TRUESSEC.EU
Towards the creation of a "European Trust Enhancing Label"

Internet Privacy Engineering Network 2017
Viena(Austria), June 9, 2017

José M. del Álamo, Yod-Samuel Martín
Departamento de Ingeniería de Sistemas Telemáticos
Universidad Politécnica de Madrid

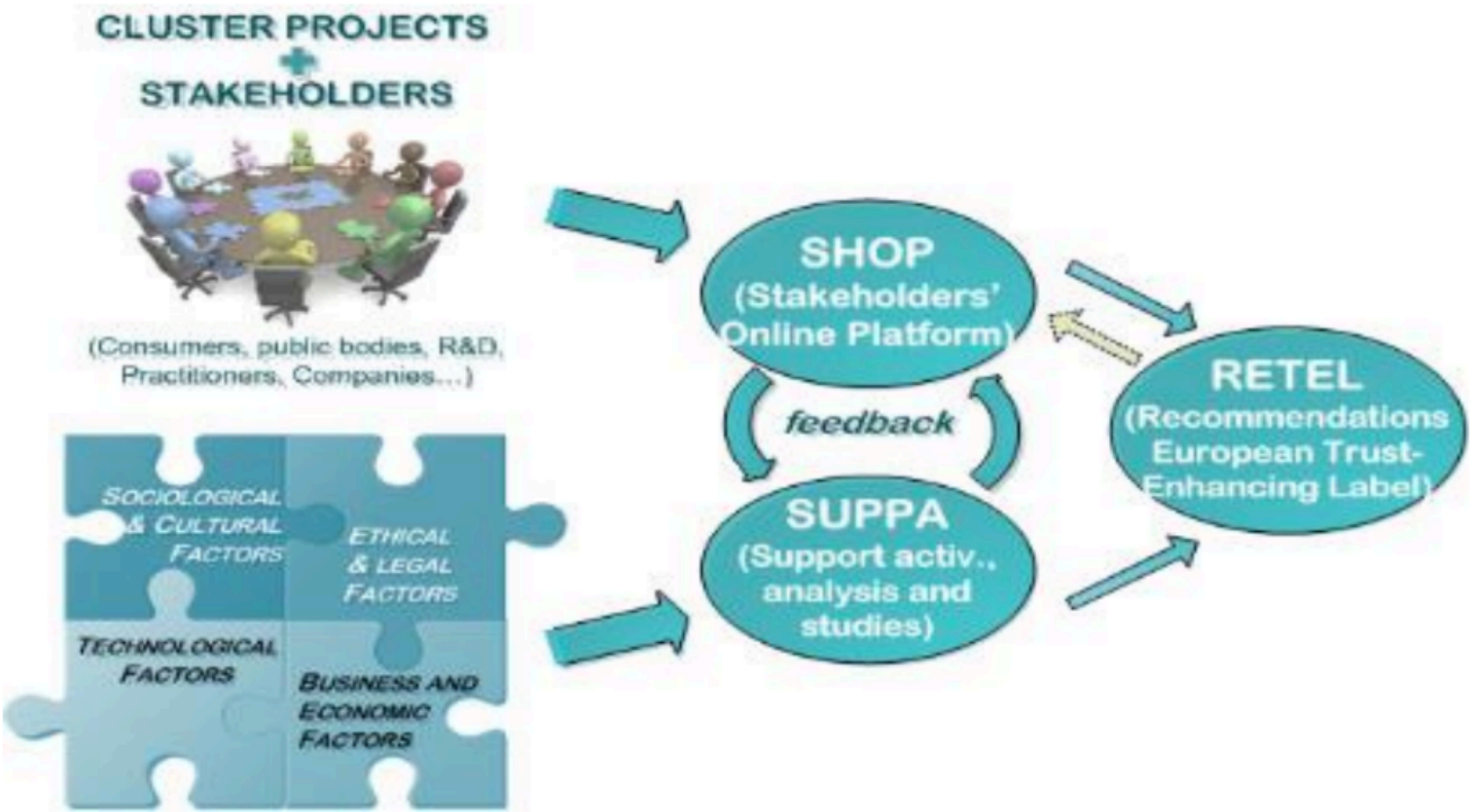
Certification

"A structured system by which an independent and impartial third party (*certification authority*), after performing an assessment of the system of interest at a point in time, issues the results in the form of a certificate, asserting that the system complies with public and standard criteria under specific conditions"

