IBM Identity Mixer
Authentication without identification

Jan Camenisch, Maria Dubovitskaya, Peter Kalambet, Anja Lehmann, Gregory Neven, Franz-Stefan Preiss, Timur Usatiy

IBM Research – Zurich
idemix@zurich.ibm.com
33% of cyber crimes, including identity theft, take less time than to make a cup of coffee.
10 Years ago your personal data on the black market was worth $150. Today....
Houston, we have a problem!
Houston, we have a problem!

“Buzz Aldrin's footprints are still up there”
(Robin Wilton)
Computers don't forget

- Data storage ever cheaper → “store by default”
  - also collateral collection, surveillance cameras, Google Street View with wireless traffic, Apple location history,…

- Data mining ever better
  - self-training algorithms cleverer than their designers
  - not just trend detection, even prediction, e.g., flu pandemics, ad clicks, purchases,…
  - what about health insurance, criminal behavior?

- The world as we know it
  - Humans forget most things too quickly
  - Paper collects dust in drawers

We build apps with the paper-based world in mind :-(
  - if it works it works
  - security too often still an afterthought
  - implementors too often have no crypto education
... “I have nothing to hide!”
... “The intelligence agencies have all my data anyway”

- Huge security problem!
  - Millions of hacked passwords (100,000 followers $115 - 2013)

- Difficult to put figures down
  - Credit card fraud
  - Spam & marketing
  - Manipulating stock ratings, etc..
  - (Industrial) espionage

- We know that 3 letter orgs can do it easily, but they are not the only ones
  - however, this is not about homeland security
  - and of course there are limits to the degree of protection that one can achieve

- Last but not least: data are the new money, so they need to be protected!
Privacy is not a lost cause!

we need paradigm shift &
build stuff for the moon
rather than the sandy beach!
IBM Identity Mixer
The paradigm shift for authentication
Alice wants to watch a movie at Movie Streaming Service

I wish to see Alice in Wonderland
Alice wants to watch a movie at Movie Streaming Service

You need:
- subscription
- be older than 12
Watching the movie with the traditional solution

Using digital equivalent of paper world, e.g., with X.509 Certificates

ok, here's
- my eID
- my subscription

Alice

Movie Streaming Service
Watching the movie with the traditional solution

...with X.509 Certificates

Aha, you are
- Alice Doe
- born on Dec 12, 1975
- 7 Waterdrive
- CH 8003 Zurich
- Married
- Expires Aug 4, 2018

Mplex Customer
- #1029347
- Premium Subscription
- Expires Jan 13, 2016

Movie Streaming Service
This is a privacy and security problem!
- identity theft
- discrimination
- profiling, possibly in connection with other services
Watching the movie with the traditional solution

With OpenID and similar solution, e.g.,
log-in with Facebook

ok, I'm Alice@facebook.com

Alice

Movie Streaming Service
Watching the movie with the traditional solution

With OpenID and similar solution, e.g., log-in with Facebook

Aha, Alice is watching a 12+ movie
Watching the movie with the traditional solution

With OpenID and similar solution, e.g., log-in with Facebook

Aha, Alice is watching a 12+ movie

Aha, you are
- Alice@facebook.com
- 12+
Mplex Customer
- #1029347
- Premium Subscription
- Expires Jan 13, 2016

Movie Streaming Service
Identity Mixer solves this.

When Alice authenticates to the Movie Streaming Service with Identity Mixer, all the services learns is that Alice

    has a subscription

    is older than 12

and no more!
Users' Keys:

- One secret Identity (secret key)
- Many Public Pseudonyms (public keys)
Privacy-protecting authentication with Privacy ABCs

Certified attributes from Identity provider

- Issuing a credential

Name = Alice Doe
Birth date = April 3, 1997
Alice

I wish to see Alice in Wonderland

You need:
- subscription
- be older than 12

Movie Streaming Service
Privacy-protecting authentication with Privacy ABCs

Alice

Movie Streaming Service
Privacy-protecting authentication with Privacy ABCs

Alice

Movie Streaming Service
Privacy-protecting authentication with Privacy ABCs

Alice

I wish to see Alice in Wonderland

You need:
- subscription
- be older than 12

Movie Streaming Service

Concept: presentation policy
Proving identity claims

- but does not send credential
- only minimal disclosure
Privacy-protecting authentication with Privacy ABCs

Proving identity claims
- but does not send credential
- only minimal disclosure

Aha, you are
- older than 12
- have a subscription

Movie Streaming Service

(Public Verification Key of issuer)
Proving Identity Claims: Minimal Disclosure

Alice Doe
Dec 12, 1998
Hauptstr. 7, Zurich
CH
single
Exp. Aug 4, 2018

verified ID

Age: 12+
Exp. Valid

verified ID
So, let's watch a movie! – Try for yourself w/ Web-based Demo

idemixdemo.mybluemix.net
idemixdemo.zurich.ibm.com
Identity Mixer Not Only Benefits Consumers

Identity Mixer eliminates the need for retailers and other service providers from collecting the data in the first place.

- Less storage costs,
- less security costs and
- Less public apologies.
Coming to Mobile soon: iOS and Android

Similar to the Wallet App in iOS

- users will have different cards or credentials with each piece personal information

- you would only show what you want, nothing else.
Available as Open Source

Available in GitHub.

https://github.com/p2abcengine/p2abcengine
Easy to integrate into your app with IBM Bluemix

Identity Mixer as a service on Bluemix.

