Transparency Enhancing Technologies

Hans Hedbom

Karlstad University

Transparency tools

- A transparency tool for privacy purposes is a technological tool that that provides the data subject with one or more of the following :
  - information on intended collection, storage and/or data processing to the end user.
  - information on personal data released and negotiated policies.
  - access to stored data and/or to logic of data processing in order to enhance the end users privacy;.
  - access to profiles and/or makes it possible to control the results of profiles that may affect the risks and opportunities of the data subject.

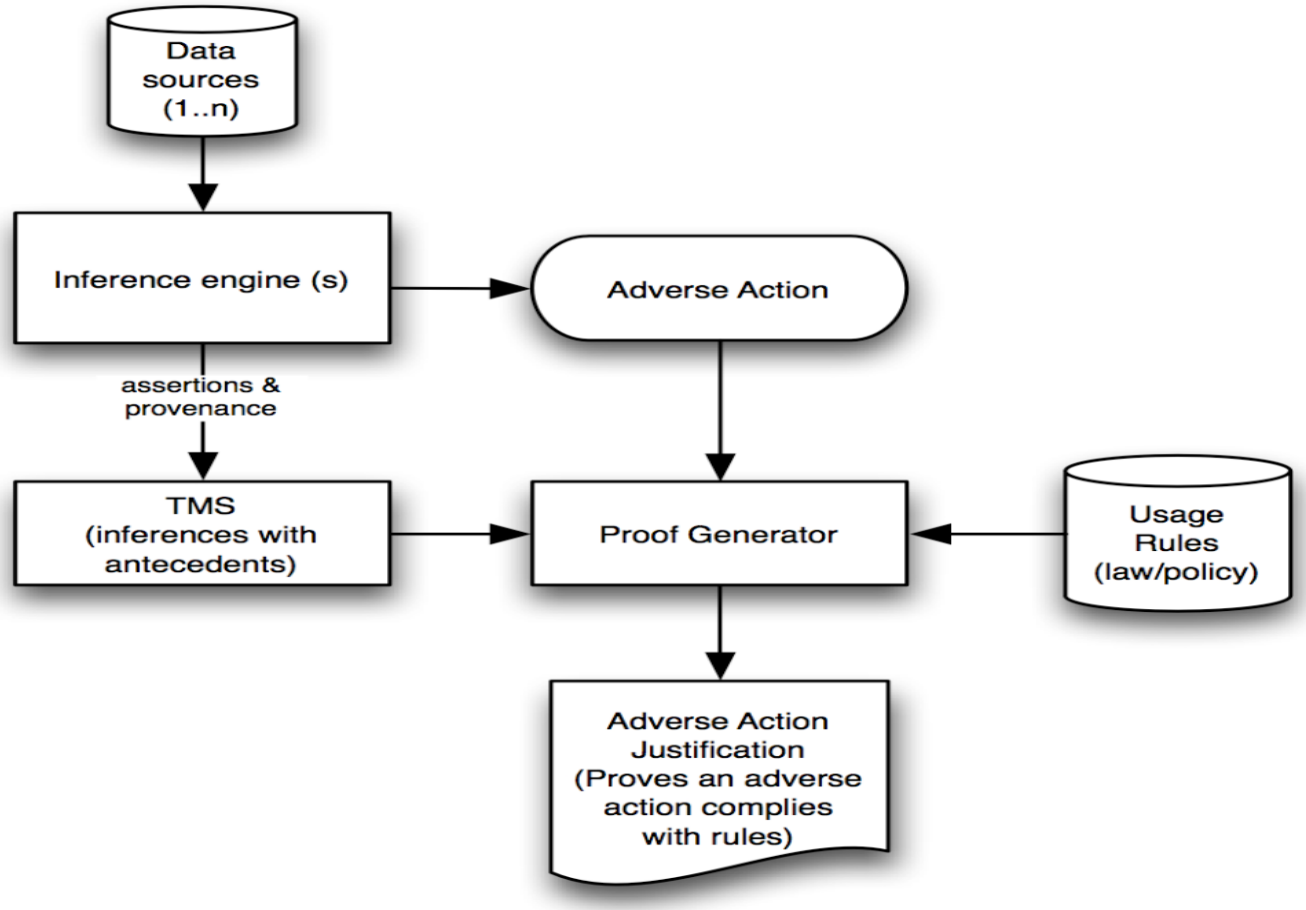
Why Transparency tools?

- New technologies makes it hard to controll access and the existence of data
  - AmI, Data Mining, Web 2.0, Online Comunities
  - Control use as a complement to Consealment?
- European Law requires transparency
  - Not online requirement, but online tools will probably make things more costeffective.

