



# Transparency Enhancing Technologies

Hans Hedbom  
Karlstad University

# Transparency tools

---

- A transparency tool for privacy purposes is a technological tool 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 control access and the existence of data
  - Aml, Data Mining, Web 2.0, Online Communities
  - Control use as a complement to Concealment?
- + European Law requires transparency
  - Not online requirement, but online tools will probably make things more costeffective.

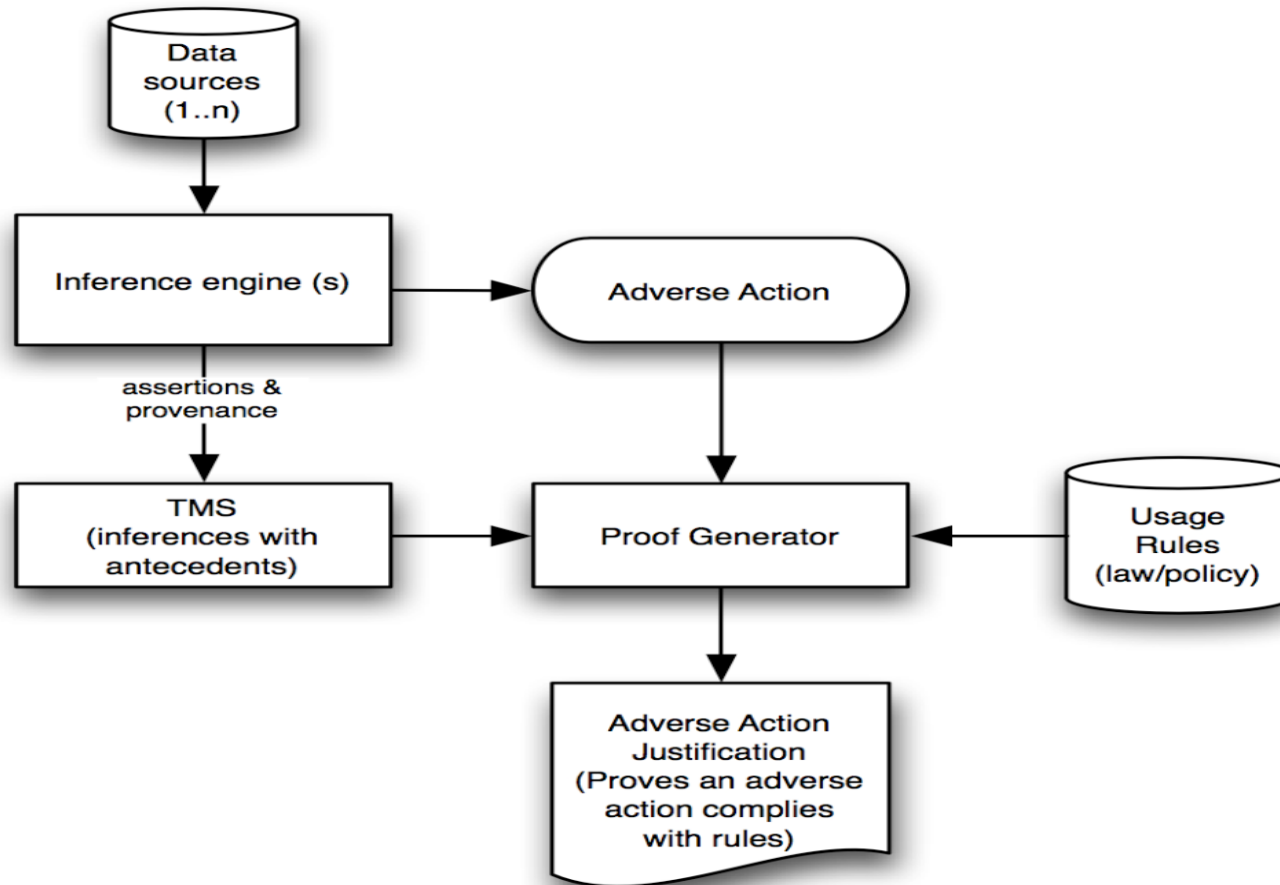


# Risks

---

- 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. McGuinness, G. J. Sussman, and K. Waterman. Transparent accountable 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.