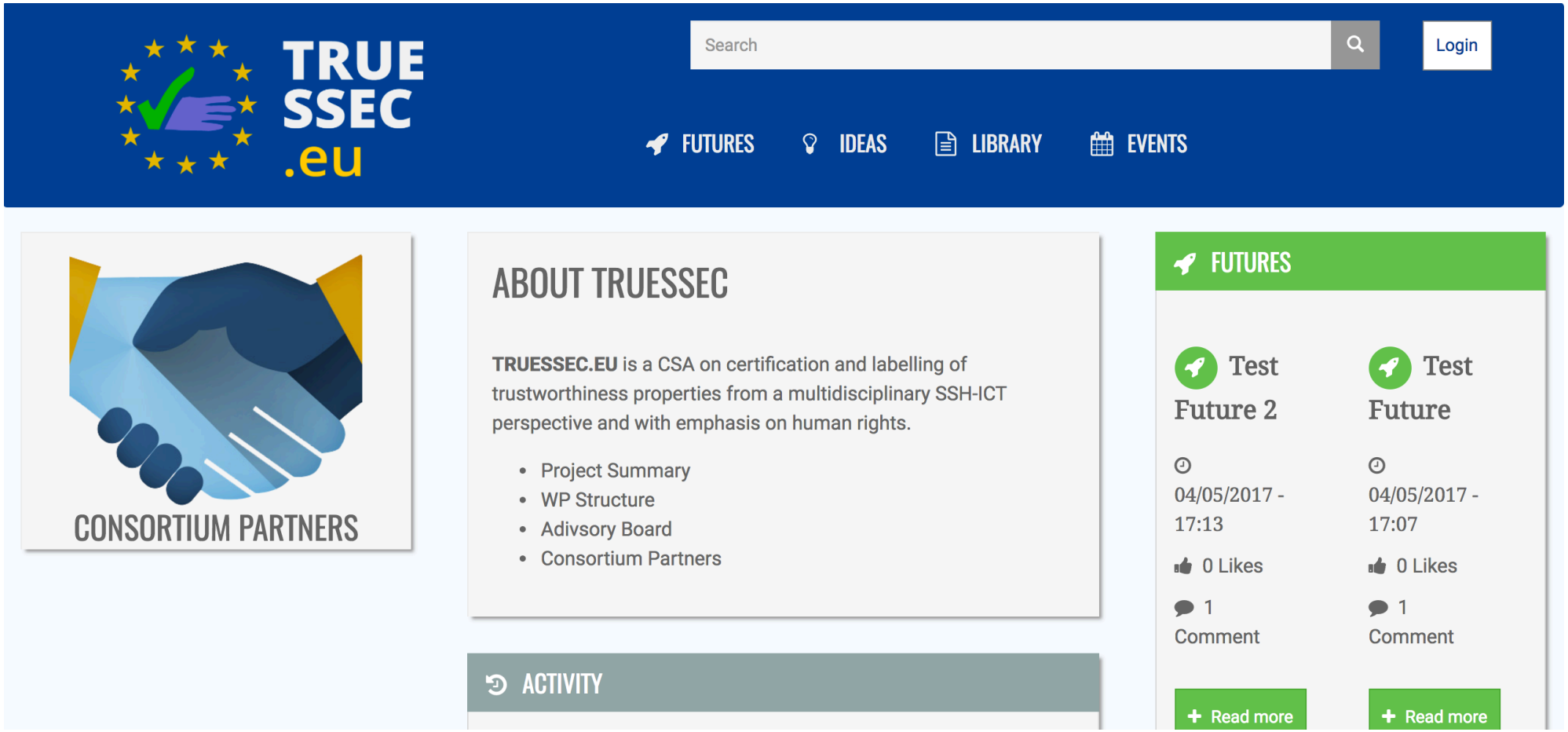
Challenges

- **Flexibility**
  - Domain
  - Organization
  - Product/Process/People
- **Scalability**
  - From self-assessment to 3rd party certification
- **Requirements**
  - Depend on domain/product
  - Might depend on stakeholder

TRUESSEC.eu

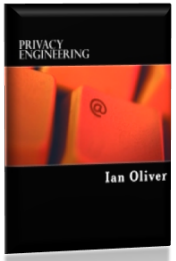

CLUSTER PROJECTS
+
STAKEHOLDERS
(Consumers, public bodies, R&D, Practitioners, Companies...)
SOCIOLOGICAL & CULTURAL FACTORS
ETHICAL & LEGAL FACTORS
TECHNOLOGICAL FACTORS
BUSINESS AND ECONOMIC FACTORS
SHOP
(Stakeholders' Online Platform)
feedback
SUPPA
(Support activ., analysis and studies)
RETEL
(Recommendations European Trust-Enhancing Label)