Risks

- Gives a lot of information and thus requires strong authentication not to be a privacy risk.
- Requires extensive logging on server side which could be a problem if not handle correctly.

Interesting approaches: TAMI



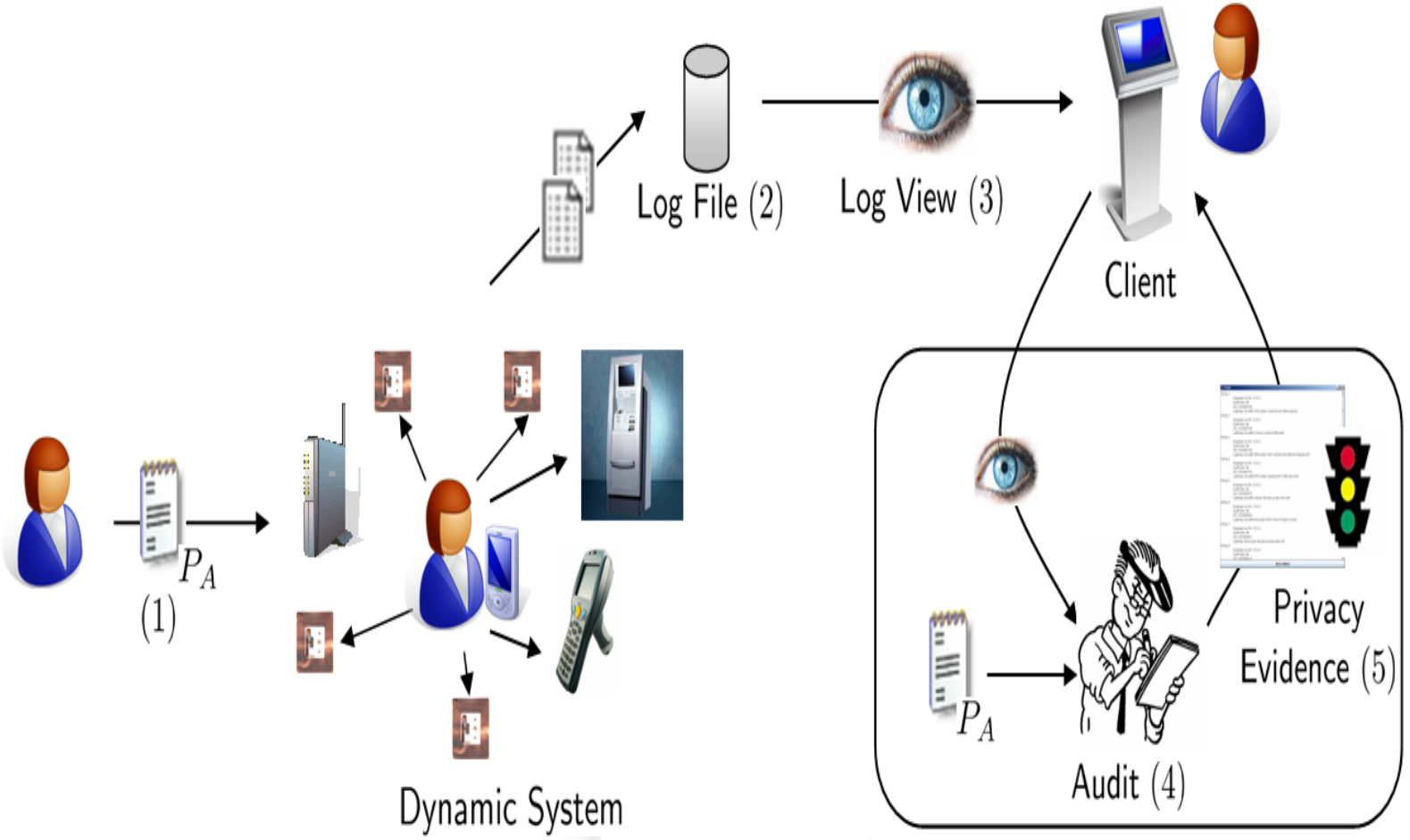
Pictures from: J. Weitzner, H. Abelson, T. Berners-Lee, C. Hanson, J. Hendler, L. Kagal, D. L. McGuiness, G. J. Sussman, and K. Waterman. Transparent acountable data mining: New strategies for privacy protection. Computer Science and Artificial Intelligence Laboratory Technical Report MIT-CSAIL-TR-2006-007, Massachusetts Institute of Technology, Cambridge, Ma, USA, 2006.

