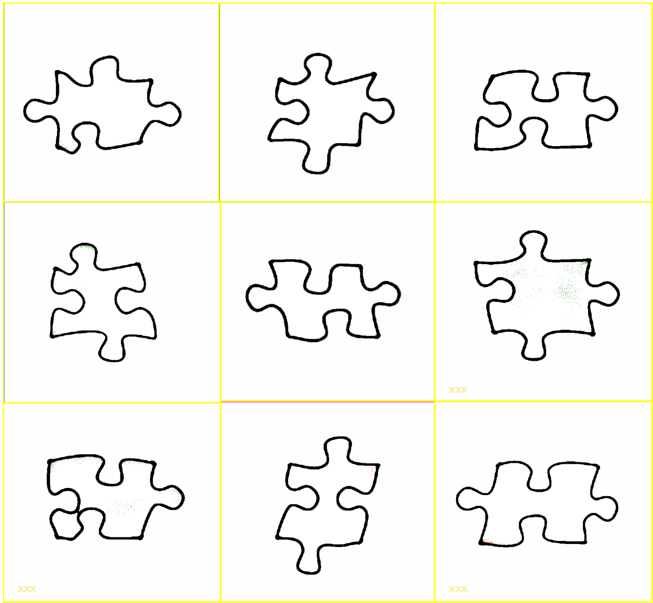
Do you like to puzzle?

Build an AA Infrastructure!

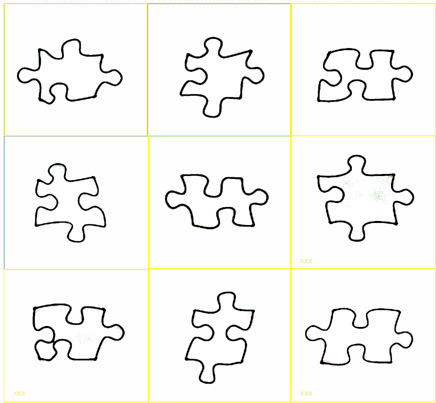


CARnet Users Conference

September, 29th, 2004

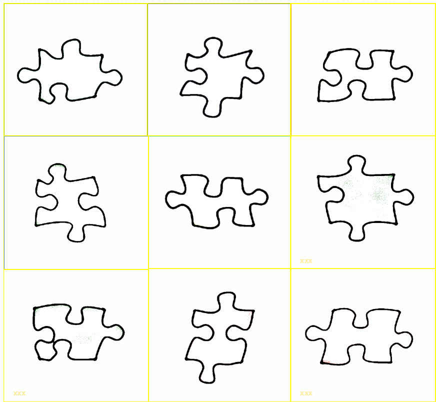
Ton.Verschuren@SURFnet.nl

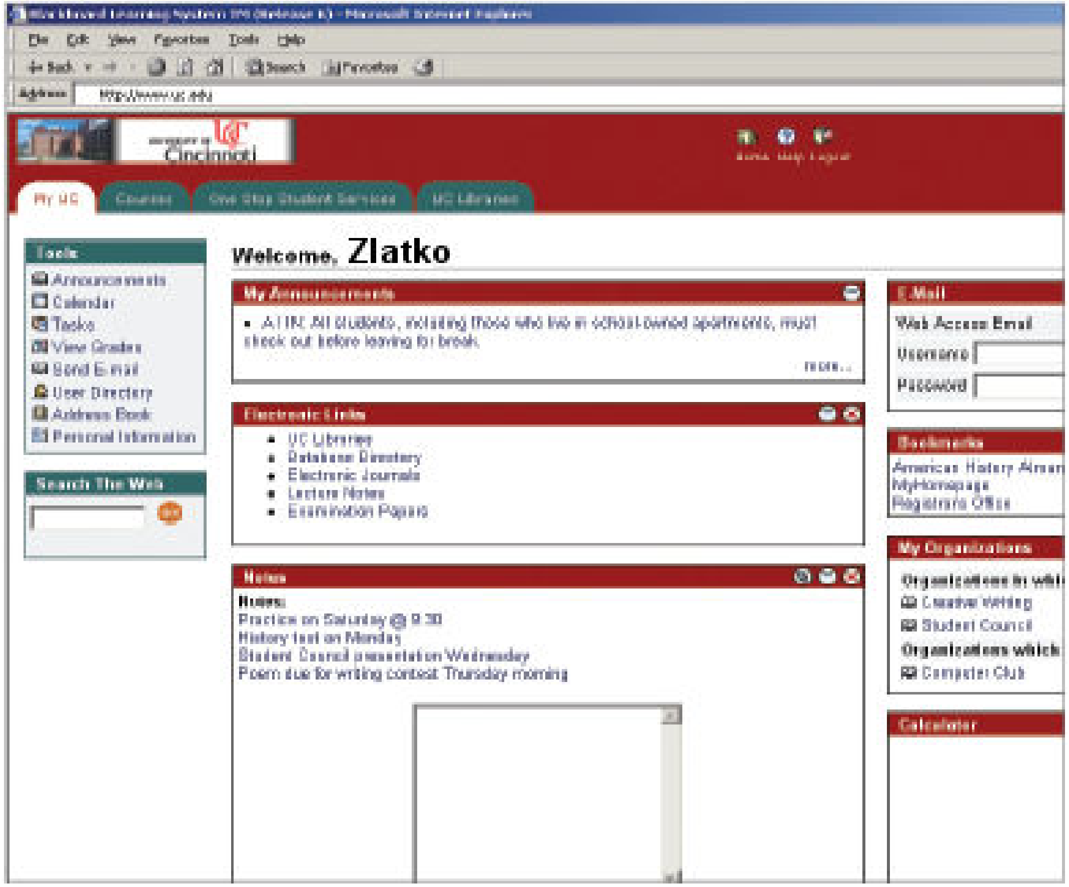
Roadmap



- Drivers for an AAI
- The pieces of the puzzle: network and application access, login, authentication, authorisation, identity management
- Federations
- Diagnostics
- Standards
- Homework

Why AAI?
Personalised service provisioning!





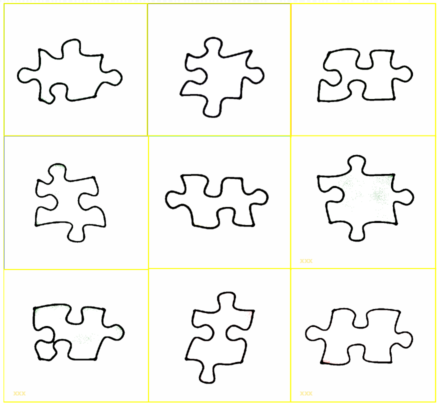
Welcome, Zlatko

- ATTN: All students, including those who live in school-owned apartments, must check out before leaving for break.

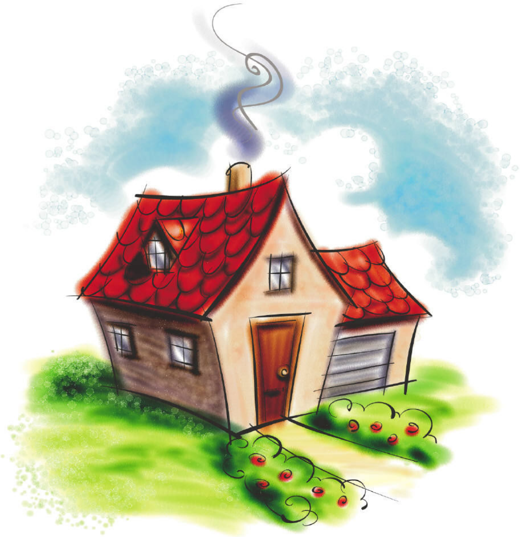
Notes:
Practice on Saturday @ 9:30
History test on Monday
Student Council presentation Wednesday
Poem due for writing contest Thursday morning

Why AAI?
Educational mobility!

