

# Privacy Enhanced Identity Management

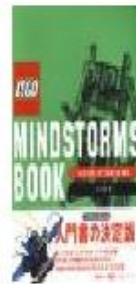
Caroline Sheedy  
School of Computing  
Dublin City University

`caroline.sheedy@computing.dcu.ie`

1 December 2005



# Introduction



# Outline

- Introduction
  - What is identity?
- Certificates and identity
  - Current structure
  - Rethinking
  - Proposed framework
- Work to date
  - Core components
- Future work

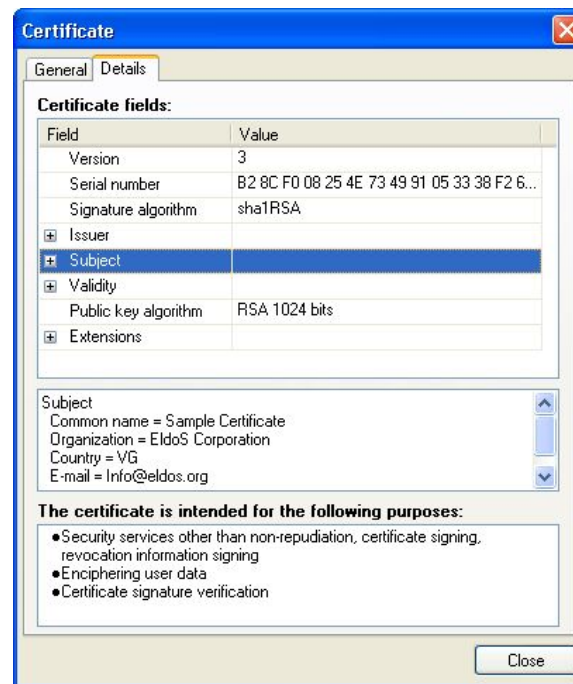


# What is Identity used for?

- Establishing relationships
  - Client / Server
  - Trust
- Authentication
  - username / password
  - biometric
  - smartcards
  - certificates
  - cookies

# Digital Certificates and Identity

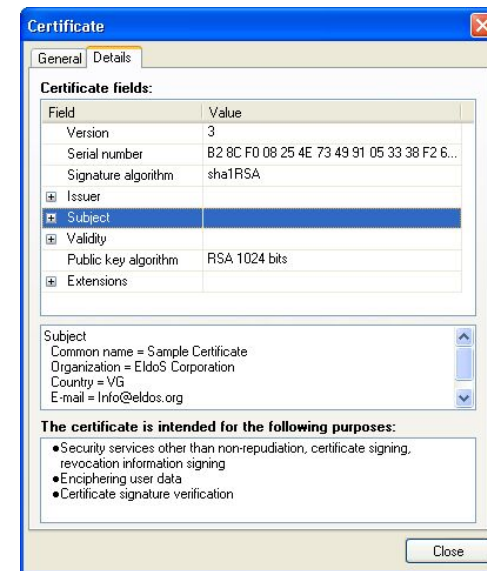
- A *Digital Certificate* is a signed assertion about a public key
- Binds a key to one or more attribute
- Used to establish trust relationship



# Identity and Privacy

The requirement for a change in the way privacy and identity are managed is argued by Brands:

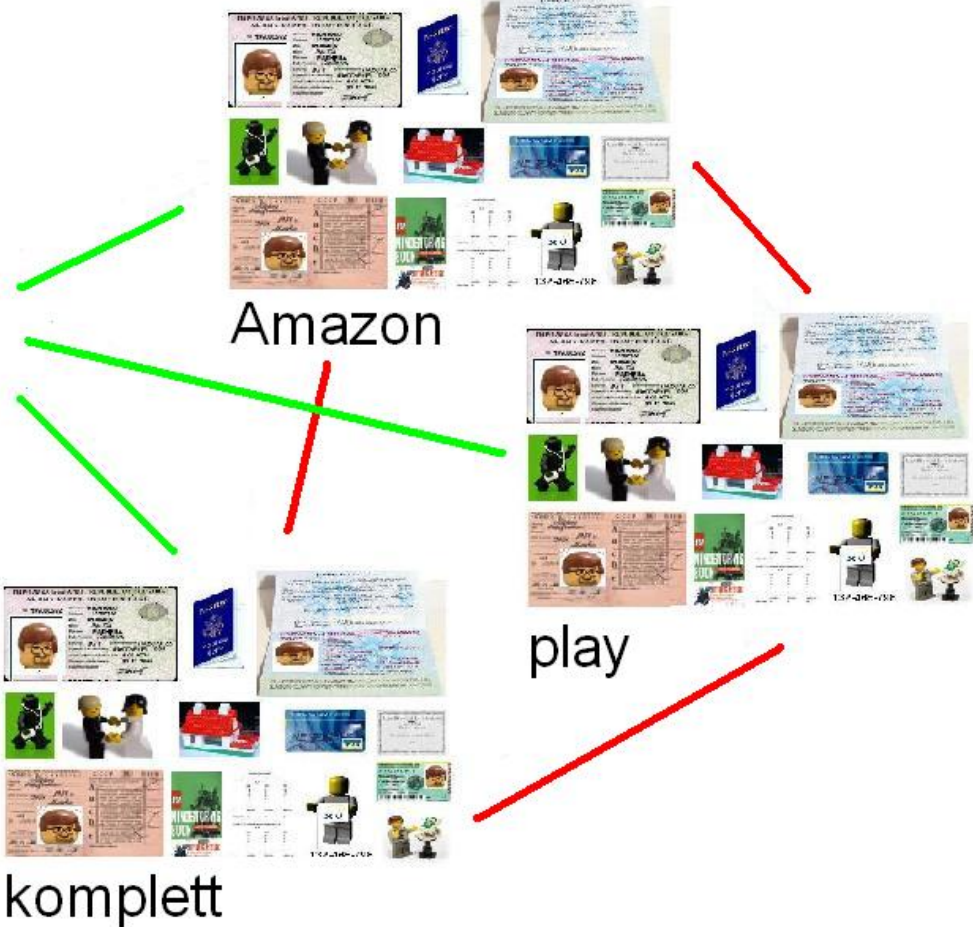
*‘ Schemes in which users do not have control over their own personal data offer zero privacy ’*