Interesting approaches: TAMI

- Relies on WEB technology e.g
  - N3 RDF
    - :pnr-1 a :PassengerNameRecord;
      :source :AA-PNR;
      :date 2004-06-14;
      :passenger
      [:name
      [:personGivenName "John",
      :personMiddleName "Henry",
      :personSurName "Doe"];
      :birthDate 1975-08-24];
  - N3 Logic
  - { ?X a Person.
    ?X outstandingObligation ?ChildSupport.
    ?ChildSupport a ChildSupportOutstandingObligation.
    ?ChildSupport value ?Amt.
    ?Amt math:greaterThan 1000.
    ?ChildSupport obligee ?Y.
    ?Y a Child.
    ?X residence [geo:inRegion [usps:stateAbbr ?XState]].
    ?Y residence [geo:inRegion [usps:stateAbbr ?YState]].
    ?XState string:notEqualIgnoringCase ?YState. }
    => { ?X a :DeadbeatDad }.

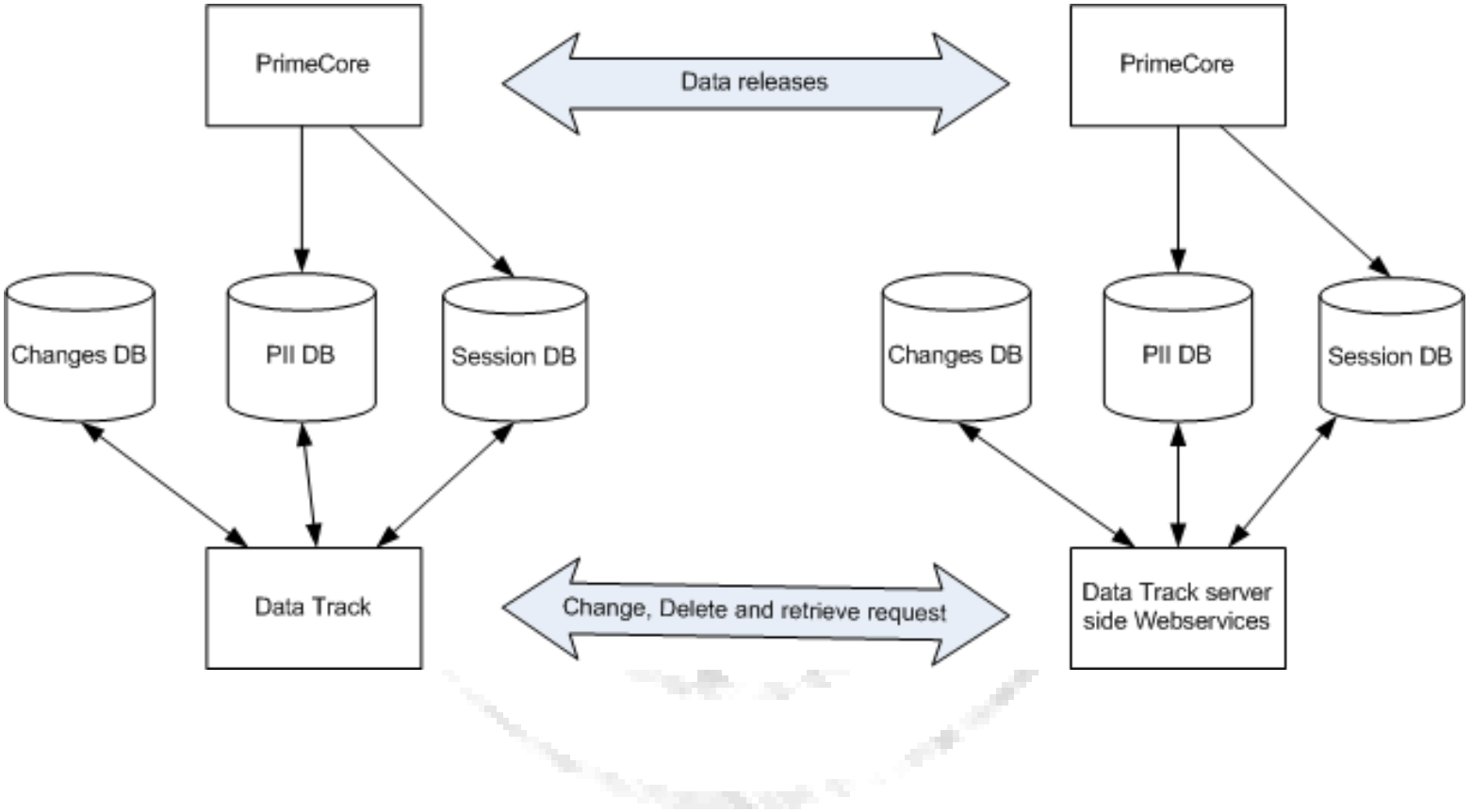
Pictures from: J. Weitzner, H. Abelson, T. Berners-Lee, C. Hanson, J. Hendler, L. Kagal, D. L. McGuiness, G. J. Sussman, and K. Waterman. Transparent acountable data mining: New strategies for privacy protection. Computer Science and Artificial Intelligence Laboratory Technical Report MIT-CSAIL-TR-2006-007, Massachusetts Institute of Technology, Cambridge, Ma, USA, 2006.

