PRIPARE

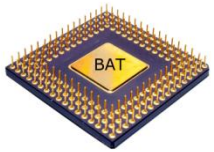
Integrating Privacy Best Practices into a Privacy Engineering Methodology

Jose M. del Alamo (Universidad Politécnica de Madrid)
jm.delalamo@upm.es

Privacy Engineering

An **approach** that takes privacy into account during the whole software and systems engineering process

A set of privacy principles **guiding** the process



Helps to design and choose best available **solutions**

Ensuring that engineered systems are secure and privacy-respectful

Best Practice

"***A best practice is a method or technique that has consistently shown results superior to those achieved with other means***"

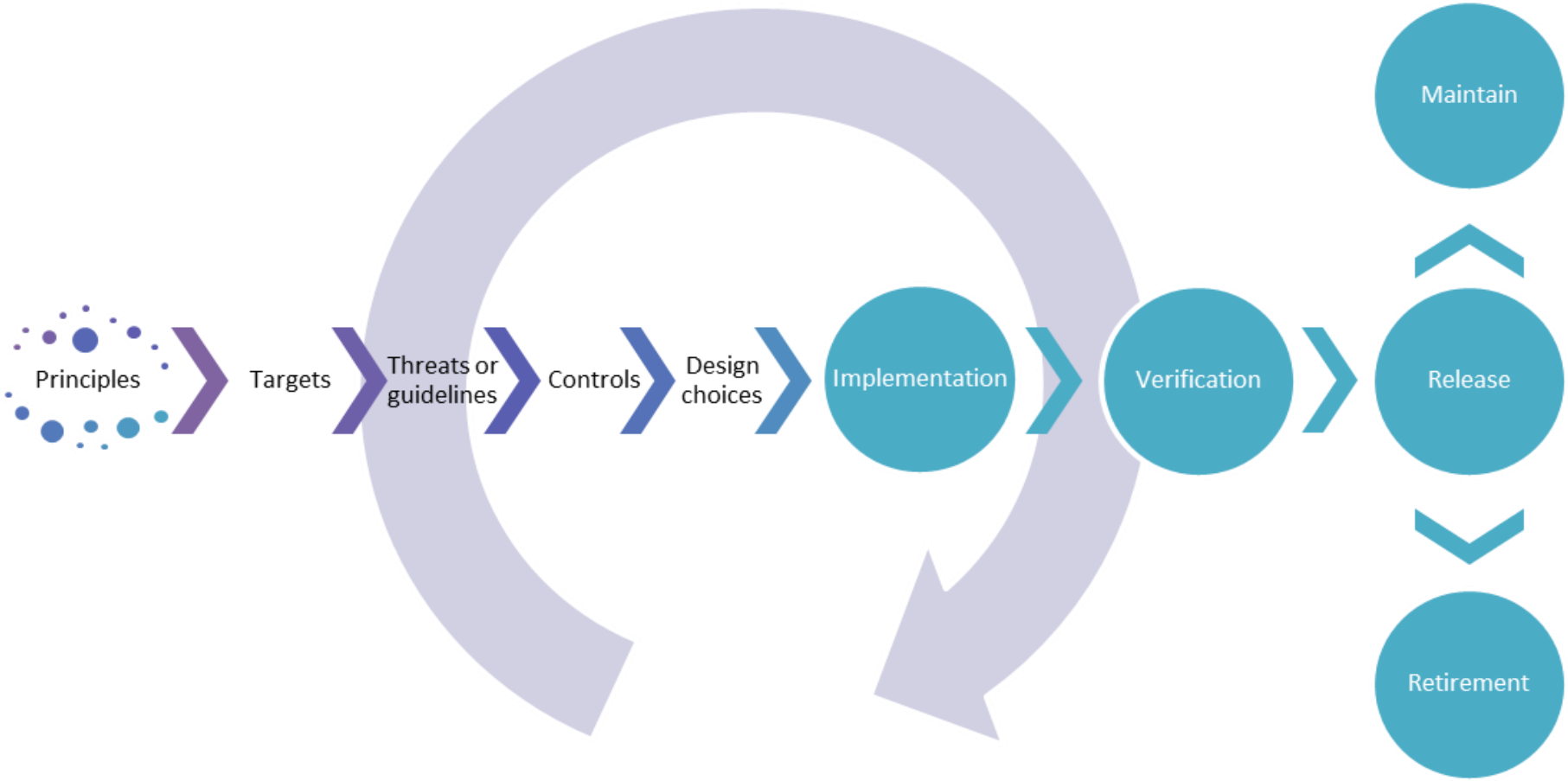
Example of best practices in development processes:

