

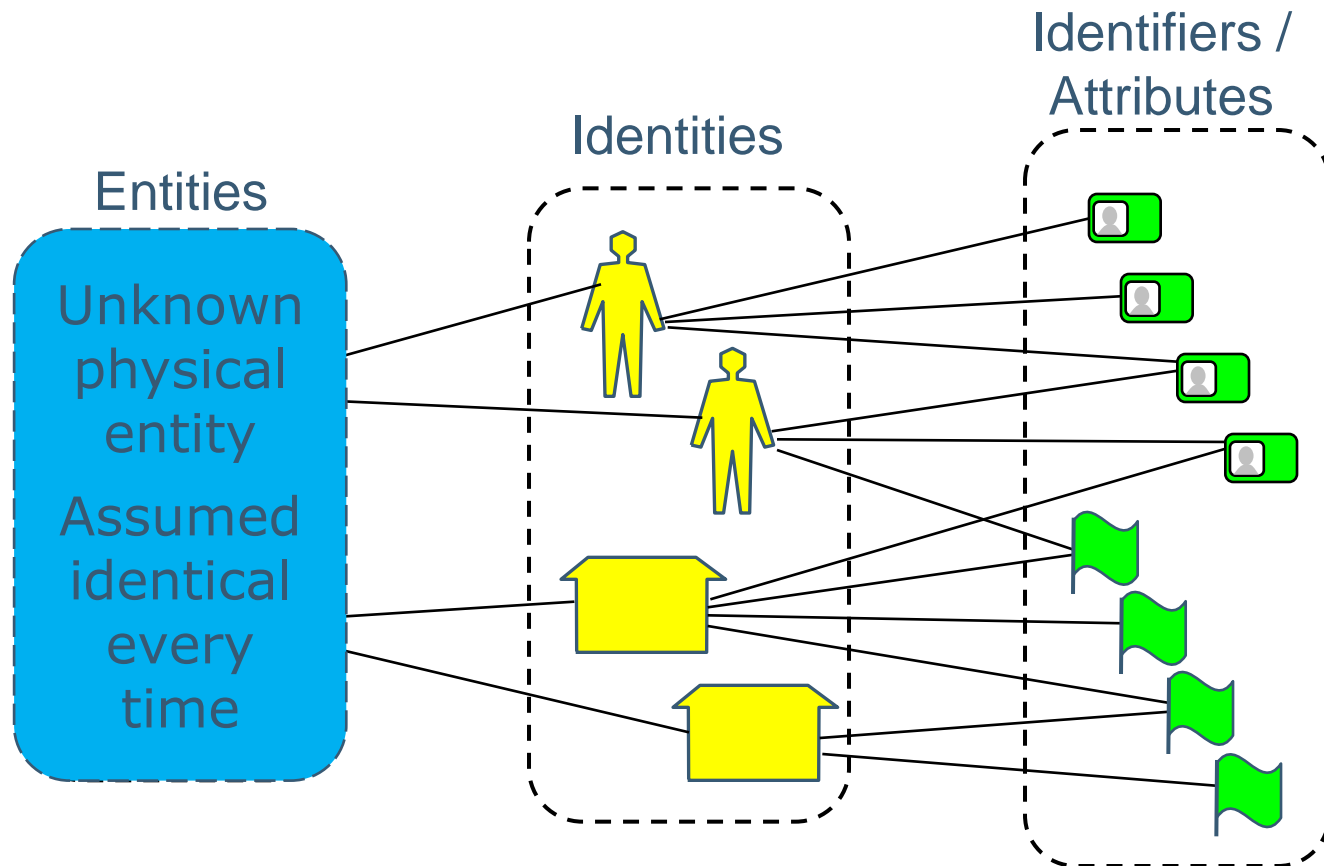


# Research Challenges in Identity Management

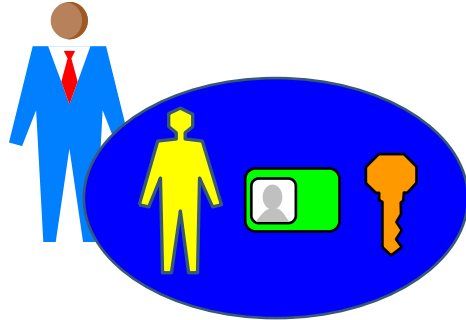
AF Security  
14 August 2008

Audun Jøsang, UNIK  
<http://www.unik.no/people/josang/>

# Relationship between Entities, Identities and Identifiers

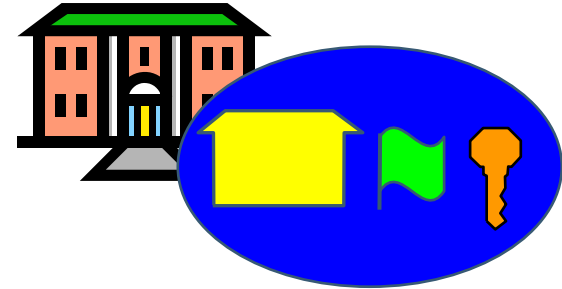


# Who's identity?



## User Ids:

- Issued by: SPs & IdP
- Managed by users & SPs
- Application layer authentication
- Traditional identity management

