The FutureID approach to interoperable, cross-border digital identity

Fraunhofer

Newcastle University

Radboud University Nijmegen

KU LEUVEN

Infineon

Atos

TU Graz

Universität Stuttgart

DTU

eema

esec

TECHNISCHE UNIVERSITÄT DARMSTADT

COMARCH

IBM

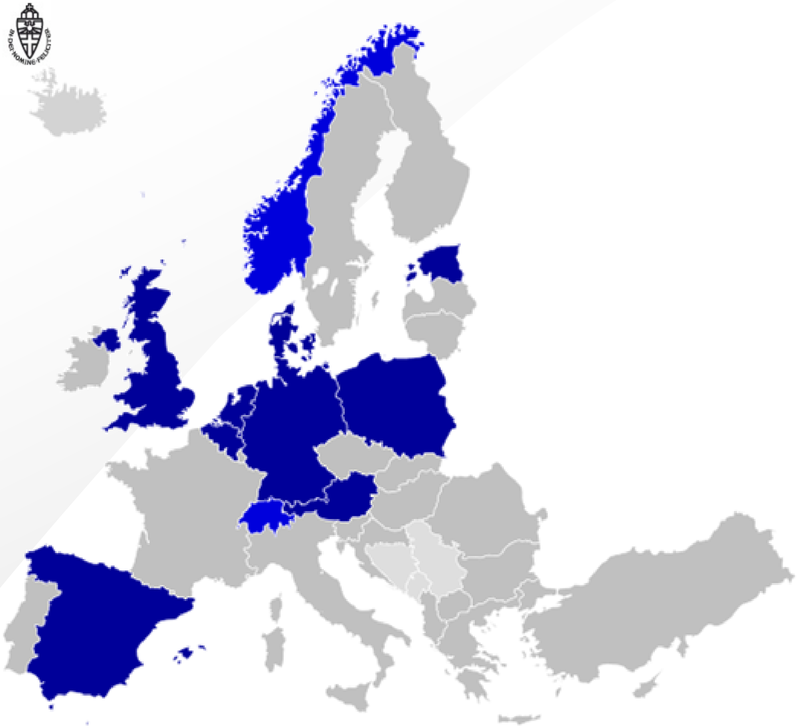
AGETO

SK

ULD

Giesecke & Devrient
Creating Confidence.

NR Norsk Regnesentral
NORWEGIAN COMPUTING CENTER



AFSecurity Seminar

17 September 2014, University of Oslo, Norway

Bud P. Bruegger, Fraunhofer IAO

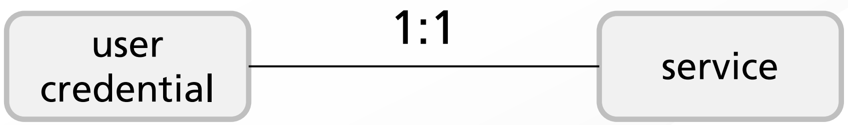
FutureID is partly funded by EU FP7 under GA n°318424

Agenda

- Motivation
- Decentralized Identity Management Ecosystem (DIME)
- The Authentication Process
- User Control and Privacy

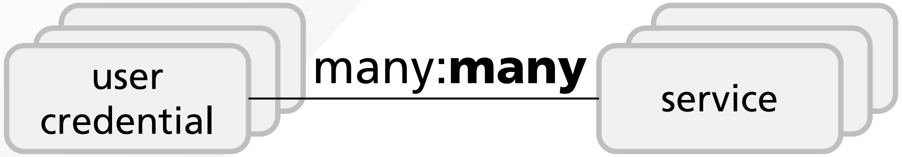
Social Media:
a Paradigm Shift in Identity Management

Before:



- Service Providers issue/manage identity
- Users obtain/manage one identity per service

Social Media:



- Service Providers reuse 3rd Party identities
- Users reuse their existing identity for new services

Benefits:
Service Providers

Identity Management is outsourced to social media operators

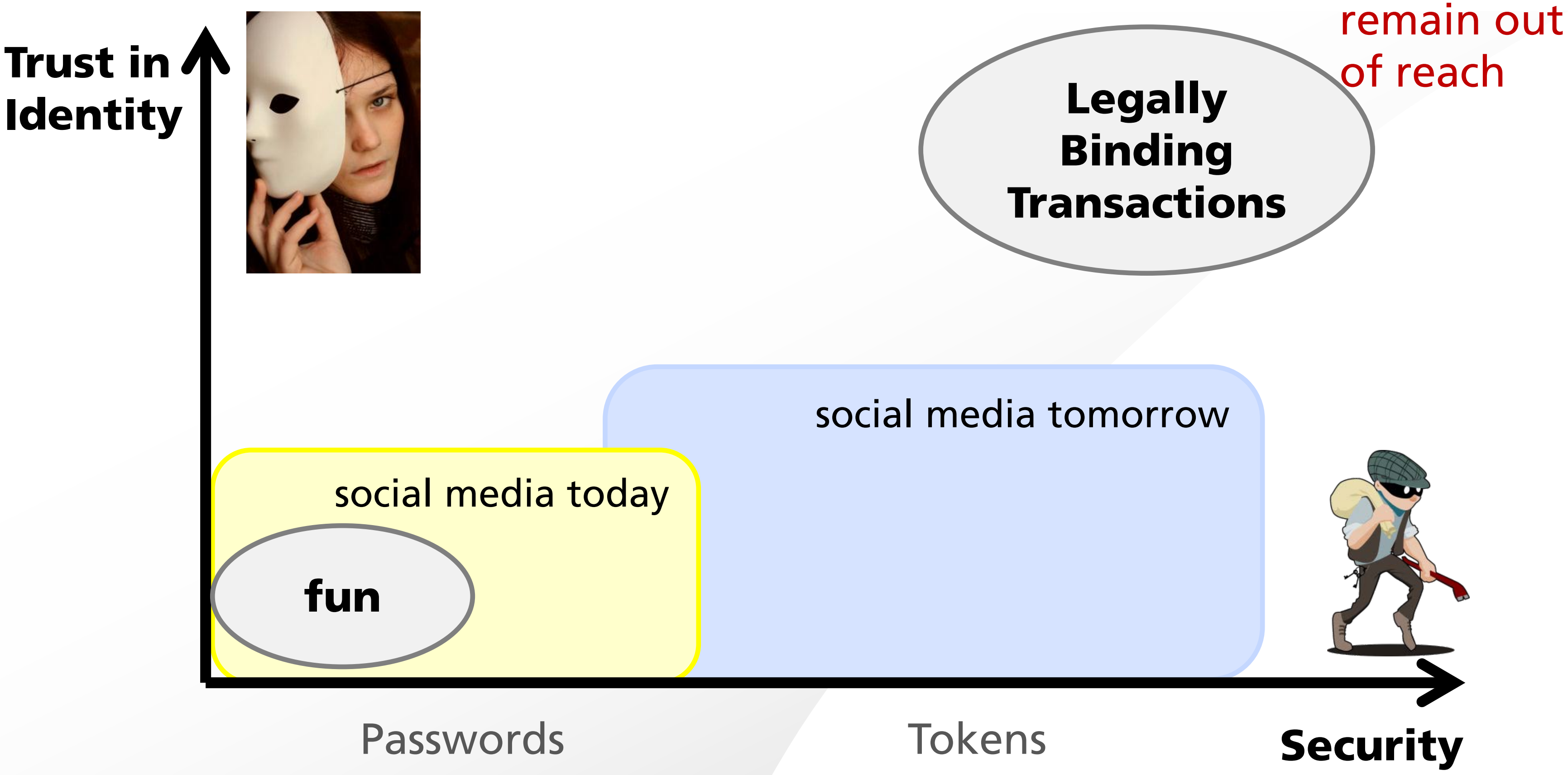
	Before	Social Media
Registration	X	--
Support (lost password)	X	--
Securing Password Store	X	--
Cost per User	**High**	**Very Low**

Benefits:
Users

	Before	Social Media
Register	for every Service	--
Remember Password	for every Service	--
Recover Password	often (remember many different Passwords)	rarely
Cost per Service	**High**	**Almost Zero**

FutureID is partly funded by EU FP7 under GA n°318424

“Social Identities” have a limited Domain of Application



Trust in Identity

remain out of reach

Legally Binding Transactions

social media tomorrow

social media today

fun

Passwords

Tokens

Security

FutureID is partly funded by EU FP7 under GA n°318424

Trusted and Secure Identities exist, but are locked into the old paradigm

Single service,
significant effort,
not worth while!

Too costly,
too small user base,
maximum one type
if really necessary

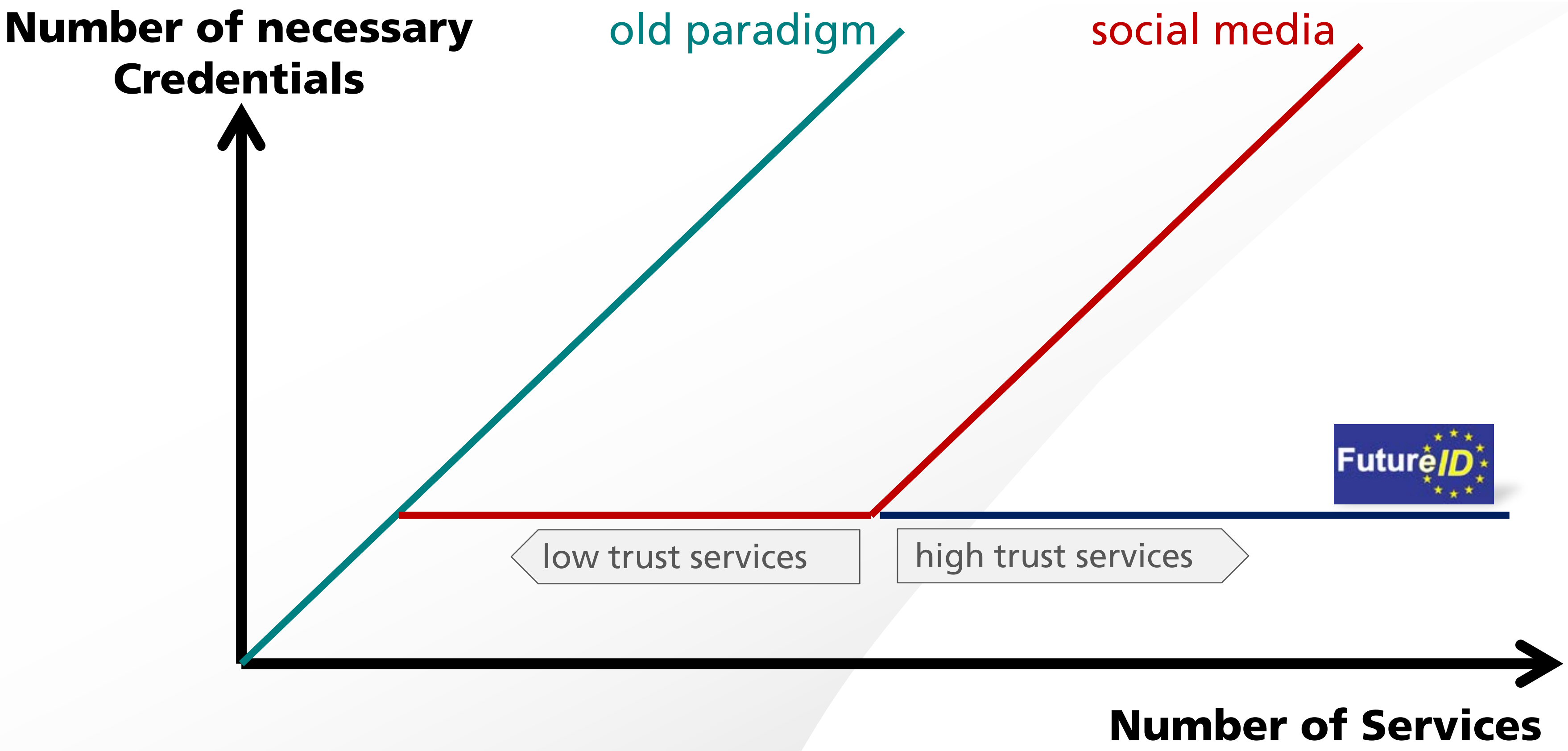
User

Service Provider

How can trusted identities be used with the new paradigm?