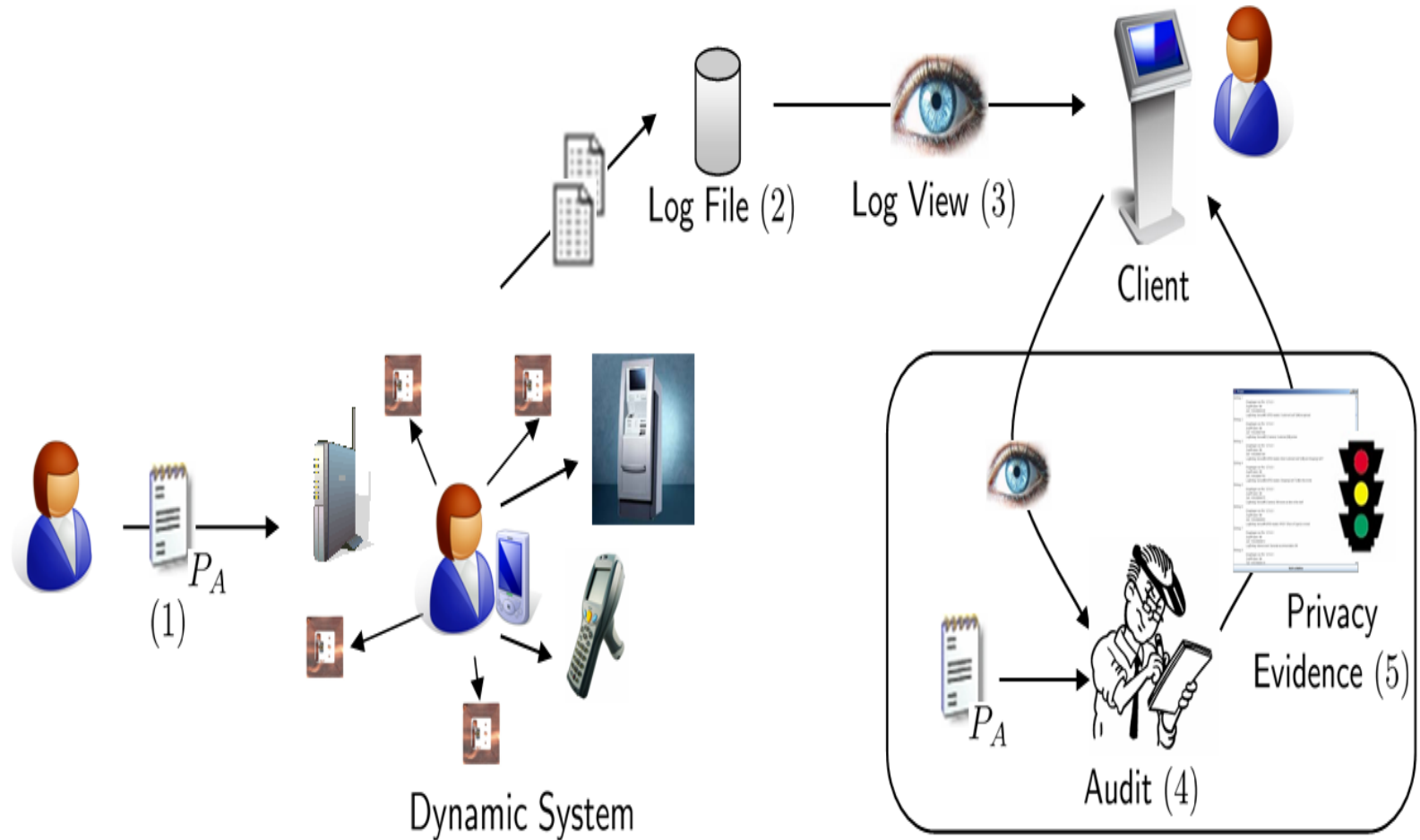


# Interesting approaches: TAMI

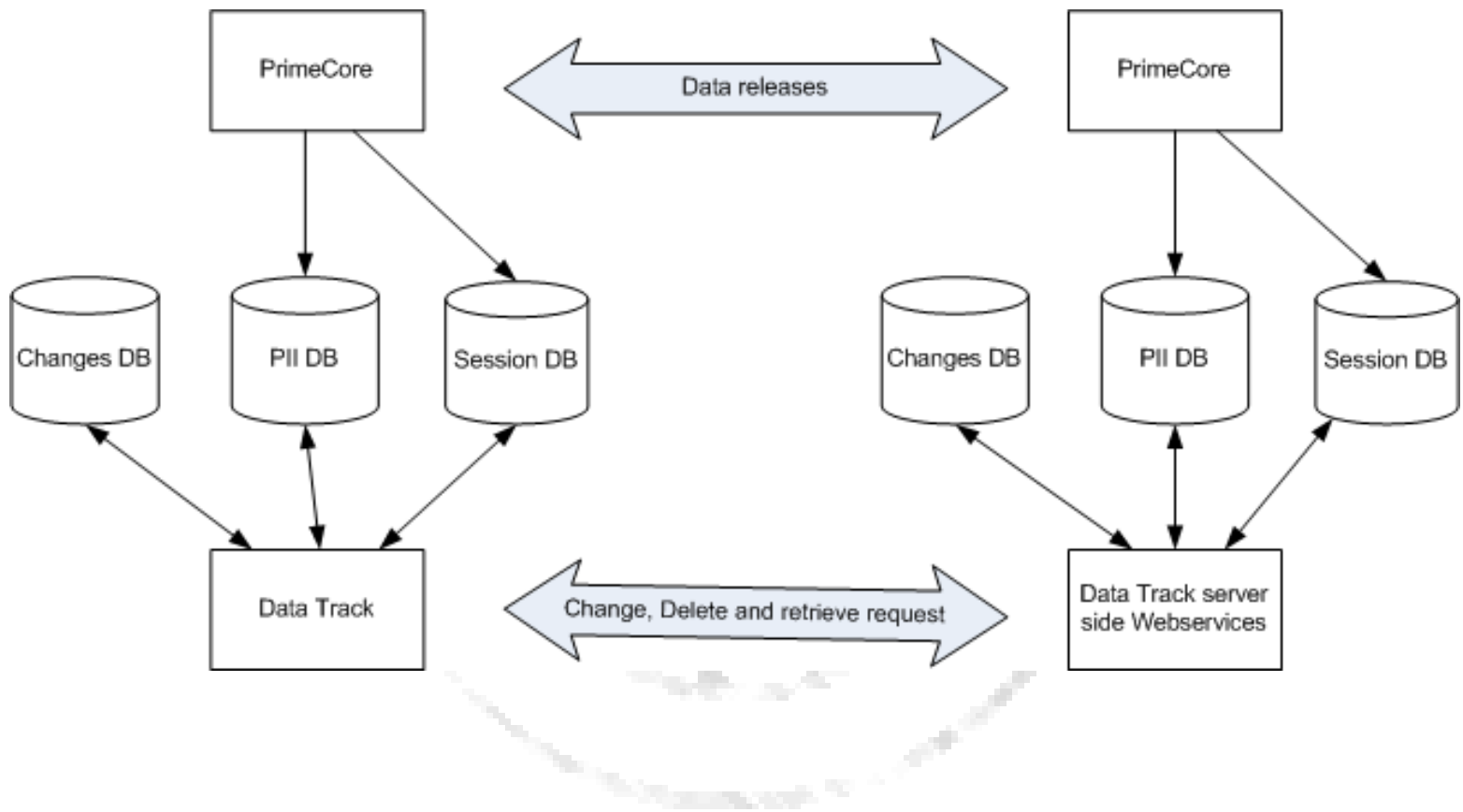
- Relies on WEB technology e.g.
  - N3 RDF
    - :pnr-1 a  
:PassengerNameRecord;  
:source :AA-PNR;  
:date 2004-06-14;  
:passenger  
[:name  
"John",  
[:personGivenName  
"Henry",  
:personMiddleName  
"Doe"];  
:personSurName  
"Doe"];  
:birthDate 1975-08-24];
  - N3 Logic
    - { ?X a Person.  
?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 }.



