

Information Privacy?!



Dr. Jan Camenisch

Member, IBM Academy of Technology; IBM Research – Zurich



no more privacy
in an electronic world!



just getting over it ?!?

it is **HUGE** security & privacy problem!

incidents all over the news...

- sony's loss of credit card #, ...
- job lost, blackmailing, suicide, ...
- burglary,
- ID theft (billions of \$\$\$ lost in the US in 2010)
- ...

also:

- social impact not even considered (elections,)
- last but not least: PII is the new currency....

What's the problem? Here's the solutions!



Mix Networks Oblivious Transfer

Searchable Encryption

Onion Routing

Confirmer signatures

Anonymous Credentials

Group signatures

Pseudonym Systems

OT with Access Control

e-voting

Priced OT

Blind signatures

Private information retrieval

Secret Handshakes

Homomorphic Encryption

That's nice, but all this cryptography is not used!

Why?

- Too expensive?!
- Just not needed?!
- Too hard to understand?!
- Too complex too use (right)?!
- Keys too hard to manage?!
-

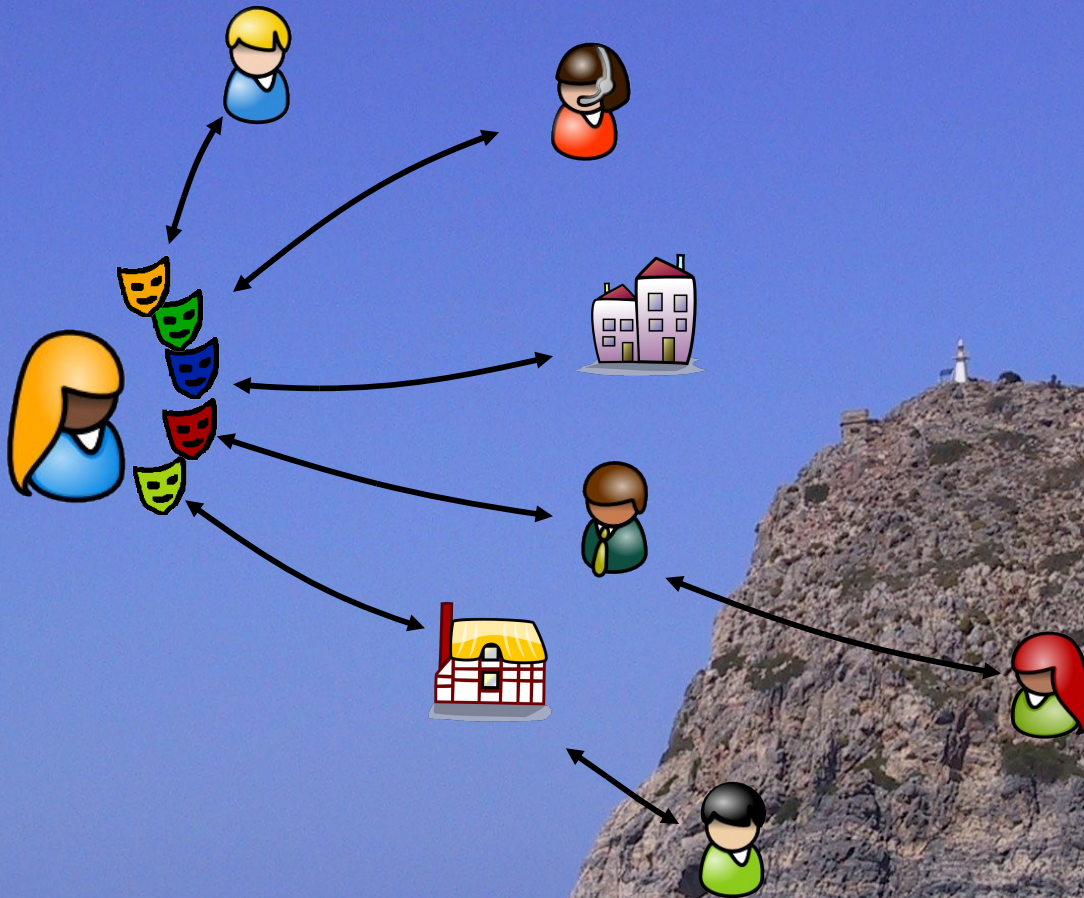
.... so, need to enable “privacy by design”!

of course there are limits...

- tracing is so easy
 - each piece of hardware is quite unique
 - log files everywhere
- but that's not the point!
 - it's not about NSA et al.
 - active vs passive “adversaries”

so still, *privacy by design!*

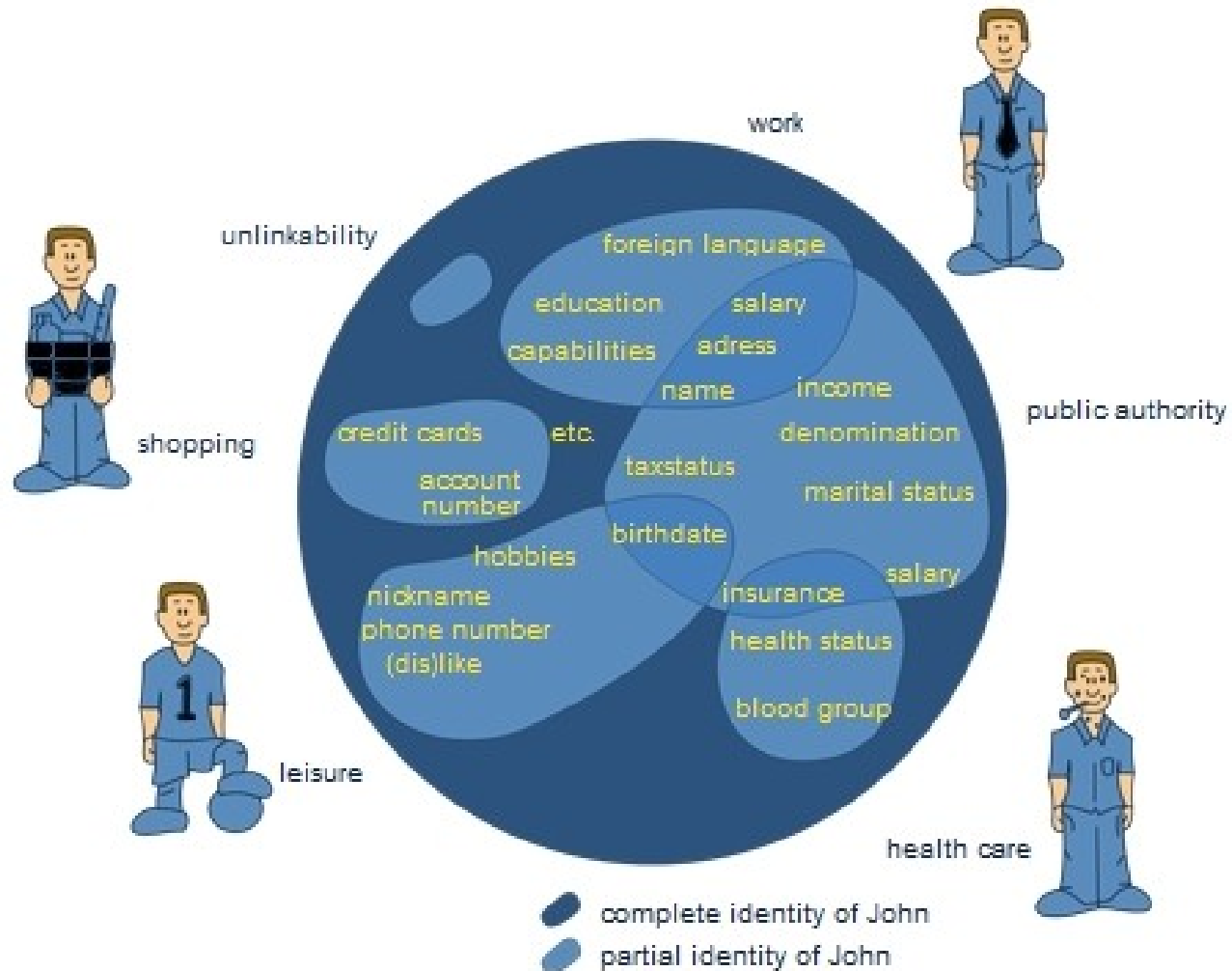
vision:
a secure and privacy-protecting e-world