- Iterative, incremental approaches for rapid development
- Risk assessment and management
- Checklists for domains with a matured community of practice

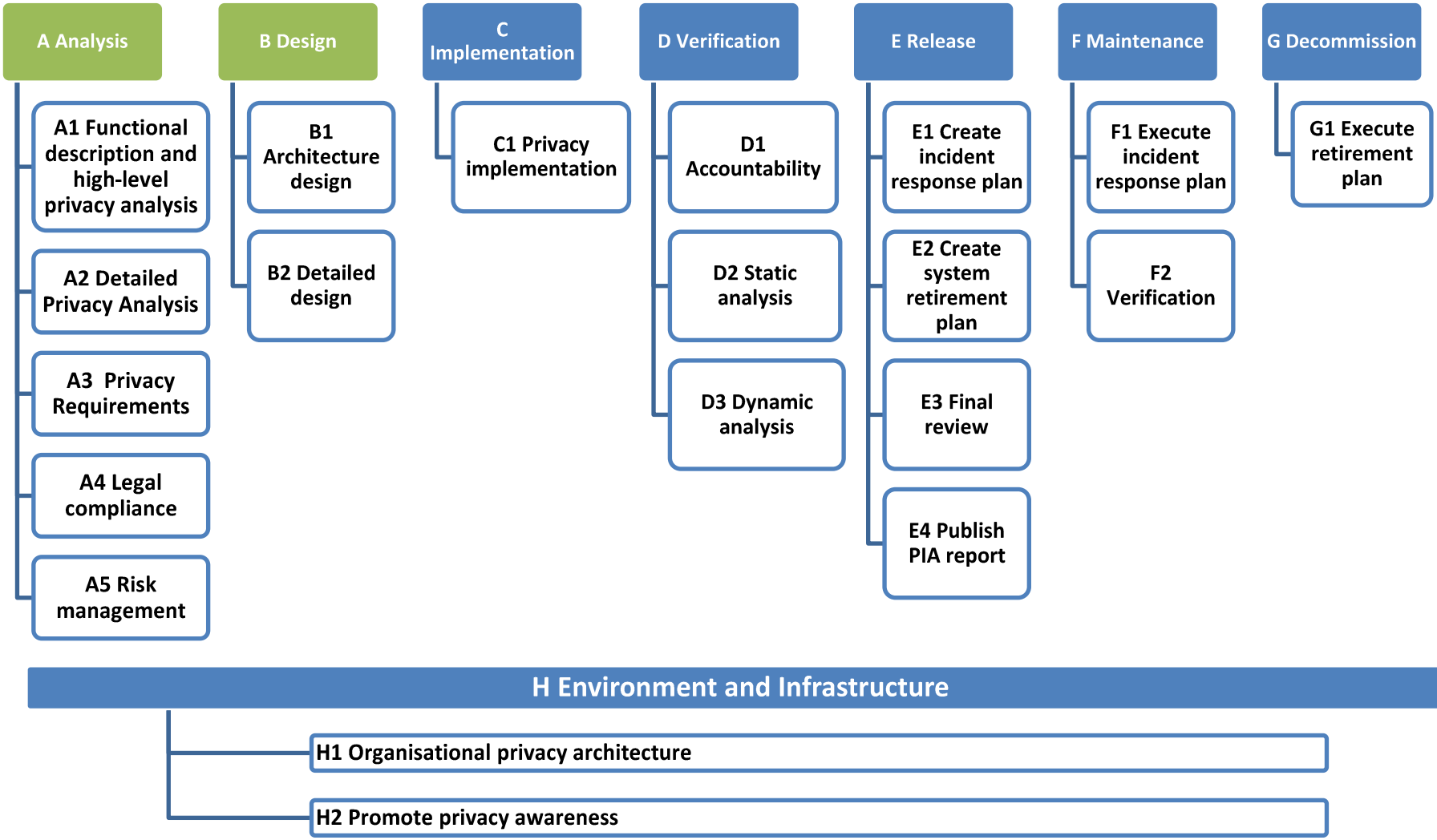
Example of a best practice in software analysis and design:

