IBM Zurich Research Laboratory

PRIME Architecture

Dr. Susan Hohenberger
PRIME, IBM Research

Privacy and Identity Management for Europe

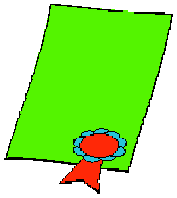
- **Who?**
  - 20 partners from industry, academia, government
- **When?**
  - March 2004 to February 2008
- **How?**
  - 10+ Million Euros from EU and Swiss Federal Office
- **What?**
  - user-controlled, privacy-friendly identity management
- **Where?**
  - https://www.prime-project.eu

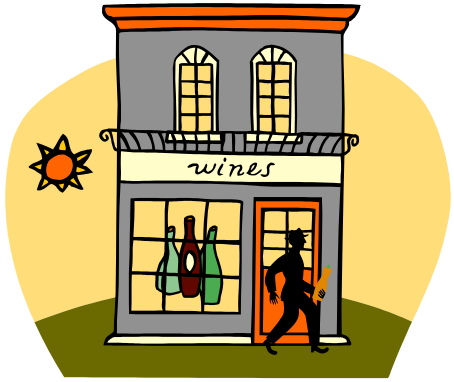
PRIME - what is the problem?

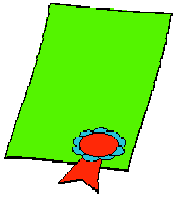
- **Today an excessive amount of personal info is released in day-to-day business.**
- **Surveys show that citizens are worried about:**
  - erosion of privacy
  - identity theft
  - not having a choice about the information they reveal

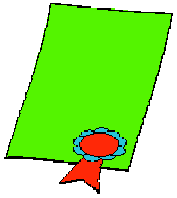
Credentials

User



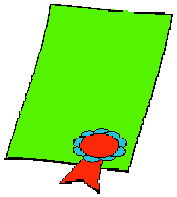


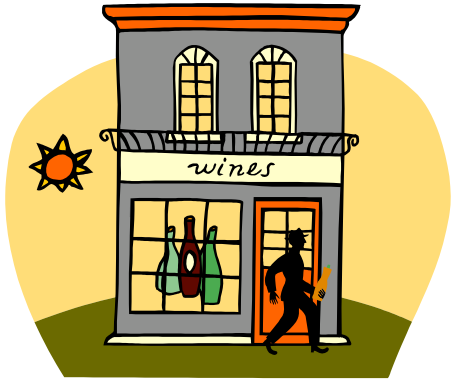
How does the user use  to prove she is over 21?

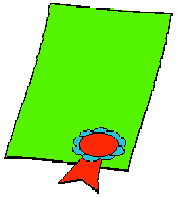
Today's option: release  with birth date, name, address, etc. .....

Credentials

User





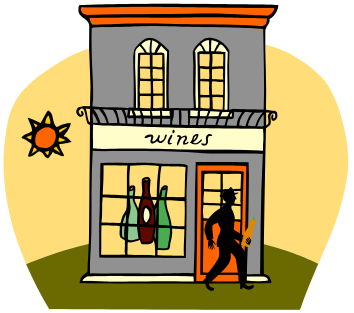
How does the user use  to prove she is over 21?

Better option: user **proves** she has a certificate with a birth date making her over 21 **without** showing it.

Example: zero-knowledge proofs

Prover

I can convince you that I know some information without you learning it.

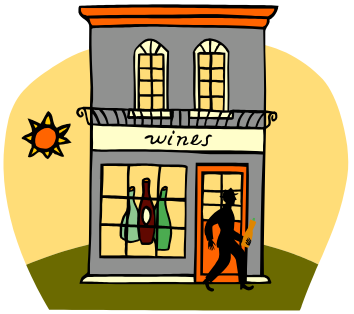


Verifier

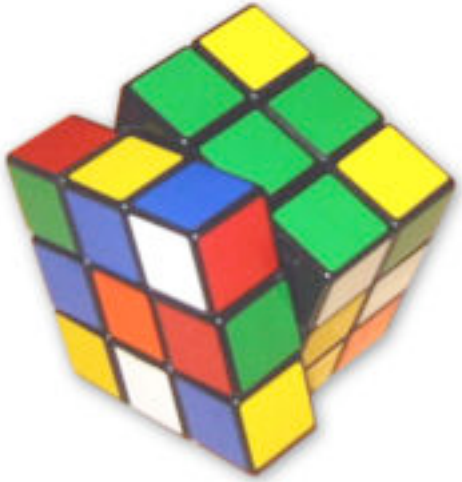
Example: zero-knowledge proofs

Prover

I know the strategy for solving Rubik's cubes!