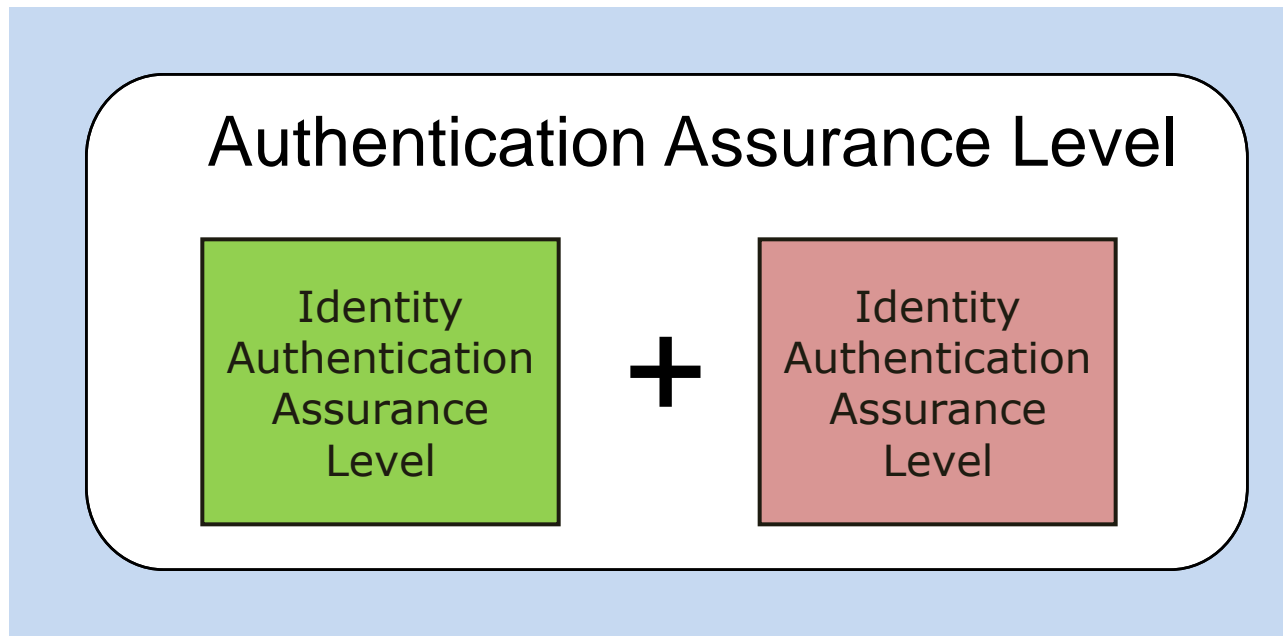


## SP Ids:

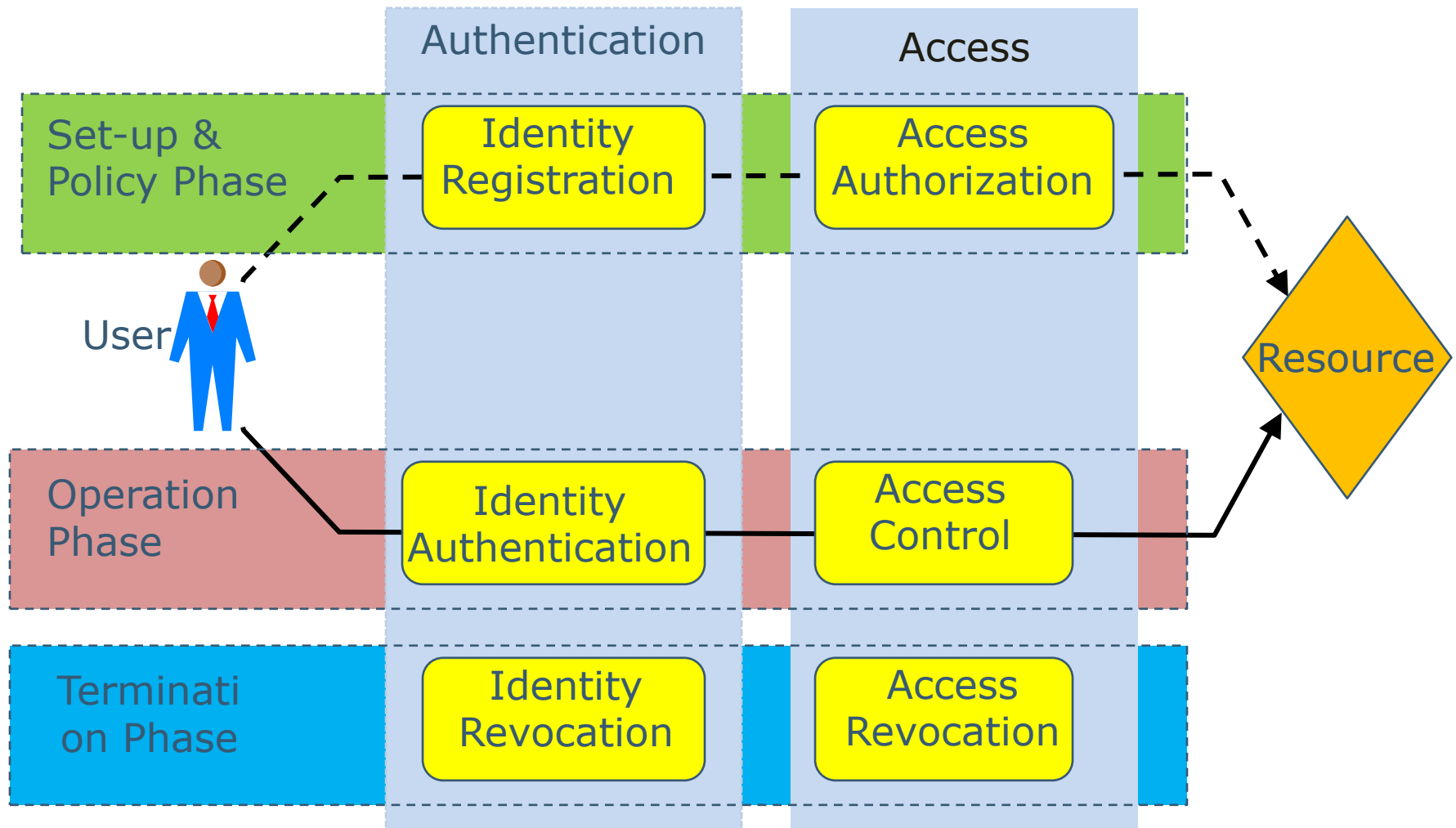
- Issued by DNS registrars & CAs
- Managed by users & SPs
- Transport layer authentication
- Traditionally part of web security

# Authentication Assurance Level (AAL)

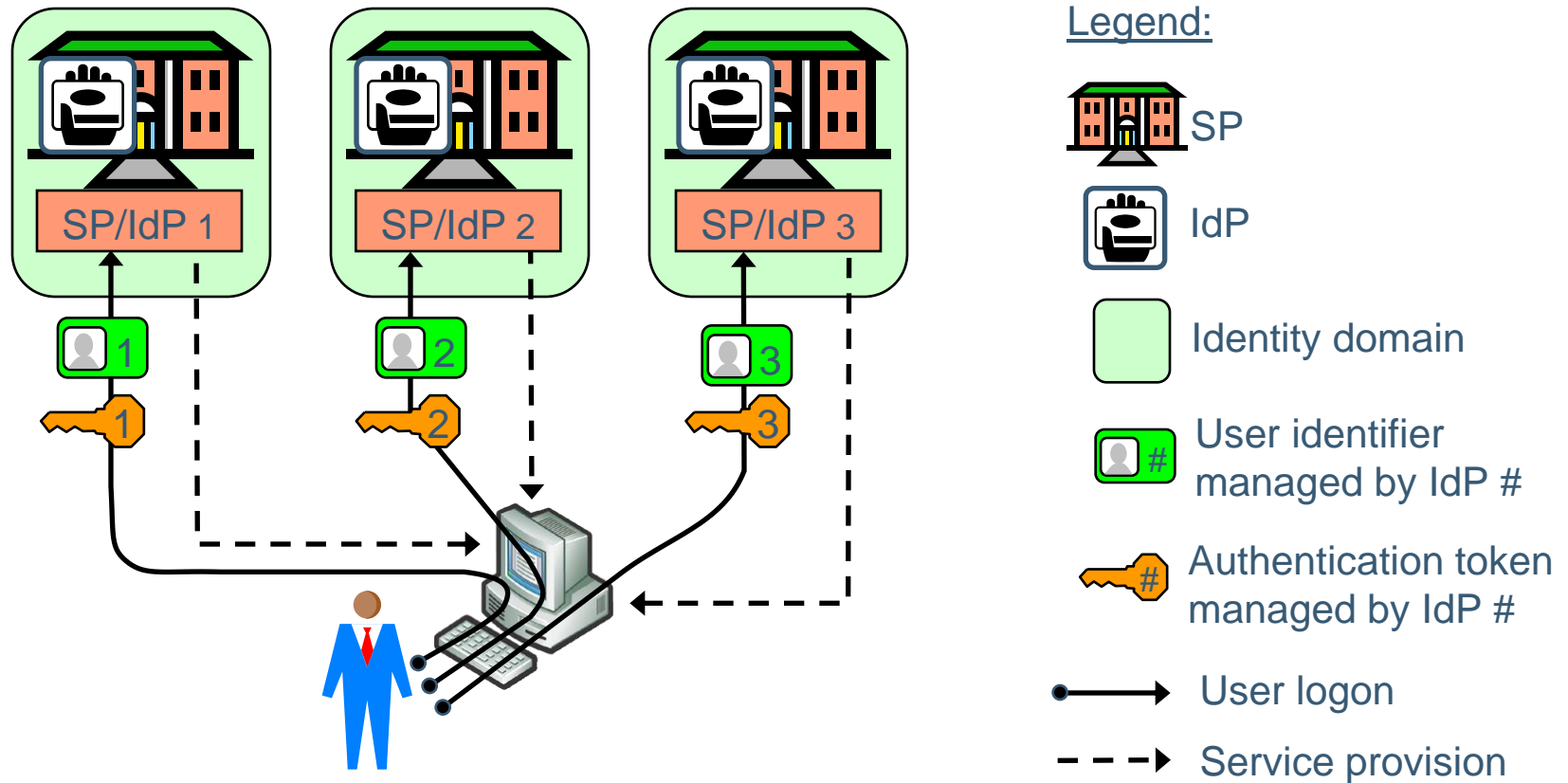
- AAL is a combination of
  - Identity Registration Assurance Level (IRAL)
  - Identity Authentication Assurance Level (IAAL)



