




# A Model for Privacy Enhanced Federated Identity Management

Rainer Hörbe, EUSTIX Alliance

A 3D rendered white character with a large spherical head, standing and holding a large rectangular sign. The sign is white with a thin black border and contains the text 'Privacy Issues in Federated Identity Management'.

# Privacy Issues in Federated Identity Management

# Technical Privacy Controls for FIM

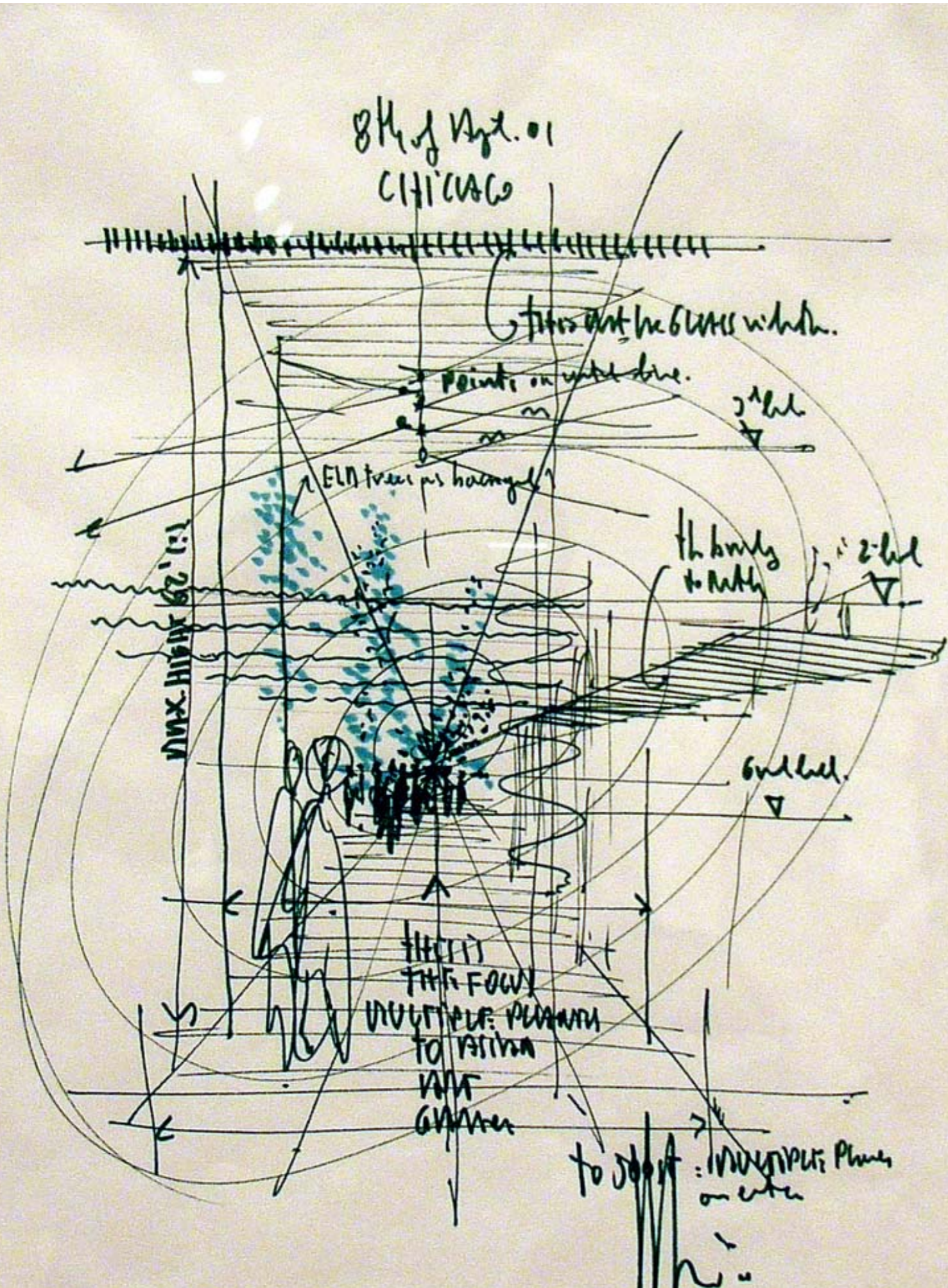
## Standard FIM (e.g. SAML WebSSO)

