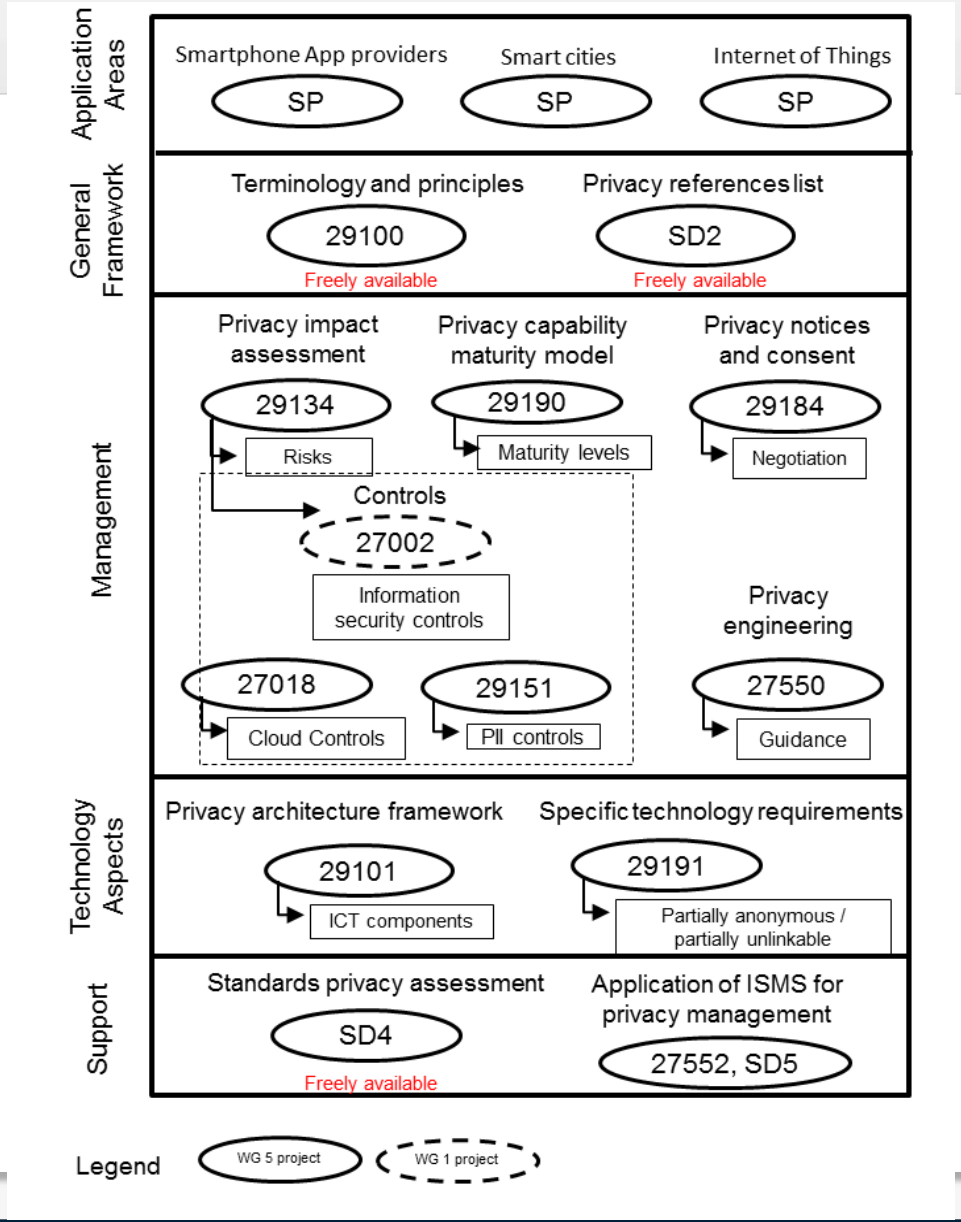
Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2013-07)



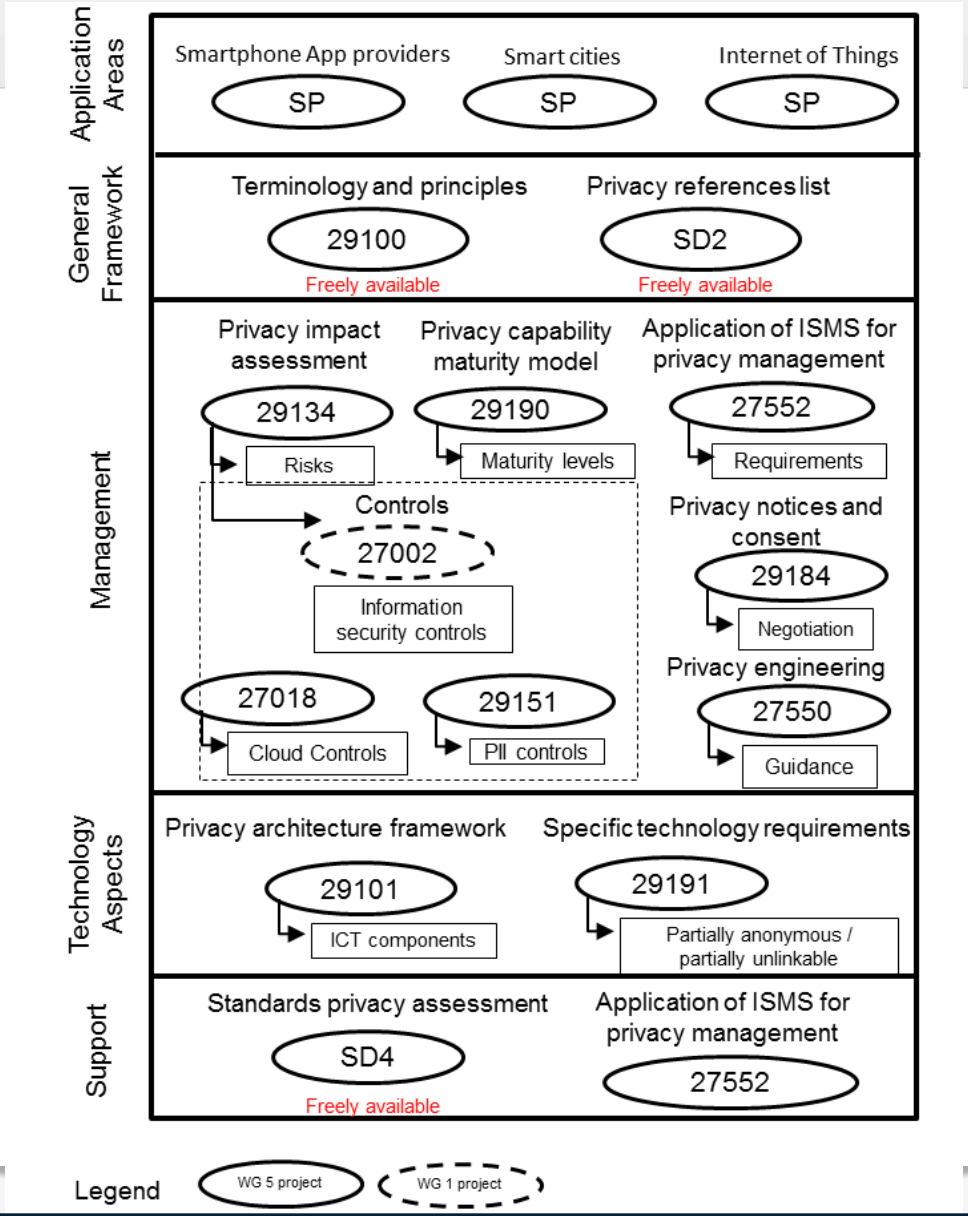
Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2014-12)