Photos: Urs Siegenthaler

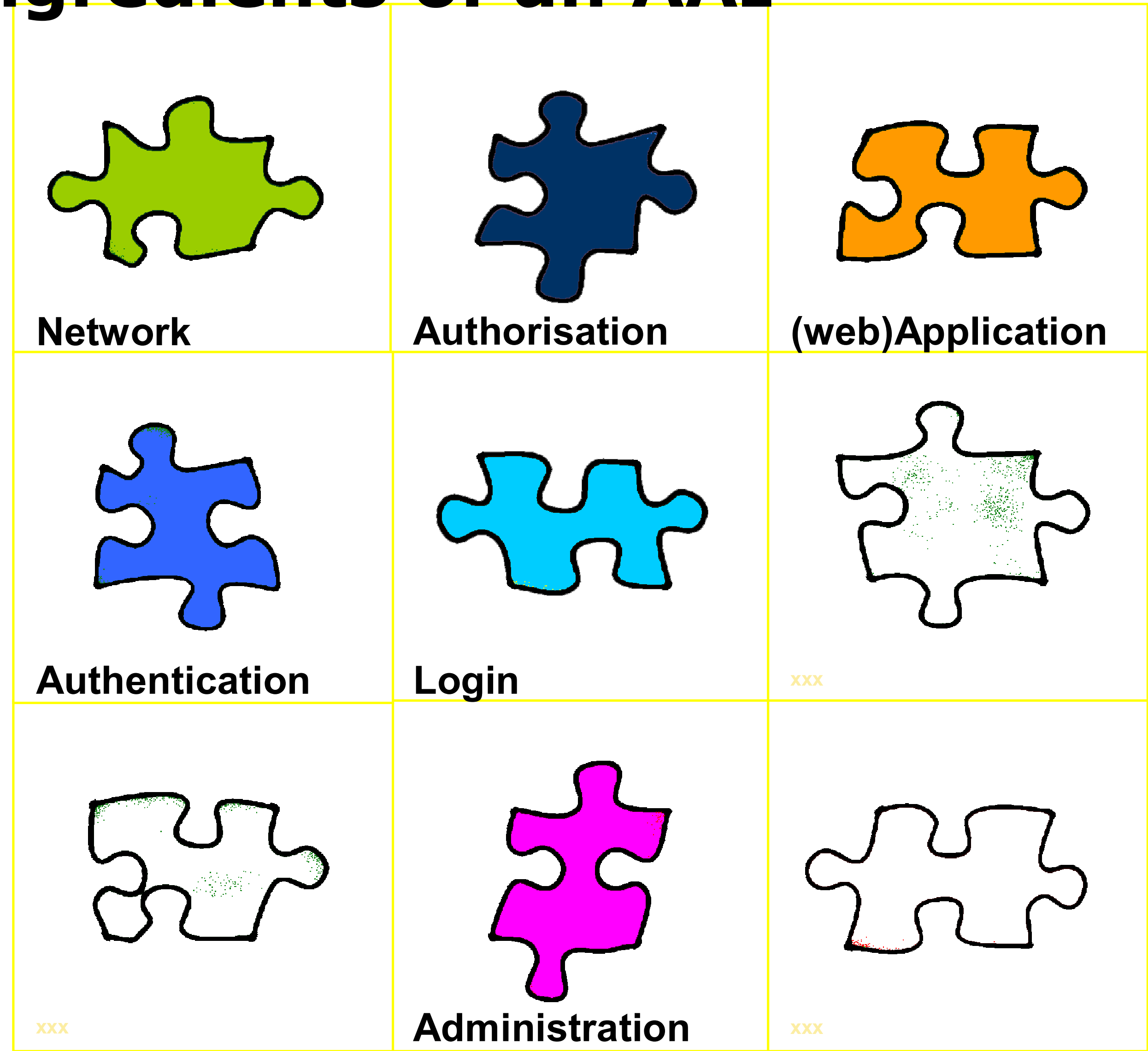


Why AAI?
Network mobility!



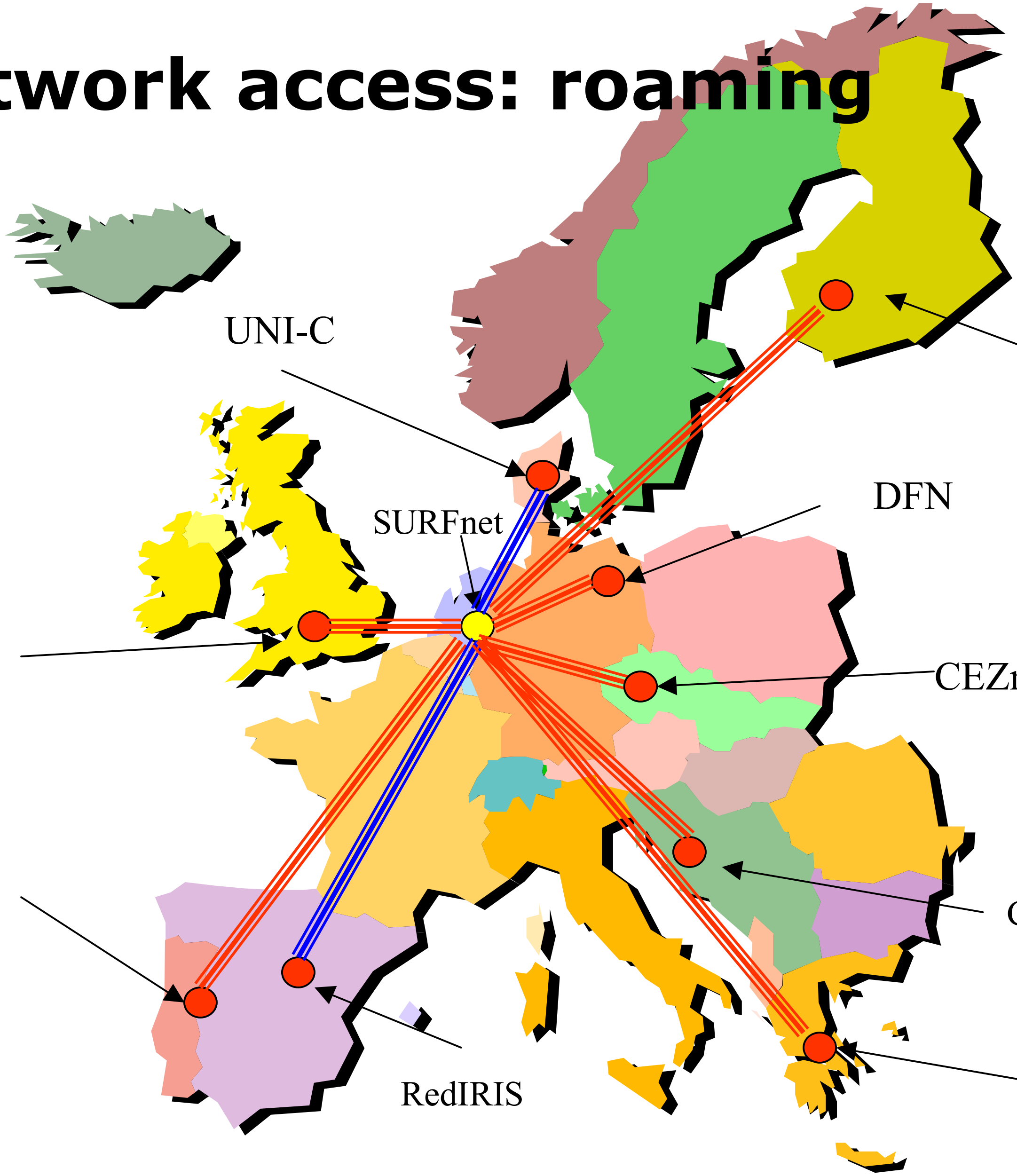
Why AAI?
Reduce the digital key ring!