FutureID is partly funded by EU FP7 under GA n°318424

Objective for User



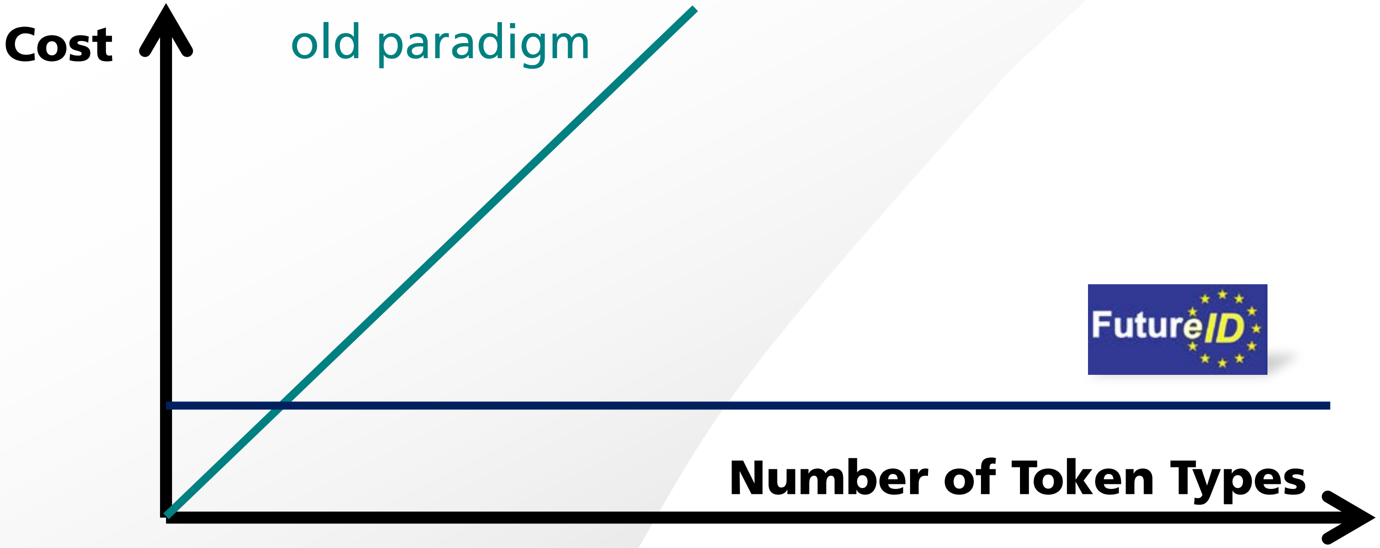
FutureID is partly funded by EU FP7 under GA n°318424

Objective for Service Provider

- The targeted user base has many different existing secure token types.
  - Example: European Marketplace of Services

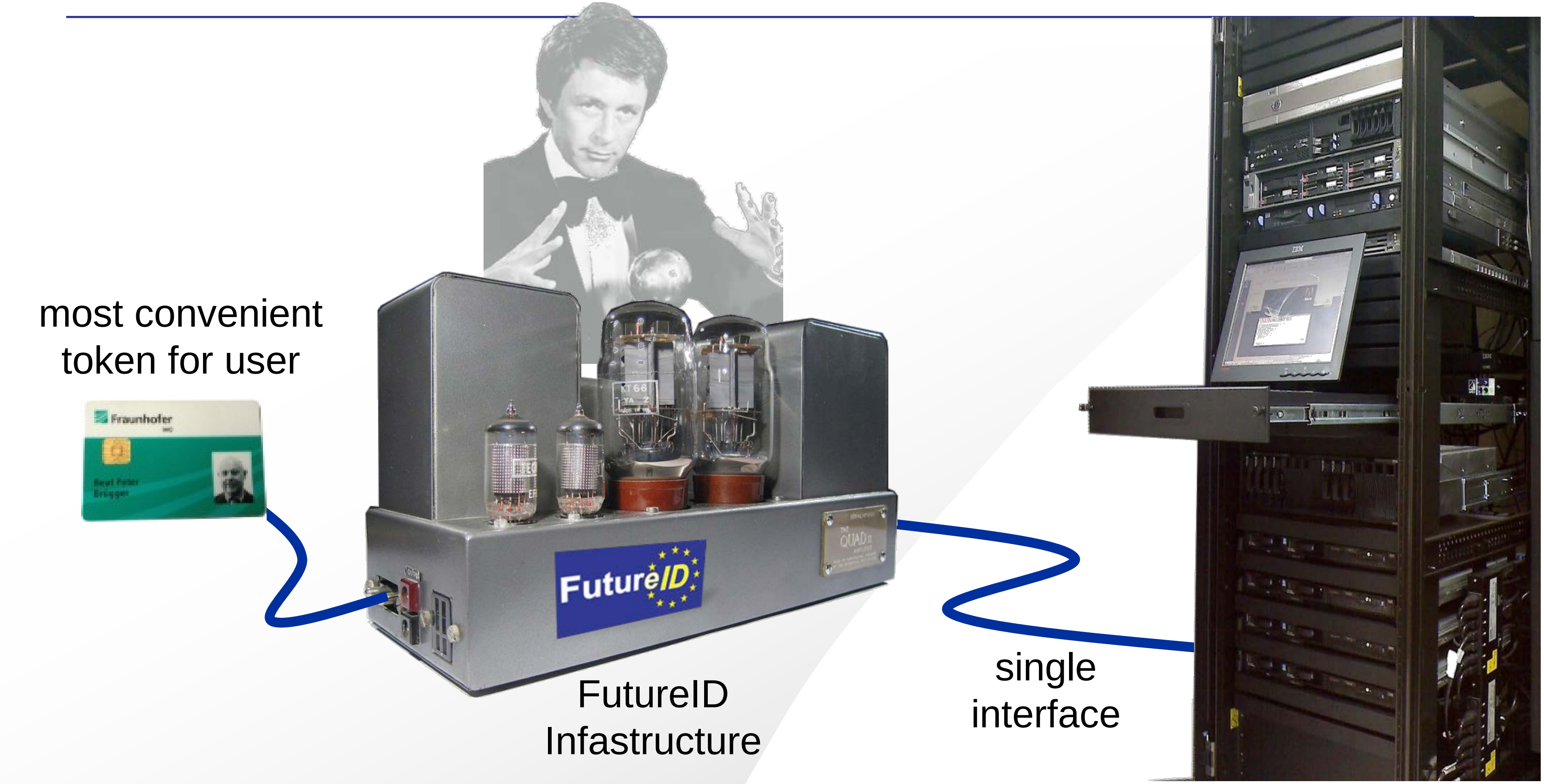
    Many different national eIDs

- The cost of supporting a large number of token types must be contained.



FutureID is partly funded by EU FP7 under GA n°318424

How?: Transformer that matches any ID to any Service



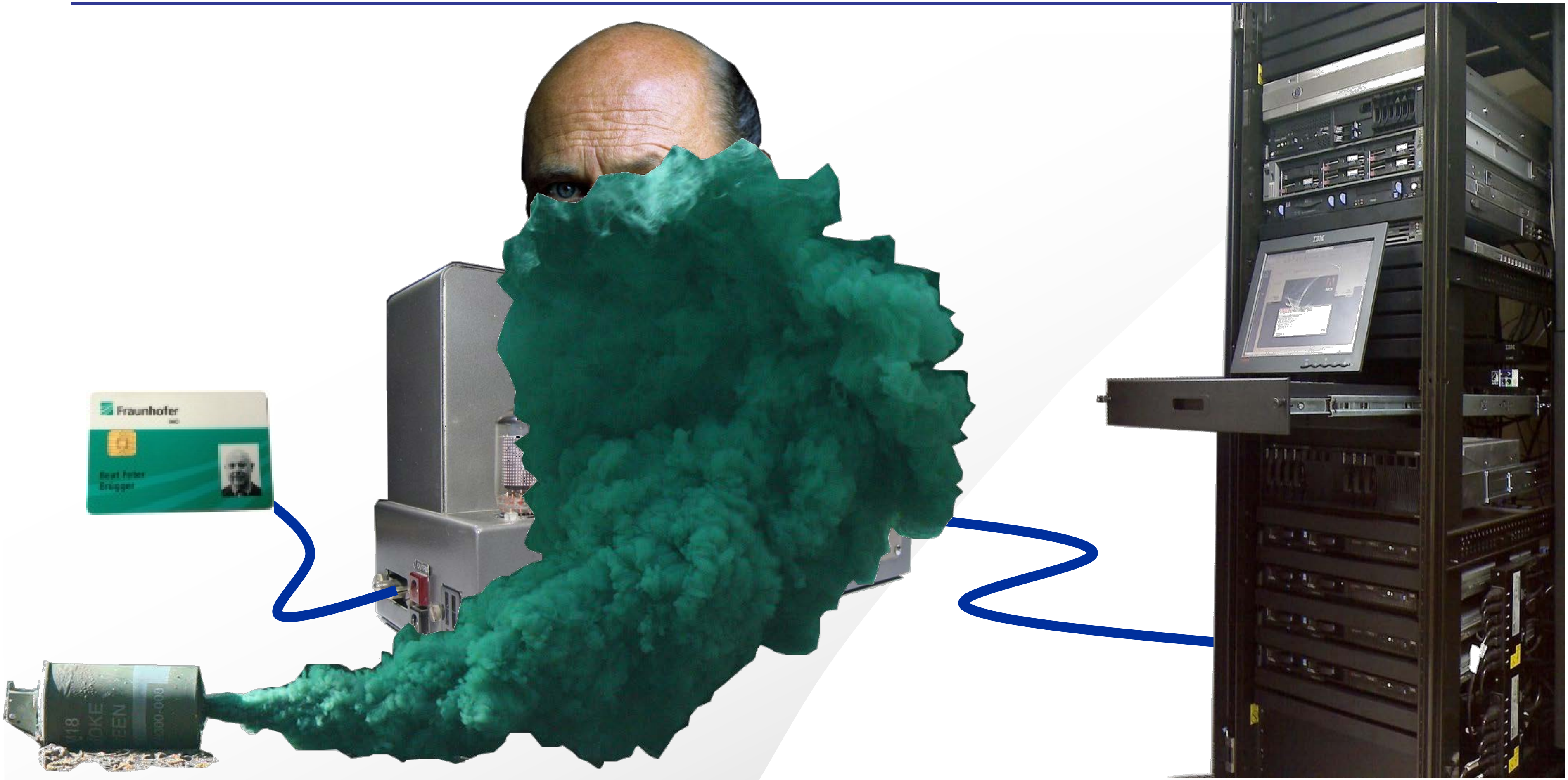
most convenient token for user

FutureID Infastructure

single interface

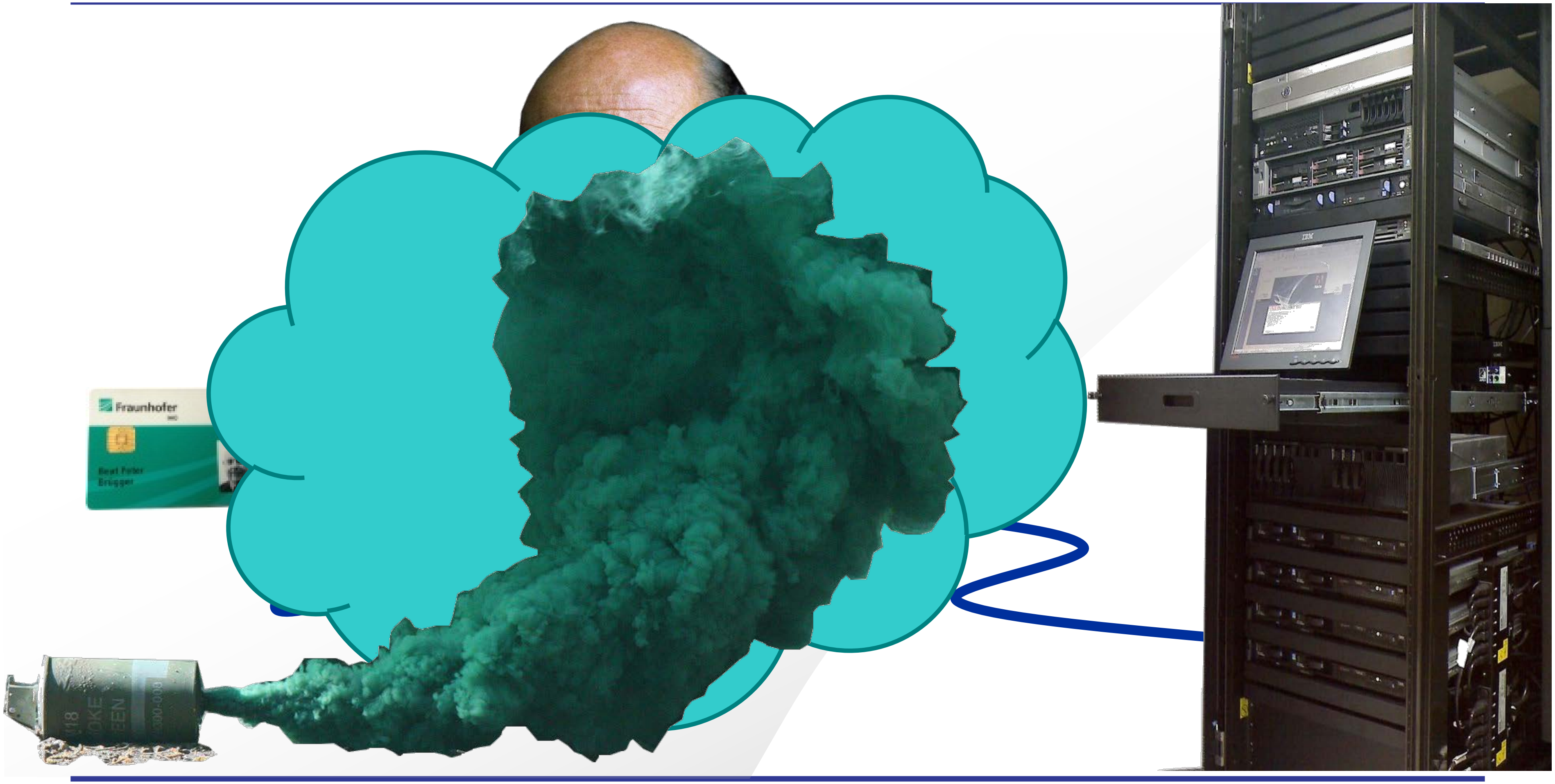
A Centralized Infrastructure would create a Big Brother

