


# Identity Management and Privacy

Prof. Bart Preneel  
COSIC  
Katholieke Universiteit Leuven, Belgium  
Bart.Preneel(at)esat.kuleuven.be  
<http://homes.esat.kuleuven.be/~preneel>  
June 2010

Special thanks to  
Claudia Diaz and  
Carmela Troncoso

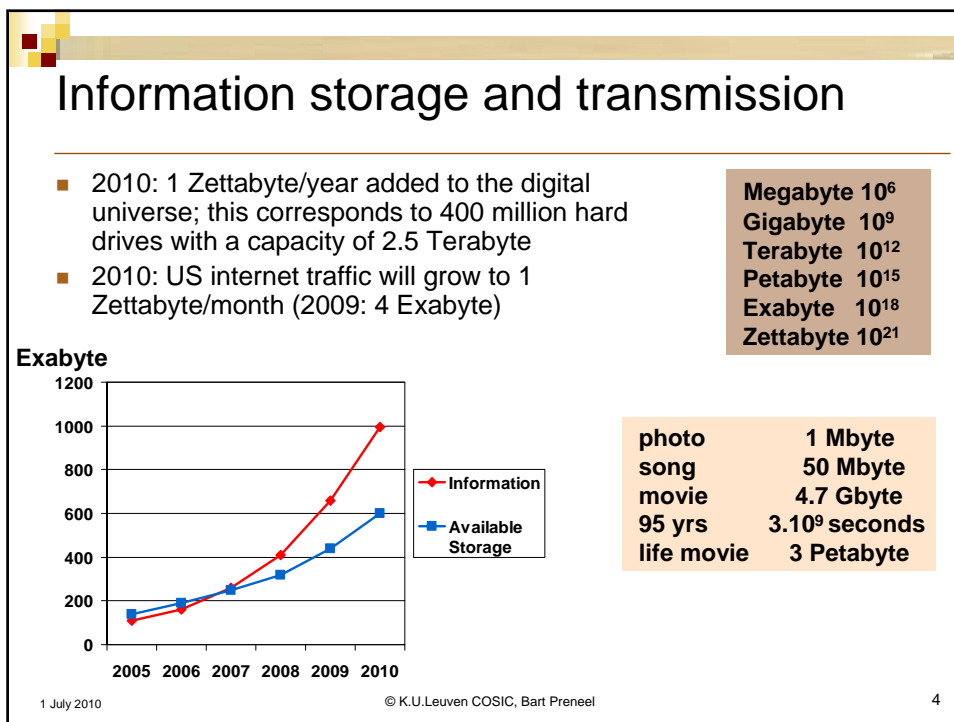
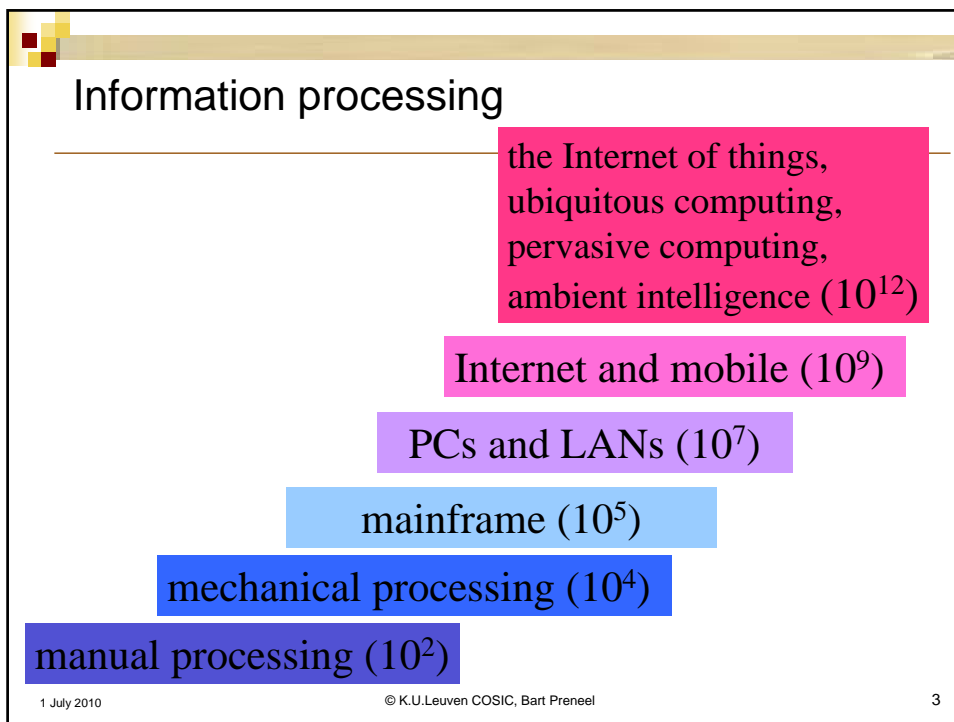


## Outline

---


- context: information processing and uniqueness
- do we need privacy?
- what is privacy anyway?
- identity management
- privacy by design
- conclusions

1 July 2010 © K.U.Leuven COSIC, Bart Preneel 2

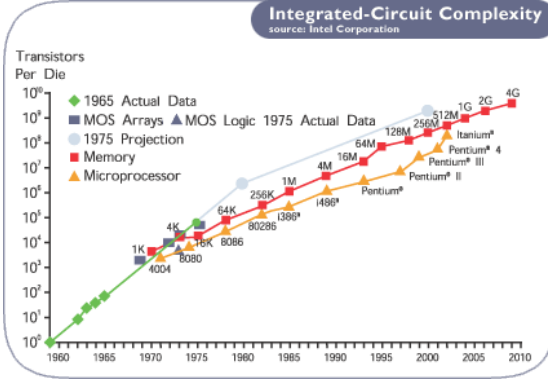


## Exponential growth

Ray Kurzweil, KurzweilAI.net





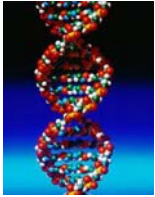
- human brain:  $10^{14}$  ...  $10^{15}$  ops and  $10^{13}$  bits memory
- 2025: 1 computer can perform  $10^{16}$  ops ( $2^{53}$ )
- 2013:  $10^{13}$  RAM bits (1 Terabyte) cost 1000\$



1 July 2010 © K.U.Leuven COSIC, Bart Preneel 5

## Uniqueness

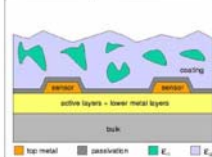

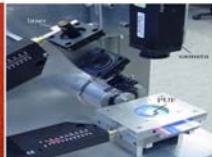
- physics and electronics (accidental)
  - process variation in deep submicron processes
  - radio fingerprinting: unique pattern of each wireless antenna, modulator, filter, oscillator
  - fibers in paper
  - magnetic behavior of certain materials
- human: biometry
  - fingerprint
  - iris
  - DNA
  - face
  - gait
  - ...

