

Introduction – Demo – Use Cases – Features Overview – Deployment

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



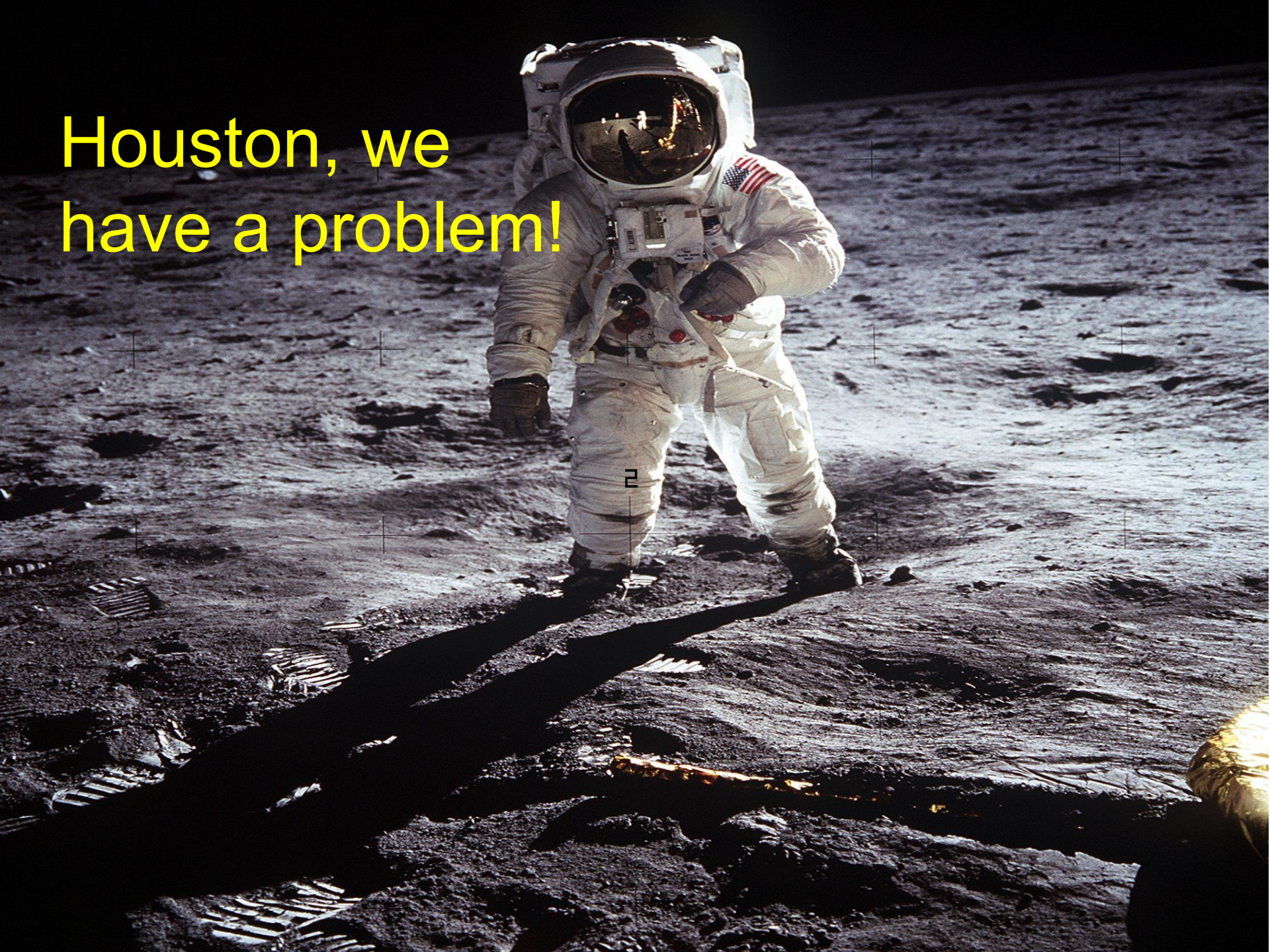
33% of cyber crimes, including identity theft, take less time than to make a cup of coffee.



10 Years ago your personal data on the black market was worth \$150. Today....



Houston, we
have a problem!



A full-page photograph of astronaut Buzz Aldrin on the Moon. He is wearing a white spacesuit with an American flag patch on the right shoulder and is standing on the dark, cratered lunar surface. His shadow is cast long and dark to his left. The background shows the horizon of the Moon under a black sky.

Houston, we
have a problem!

“Buzz Aldrin's footprints are still up there”
(Robin Wilton)



- 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)
- Stolen identities (\$150 - 2005, \$15 - 2009, \$5 – 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



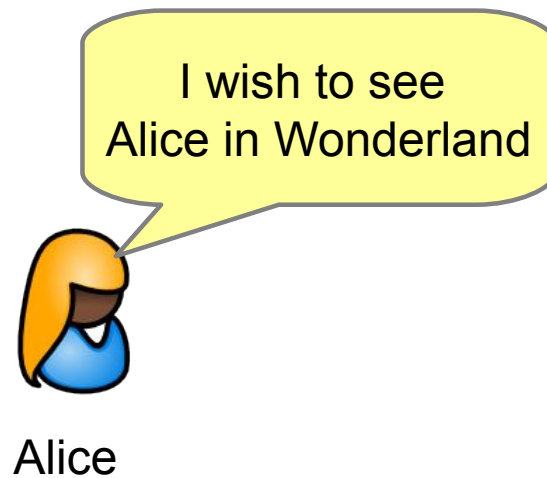
- Last but not least: data are the new money, so they need to be protected!

we need paradigm shift &
build stuff for the moon
rather than the sandy beach!

A wooden crate, possibly containing books or documents, sits on a rough, rocky, and uneven ground. The crate is made of light-colored wood and has a dark, possibly black, material covering the bottom. The background is a textured, greyish-brown surface.

IBM Identity Mixer

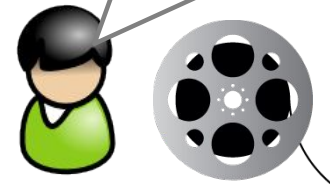
The paradigm shift for authentication





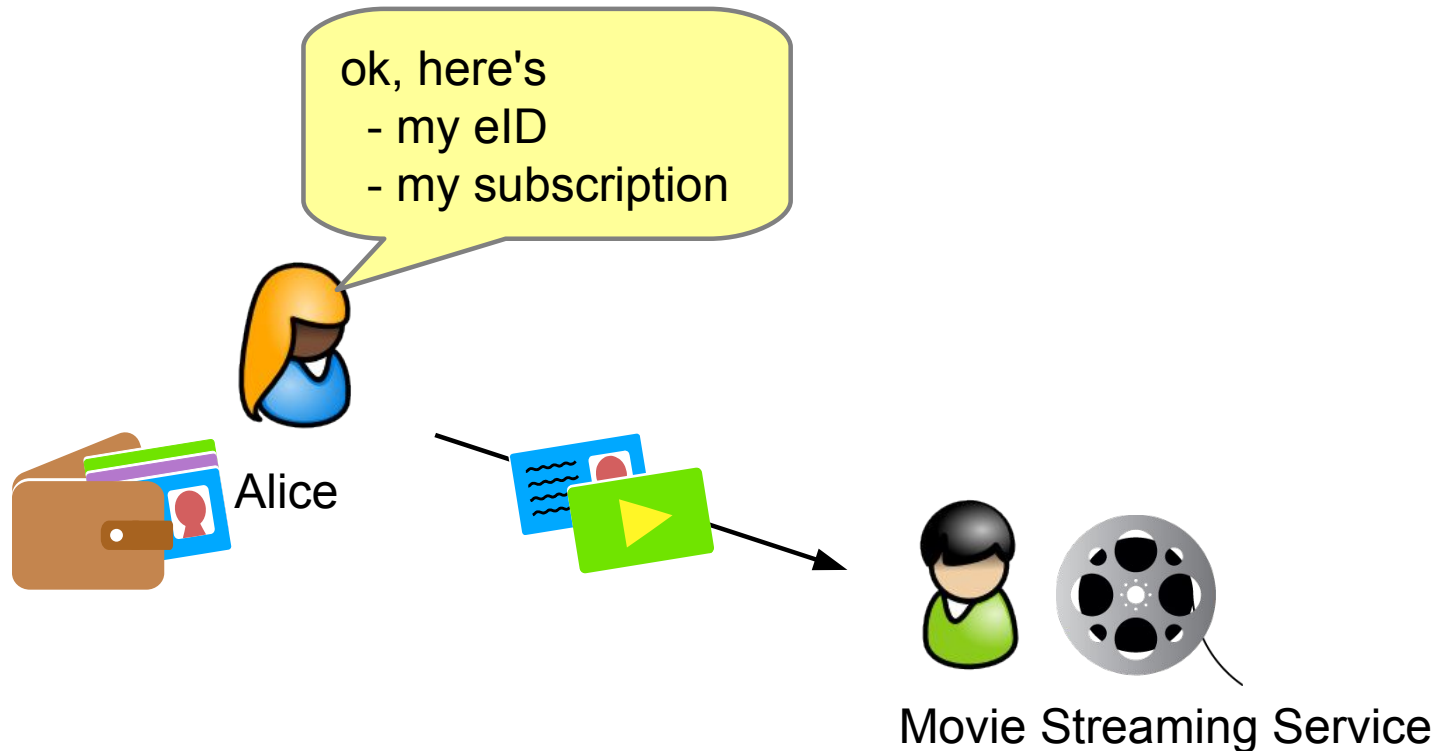
Alice

You need:
- subscription
- be older than 12

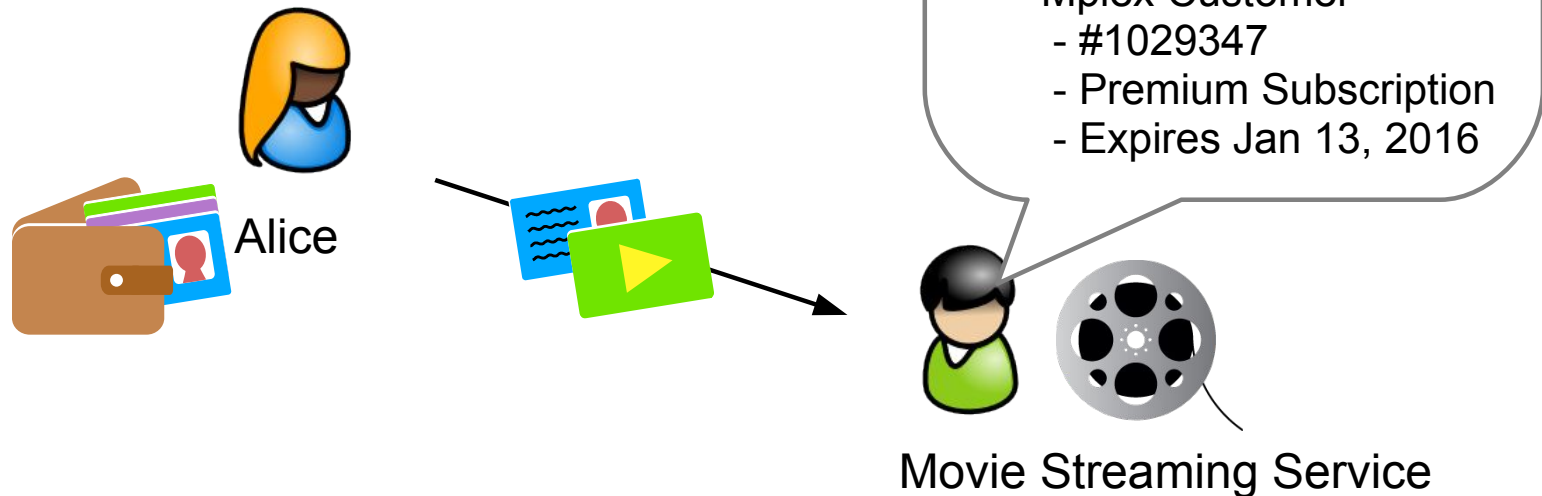


Movie Streaming Service

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

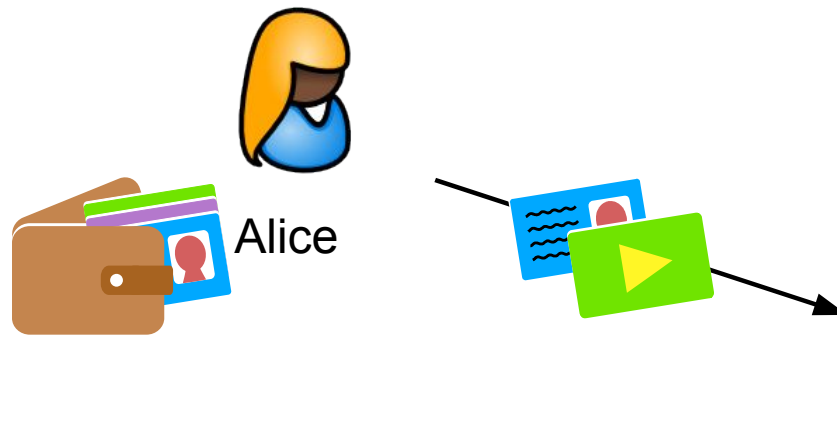


...with X.509 Certificates



This is a privacy and security problem!