We need Privacy Counter Measures



FutureID is partly funded by EU FP7 under GA n°318424

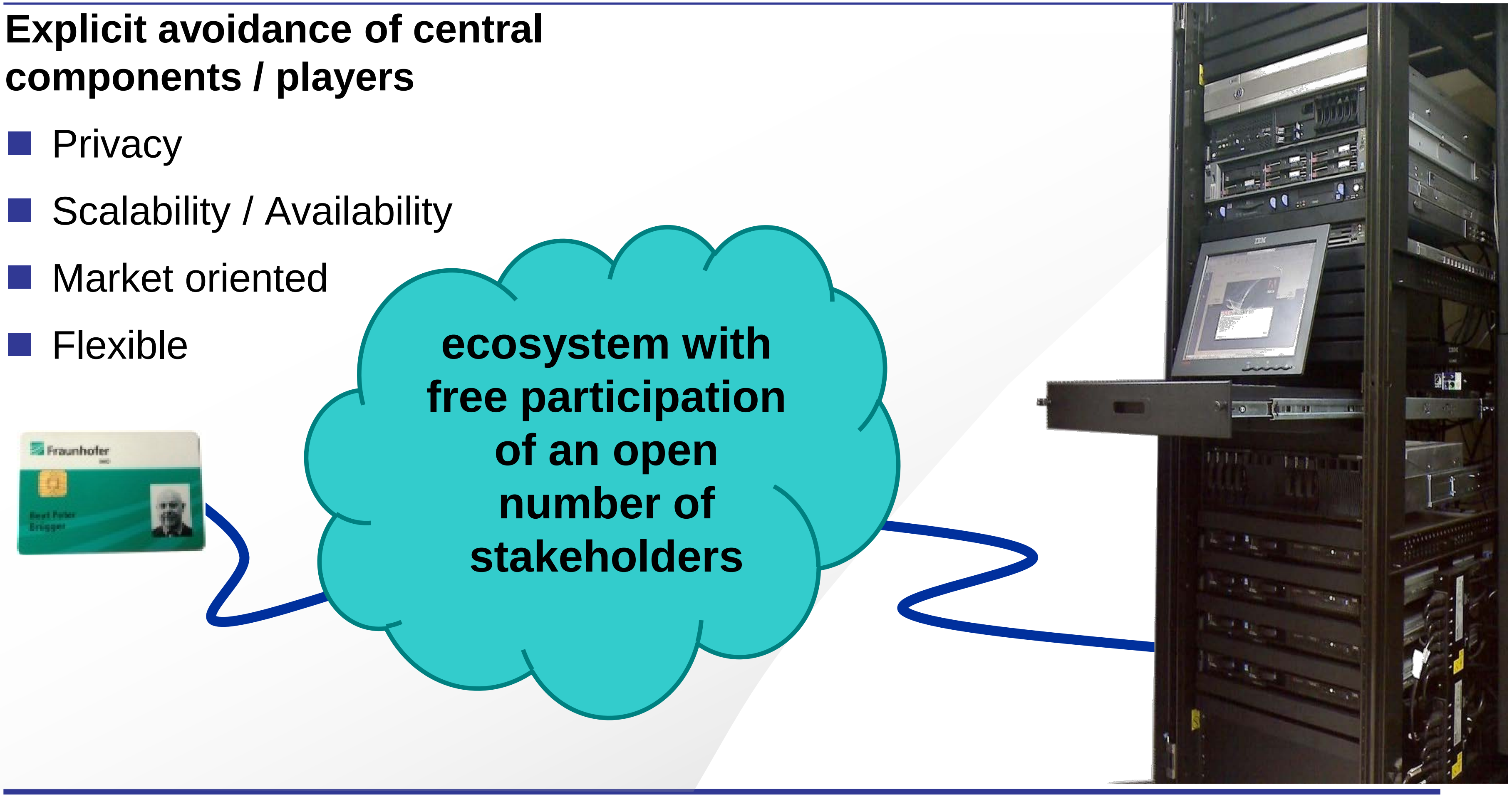
We need Privacy Counter Measures



A Better Design: Decentralized and User-Centric

Explicit avoidance of central components / players

- Privacy
- Scalability / Availability
- Market oriented
- Flexible



ecosystem with free participation of an open number of stakeholders

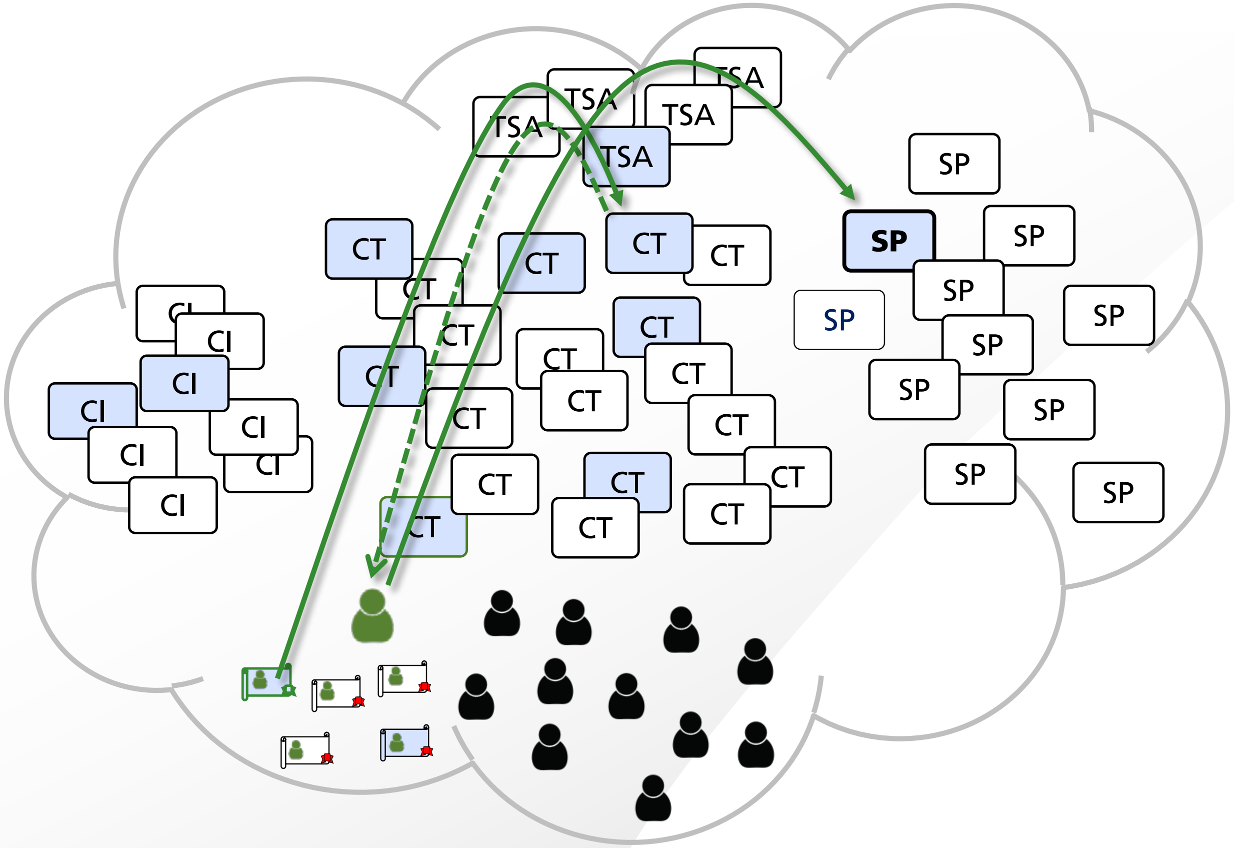
Decentralized Identity Management Ecosystem -- DIME

- Service Providers use identity services to amplify their outreach to users
- Free market for identity and trust services:
  - Competition of multiple vendors
  - Vendors can adapt to their market
    - Legislation
    - Language
- Multiple trust-schemes can co-exist and be combined in SP’s policy
- Only centralized component: existing Domain Name System
    - Global registry of unique names
    - Locate services from global root
  - Trust Infrastructure explicitly DNS-based

FutureID is partly funded by EU FP7 under GA n°318424

The FutureID Infrastructure Overview

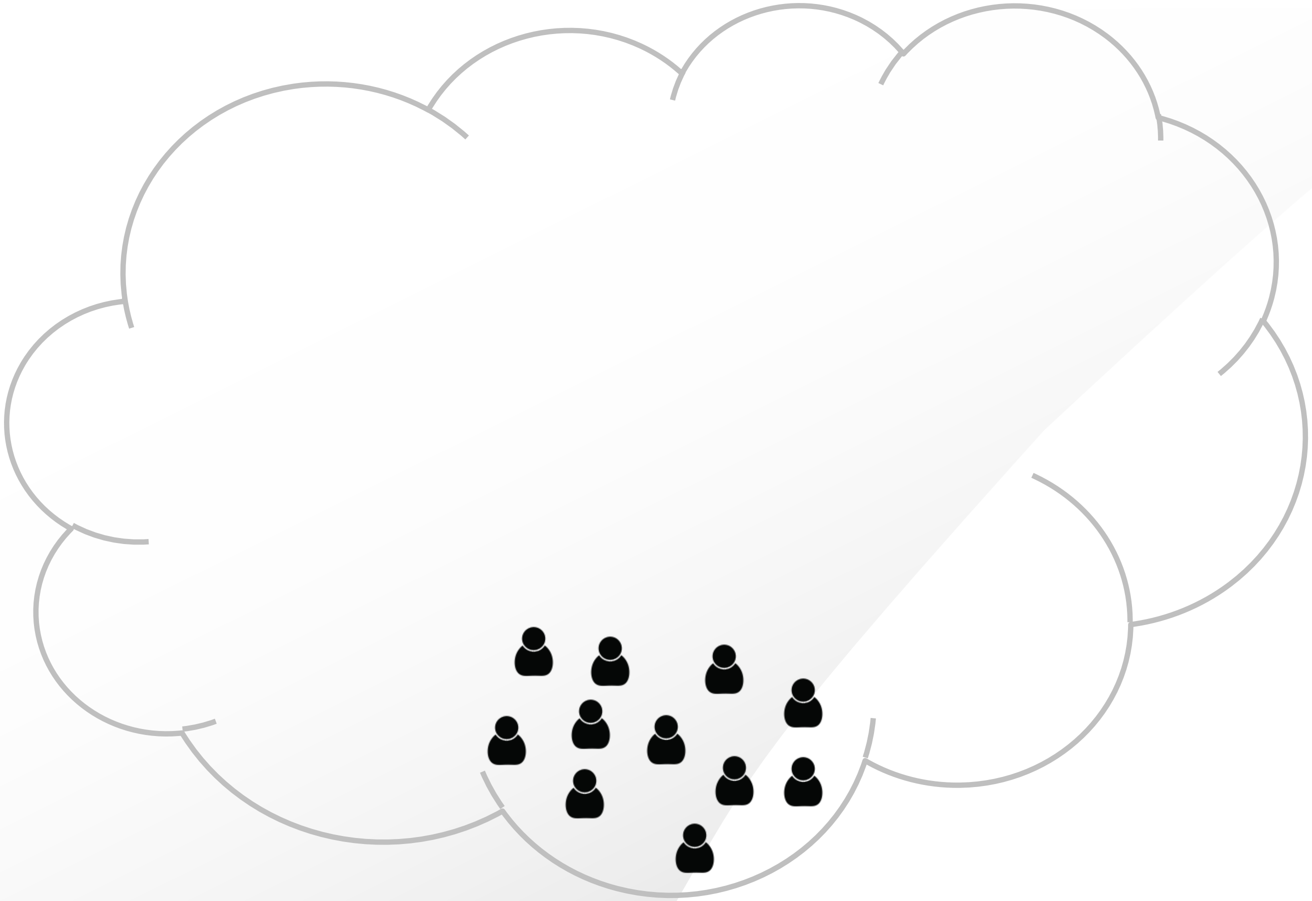
A Decentralized Identity Management Ecosystem -- DIME



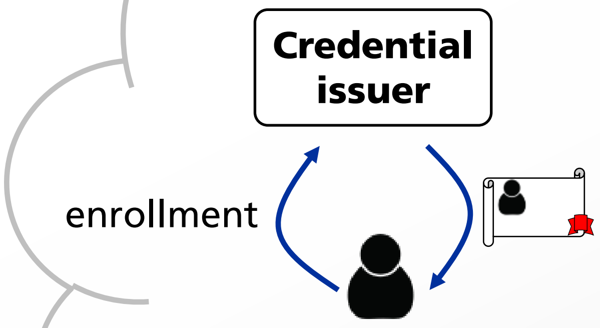
Free participation of an open number of stakeholders

FutureID is partly funded by EU FP7 under GA n°318424

Users



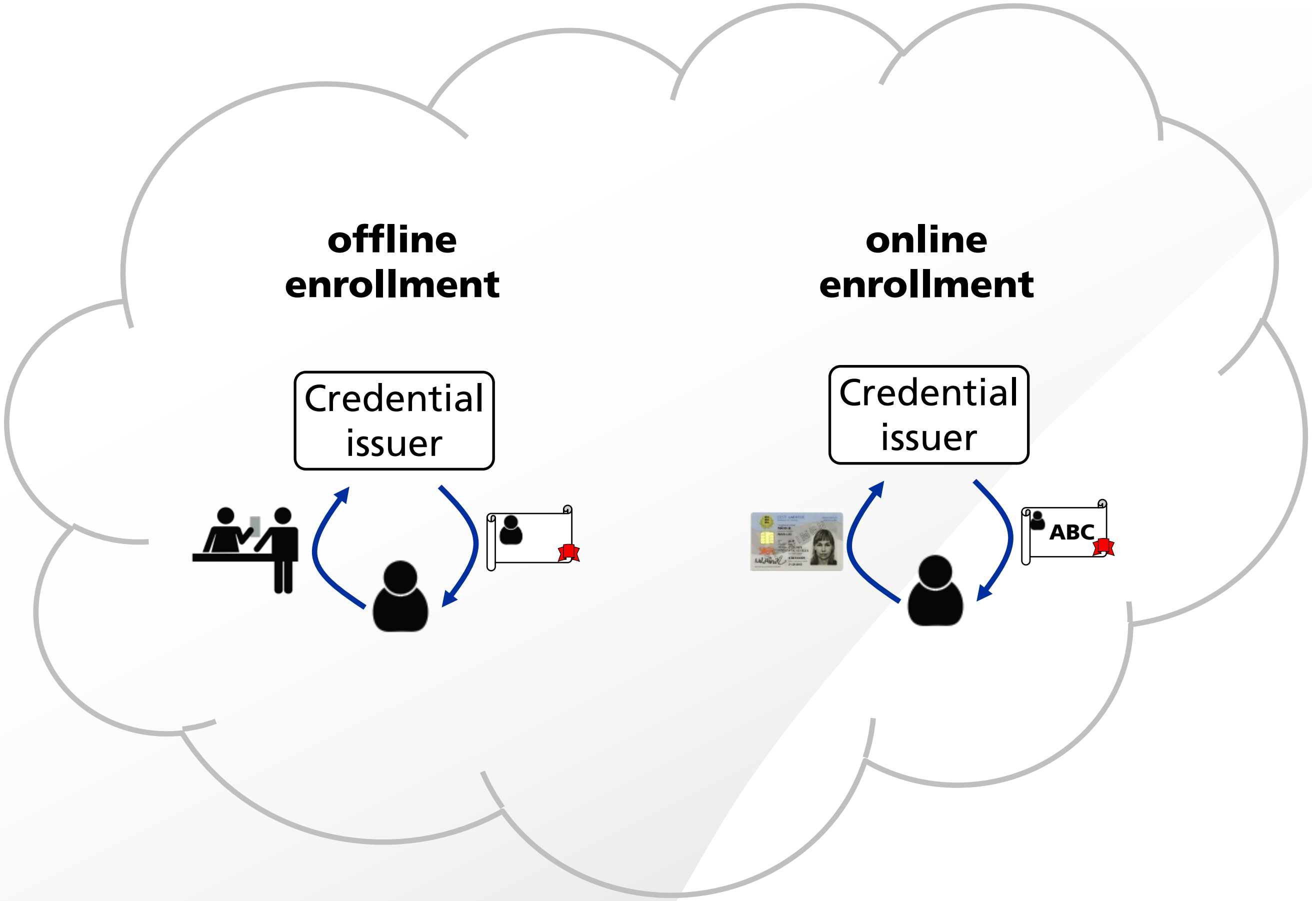
Credential Issuers (CIs)