- Data minimization:
  - IdPs release only required attributes, only to authorized services
- Limited unlinkability between services
  - Identifiers are targeted
- Impersonation
  - (HoK)

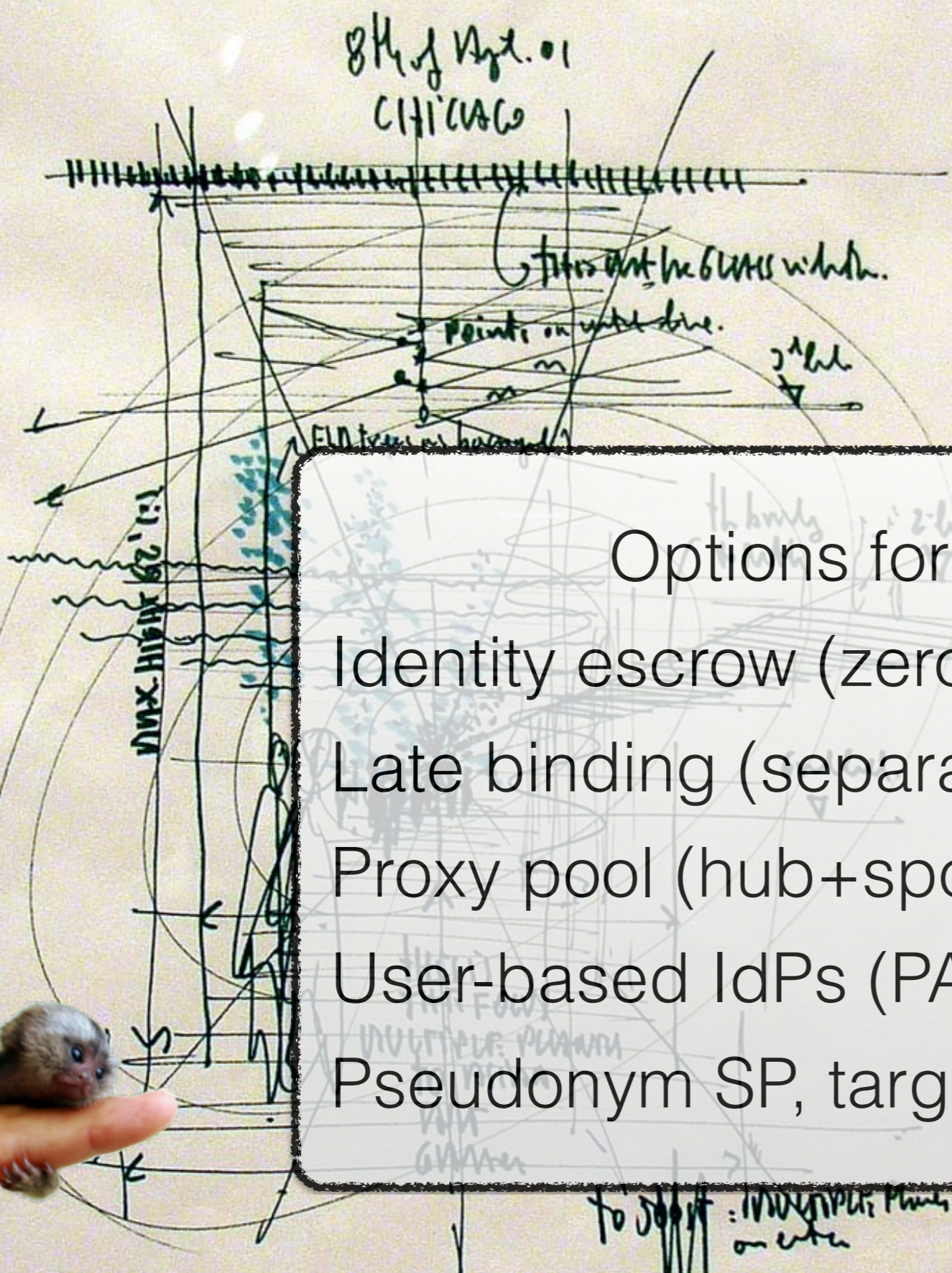
## PE-FIM

- Limited unobservability by TTP
  - IdP/AP talks to groups of services, cannot identify service
- Limited unlinkability between services
  - Messaging, payment and delivery are pseudonymized; e.g. IdP will proxy SMTP traffic from targets email address to registered one