# Interesting approaches: Privacy Evidence



# PRIME/PrimeLife Data Track






# PRIME/PrimeLife Data Track

**PrimeLife - Data Track**

**Data Track** Here you can see who knows your data, and get assistance with data correction or removal

Record List Changes Record Slider Own Credentials

 Add Columns

Recipient	Time Stamp	Occurences
<input type="text" value="Search..."/>	<input type="text" value="Search..."/>	<input type="text" value="Search..."/>
▶ Shake My World	2007-01-30 - 2008-01-30	3
▶ SBAB	2007-03-12 - 2009-11-15	4
▶ SEB	2007-03-12 - 2009-11-15	4
▶ SJ	2009-07-12 - 2010-02-01	4
▶ Ving	2006-03-12 - 2010-01-15	4
▶ Adobe	2010-01-05 - 2010-02-01	2
▶ Helmia	2006-01-30 - 2010-02-01	3
▶ HTH	2009-06-10 - 2009-06-10	1
▶ Adlibris	2009-01-30 - 2009-03-15	2
▶ SAS	2009-05-28 - 2010-01-17	4
▼ Skandia	2007-03-22 - 2009-09-15	4
Skandia	2008-05-26 19.19	1
Skandia	2009-06-24 13.43	1
Skandia	2009-09-15 16.04	1
Skandia	2007-03-22 17.12	1
▶ LaRedoute	2008-06-13 - 2009-11-09	2
▶ DPI	2010-01-13 - 2010-01-21	2
▶ Landstinget i Värmland	2007-05-12 - 2009-08-15	4
▶ MQ	2008-05-22 - 2008-08-30	2
▶ Amazon	2010-01-21 - 2010-01-21	1

**PrimeLife**



# PRIME/PrimeLife Data Track



PrimeLife - Data Track

Contact information..

Summary Privacy Policy

Name : Skandia  
Organization: Unknown  
Street: Unknown  
City: Unknown  
Country: Unknown  
URL: http://www.skandia.se  
Date: 2009-06-24 13.43.00

Revealed Data 2009-06-24 13.43.00..

Retrieve data Delete all data  
from Skandia from Skandia

Category	Data	Remote Data	Verified By	Purpos
First name	Inga	Inga		Identification
Identifier	621221-6200	621221-6200	Transportstyrel...	Identification
Password	inga1221	inga1221		Identification
Official family ...	Vainstein	Vainstein		Identification

# PRIME/PrimeLife Data Track

PrimeLife - Data Track

Contact information..

Name : Skandia  
 Organization: Unknown  
 Street: Unknown  
 City: Unknown  
 Country: Unknown  
 URL: http://www.skandia.se  
 Date: 2007-03-22 - 2009-09-15

Record List | Changes | Record Slider | Own Credentials

Retrieve data from Skandia | Change data at Skandia | Delete data at Skandia

Category	Data Sent	Verifier Sent	Remotely Stored Data	Remote Stored Verifier	Time Stamp
Search...	Search...	Search...	Search...	Search...	Search...
Identifier	621221-6200	Transportstyrelsen	621221-6200	Transportstyrelsen	2008-05-26 19.19.00
Identifier	621221-6200	Transportstyrelsen	621221-6200	Transportstyrelsen	2009-06-24 13.43.00
Identifier	621221-6200	Transportstyrelsen	621221-6200	Transportstyrelsen	2009-09-15 16.04.00
Identifier	621221-6200	Transportstyrelsen	621221-6200	Transportstyrelsen	2007-03-22 17.12.00
Official family name	Vainstein		Vainstein		2008-05-26 19.19.00
First name	Inga		Inga		2008-05-26 19.19.00
Password	inga1221		inga1221		2009-06-24 13.43.00
Professions	Journalist		Journalist		2007-03-22 17.12.00
Street	Lingonstigen 8		Lingonstigen 8		2007-03-22 17.12.00