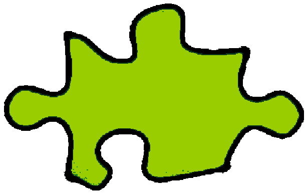
Ingredients of an AAI



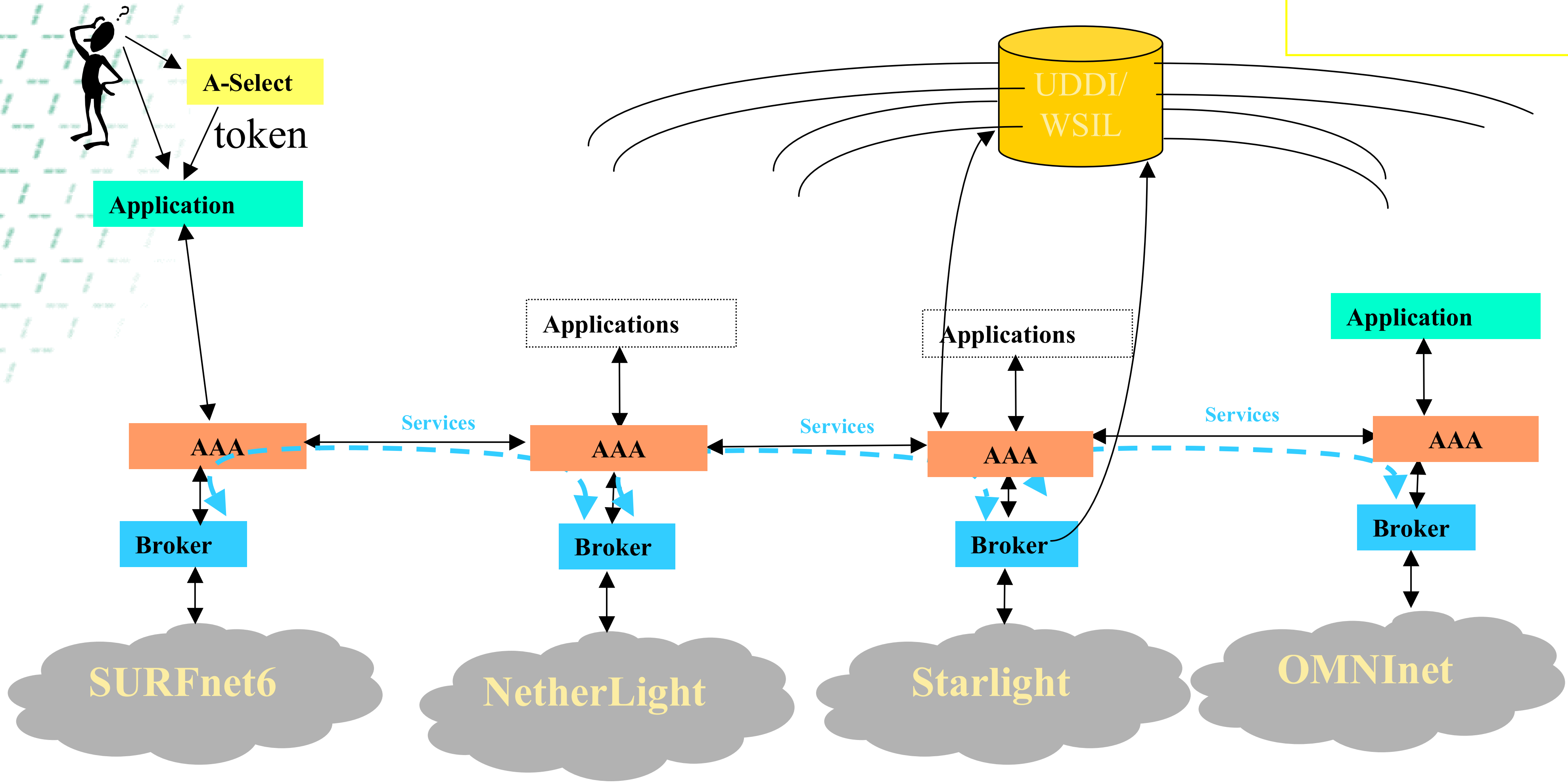
Network	Authorisation	(web)Application
Authentication	Login	xxx
xxx	Administration	xxx

Network access: roaming

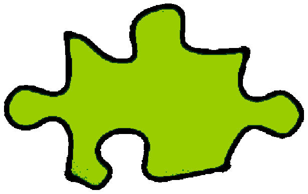




Network access: user-controlled light paths



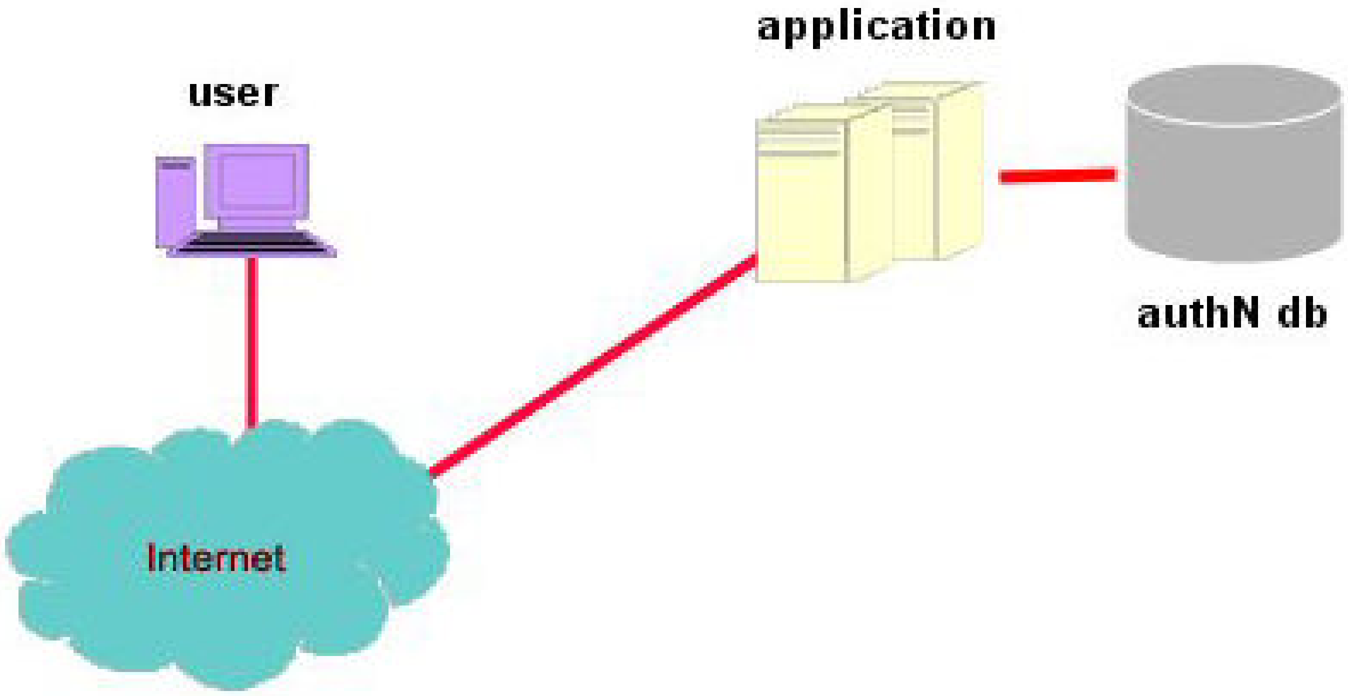
Network access: Who can connect?