Rationale for enhanced privacy: scaling federation across vertical sectors



Architectural challenge:  
Technical controls to  
enhance privacy



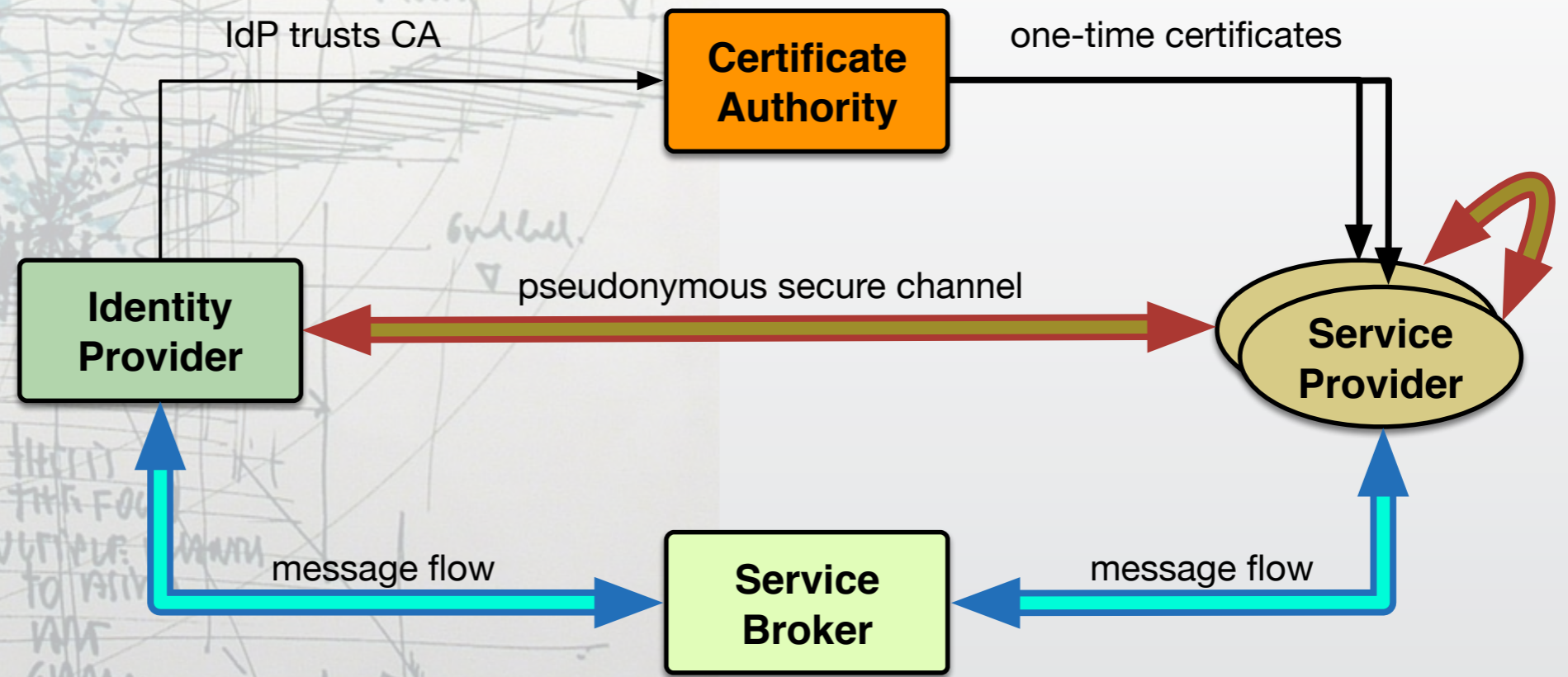
- Options for technical controls
- Identity escrow (zero-knowledge proof)
- Late binding (separate authN from attributes)
- Proxy pool (hub+spoke with many hubs)
- User-based IdPs (PAD, IMI)
- Pseudonym SP, targeted attributes (PE-FIM)