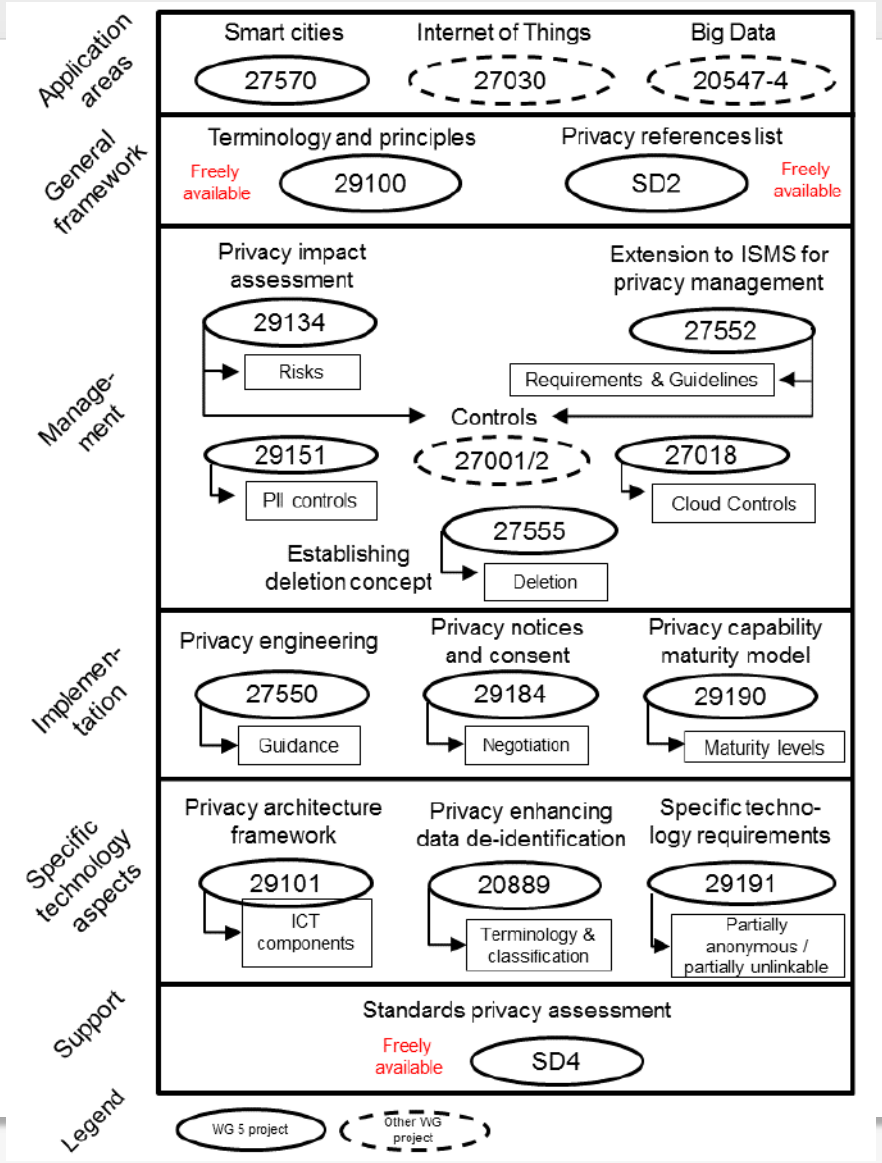
Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2016-09)



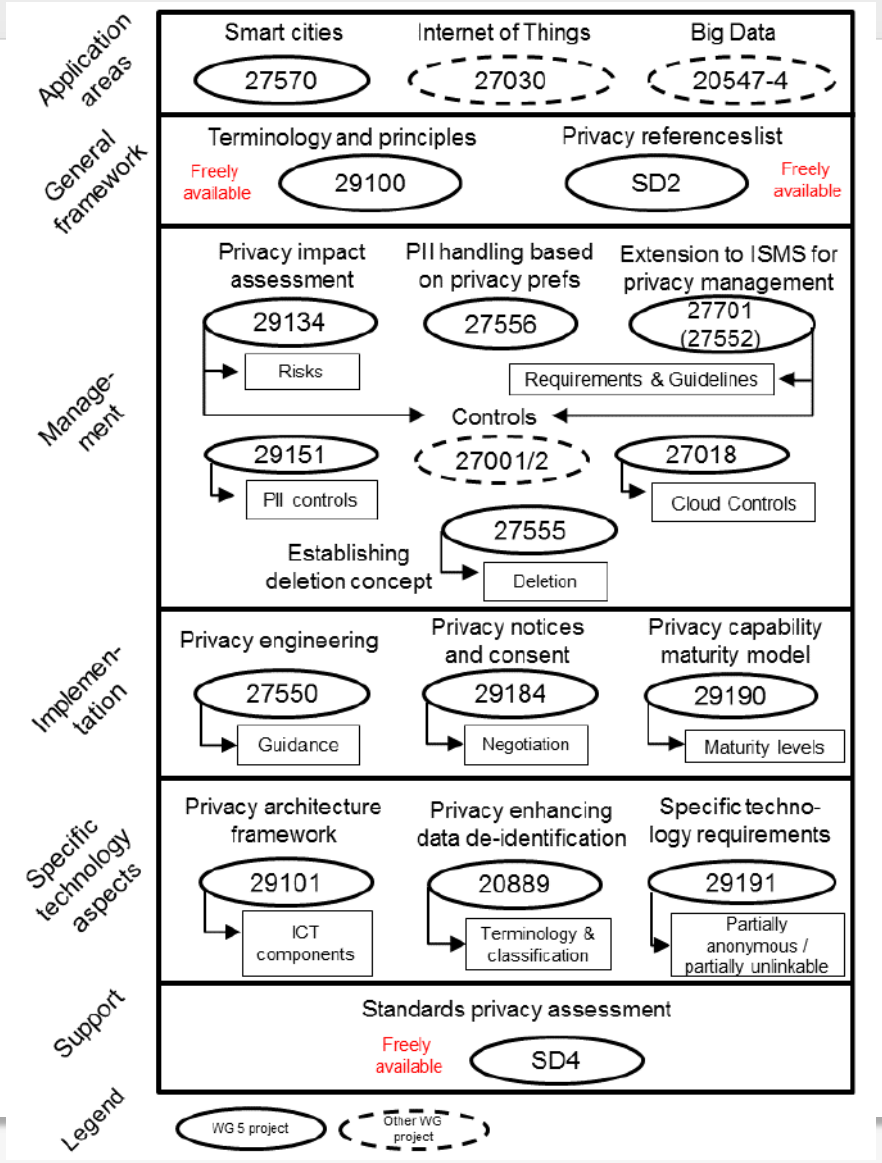
Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2016-12)