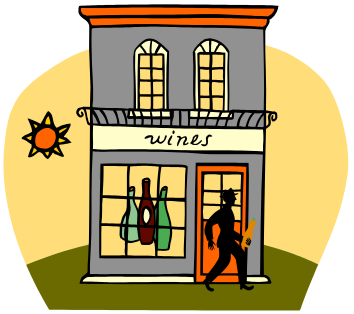
Verifier



Example: zero-knowledge proofs

Prover

I know the strategy for solving Rubik's cubes!

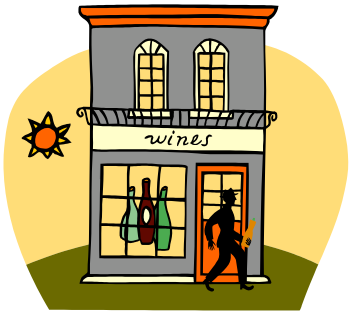


Verifier

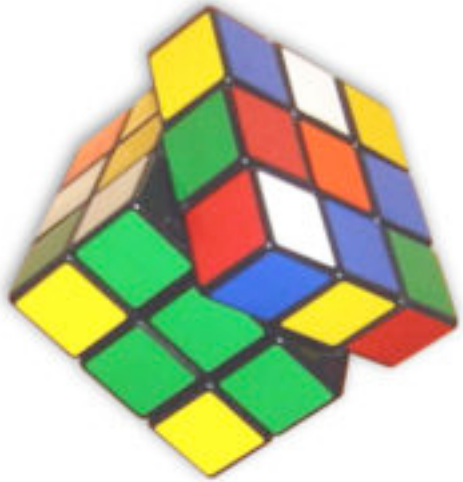
Example: zero-knowledge proofs

Prover

I know the strategy for solving Rubik's cubes!



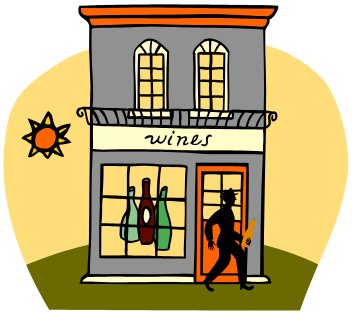
Verifier



Example: zero-knowledge proofs

Prover

I know the strategy for solving Rubik's cubes!

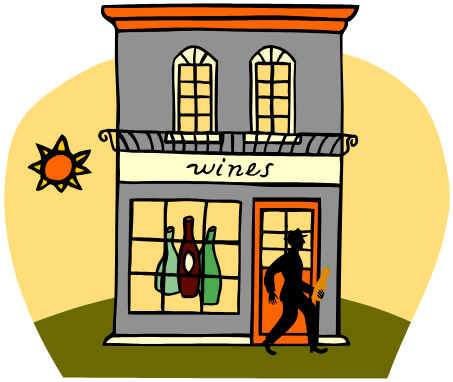


Verifier

[GMW87]: can do such a proof for almost anything.

But how efficiently?