Easy to set up and integrate:
In Bluemix developers simply choose what data they don’t want to collect and a piece of code is available to copy and paste.
Identity Mixer in the Cloud
An Authentication Service on Bluemix
IBM Bluemix is a cloud platform as a service (PaaS)

- **Build & Run Apps in the Cloud**
  - Build, run, deploy, scale, manage, monitor
  - Java, Node.js, Python, PHP, etc.
  - You provides application. IBM runs it.
  - Pay only for what you really need

- **Use Services & APIs**
  - Watson, Mobile, Data, Analytics, etc.
  - New in Security: **Identity Mixer**
Identity Mixer is freely available on GitHub 😊
Integration is involved and time consuming 😞
Our Bluemix service fixes this 😊

- Act as Issuer
  - Define credential specification
- Or as Verifier
  - Define access policy

Get up and running within minutes with our template applications
Identity Mixer service

Issuer as a service

Verifier as a service

Credential Wallet
Getting example Issuer up and running

1. Bind Identity Mixer service to your Bluemix App
2. Define **credential specification with a GUI** (or use ready-made example)
3. Copy a code snippet

4. Duplicate template issuer (Open Source Software) on Bluemix DevOps
5. Paste the code snippet into duplicated application
6. Update deployment info and deploy to Bluemix

Done.
Getting an Issuer up and running
Getting example Verifier up and running

1. Bind Identity Mixer service to your Bluemix App

2. Define **access policy with a GUI** (or use ready-made example)

3. Copy a code snippet

4. Duplicate template verifier (Open Source Software) on Bluemix DevOps

5. Paste the code snippet into duplicated application

6. Update deployment info and deploy to Bluemix

Done.
Getting a Verifier up and running

Verifier Configuration: Create Access Policies

Policies

Add New Policy: Create New Policy

Policy: Over 16 according to eGov ID

Issuer: eGovernment
Credential Type: ID card
Attribute Type: Date of
Operator: <=
Constant: choose constant
now
now - 18 years
now - 16 years

ADD PREDICATE
Here's what the verifier has to paste into his app:

```json
{
    "issuer_data": null,
    "verifier_data": [
        {
            "uid": "idmx:bluemix://idmx-directory.mybluemix.net/policies?type=presentation,
                        name=you_are_older_than_16,
                        version=1",
            "friendlyName": "You are older than 16"
        }
    ]
}
```
Identity Mixer status

- Scientific foundation laid 15 years ago, well studied & award winning
- Successful real-world pilots in series of EU projects

- You can have identity mixer, too!
  - Open-source implementation: https://github.com/p2abcengine
  - Idemix-as-a-Service on IBM Bluemix
  - Web-based demo to try for everyone
  - Coming soon: Idemix on mobile
Extended Features
If car is damaged: ID with insurance or gov't needs be retrieved

Similarly: verifiably encrypt any certified attribute (*optional*)

TTP is off-line & can be distributed to lessen trust
If Alice was speeding, license needs to be revoked!

There are many different use cases and many solutions

• Variants of CRL work (using crypto to maintain anonymity)
  • Accumulators
  • Signing entries & Proof, ....
• Limited validity – certs need to be updated
• ... For proving age, a revoked driver's license still works
Degree of anonymity can be limited:

- If Alice and Eve are on-line at the same time, they are caught!

- Use Limitation – anonymous until:
  - If Alice used certs > 100 times total...
  - ... or > 10'000 times with Bob

- Alice's cert can be bound to hardware token (e.g., TPM)
Some Use Cases
Age verification

Proving 12+, 18+, 21+ without disclosing the exact date of birth – privacy and compliance with age-related legislation

- Movie streaming services
- Gaming industry
- Online gambling platforms
- Dating websites
- Social benefits for young/old people
Who accesses *which data* at which time can reveal sensitive information about the users (their research strategy, location, habits, etc.)

- Patent databases
- DNA databases
- News/Journals/Magazines
- Transportation: tickets, toll roads
- Loyalty programs
Anonymous consultations with specialists
- online chat with a psychologist
- online consultation with IBM Watson

1. Alice proves she has insurance
2. Alice describes symptoms
3. Alice gets credential that she is allowed to get treatment

4. Alice gets treatment from physician, hospital, etc
5. Alice sends bill to insurance and proves that she had gotten the necessary permission for the treatment.
Payment Use Case

- Credential = Bank note
- Double spending need to be prevented/detected
  - On-line or Off-line modi possible
- Money laundering can also be taken care of
Securing Credit Card Payments

The credit card data is never revealed to the merchant, only to the credit card provider

- Bank issues a classic credit card
- User registers at a special portal to obtain the Identity Mixer credential
- User derives a token allowing that store to withdraw the money
- Users cannot be linked across purchases/shops
- Stored credit card info useless to hackers!
Polls, recommendation platforms

Providing anonymous, but at the same time legitimate feedback

- Online polls
  - applying different restrictions on the poll participants: location, citizenship

- Rating and feedback platforms
  - anonymous feedback for a course only from the students who attended it
  - wikis
  - recommendation platforms
Thank you!

- eMail: idemix@zurich.ibm.com
- twitter: @IdentityMixer
- Links:
  - www.zurich.ibm.com/idemix
  - idemixdemo.zurich.ibm.com
  - www.abc4trust.eu
  - www.futureID.eu
  - www.au2eu.eu
  - www.PrimeLife.eu
  - github.com/p2abcengine & abc4trust.eu/idemix
  - console.ng.bluemix.net/catalog/services/ibm-identity-mixer/