1 July 2010 © K.U.Leuven COSIC, Bart Preneel 6

## Uniqueness

- physics and electronics (deliberate)
  - MAC address, IMEI
  - Pentium III Processor Serial Number 1999
  - yellow dots produced by laser printers
  - PUF Physical Unclonable Function

| Coating PUFs  | Acoustic PUFs   | Optical PUFs   |
|---|---|--|
| Measuring the capacitances of a coating with random dielectric particles          | Probing structures with acoustic waves  | Disordered structures illuminated by a laser beam                                  |
|  |  |  |

credit:  
Philips/  
Intrinsic ID

1 July 2010

7

## How many ways have you been located today?

- cell phone (turned on?)
- laptop computer
- credit card at the gas station
- bank card in the ATM machine
- driving through a monitored intersection
- security camera at the supermarket
- scan badge to enter a building
- pass a Bluetooth-enabled printer

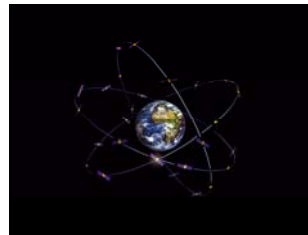
1 July 2010

© K.U.Leuven COSIC, Bart Preneel

8

## “Chattering” devices

- RFID
- Bluetooth/Zigbee
- WLAN
- WiMAX
- 2G/GSM
- 3GSM
- GPS/Glonass/Galileo



1 July 2010

© K.U.Leuven COSIC, Bart Preneel

9

## Location Based Services

- location-based traffic monitoring and emergency services
  - e-Call, traffic congestion control
- location finder:
  - where is the nearest restaurant, gas station,...
  - variable pricing applications
  - congestion pricing
  - pay-as-you-drive
- social applications
  - Geotagged Twitter
  - Google Latitude

### Gartner on LBS:

- 2008: 998.3 M\$ revenue
- 2009: 2.2 B\$ revenue
- 2012: 0.5 B users

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

10

## Why is this a problem?

- do you want to be seen at certain locations?
  - abortion clinic, AIDS clinic, business competitor, or political headquarters (Google Street View)
  
- what can be automatically inferred about a person based on location?
  - any important location...
    - desk in a building
    - home location
    - future locations
  - and even identification!
    - <http://www.batchgeocode.com/lookup/>



Source: John Krumm, "A survey of computational location privacy", *Personal and Ubiquitous Computing*, Volume 13, Issue 6, 2008

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

11

## Intelligent processing uniqueness + connectivity + processing power

- create "big brother" or "Kafka" for specific purposes
  - protecting children
  - road pricing and congestion control
  - public transport
  - car insurance
  - car pool
  - social networking
  - anti-counterfeit
  - copyright infringements
  - ...
  
- individual applications are legitimate
- cost effective
  - limited need for tamper resistance: cost reduction
  - allows for effective pricing (and price discrimination)
- long term incentive for integrating solutions and function creep

inexpensive  
mass surveillance



1 July 2010

© K.U.Leuven COSIC, Bart Preneel

12

## The privacy debate

---

- “if you care so much about your privacy it’s because you have *something to hide*”
- “surveillance is good and privacy is bad for national security. We need a *tradeoff* between privacy and security”
- “people don’t *care* about privacy”

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

13

## The privacy debate

---

- “if you care so much about your privacy it’s because you have *something to hide*”
- Solove:
  - “the problem with the ‘nothing to hide’ argument is its underlying assumption that **privacy is about hiding bad things.**”

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

14

## The privacy debate

- “surveillance is good and privacy is bad for national security. We need a *tradeoff* between privacy and security”
- “we need more surveillance” is a powerful argument
  - if attacks increase, you can argue that you need even more
  - if attacks decrease, you take credit

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

15

## The privacy debate

- “surveillance is good and privacy is bad for national security. We need a *tradeoff* between privacy and security”
- not **effective**: smart adversaries evade surveillance
- risk of **abuse**: lack of transparency and safeguards
- risk of **subversion** for crime/terrorism

example: Greek Vodafone scandal (2006):  
“someone” used the **legal interception**  
functionalities (backdoors) to monitor 106 key  
people: Greek PM, ministers, senior military,  
diplomats, journalists...



1 July 2010

© K.U.Leuven COSIC, Bart Preneel

16



## The privacy debate

- “people don’t *care* about privacy”
- people want to **control** information:
  - impression management /self-presentation
    - what do we tell to whom
    - concerns over information taken out of context
  - personal safety
  - we value friends who are discreet

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

17

## The privacy debate

- [Solove] “Part of what makes a society a good place in which to live **is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be suffocation.**”
- [Diffie and Landau] “Communication is fundamental to our species; **private communication is fundamental to both our national security and our democracy.**”
- [Diffie] “In the long run privacy and individual autonomy have no chance against increase in communications.”



1 July 2010

© K.U.Leuven COSIC, Bart Preneel

8

## Taking privacy to create security



Source: <http://www.myconfinedspace.com/>

Is there a tradeoff between privacy and security?

## Privacy = Security Property

- individuals
  - freedom from intrusion, profiling and manipulation, protection against crime / identity theft, flexibility to access and use content and services, control over one's information
- companies
  - protection of trade secrets, business strategy, internal operations, access to patents
- governments / military
  - protection of national secrets, confidentiality of law enforcement investigations, diplomatic activities, political negotiations
- shared infrastructure
  - despite varying capabilities infrastructure is shared
  - telecommunications, operating systems, search engines, on-line shops, software, . . .
  - denying security to some, means denying it to all: *crypto wars redux?*

## What is privacy?

- abstract and subjective concept, hard to define
  - fuzziness can be seen as an advantage
- dependent on cultural issues, study discipline, stakeholder, context
- privacy as **confidentiality**
  - “The right to be let alone”; focus on freedom from intrusion
- privacy as **control**: informational self-determination
- privacy as a **practice**
  - focus on user experience

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

21

## Recent definition of privacy

(US) National Strategy for Trusted Identities in Cyberspace -  
Creating Options for Enhanced Online Security and Privacy  
[http://www.dhs.gov/xlibrary/assets/ns\\_tic.pdf](http://www.dhs.gov/xlibrary/assets/ns_tic.pdf)

The appropriate use of personal information under the circumstances.

What is appropriate will depend on context, law, and the individual's expectations;

also, the right of an individual to control the collection, use, and disclosure of personal information.

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

22

## Data protection: legal basis

- 1950: European Convention on Human Rights (ECHR)
  - Art. 8 provides a right to respect for citizen's "private and family life, his home and his correspondence," subject to certain restrictions.
  - very broad interpretation by the European Court of Human Rights (Strasbourg)
  - part of Lisbon treaty (2009)
- 1981: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe)
- 1995: EU Data Protection Directive 95/46/EC

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

23

## Data protection

- data collected for specific and legitimate **purpose**
- **proportional**: adequate, relevant and not excessive (data minimization)
- with the subject's awareness and **consent**
  - unless data is necessary for...
- data subject's right to access, correct, delete her data
- data security: integrity, confidentiality of the data
  - unfortunately, millions of records with personal data are breached every year
- weak enforcement, low penalties
- creates database of databases
- USA: fair information practices
  - many individual laws (HIPAA, California disclosure laws)

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

24

## Solove's taxonomy of privacy

- information collection
  - surveillance
  - interrogation
- information processing
  - aggregation
  - identification
  - insecurity
  - secondary use
  - exclusion
- information dissemination
  - breach of confidentiality
  - disclosure
  - exposure
  - increased accessibility
  - blackmail
  - appropriation
  - distortion
- invasion
  - intrusion
  - decisional Interference

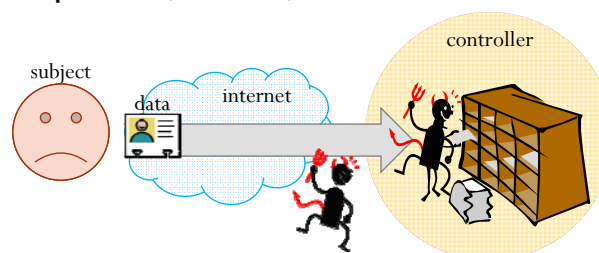
1 July 2010

© K.U.Leuven COSIC, Bart Preneel

25

## Soft privacy

- system model
  - data subject provides her data
  - data controller responsible for its protection
- threat model
  - external parties, errors, malicious insider



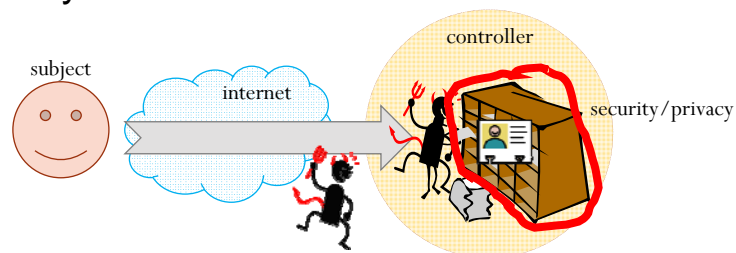
1 July 2010

© K.U.Leuven COSIC, Bart Preneel

26

## Soft privacy

- controller: main security “user”
- policies, access control, audits (liability)
- goal (data protection): purpose, consent, data security