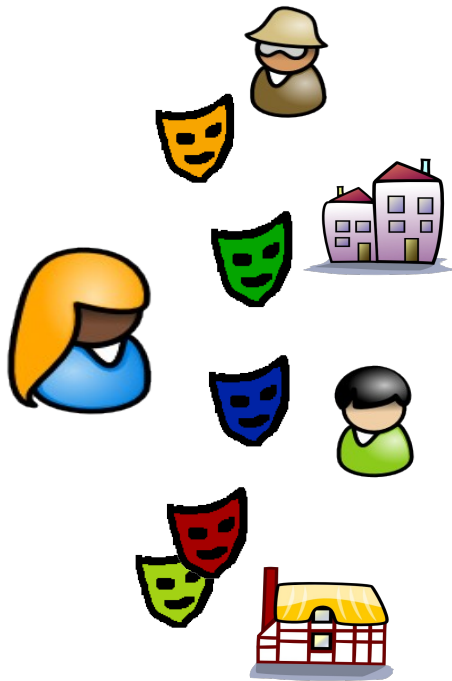


Privacy by design

- Communication layer
 - tor, JAP, etc
- Authentication layer
 - attribute based credentials
- Application layer
 - eVoting, ePolls,
 - any apps needs privacy by design

what is an identity?





- ID: set of attributes shared w/ someone
 - attributes are not static: user & party can add
- ID Management: two things to make ID useful
 - authentication means
 - means to transport attributes between parties
- Control attributes with policies:
 - define requested data
 - define allowed usage (audience)
- Policies authored by user or requestor
 - e-commerce
 - social networks, delegation
- Policies enforced technically (as much as possible)
 - no side information are revealed
 - anonymous credentials, encryption, etc

First Four Concepts

1. ID is set of attributes shared w/ someone
2. ID comes with authentication means:
Key binding & Public key / pseudonym
3. Means to transport attributes between parties:
Credentials & presentation token
4. Define requested data:
Presentation policy

Privacy ABCs: how they work

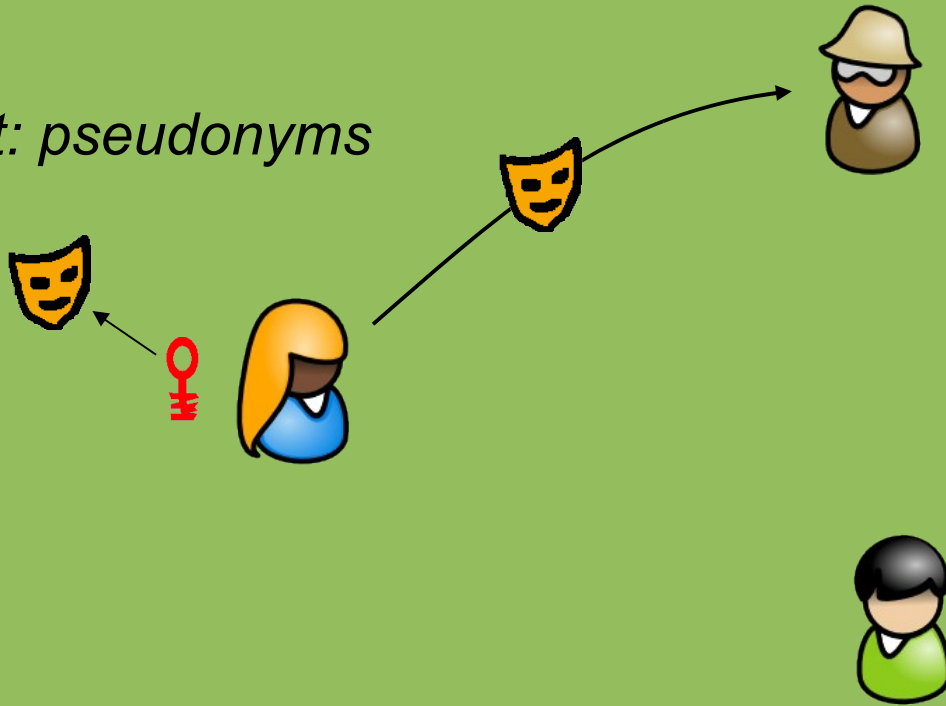


Concept: key binding



Privacy ABCs: how they work

Concept: pseudonyms



Pseudonym

Two kinds of pseudonyms

- Regular
- Scope exclusive (also called domain pseudonym)

Specification of pseudonym very generic, still:

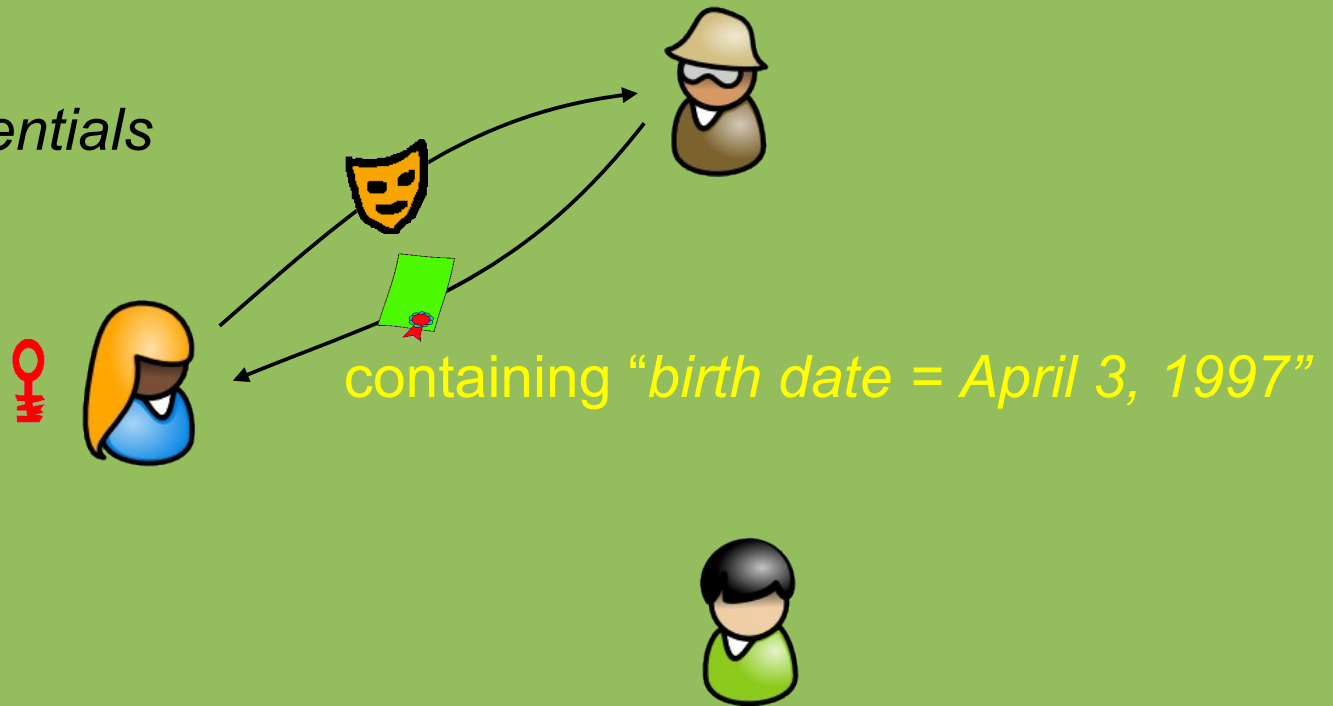
- Scope: String
- Exclusive: Boolean
- PseudonymValue: AnyValue