- identity theft
- discrimination
- profiling, possibly in connection with other services



Aha, you are

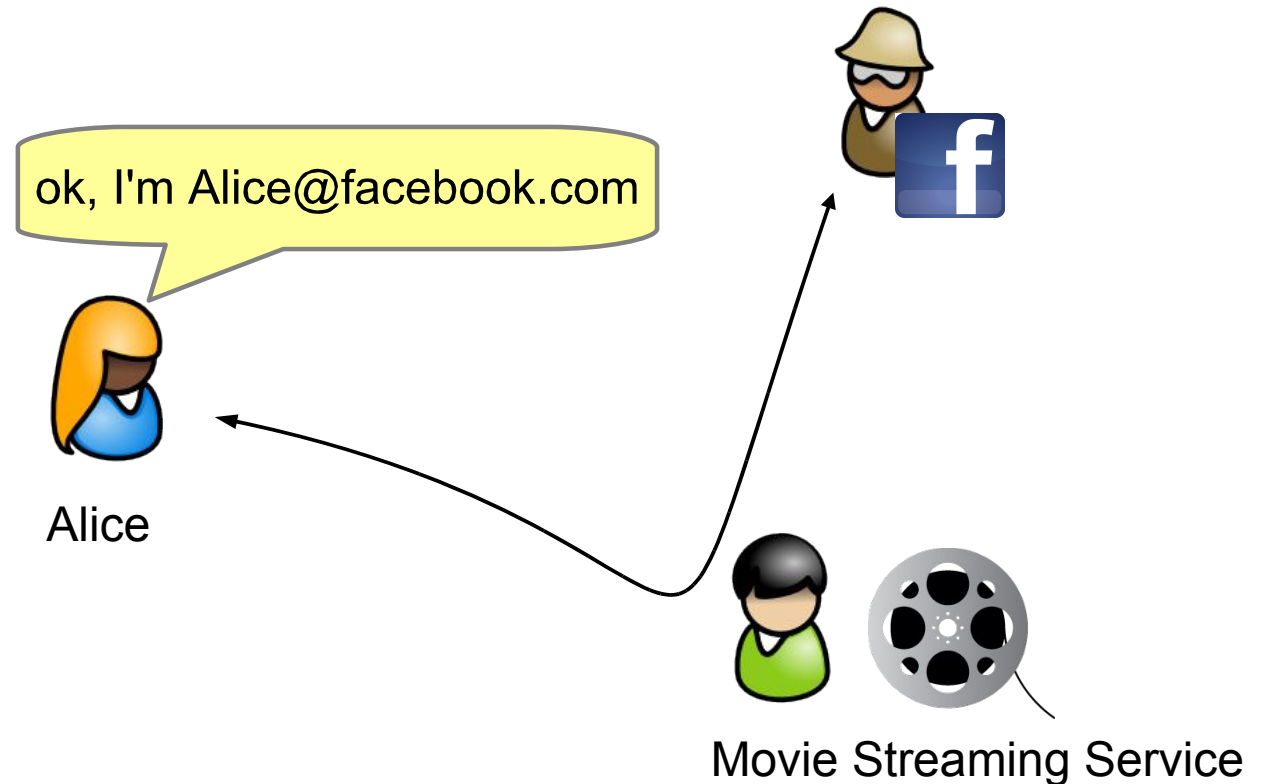
- Alice Doe
- born on Dec 12, 1975
- 7 Waterdrive
- CH 8003 Zurich
- Married
- Expires Aug 4, 2018

Mplex Customer

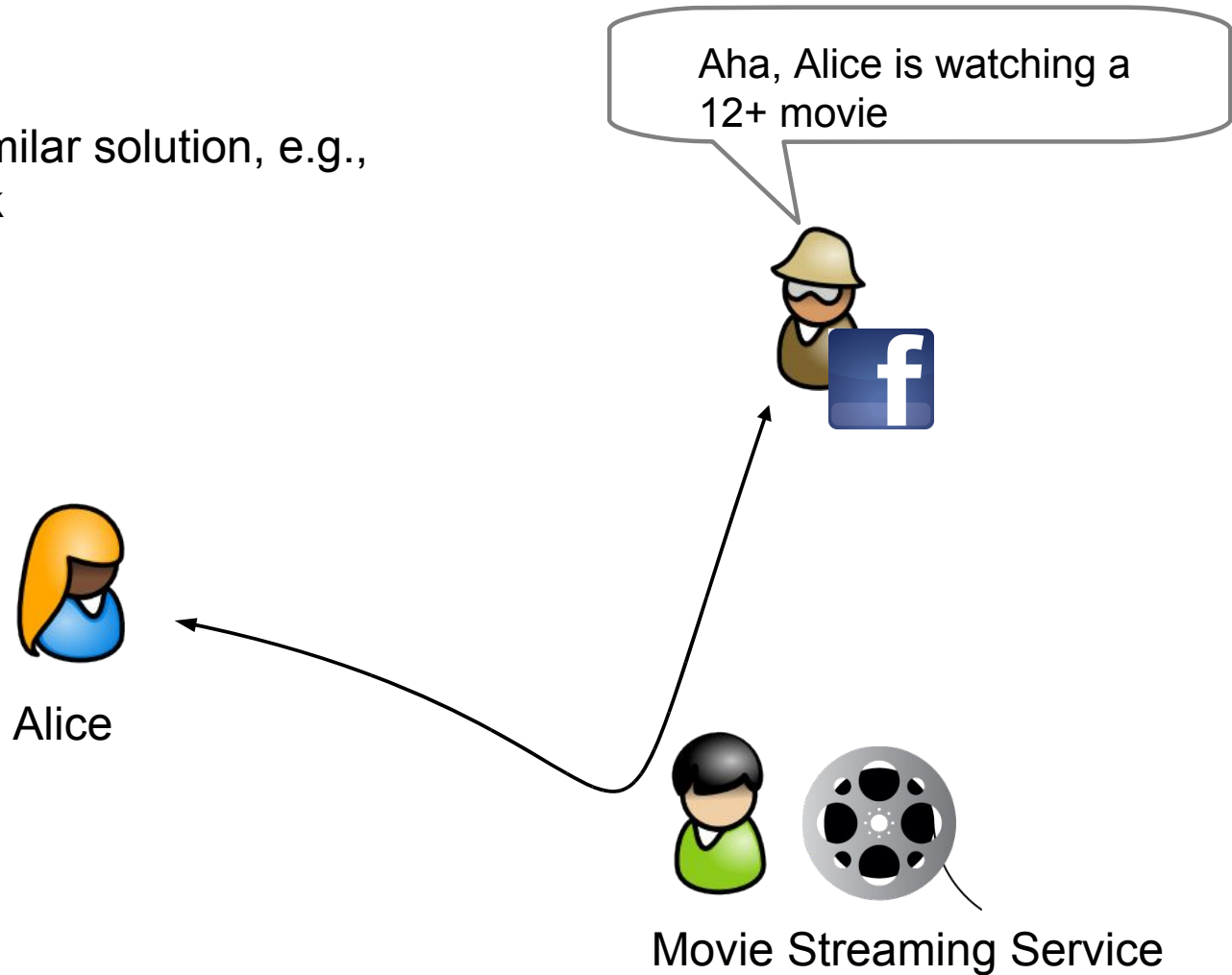
- #1029347
- Premium Subscription
- Expires Jan 13, 2016

Movie Streaming Service

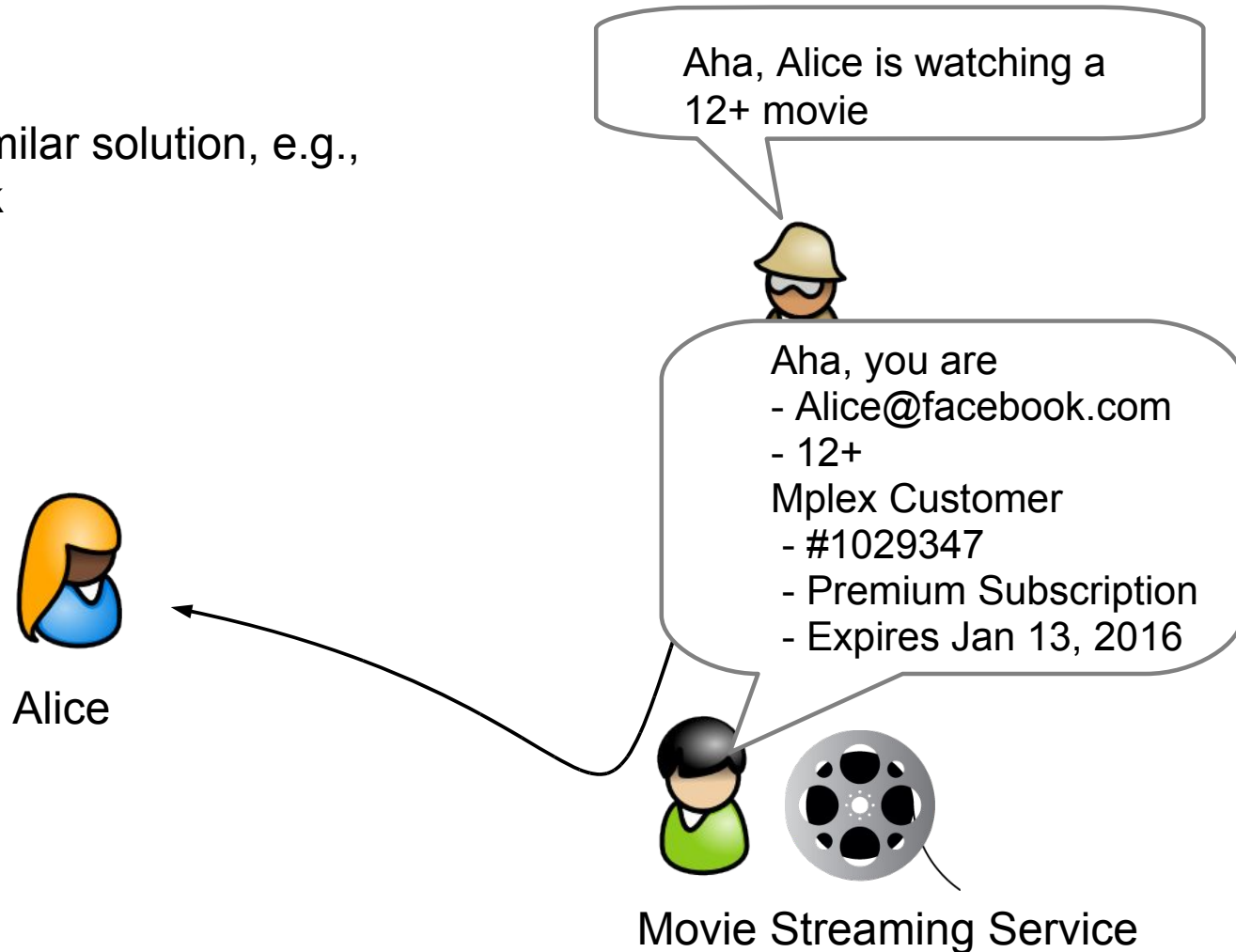
With OpenID and similar solution, e.g.,
log-in with Facebook



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



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



Identity Mixer solves this.

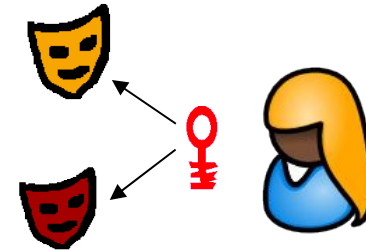
When Alice authenticates to the Movie Streaming Service with Identity Mixer, all the services learns is that Alice

- has a subscription
- is older than 12

and no more!