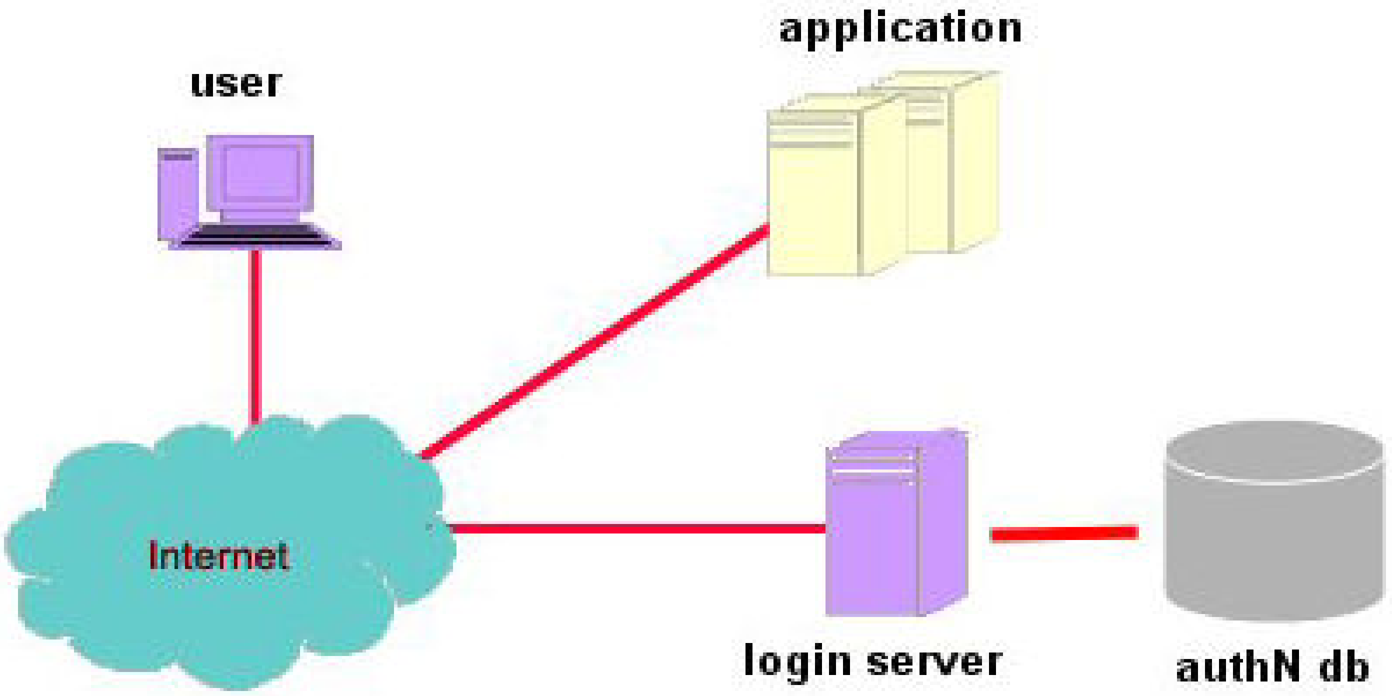
- Commercial WiFi providers
- Commercial backup service providers

- Needed:
  - Acceptable use policy
  - Federation(s)
  - More attributes?

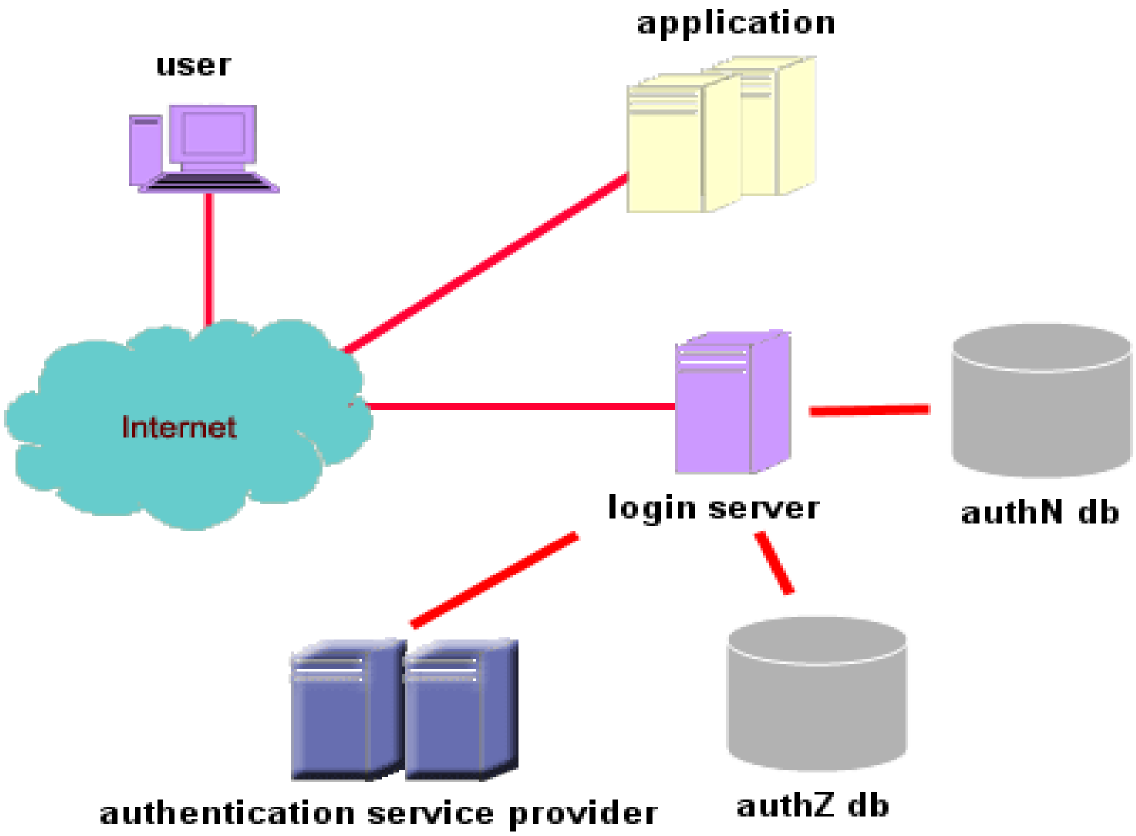
Application access: centralise intelligence