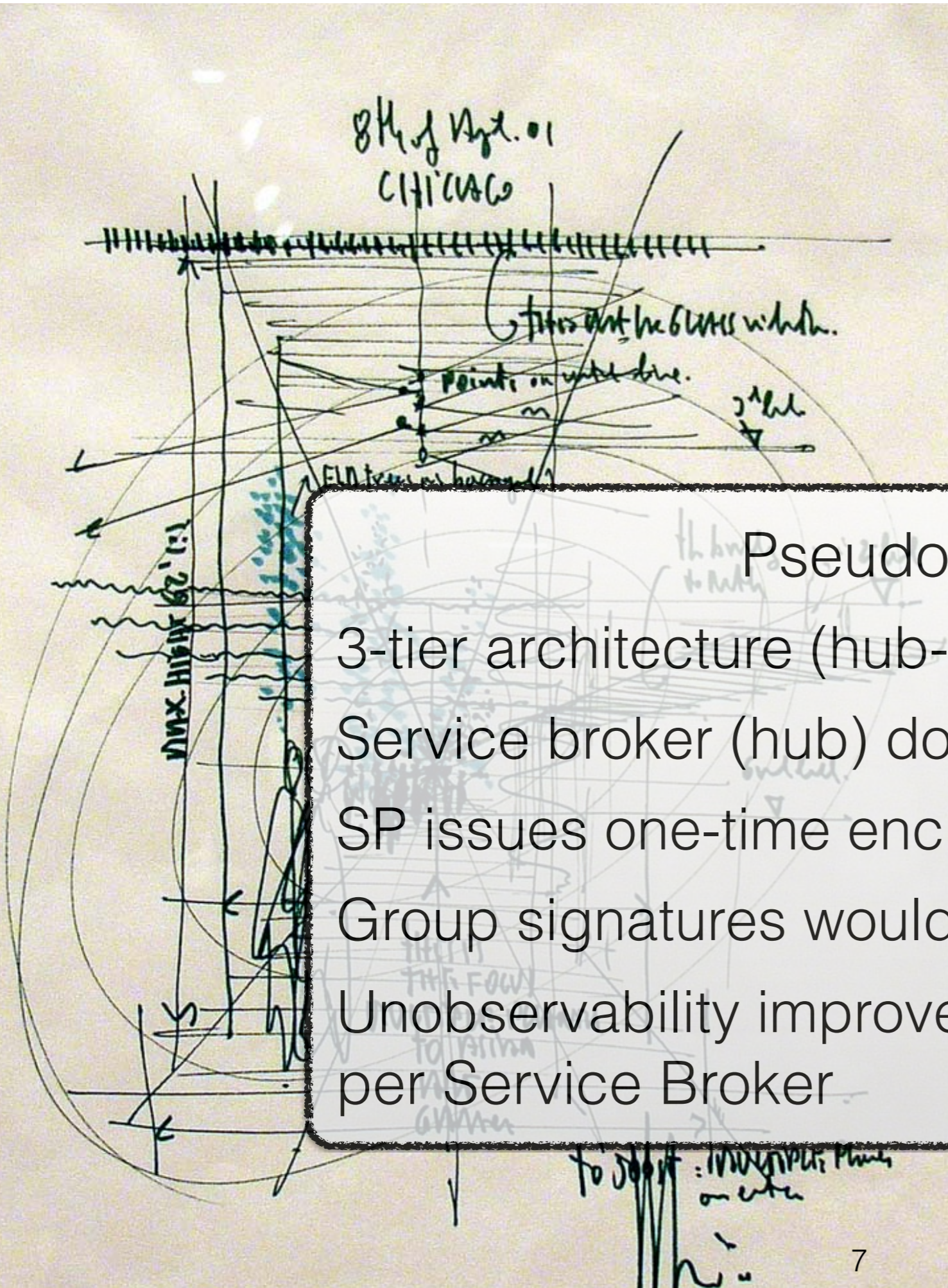


8th of Sept. 01  
CITICAC

points on white line.