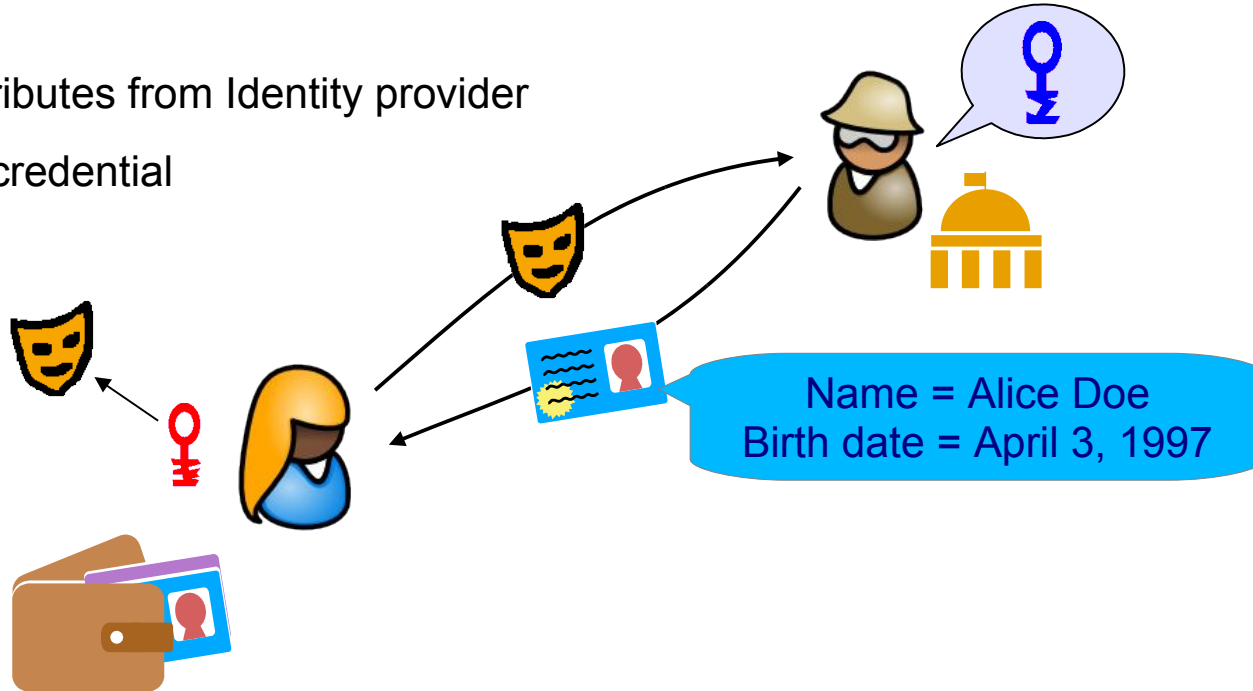
Users' Keys:

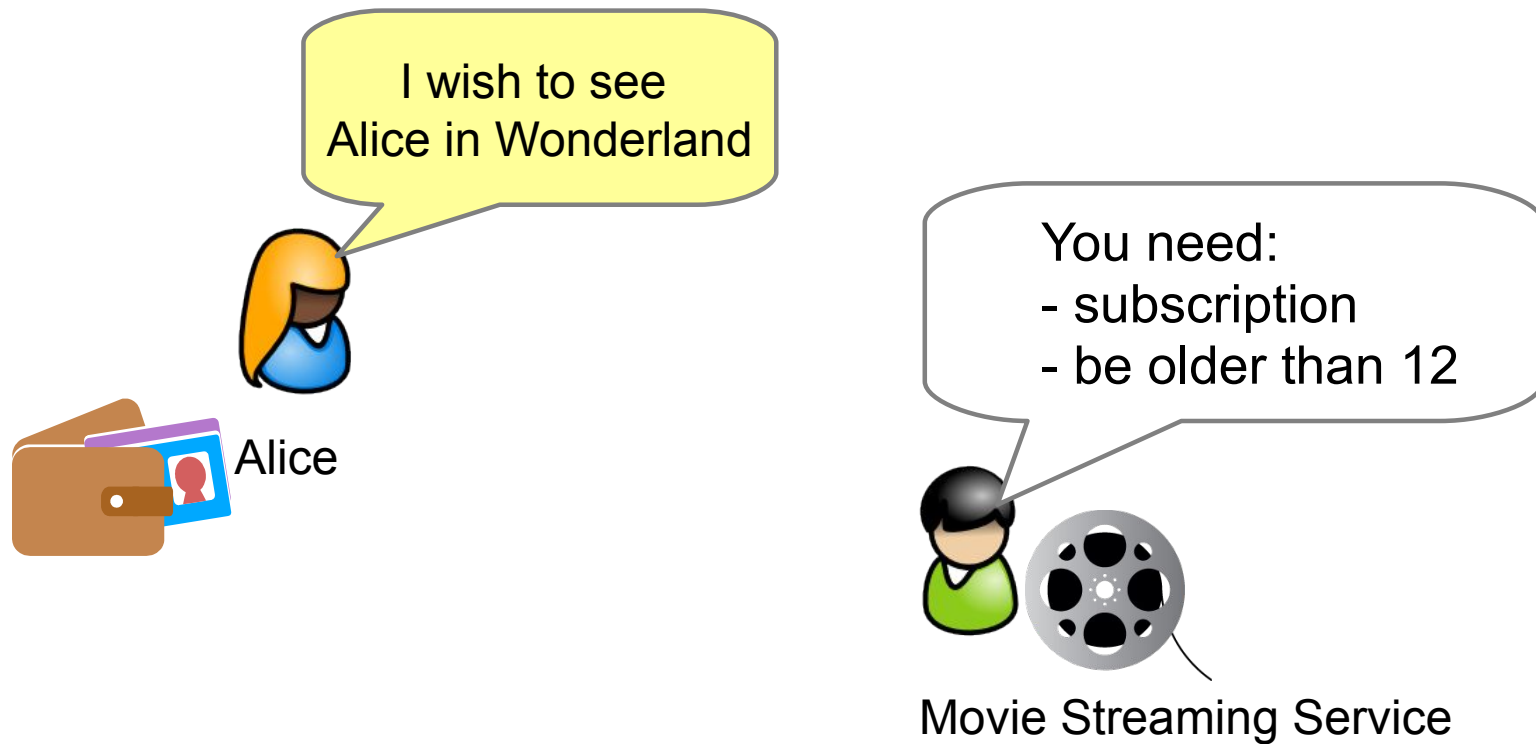
- One secret Identity (secret key)
- Many Public Pseudonyms (public keys)

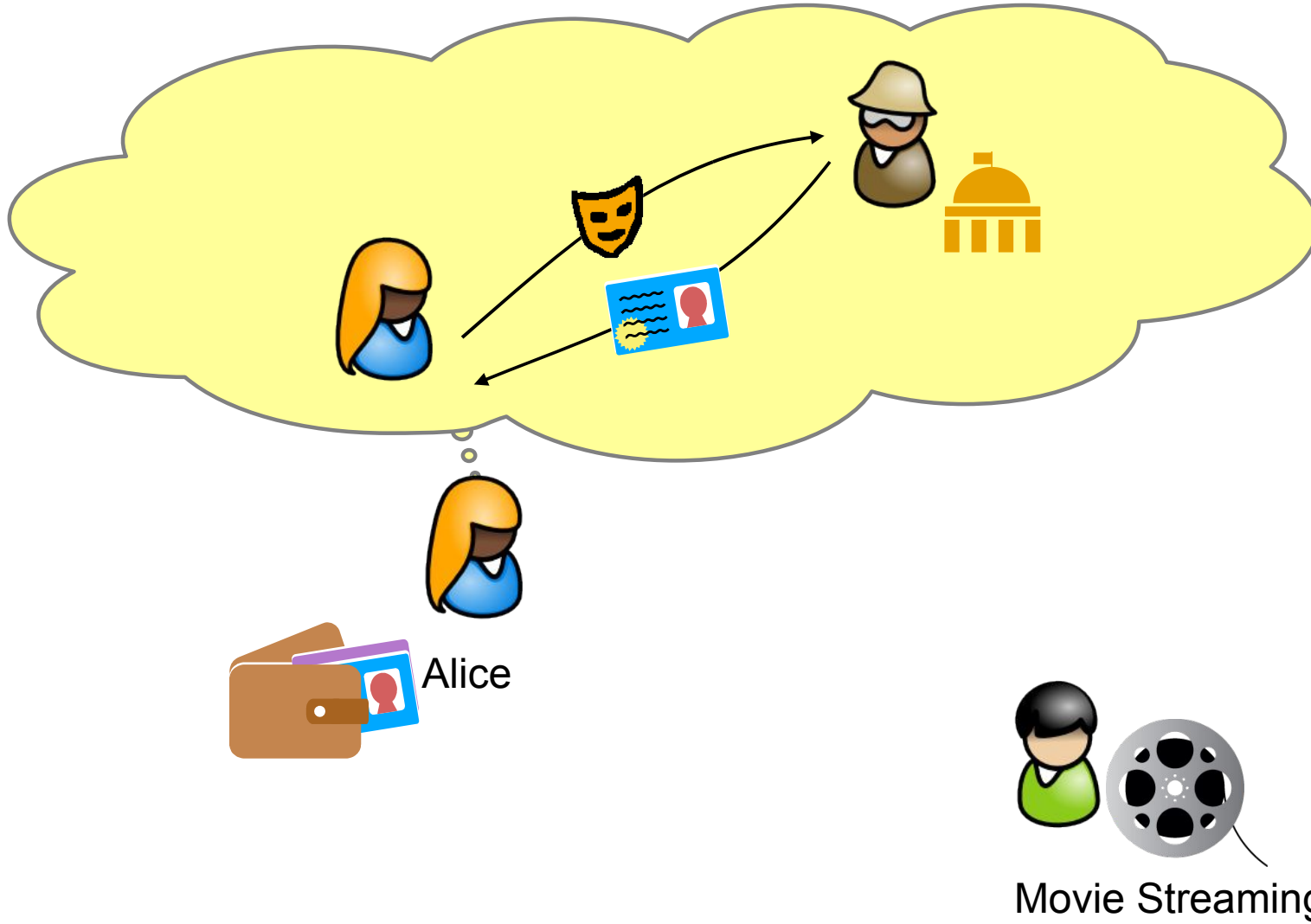


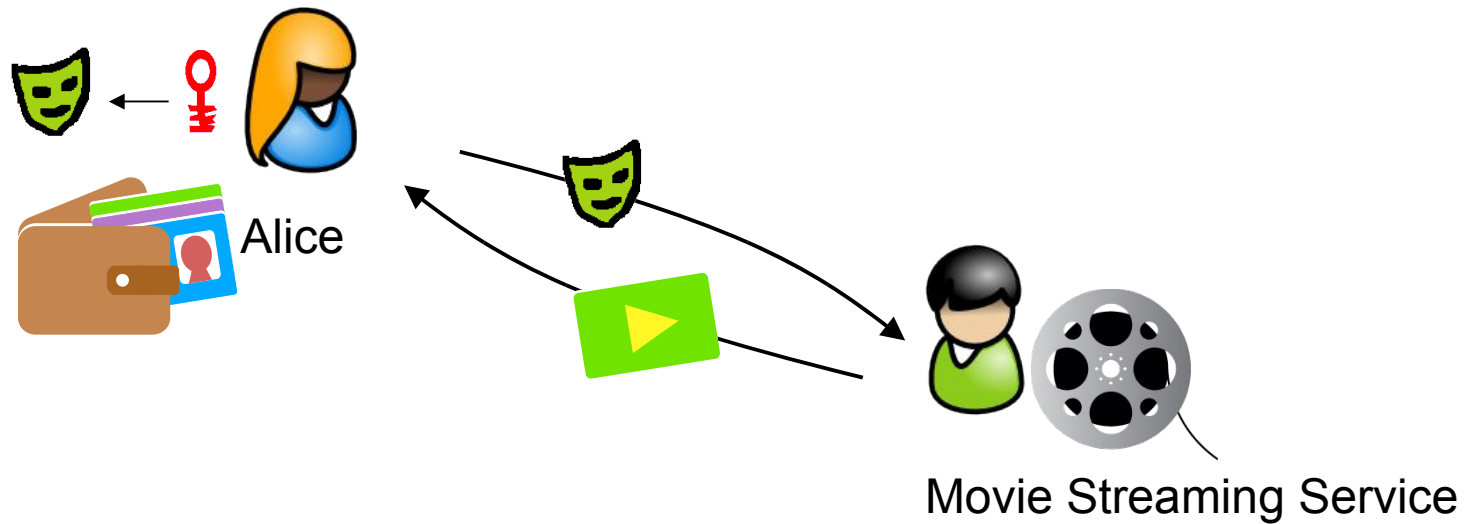
Certified attributes from Identity provider