Interesting approaches: Privacy Evidence

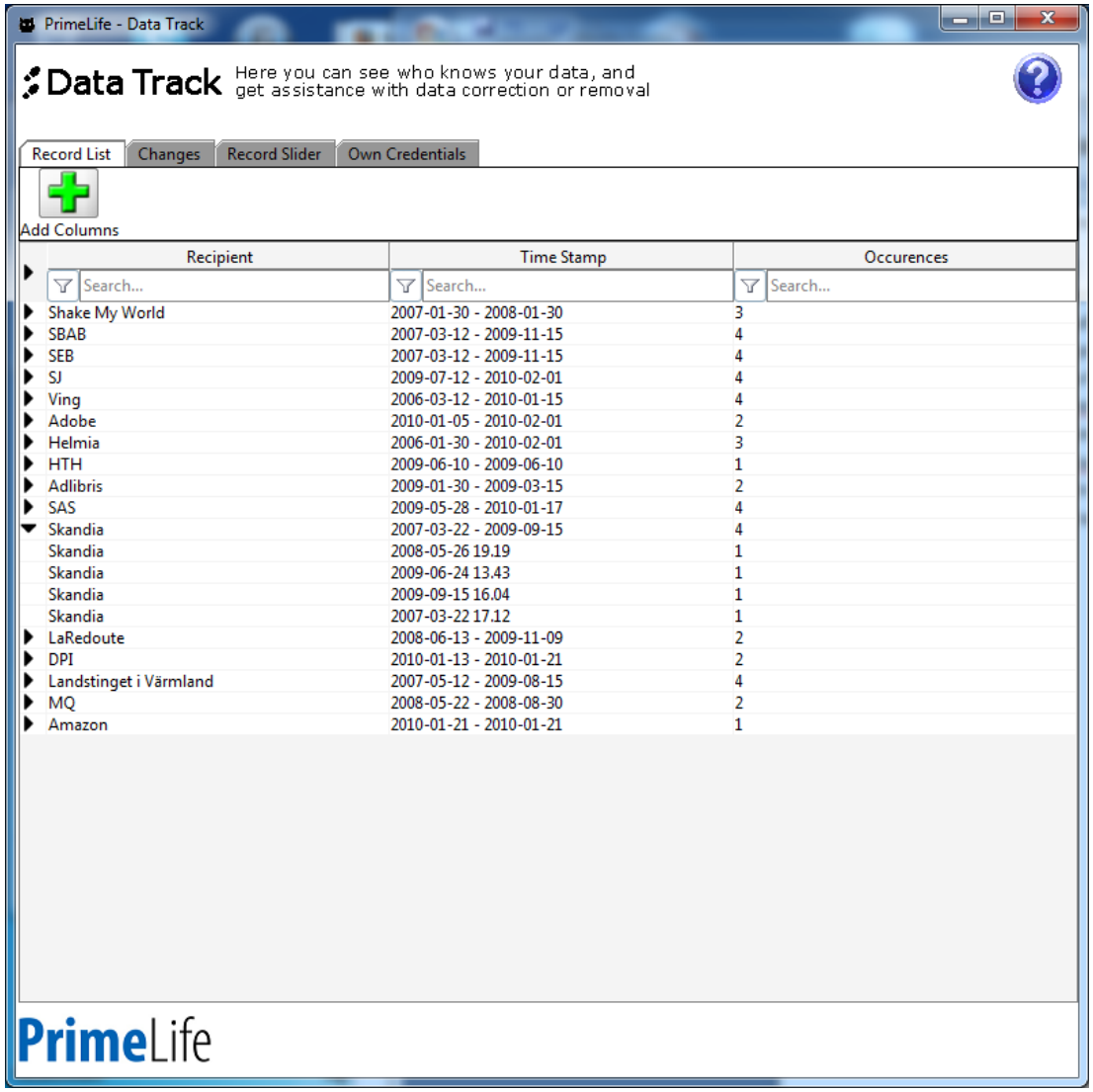


Picuters from : S. Sackmann, J. Strüker, and R. Accorsi. Personalization in privacy-aware highly dynamic systems. COMMUNICATIONS OF THE ACM, 49(9), September 2006.

