



An example of a strategic privacy technology and implications for policy

Caspar Bowden

Chief Privacy Adviser, Microsoft EMEA

9th December 2008

Future of the Internet - Madrid



Privacy vs. Security ?

“Everybody knows” :

- to get authorized to access a system a person must disclose their identity ?
 - ...but suppose that's not true
- the accepted principles of privacy protection are technology-neutral
 - ...but perhaps some technologies are intrinsically better for privacy than others
- cyber-security and privacy is a tradeoff
 - ...but perhaps both can be improved together

The trouble with PKI (“public-key infrastructure”)

- “certificate” contains identity attributes
 - verifiable by a digital signature
- must disclose entire certificate in order for verification mechanism to work
 -results in disclosure of “excessive” data for any particular transaction
- Cert ID is inescapable persistent identifier
 - “Too bad!” - just the way the maths works
- Well, no...can do (much) better
 - 20 years of research into “multi-party” security and privacy techniques

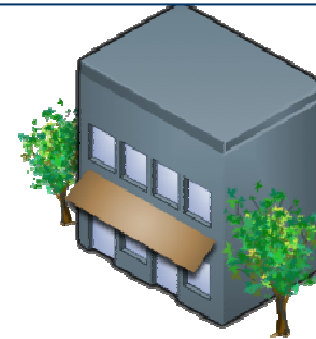
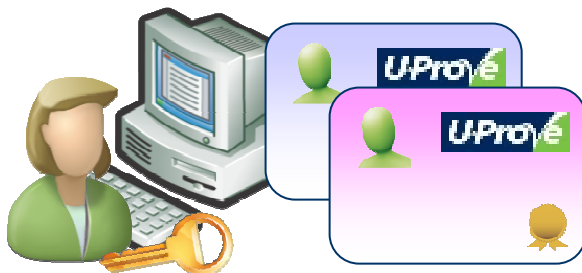
Minimal disclosure tokens



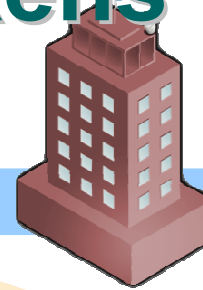
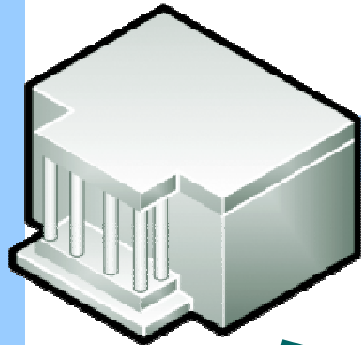
Name: Alice Smith
Address: 1234 Crypto, Seattle, WA
Status: gold customer



DOB: 03-25-1976
Reputation: high
Gender: female



Minimal disclosure tokens



Prove that you
are from WA
and over 21

Which adult
from WA is
this?

U-Prove

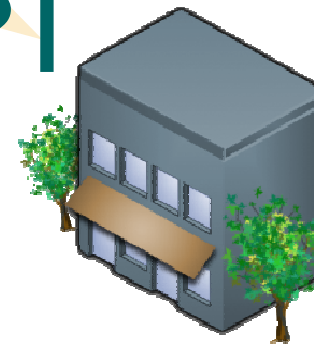
Name: _____
Address: _____
Status: _____

U-Prove

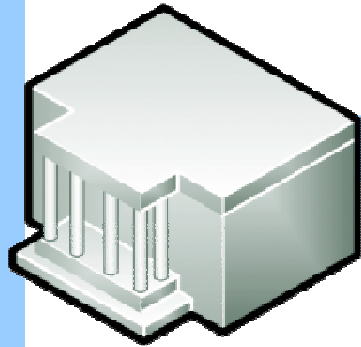
DOB: _____
Reputation: _____
Gender: _____