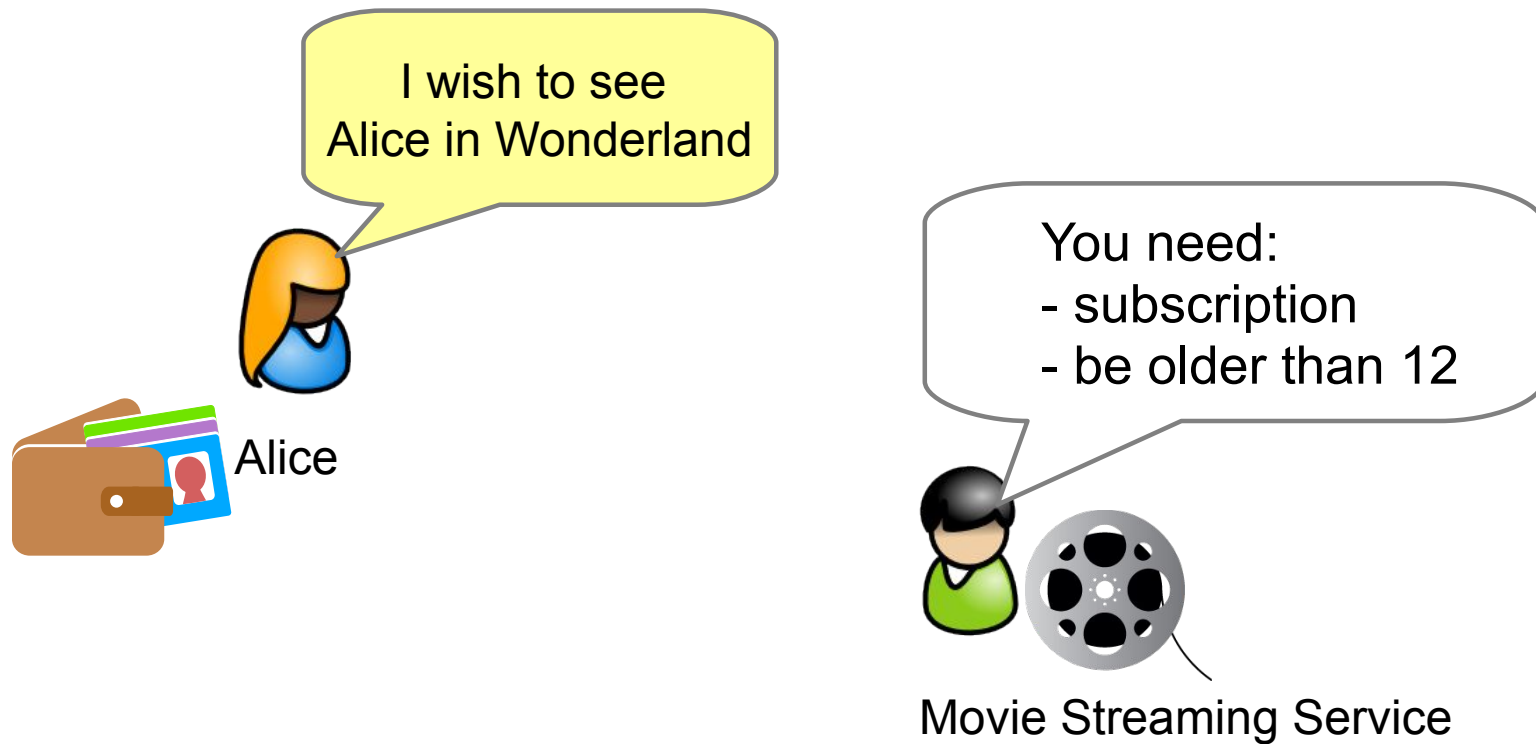
- Issuing a credential







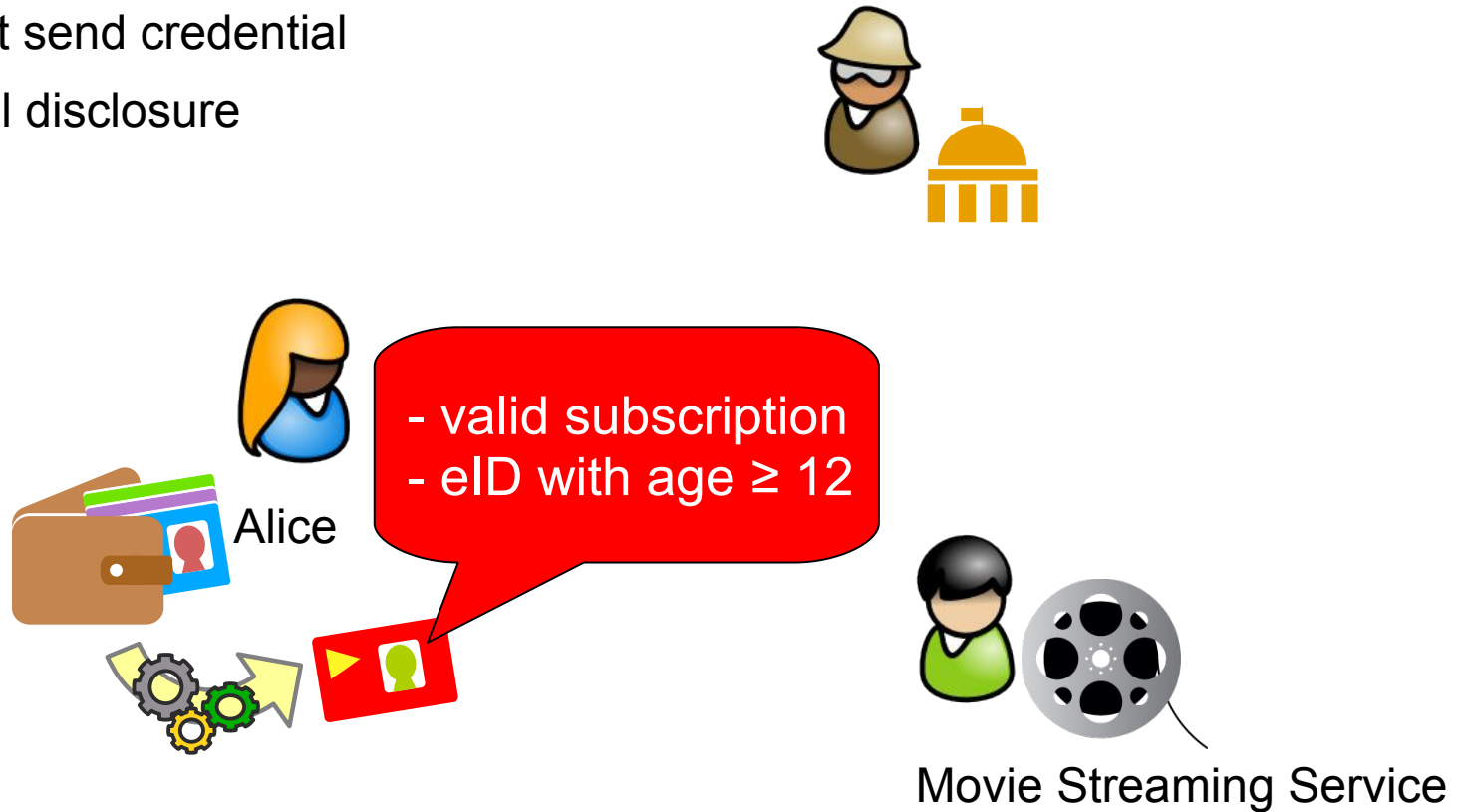




Concept: presentation policy

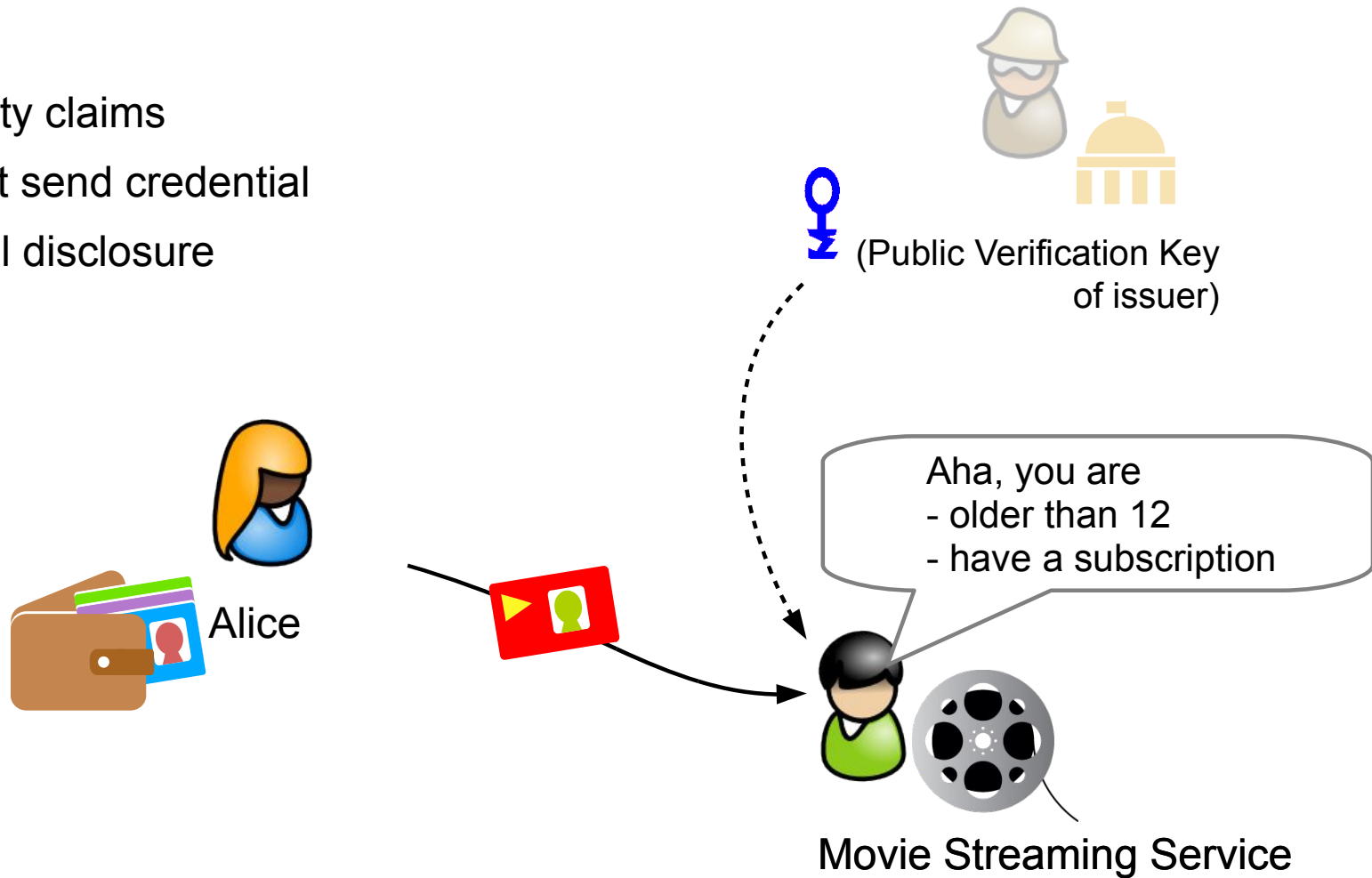
Proving identity claims

- but does not send credential
- only minimal disclosure



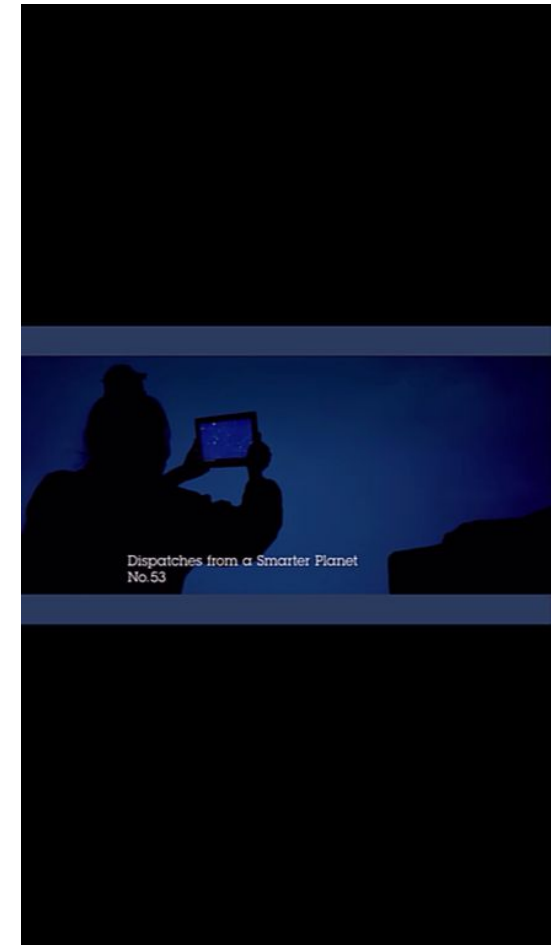
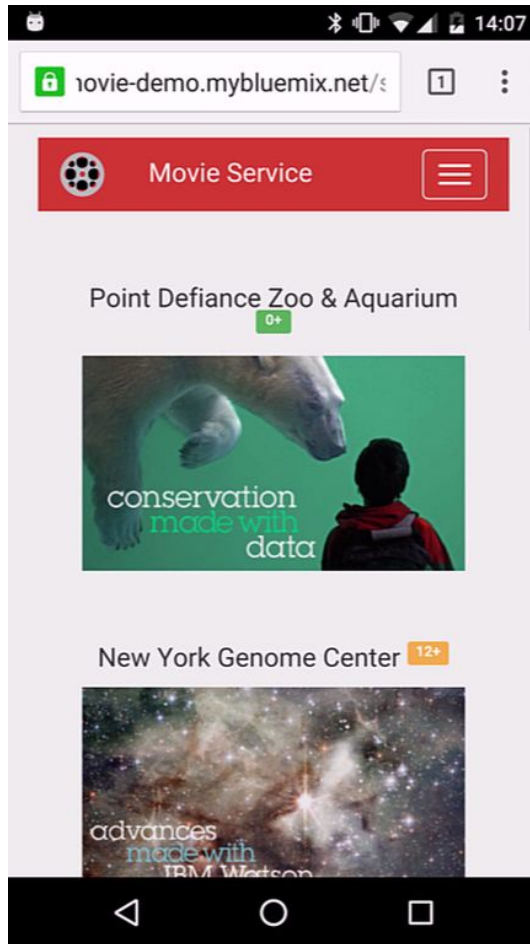
Proving identity claims

- but does not send credential
- only minimal disclosure





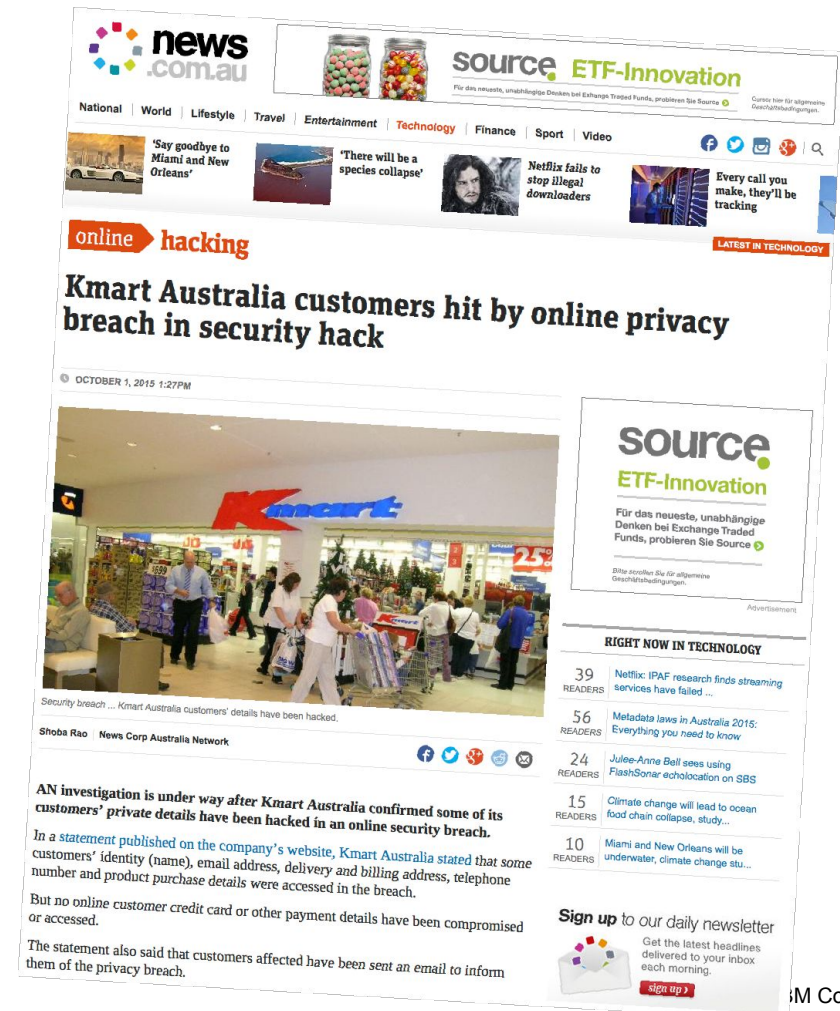
So, let's watch a movie! – Try for yourself w/ Web-based Demo

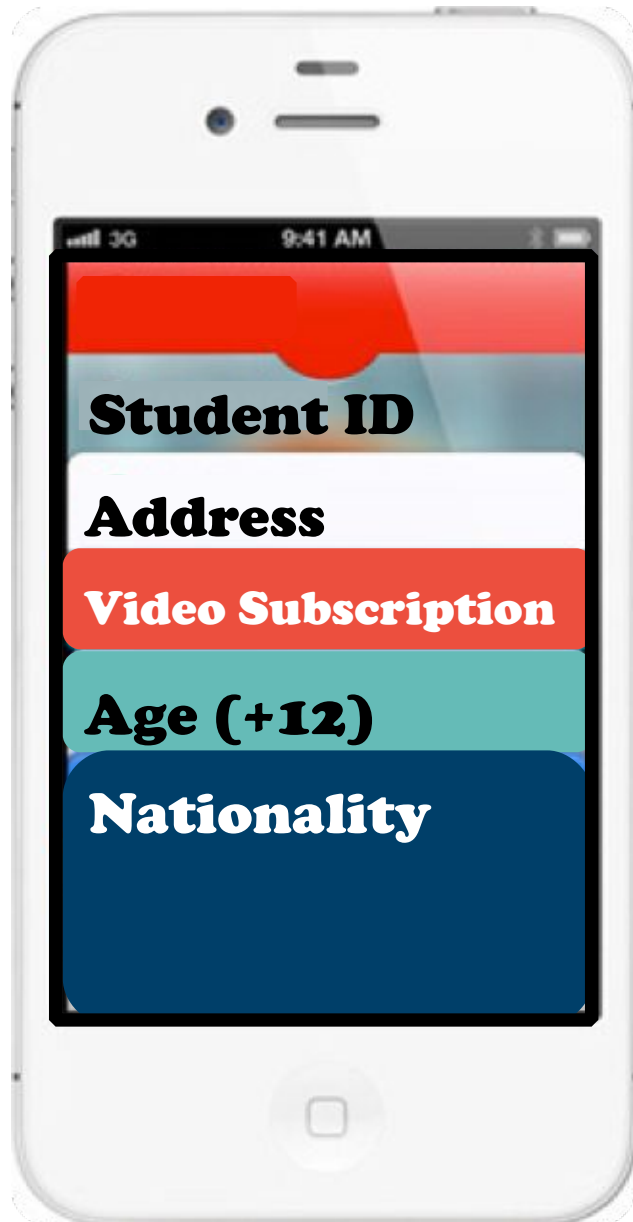


idemixdemo.mybluemix.net
idemixdemo.zurich.ibm.com

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

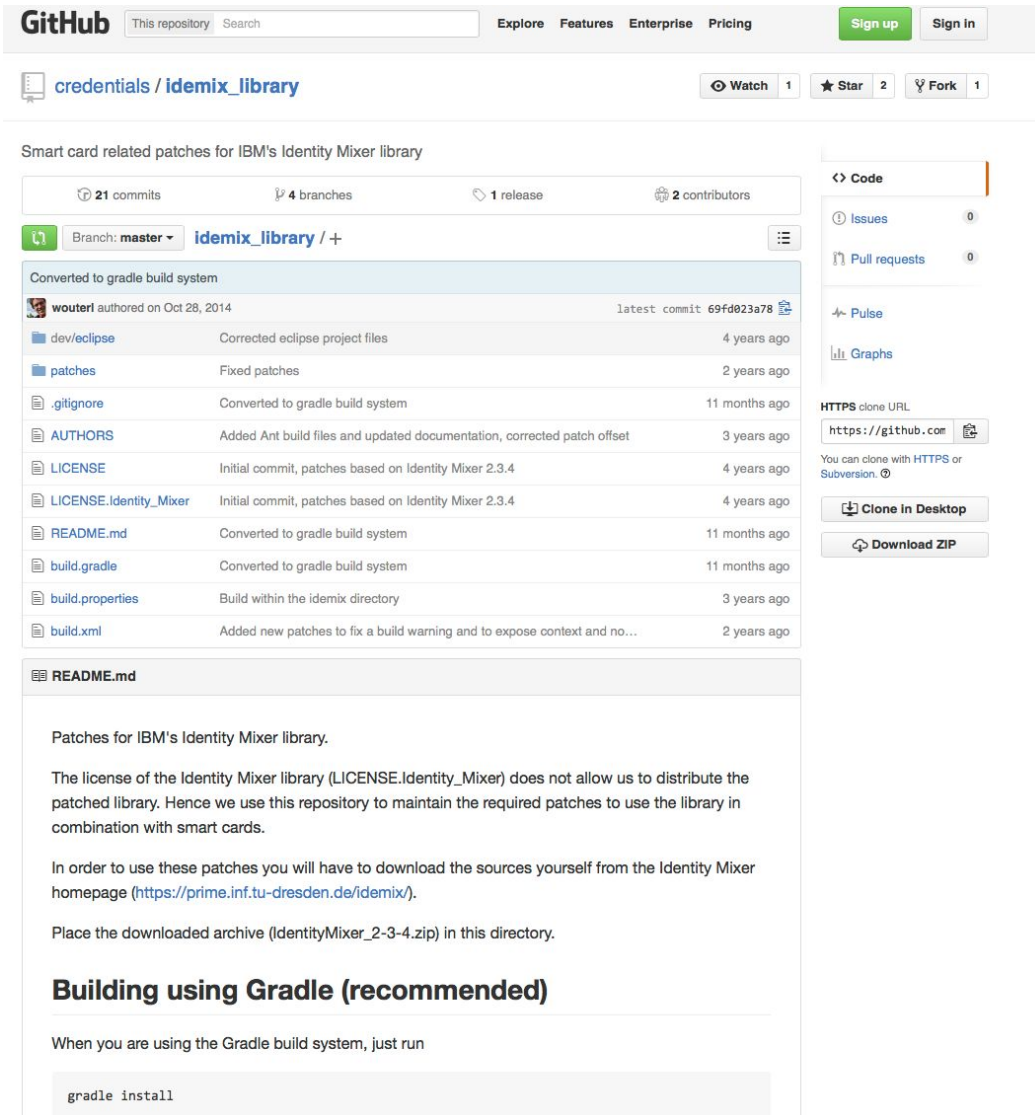
- Less storage costs,
- less security costs and
- Less public apologies.





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.



The screenshot shows the GitHub interface for the repository 'credentials / idemix_library'. At the top, there's a navigation bar with 'GitHub', a search bar, and links for 'Explore', 'Features', 'Enterprise', 'Pricing', 'Sign up', and 'Sign in'. Below this, the repository name is displayed with 'Watch', 'Star', and 'Fork' buttons. The main content area shows the repository's commit history, listing files like 'dev/eclipse', 'patches', '.gitignore', 'AUTHORS', 'LICENSE', 'LICENSE.Identity_Mixer', 'README.md', 'build.gradle', 'build.properties', and 'build.xml' with their respective commit dates. On the right side, there's a sidebar with 'Code', 'Issues', 'Pull requests', 'Pulse', and 'Graphs' sections. Below the commit history, the 'README.md' file is expanded, showing the project's purpose, license information, and instructions for building the project using Gradle.