# 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

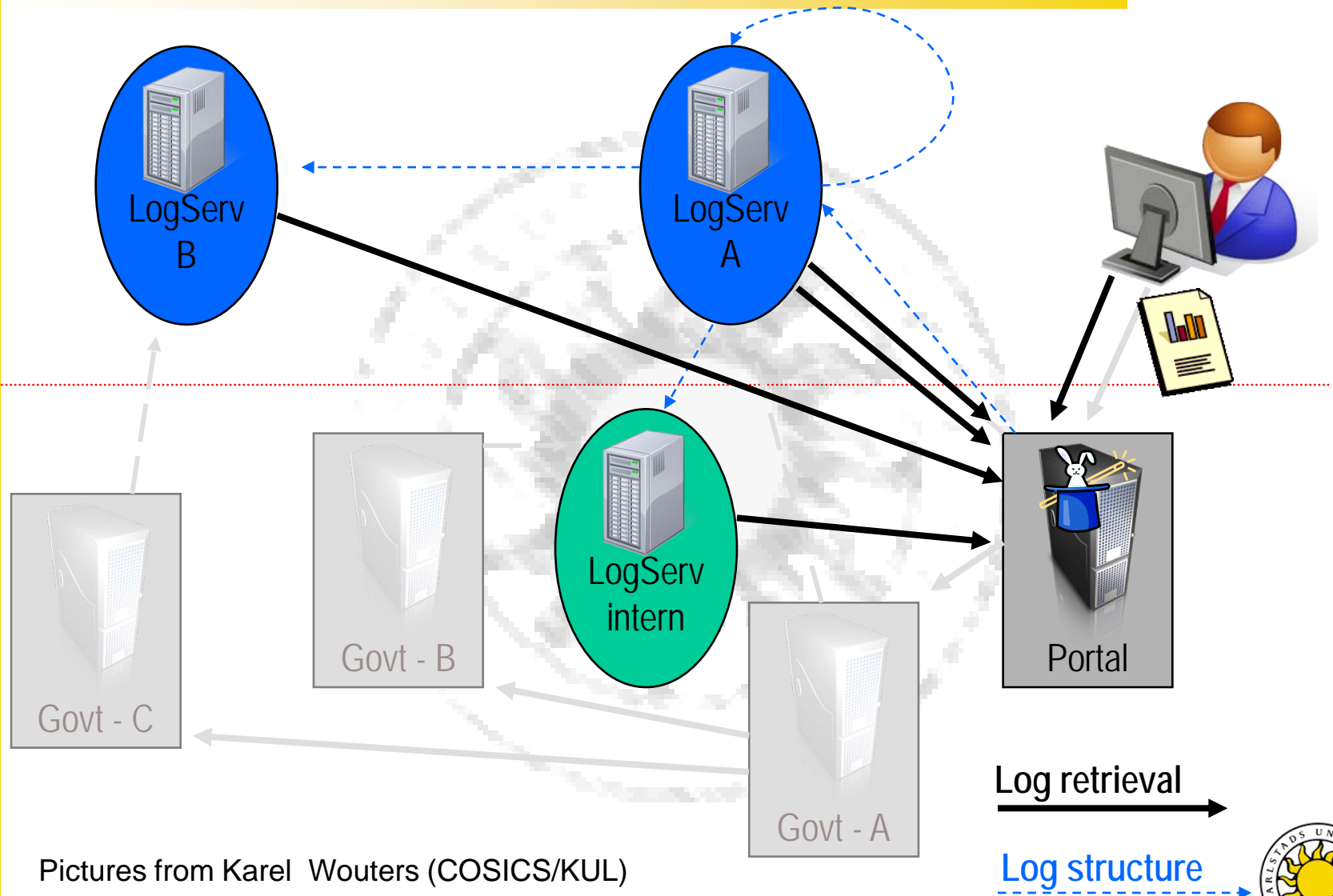


# Privacy Preserving Secure Logging

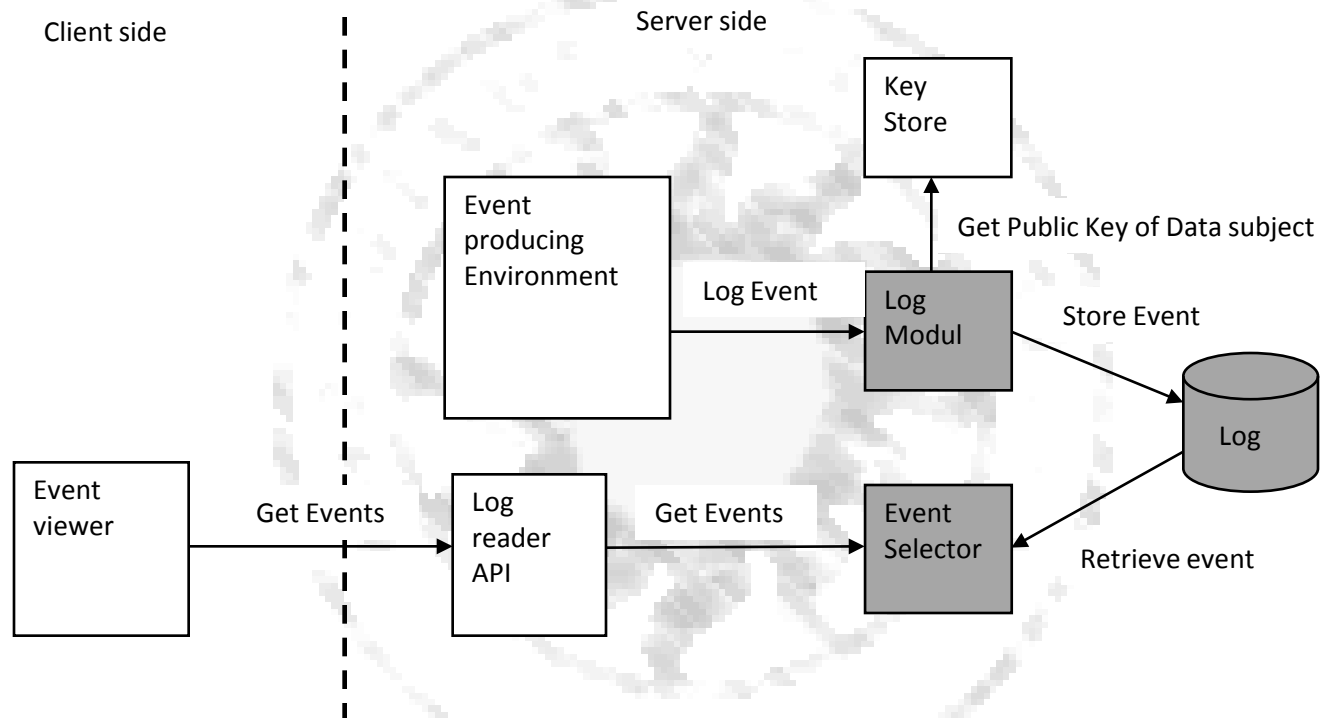
- ✚ Like a secure log, with the addition of:
  - Only the data subject for whom a log entry concerns can read its contents
  - Unlinkability of data subject's entries
  - Independent integrity validation
  - Provides anonymous access to the log entries
- ✚ And we need KEM-DEM hybrid cipher using probabilistic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