Application access: centralise intelligence

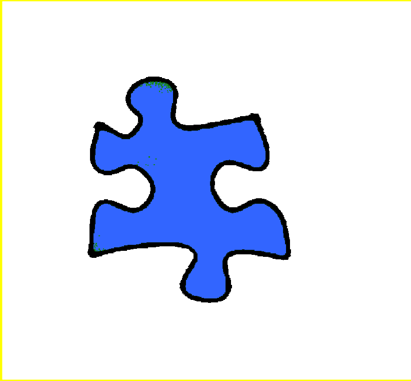


Login server: intermediary between application and AA

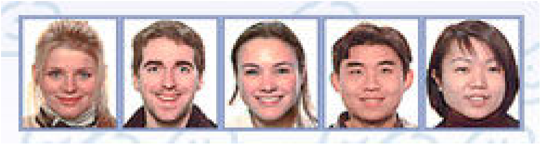


Authentication: user perspective

Authentication: choose your own method

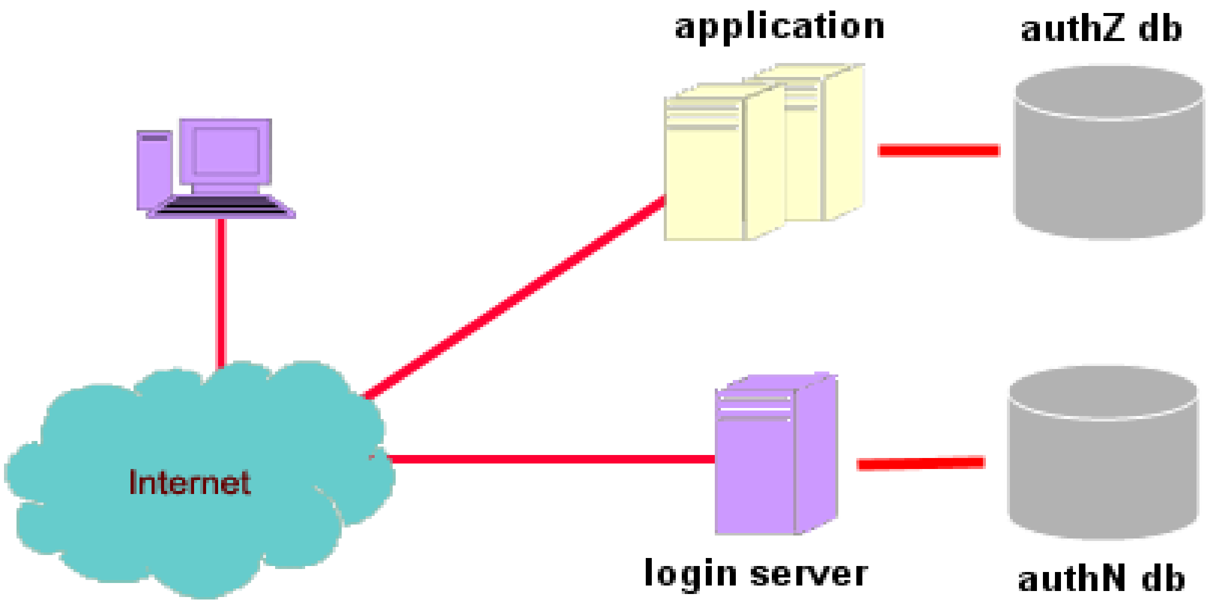


- IP address
- Username / password
  - LDAP
  - RADIUS
  - SQL
- Passfaces
- PKI certificate
- OTP through SMS
- OTP through internet banking
- Tokens (SecurID, Vasco, …)
- Biometrics