# Authentication and Access

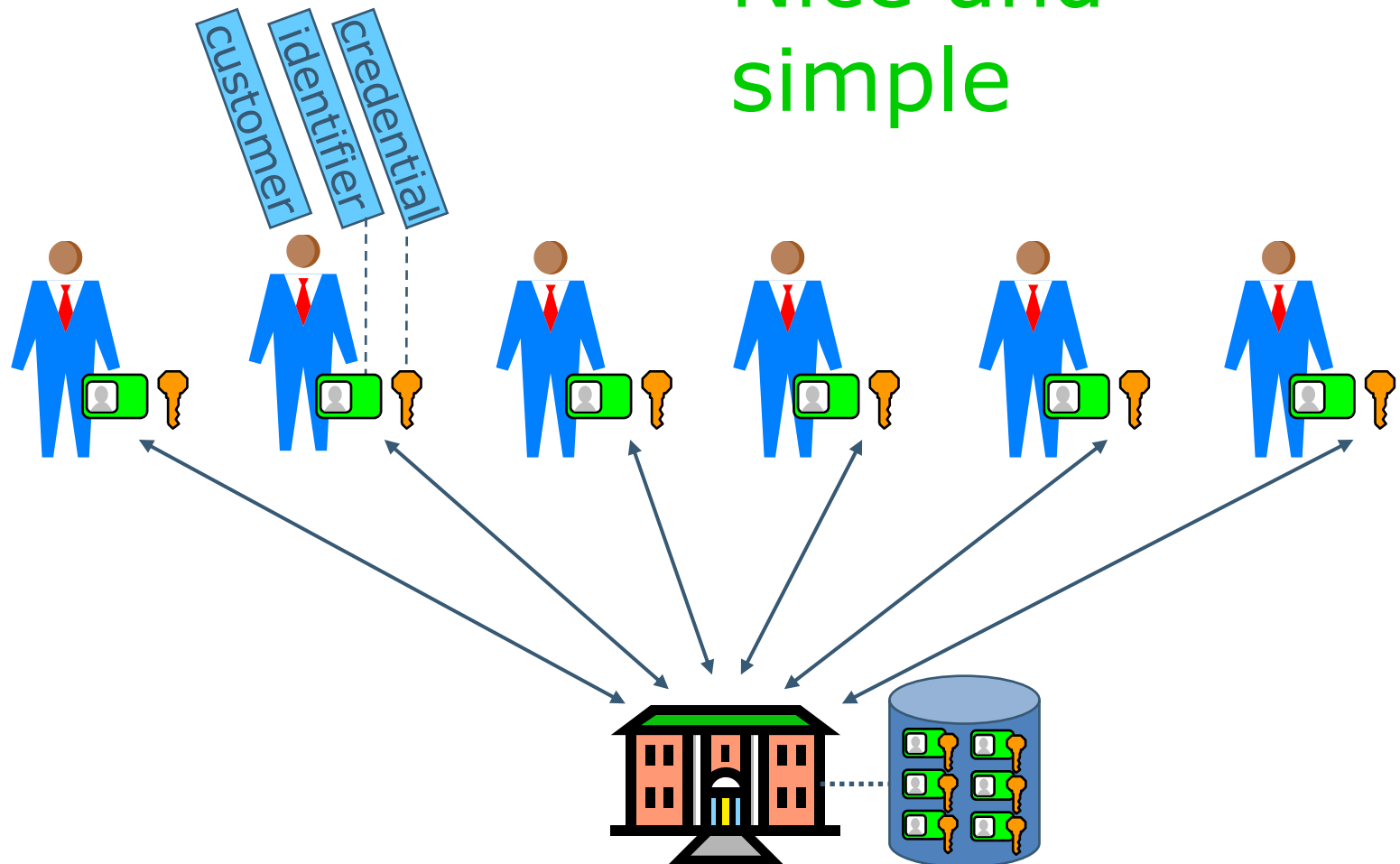


# Silo domain model



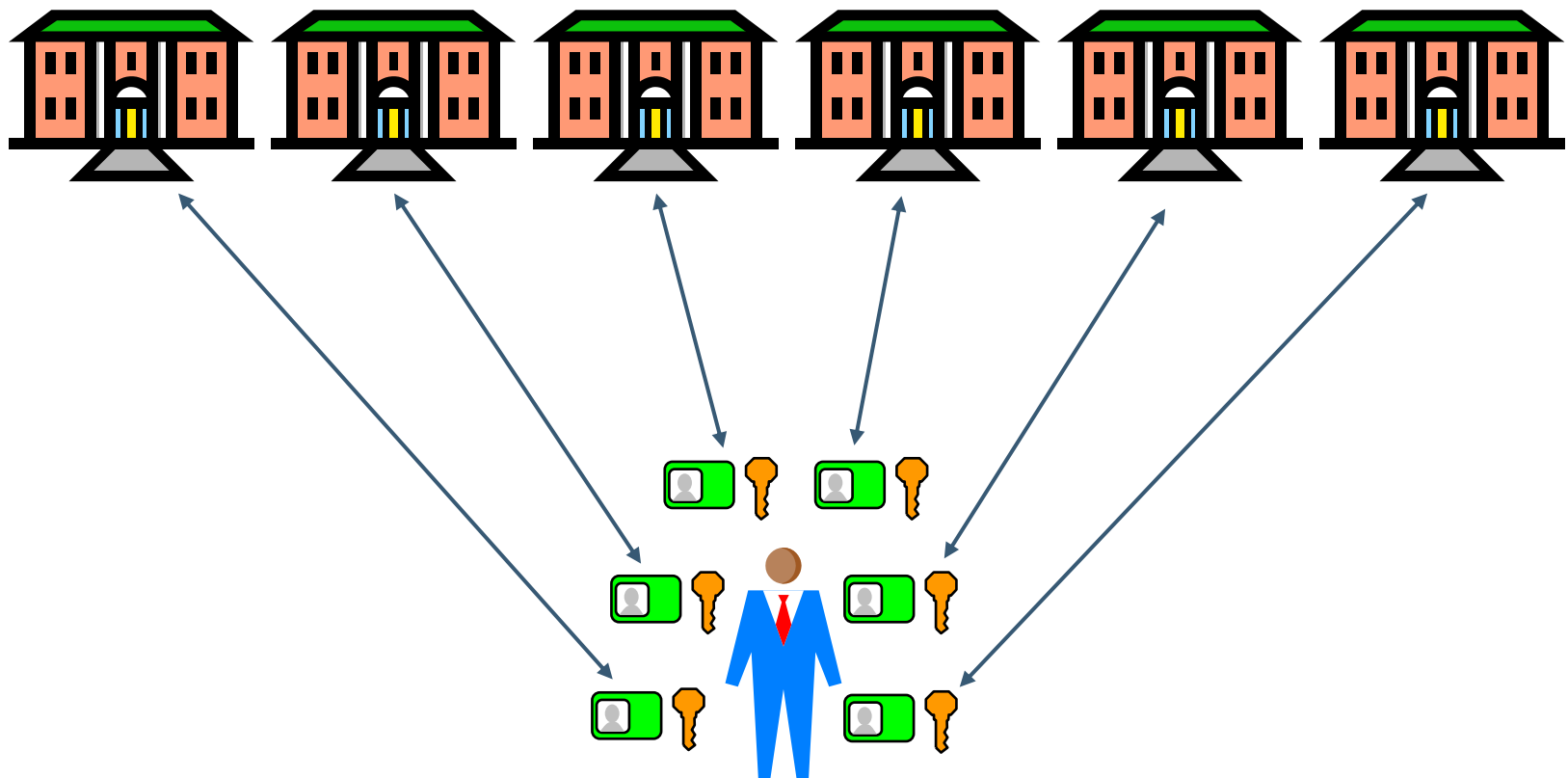
# *Imagine you're a service provider*

Nice and simple



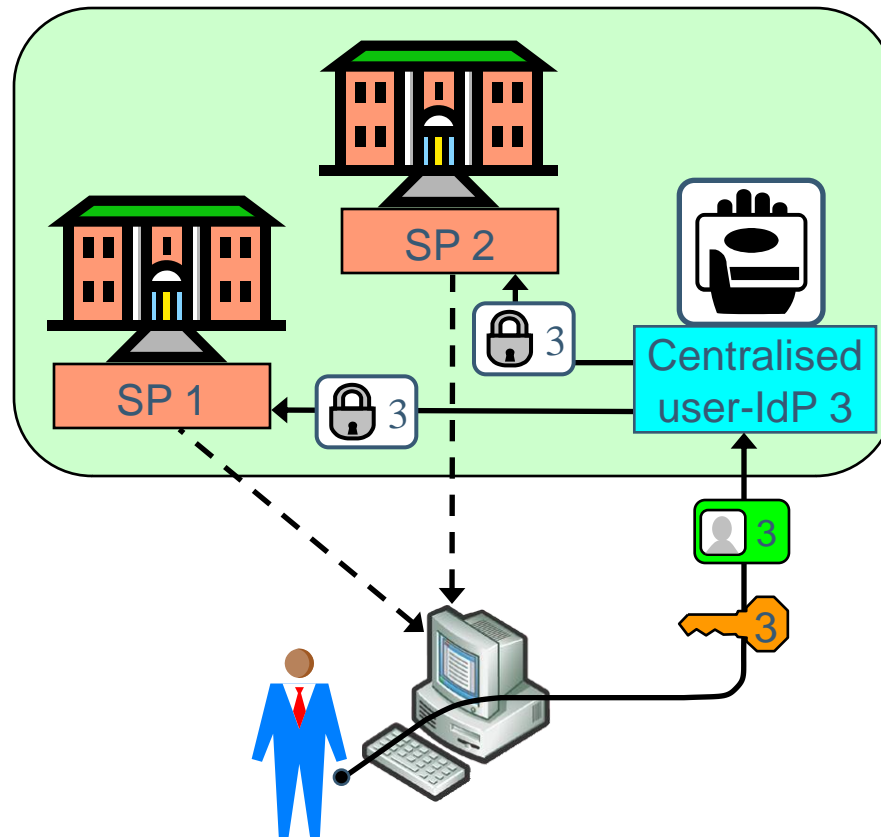
*Imagine you're a customer*

**It's a  
nightmare**

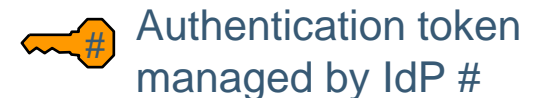
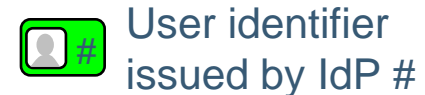