# Pseudonym SP





## Pseudonymous SP

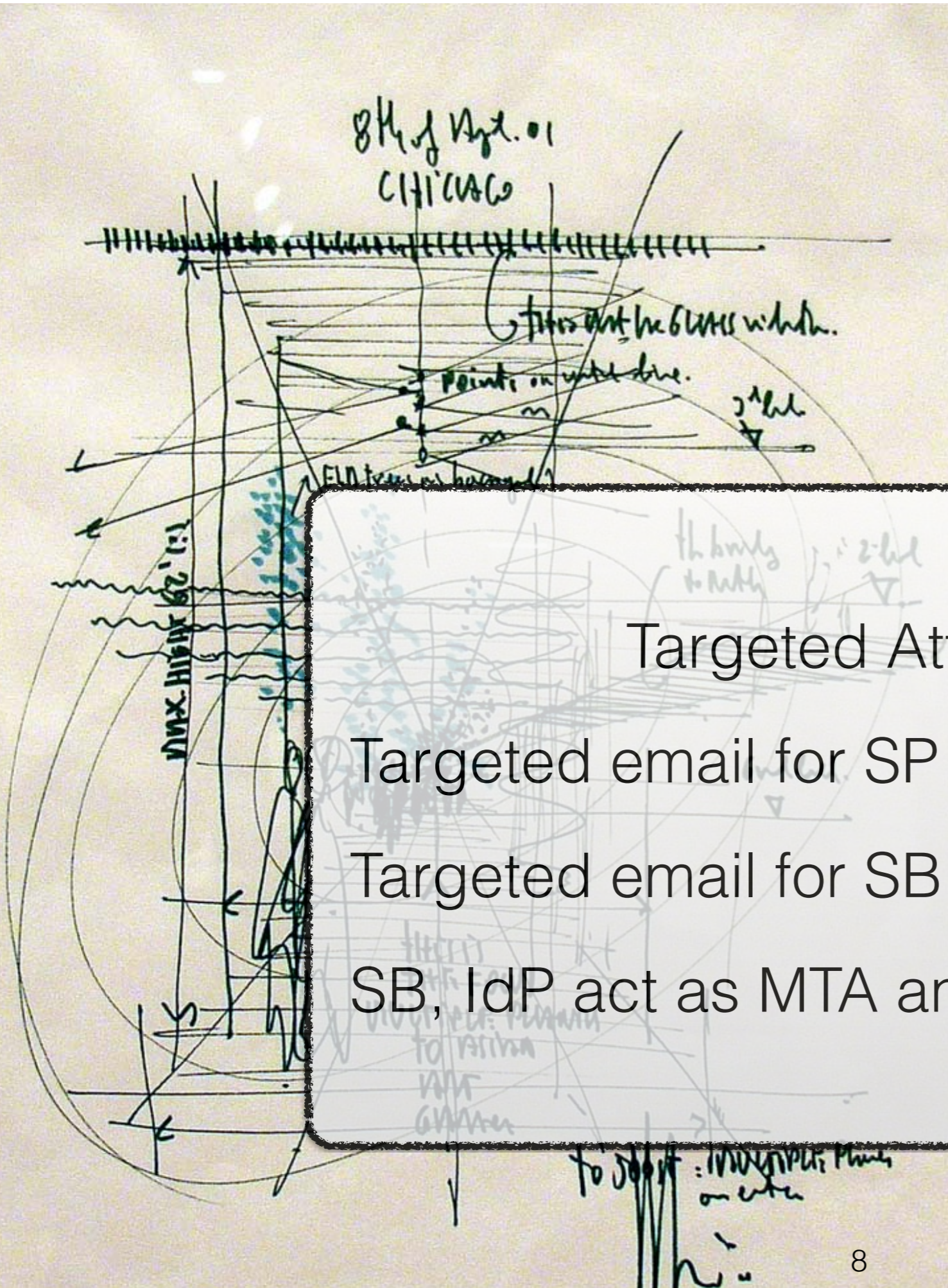
3-tier architecture (hub-and-spoke)