For regular pseudonym, scope is non-binding description

```
<abc:Pseudonym Scope="xs:string"? Exclusive="xs:boolean"?>  
  <abc:PseudonymValue>...</abc:PseudonymValue>  
</abc:Pseudonym>
```

Privacy ABCs: how they work

Concept: credentials



Credential

Credential Specification

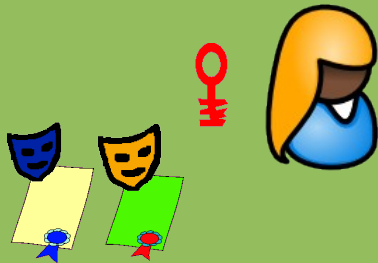
- Specification ID: URN
- NumberOfAttributes: INT
- List of Attributes, each consisting of:
 - Type: URN *first name*
 - DataType: URN *string*
 - Encoding: URN *sha256*
- KeyBinding *true*
- Revocation *false*

Credentials is essentially the same extended with:

- Each attribute consists additionally
 - Value: DataType
- Crypto Value: AnyValue (according to alg.; digital signature)

Privacy ABCs: how they work

Concept: presentation policy



goes off-line

- valid subscription
- age > 18



Presentation policy

Presentation policy: which attributes certified by whom a verifier requires to grant access

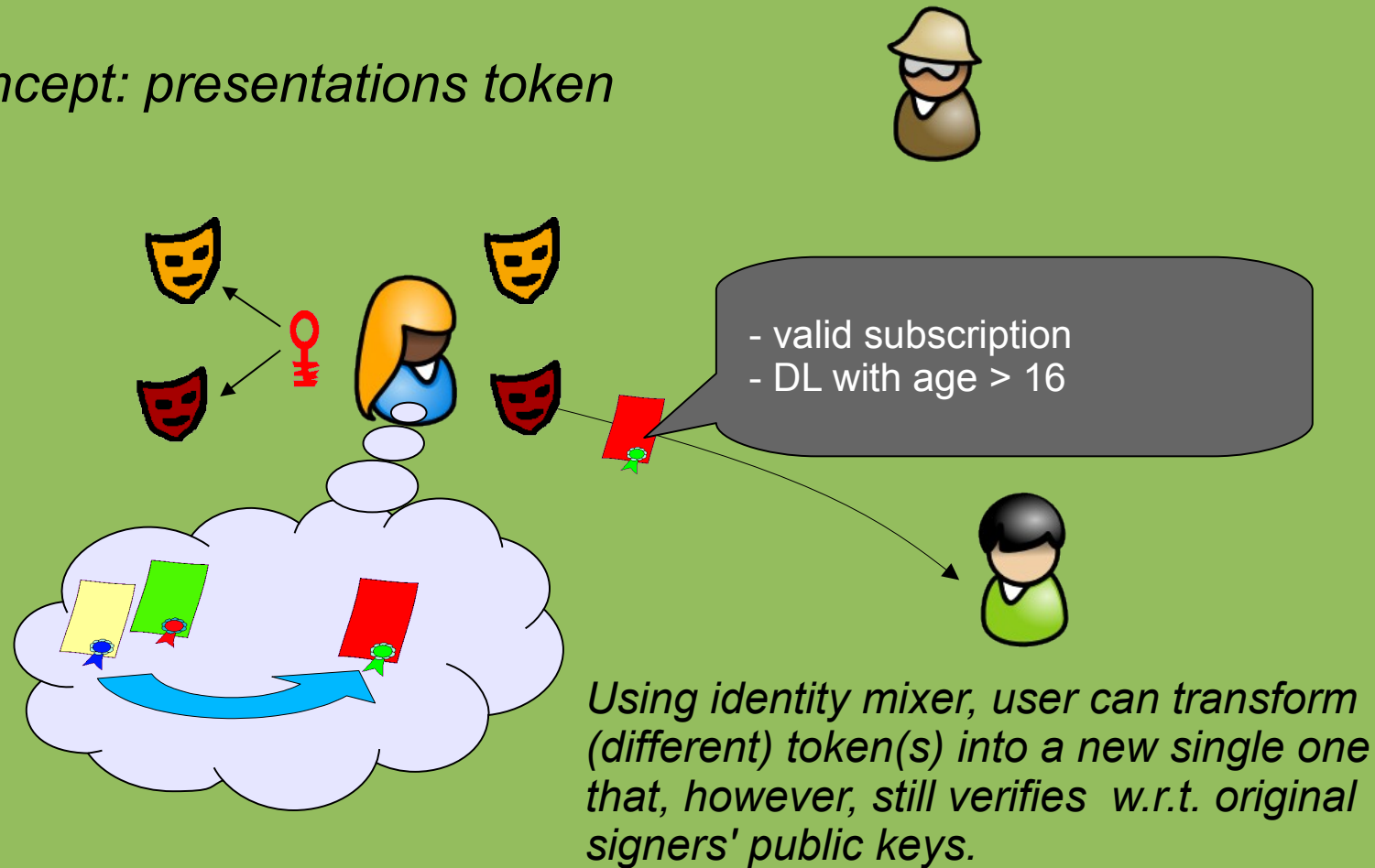
- Credential Alias = String *Driver's License*
 - Possible Credentials: {Credential Spec}
 - Possible Issuers: {IssuerParameters}
 - {Disclosed Attributes: AttributeType}
 - Possible Inspectors: {InspectorPublicKey}
 - Inspection Grounds
 - SameKeyBindingAs: String *Credential Alias*

- AttributePredicate
 - Function: definedFunctions *DateGreaterThan*
 - Attribute: CredentialAlias, AttributeType
 - ConstantValue: AnyValue 1987-03-05