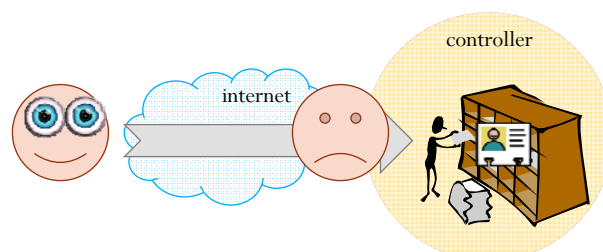
1 July 2010

© K.U.Leuven COSIC, Bart Preneel

27

## Soft privacy

- data subject has already **lost control** of her data
  - in practice, very difficult for data subject to verify how her data is collected and processed



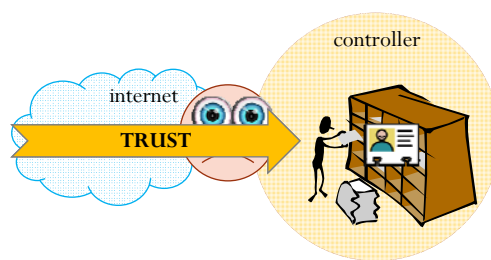
1 July 2010

© K.U.Leuven COSIC, Bart Preneel

28

## Soft privacy

- data subject has already **lost control** of her data
  - in practice, very difficult for data subject to verify how her data is collected and processed
  - need to trust data controllers (honesty, competence) and hope for the best



TRUST ASSUMPTIONS?

INCENTIVES?

TECHNOLOGICALLY ENFORCED?

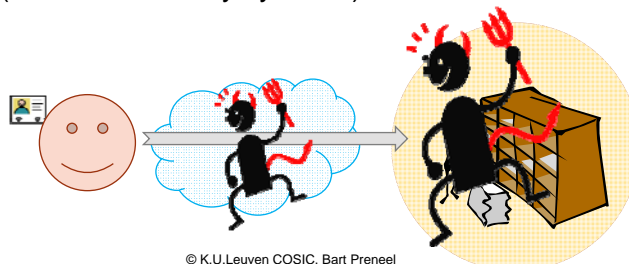
1 July 2010

© K.U.Leuven COSIC, Bart Preneel

29

## Hard privacy

- system model
  - subject provides as little data as possible
- reduce as much as possible the need to “trust” other entities
- threat model
  - adversarial environment: communication provider, data holder
  - strategic adversary with certain resources motivated to breach privacy (similar to security systems)



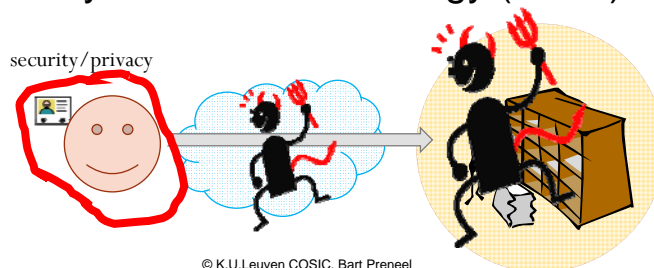
1 July 2010

© K.U.Leuven COSIC, Bart Preneel

30

## Hard privacy

- subject is an active security “user”
- goal (data protection): data minimization
- goal (Solove): protect against surveillance, interrogation, aggregation, identification
- hard privacy solutions: technology (PETs)



1 July 2010

© K.U.Leuven COSIC, Bart Preneel

31

## Outline

- Context: information processing and uniqueness
- Do we need privacy?
- What is privacy anyway?
- Identity management
  - What is identity management?
  - ID management 1.0
  - ID management 1.5
  - Principles of identity and ID management 2.0
- Privacy by design
- Conclusions

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

32

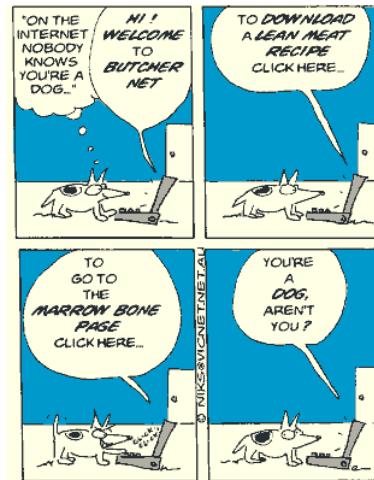


## A picture is worth more than a thousand words



"On the Internet, nobody knows you're a dog."

New Yorker, 1993



1 July 2010

© K.U.Leuven COSIC, Bart Preneel

33

## What is Identity Management (IDM)?

- secure management of the identity life cycle and the exchange of identity information (e.g., identifiers, attributes and assertions) based on applicable **policy** of entities such as:
  - users/groups
  - organizations/federations/enterprise/service providers
  - devices/network elements/systems
  - objects (application process, content, data)

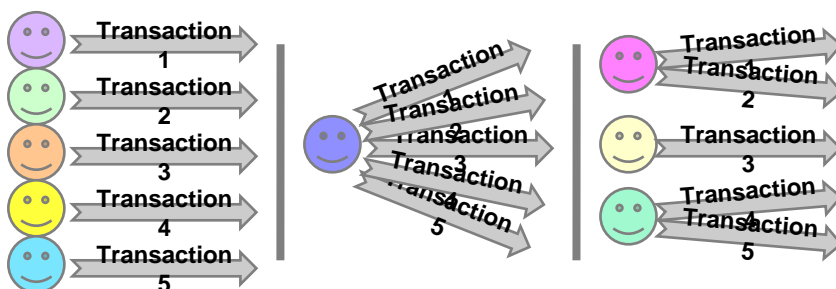
1 July 2010

© K.U.Leuven COSIC, Bart Preneel

34

## Pseudonymous identity management

- one-time pseudonyms: anonymity
- persistent pseudonyms: they become an identity
- solutions in between: partial identities

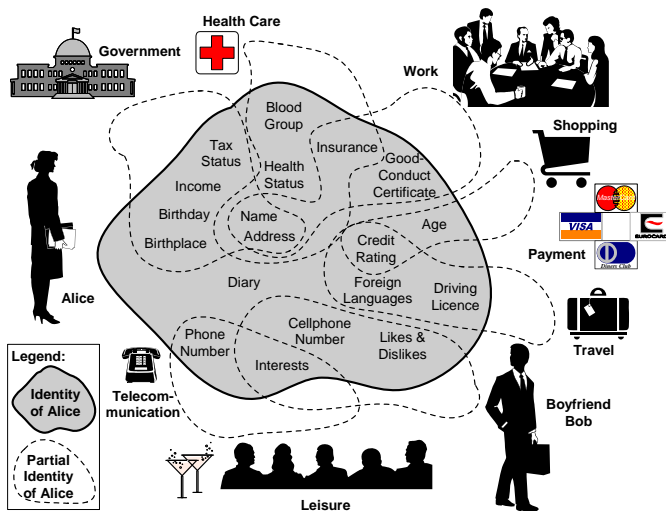


1 July 2010

© K.U.Leuven COSIC, Bart Preneel

35

## Identity Management: partial identities



1 July 2010

© K.U.Leuven COSIC, Bart Preneel

36

## Identity: definitions (1)

- **attributes:** distinct & measurable properties belonging to a particular entity
- **identity:** dynamic collection of all of the entity's attributes (1 entity: 1 identity)
- **partial identities:** specific subset of relevant attributes
- **identifier:** attribute or set of attributes of an entity which uniquely identifies the entity in a given context
- **credential:** piece of information attached to an entity and attesting to the integrity of certain stated facts



!! these definitions reflect a specific vision on identity and identity management

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

37

## Identity: definitions (2)

- **entity authentication or identification:** using claimed or observed attributes of an entity to distinguish the entity in a given **context** from other entities it interacts with
  - **Note:** in computer security, often identification is providing one's username and authentication is proving who an entity is
- **authorization:** the permission of an authenticated entity to perform a defined action
- **registration:** process in which a **partial identity** is assigned to an entity and the entity is granted a means by which it can be authenticated in the future