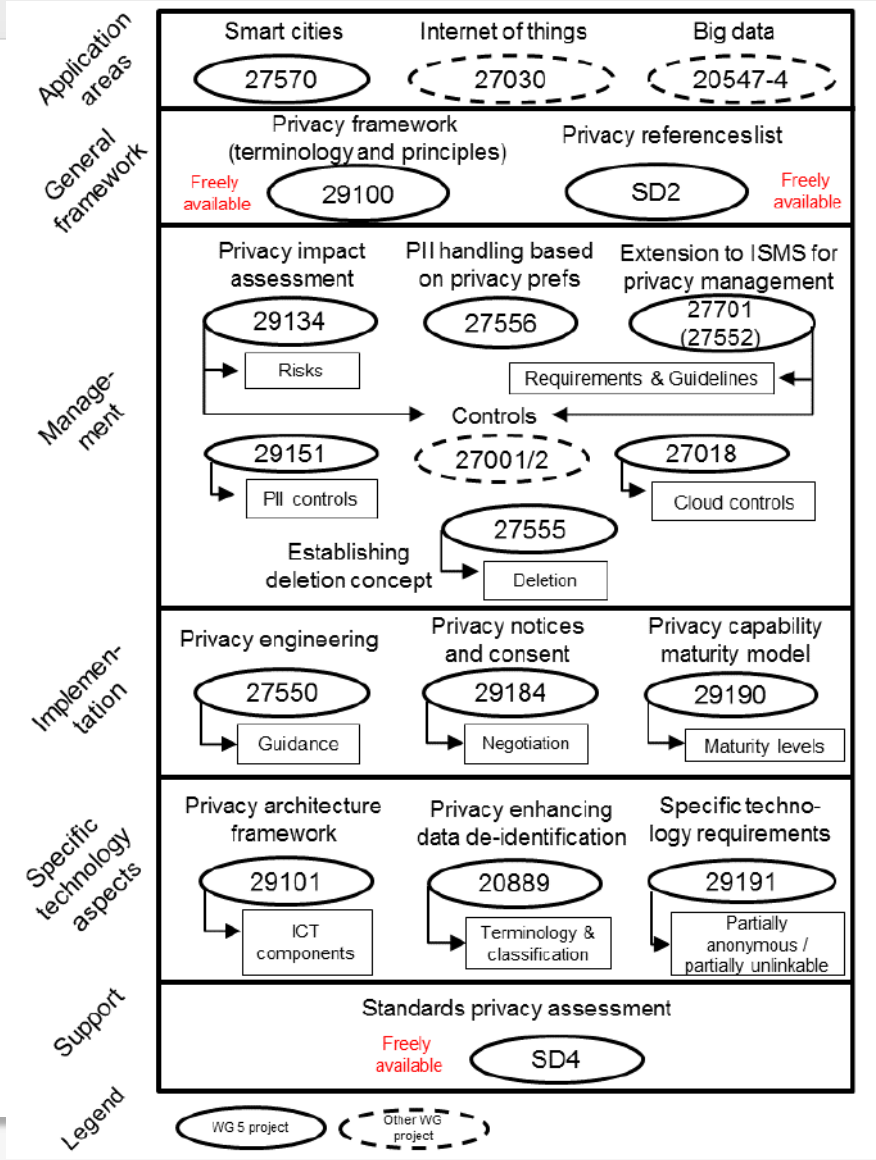
Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2018-10)



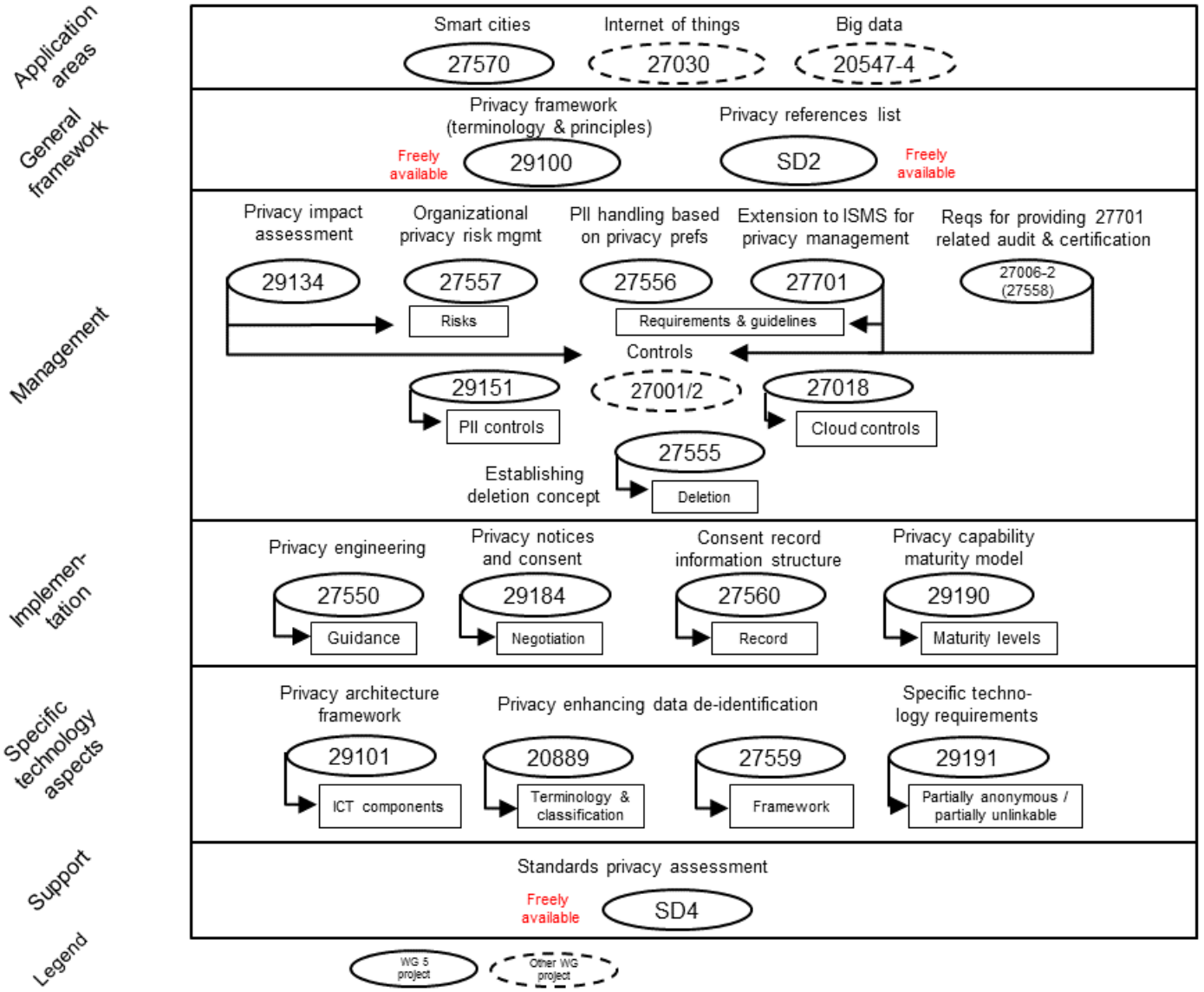
Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2019-07)