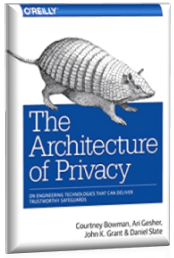
Stakeholders Online Platform



"Privacy Engineering"

- Books:





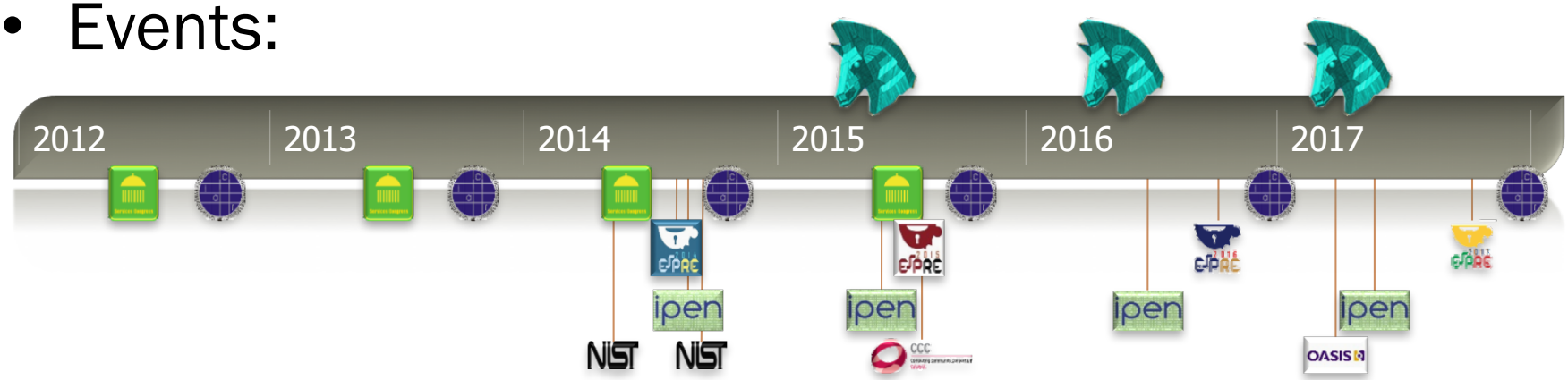
- Courses and training programs:

JOHNS HOPKINS WHITING SCHOOL of ENGINEERING

ulm university universität uulm

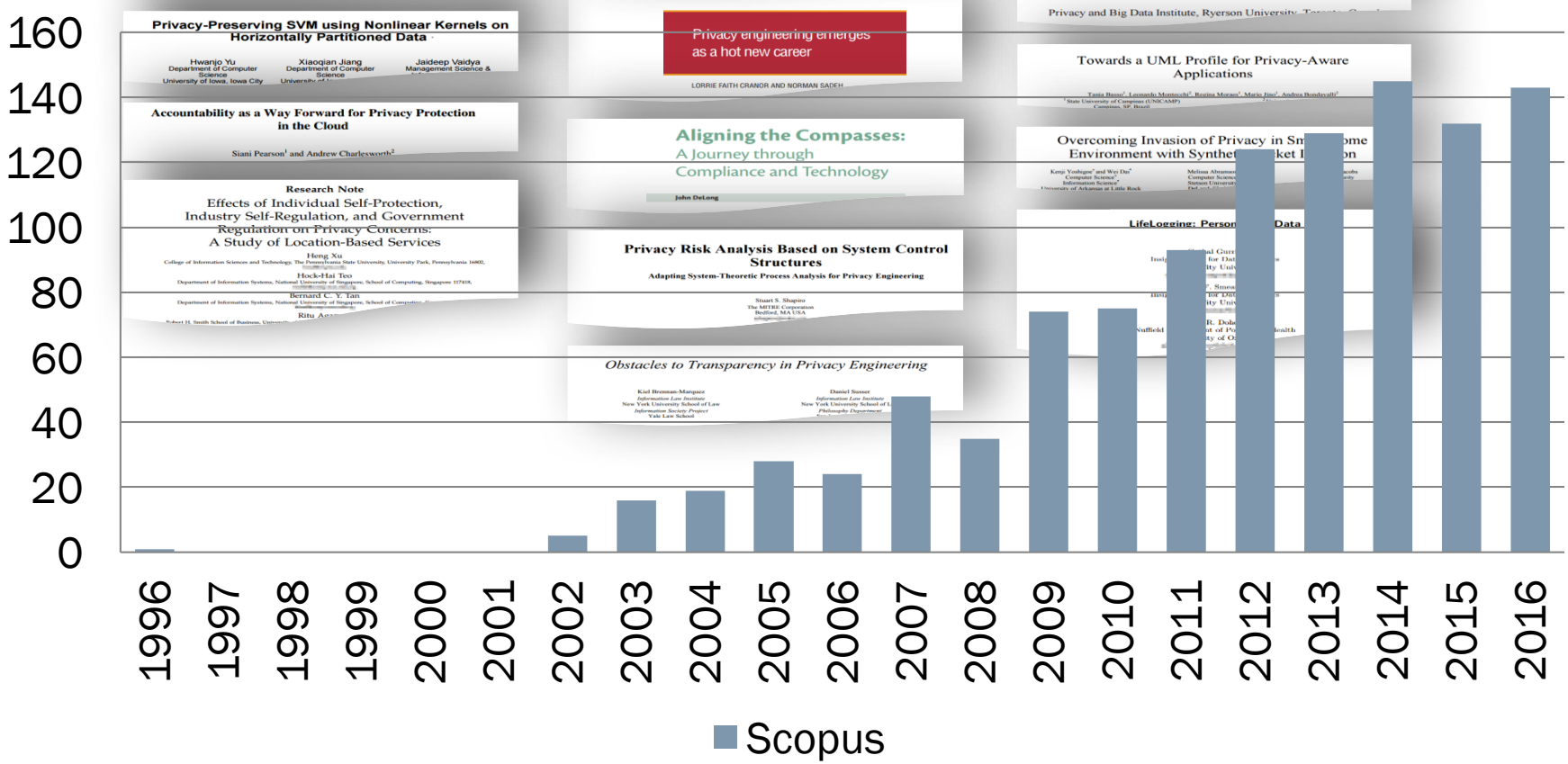
Carnegie Mellon University
Master of Science in Information Technology
privacy ENGINEERING

- Events:



"Privacy Engineering"

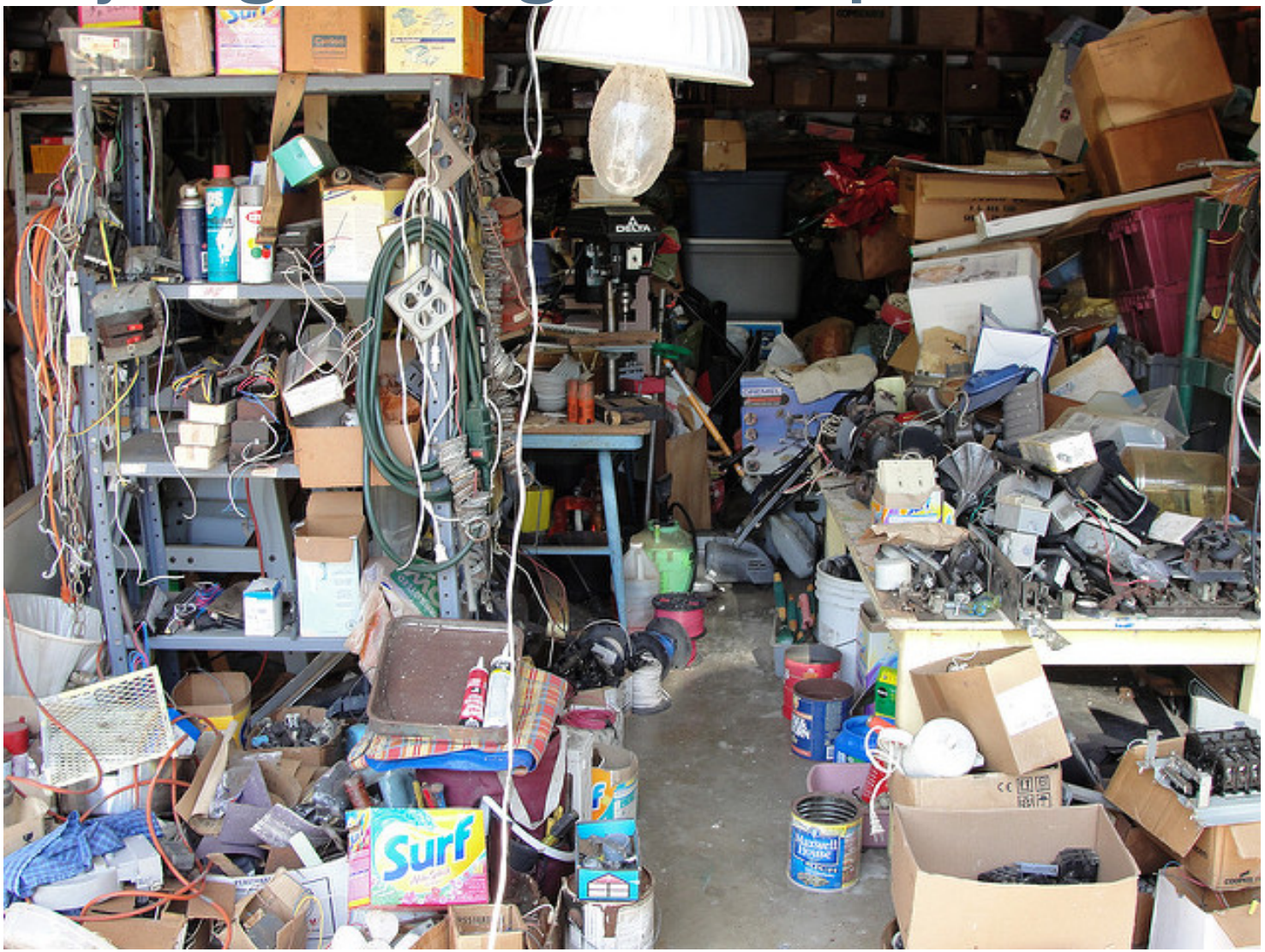
Research publications (Scopus)