Example: Anonymous Wine Shop



Wine Shop

Proof (age > 21),
enc_K(name, address)

User

enc_K(name, address)

Shipping Company

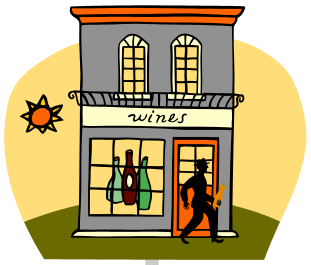
K (public key)

Access Control Policy

"Anonymous user"
Proof of age > 21 AND
Encryption of name & addr with K

"Registered user"
Cryptographic pseudonym

Attribute and Policy Exchange



Resource access

Access control

Assertion request + DHP + Obl

Access control

Release decision

Assertion request 2

Access control

Optional

Assertion & evidence 2

Verification

Access control

Assertion & evidence + DHP' + Obl'

Logging

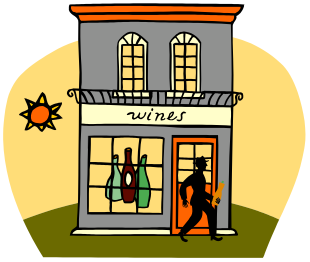
Verification

Access control

Store assertion

Handle DHP, Obl

Credential Handling



Assertion request + DHP + Obl

Session Context

Access Decision

Access Control Policies

Ontologies

Assertion request + DHP + Obl

Access decisions

Assertion Mapping

Credential Storage

Assertions + DHP + Obl

Disclosure Decision & Consent

Transaction History

Assertion + DHP' + Obl'

DHP & Obl Conformance

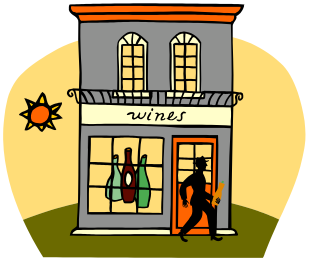
Privacy Preferences

Proof Engine

Assertion & evidence + DHP' + Obl'

Proof Engine

Credential Handling



Assertion request + DHP + Obl

age > 21 ← OECD_Passport AND
enc_K(name, address) ← OECD_PhotoId
OR
pseudonym ← WineShop

Access decisions

Access Control Policies

Ontologies

Assertion Mapping

Credential Storage

Assertions + DHP + Obl

Disclosure Decision & Consent

Transaction History

DHP & Obl Conformance

Privacy Preferences

Assertion + DHP' + Obl'

Proof Engine

Assertion & evidence + DHP' + Obl'

Proof Engine

age > 21 ← SwissPassport AND
enc_K(name, address) ←
SwissDriversLicense

Credential Handling

Assertion request + DHP + Obl

Enc_K(name, address) provided to Shipping Company (Purpose: service)

Data will be retained for 3 years to comply with legal requirements

Access Control Policies

Ontologies

Access decisions

Assertion Mapping

Credential Storage

Assertions + DHP + Obl

Disclosure Decision & Consent

Transaction History

Assertion + DHP' + Obl'

DHP & Obl Conformance

Privacy Preferences

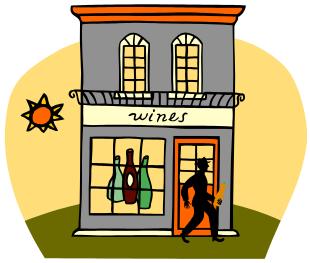
Proof Engine

Assertion & evidence + DHP' + Obl'

Proof Engine

age > 21 ← SwissPassport AND
enc_K(name, address) ← SwissDriversLicense

Data Management



Obligation Manager

Obl

Delete, …

Proof Engine

Controller

enc_K(name, address)

Identity Data Storage

Session Context

Data Handling Policy

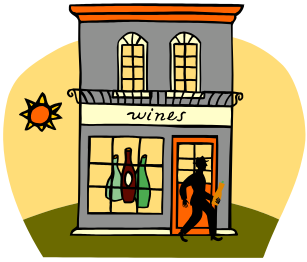
Access Control Policies

age > 21 ← SwissPassport AND
enc_K(name, address) ← SwissDriversLicense

Access Control

User's Request

Access to service requires:
age > 21 ← OECD_Passport AND
enc_K(name, address) ← OECD_PhotoId
OR
pseudonym ← WineShop