# Traditional Single Sign-On (SSO)

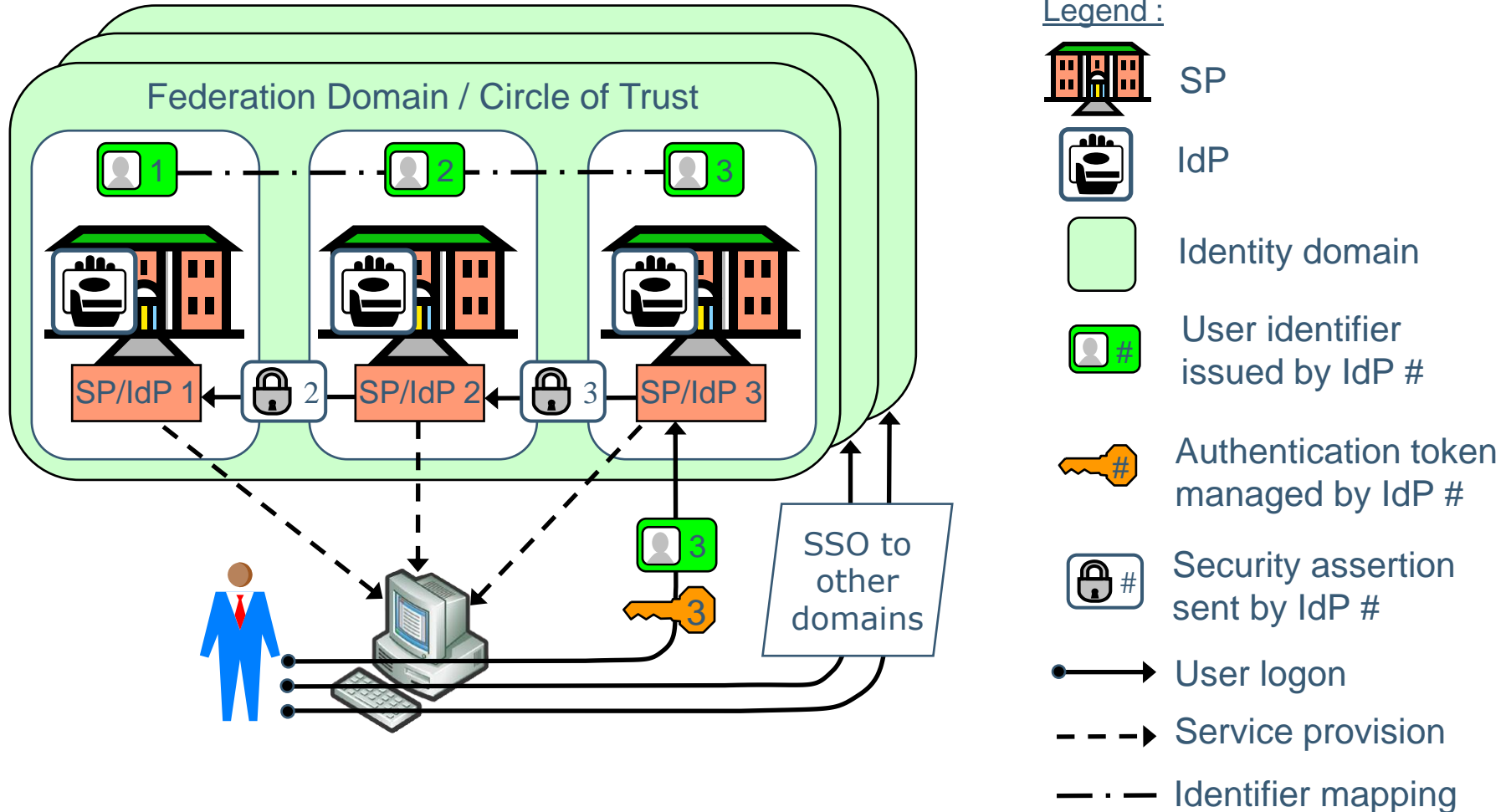


## Legend:



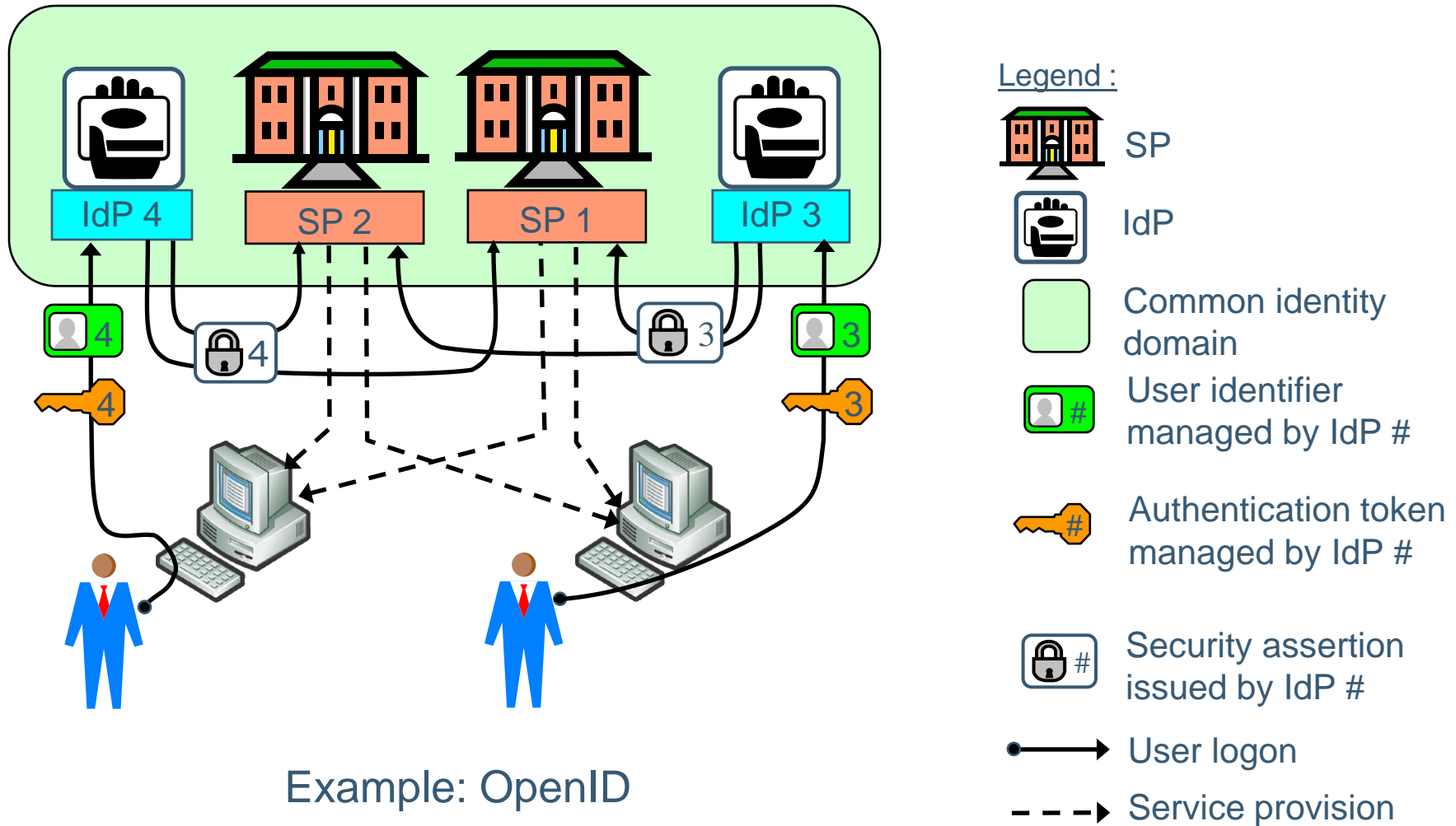
Examples: Kerberos,  .net Passport

# Federated SSO model



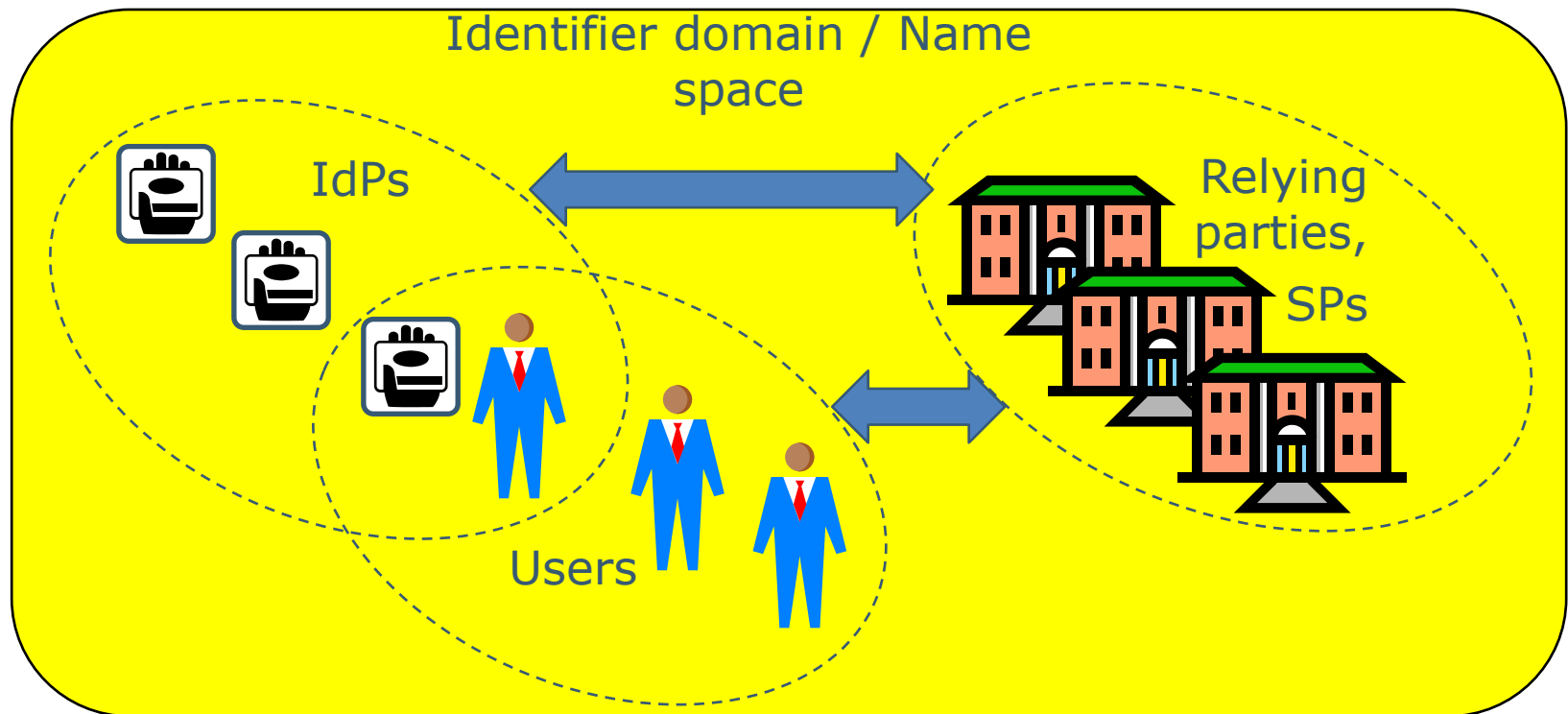