!! these definitions reflect a specific vision on identity and identity management

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

38

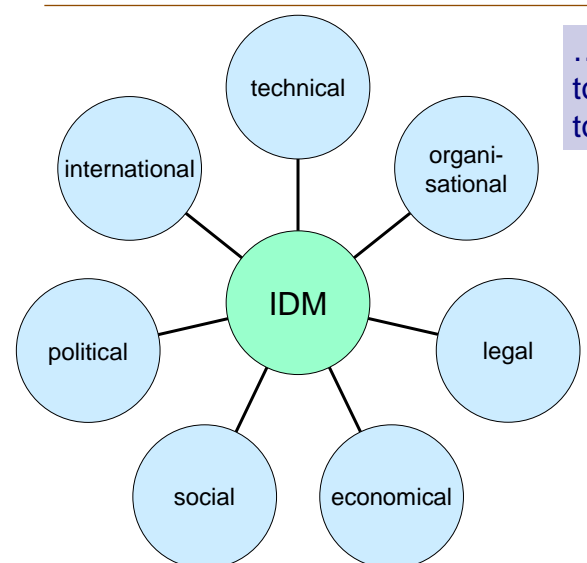
## Identity management

- physical world
- consumer space
- business environment
- e-government
- services and objects



1 July 2010 © K.U.Leuven COSIC, Bart Preneel 39

## Identity management has many dimensions






.... so it's not sufficient to add an "identity layer" to the Internet

40

## Real life: growing number of applications

- financial, e-commerce, e-government, e-health, social networks, airlines, car rental, ...



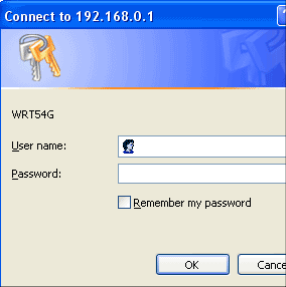
Ordering online is easy.  
We'll walk you through the process, step by step.

Enter your e-mail address:

I am a new customer.  
(You'll create a password later.)
   
 I am a returning customer, and my password is:
   

  
[Forgot your password? Click here](#)



## Changing IT landscape

|      |  | # of applications |
|------|--|-------------------|
| 2005 | <b>Cloud Computing</b><br>RIA's, AJAX, Flash, Silverlight, SaaS, IaaS, PaaS, Virtualization, RSS, Social Media, Wikis, ... | 10000             |
| 2000 | <b>Web Services &amp; SOA</b><br>XML, SOAP, WS - *, REST, ESB, WSM, Java   | 1000              |
| 1995 | <b>Web Applications</b><br>HTTP, HTML, .Net, Java, J2EE, TCP/IP  | 100               |
| 1990 | <b>Client/Server &amp; Distributed Computing</b><br>VB, C++, SmallTalk, ERP, Tuxedo, MQ, DCE, COM, DCOM, Corba             | 10                |
|      | <b>Mainframe/mini</b><br>MVS, Top Secret, RACF, ACF  | 10                |

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

42

## Step 1: centralize (identity 1.0)

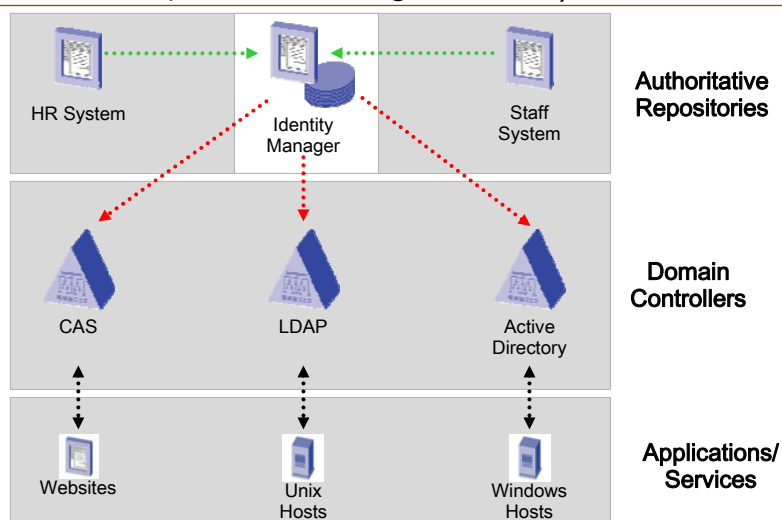
- **integrate** entity authentication
  - but move authorization decision to application and services
- embrace multiple authoritative sources
  - authoritative for attributes, not people
- account names should be ephemeral
  - users should be free to select and change
- dynamic rules, not static roles

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

43

## Integrated identity management (inside one organization)



1 July 2010

© K.U.Leuven COSIC, Bart Preneel

44

## How to grow? Step 2: federate (identity 1.5)

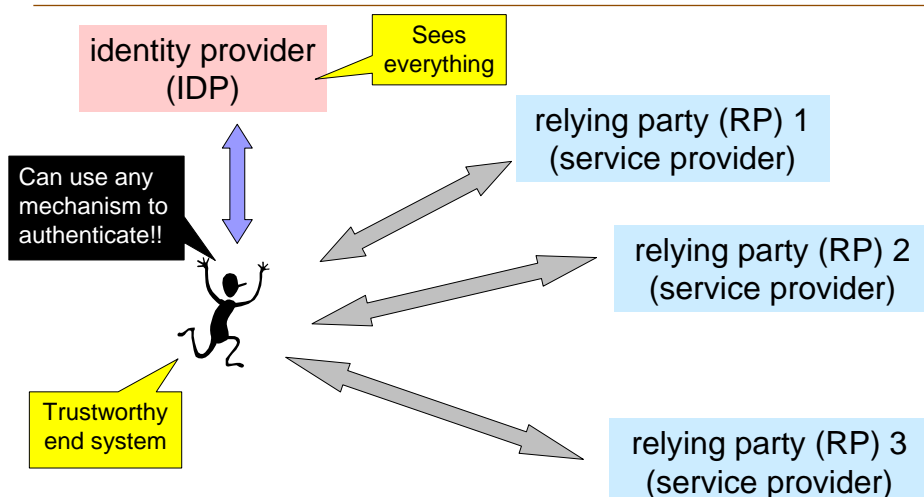
- **federated identity:** credential of an entity that links an entity's partial identity in one **context or trust domain** to an entity's partial identity in another **context or trust domain**
- **note:** can also be used inside an organization for convenience