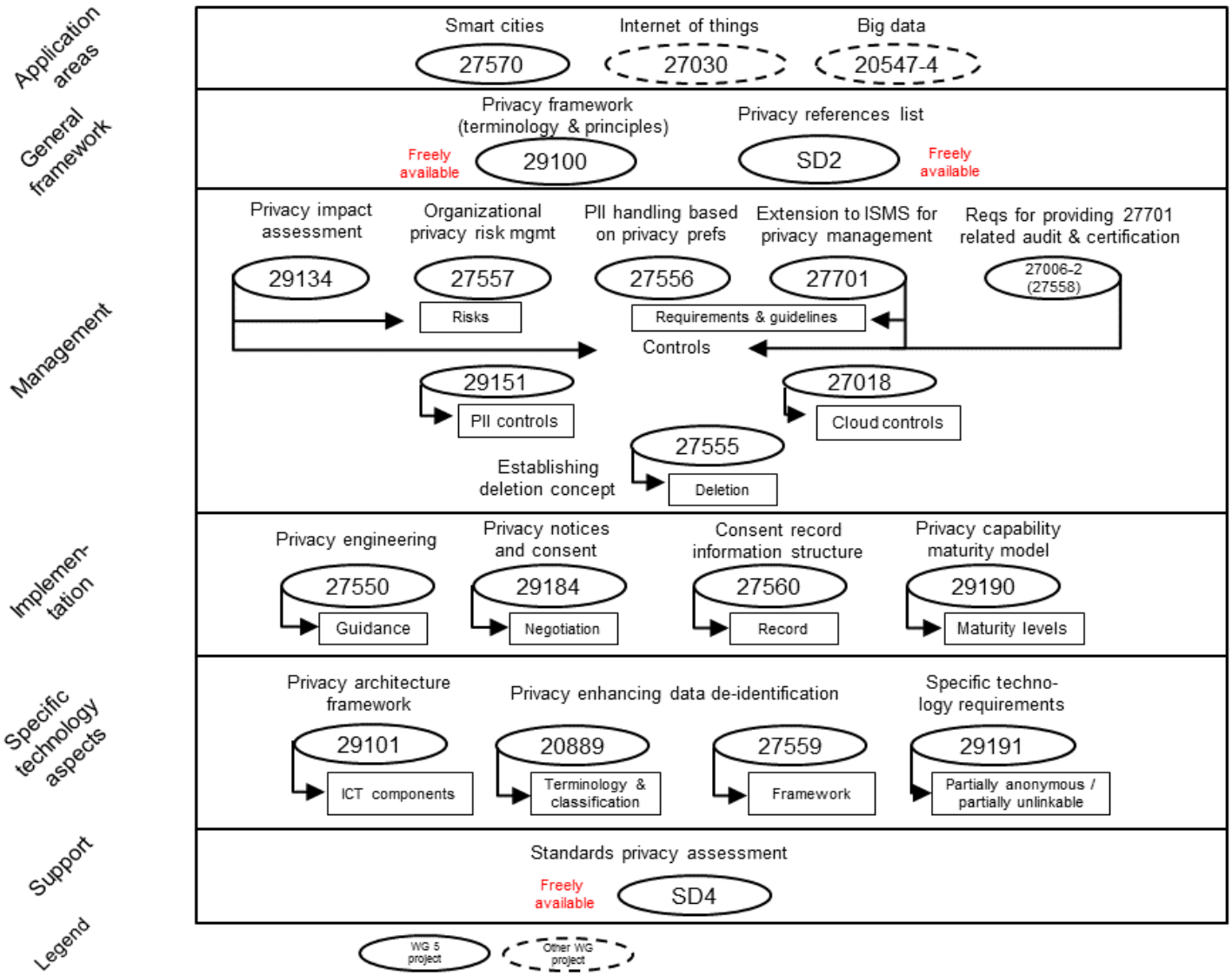
Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2020-01)



Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2020-06)



Privacy/PII Standards and Projects in SC 27, mainly WG 5 (2020-11)



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)

Art 4: Definition of personal data and pseudonymisation	**20889:2018** Privacy enhancing data de-identification terminology and classification of techniques **27559 WD** 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 **TS 27560 WD** 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 WD** Organizational privacy risk management
Art 35: DPIA	**29134:2017** 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 DTS** Requirements for bodies providing audit and certification of information security management systems – Part 2: Privacy information management systems

mobile business

Agenda

- Data Protection and Privacy
  - Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Communication systems
  - Transaction systems
- Concepts of Privacy Protection
  - Privacy by Design (PbD)
  - Privacy Engineering
  - Transparency
  - Usability
- Integrated Privacy Protection
  - PRIME LBS
  - ABC4Trust
  - Privacy Advisor
  - Privacy Risk Communication and Mitigation

Technical Privacy Protection

- Individuals
  - want to control the amount of identity information visible from the outside.
  - consider what personal information they reveal to whom.
- Typical protection techniques are:
  - Anonymization and identity management tools
  - Spontaneous switching between different levels of anonymity and pseudonymity depending on the context

mobile business

Privacy-X Technologies

- Privacy-enhancing technologies
- Privacy-friendly technologies
- Privacy-preserving technologies
- Privacy-protecting technologies
- Privacy-respecting technologies

Building Blocks and Approaches for Privacy Technologies

- Strong privacy requirements:
  - No trust in the system operator, and
  - No trust into one centralized entity.
- Most common methods consider:
  - Communication systems, or
  - Transactions systems

mobile business

Communication Systems

- The Anonymizer

  www.anonymizer.com
- Mixmaster – Anonymous Remailer

  http://mixmaster.sourceforge.net
- Onion Routing: Tor Network

  http://tor.eff.org/
- Java Anonymous Proxy (JAP)

  http://anon.inf.tu-dresden.de
- Cookie Cooker

  www.cookiecooker.de
- P3P – Platform for Privacy Preferences

  www.w3.org/P3P

Transaction Systems

- Reachability management
- Credential technologies
  - U-Prove

    www.microsoft.com/uprove
  - Idemix

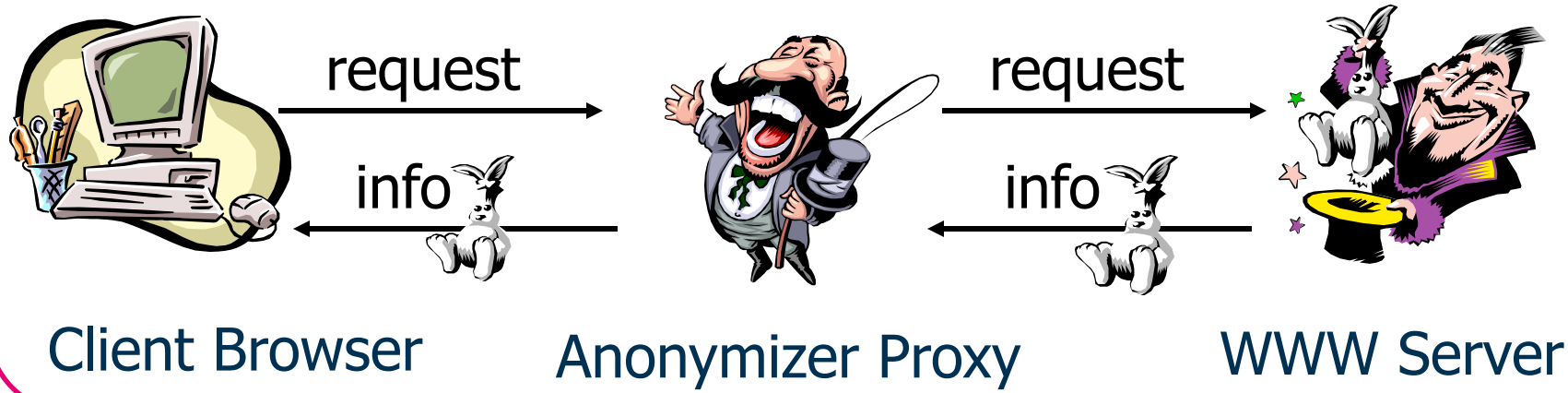
    www.zurich.ibm.com/security/idemix

mobile business

Agenda

- Data Protection and Privacy
  - Origin and definition
  - Law, Technology, Standardization
- Technical Privacy Protection
  - Communication systems
  - Transaction systems
- Concepts of Privacy Protection
  - Privacy by Design (PbD)
  - Privacy Engineering
  - Transparency
  - Usability
- Integrated Privacy Protection
  - PRIME LBS
  - ABC4Trust
  - Privacy Advisor
  - Privacy Risk Communication and Mitigation