"Privacy Engineering"

access accuracy address agents aggregation algorithm analysis analyze anonymization applications applied approach architecture assessment association attacks attributes authentication authors available business case challenges classification cloud clustering collaborative collected combined communication compared complexity computing concerns confidentiality content context control cost cryptography customers data database datasets decision demonstrate describe design detection development devices digital directions disclosure distributed drm effective efficient eid electronic enables encryption engineering enhancing environment evaluation experimental experiments extract features framework frequent function fuzzy general health hiding https identify identity image impact implementation individual information integrity intelligence interaction international internet introduce inward issues item itemsets key knowledge learning legal level limited location machine management measures mechanisms medical method mining mobile model multi-party multiple needs network novel number objects online operations optimization order organizations original outsourced participants parties partitioned patterns performance personal perturbation policy potential power practical prediction present preserving principles privacy private problem process product properties proposed protection protocol provide public publishing purpose quality query random real recent recommender record regulation related release requirements research reserved resources results rights risk rules scenario scheme science security selection sensitive sensor server services sets several sharing sites smart social software solutions source specific statistical storage structure study support survey systems task technical techniques technology terms test theory threats tools transaction tree trust types used users utility values various webwork

Privacy Engineering landscape?



Christian Lopez (the garage) https://www.flickr.com/photos/andidigress/4471100232

A Privacy Engineering Methodology Metamodel

Justin de la Ornellas (avex2) https://www.flickr.com/photos/ornellas/2835160463/

Privacy Engineering

Privacy Engineering

"Privacy engineering is an emerging research framework that focuses on designing, implementing, adapting, and evaluating ***theories, methods, techniques****, and* ***tools*** *to systematically capture and address privacy issues in the development of sociotechnical systems."*
(Gürses & Del Álamo, 2016)

Privacy Engineering revisited

Privacy Engineering contributions
define **Method(ologie)s** or Methodological elements **(Fragments)**
to systematically capture and address privacy issues
in the development of information systems
made of:

Producers (role, tool or team)
who perform some **Work Units** (process [goal], task [what], technique [how])
which **act upon** (reads, creates, modifies, deletes)
some **Work Products** (documents, models*, software items)
while at a **Stage** (at a milestone, or during a phase, build, or time cycle)
and using some ***given* Resources**
(languages, notations, guidelines and constraints).

*Models
are composed of Model Units,
conform to a Language,
and are expressed in a Notation

Conclusions

- Certification challenges
  - Diversity of approaches but lack of guidance and requirements
- Privacy engineering can deliver
  - A common conceptual framework
  - Methodologies defined in compatible terms
  - A reusable knowledge base
- TRUESSEC.eu is addressing these challenges
  - Organizing debates on different topics

Join and participate!!!

Thank you

jmdela@dit.upm.es