- Message: String

Private Credentials: how they work

Concept: presentations token

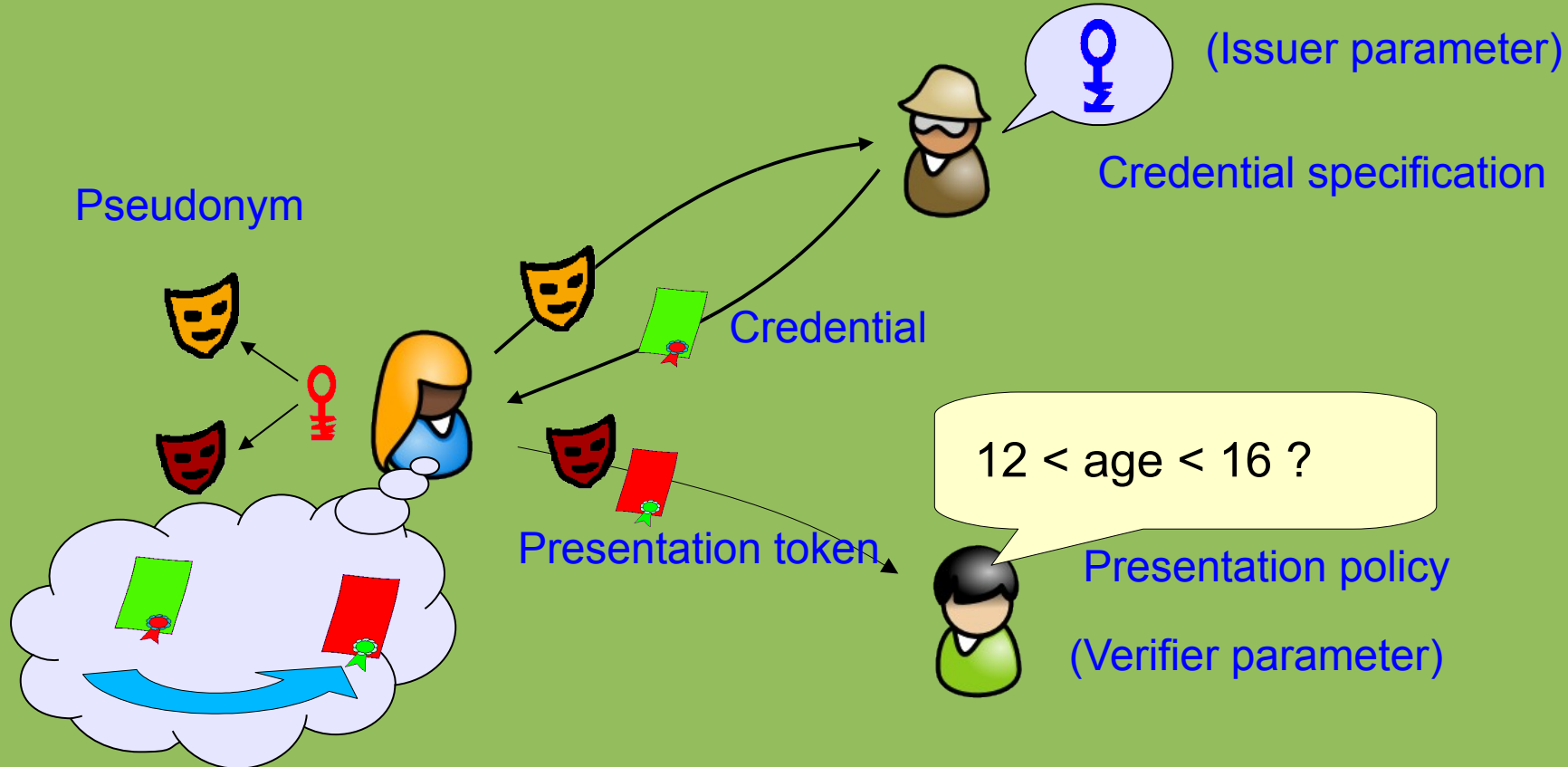


Presentation token

Presentation token: essentially presentation policy

- Concrete values for attributes
- Cryptographic evidence (signature/transformed credential)

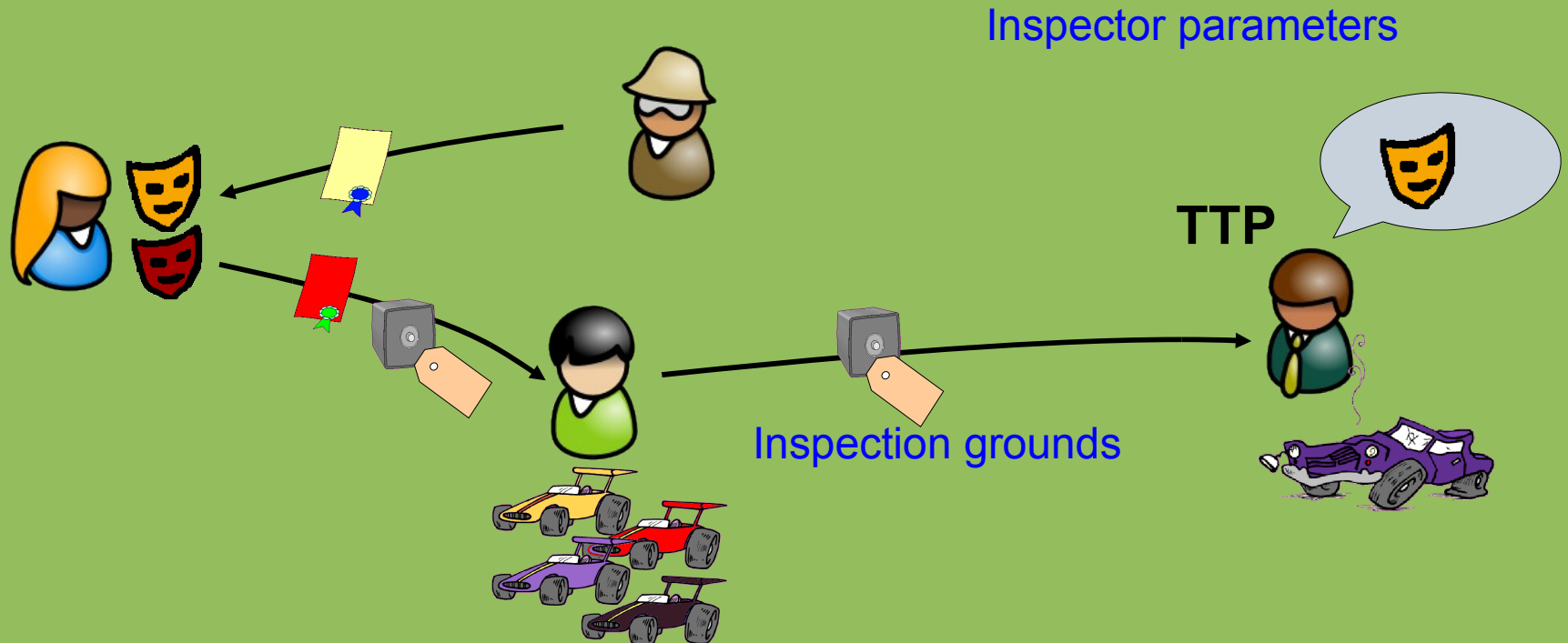
Recall Concepts



A photograph of a beach at sunset. The sky is a mix of orange, yellow, and blue. Waves are breaking on the shore, creating white foam. The sand is dark and has several footprints in it. The text "Further Concepts" is overlaid on the sand in white.

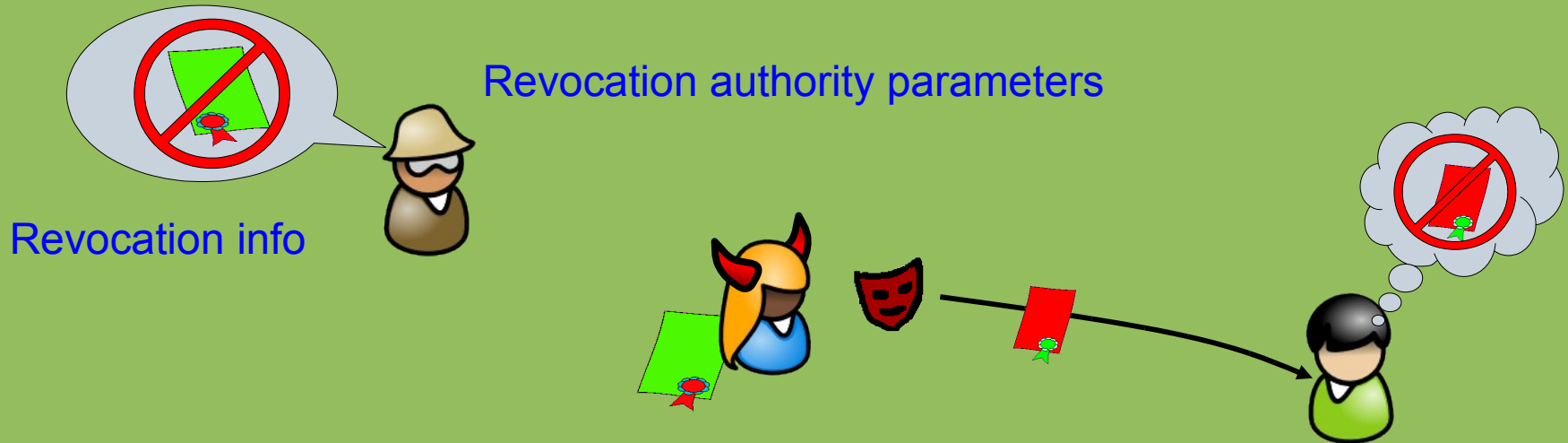
Further Concepts

Concept: Inspection



- If car is broken: ID with insurance needs be retrieved
- Can verifiably encrypt any certified attribute (*optional*)
- TTP is off-line & can be distributed to lessen trust