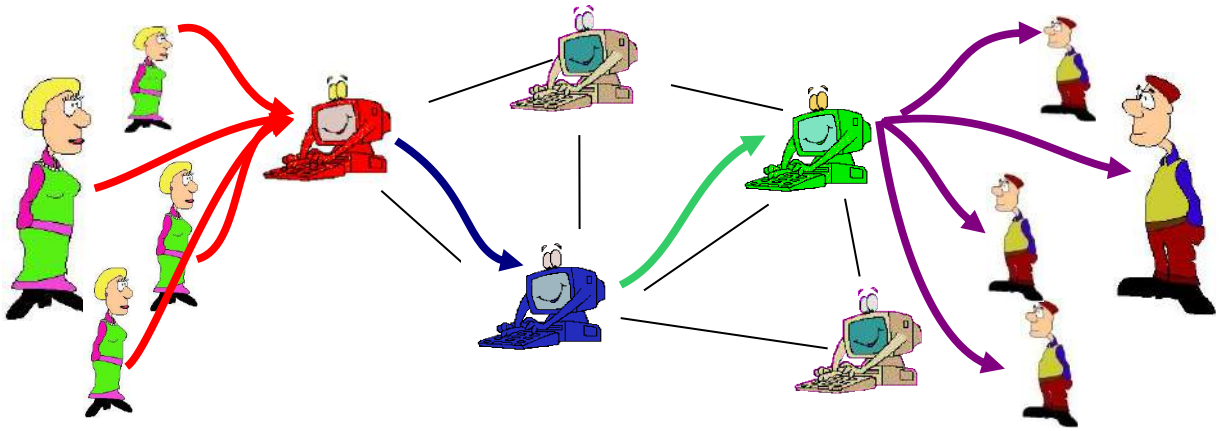
www.anonymizer.com



www.anonymizer.com

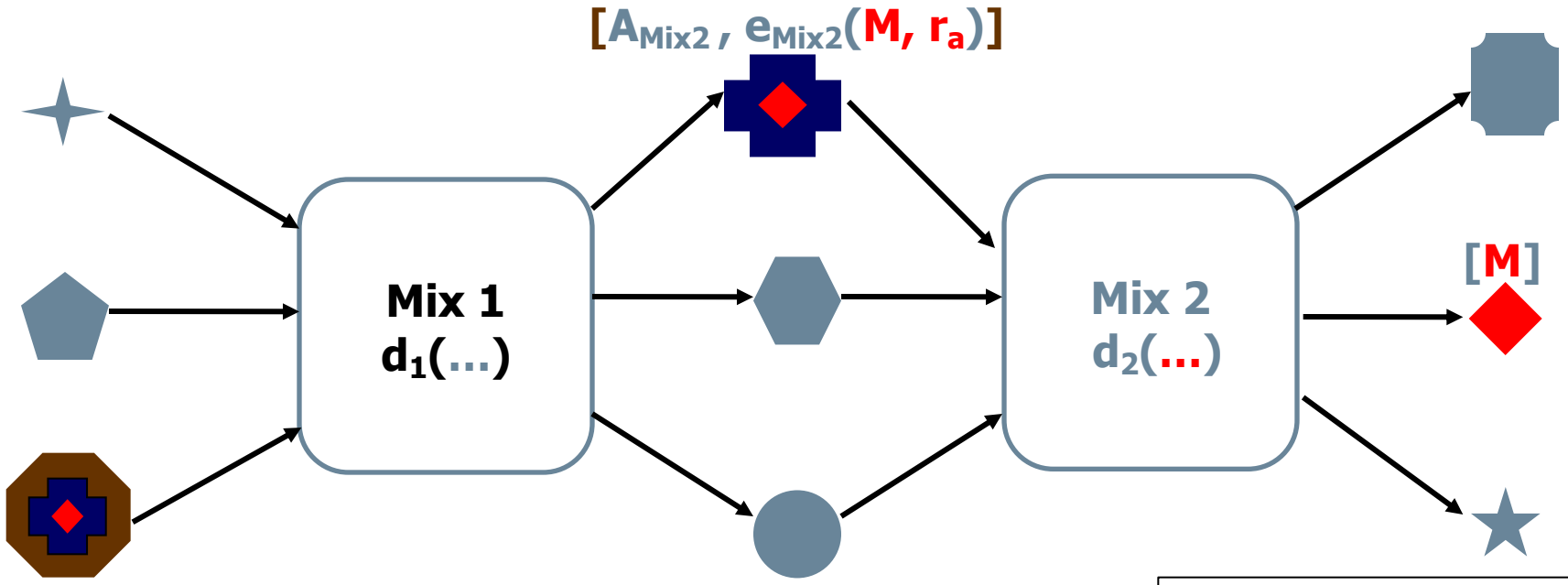
- ↑ Client (anonymity) is protected in an "**anonymity set**" of all possible proxy clients.
- ↓ Anonymizer learns about client's activities / interests.
- ↓ No protection against attackers with global view.

Mixes and Onion Routing



- *Communication is anonymized by multiple mix servers, also called onion routers.*
  - *Both onion routing and JAP are based on the same Mix concept.*

Mixes



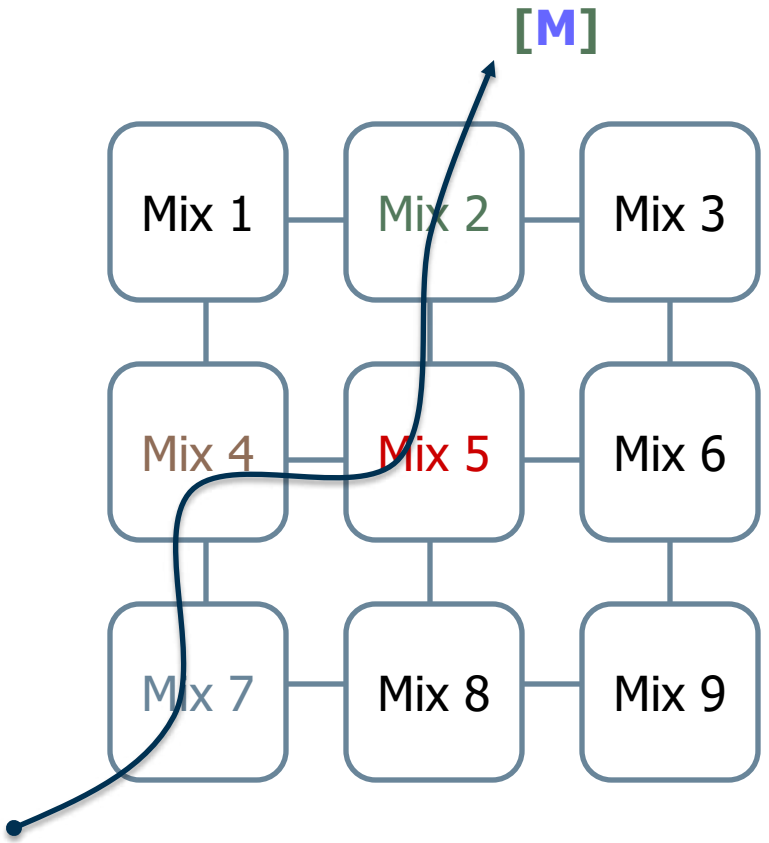
- Decode, buffer, reorder, and resend incoming messages
- Protect **unlinkability** of input / output messages
- Protect **unobservability** of connections and relations
- No single point of trust / failure

Symbols:
A address
e() encryption function
d() decryption function
M core message
r random value
[] message boundary

[Chaum1981]

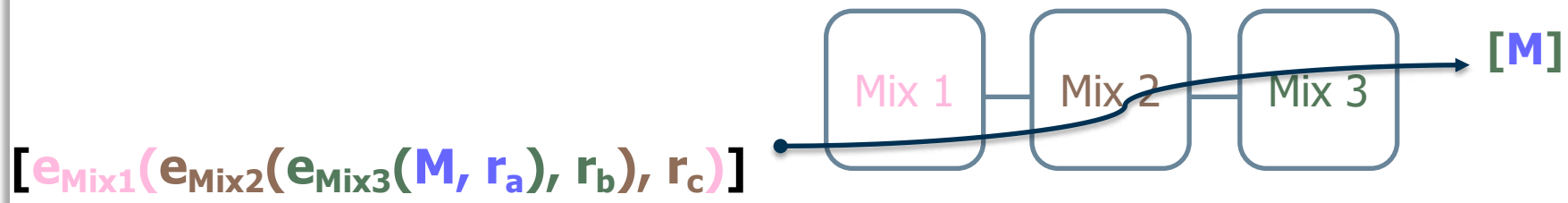
Mix Network

- Choose the way of your message through the mixes!
- Protection guaranteed as long as one chosen mix withstands attacks.
- Free path results in additional confusion, but smaller anonymity set.