Examples: Liberty Alliance, SAML2.0, WS-Federation, Tivoli, Shibboleth

# Distributed SSO identity model

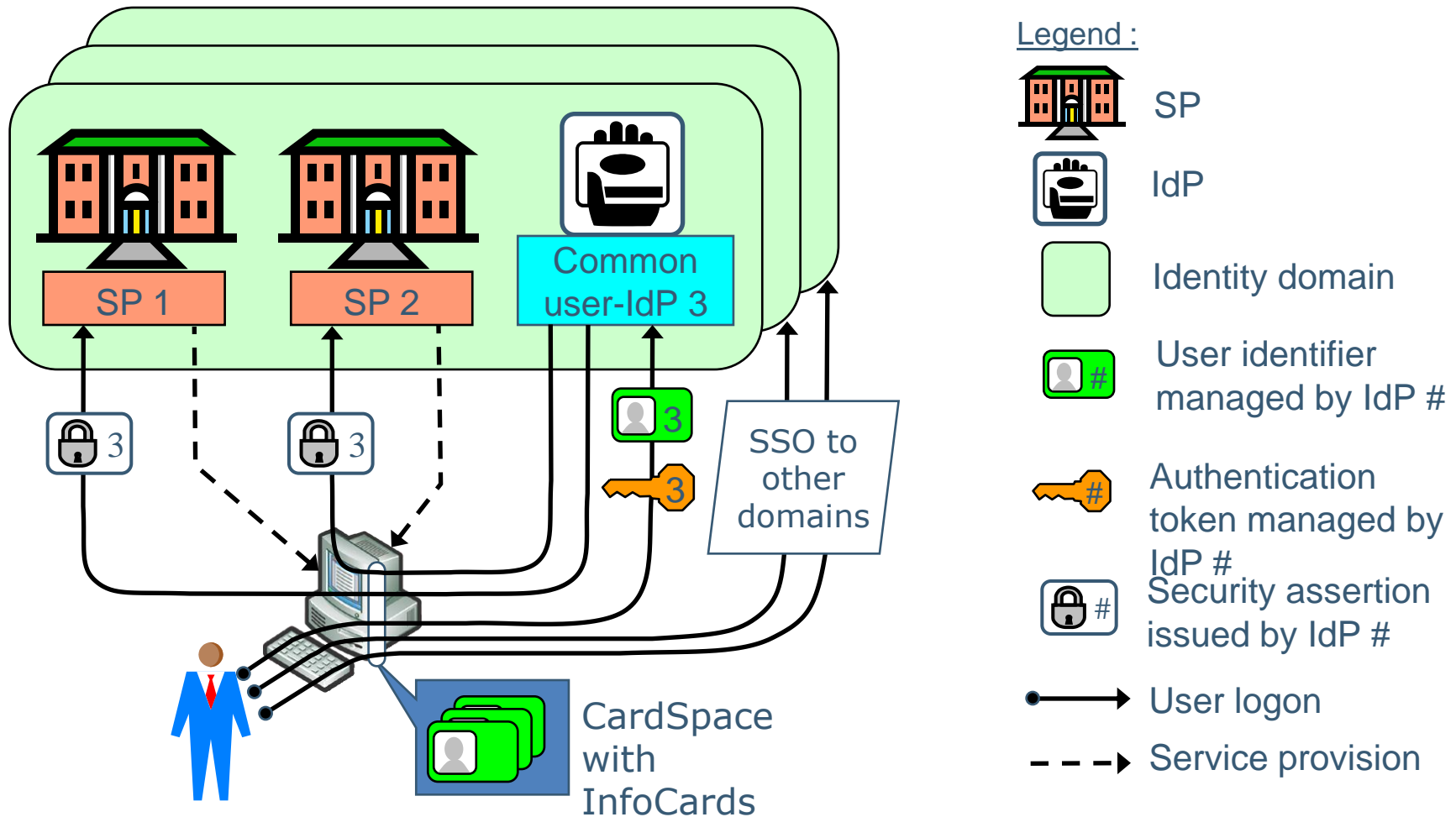


# OpenID distributed SSO

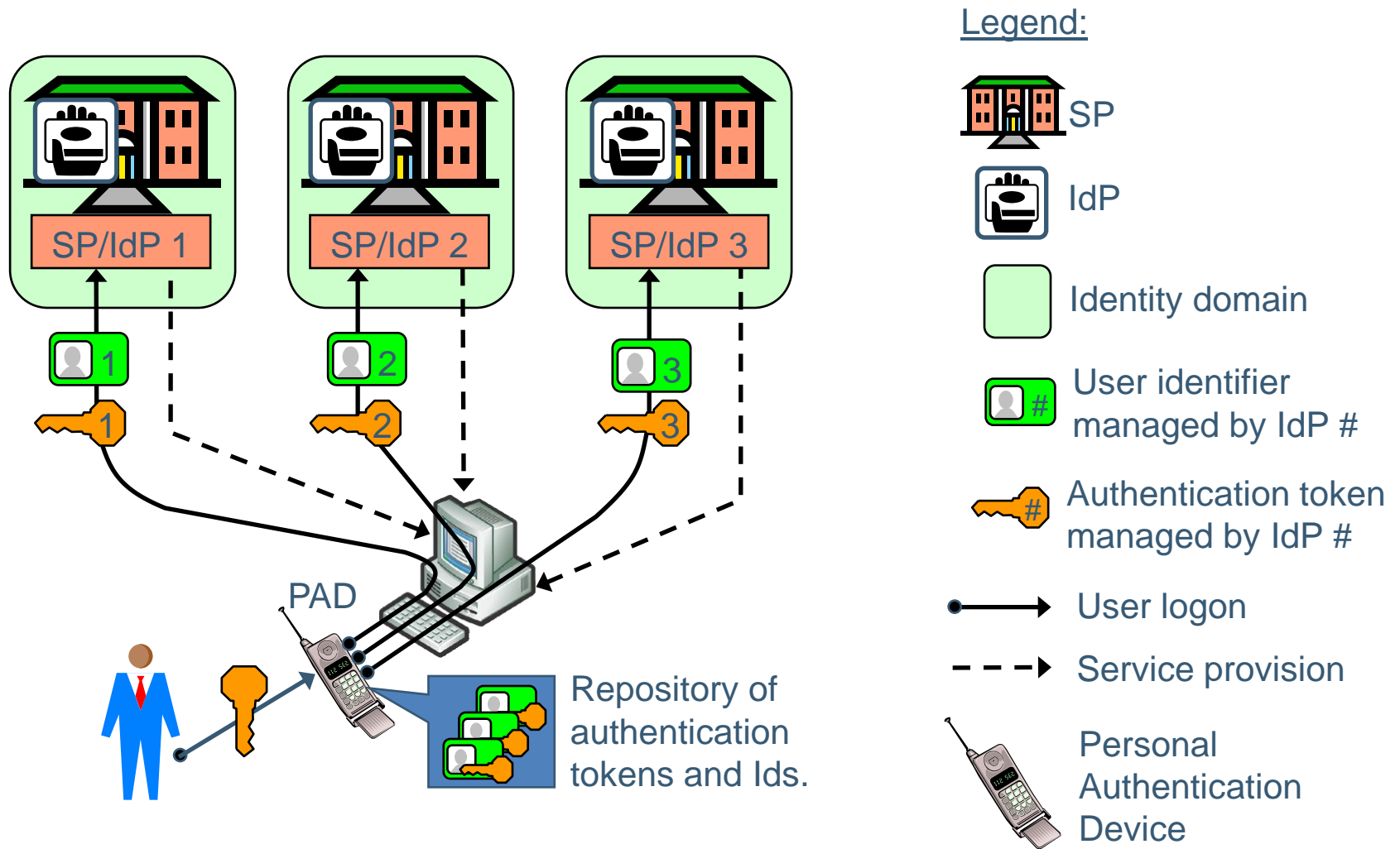
- Common name space
- Distributed IdPs
- No authorities