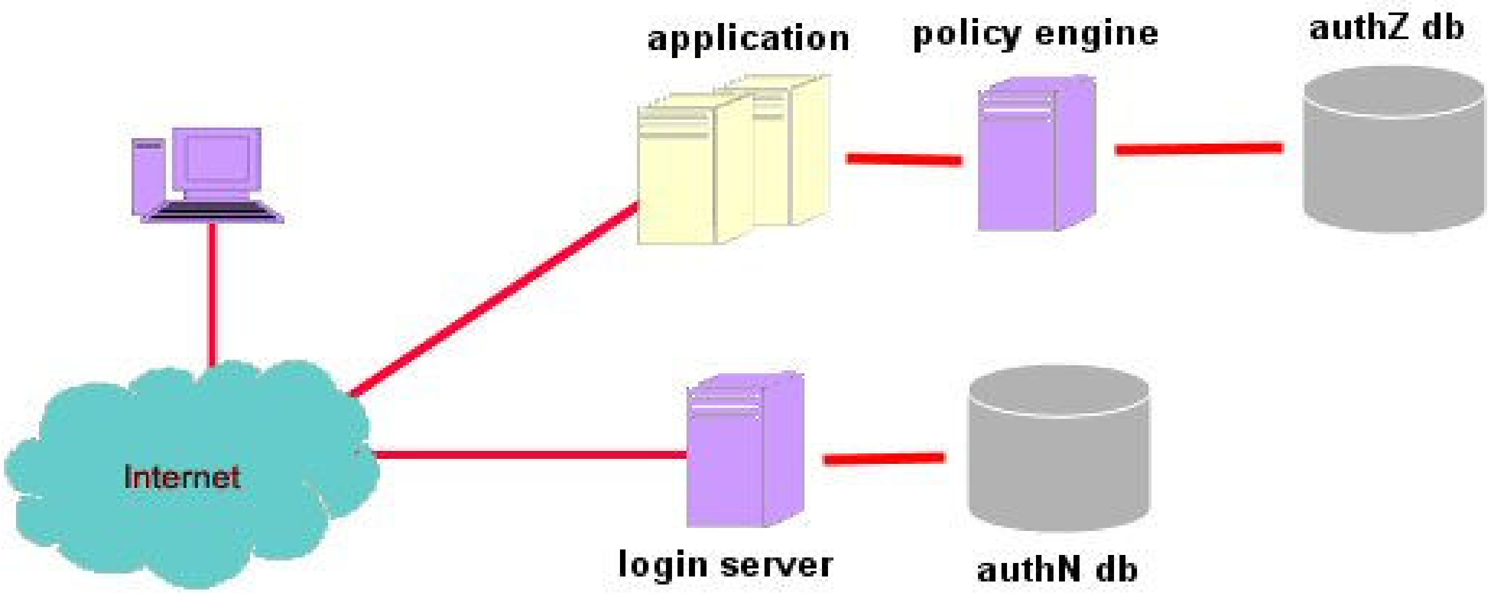


SURFKEY

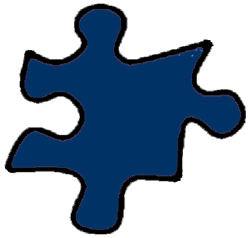
Authorisation: Policy engines



Authorisation: Policy engines



Authorisation:
3 scenario’s



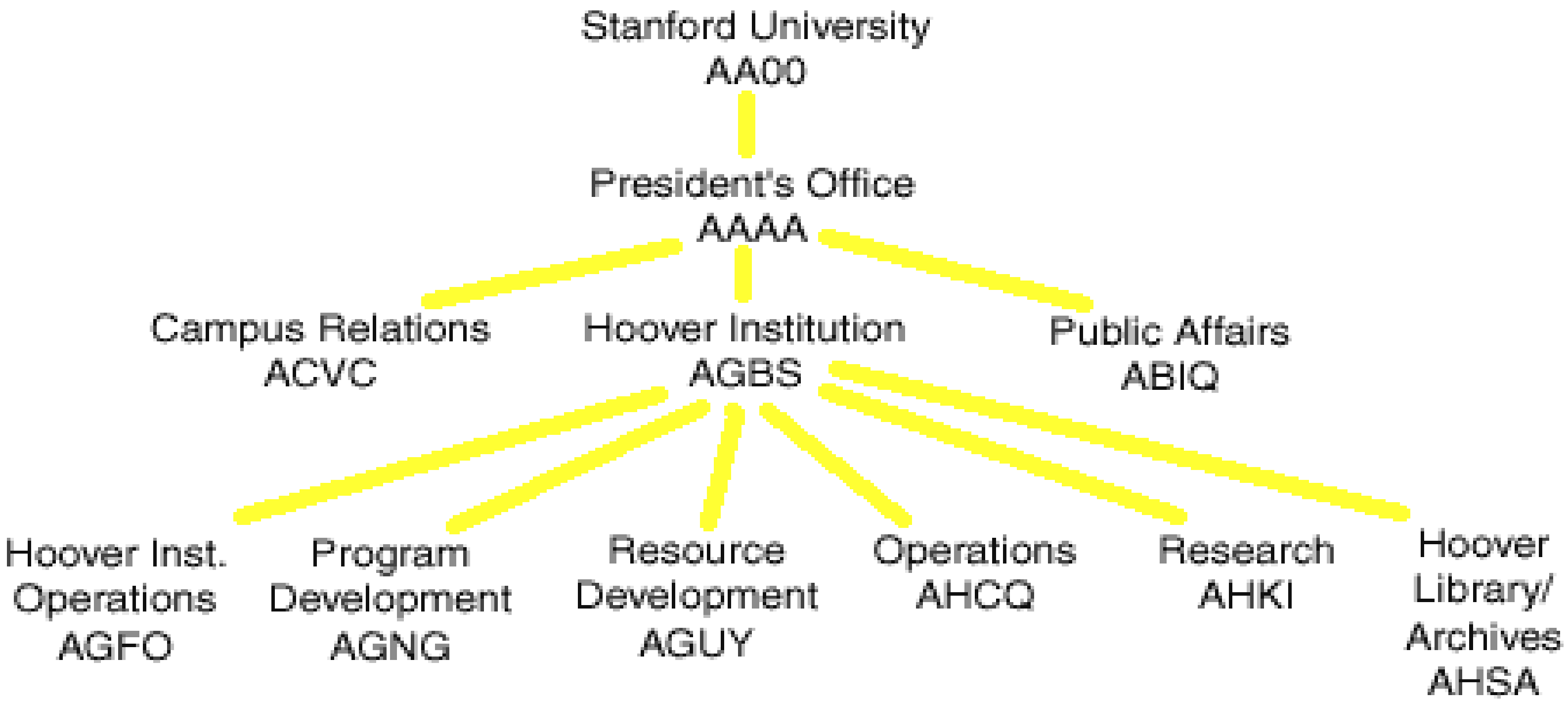
1. Authentication = authorisation

2. Identity plus a few attributes

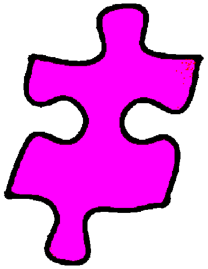
3. Privacy-preserving negotiation about attributes to be exchanged

Authorisation: privilege management

NEW!

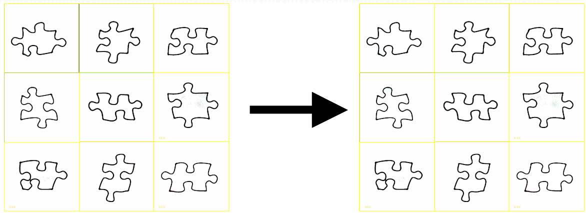


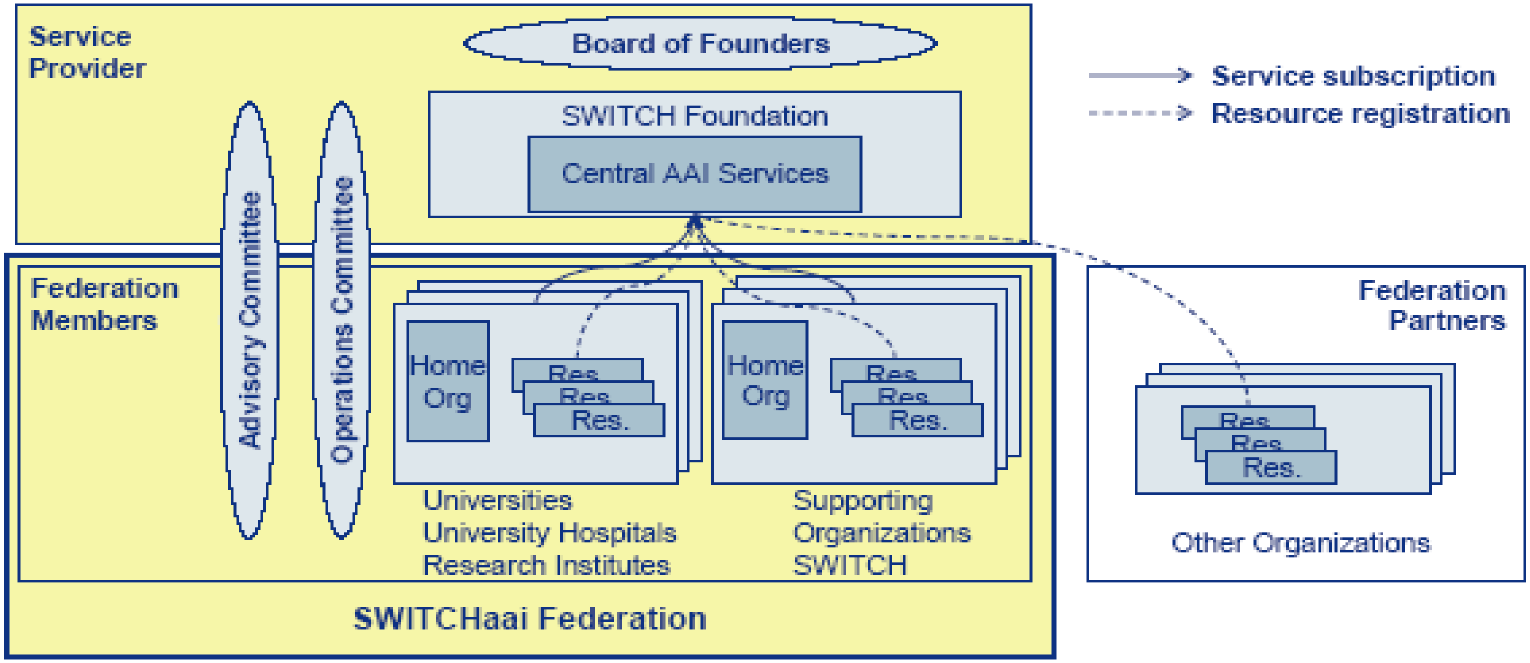
Administration:
Identity Management



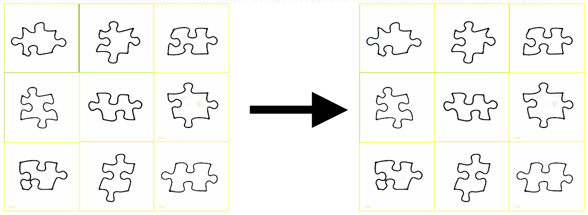
- How to record the identities, credentials (attributes or roles), and privileges?
- Enterprise (or meta) directory to glue all sources of information together
- It’s the underlying basis for an AAI!
- …and it’s a hype…