Smart card related patches for IBM's Identity Mixer library

21 commits 4 branches 1 release 2 contributors

Branch: master idemix_library / +

Converted to gradle build system

wouteri authored on Oct 28, 2014 latest commit 69fd023a78

dev/eclipse	Corrected eclipse project files	4 years ago
patches	Fixed patches	2 years ago
.gitignore	Converted to gradle build system	11 months ago
AUTHORS	Added Ant build files and updated documentation, corrected patch offset	3 years ago
LICENSE	Initial commit, patches based on Identity Mixer 2.3.4	4 years ago
LICENSE.Identity_Mixer	Initial commit, patches based on Identity Mixer 2.3.4	4 years ago
README.md	Converted to gradle build system	11 months ago
build.gradle	Converted to gradle build system	11 months ago
build.properties	Build within the idemix directory	3 years ago
build.xml	Added new patches to fix a build warning and to expose context and no...	2 years ago

README.md

Patches for IBM's Identity Mixer library.

The license of the Identity Mixer library (LICENSE.Identity_Mixer) does not allow us to distribute the patched library. Hence we use this repository to maintain the required patches to use the library in combination with smart cards.

In order to use these patches you will have to download the sources yourself from the Identity Mixer homepage (<https://prime.inf.tu-dresden.de/idemix/>).

Place the downloaded archive (IdentityMixer_2-3-4.zip) in this directory.

Building using Gradle (recommended)

When you are using the Gradle build system, just run

```
gradle install
```

Available in GitHub.

<https://github.com/p2abcengine/p2abcengine>

IBM Research announces breakthrough in protecting personal data using the Cloud



IBM Research



10,575

YouTube

5,523

+ Add to ↻ Share ... More

👍 17 🗨️ 3

Share **Embed** Email

```
<iframe width="560" height="315" src="https://www.youtube.com/embed/gKK1PxGu6Fo" frameborder="1">
```

Preview:



Video size: 560 × 315

- ☒ Show suggested videos when the video finishes
- ☒ Show player controls
- ☒ Show video title and player actions
- ☐ Enable privacy-enhanced mode [?]

By displaying YouTube videos on your site, you are agreeing to the [YouTube API terms of service](#).

SHOW LESS

Identity Mixer as a service on Bluemix.

Easy to set up and integrate:

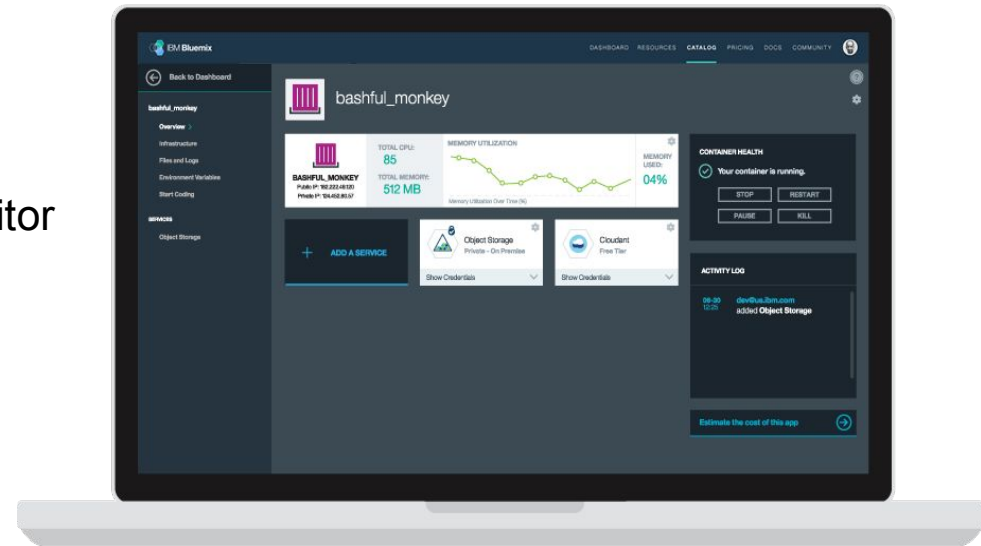
In Bluemix developers simply choose what data they don't want to collect and a piece of code is available to copy and paste.

A close-up photograph of a dry, brown leaf on a dark, textured surface, possibly sand or soil. The leaf is positioned in the upper right quadrant of the frame. The background is a dark, granular material with many small pits and indentations, resembling sand or a coarse surface.

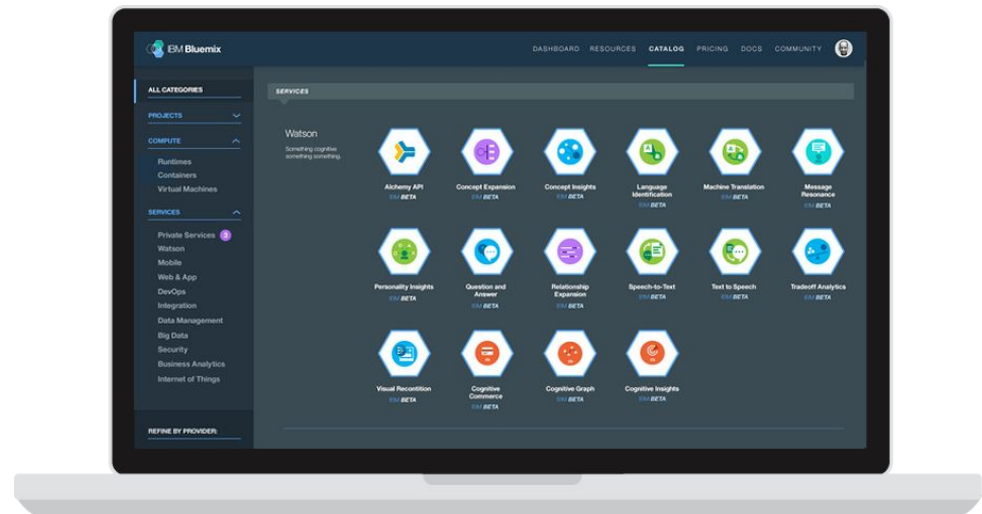
Identity Mixer in the Cloud

An Authentication Service on Bluemix

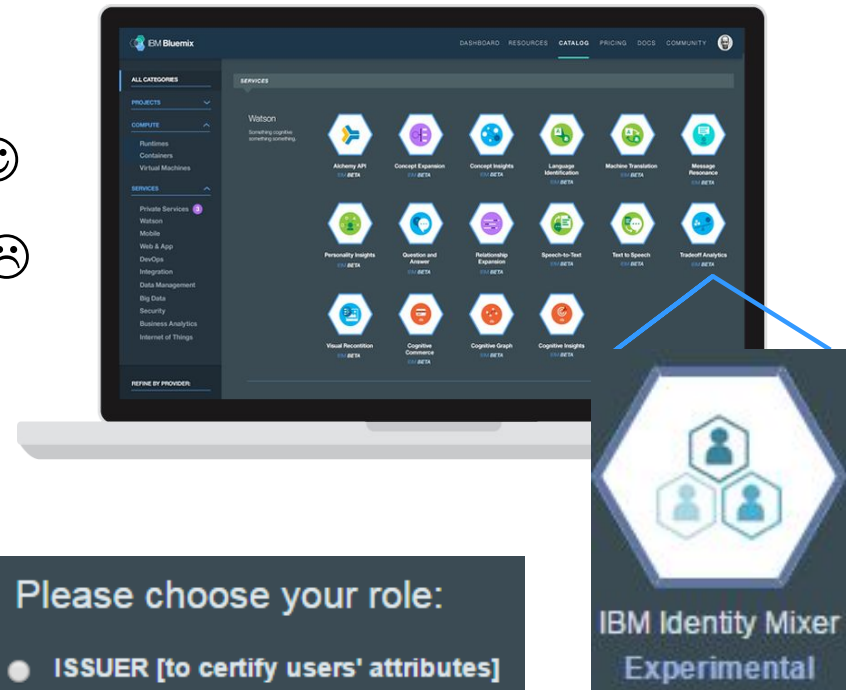
- Build & Run Apps in the Cloud
 - Build, run, deploy, scale, manage, monitor
 - Java, Node.js, Python, PHP, etc.
 - You provides application. IBM runs it.
 - Pay only for what you really need



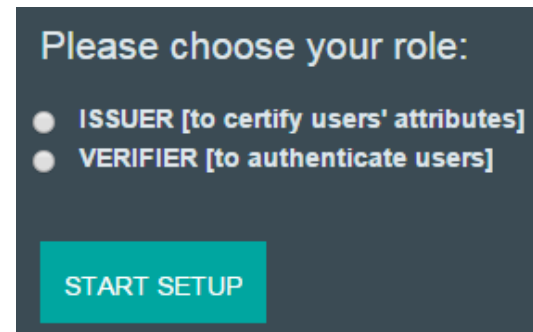
- Use Services & APIs
 - Watson, Mobile, Data, Analytics, etc.
 - New in Security: **Identity Mixer**



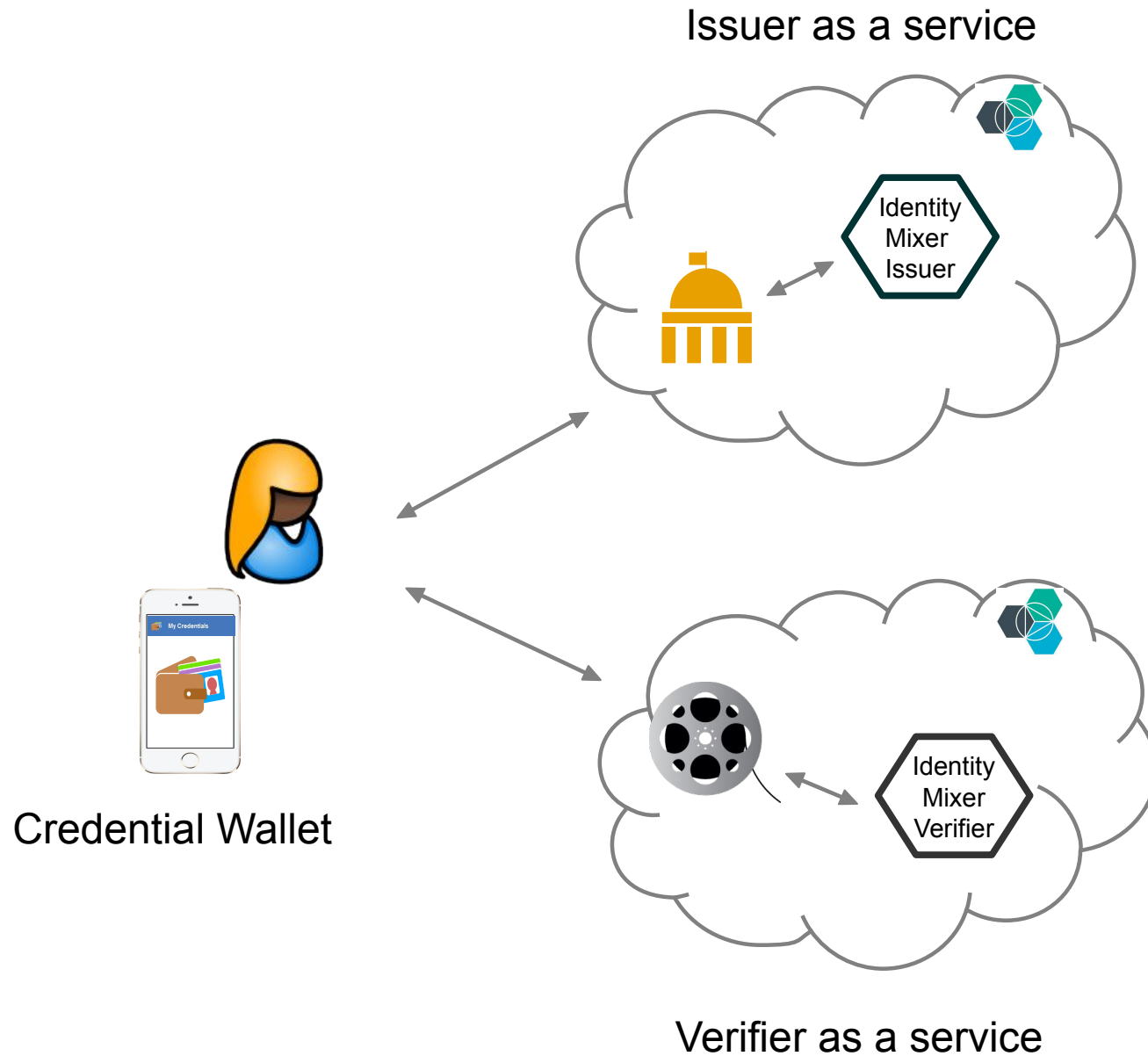
- Identity Mixer is freely available on GitHub 😊
- Integration is involved and time consuming 😞
- Our Bluemix service fixes this 😊



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

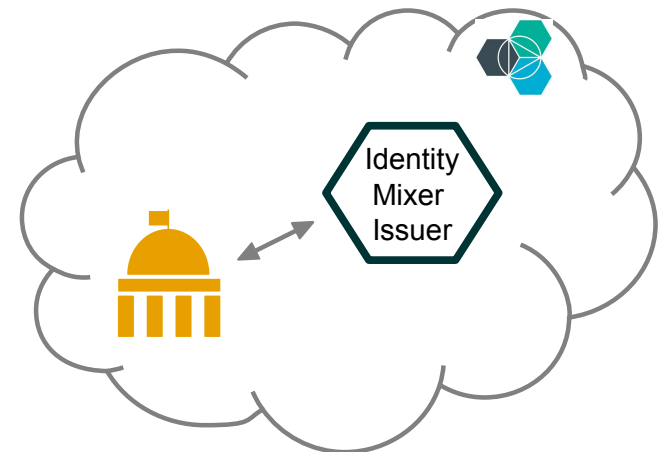


- Get up and running **within minutes** with our template applications



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.



