The Nexus of Identity

IBM's submission for the W3C “Identity in the Browser” Workshop

by Maryann Hondo, Mary Ellen Zurko, Matthew Flaherty,
Paula K. Austel, Sridhar Muppidi

Net - net of the paper

Our customers expect us to give them the ability to adjust the transparency knob
Based on their use case and to be able to control what users do
I’ve been sitting in the back, not saying anything
Because trying to represent an aggregate answer from IBM is “yes”….to everything

Whatever we can do to improve the usability, the scalability
the security
Lets do it.

Since More, better, faster is the way of the internet
We need to be adaptive,
Look for optimizations and get out of the way
In addition to our “base” products that deal with identity and identity services (Tivoli Identity products, Lotus collaboration software WebSphere Application Servers)…… we also have products & services that mitigate threats, track vulnerabilities, and offer risk based policy and access.
My particular interest ....

Mobile applications ....

What would a well behaved mobile web application look like?

And what expectations should users have with regard to trust and privacy

I’m less concerned with what it is, than being able to tell that it is one [I’m optimistic that we can improve this over time]
Our Vision

In the Information Society, users can act and interact in a **safe and secure** way while **retaining** control of their private spheres.
Research topics presented at RSA

IBM Identity Mixer

A flexible cryptographic framework

Paradigm Shift in Access Control

European Projects to make this real
Research Perspective

• One can prove statements such as “I'm between 12-15 years old” using an electronic ID without revealing any data stored in the eID such as name, address or birthdate

• Technology can be used with today's Smartcards

• Identity Mixer is a framework that addresses all requirements of privacy-protecting PKI

• Paradigm shift in authentication: Who are you vs. these are the properties required for access
Identity Mixer: Framework

Policy Layer

Crypto Token Layer

Composed schemes
- Minimal disclosure tokens
- Group signatures
- Direct Anonymous attestation
- Limited-use tokens
- ...

Building blocks
- Commitments
- Signatures on lists of messages
- Verifiable Encryption
- Verifiable Random Functions
- Revocation

Instantiations
- U-Prove signatures
- CL signatures

Efficient zero-knowledge proofs

Identity Mixer Core
Resources

• PrimeLife: www.Primelife.eu

• Identity Mixer:
  – idemix.wordpress.com

• Contacts:
  – Andreas Wespi: anw@zurich.ibm.com
  – Jan Camenisch: jca@zurich.ibm.com