Cross-domain AA: Federations



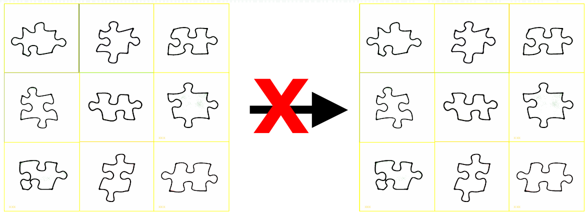


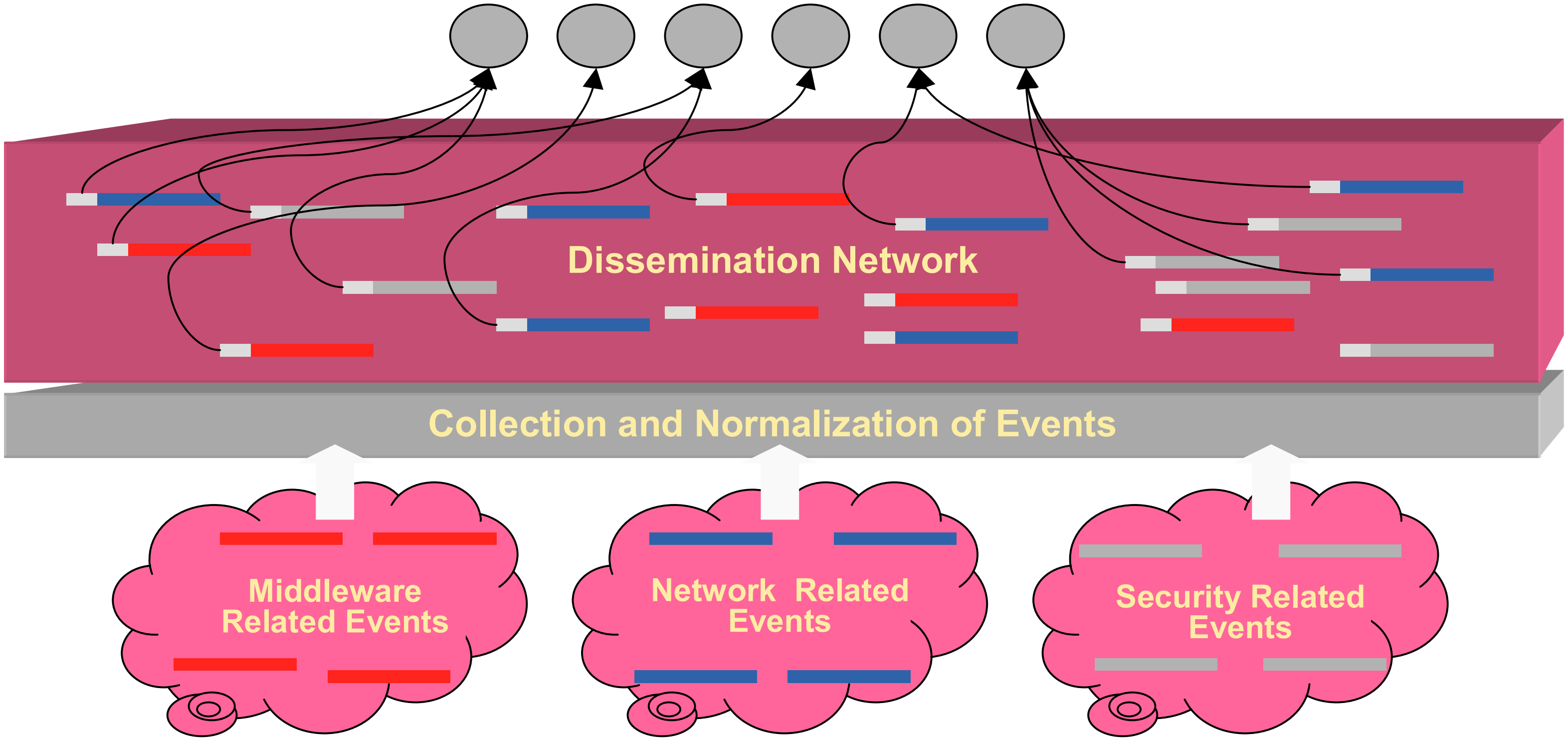
Cross-domain AA: Ingredients



- Policies (e.g. InCommon):
  - Federation Operating Practices and Procedures
  - Participant Agreement
  - Participant Operating Practices
- Technologies:
  - PKI
  - Schema’s

E2e diagnostics: what if there’s an error?





Dissemination Network

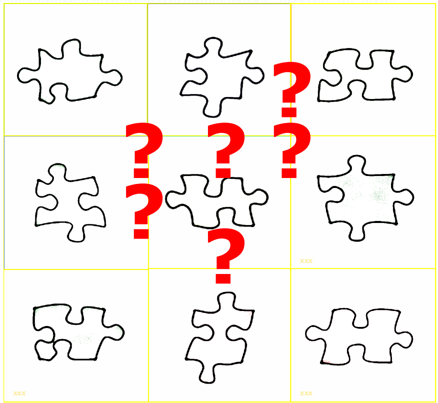
Collection and Normalization of Events

Middleware Related Events

Network Related Events

Security Related Events

What about…
…standards?

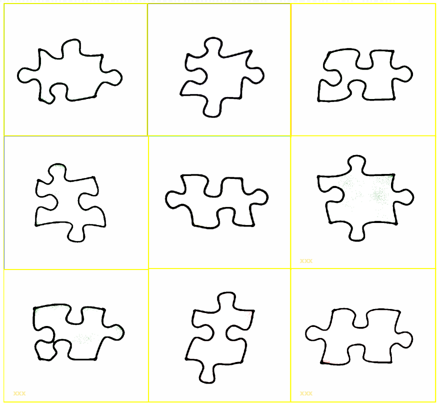


- Currently many proprietary solutions (sockets, cookies, redirects, …)
- Webservices
  (SOAP, XML RPC, WSDL, WS-*)
- SAML

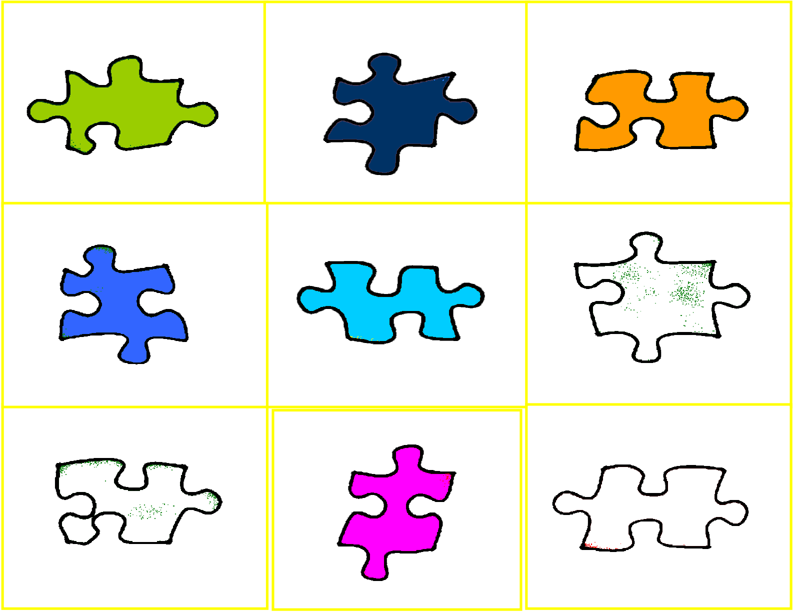
- For federations:
  - WS-Federation (Microsoft, IBM)
  - SAML (OASIS: 150 companies, Internet2)
  - Liberty Alliance (Sun, 170 companies)

And the future...?