# Microsoft's InfoCard model

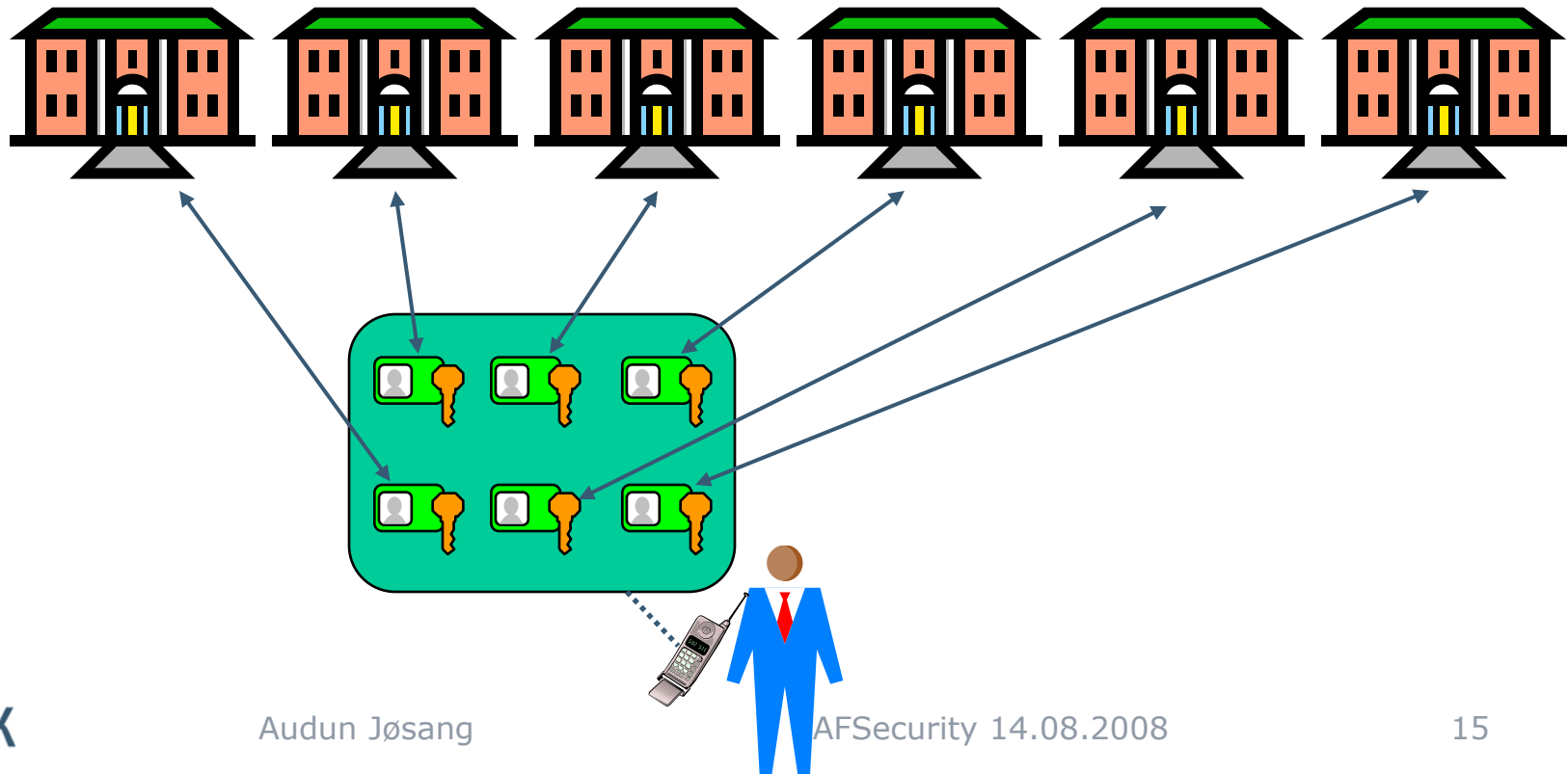


# User centric model



# User centric SSO: Imagine you're a customer

It's a dream

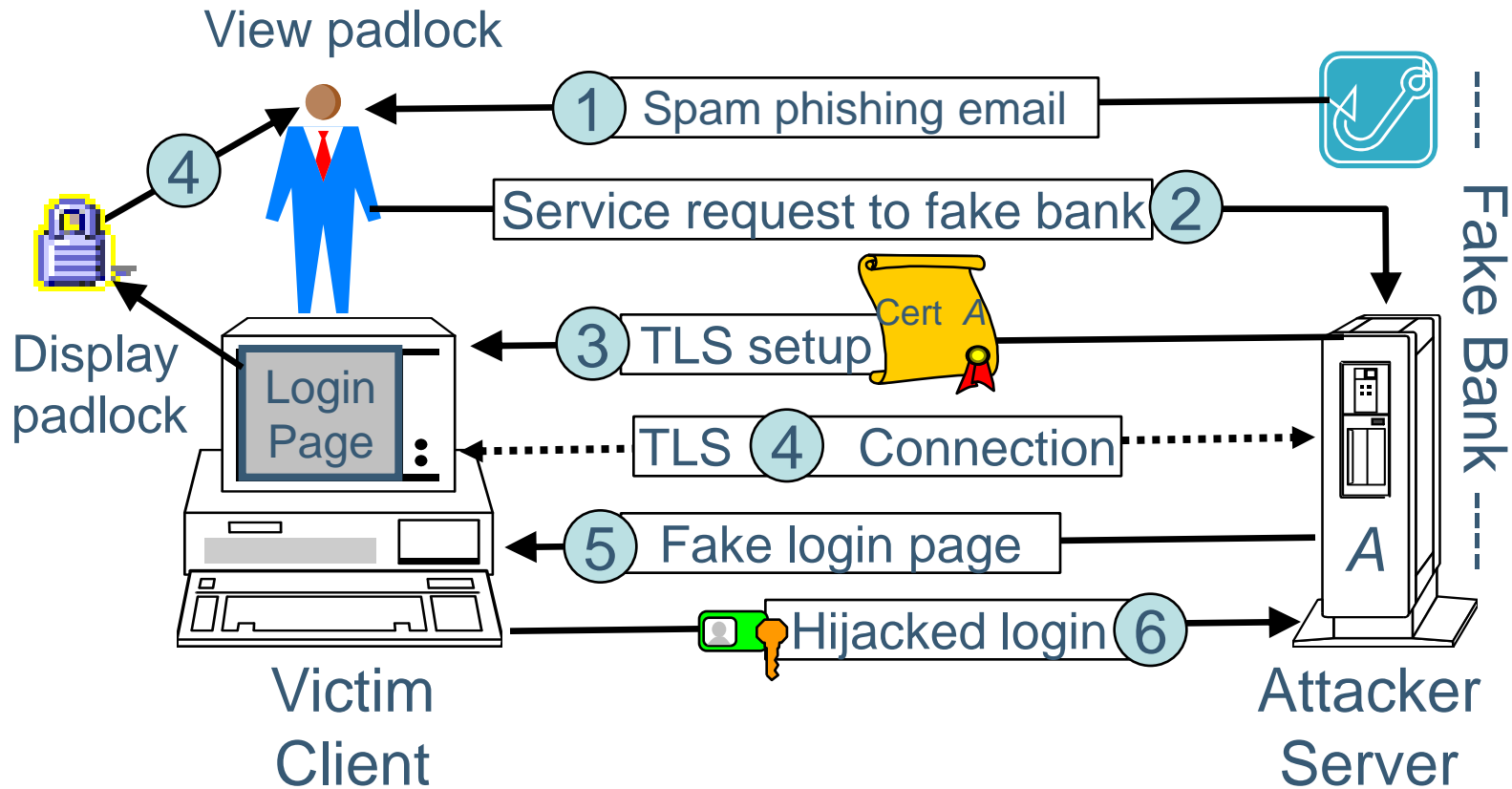


# Closer look at SSO

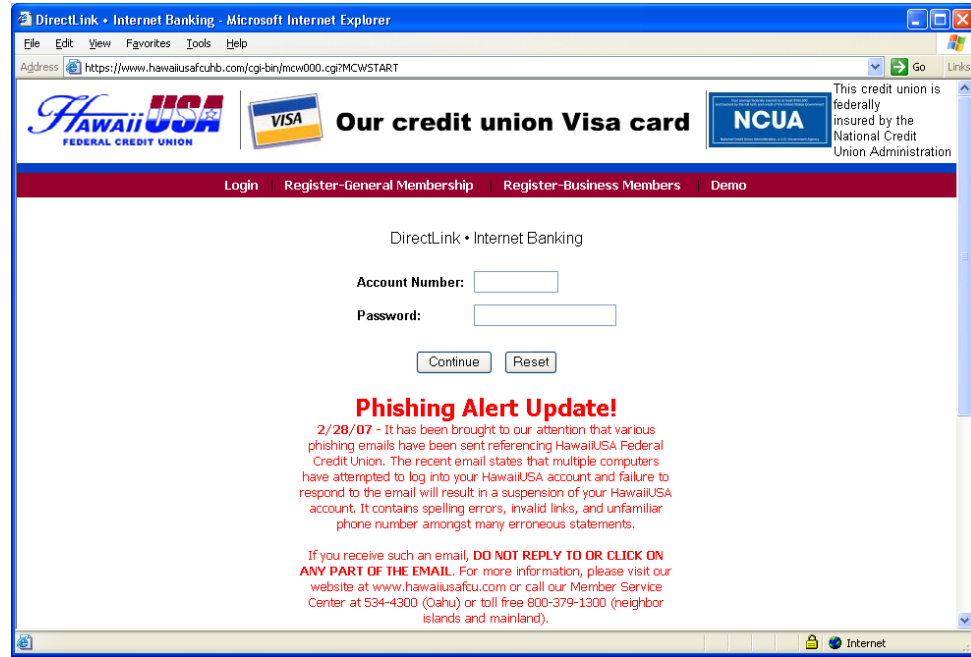
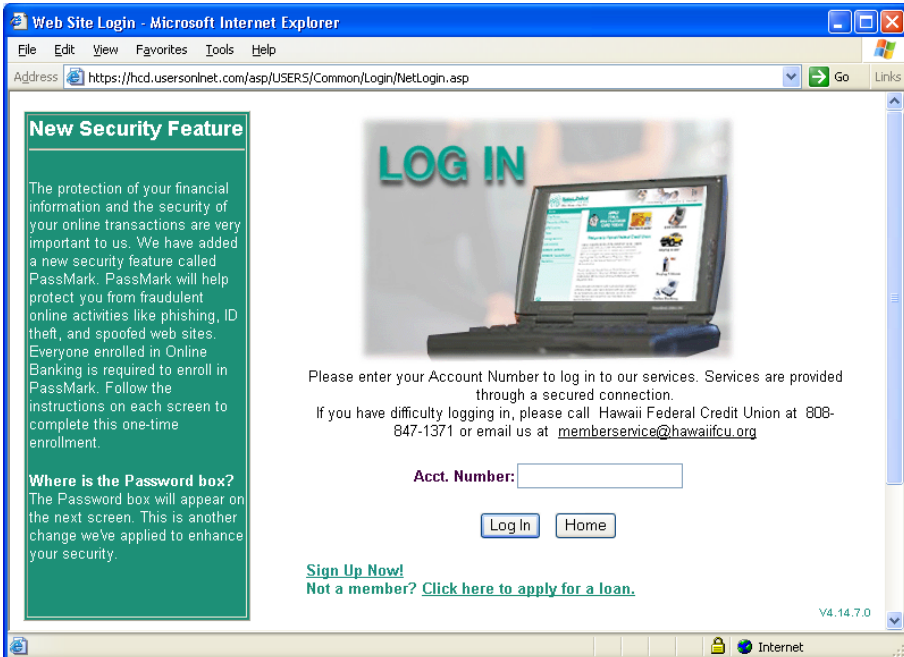
- Single manual sign-on
- Automated sign-on every time
- Where is the automation technology?
  - Both client & server side: Kerberos
  - Server side: Federation, CardSpace, Sxip, OpenId
  - Client side: User-centric model
- Business models based on data collection