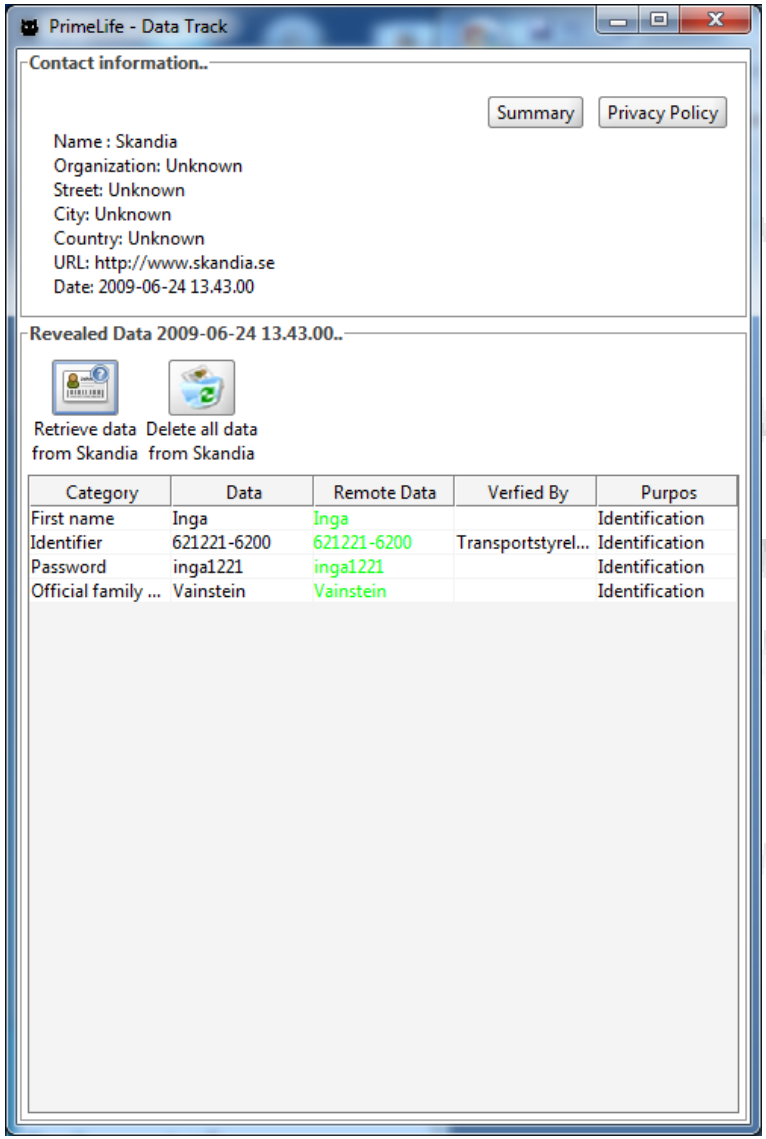
PRIME/PrimeLife Data Track



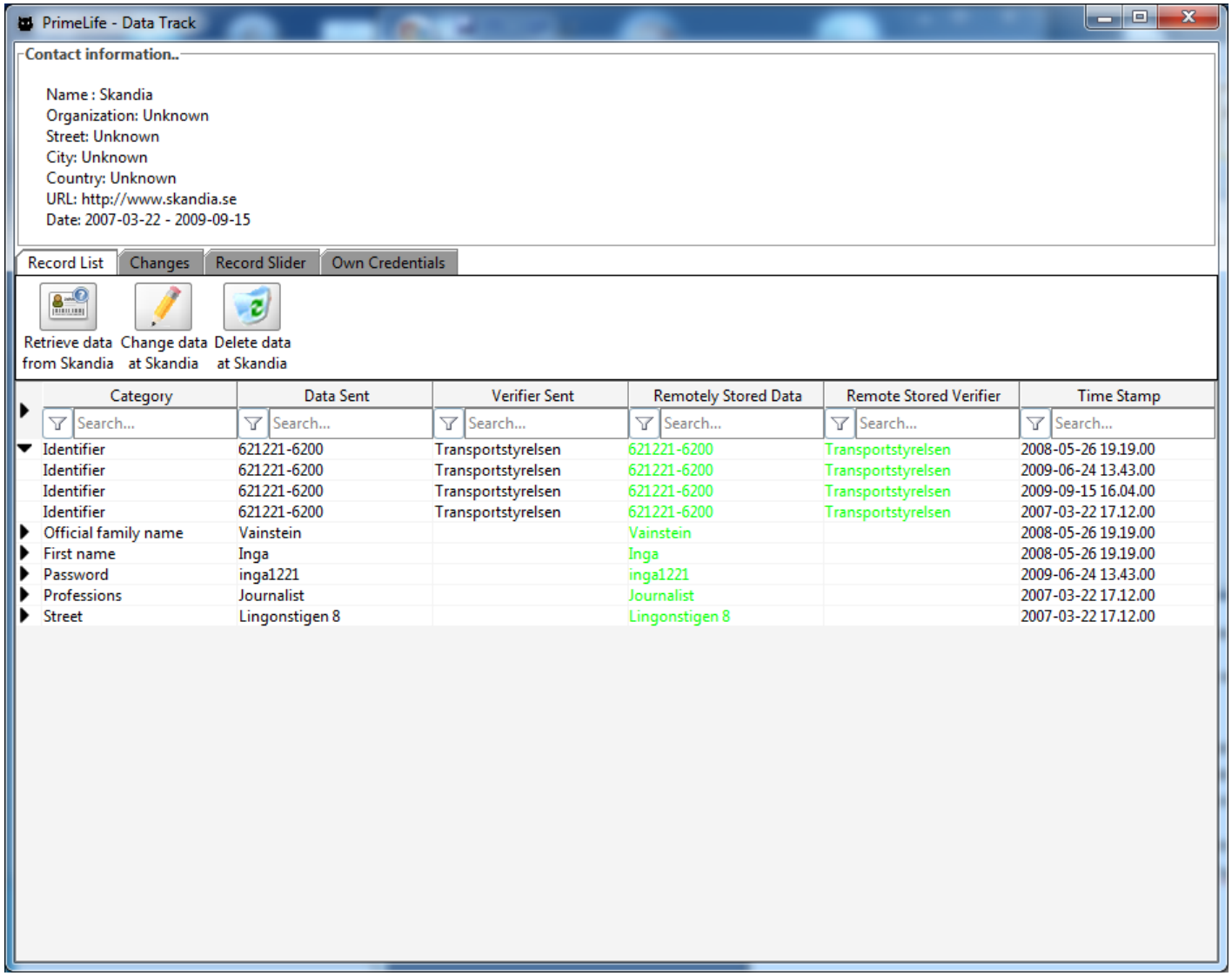
PRIME/PrimeLife Data Track



PRIME/PrimeLife Data Track



PRIME/PrimeLife Data Track



Why privacy preserving secure logs?

- A need to know how data been handled.
- Realtime access for data subjects to processing and access history.
- Detection of policy violations.
- Should not reveal new personal information to others.