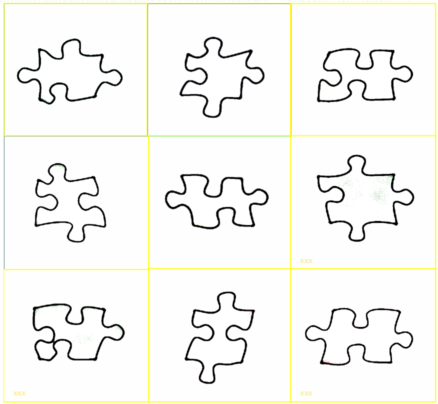
- Converging or dominant standard(s)
  - Means better interoperability between the pieces of the puzzle
- Universal single sign-on across network and application domain
  - Convergence of EduRoam and weblogin services
  - Including non-web-based applications

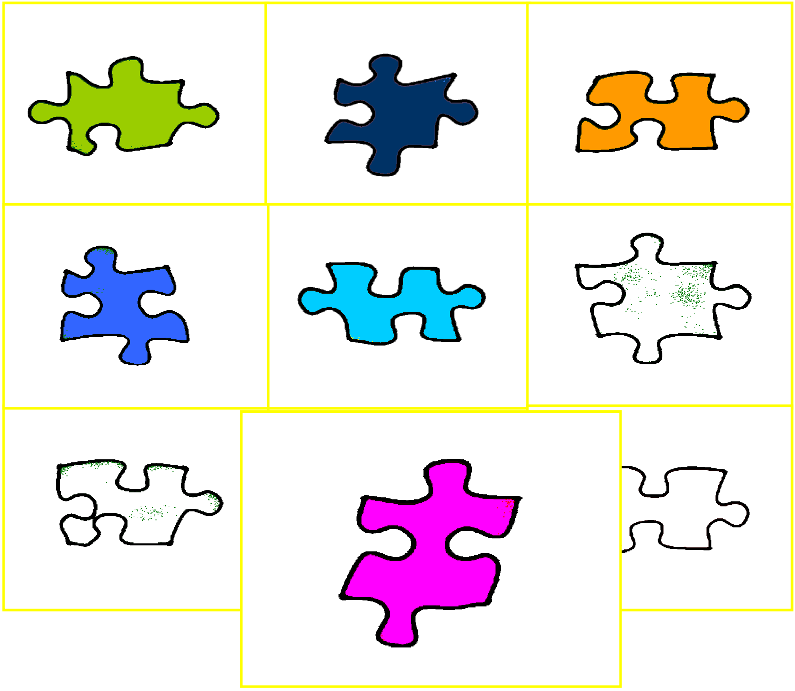


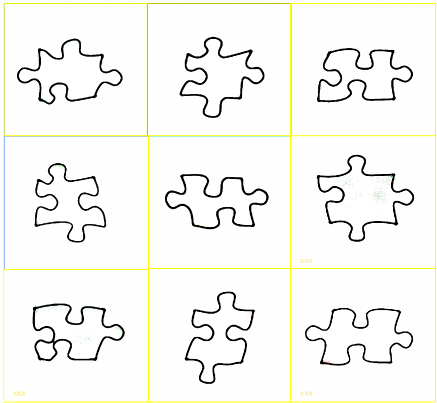
Homework:
Manage your identities!



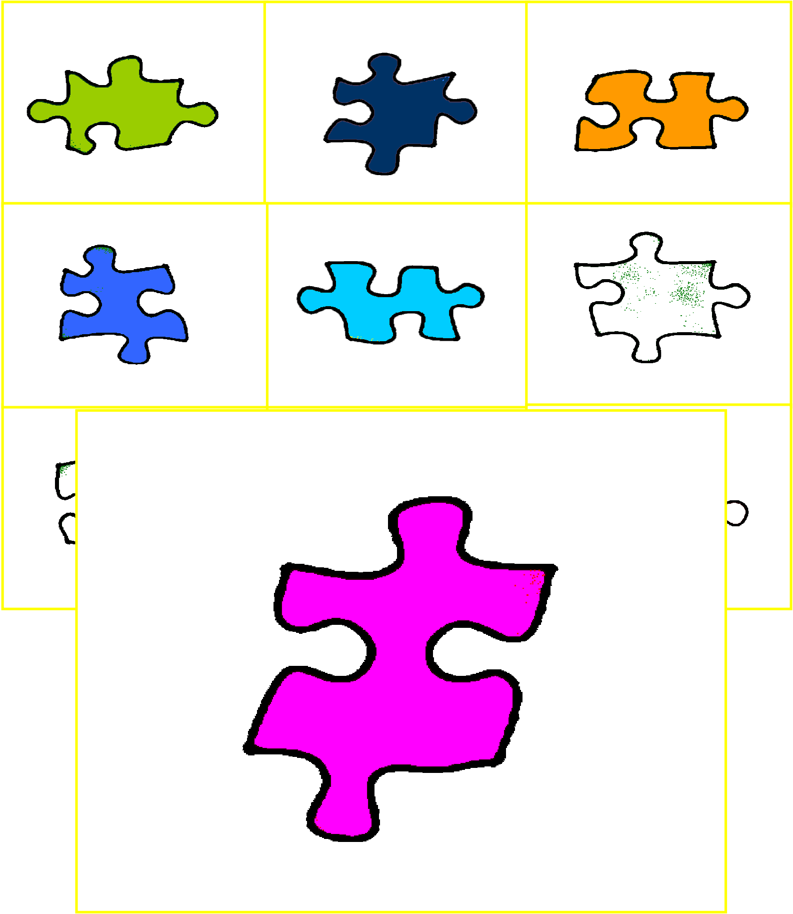
Homework:
Manage your identities!

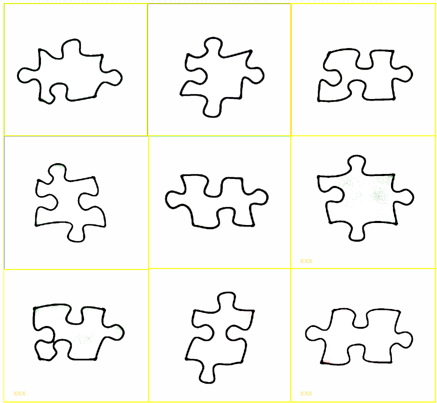






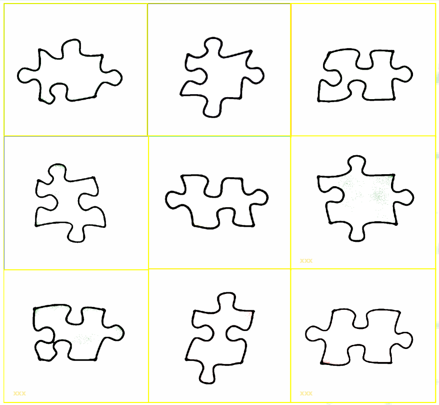
Homework:
Manage your identities!





References

- Identity Management
- EduRoam
- A-Select weblogin
- Privilege Management
- Intro on federations
- Internet2 Federation
- Swiss Federation
- End-to-end diagnostics



Thank you!

Questions?