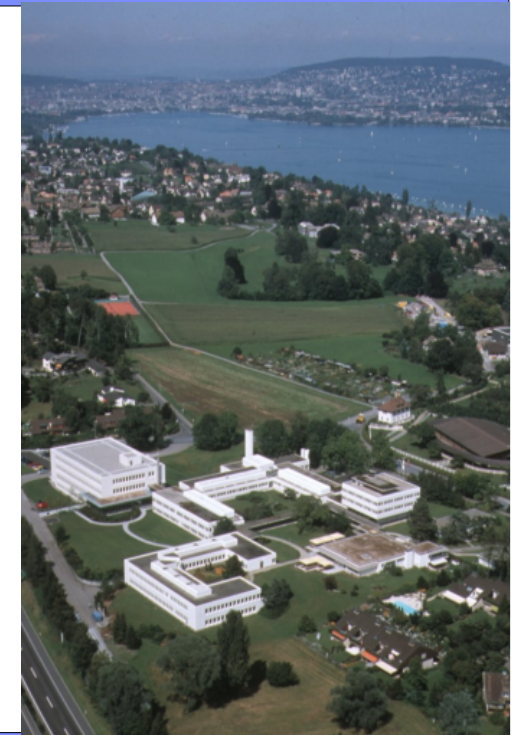




IBM Research

Privacy Challenges in the Future Internet

Phil Janson (pj@zurich.ibm.com)
Manager, Security & Cryptography
IBM Zurich Research Laboratory
IBM Academy of Technology





Problem Statement

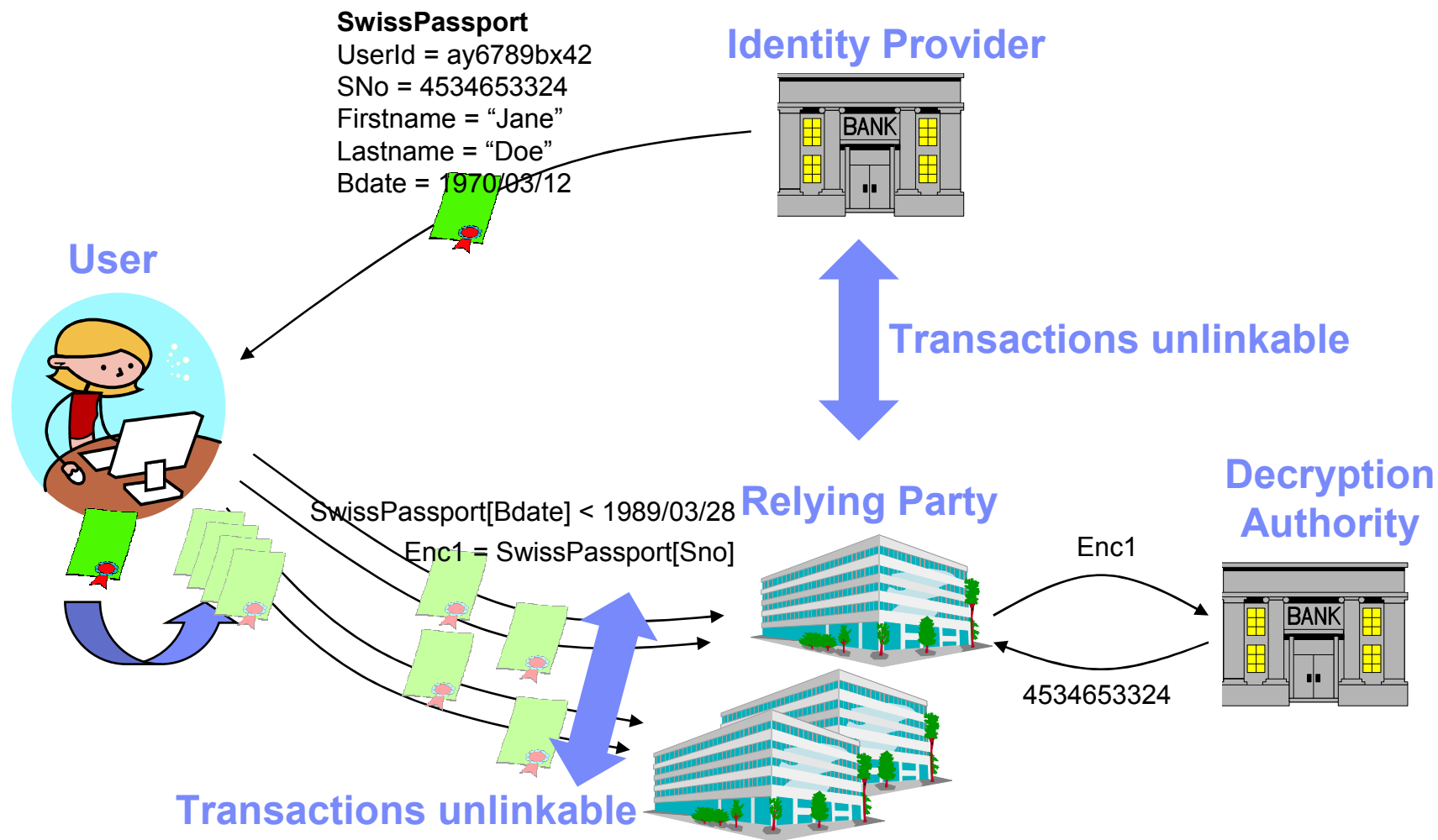
- **The physical world is forgetful - The digital world is not**
 - No train conductor or bar tender remembers all the ID cards they see in a day
 - But every visited service provider is eager to log as much as it can about users
 - allegedly to serve them better, usually to pester them with more marketing junk
- **Content accumulates ever faster**
 - Much collected behind our backs by sensing devices (e.g. surveillance cameras)
 - Much also volunteered by unsuspecting users themselves (e.g. social networking sites)
- **Data mining capabilities continue to increase exponentially**
 - incl. open crawling over the web and public info records
- **Our privacy shrinks as we grow up**
 - The whole life of millennium children will be on the web for all to see by the time they start applying for jobs (or looking for spouses ;-)
- **The digital world will not only record but increasingly control the physical one**
 - Location-based services are only a harmless basis to start from
 - Spontaneous behavior will emerge
- **Accountability is hard in a global world for lack of global regulations**