  - Requires server side technology
- User-centric model prevents data collection



# Phishing: Failed server authentication



# A phishing example: Hawaii Federal Credit Union



## Genuine bank login

<https://hcd.usersonlnet.com/asp/USERS/Common/Login/NettLogin.asp>

## Fake bank login

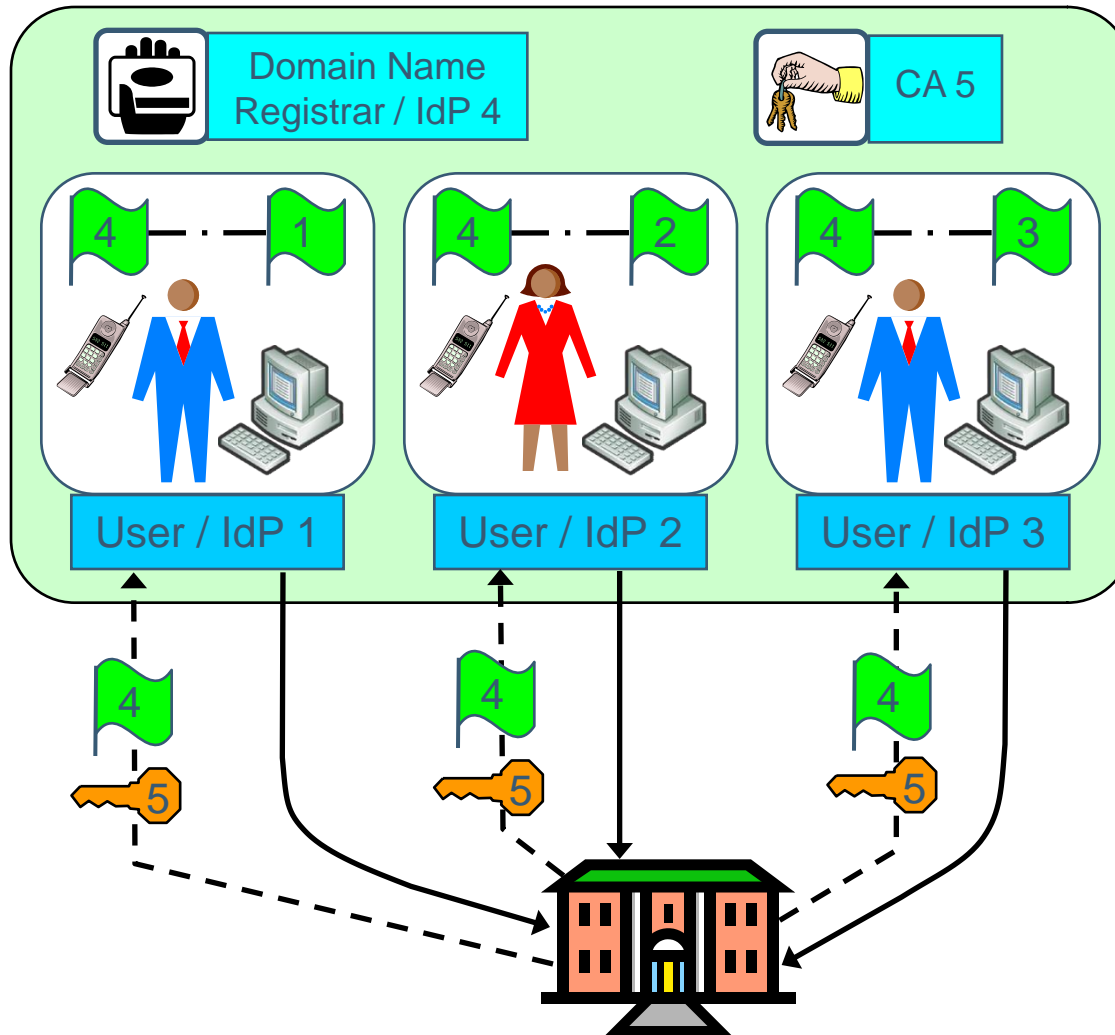
<https://hawaiiusafcuhb.com/cgi-bin/mcw000.cgi?MCWSTART>

# Identifier characteristics











- Local or global
- Assigned by authority or self assigned
- Permanent or temporary
- Reassignable or not
- Persistent or not
- Human or machine readable