Service broker (hub) does not see user attributes

SP issues one-time encryption keys signed by CA

Group signatures would work as well

Unobservability improves with number of services per Service Broker



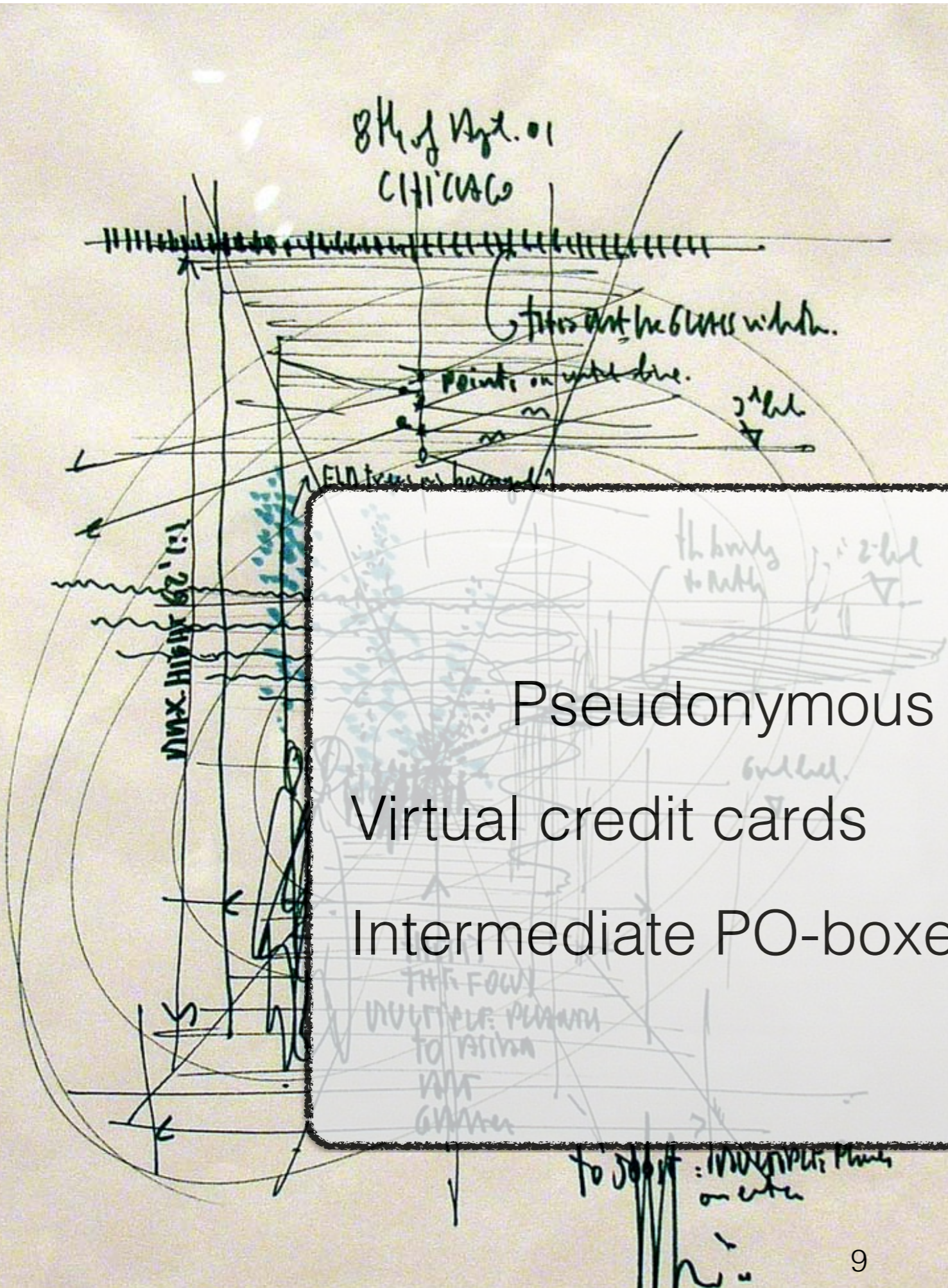
## Targeted Attributes (e-mail)