Concept: Revocation



- 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

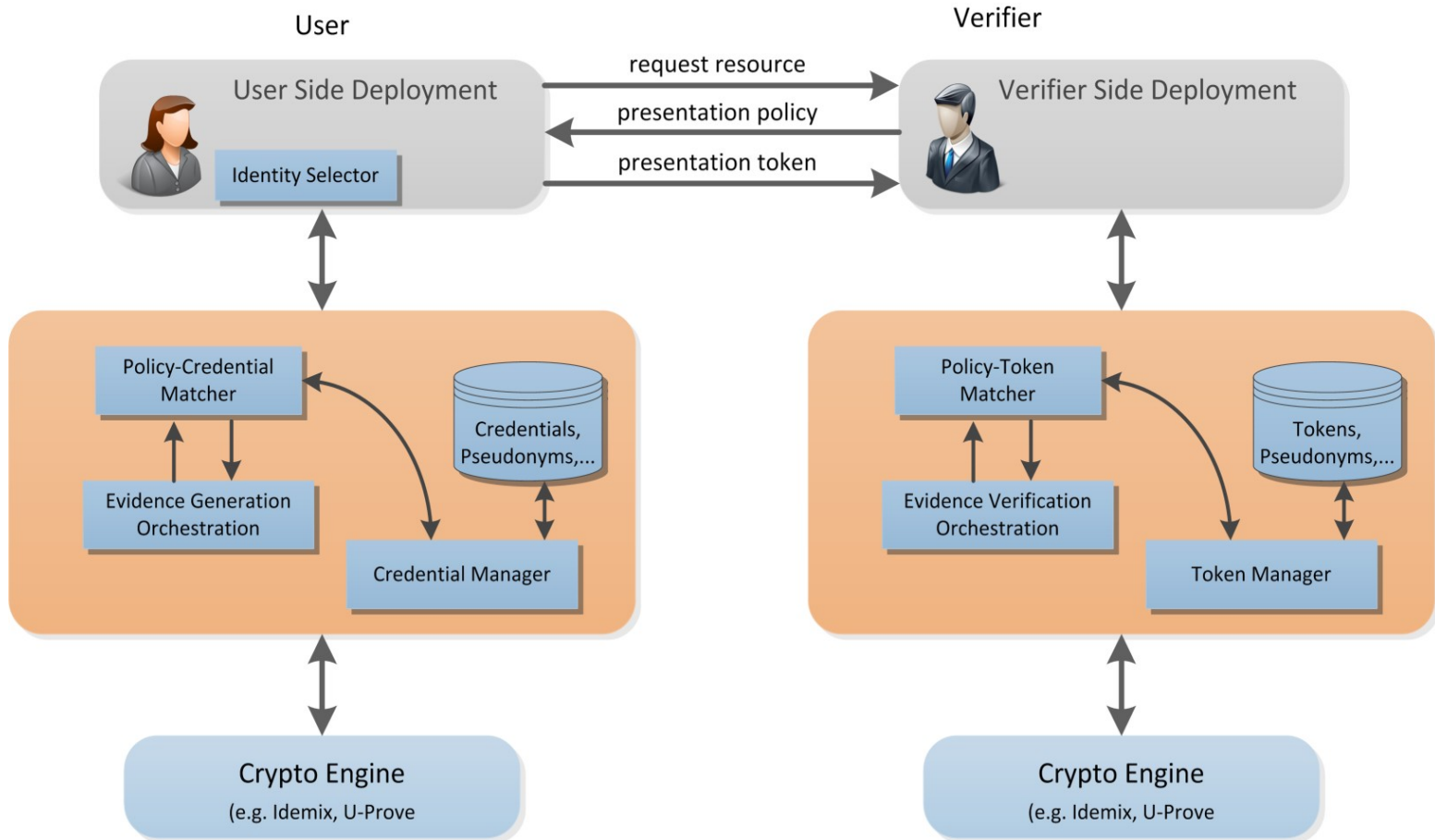
Recall Concepts of Privacy ABCs

- *Credentials* contain attributes, revocation handlers, and (user) secret keys
- *Presentation token*
 - Derived from credential(s), pseudonyms, contains subset of attributes of credentials
- *Key-binding*
 - Issue credential to the same key as another credential or a pseudonym
 - Key can be but does need to be stored on a device such as a smartcard
- *Pseudonyms*
 - Random
 - Scope-exclusive
- *Revocation of credentials*
 - Issuer-driven
 - Verifier-driven (blacklists)
- *Inspection*
 - Only encryption of attribute is contained in presentation token
 - Includes inspection grounds
 - Optional per transaction

A close-up photograph of a sandy beach. The sand is light-colored and has a fine, granular texture. In the upper left quadrant, there is a small, light-colored, elongated shell fragment. In the upper right quadrant, there is a dark, irregular mark on the sand, possibly a footprint or a shadow. The text "Implementation of concepts" is overlaid in the center of the image in a bold, blue, sans-serif font.

Implementation of concepts

User – Verifier: architectural view [abc4trust.eu]



Available on github.com/p2abcengine

A wooden crate filled with books is lying on a grassy field. The crate is tilted, and the books inside are visible. The background is a lush green lawn with some shadows cast by the crate.

It's all about policies

it's all about policies....