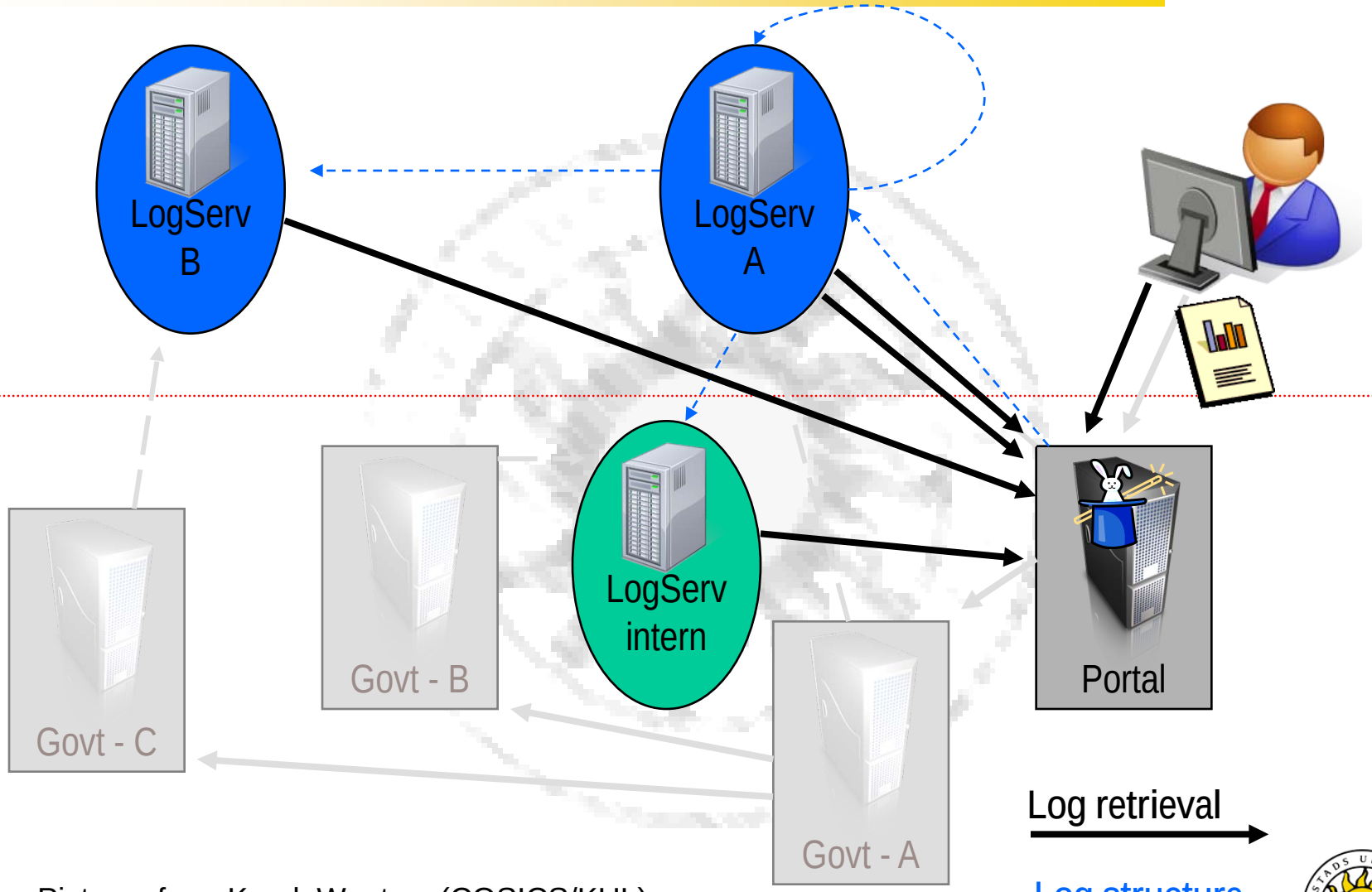
Privacy Preserving Secure Logging

- A log:
  - A record of sequential data
    - In this case, each entry concerns exactly one data subject
- A Secure Log:
  - Protects the confidentiality and integrity of entries
    - Confidentiality provided by encrypting the data in the entries
    - Integrity provided by using hashes and MACs
  - *Prior to* an attacker compromises the logging system
    - Forward secrecy