U-Prove

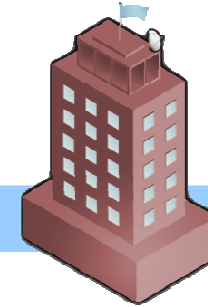
21 proof



Authentication ≠ Identification



Prove that you
are a gold
customer



U-Prove

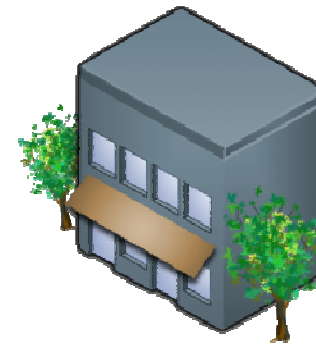
Name:



Address:



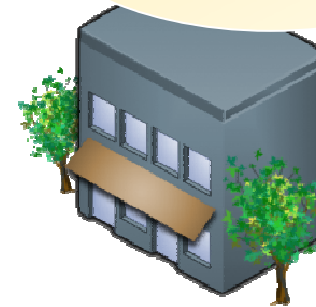
Status: gold customer



Privacy-friendly revocation



Prove that you
are a gold
customer



Name: **not revoked proof**
Address: **[REDACTED]**
Status: gold customer



Applications

- Avoid unnecessary (“excessive”) data trails in transactional systems
 - Access services based on proof-of-age-limits, or class of entitlement
 - reduce liabilities, exposure to breaches / insider-attacks
 - safe private-sector use of data in national eID systems
- Verifiable audit trails
 - can show different parts of trail to different parties according to need-to-know
- Apply different policies to different risks
 - revocable tokens which preserve privacy
- These capabilities are counter-intuitive !



Evolution of law and technology

- 1970s – 1st Data Protection laws, Fair Information Practices
 - ...invention of asymmetric cryptography
- 1980s – Council of Europe 108, OECD principles
 - ...invention of concept of cryptographic “blinding”
- 1990s – EU Data Protection, US-EU Safe Harbor
 - PKI standards, Digital Signature laws
 - ...refinement of “blinding”, fraud-control techniques
- 2000s – APEC, security breach notification laws
 - federated identity system architecture
 - ...rich family of “multi-party” security/privacy techniques
- 2010s - is the law still technology-neutral ?
 - What does personal information mean ?
 - What does data minimisation mean ?
 - What does identifiable mean ?

A dialogue between policy and technology

- “de-identification” doesn’t really work
- Advances in re-identification algorithms are undermining distinctions between personal and non-personal data
 - (e.g. Shmatikov – PETS Award winner 2008)
- Profiles based on “anonymous” data result in people being treated differently – but with no transparency ?
- What to do....
 - continue legal fiction of effective remedies and tech neutrality
 - ...or perhaps can reinterpret privacy principles ?
- Three ideas:
 1. Regulate the application of re-identification and profiling
 2. Consider the specific legal grounds when justifiable for a system to “recognize” a person without their consent
 3. Build systems around concept of individual access

Fundamental legal and policy issue

- Systems increasingly collect transactional data identifiably – and disproportionately (various Art.29 WP Opinions)
 - “side-effect” is that a database of all transactions is retained (e.g. for retrospective fraud tracing), but can the database be used for surveillance purposes as a “free by-product” ?
 - (also remember CoE R.87 requires specific law authorizing blanket collection....)
- Art.8 of ECHR:
 - state should limit intrusions into privacy to that which is necessary, **if possible** case-by-case according to the circumstances of the individual (and according to law, foreseeability etc.)
- Use of certain strategic PET techniques is **mandatory** under ECHR (subject to reasonable feasibility), because it infringes privacy **only to an extent that is individually proportionate**.
 - “balancing” with positive obligations of ECHR Art.2 (“right to life”) ?
 - Osman vs. UK 1998 : “**real and immediate risk to life of an identified individual or individuals from the criminal acts of third parties.**” => there is no “free pass” for surveillance systems

“Strategic” PETs in a legal framework

● Strategic PETs

- improve both privacy and cyber-security
- have to be designed into the whole system
- are “conceptually generic” – only realistic option
 - Others:
 - ? “Differential Privacy” in statistical databases
 - ? Transport-layer identifiability (e.g. ToR)

● Consider phase-in timelines

- public-sector lead by example ?
 - EU Commission Communication 20.9.03
 - Procurement guidelines referencing strong data minimization, unlinkability as basic capability ?