different kinds of interaction

- policy authored by businesses

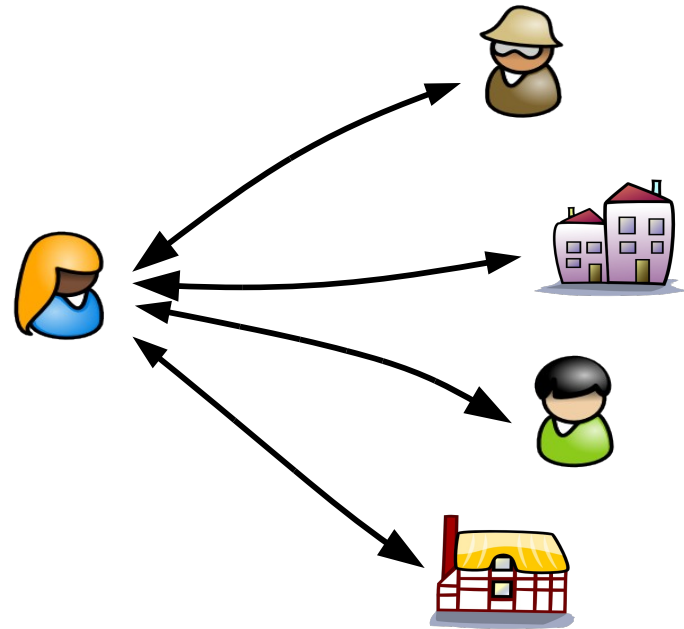
attribute based access control

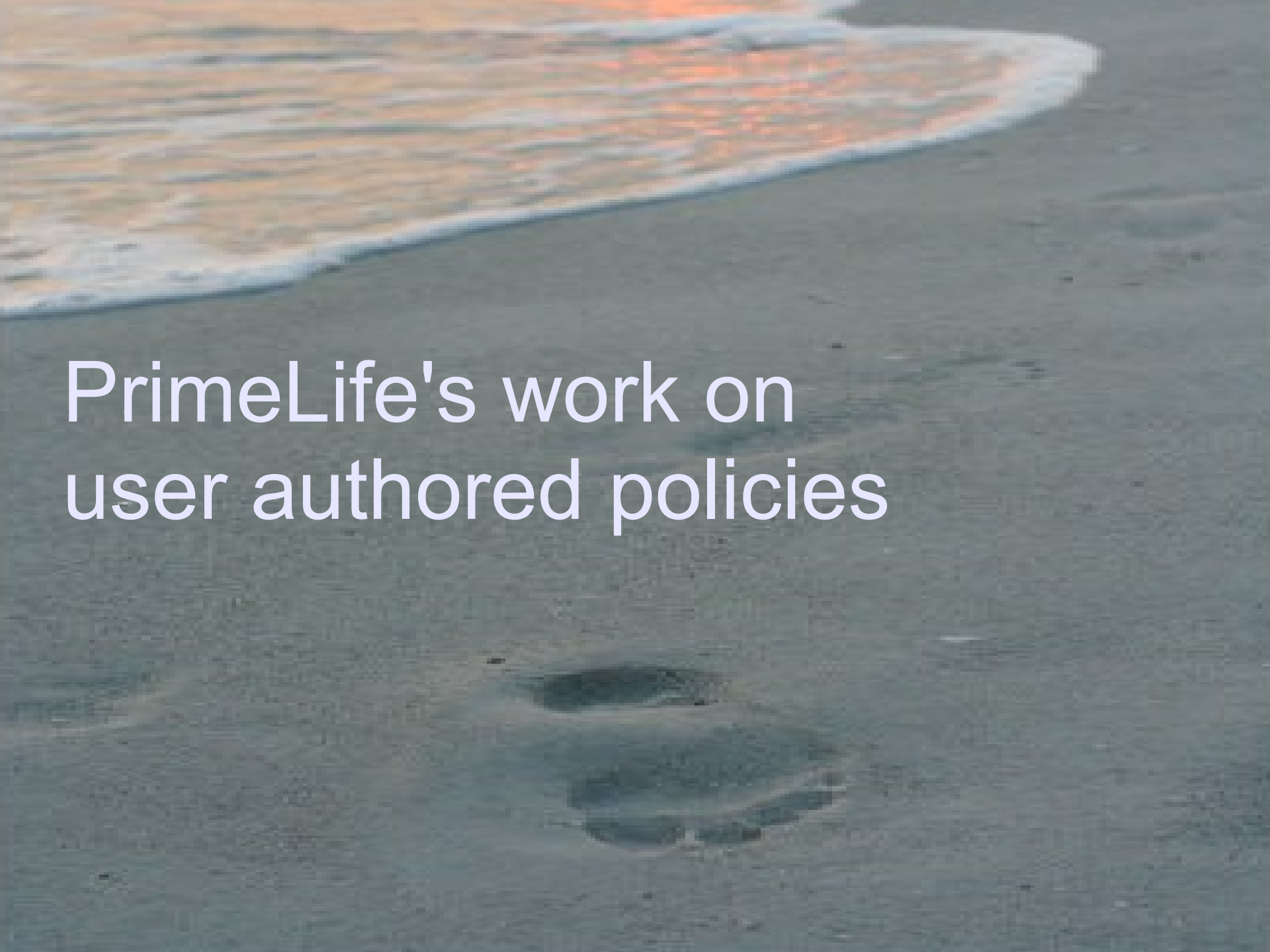
- policy sanitization
- presentation policy
- data handling policies
- downstream usage control
- user's preferences

- policy authored by users (blogs, wikis, etc)

user determines who can access here data

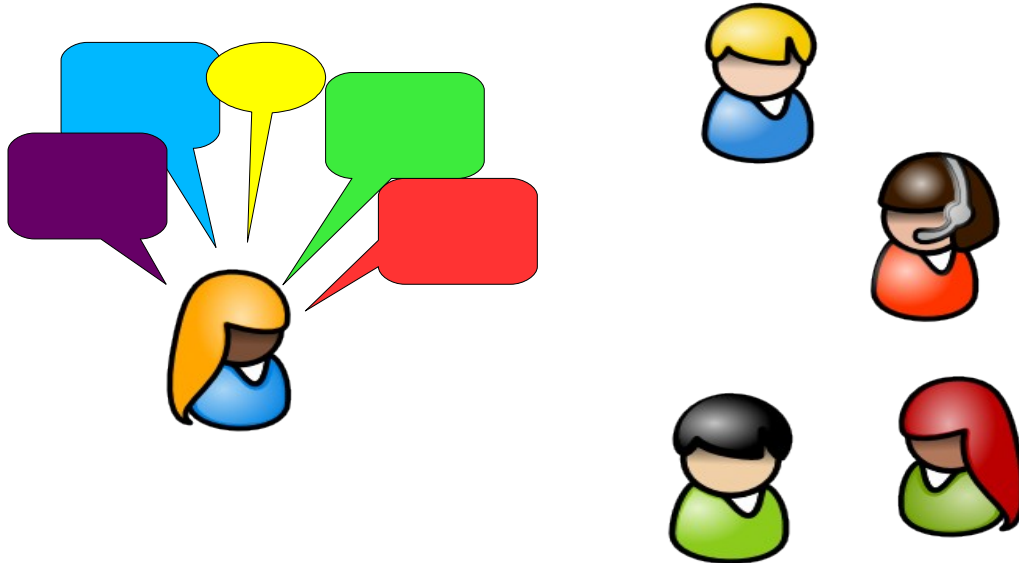
- we need simple languages
- depending on setting



A photograph of a beach at sunset. The ocean waves are crashing onto the shore, creating white foam. The sky is a mix of orange and blue. In the foreground, there is a single footprint in the sand.

PrimeLife's work on
user authored policies

ac for posting on blogs, social networks, etc



- user posts on blogs, social network etc & still wants privacy
- user needs to generate access control policy by herself
- needs to be really simple, fast, dynamic
 - best friends except John
 - all my professional colleagues on project x
- to test this, we build on social network: clique

group your friends

principles:

- collections
- faces
- defaults

The screenshot shows a web browser window with the URL `http://clique.primelife.eu/pg/collections/94`. The page title is "Clique: Contacts collections". The user is logged in as "Bibi van den Berg". The interface features a navigation menu with "Dashboard", "Tools", "Settings", and "Log out". A search bar is also present. The main content area is titled "Contacts collections" and displays a list of collections:

- UvT collega's (10)
- TILT (8)
- PrimeLife (5)
- Studenten TILT (1)

There is a "Save default collection" button at the bottom of the list. On the left side, there is a sidebar for the user "Bibi van den Berg" with options like "Bookmark this", "Report this", "New contacts collection", "Contacts", "Contacts of", and "Invite contacts". At the bottom, there is a "Spotlight" section with a "Welcome to Clique" message and a definition of "clique".

Spotlight

Welcome to Clique

clique [klek; klik]
noun
a small group of people, with shared interests or other feature in common, who spend time together and do not readily allow others to join them.

Information

- PrimeLife
- Elgg open source community

At the bottom of the page, there is a "POWERED BY ELGG" logo and a footer with links for "About", "Terms", and "Privacy", along with the text "Powered by Elgg, the leading open source social networking platform".

adding access control policy

Clique: Upload a file

http://clique.primelife.eu/mod/file/edit.php?file_guid=1808

Google

Who can see this information

Collections and contacts...

Collections

- My best friends
- Friends
- Acquaintances
- Neighbors

Contacts

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z *

A

Allowed contacts

- Friends
- My best friends

Denied contacts

- Sandra
Friends

Private

Contacts

Public

OK


limitations

- allows only for relatively simple policies
 - who can/cannot read
 - no time, purpose, etc possible

- need to fully trust the server of SNS
 - keep data secret
 - implement access control correctly

- how can we overcome the latter?

- btw: clique.primelife.eu

A photograph of a beach at sunset or sunrise. The ocean waves are breaking on the shore, with white foam visible. The sky is a mix of orange, yellow, and blue. In the foreground, a single footprint is visible in the dark sand.

scramble: enforcing audience
segregation by encryption

writing a text on social network

The screenshot shows a web browser window with the address bar containing `http://clique.primelife.eu/pg/file/142/new/`. The browser title is "Clique: Upload a file". The page header features the "clique" logo and user avatars for "Bibi van den Berg" and "biebster", along with an "Add new face" button. A navigation bar includes "Dashboard", "Tools", "Settings", a search box, and a "Log out" link.