Arbitrary credential technology:

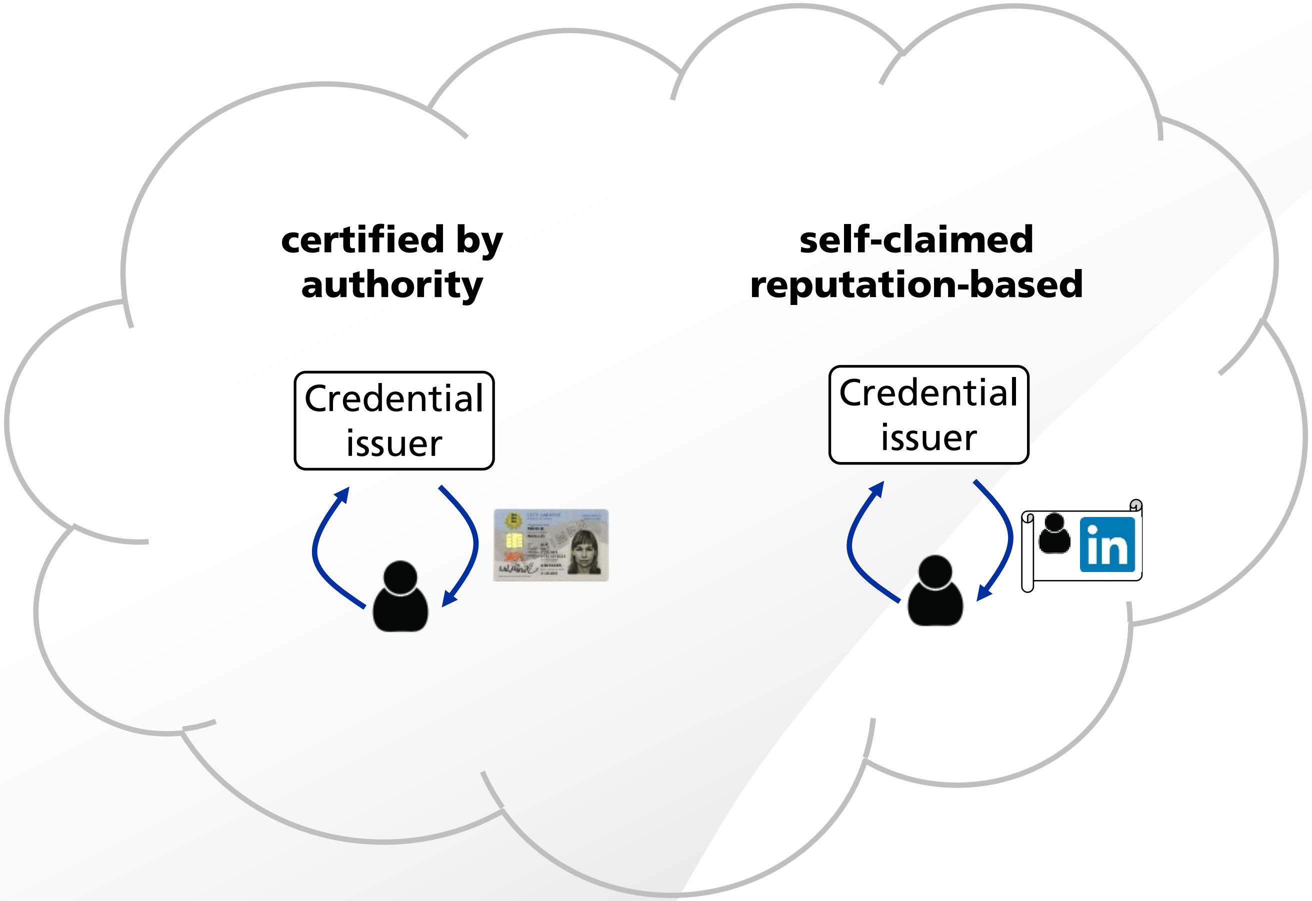
- password
- one-time pad
- OTP device
- smart card
- privacy-ABC
- mobile
- etc.

Types of Enrollment



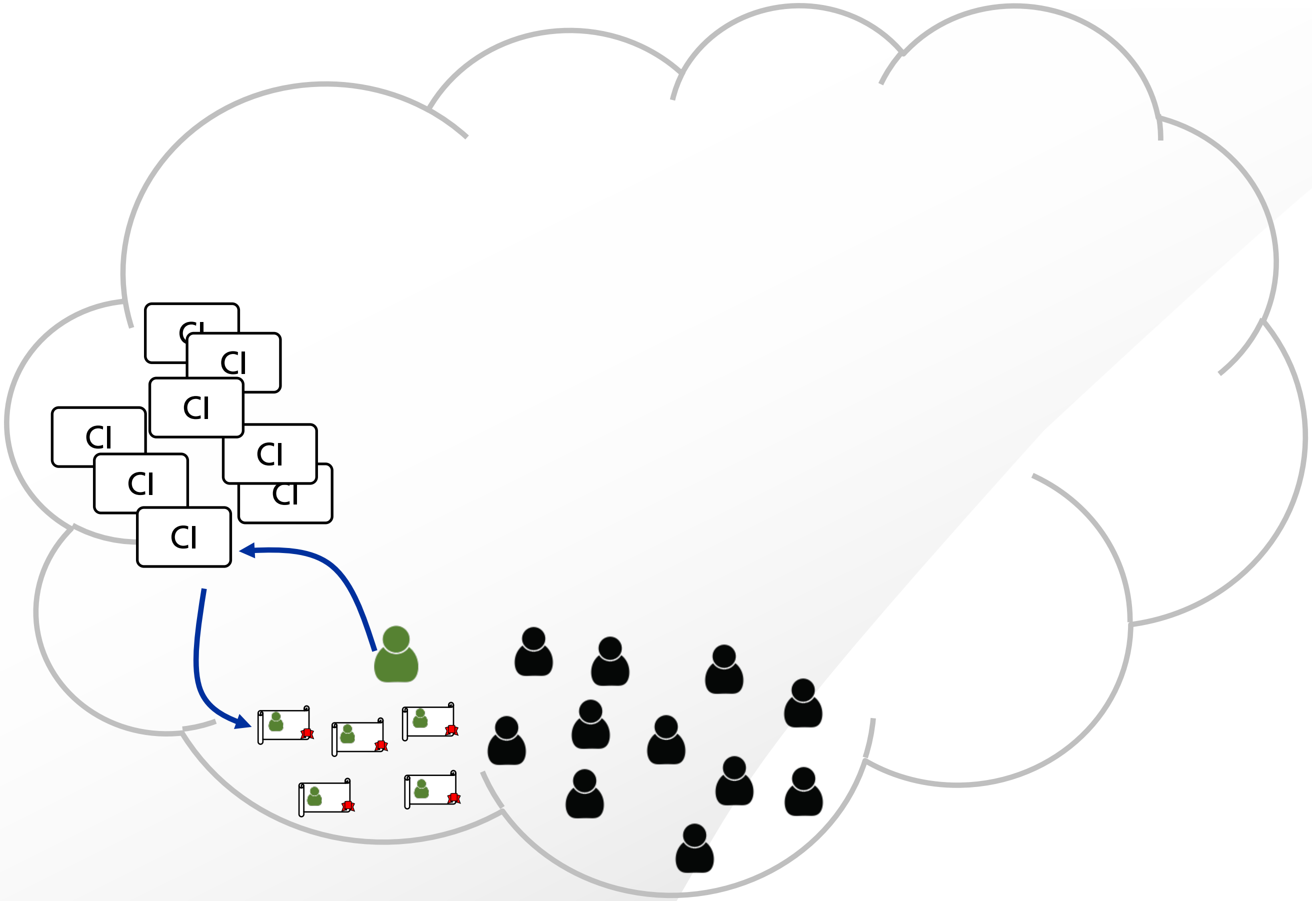
FutureID is partly funded by EU FP7 under GA n°318424

Types of Identities

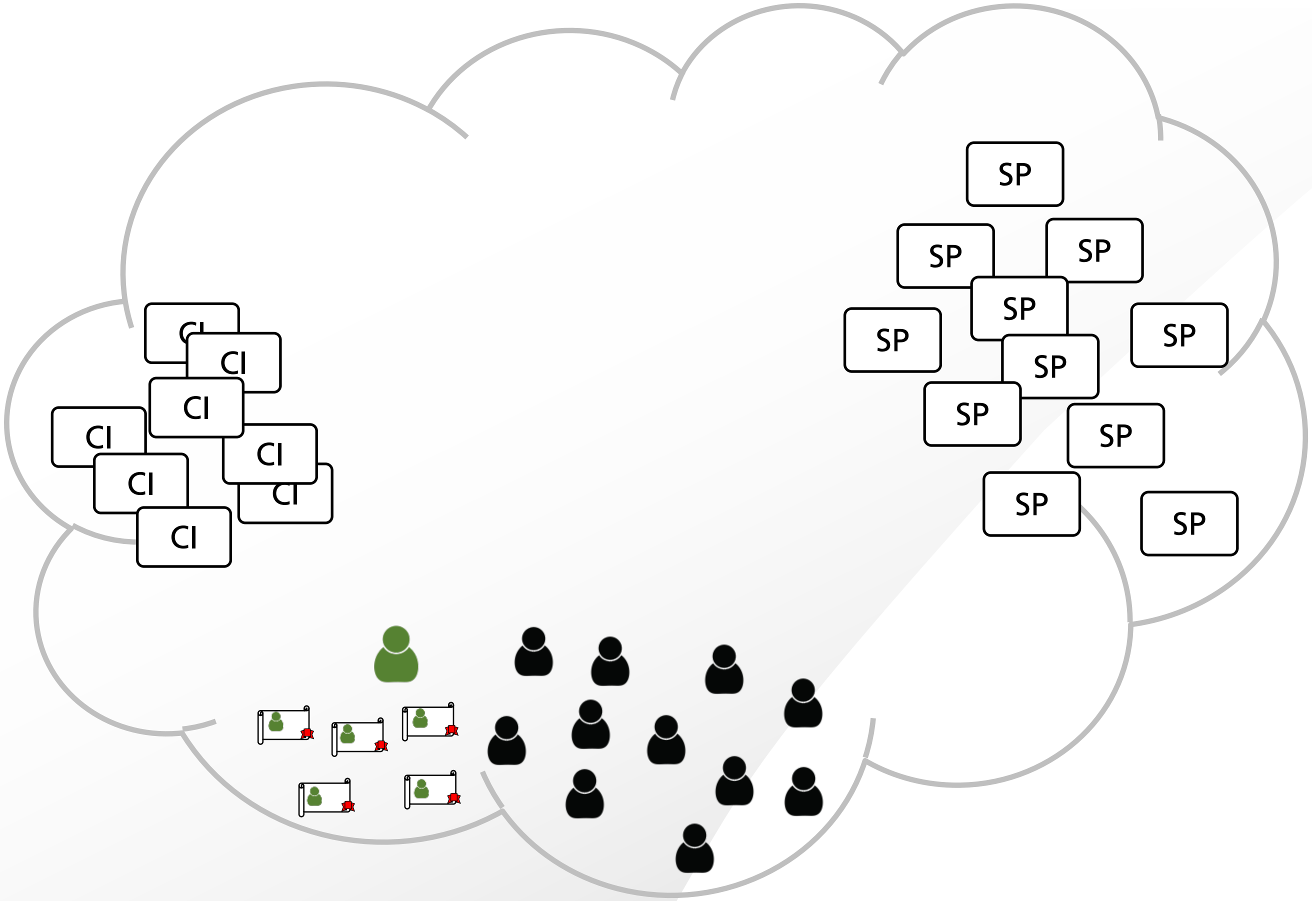


FutureID is partly funded by EU FP7 under GA n°318424

Users with Multiple Credentials



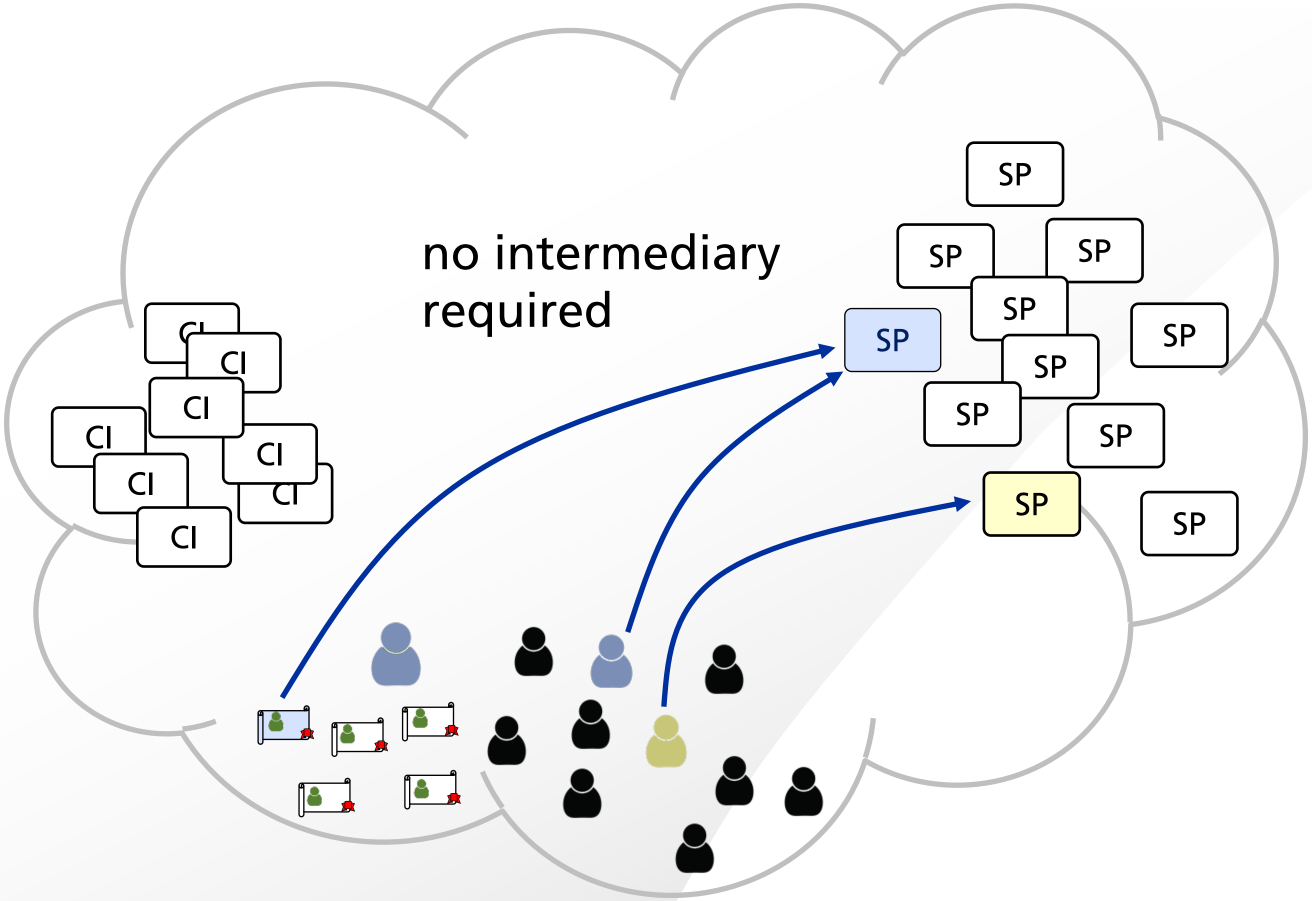
Service Providers (SPs)