- Requirements cheat sheets: Common Criteria, WAI…
- Domain-specific heuristics
- Architectural styles: client-server (n-tier), SOA, P2P…
- Design patterns: singleton, façade, observer…

PRIPARE methodology

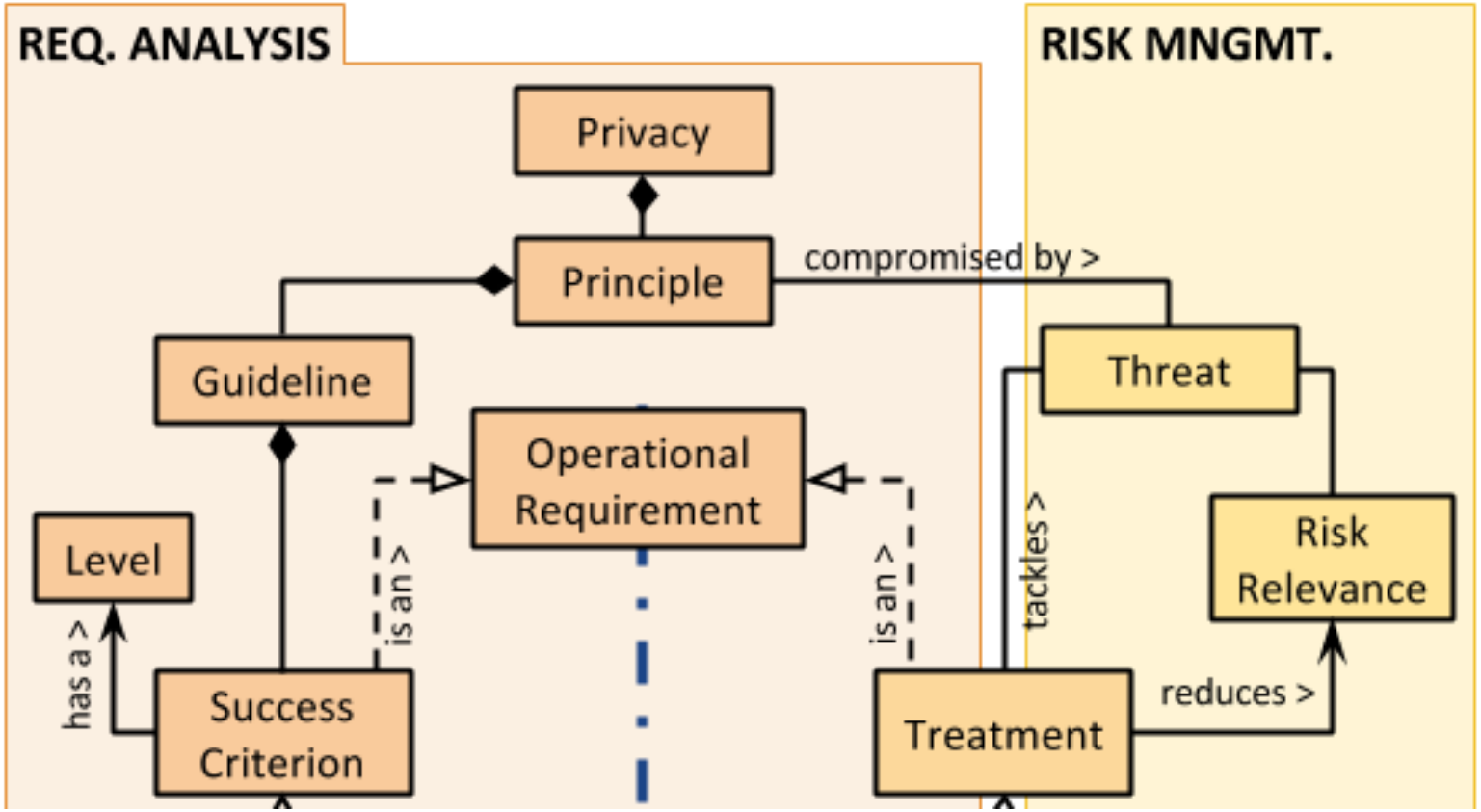


Several Phases (A to H) – Many Processes



A Analysis

Analysis Approaches



B Design

Design

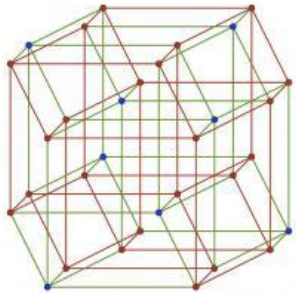
Define the hardware and software architecture, components, modules, interfaces, and data for a system to satisfy specified requirements

- **Architectural design**