    - Forward integrity

Privacy Preserving Secure Logging

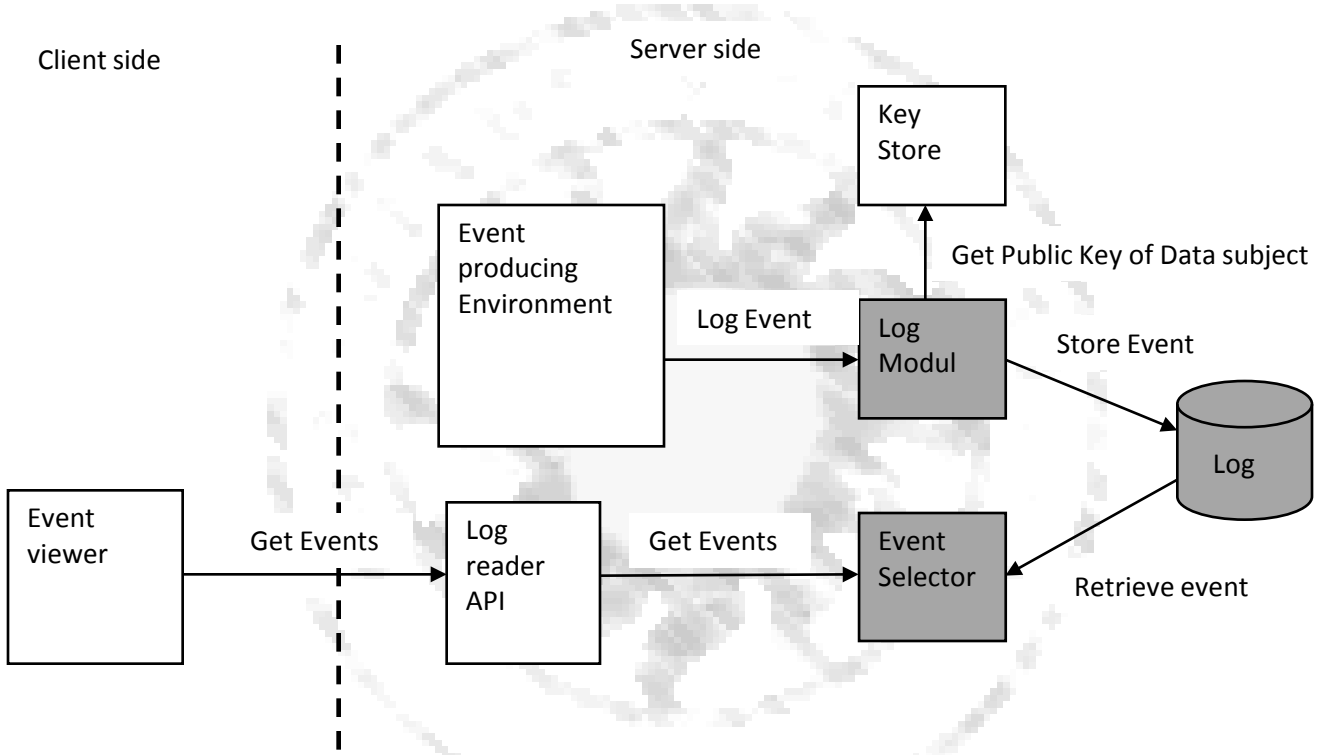
- Like a secure log, with the addition of:
  - Only the data subject for whom a log entry concerns can read its contents
  - Unlinkability of data subject's entries
  - Independent integrity validation
  - Provides anonymous access to the log entries
- And we need KEM-DEM hybrid cipher using probabilistic encryption schemes with key-privacy