# The Wouters- Lathouwers- Simoens-Log

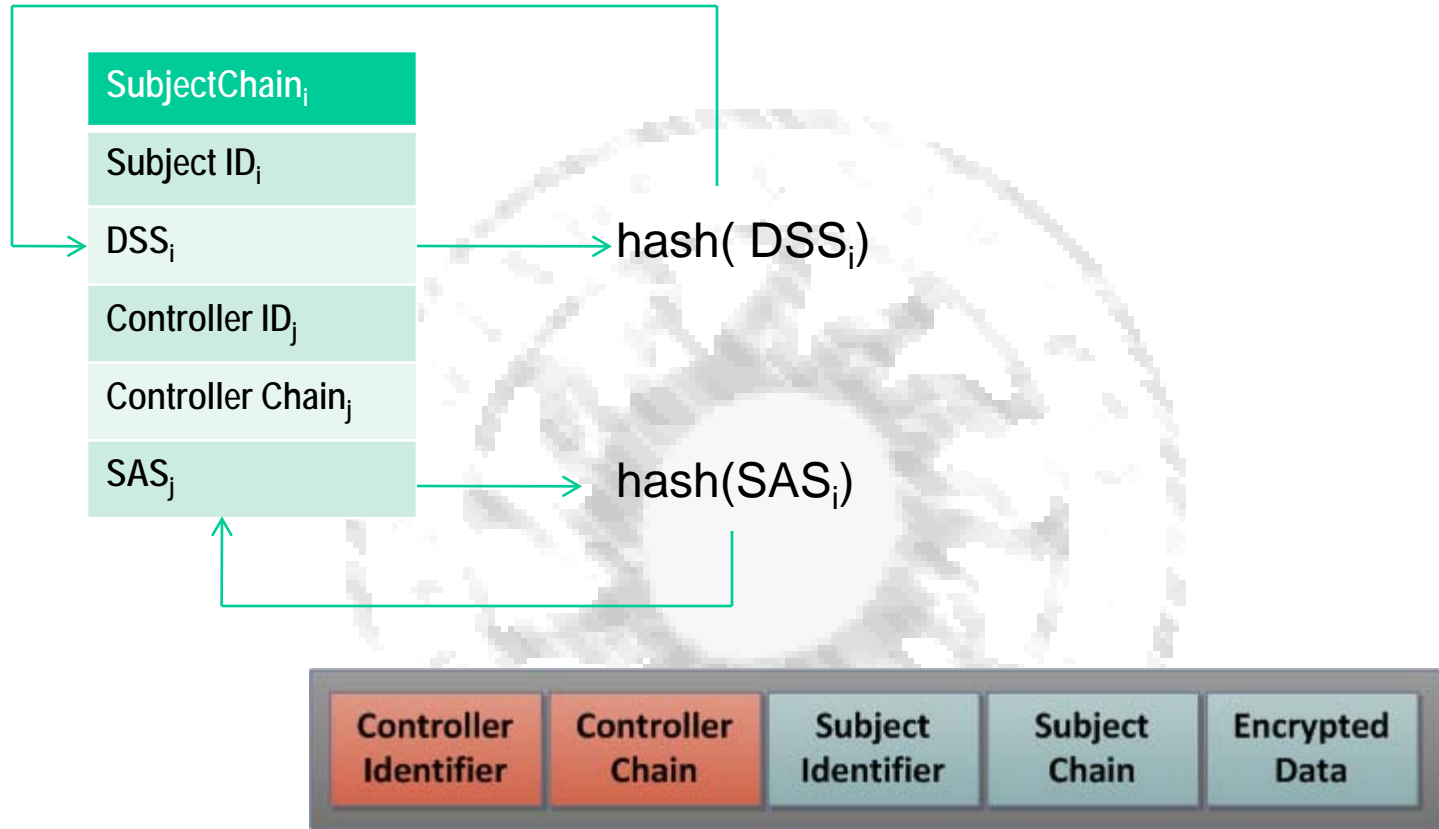


# A Privacy Preserving Secure Log





# A Privacy Preserving Secure Log



# Questions

---