FutureID is partly funded by EU FP7 under GA n°318424

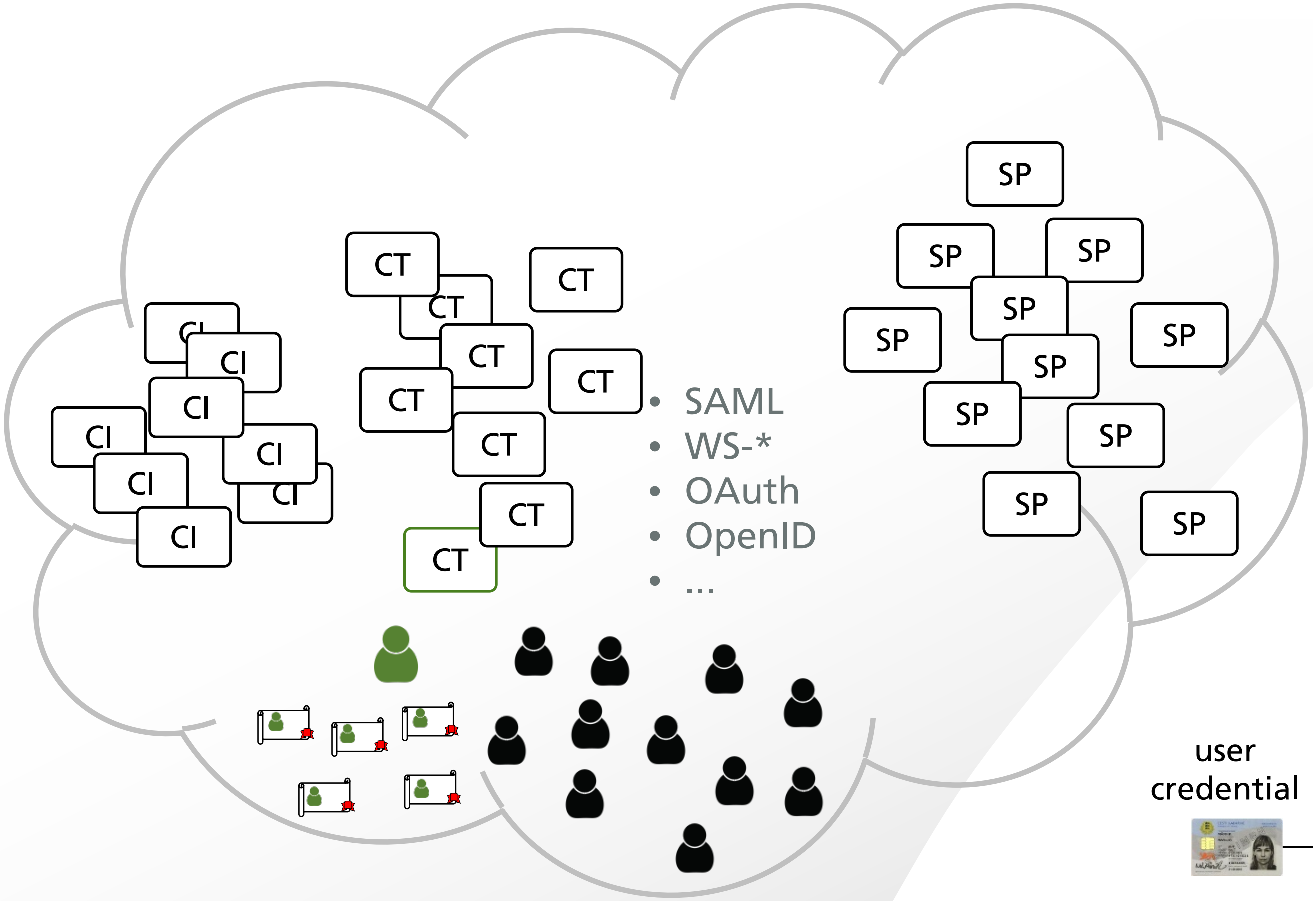
Interaction-Style 1:

Some SPs can directly consume user credentials

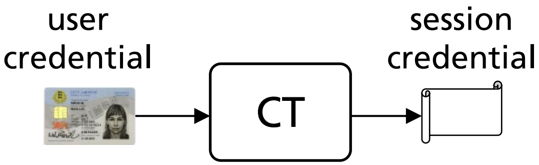


FutureID is partly funded by EU FP7 under GA n°318424

Credential Transformers (CTs): Type 1: existing Identity Providers



- SAML
- WS-*
- OAuth
- OpenID
- …

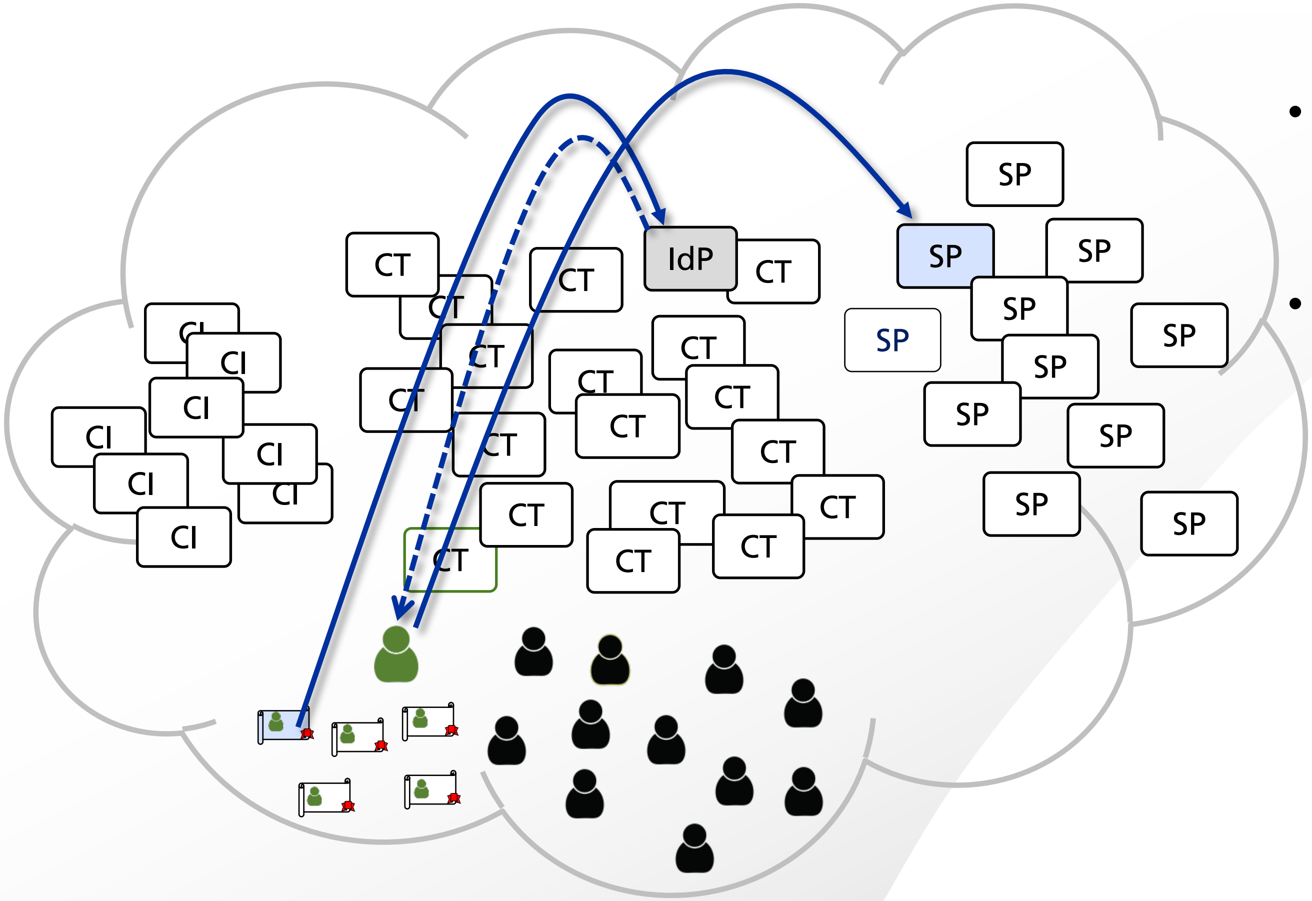


© FutureID Consortium

FutureID is partly funded by EU FP7 under GA n°318424

Interaction-Style 2:

Authentication with existing Identity Provider

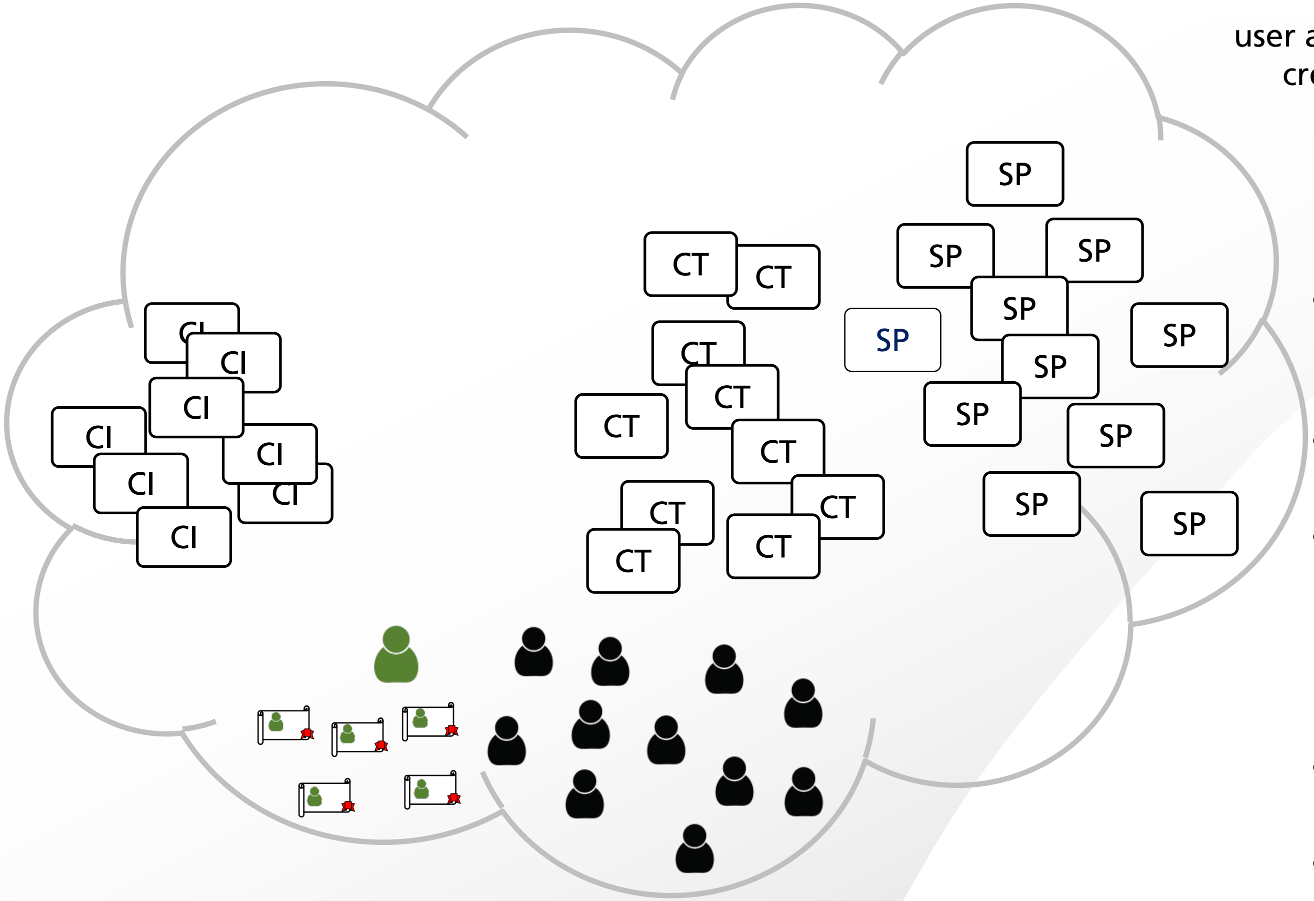


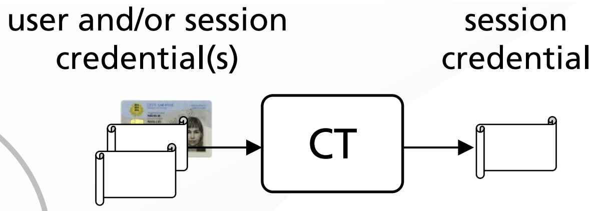
- IdP transforms:
  user credential
  to session credential
- SP can directly consume session credential