# SP identity management

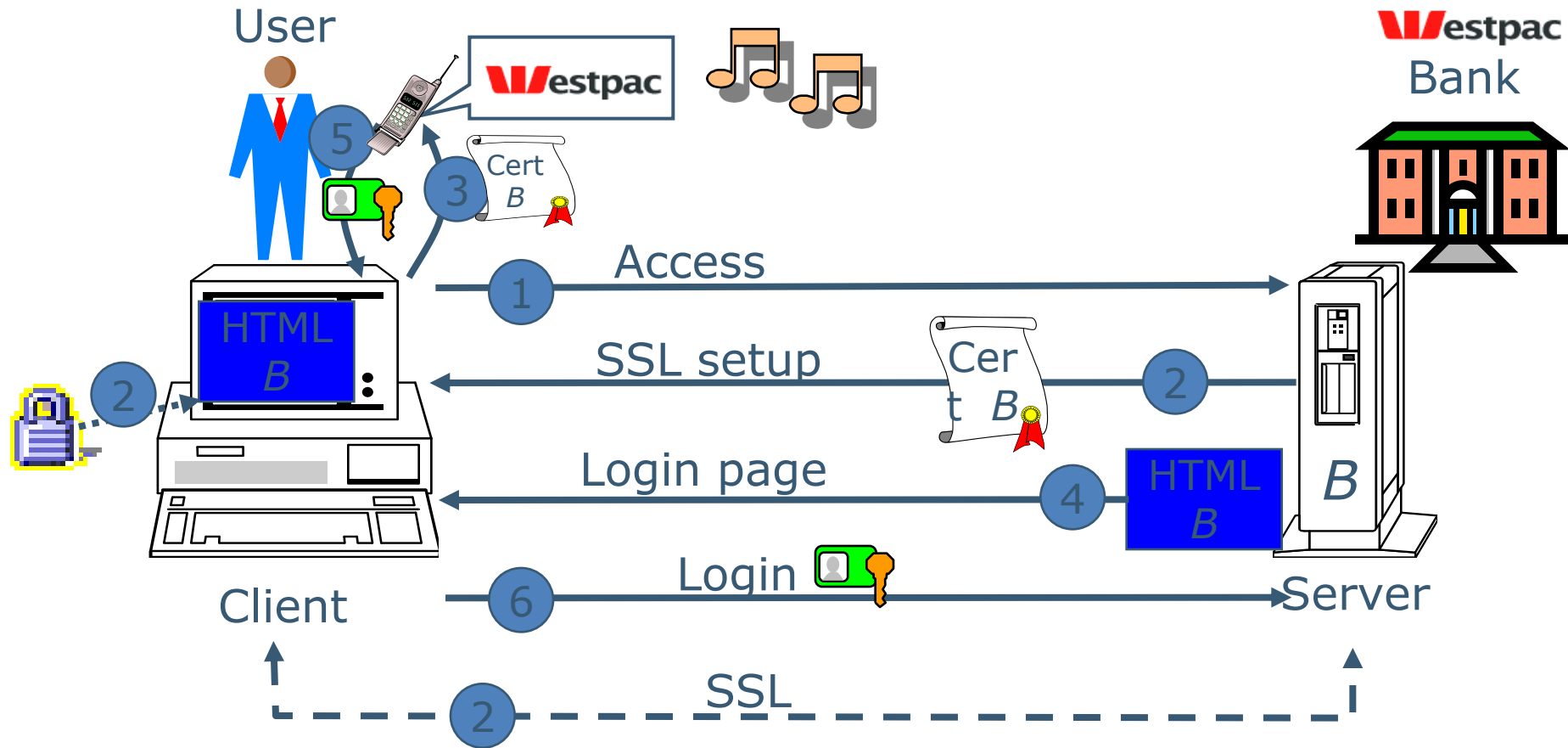
## User Centric model



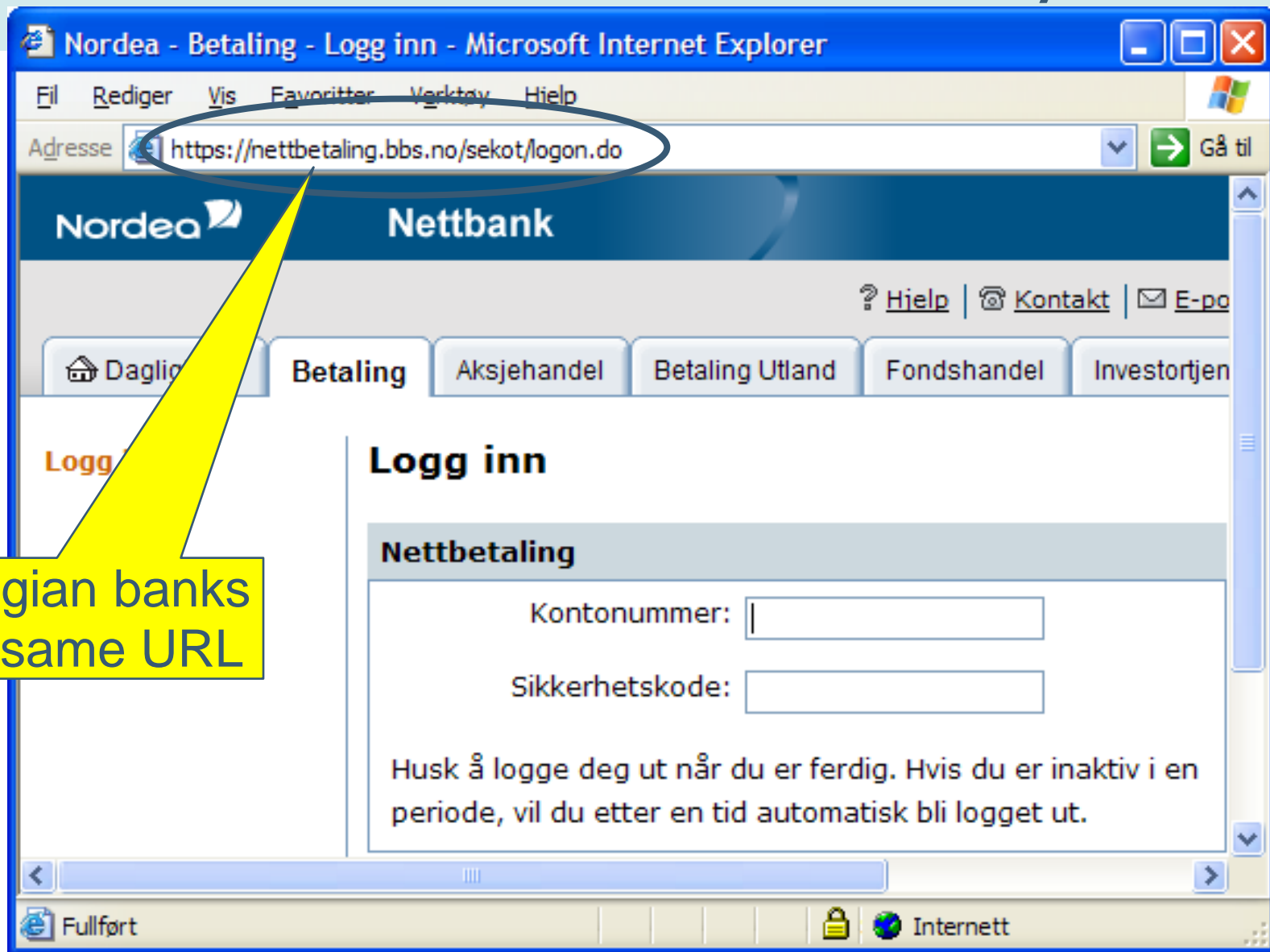
### Legend :

-  SP Identity domain
-  Domain name issued by IdP #
-  PAD
-  SP entity
-  Domain name registrar / IdP
-  CA
-  Auth. token issued by CA #
-  Service access
-  SP authentication
-  Identifier mapping

# User-centric server authentication



# Unintended vulnerability



All Norwegian banks have the same URL

# Research challenges 1

- Security usability of identity management
  - Giving sufficient info without overloading user
  - Technology support for managing identities
- Trusted personal authentication device
  - Configuration
  - Integrity (HW, SW, e.g. TPM based)
  - User authentication (PIN, biometric etc.)
  - Backup procedures
  - Interfaces (wireless, USB)
  - Protocols and interworking

# Research challenges 2

- Authentication assurance levels
  - Classification
  - Relationship with application sensitivity and risk
  - Relationship with access authorization
- Service provider and device authentication
  - Identity domains and identity mapping
  - Binding to trusted hardware
  - PKI models



# Research challenges 3

- Identity theft
  - Prevention technologies
  - Discovery methods
  - Recovery methods
- Privacy
  - Trust in virtual identities
  - Escrow technologies
  - Trusted throw-away identities

# Research challenges 4

- Interoperability between identity systems
  - TTP roles
  - Policies
  - Metafederation
- Social issues
  - Fundamental identification, DAN, biometrics
  - Use of social security numbers
  - Privacy v. national security

?