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

45

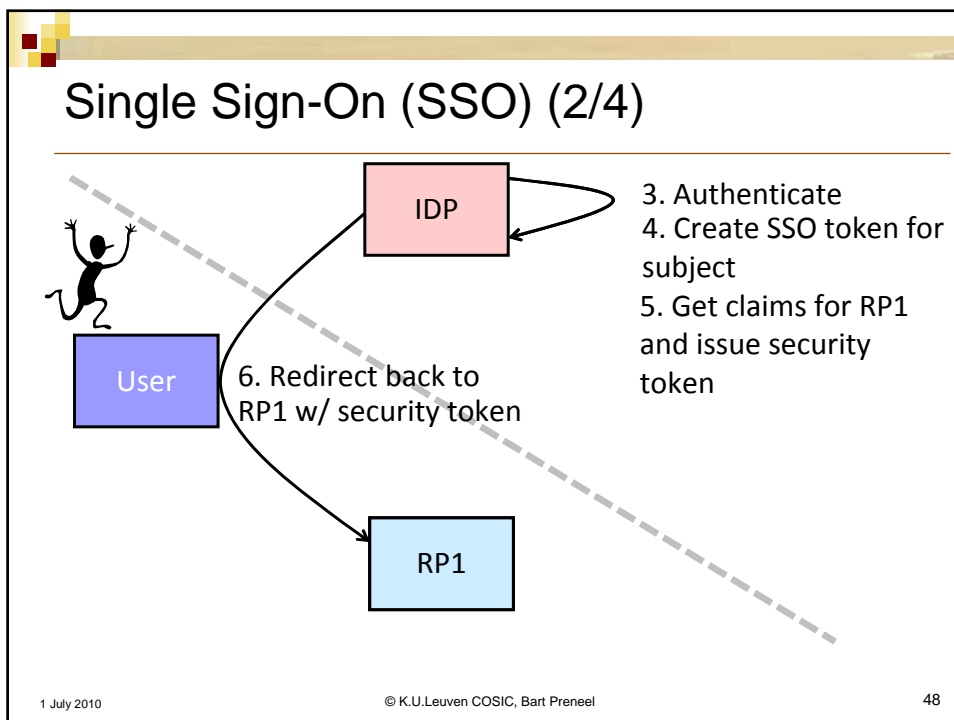
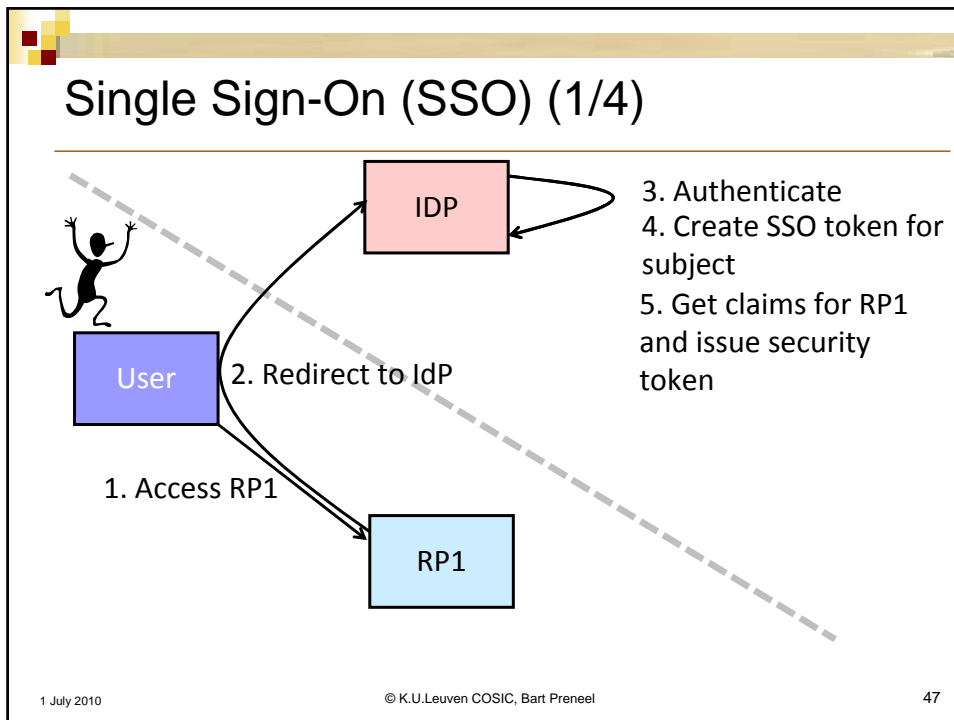
## Single sign on: login only once



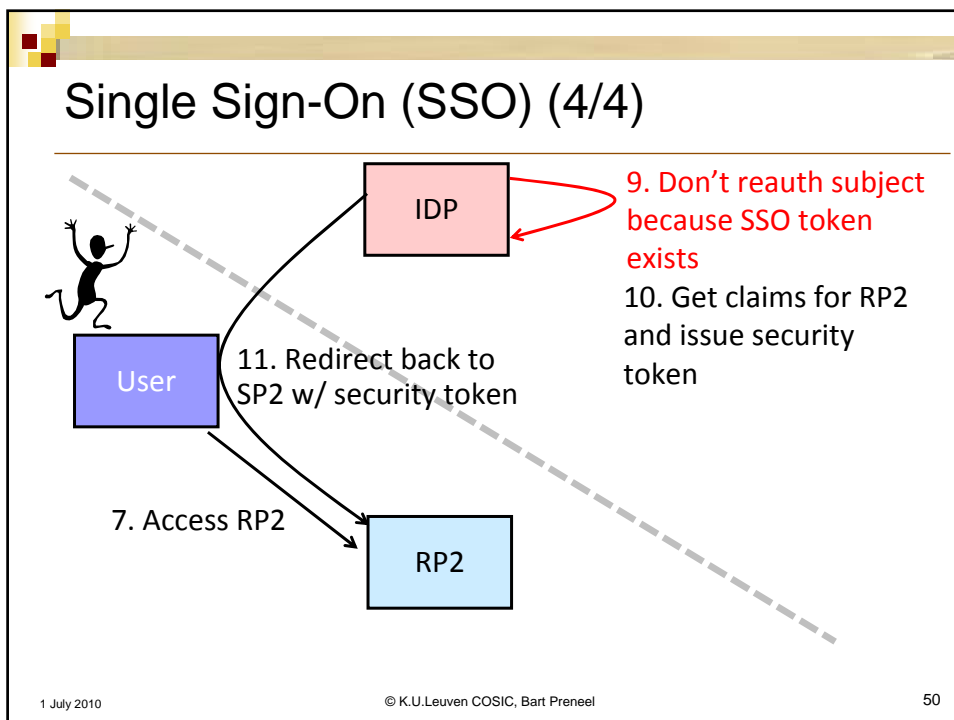
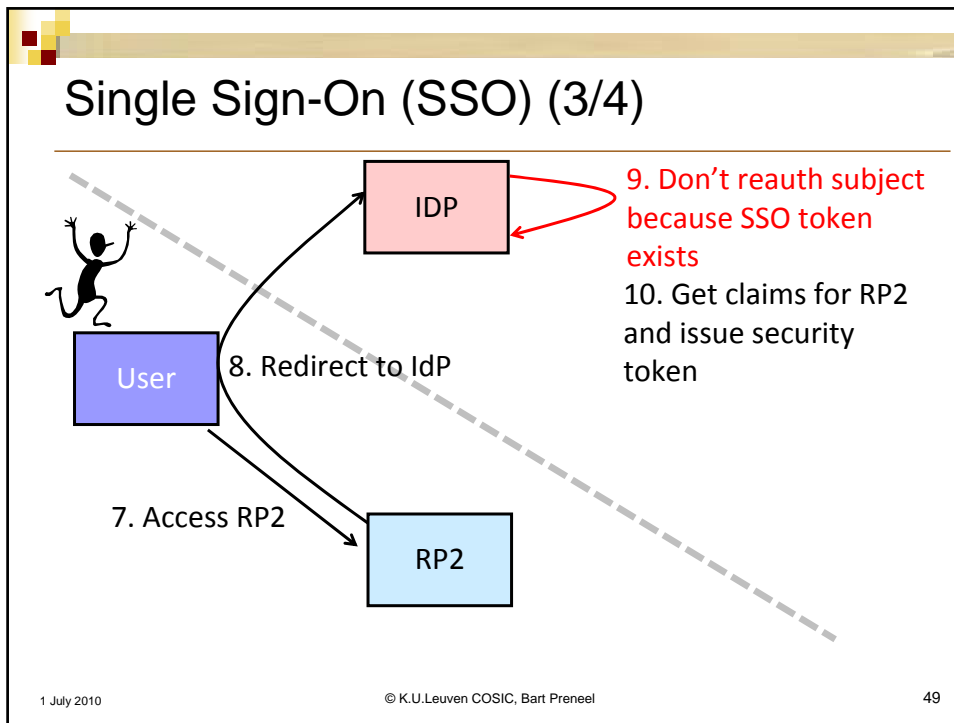
1 July 2010

© K.U.Leuven COSIC, Bart Preneel

46







## Single Sign-On Variants

- initiate contact with IDP or with RP
- access token can be pushed by user to RP or can be pulled by RP from IDP
- token: symmetric versus public key
  - symmetric token: IDP and RP have to share a secret key (example: Kerberos)
  - asymmetric token (digital signature): IDP and RP have to trust a common CA (example: SAML)