The main content area is titled "Upload a file" and contains the following sections:

- File:** A text input field containing "Kies bestand" and a file selection icon next to "IMG_4485.JPG".
- Title:** A text input field containing "Holiday 2009 in Canada".
- Description:** A rich text editor with a toolbar (bold, italic, underline, text color, background color, link, unlink, image, video, HTML) and a text area containing "Here's us white water rafting in Jasper last summer...". A link "Embed / upload media" is visible to the right.
- Path:** A text input field for the file path.
- Tags:** A text input field for tags, with an "Add/Remove editor" link to its right.
- Access:** A section titled "Define access rights" with a link below it.

On the left side, a sidebar for the user "biebster" includes options to "Bookmark this" and "Report this", and a list of file management actions: "Your files", "Your contacts' files", "All site files", and "Upload a file" (highlighted).

encrypt for only your audience to read

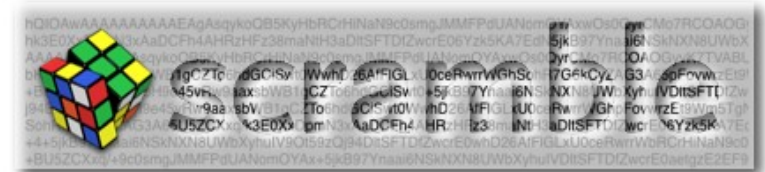
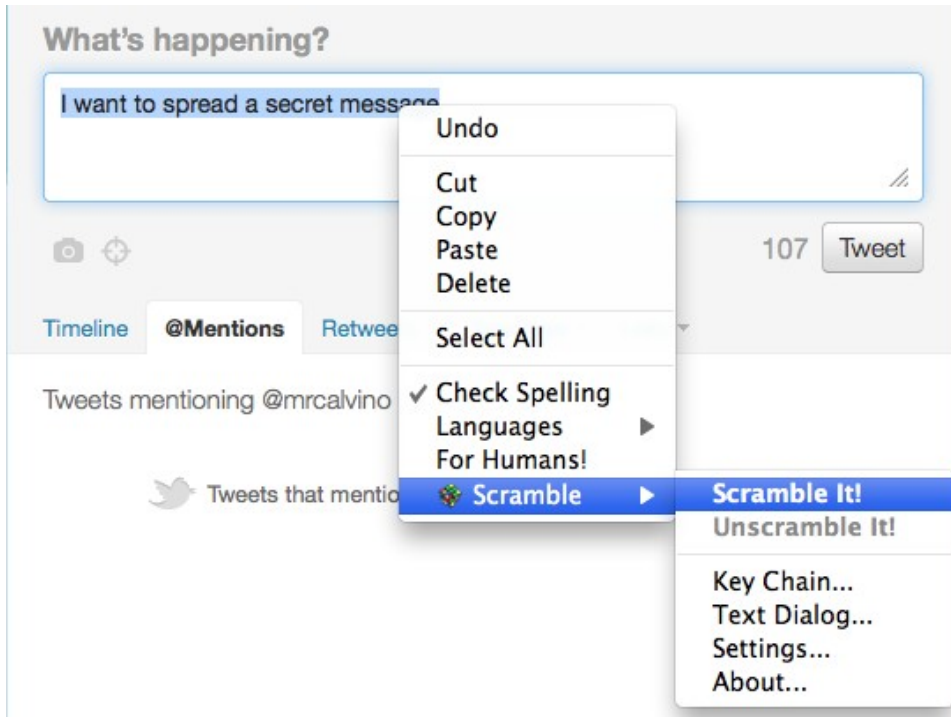
all my friends have pgp/gpg keys, so why not use them? :-)

- what I do
 - encrypt postings under the keys of my friends
 - post encryption on social net
- when my friends read my post, they just need to decrypt...

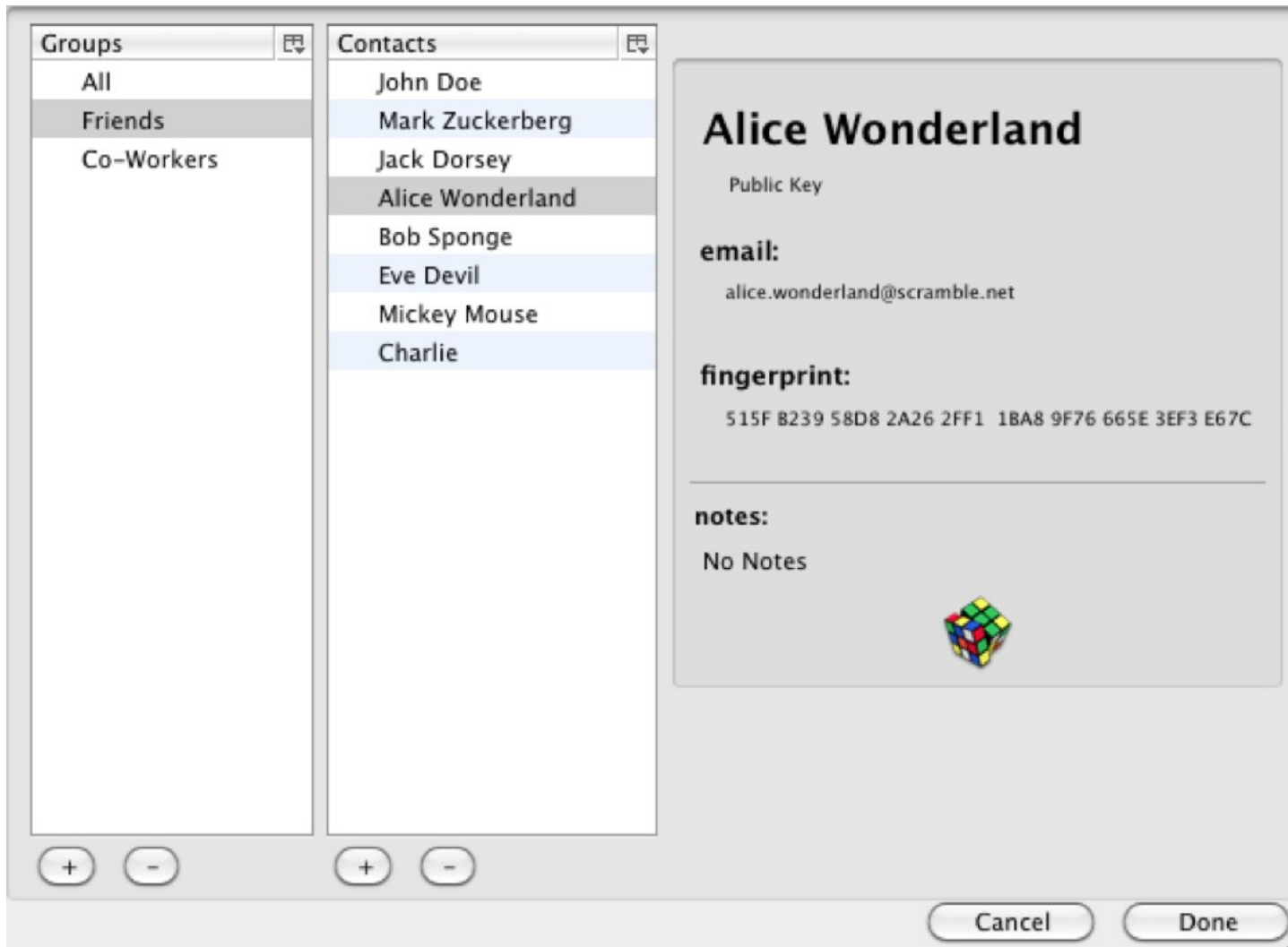
SNS do not allow for encrypted text in input fields:-)

- post encryption on some other server
- post tiny url on social net

scramble – select text you want to control



scramble – select your audience for message



scramble – and here you go: in facebook & twitter

Calvin Hobbes

Wall Info Photos

Write something...