  - Iterative approach that identifies an architecture that achieve the requirements
- **Detailed design**
  - Select, from a list of available privacy controls, those that fulfill the privacy requirements while allowing for the business functionality

B1 Architecture Design

Architectural Design

Many factors influence the architectural design:



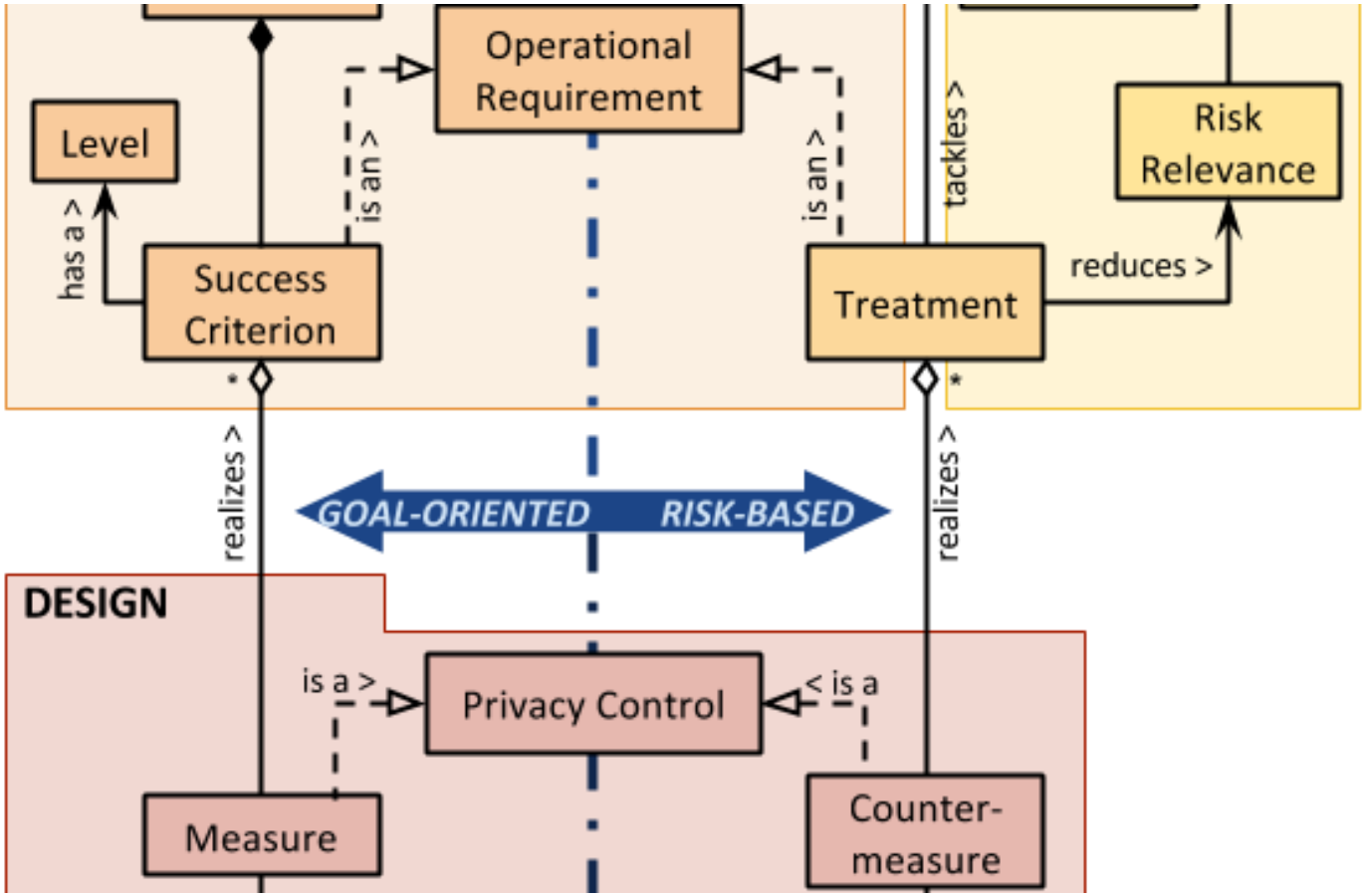
- **Privacy requirements:**
  - Network vs User centricity
  - User identifiability vs anonymity
- **Other requirements:** Performance, maintainability…