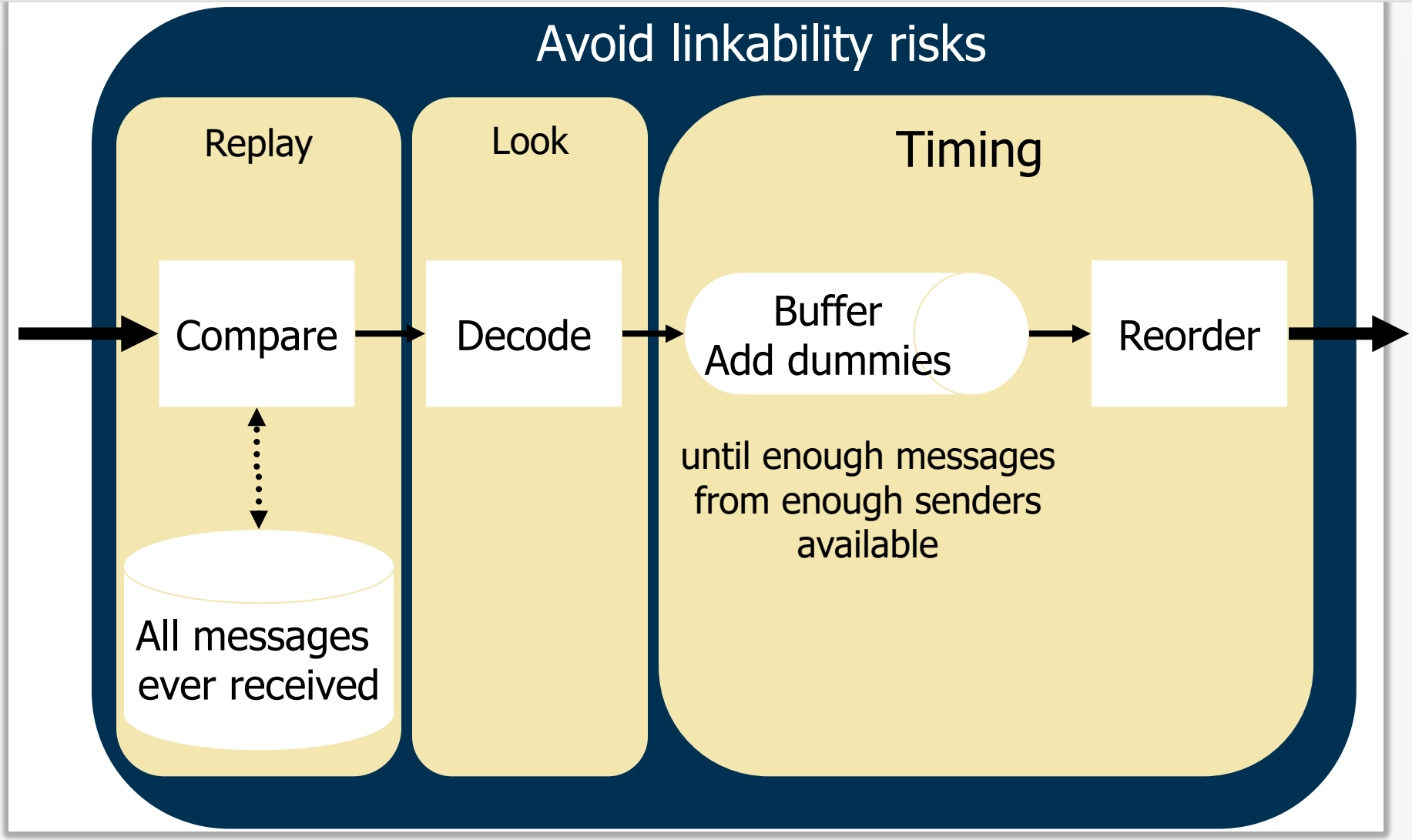
$$[A_{Mix7}, e_{Mix7}(A_{Mix4}, e_{Mix4}(A_{Mix5}, e_{Mix5}(A_{Mix2}, e_{Mix2}(M, r_a), r_b), r_c), r_d)]$$

Mix Cascade



- Fixed Path through the network
- No mix addresses required in messages
- All traffic flows over the same mixes.
- Protection guaranteed as long as one mix withstands attacks

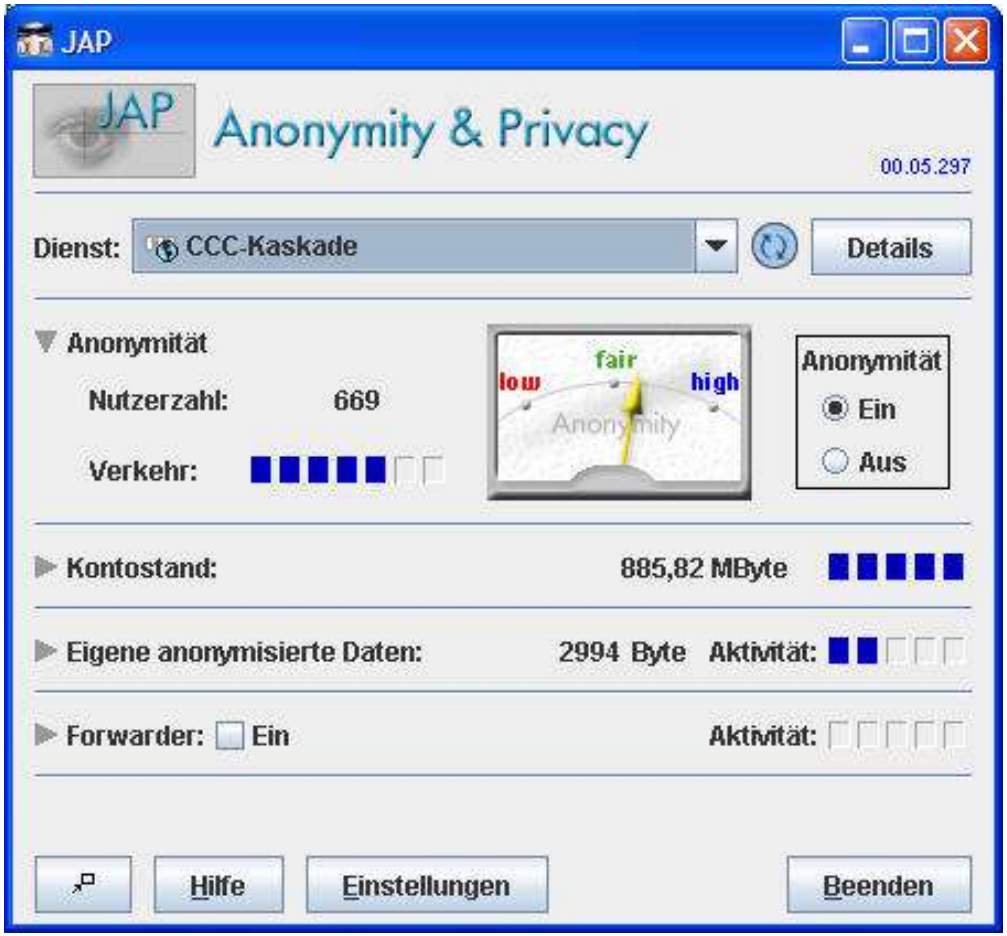
Mixes – Internally



Java Anonymity Proxy (JAP)