IBM Bluemix

DASHBOARD | SOLUTIONS | CATALOG | PRICING | DOCS | COMMUNITY

214

214

Back to Dashboar...

IBM Identity Mixer-issuer

DOCS

frp-issuer-demo

Overview

SDK for Node.js™

Files and Logs

Environment Variables

Start Coding

SERVICES

IBM Identity Mixer >

Issuer Configuration

Unique Issuer Name: idemix eGovernment Demo

Credential specifications

Add Credential Specification: - Please select Specification -

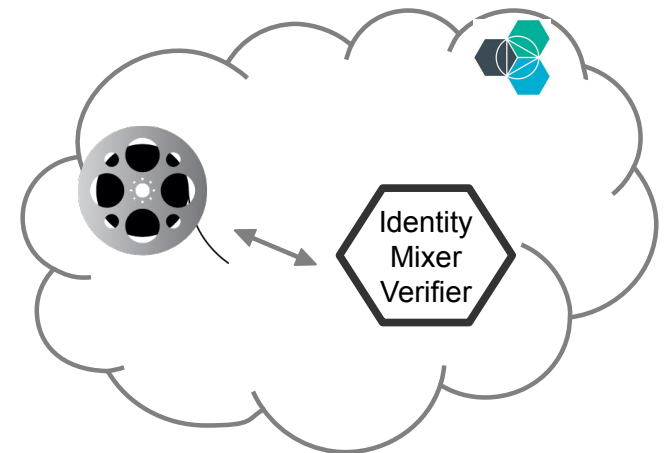
Human Readable Name:	Data Type
Name	string
Last Name	string
Date of Birth	date

Credential Type: ID card

NEXT

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.



IBM Bluemix

DASHBOARD | SOLUTIONS | CATALOG | PRICING | DOCS

Back to Dashboard...

IBM Identity Mixer-verifier

frp-issuer-demo
Overview
SDK for Node.js™
Files and Logs
Environment Variables
Start Coding

SERVICES
IBM Identity Mixer
IBM Identity Mixer >

Verifier Configuration: Create Access Policies

Policies

Add New Policy: Create New Policy ▼

Policy: Over 16 according to eGov ID

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

ADD PREDICATE

NEXT

```
{
  "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"
    }
  ]
}
```

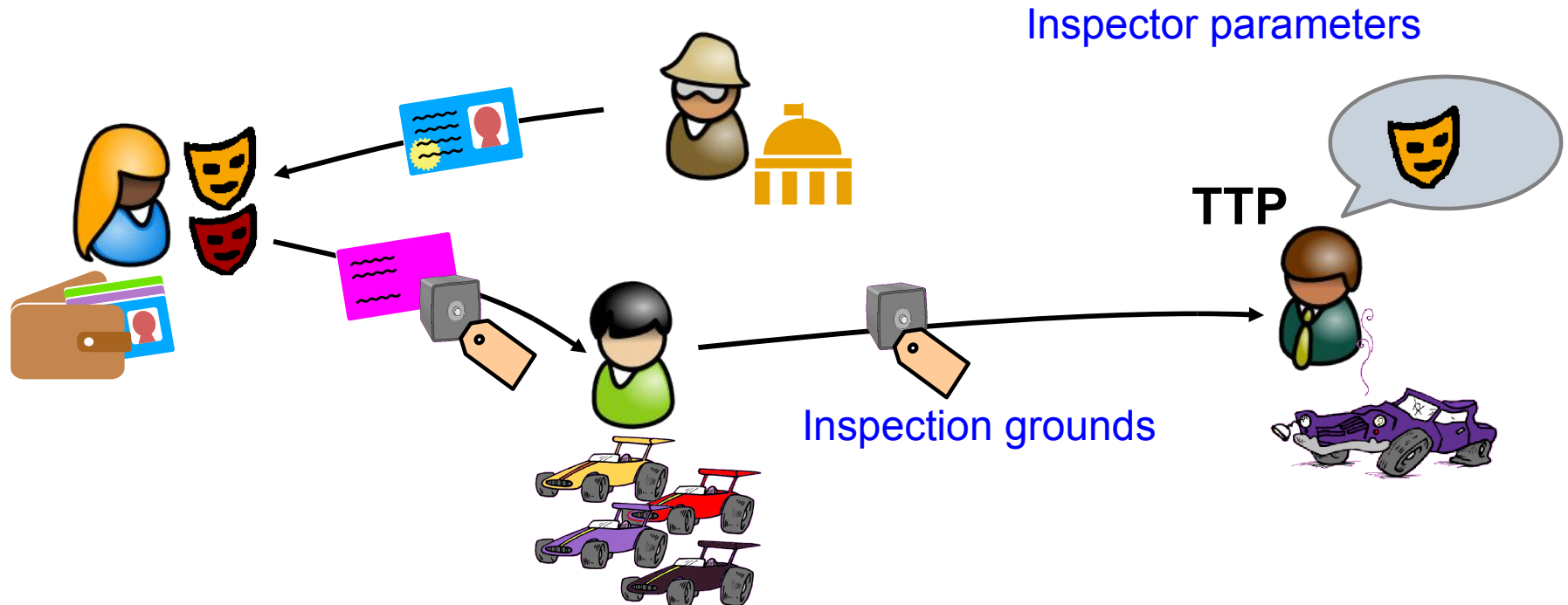
- Scientific foundation laid 15 years ago, well studied & award winning
- Successful real-world pilots in series of EU projects



- 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

A photograph of a beach scene. In the foreground, a large, dark footprint is visible in the wet sand. In the background, waves are breaking on the shore, creating a white foam line. The sky is a mix of orange and blue, suggesting a sunset or sunrise.

Extended Features

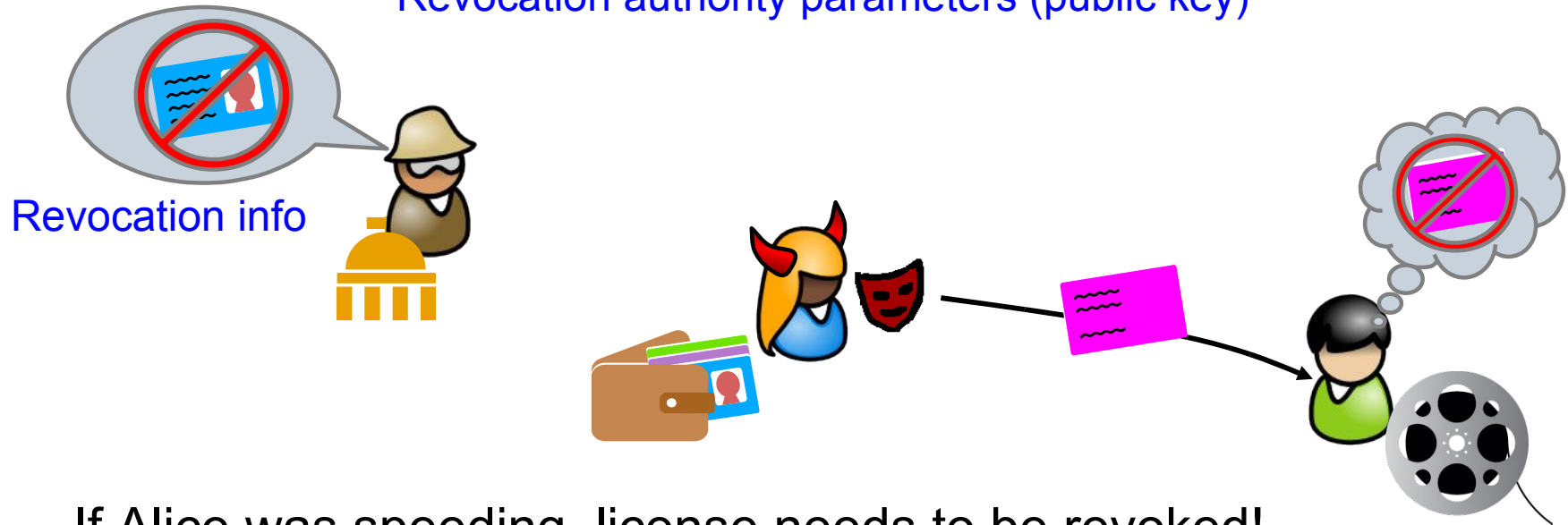


If car is damaged: ID with insurance or gov't needs be retrieved

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

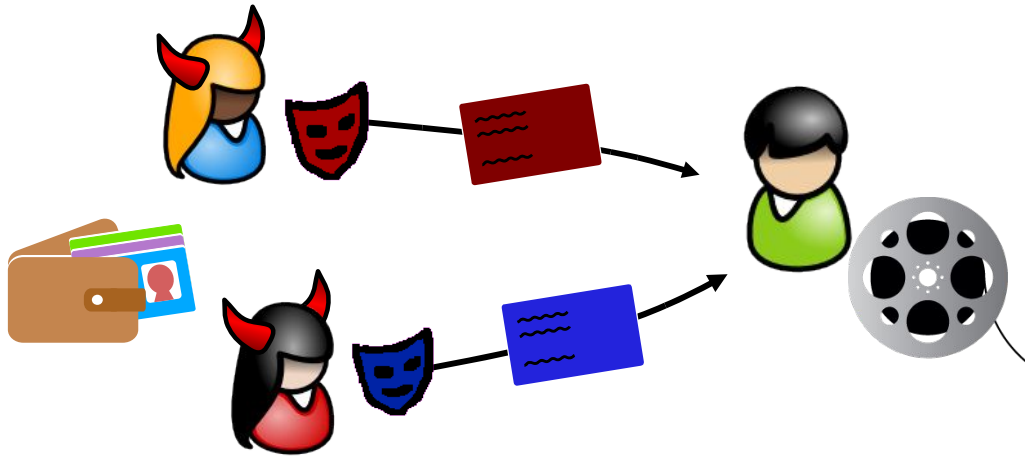
TTP is off-line & can be distributed to lessen trust

Revocation authority parameters (public key)



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:

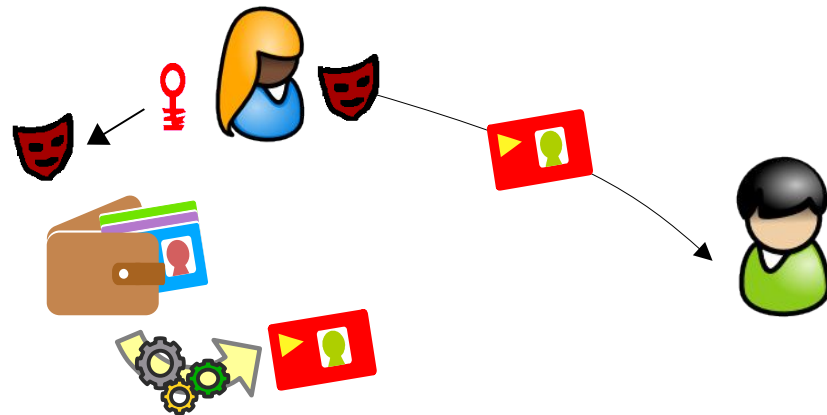
- If Alice and Eve are on-line at the same time, they are caught!
- Use Limitation – anonymous until:
 - If Alice used certs > 100 times total...
 - ... or > 10'000 times with Bob
- Alice's cert can be bound to hardware token (e.g., TPM)

A close-up photograph of a sandy surface with two footprints. One footprint is in the upper center, and another is in the lower left. The text 'Some Use Cases' is overlaid on the first footprint.