The system architect should choose the optimal architecture

- Requires specific expertise and formalization languages
- Complex task, supported by specialized CASE tools
- 3 different approaches explored

B Detailed Design

Detailed Design

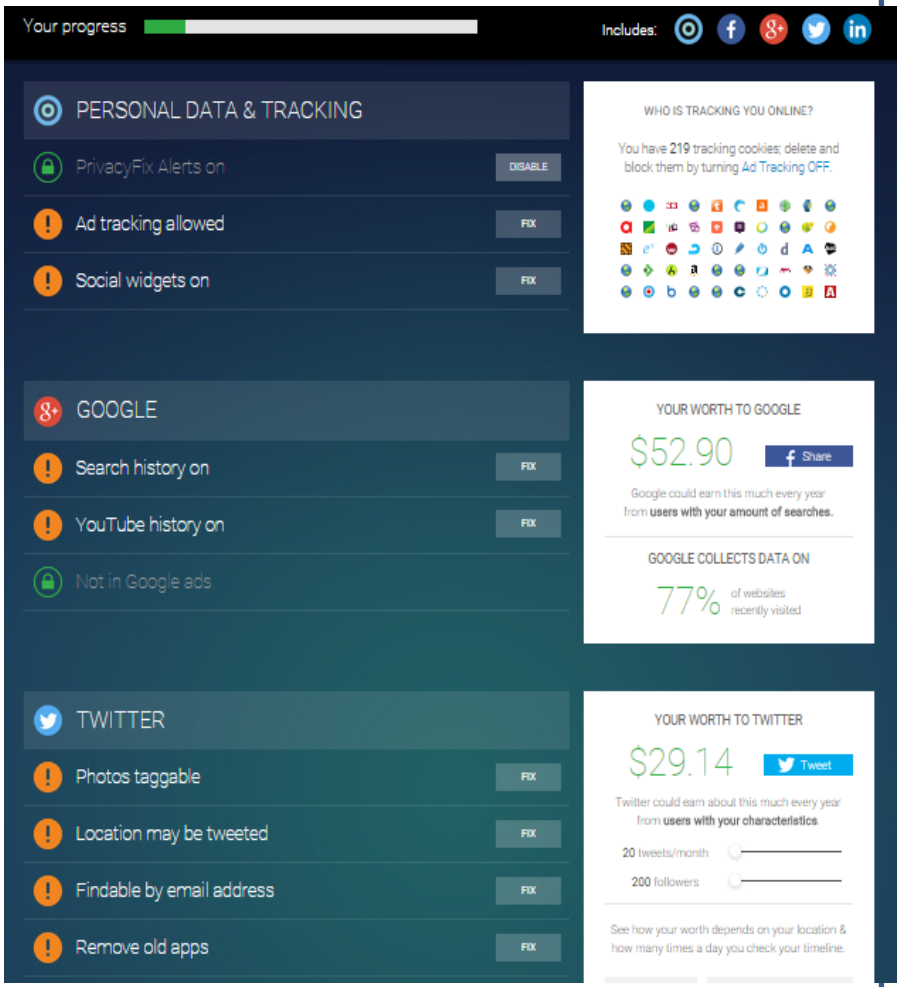


B Detailed Design

Privacy Dashboard

Requirement: Users should be aware of all the data being collected, created, maintained, processed and shared by the service provider or third parties

Control: A privacy dashboard provides a summary of the different types of personal data held by the service provider, together with user controls to restrict purposes or sharing, when applicable.