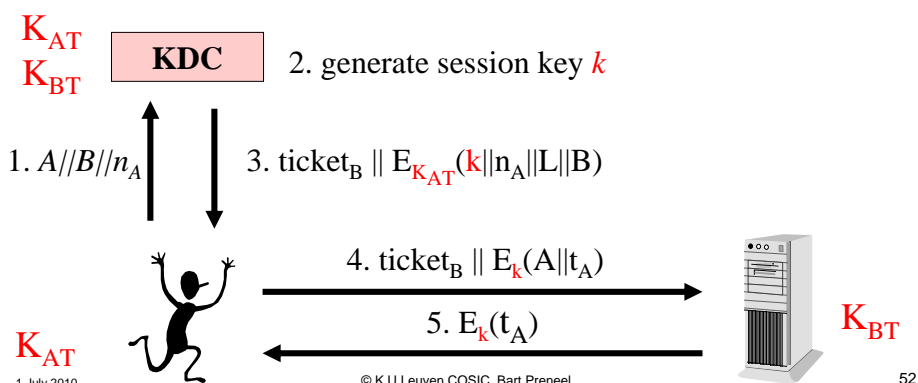
1 July 2010

© K.U.Leuven COSIC, Bart Preneel

51

## Single Sign-on with symmetric keys: Kerberos

- Alice/Bob shares a long term secret with KDC:  $K_{AT}/K_{BT}$
- Alice/Bob/KDC have synchronized clocks
- $\text{ticket}_B = E_{K_{BT}}(k \parallel A \parallel L)$
- L life time of a ticket – limits validity of a key



### Single Sign-on with symmetric keys: Kerberos

- Alice's long term key  $K_{AT}$  is derived from a password  $P$
- Alice stores  $E_{K_{AT}}(k||n_A||L||B)$  on disk for period  $L$  (1 day)
- To avoid one password entry per application: use intermediate server (ticket granting server)

AS: authentication server  
TGS: ticket granting server

1 July 2010 © K.U.Leuven COSIC, Bart Preneel 53

### SAML (Security Assertion Markup Language) (2001)

- OASIS Security Services Technical Committee (SSTC)
- XML-based standard for exchanging authentication and authorization data
  - SAML assertions that describe security tokens representing users
  - SAML bindings: map to standard communication protocol
  - SAML profiles for a single sign-on protocol
- generic but rather complex
- IDP-friendly (e.g., preconfigure large IDP in RPs)
- offers various pseudonyms
- SAML 1.0 (Nov. '02)
- SAML 2.0 (March '05) – incompatible with 1.0/1.1
  - input from Liberty Alliance ID-FF 1.2 but not compatible
  - Profiles: Web browser SSO, WSS-Security, Liberty ID-FF and ID-WSF, XAXML v2.0

1 July 2010 © K.U.Leuven COSIC, Bart Preneel 54

## Single Sign-On

- convenient
- more secure than multiple passwords
- can leverage a single but more secure authentication mechanism
- risk of breach of authentication mechanism is substantially larger
  - is there a single sign-off?
- redirection by RP may facilitate phishing
- IDP is single point of failure
- if RP is contacted first, how does it know which IDP to contact? (the discovery problem)
- privacy risks
  - data sharing: e.g., Facebook or LinkedIn access Gmail email addresses
  - central control of who accesses which services at which time

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

55

The great thing about standards is.....there are so many to choose from!



1 July 2010

© K.U.Leuven COSIC, Bart Preneel

56

## Identity: principles [Kim Cameron, Microsoft, '05] also called "laws"

1. user control and consent
2. minimal disclosure of information for a constrained use
3. disclosure limited to justifiable parties
4. directed identities: omni-directional and uni-directional
5. open – operators and technologies
6. human integration
7. consistent experience across contexts

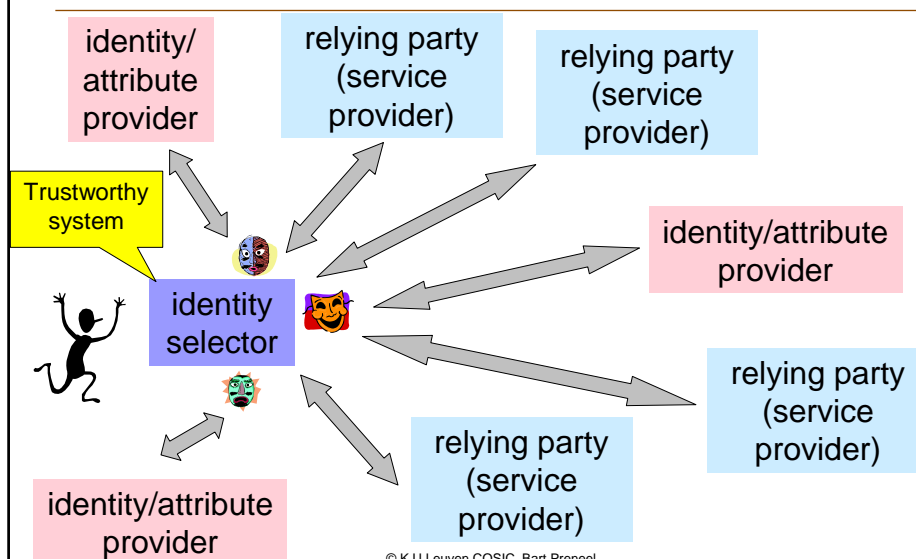
- insightful and though provoking
- dependent on IT context and technology – rather principles than "laws"
- could also be called: the 7 mistakes made by Passport

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

57

## Identity meta-system



© K.U.Leuven COSIC, Bart Preneel

58

## Main issues: "identity 2.0"

- need consistent view for user: **identity selector**
  - essential: mental model and ease of use
- move from enterprise centric to **user-centric** (user in control)
  - no unique definition
  - assuring attributes by proving claims
    - claims: "...an assertion of the truth of something, typically *one which is disputed or in doubt*".
- increased **privacy**
  - can mean many things (cf. supra)

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

59

## Identity selectors

- Microsoft CardSpace (formerly known as InfoCard) [2006]  
<http://cardspace.netfx3.com>
- Eclipse project Higgins: open source browser add-on (plug-in API)
  - Identity agent
  - Identity services
  - Personal data store<http://www.eclipse.org/higgins/index.php>

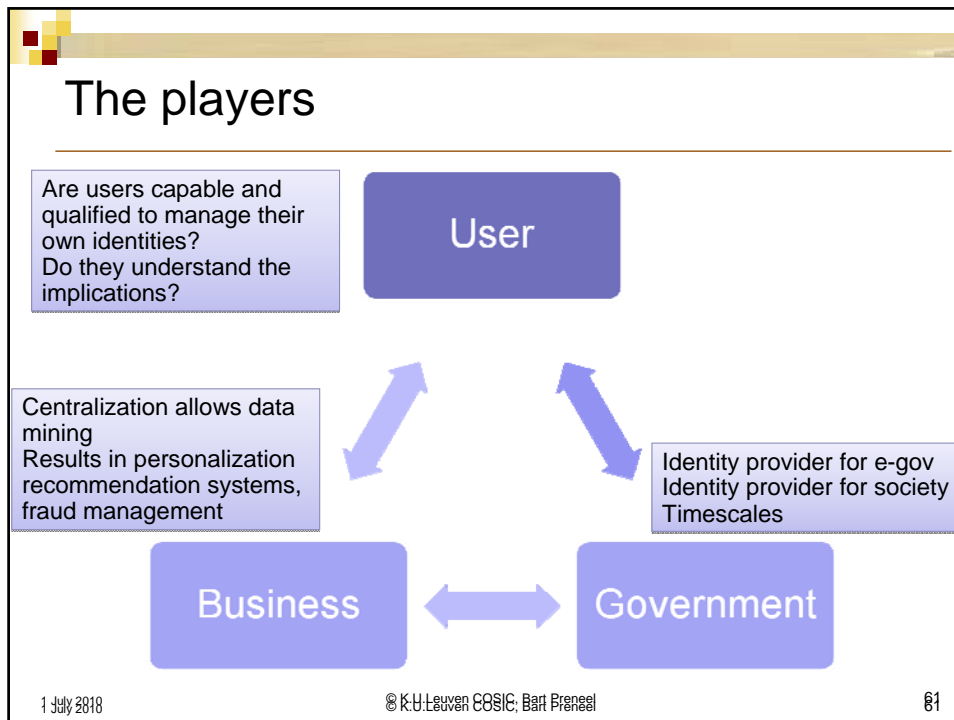


**eclipse**  
an Eclipse project

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

60



## URL-Based Identity Management: OpenID (2005)

Login with your blog URL:  Login  
For example: `happygirl1.bloghost.com`

focus on consumers: Dec. 09: > 1 billion OpenIDs on the Internet,  
9 million sites have integrated OpenID consumer support

providers include AOL, BBC, Google, IBM, Microsoft, MySpace,  
Orange, PayPal, VeriSign, LiveJournal, Yandex, Ustream, Yahoo!