Some Use Cases

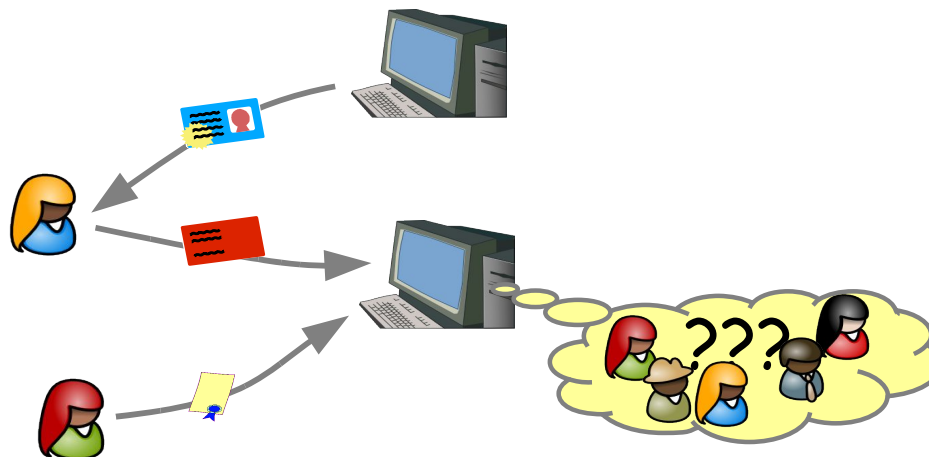
Proving 12+, 18+, 21+ without disclosing the exact date of birth – privacy and compliance with age-related legislation

- Movie streaming services
- Gaming industry
- Online gambling platforms
- Dating websites
- Social benefits for young/old people



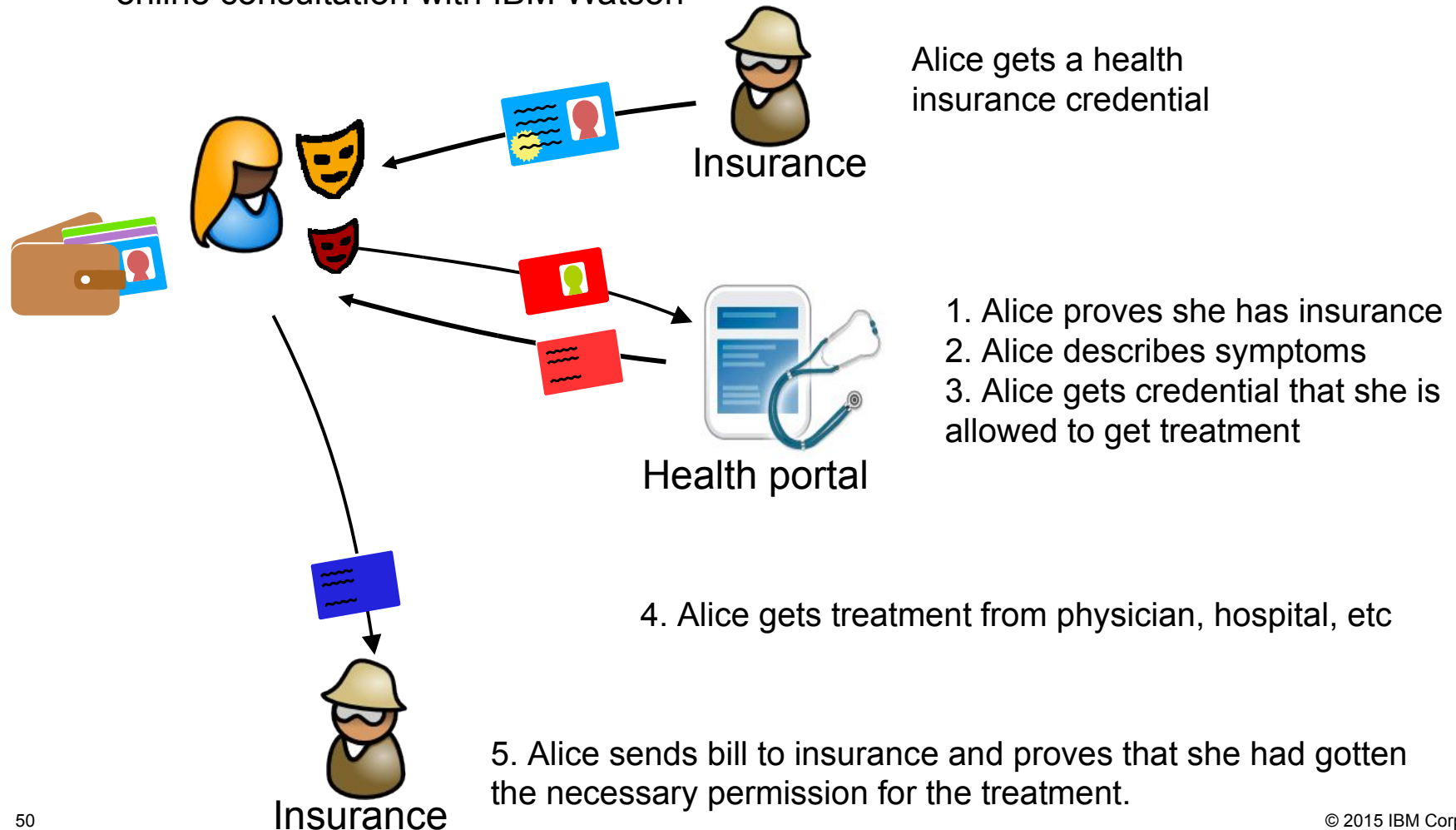
Who accesses *which data* at which time can reveal sensitive information about the users (their research strategy, location, habits, etc.)

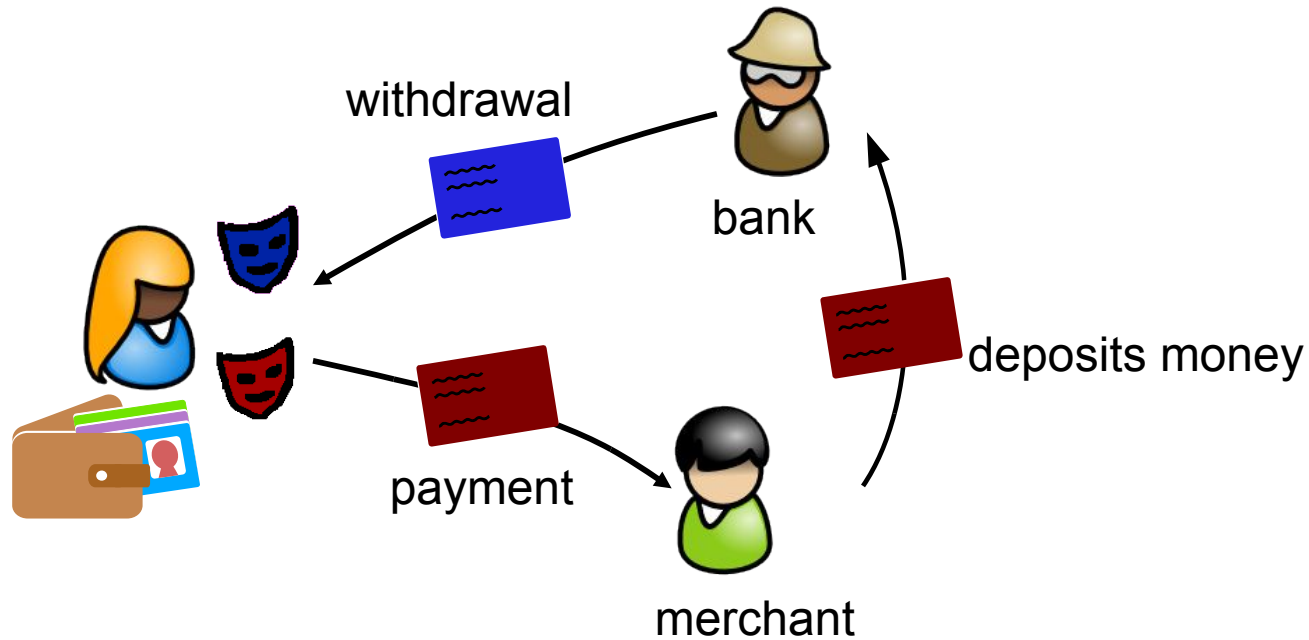
- Patent databases
- DNA databases
- News/Journals/Magazines
- Transportation: tickets, toll roads
- Loyalty programs



Anonymous consultations with specialists

- online chat with a psychologist
- online consultation with IBM Watson

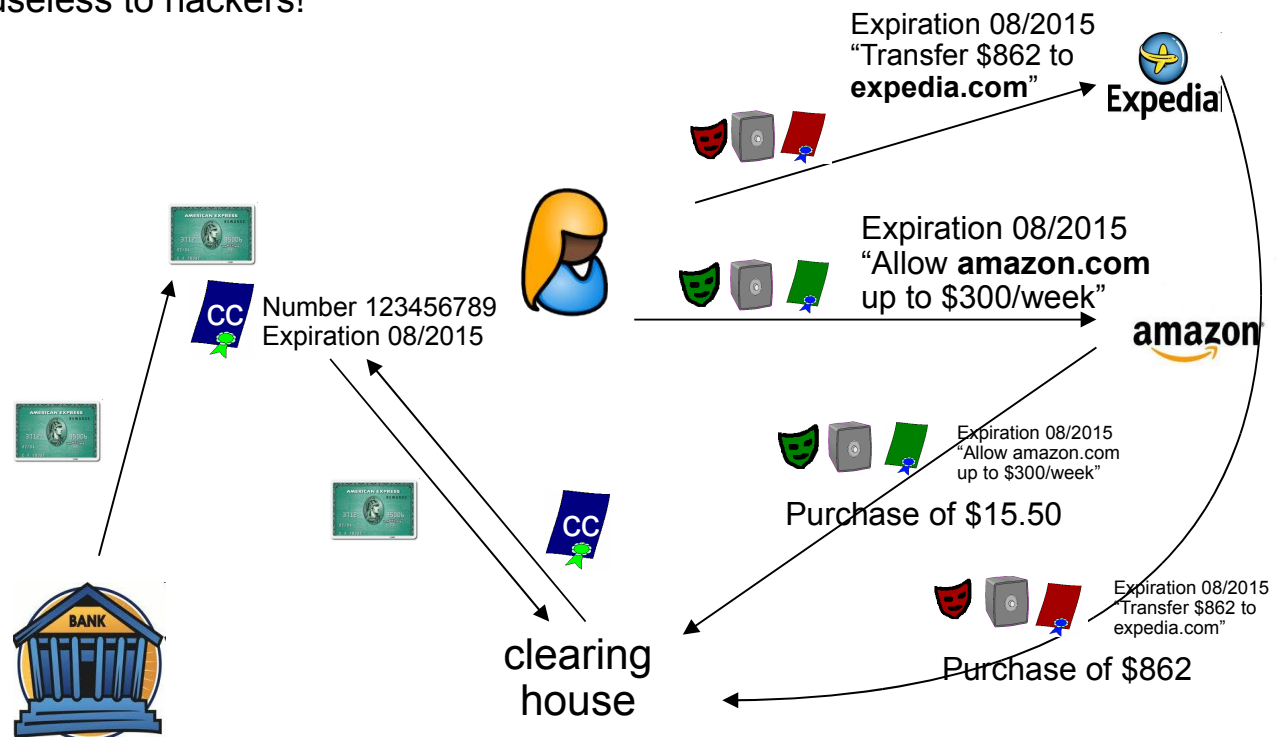




- Credential = Bank note
- Double spending need to be prevented/detected
 - On-line or Off-line modi possible
- Money laundering can also be taken care of

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!



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](https://twitter.com/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/