- Users can choose between multiple mix-cascades
- Number of active users is a heuristic for level of anonymity achieved
- Current version does not achieve security against a global attacker but can protect against local attackers
  - your boss
  - your provider
  - operator of a mix

http://anon.inf.tu-dresden.de

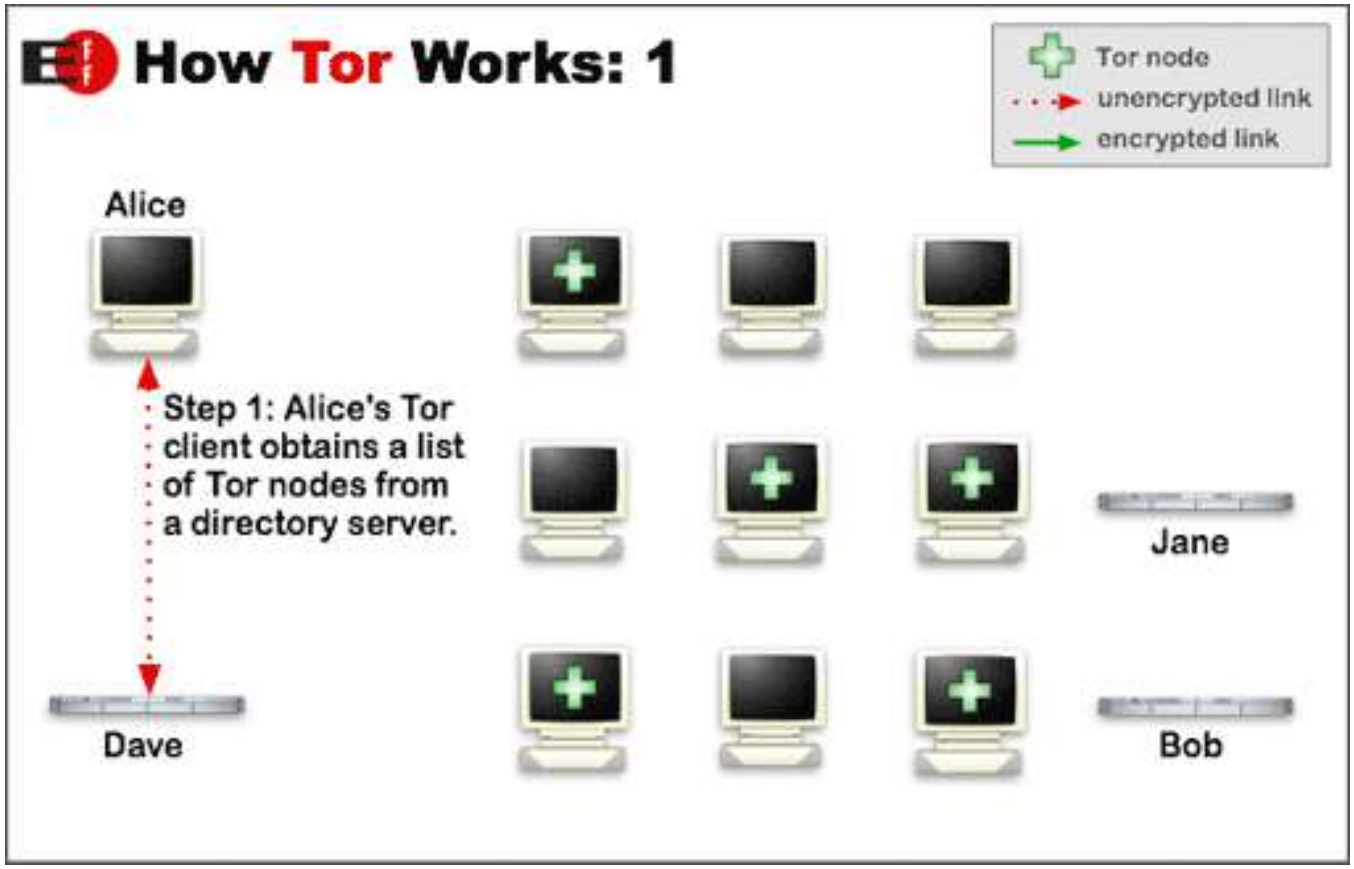


Tor Network

- Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet
- Distributed anonymous network
- Tor allows users to change circuits during sessions
  - Aims to minimize linkability of actions
- May be affected by data retention (as well as JAP)
  - Anonymity and data logs?

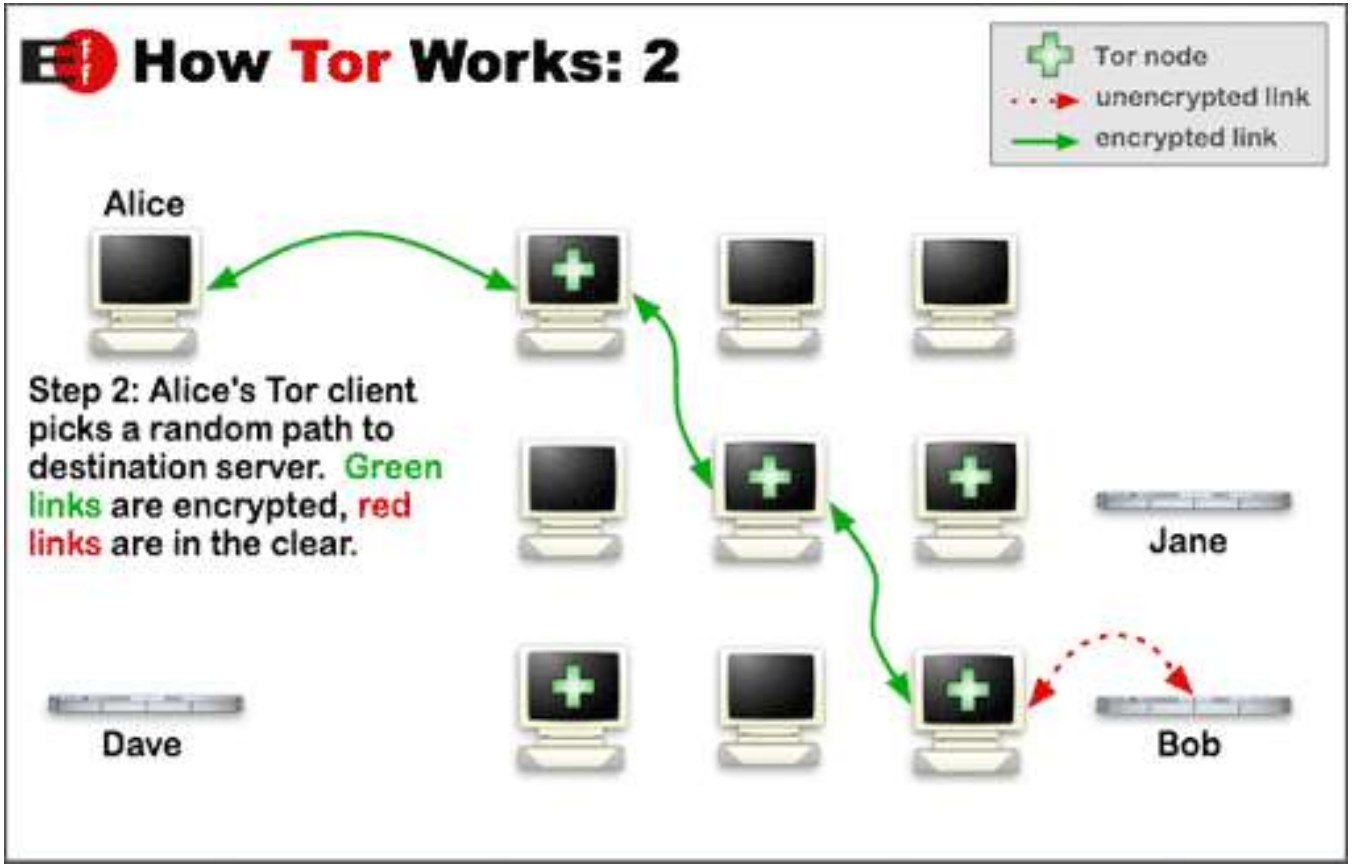
[EU2006]