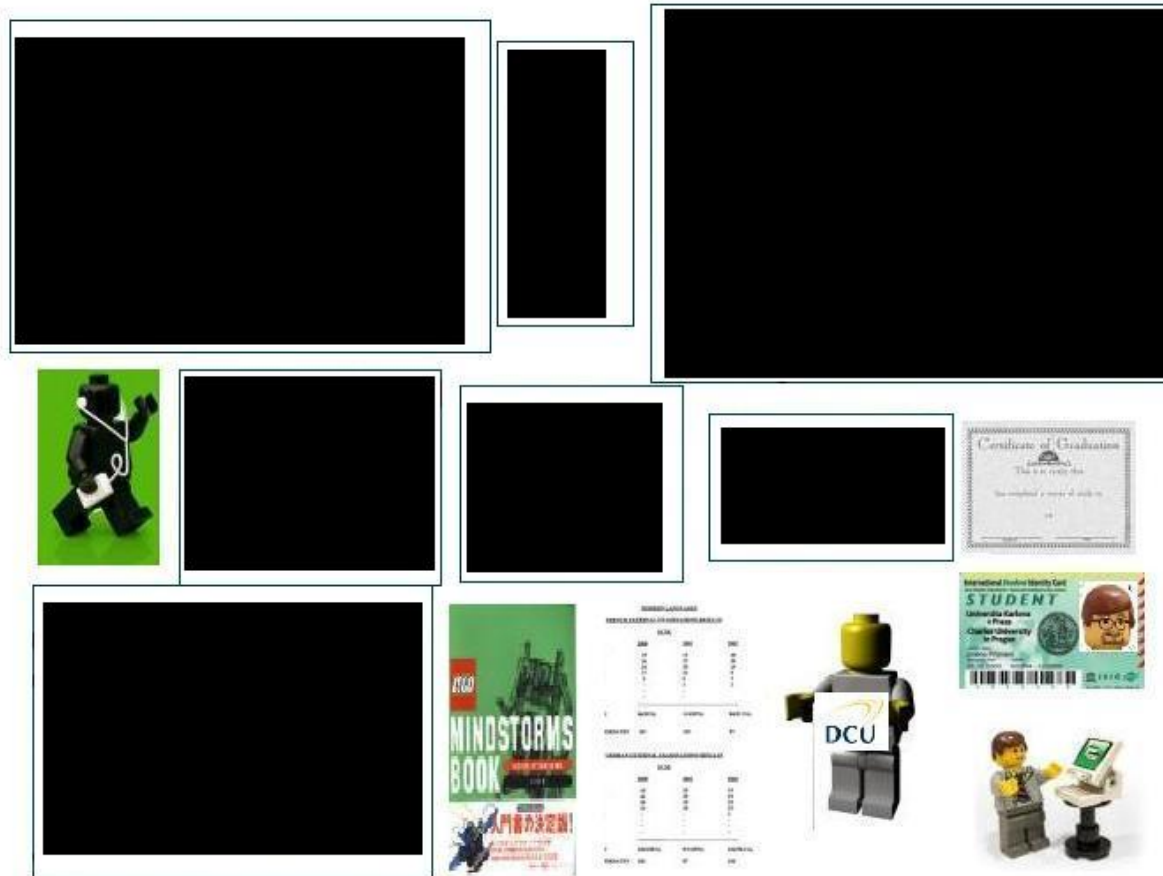
# Issues with existing structure

- Leads to disclosure of *certificate* identity
- Loss of anonymity
- Traceable actions
- Linkable actions
- Loss of control
- Persistence