SP and IdP need to support the same federation dialect

FutureID is partly funded by EU FP7 under GA n°318424

Credential Transformers (CTs):
Type 2: FutureID Brokers



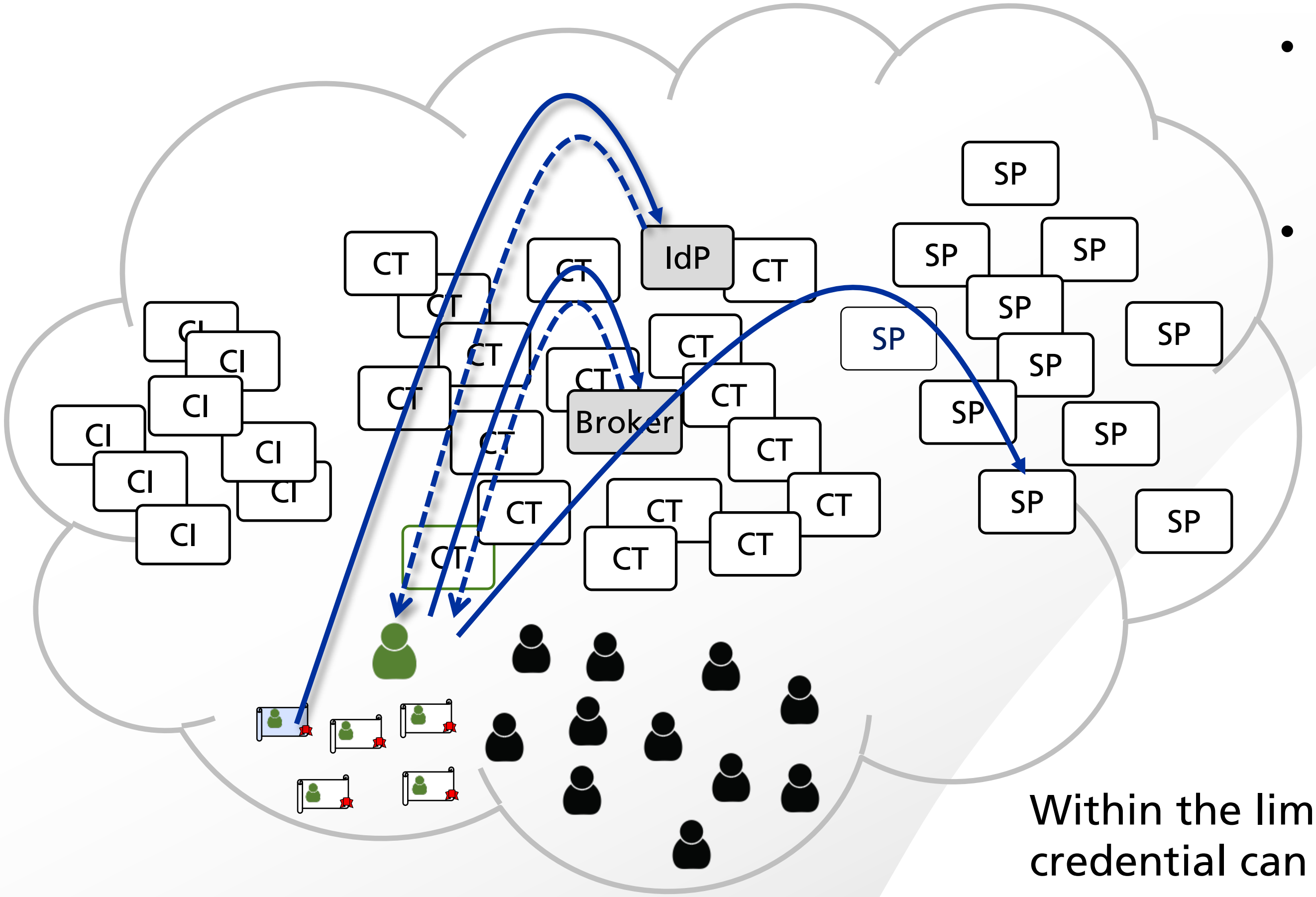


- convert format
  - OAuth -> SAML
  - SAML -> WS-*
- convert semantics
  - cognome -> lastname
- filter
  - Name
  - ~~Date of Birth~~
  - ~~Address~~
  - ~~SSN~~
- derive
  - date of B. -> age over 18
- combine attributes
  - role certificate etc.

FutureID is partly funded by EU FP7 under GA n°318424

Interaction-Style 3:

Authentication with existing Identity Provider and one/several Brokers



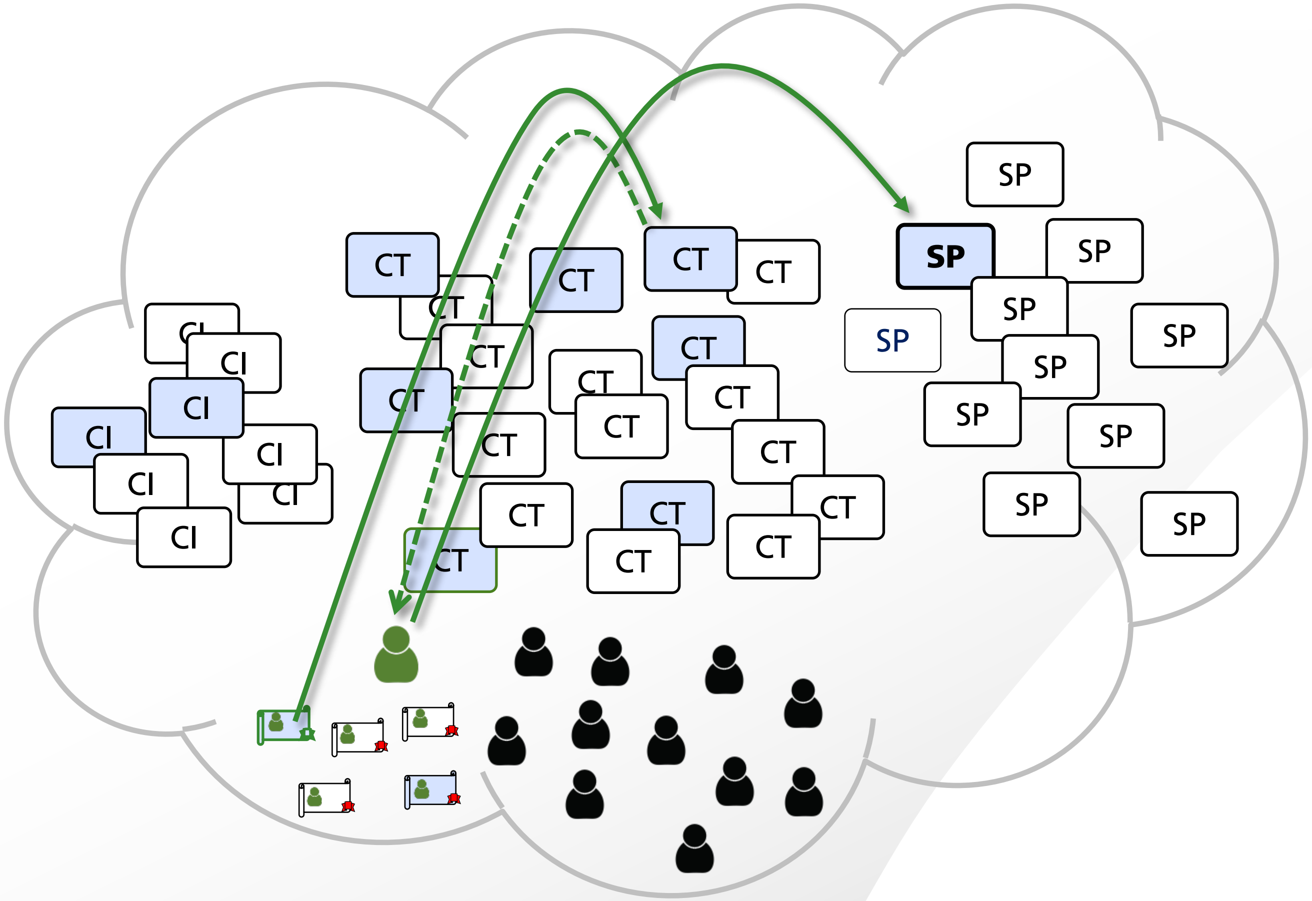
- IdP transforms:
  user credential
  to session credential
- Broker transforms:
  - format that SP can consume
  - less privacy exposure
  - etc.

SP and IdP need **not** support the same federation dialect

Within the limits of trust, any credential can be presented to any SP.

FutureID is partly funded by EU FP7 under GA n°318424

Who Controls Authentication Process?



SP

Whom to trust:

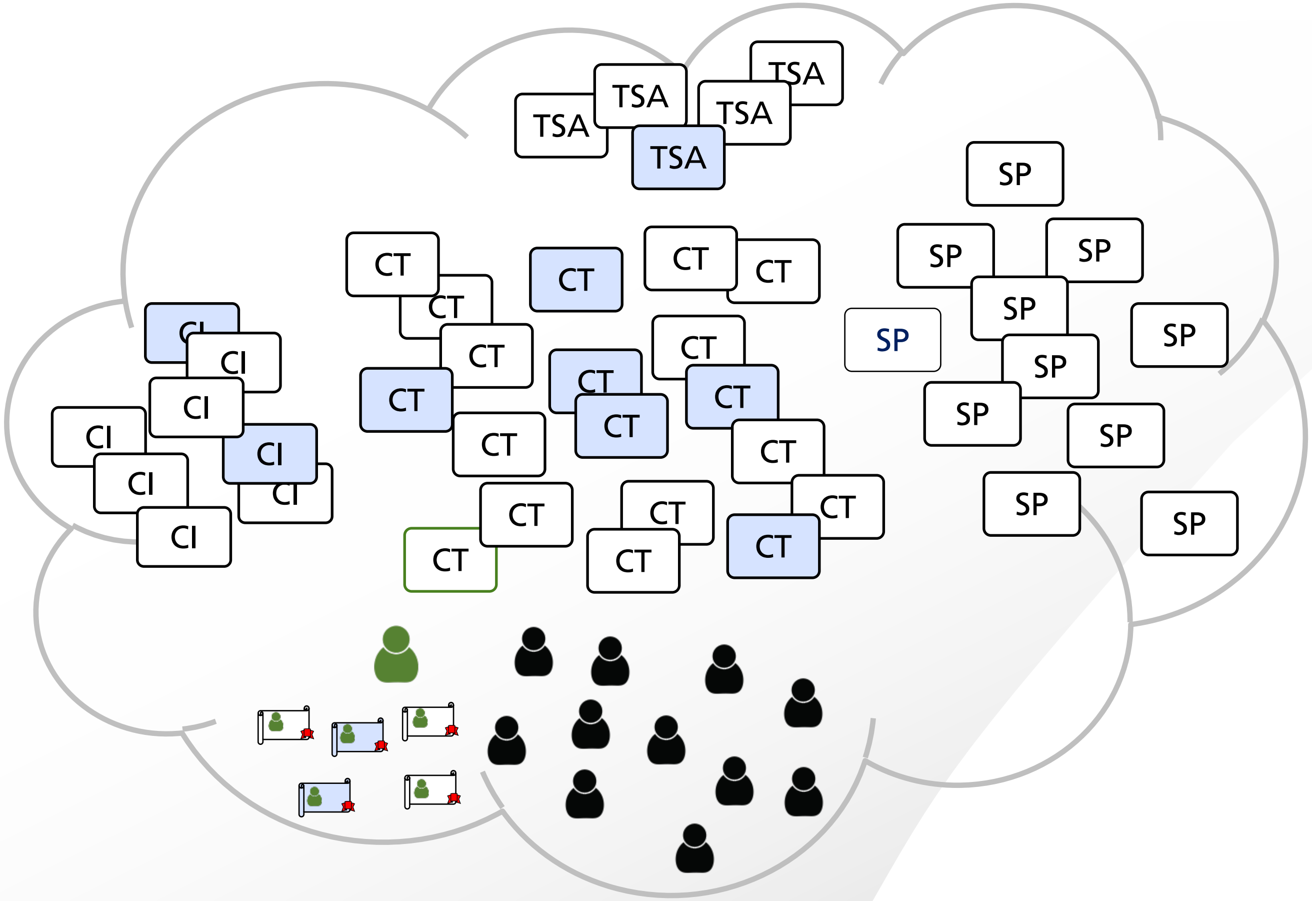
- user credentials (CIs)
- CTs

Auth. Flow:
(within limits of trust)

- which user credential
- which CTs
- which attributes to disclose

FutureID is partly funded by EU FP7 under GA n°318424

Trust Scheme Authorities (TSA) and Trust Infrastructure



SP/User Trust Issues:

- Difficult to determine trustworthiness
- cumbersome to enumerate trusted entities

Trust Scheme Authorities:

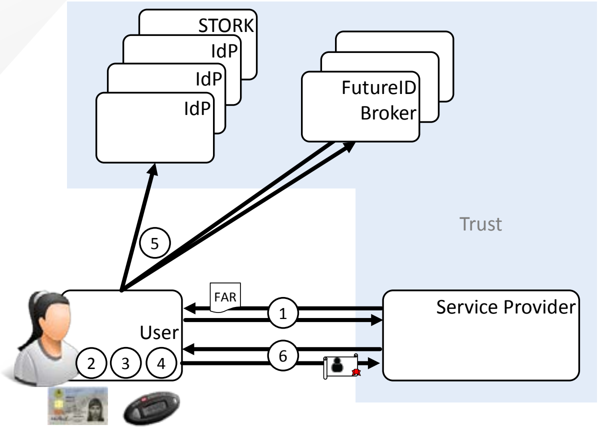
- regulation and oversight
- certify CIs and CTs
- define groups of CIs/CTs
  - EC qualified certificates
  - STORK level 3 credentials
  - Privacy-friendly CTs