age > 21 ← SwissPassport AND
enc_K(name, address) ← SwissDriversLicense

Session Context

Access Decision

Access Control Policies

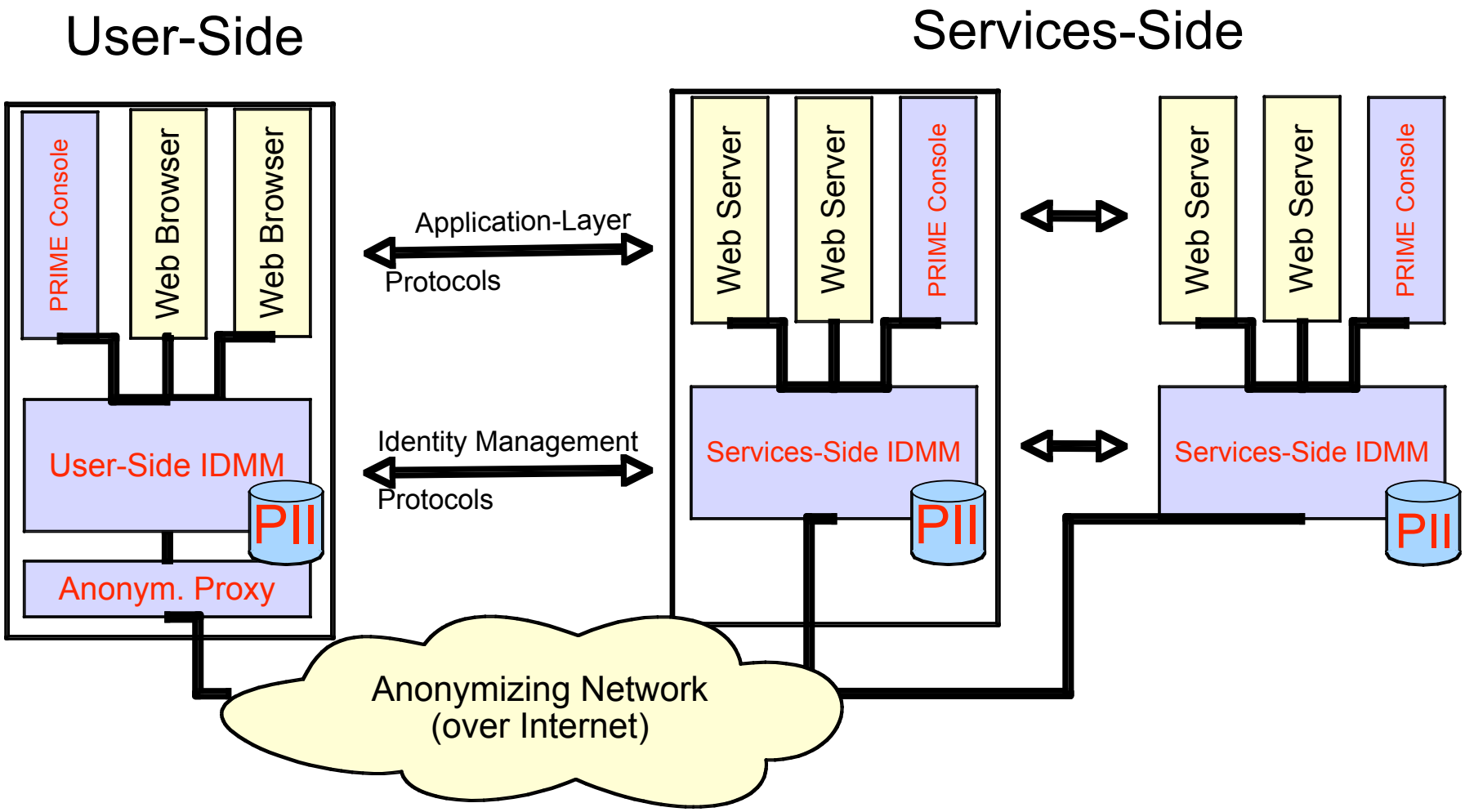
Ontologies

SwissPassport is an OECD_Passport
USPassport is an OECD_Passport
SwissDriversLicence is an OECD_PhotoId

Access decision
grant / deny / assertion request

Grant access!

PRIME Architecture



Conclusion

- **PRIME covers private identity management**
  - Access control and privacy policies
  - Trust negotiation
  - Privacy-enhancing identity federation (idemix)
  - Privacy obligations
  - Assurances

https://www.prime-project.eu

Susan Hohenberger

sus@zurich.ibm.com