Targeted email for SP is targeted id @ SB

Targeted email for SB is targeted id @ IdP

SB, IdP act as MTA and rewrite address

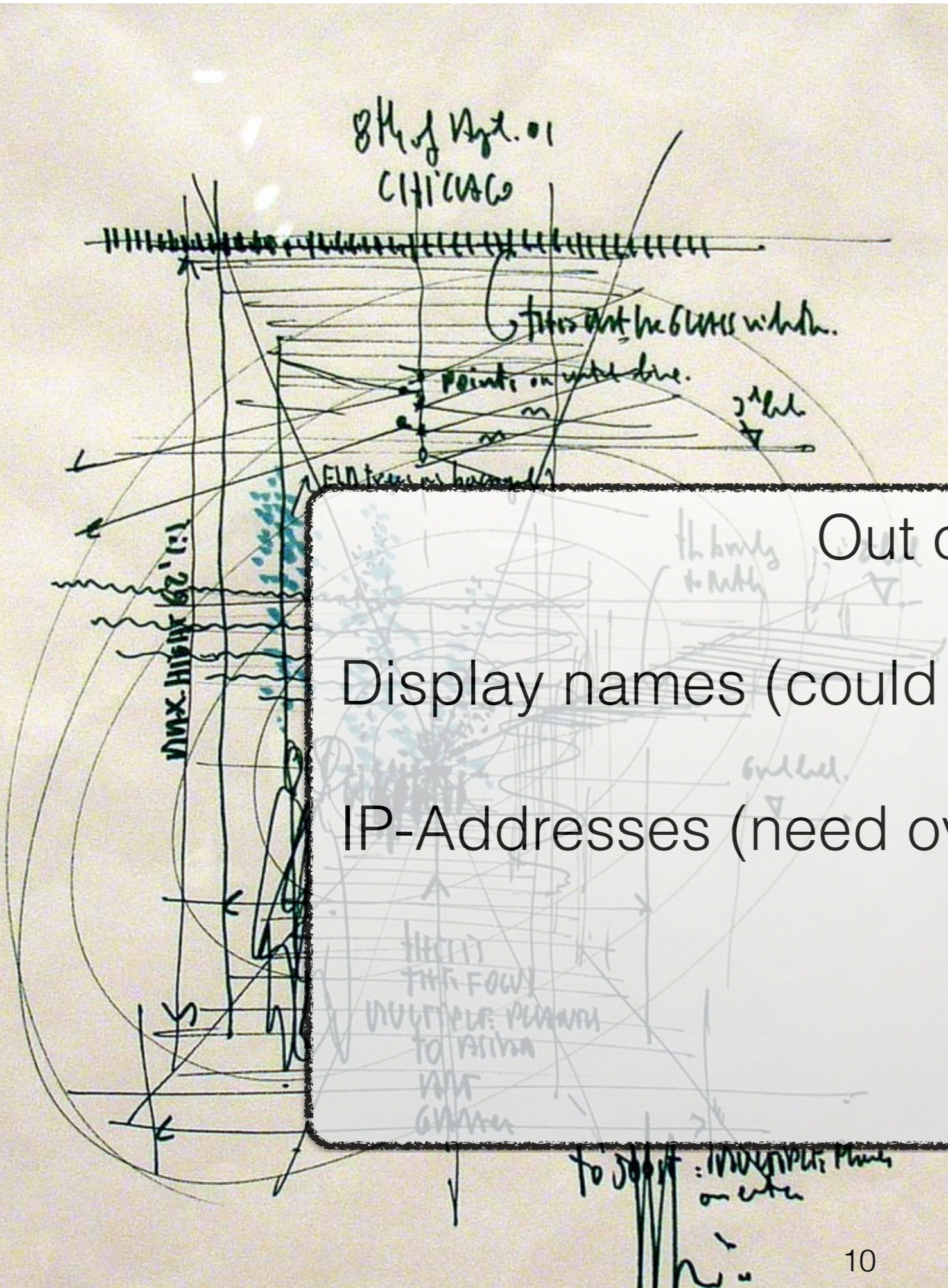




Pseudonymous Payment & Delivery

Virtual credit cards

Intermediate PO-boxes(?)