# Requirements - Multi-show unlinkability



# Requirements - Selective showing of data items



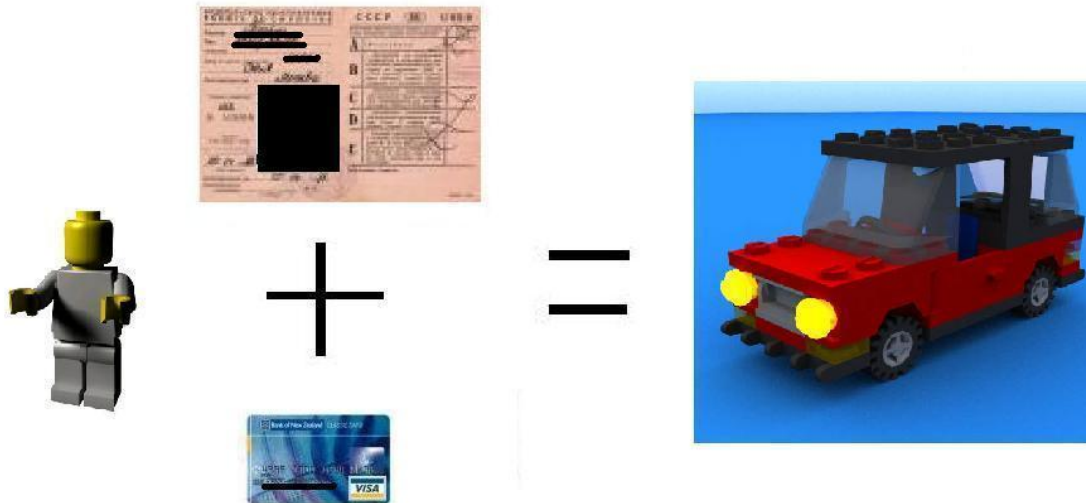
# Requirements - Proving relations between data items

Renting a car -

Need valid drivers license

Credit card with sufficient funds

Why disclose name?



# Requirements - Conditional showing of data items

if



then



# Fundamentals

- Hard Problem
  - Basis of cryptographic protocols
- Commitment schemes
  - Coin flipping schemes
- Zero-Knowledge proof systems
  - Prove something is known without revealing what it is

# Hard Problem

## Discrete Logarithm problem

Given a prime  $p$ , a generator  $\alpha$  and an element  $\beta \in \mathbf{Z}_p^*$ , find the integer  $x$ ,  $0 < x < p - 1$ , such that  $\alpha^x \equiv \beta \pmod{p}$

So for example:

From

$$\alpha = 2, p = 2579, x = 765$$

we get

$$\beta = 2^{765} \pmod{2579} = 949$$

From this we can see if we are given  $\alpha$ ,  $\beta$  and  $p$ , finding  $x$  is *Hard*



# Zero-Knowledge

An interactive proof system, with the following requirements:

- **Complete** If Peggy is honest, Victor should only accept the proof with  $P \rightarrow 1$
- **Sound** If Peggy is dishonest, Victor should only accept the proof with  $P \rightarrow 0$



# Zero-Knowledge Scheme

Input: Positive integer  $n$ , two distinct elements  $\alpha, \beta \in \mathbf{Z}_n^*$ , where the order of  $\alpha$  is  $l$ , all publicly known values and private  $k$  such that

$$\alpha^k \equiv \beta \pmod{n}.$$

- Peggy chooses random  $j$  st  $0 \leq j \leq l - 1$ , and computes  $\gamma$  to send to Victor

$$\gamma = \alpha^j \pmod{n}$$

- Victor chooses  $i = 0$  or  $1$ , and sends  $i$  to Peggy
- Peggy computes

$$h = j + ik \pmod{l} \text{ where } k = \log_{\alpha}\beta$$

and sends  $h$  to Victor

- Victor checks if

$$\alpha^h \equiv \beta^i \gamma \pmod{n}$$



# Our work to date

- OpenSSL
  - C libraries using bn
- Number theory
  - Jacobi
  - Quadratic Residues
  - Group Functionality
- Bit commitment
  - Pedersen
  - Discrete Log
  - Quadratic Residues
- Zero Knowledge
  - Discrete Log
  - Quadratic Residues



# Future work

- Full Cryptographic framework
  - Multi-show unlinkability
  - Selective disclosure
  - Conditional disclosure
- Independence of underlying libraries
  - facilitate independence of bn - eg use Miracl instead.

## **Digital Rights Ireland launch Tues Dec 6th - Invite**

Digital Rights Ireland formally launches on Tues Dec 6th at  
11.15am at the Pearse Street Library in Dublin.

[www.digitalrights.ie](http://www.digitalrights.ie)