© FutureID Consortium

FutureID is partly funded by EU FP7 under GA n°318424

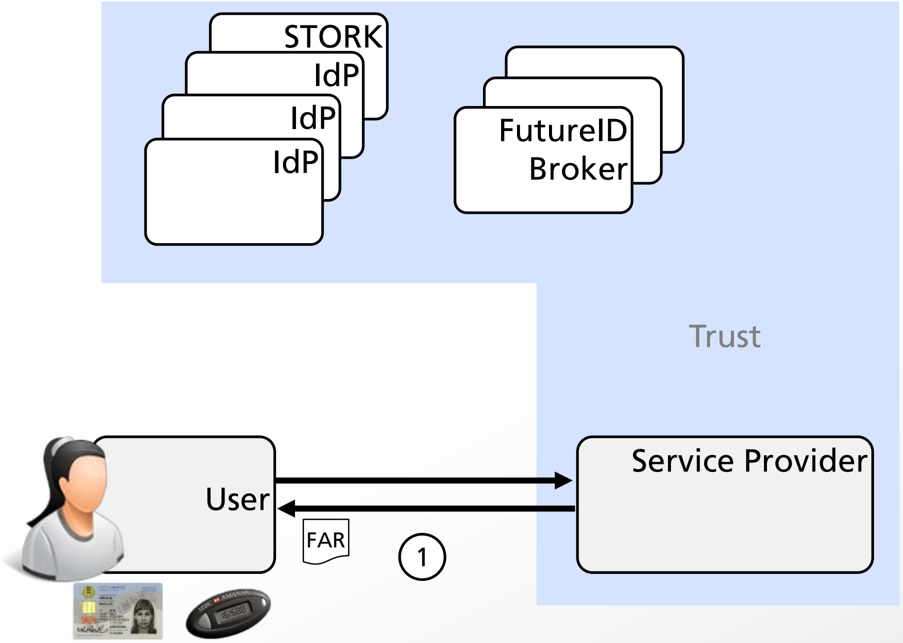
Steps of Authentication

- High-level view:
  - Authentication is done in 6 steps
- User-centric design
  - Avoids unnecessary intermediates
  - Intermediates chosen by user
  - User is in control
    - can also abort authentication



Authentication: Step 1

SP requests authentication for user



- Unauthenticated user requests resource
- SP issues a FutureID authentication request (FAR) **to user**:
  - Credentials it can directly consume
  - Trusted credentials / CTs
  - Required identity attributes

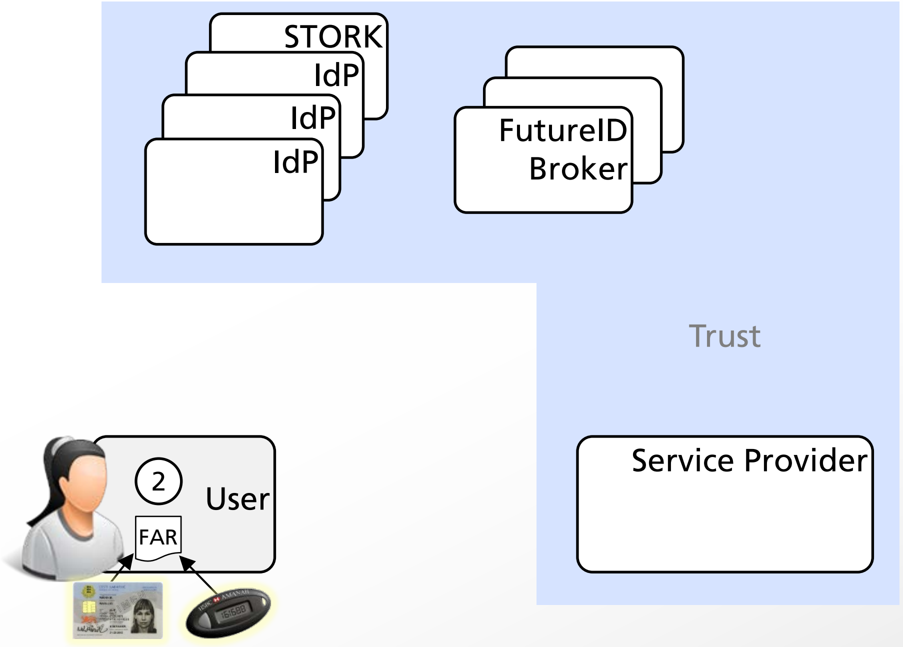
```
CredentialTransformer
  name = SP
  credentialConsumers
    credentialConsumer
      name = S-C
      acceptedFormat = SAML.bearer
      acceptedIssuers = [B1]
      requestedAttributes
        mandatory
          alternatives
            choice
              userId.nationallyUnique.natlGov
            choice
              userId.nationallyUnique.pseudonym
        optional firstName
        optional lastName

CredentialTransformer □
  name = B1
```

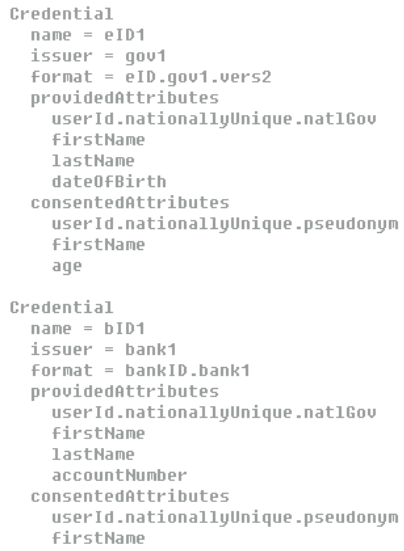
```
issuer = B2
credentialConsumers
  credentialConsumer
    name = SC
    acceptedFormat = [SAML.bearer]
    acceptedIssuers = [IdP1, ..]
credentialProducers
  credentialProducer
     name = SP
     issuedFormat=SAML.bearer
 attributeFilter = True
 attributeDerivations
   derivation
     name = pseudomize
     from = userId.nationallyUnique.natlGov
     to = userId.nationallyUnique.pseudonym
 interfaces
   interface
     name = transf-IF
```

FutureID is partly funded by EU FP7 under GA n°318424

Authentication: Step 2
user adds own resources to FAR



- User complements FutureID authentication request:
  - available credentials



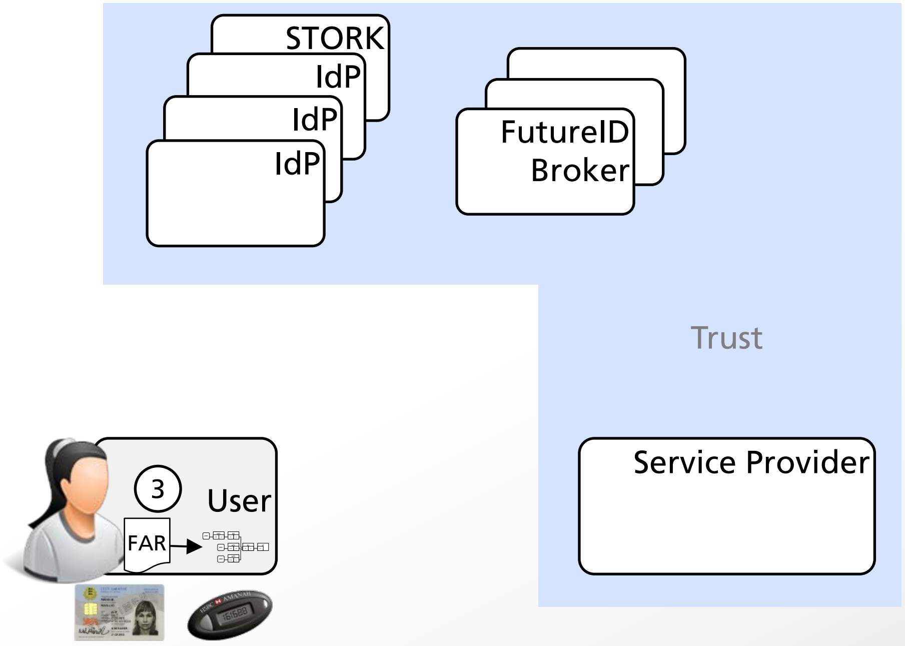
```
Credential
  name = eID1
  issuer = gov1
  format = eID.gov1.vers2
  providedAttributes
    userId.nationallyUnique.natlGov
    firstName
    lastName
    dateOfBirth
  consentedAttributes
    userId.nationallyUnique.pseudonym
    firstName
    age

Credential
  name = bID1
  issuer = bank1
  format = bankID.bank1
  providedAttributes
    userId.nationallyUnique.natlGov
    firstName
    lastName
    accountNumber
  consentedAttributes
    userId.nationallyUnique.pseudonym
    firstName
```

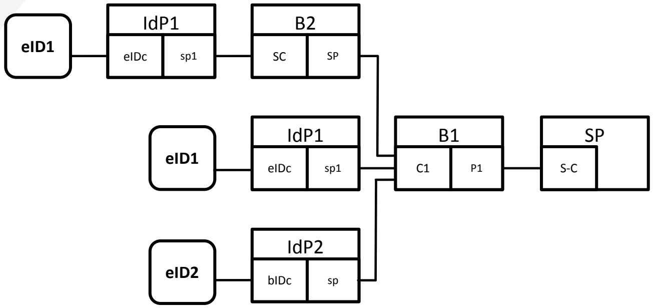
FutureID is partly funded by EU FP7 under GA n°318424

Authentication: Step 3

Generation of possible Authentication Plans

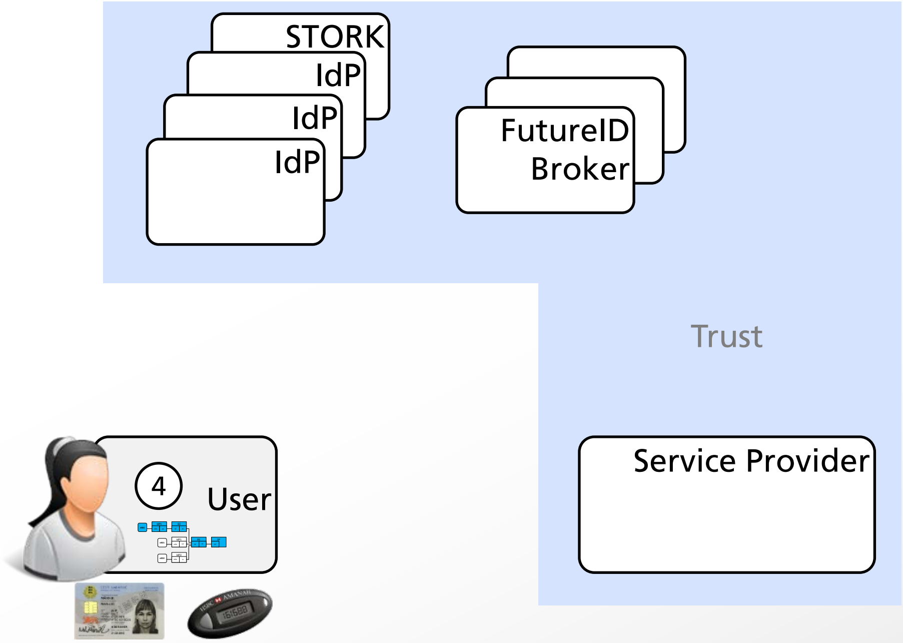


- User’s local or remote Authentication Solver:
  - Find possible authentication plans

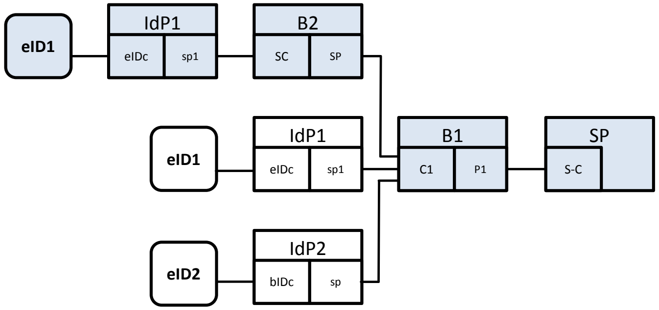


Authentication: Step 4

User selects Best Authentication Plan

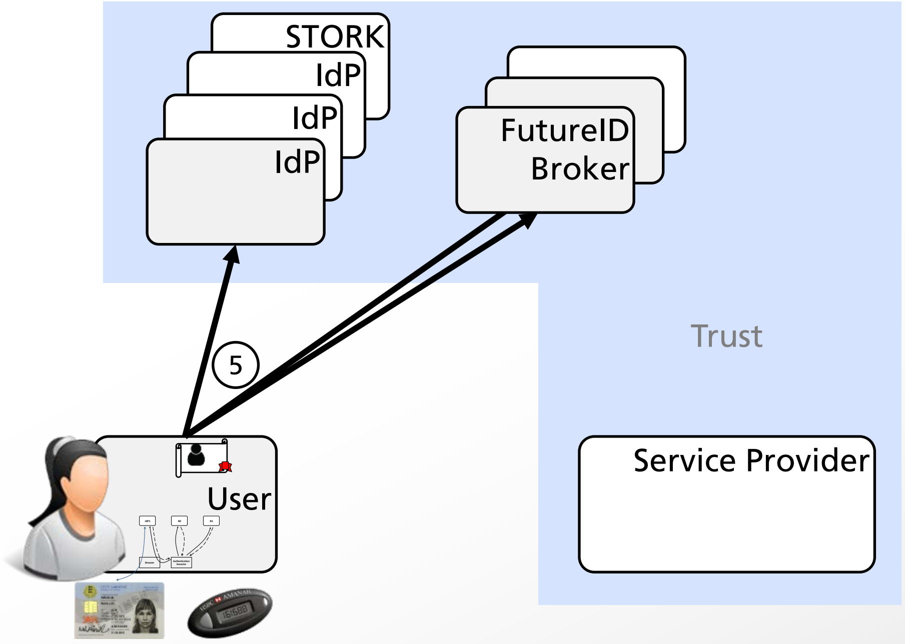


- User selects best authentication plan or aborts
  - which credential to use
  - which intermediates are trusted
  - which attributes to disclose

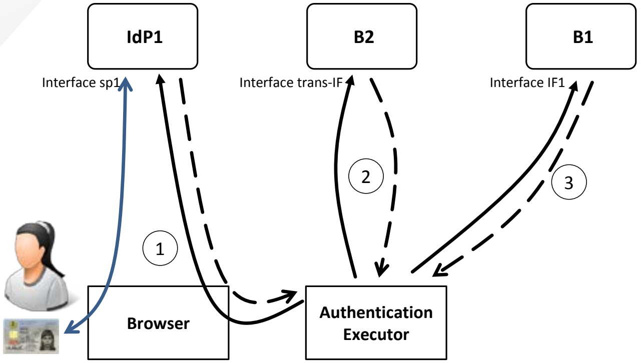


Authentication: Step 5

Execution of Authentication Plan



- User’s local or remote Authentication Executor:
  - communicates with CTs
  - obtains a final session credential

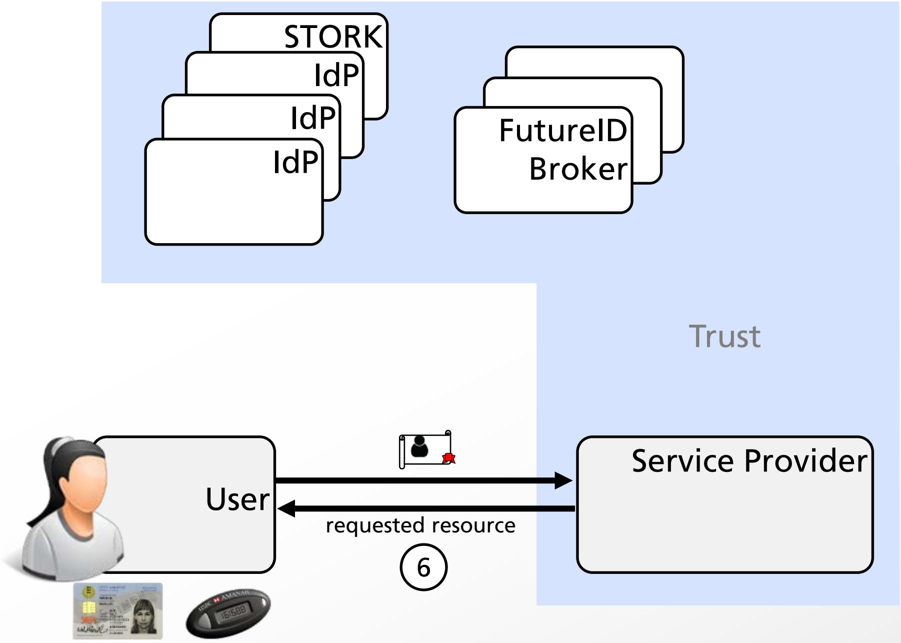


FutureID is partly funded by EU FP7 under GA n°318424

Authentication: Step 6

Presentation of Session Credential

- User presents final session credential to SP.
- SP verifies and serves resource to user.