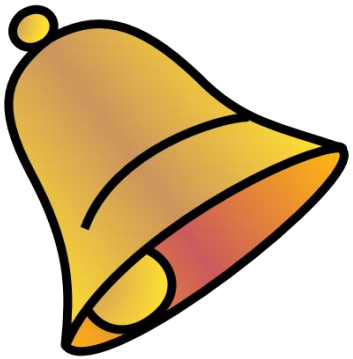


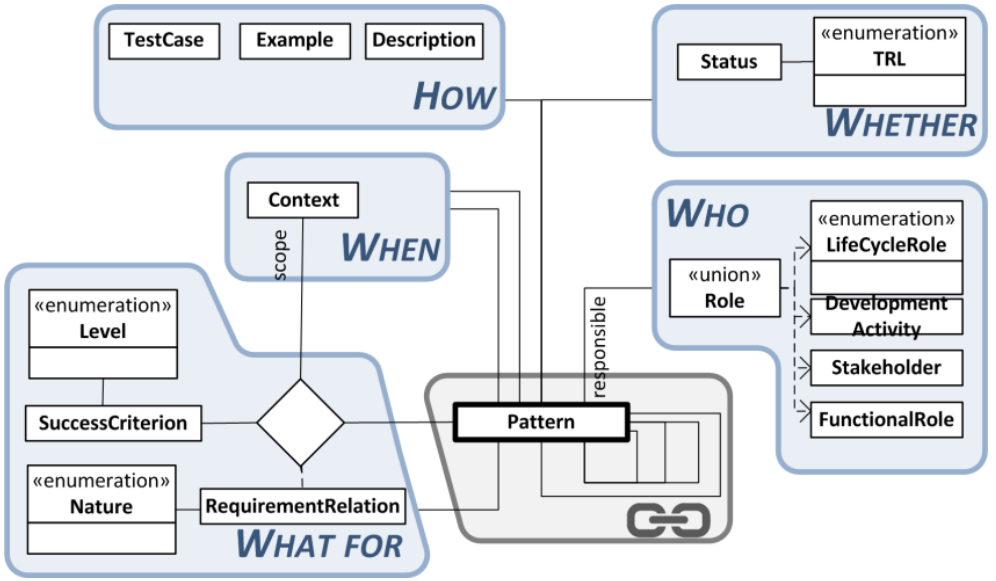
B Detailed Design

Privacy Control Catalogue

A privacy control is a reliable, implementable way to meet privacy requirements

They have heuristically shown to be good solutions to recurring problems



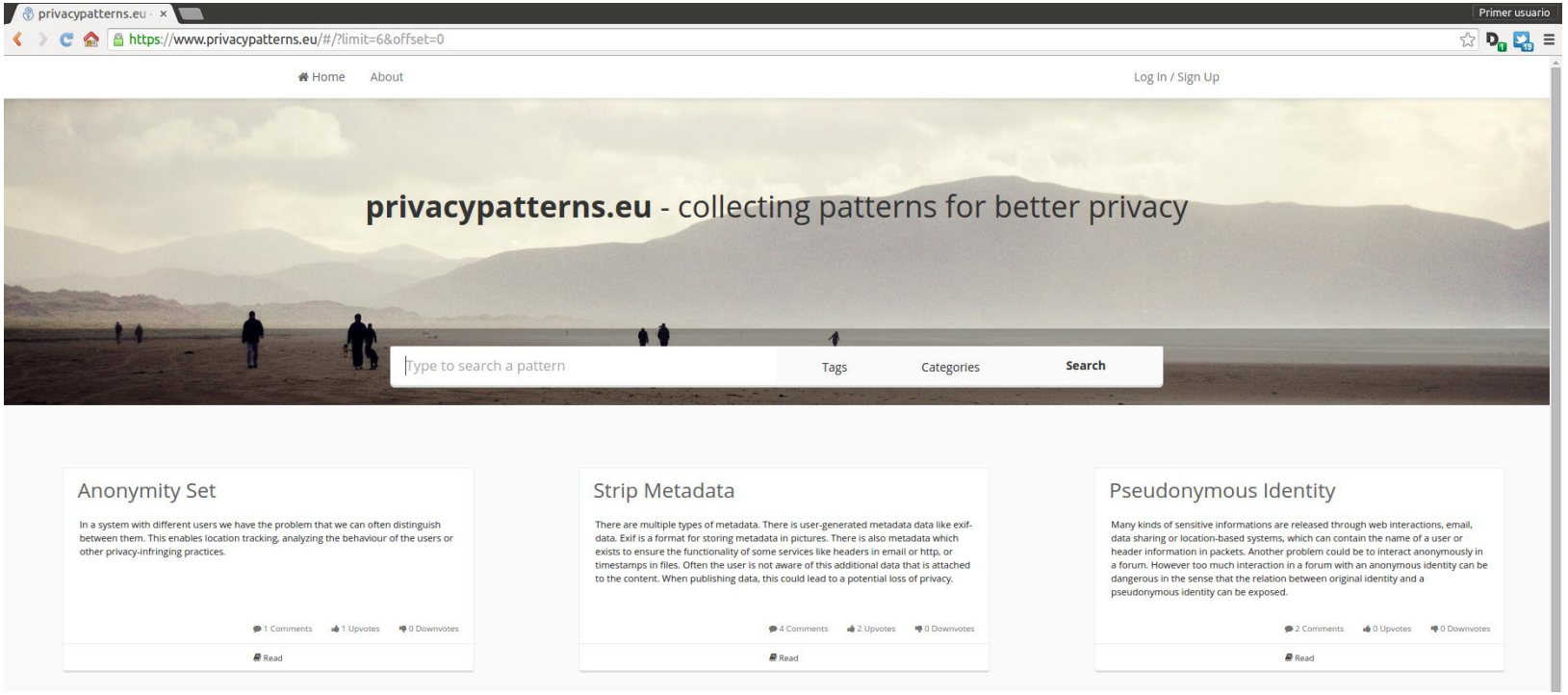


B Detailed Design

Privacy Patterns Catalogue

www.privacypatterns.eu

Website to collect and discuss about privacy patterns



PRIPARE Results Impact

Conclusions

- **Privacy engineering methodology integrating best practices**
  - Moving towards systematic engineering approaches
- **Issues detected**
  - Missalignment of technical and legal backgrounds
  - Rough transition between phases
  - Lack of standardization and education initiatives
    - Specially for catalogues and cheat sheets

PRIPARE

Integrating Privacy Best Practices into a Privacy Engineering Methodology

N. Notario, A. Crespo, Y.S. Martín, **J.M. del Álamo**,

D. Le Metayer, T. Antignac, A. Kung, I. Kroener, D. Wright