- V 1.0 2005 - V 2.0 2007
- openness is privacy challenge:
  - no agreement needed between RPs and IDPs
  - RPs can correlate information
  - IDP knows which RPs are visited

1 July 2010 © K.U.Leuven COSIC, Bart Preneel 62

## Pros and Cons of URL-Based Identity

- + simple, lightweight and scalable
- + RP friendly
- + user can self-assert attributes and host its own provider
- + uses existing web & browser technologies
  - + easy to adopt: no new software needed
  - + accessible from anywhere
- inconvenient typing of URLs (no IDP discovery by RP)
- open to phishing attacks (because of redirection)
- black and white trust model
- user interface not always consistent
- no SSL required
- can self-asserted claims be trusted?



1 July 2010

© K.U.Leuven COSIC, Bart Preneel

63

## OpenID vs. SAML

- OpenID advantages
  - more open source stacks, i.e. free
  - IDPs can support new RPs without requiring them to register
  - RPs can support new IDPs without registering with them, but may still need a list of ones it trust (or a list from a trusted authority)
  - lighter and more scalable but less focus on security
- SAML advantages
  - higher industry confidence in security details of protocols and existing implementations
  - much larger number of existing E-mail domains have a SAML IDP
  - IDP discovery can be hard
- Conclusions
  - **both can be user-centric and enable direct interactions between IDPs and RPs**
  - SaaS vendors will focus on SAML
  - consumer RP sites will use whatever big IDPs deploy (which happens to be OpenID)
  - longer term the vendors and open source implementations will support both

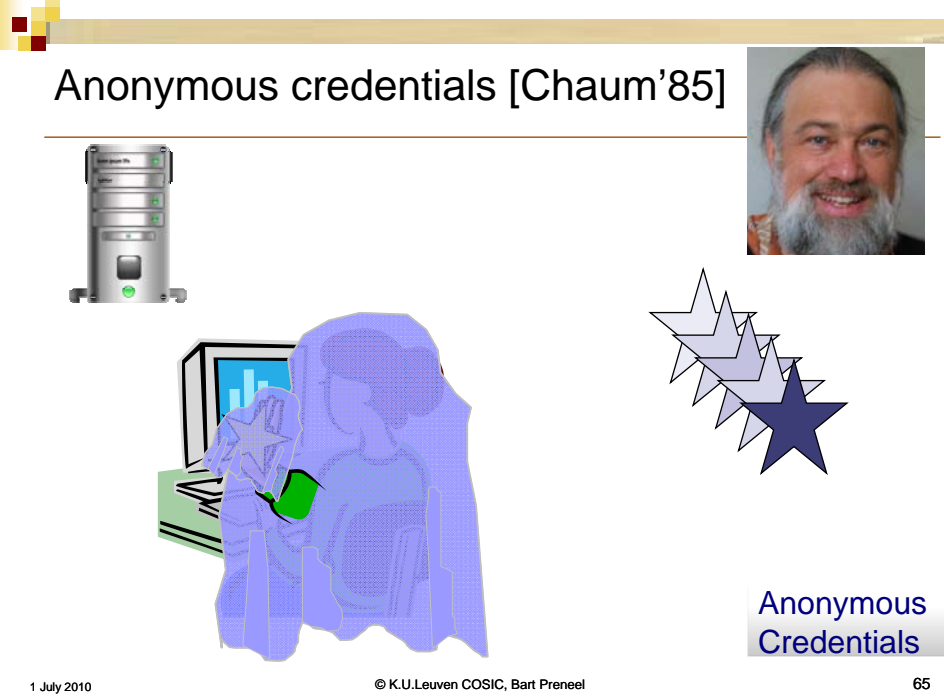
1 July 2010

© K.U.Leuven COSIC, Bart Preneel

64



## Anonymous credentials [Chaum'85]



1 July 2010

© K.U.Leuven COSIC, Bart Preneel

65

## Trends in identity management

- evolution towards further integration and open systems: Kantara Initiative, Identity Commons' Open Source Identity System working group
- integration with mobile phones (SIM/USIM) and eID?
- architecture:
  - more pull than push (since too many applications)
  - user control may be replaced by third party supervision or management
- reputation based mechanisms originating from social networks
- cultural differences very hard to overcome: role of government, banks, credit rating bureaus,...

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

66

## Anonymous communications

- Applications assume that the **communication** channels are secured / maintain privacy properties
  - previous protocols are useless if the adversary can link transactions based on traffic data (e.g., IP/MAC address, IMEI, GPS, browser: <https://panopticlick.eff.org/>)

The diagram illustrates anonymous communications between Alice and Bob. Alice and Bob are represented by vertical rectangles divided into 'App' (yellow) and 'Com' (blue) layers. A dashed line connects the 'App' layers, with icons for a cookie, a notepad, a document, and a mobile phone. A solid line connects the 'Com' layers, passing through a central network represented by a starburst shape. A green line traces a path through the network. A small box labeled 'IP' is positioned near the network. The text 'Alice' and 'Bob' are placed below their respective rectangles.

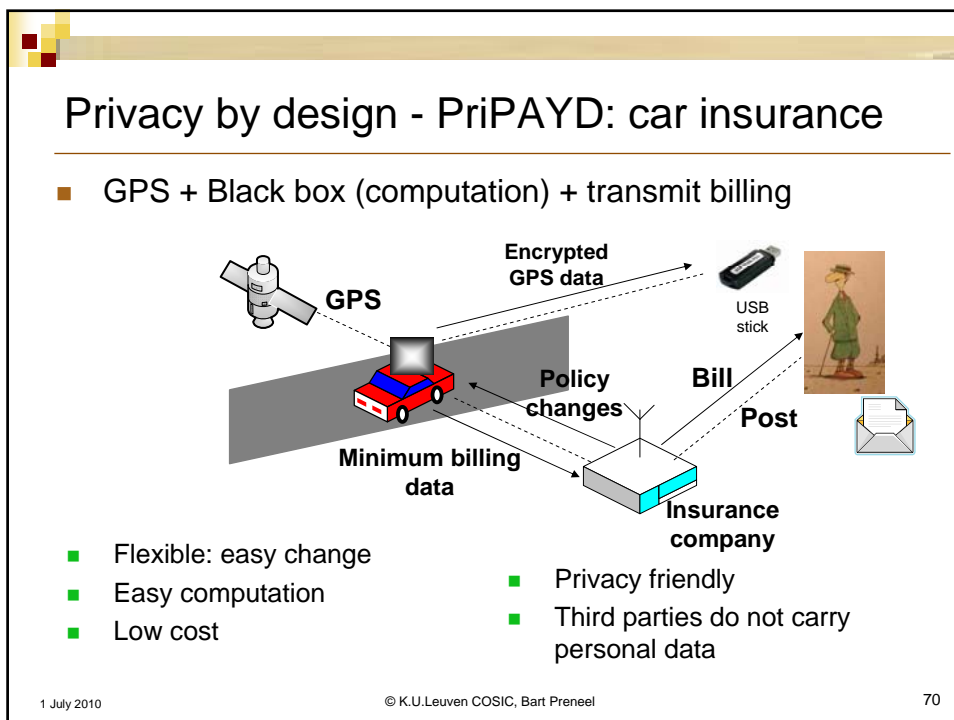
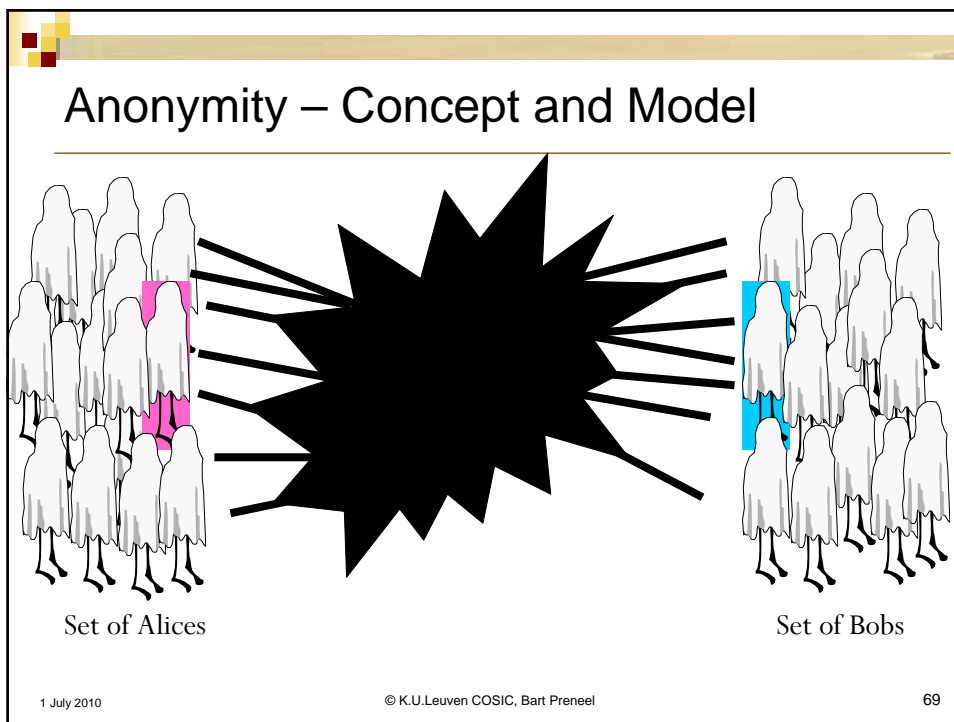
1 July 2010 © K.U.Leuven COSIC, Bart Preneel 67