Out of scope

Display names (could be first name + number)

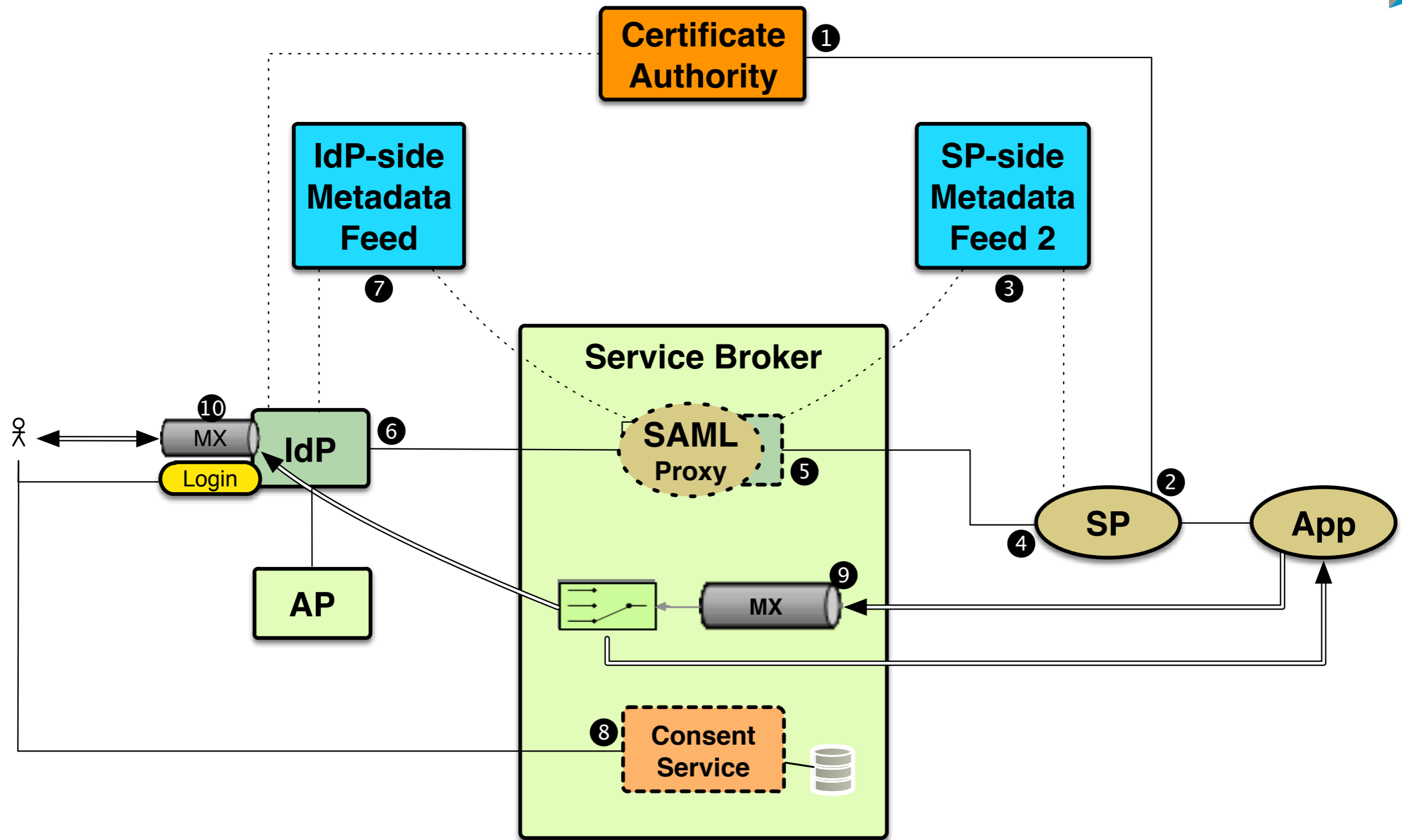
IP-Addresses (need overlay networks)

What else?

The model can be applied to SAML BAE, WS-Trust and OIDC as well.

A profile for SAML looks like this:





(4) /AuthnRequest/extension/pefim:SPCertEnc/ds:KeyInfo/..

(6) /Assertion/Advice/EncryptedAssertion

# Project Status

Development underway for PoC using OpenAM, Shibboleth and pysaml2

Demo @ EEMA/Vienna April 2014

Pilot project: EDI-federation in Austria