Attach:

Lea Torn -----BEGIN PrimeLife URL-----
<http://tinyurl.com/39otn9f>
 -----END PrimeLife URL-----
 May 4 at 7:36pm · Comment · Like · See Wall-to-Wall

Lea Torn -----BEGIN PrimeLife URL-----
<http://tinyurl.com/3x87onf>
 -----END PrimeLife URL-----
 May 4 at 7:34pm · Comment · Like · See Wall-to-Wall

Calvin Hobbes

Wall Info Photos +

What's on your mind?

Attach: Share

Lea Torn BMW Rocks More
 May 4 at 7:36pm · Comment · Like · See Wall-to-Wall

Lea Torn BMW rocks
 May 4 at 7:34pm · Comment · Like · See Wall-to-Wall

In Facebook

leaprimelife

This is a sample for Scramble

1:59 AM May 5th via web

Windows bug seems to be fixed. well, at least the bug in the windows version of the Scramble! plugin. Windoze as a bug wil never be fixed, I'm afraid :-P

1:20 AM May 5th via web

leaprimelife

-----BEGIN PrimeLife URL-----
<http://tinyurl.com/39nld29> -----
 END PrimeLife URL-----

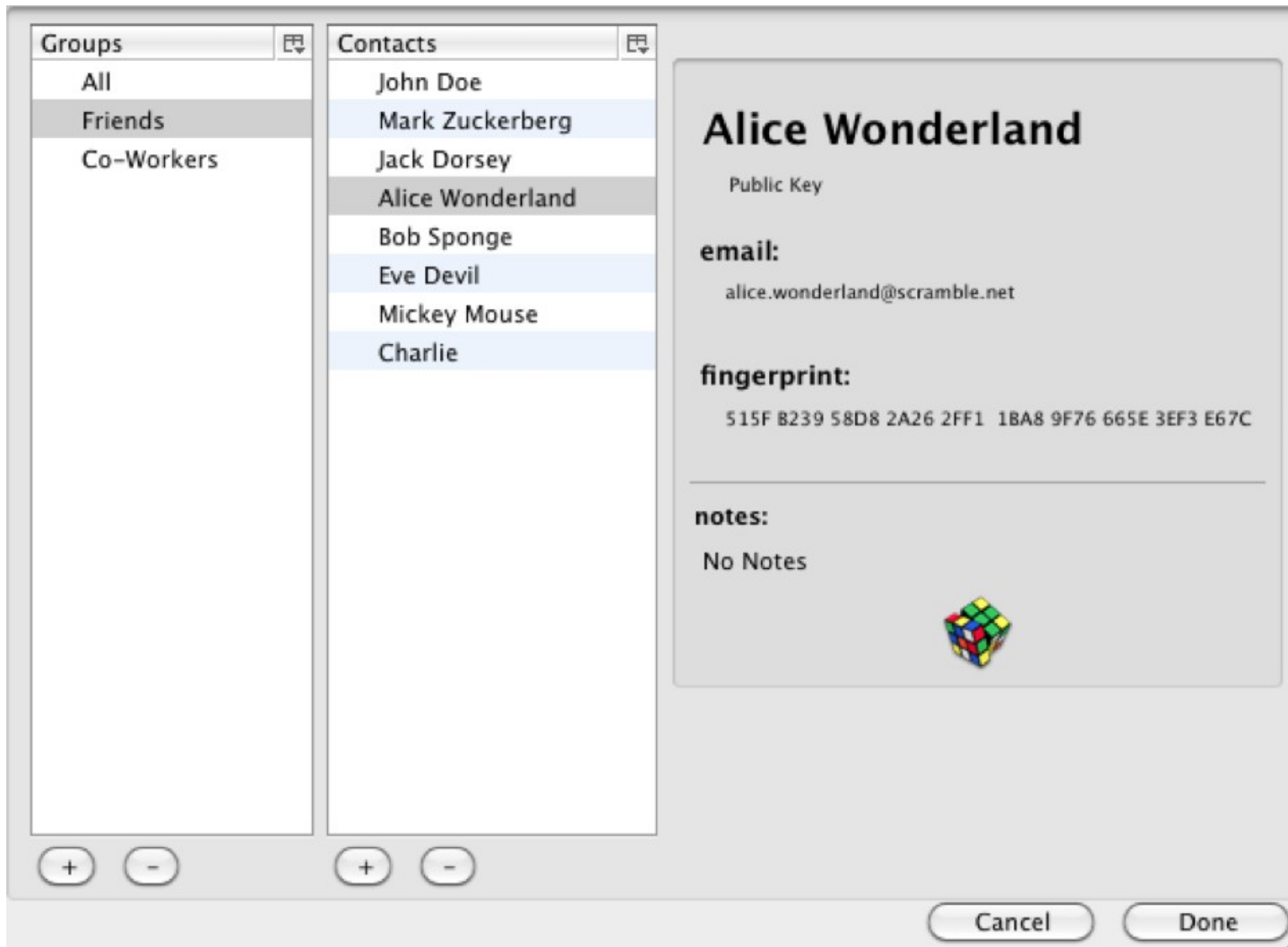
1:59 AM May 5th via web

-----BEGIN PrimeLife URL-----
<http://tinyurl.com/3xxh66g> -----END PrimeLife URL-----

1:20 AM May 5th via web

In Twitter

scramble – select your audience for message



scramble – and here you go: in facebook & twitter

Calvin Hobbes

Wall Info Photos

Write something...

Attach:

Lea Torn -----BEGIN PrimeLife URL-----
<http://tinyurl.com/39otn9f>
 -----END PrimeLife URL-----
 May 4 at 7:36pm · Comment · Like · See Wall-to-Wall

Lea Torn -----BEGIN PrimeLife URL-----
<http://tinyurl.com/3x87onf>
 -----END PrimeLife URL-----
 May 4 at 7:34pm · Comment · Like · See Wall-to-Wall

Calvin Hobbes

Wall Info Photos +

What's on your mind?

Attach: Share

Options

Lea Torn BMW Rocks More
 May 4 at 7:36pm · Comment · Like · See Wall-to-Wall

Lea Torn BMW rocks
 May 4 at 7:34pm · Comment · Like · See Wall-to-Wall

In Facebook



This is a sample for Scramble

1:59 AM May 5th via web

Windows bug seems to be fixed. well, at least the bug in the windows version of the Scramble! plugin. Windoze as a bug wil never be fixed, I'm afraid :-P

1:20 AM May 5th via web



-----BEGIN PrimeLife URL-----
<http://tinyurl.com/39nld29> -----
 END PrimeLife URL-----

1:59 AM May 5th via web

-----BEGIN PrimeLife URL-----
<http://tinyurl.com/3xxh66g> -----END PrimeLife URL-----

1:20 AM May 5th via web

In Twitter

Conclusion



Conclusion

- Roadmap
 - Spreading the word to engineers, policy maker, ...
 - Public infrastructure for privacy
 - Legal framework with more teeth

- Challenges
 - Internet lives on personal information
 - Lift the burden from the users (for all their data)

- Towards as safe digital society
 - Society is shaped by technology increasingly faster
 - Consequences hard to understand
 - Our duty to explain (better) and dialog

Open Research Problems

- Usability – User
 - Visualizing concepts & informed decisions by user
 - Smart cards / NFC
- Usability – Developer, Designer, & Policy Maker
 - Simplify concepts, fool proof use
 - Bridge the gap between theory and practice
- Crypto research
 - Efficient building blocks (smart cards)
 - Different assumption (non random oracles, quantum)

Links

- ABC4Trust.eu
 - EU-funded project with 12 partners
 - universities and industry
 - architecture for anonymous credentials
 - definition of protocols and data formats
 - interoperability of U-Prove and Identity Mixer
 - pilots:
 - school in Sweden
 - university in Greece
 - in case this talk got you interested :-)
 - provides filmed tutorials (see under “events”)

- github.com/p2abcengine

Thank you!

- Email me: jca@zurich.ibm.com
- Links:
 - www.abc4trust.eu
 - www.PrimeLife.eu
 - idemix.wordpress.com
 - www.zurich.ibm.com/idemix