## Classical communications security model

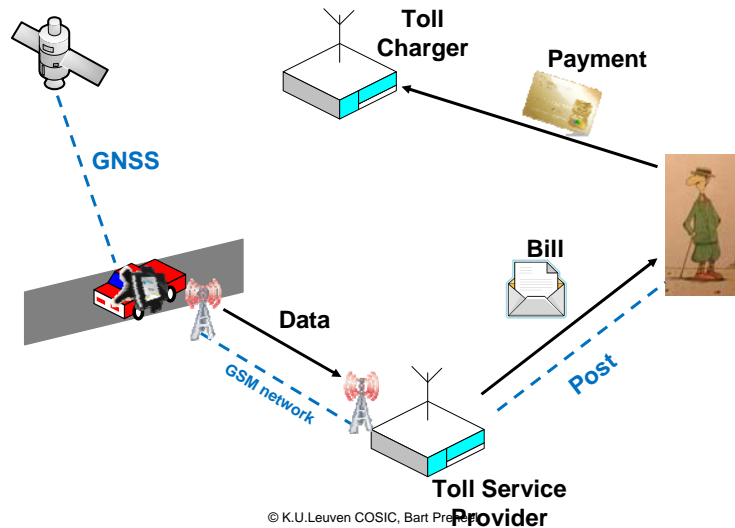
- data confidentiality
- data authentication
- entity authentication
- non repudiation: origin/receipt
- availability

The diagram shows the classical communications security model. Alice (pink stick figure) is on the left, and Bob (blue stick figure) is on the right. A horizontal line represents the communication channel, with an envelope icon above it. Eve (green stick figure) is positioned below the channel, representing an eavesdropper. The text 'Alice', 'Eve', and 'Bob' are placed below their respective figures. The text 'Passive / Active' is centered below Eve.

1 July 2010 © K.U.Leuven COSIC, Bart Preneel 68

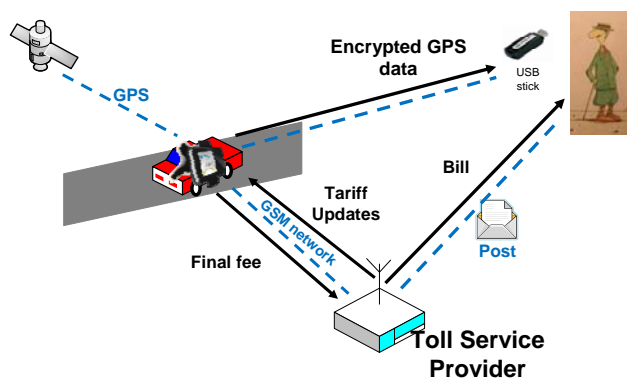


## Road pricing: straightforward implementation



## Privacy-Friendly Electronic Toll Pricing

No personal data leaves the domain of the user



## Cryptography versus privacy

- crypto is success story: 1975-2010
  - from engineering discipline to science (with heuristic assumptions)
  - massive deployment
  - essential building block in IT systems
- even if issues with
  - weak legacy systems
  - long term security (e.g., MD5 story)
  - insecure implementations
  - attacks that bypass cryptography
  - usability

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

73

## Privacy challenges

- privacy requirements and privacy by design
- finding efficient and secure mechanisms
  - complex systems require privacy at every level: the chain is as strong as its weakest link
  - proposed techniques keep getting broken: lack of models and proofs
  - secure implementation is even harder
  - easy to defeat by “changing” abstraction layer
    - cameras, RFID tags, unique device properties, singulation protocols, traffic analysis, ...

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

74

## Privacy and identity management challenges

- usability issues
- economic incentives
- awareness and transparency
- PETs can be misused: conditional privacy
  
- identity management is closely intertwined with our social and economic interactions
- identity management technology is evolving quickly, yet the concepts in our society change only slowly
  - concept of identity will probably evolve
- ease of use and increased profiling has higher importance than data minimization

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

75

## New challenging scenarios

- location privacy
  - real time
  - space-time relation
  - dummy traffic?
- ubiquitous environments
  - constrained devices
  - securing the physical link
- social networks: tension with data sharing
- cloud computing (or is it swamp computing?):  
outsourcing of storage/computations

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

76

## Conclusions (1)

---

- Privacy is not “opposed” to security, but rather a security property
- compliance is a strong driver
  - data Protection
  - US disclosure legislation
- Soft Privacy is the state of the art
  - hidden costs of securing the data silos
- Hard Privacy solutions:
  - active research
  - poor deployment: cost/security benefit

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

77

## Conclusion (2)

---

- security for society will grow
- privacy of individual will erode
- security of individual:?
  - concept of identity will probably evolve
  - need for interdisciplinary research
- impact on organization of society not understood

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

78

## Further reading

---

- W. Diffie, S. Landau, *Privacy on the line. The politics of wiretapping and encryption*, MIT Press, 2<sup>nd</sup> Ed., 2007.
- D.J. Solove, *Understanding Privacy*, Harvard University Press, 2008.
- A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management - a consolidated proposal for terminology", *Technical Report v0.31*, 2008.
- D.J. Solove, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, *San Diego Law Review*, 2007.

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

80

## Further reading

---

- G. Danezis and C. Diaz, "A Survey of Anonymous Communication Channels", Microsoft Technical Report MSR-TR-2008-35, 2008.
- J. Krumm, "A Survey of Computational Location Privacy", *Personal and Ubiquitous Computing*, 2009.
- Privacy Enhancing Technologies proceedings, Lecture Notes in Computer Science
- J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede, "PrETP: Privacy-Preserving Electronic Toll Pricing," *19th USENIX Security Symposium 2010*, 2010.  
<https://www.cosic.esat.kuleuven.be/publications/article-1408.pdf>

1 July 2010

© K.U.Leuven COSIC, Bart Preneel

81