FutureID is partly funded by EU FP7 under GA n°318424

The FutureID’s Approach to Privacy is Evolutionary

- Reuse of existing user-bases, investments, agreements
    - Existing eIDs/credentials
    - Existing IdPs, infrastructures (STORK)
    - Existing Services (easy for SPs to participate)
- Fixes for biggest concerns
- Ease transition to/roll-out of revolutionary approaches
    - Support of Attribute Based Credentials (privacy ABCs)
        - ABC4Trust
            - IBM’s Identity Mixer (Idemix)
            - Microsoft’s uProve
        - IRMA   (smart card implementation of idemix algorithms)

Concerns with Government eIDs

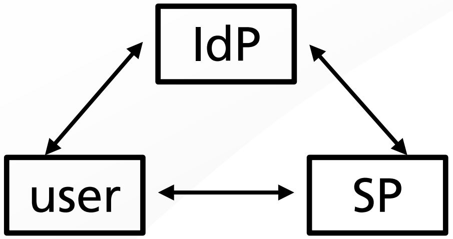
- Unique Identifier
- Excessive disclosure of attributes

- FutureID Broker:
  - Derivation of sector- or service-specific pseudonyms
  - Filtering of attributes
  - Derivation of attributes:
    - Nationality -> EU-citizen
    - Date of Birth -> 18 or older

FutureID is partly funded by EU FP7 under GA n°318424

Federated Identity Management lacks User Control

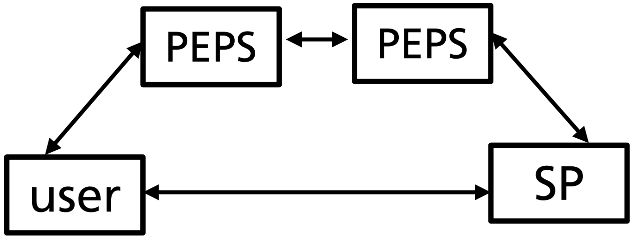
- SP determines Intermediaries
  - Users unaware of who processes personal data
  - No possibility to intervene (incl. abort)
- SP determines which user attributes are disclosed
  - direct query from SP to IdP (e.g., SAML artifact resolution profile)



- FutureID: Solver provides control:

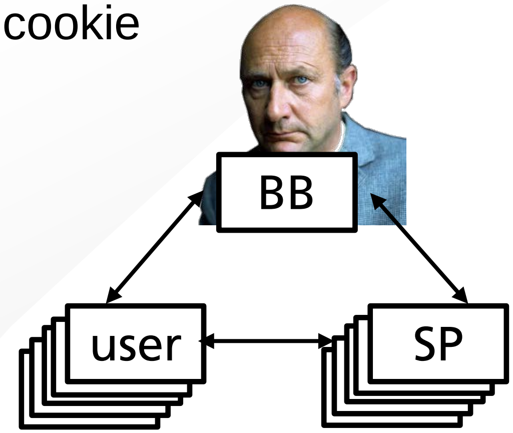
  (possibly automated via user policy):

  - Awareness who processes which data
  - Selection of intermediaries (within limits of SP's trust)
  - Control over disclosed data
  - Possibility to abort (before disclosing identity data)



Big Brother:
Collection of “meta data”

- WHO accesses WHAT, when
    - WHO: Unique identifier, browser fingerprint, cookie
- Profiling individuals
    - Link activities of given individual

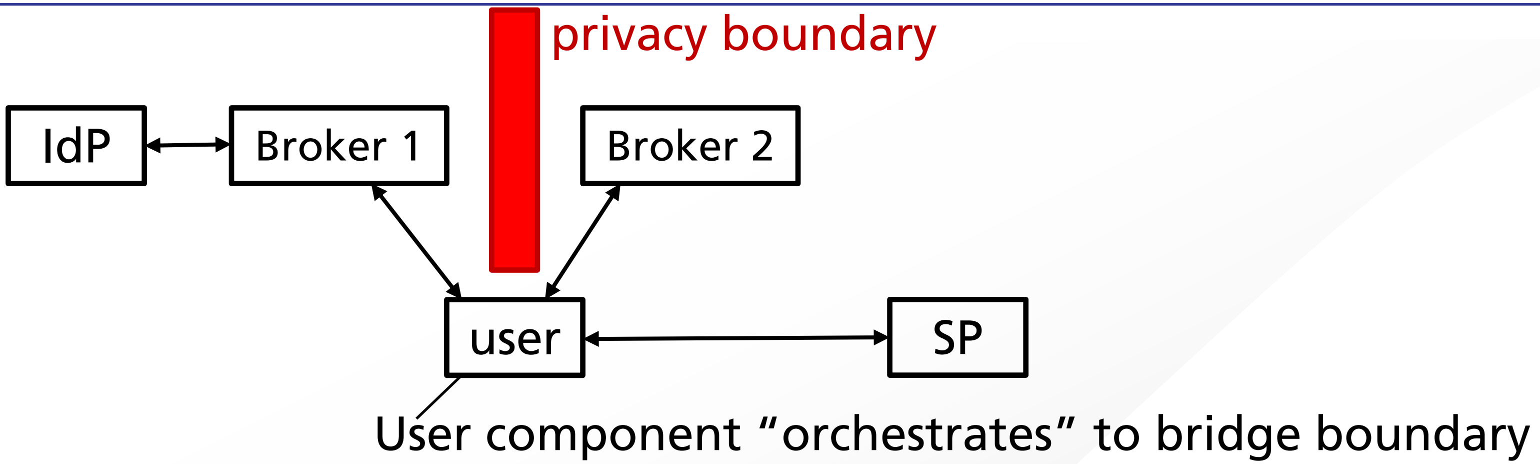


- FutureID architecture:
    - Decentralize   (many intermediaries)
    - User chooses trusted intermediary, arbitrary number of intermediaries
    - Direct presentation of credential without intermediary
        - Privacy ABCs
    - Do not track pattern

FutureID is partly funded by EU FP7 under GA n°318424

Do Not Track Pattern

(Ronny Bjones, Microsoft)



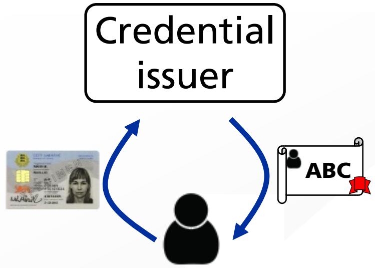
- Broker 1 cannot see SP
- Broker 2 cannot see IdP
- Connection through user component (FutureID executor)

This pattern stops big brothers

FutureID is partly funded by EU FP7 under GA n°318424

FutureID Support of “revolutionary” Privacy ABCs

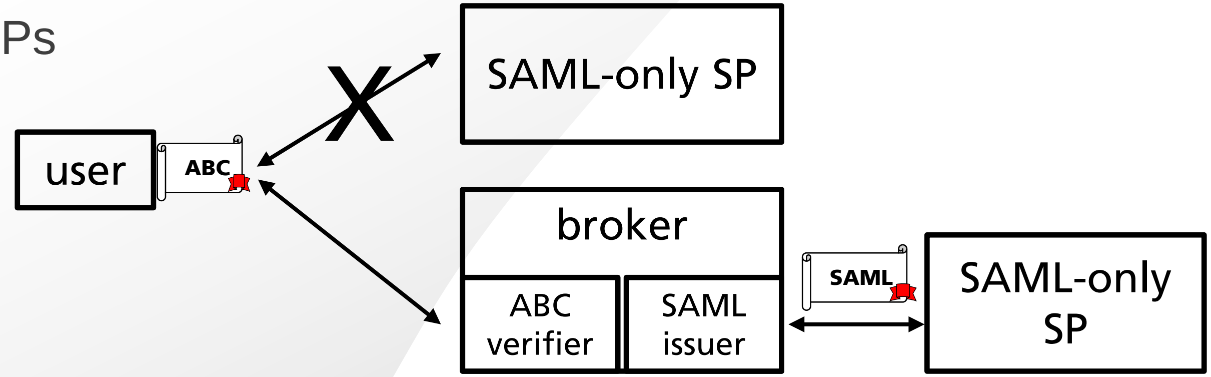
- Bootstrap privacy friendly credentials with gov. eIDs
  - Gov. eIDs: secure enrollment
  - Even if pseudonyms:
    - It is a person
    - A person has only one pseudonym in a given domain
- Present credential without need for intermediary



Credential issuer

ABC

- ABC-enable legacy SPs



user

ABC

X

SAML-only SP

broker

ABC verifier

SAML issuer

SAML

SAML-only SP

FutureID is partly funded by EU FP7 under GA n°318424

Conclusions

- The FutureID architecture is mostly economically motivated:
  - Open market of identity and trust services
  - Business models that make it economically sustainable
  - Maximize user acceptance
- FutureID has an evolutionary approach to privacy
- Privacy-unfriendly authentication is anyhow possible (if user consents)
- FutureID adds privacy-enhancement over status quo
  - User centric: awareness, consent, choices (intermediaries, disclosure)
  - Possibility to filter, derived attributes, pseudonyms
  - Possibility to avoid big brothers
- FutureID supports a smooth transition to “revolutionary” privacy solutions (ABCs)

FutureID is partly funded by EU FP7 under GA n°318424

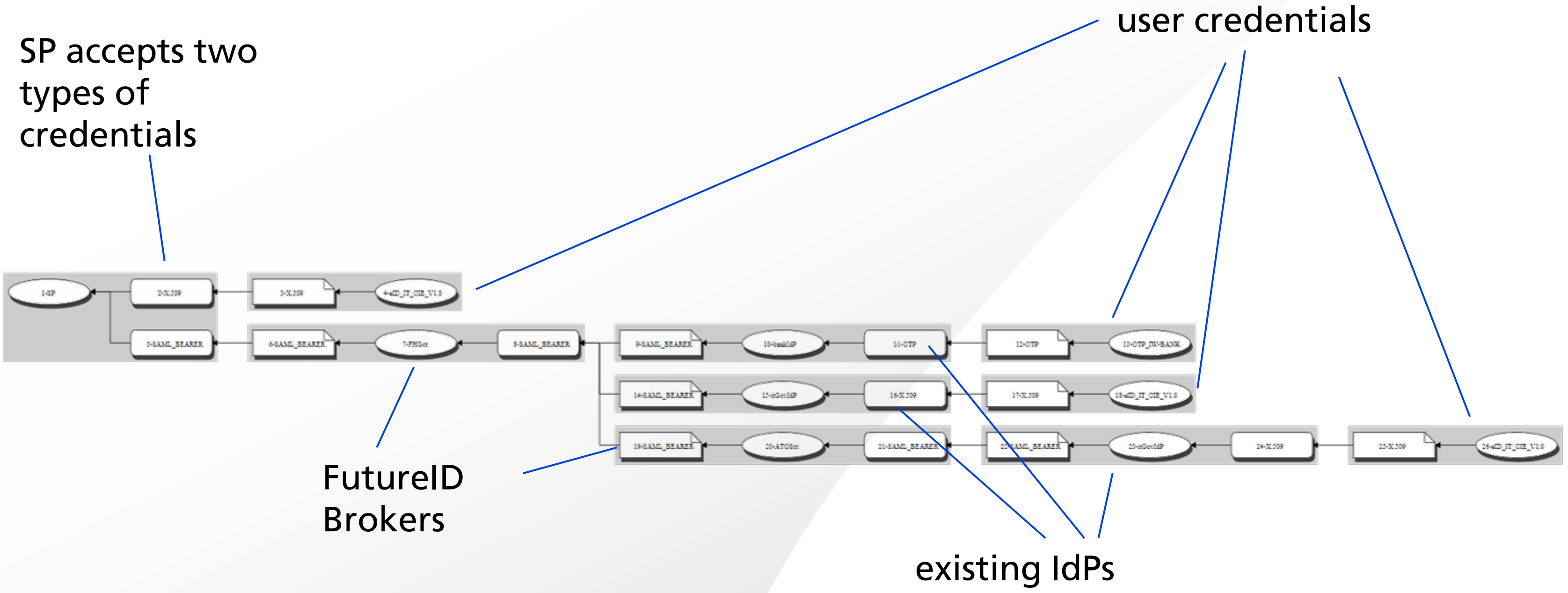
Contact

Bud P. Bruegger

<bud.bruegger@iao.fraunhofer.de>

Example of Possible Authentication Plans

Visualization from a prototype implementation



SP accepts two types of credentials

user credentials

FutureID Brokers

existing IdPs

FutureID is partly funded by EU FP7 under GA n°318424