How Tor Works I



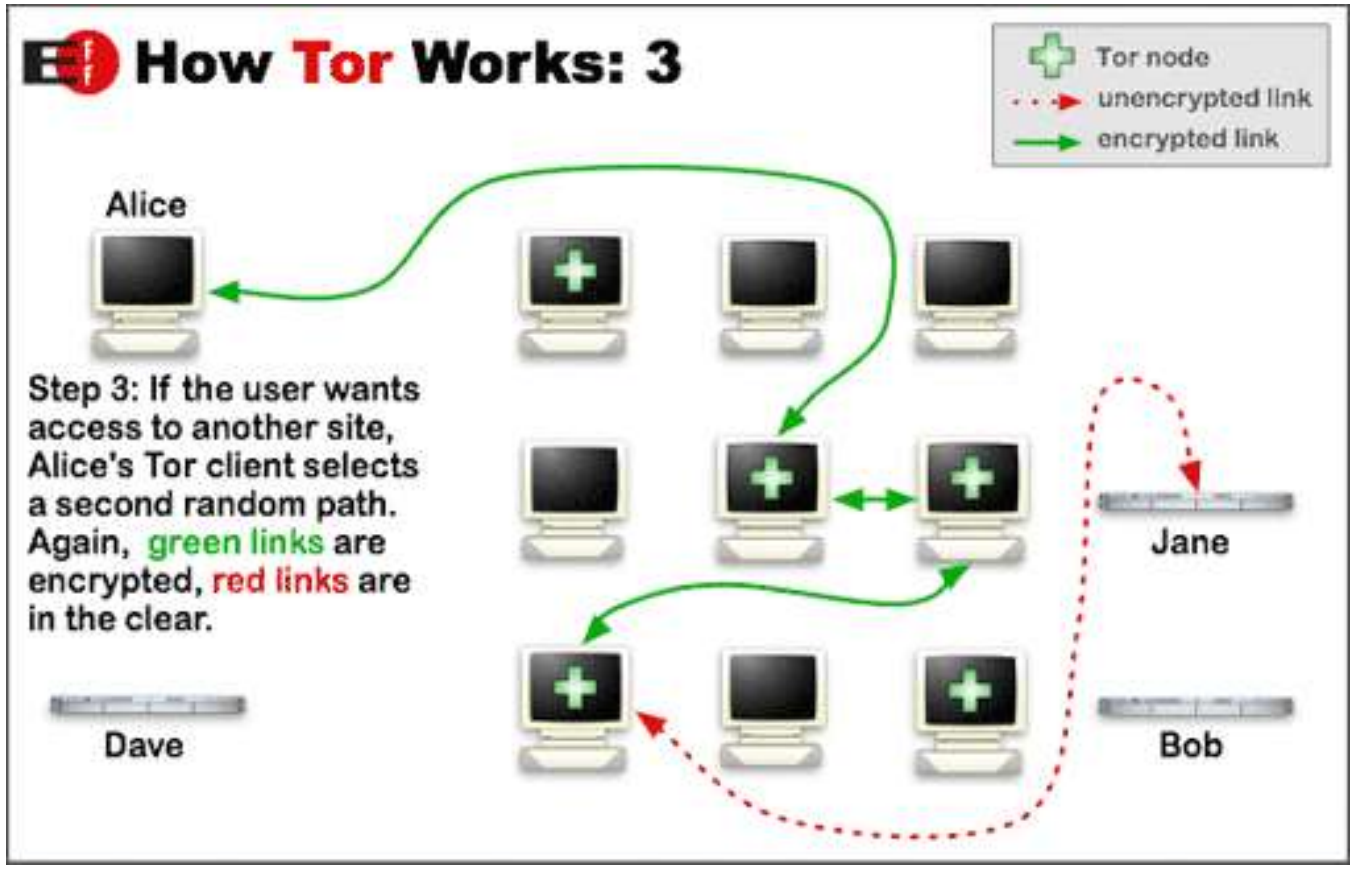
http://tor.eff.org

How Tor Works II



http://tor.eff.org

How Tor Works III



http://tor.eff.org

CookieCooker

- Confuse data collectors
  - Exchange of cookies between users
  - Exchange of identities
  - Use of „faked“ data
- User-defined identity management
  - Assistance for the registration
  - Application of „real“ and „faked“ data
- Spam protection through disposable email addresses
- Ad blocking
- Integrated with JAP Anonymizer

Nowadays only disposable email addresses

Platform for Privacy Preferences (P3P)

- Standard of declaring privacy preferences in a standardized way
  - snapshot of how a web site handles personal information about its users
  - P3P enabled browsers can "read" this snapshot and compare it to the consumer's set of privacy preferences.
- P3P aimed at enhancing user control by
  - putting privacy policies where users can find them,
  - in a form users can understand, and
  - enables users to act on what they see. [W3C P3P]

- Unfortunately this promise has not yet been fulfilled.

References I

[AbLa2007] Timothy G. Abbott, Katherine J. Lai, Michael R. Lieberman, Eric C. Price Browser-Based Attacks on Tor. In 7th International Symposium, PET 2007 Ottawa, Canada, June 20-22, 2007 Revised Selected Papers, pp 184-199.

[Allen2016] Allen & Overy: The EU General Data Protection Regulation is finally agreed, www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

[Bell2001] Tom W. Bell, Internet Privacy and Self-Regulation: Lessons from the Porn Wars, Cato Institute Briefing Papers, No 65., 2001, www.cato.org/pubs/briefs/bp65.pdf

[BlaBorOlk2003] G. W. Blarkom, John J. Borking, and J.G. Olk. Handbook of Privacy and Privacy-Enhancing Technologies - PISA Privacy Incorporating Software Agent. The Hague, 2003.

[BVG83] Bundesverfassungsgericht: Entscheidung BVerfGE 65, 1 – Volkszählung; Urteil des Ersten Senats vom 15.12.1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden, www.datenschutz-berlin.de/gesetze/ sonstige/volksz.htm, accessed 2007-03-02.

[Cavoukian2009] Privacy by Design The 7 Foundational Principles, https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[Chaum1981] David Chaum: *Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms*; Communications of the ACM February 1981 Volume 24 Number 2

References II

[EU2006] European Union: REGULATION (EU) 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC; Official Journal of the European Union L 105/54, 13.04.2006 http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN: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, 04.05.2016 http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[Hoofnagle2005] Chris Jay Hoofnagle, Privacy Self Regulation: A Decade of Disappointment, 2005, www.epic.org/reports/decadedisappoint.html

[ISO/IEC 29100:2011] Information technology – Security techniques – Privacy framework; http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[Rannenberg2000] 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

[Reagle1998] Joseph M. Reagle Jr., Boxed In: Why US Privacy Self Regulation Has Not Worked, Berkman Center for Internet & Society, Harvard Law School, 1998, http://cyber.law.harvard.edu/people/reagle/privacy-selfreg.html

[SelfReg1999] Self-Regulation: Regulatory Fad or Market Forces? Paper prepared for Cato Roundtable „Privacy vs. Innovation“ by Solveig Singleton, May 7, 1999. https://www.cato.org/publications/white-paper/selfregulation-regulatory-fad-or-market-forces

[W3C P3P] Platform for Privacy Preferences (P3P) Project, W3C, www.w3.org/P3P

[WaBr1890] Samuel D. Warren, Louis D. Brandeis: The Right to Privacy, Harvard Law Review; Vol. IV; December 15, 1890, No. 5; http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html