The Wouters- Lathouwers- Simoens-Log

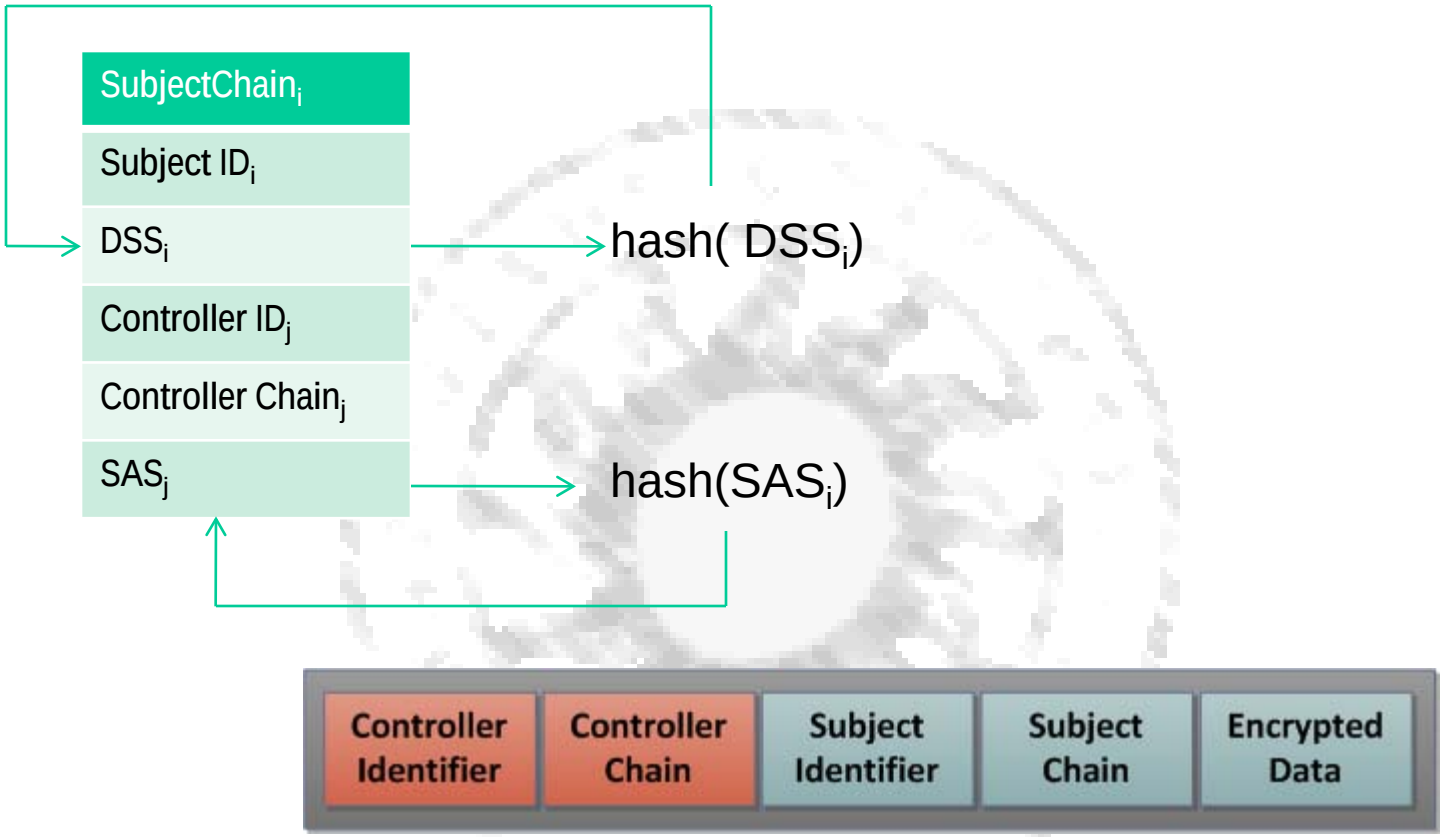


Pictures from Karel Wouters (COSICS/KUL)

A Privacy Preserving Secure Log



A Privacy Preserving Secure Log



Questions