Challenges

- **Security is about controlling access (to info)**
Privacy is about controlling accuracy and usage (of personal info)
It is about controlling access to PII at info custodians / by 3rd parties
It implies sticking policies to PII as it moves around
and enforcing these policies + auditing usage over time
- **Security and IDM have traditionally been driven by provider requirements**
Privacy now requires putting users at the center – user-centric IDM
- **Privacy clashes with accountability, anonymity with traceability**
- **Privacy requires the ability to conduct transactions under pseudonyms or even anonymously at all levels with some potential safeguards**
 - Network (e.g. onion routing)
 - Application (e.g. attribute-based identification)
- **Scenarios**
 - Voting, blind decision-making, opinion survey
 - E-Service provision to restricted classes of users
(e.g. members, children, adults, seniors, residents, nationals, gender, etc.)

Federated, user-centric, privacy-enhanced identity management

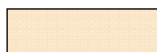




Privacy-enhanced (Hippocratic) Database technology

This solution consists of –

a) Active Enforcement Component

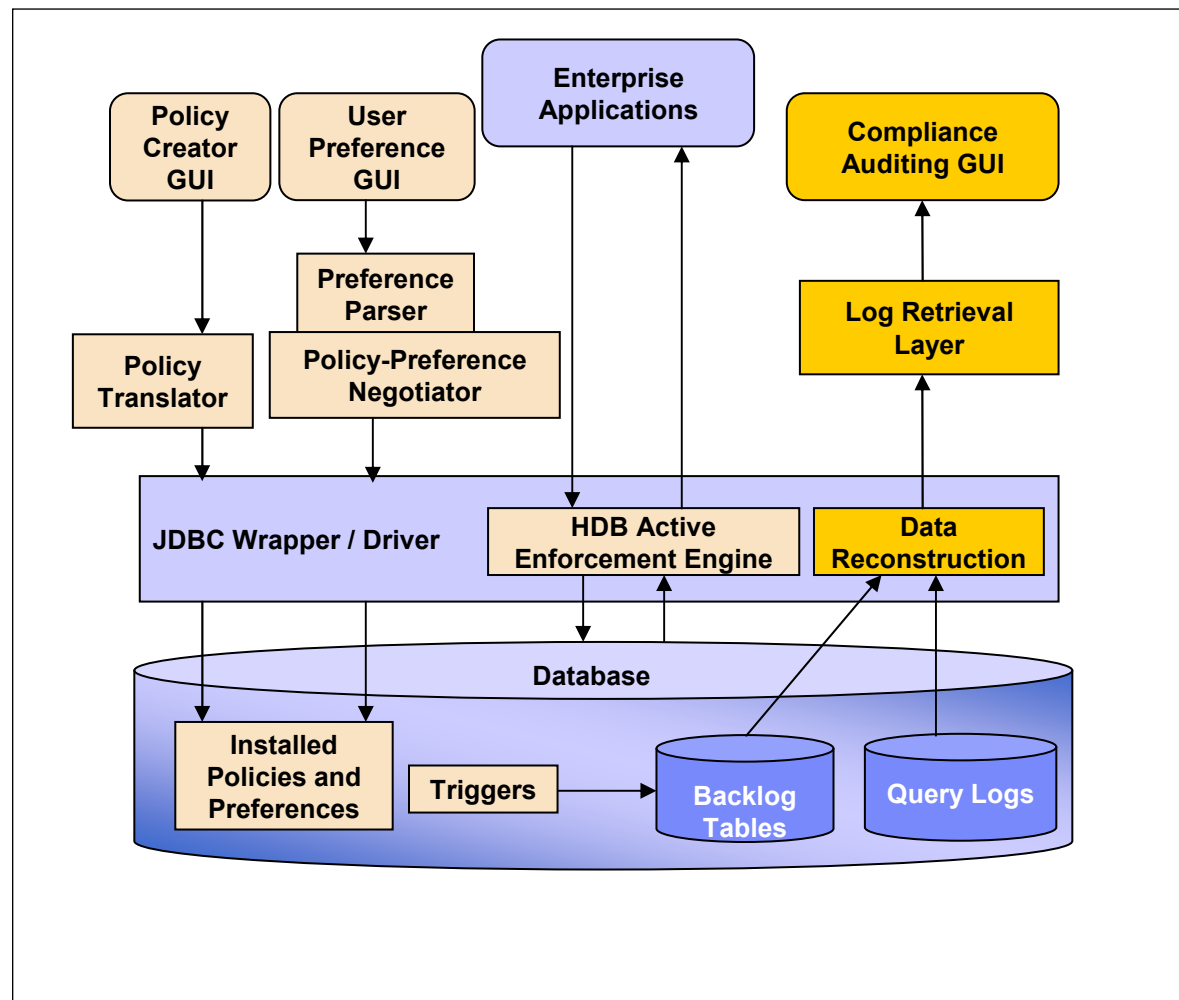


- Fine-grained
- Database-agnostic
- Application transparent

b) Compliance Auditing Component



- Supports compliance and accountability





Research Directions

- 1. Policy languages for policy description, composition, evaluation, matching, translation, etc.**
- 2. User interfaces to manage and deal with policies as needed / desired**
- 3. Cryptographic support for additional functional requirements**
 - Delegation, escrowing, revocation, restrictions
 - Dynamic cross-domain service composition
 - New scenarios and applications
 - Built-in support requirements
- 4. Leveraging eID, e-passport, e-banking, SIM and other cards**
 - Putting the technologies on identity provider chip cards
- 5. Key / credential management, esp. recovery through events of life**
- 6. Sticky policy enforcement through Trusted Computing infrastructure**
- 7. Compliance monitoring tools**
- 8. Privacy in computing clouds**
- 9. Standards, infrastructures, open source packages, education, regulations, legislation**