INF3510 Information Security
University of Oslo
Spring 2010

Lecture 7

Identity and Access Management

Audun Jøsang

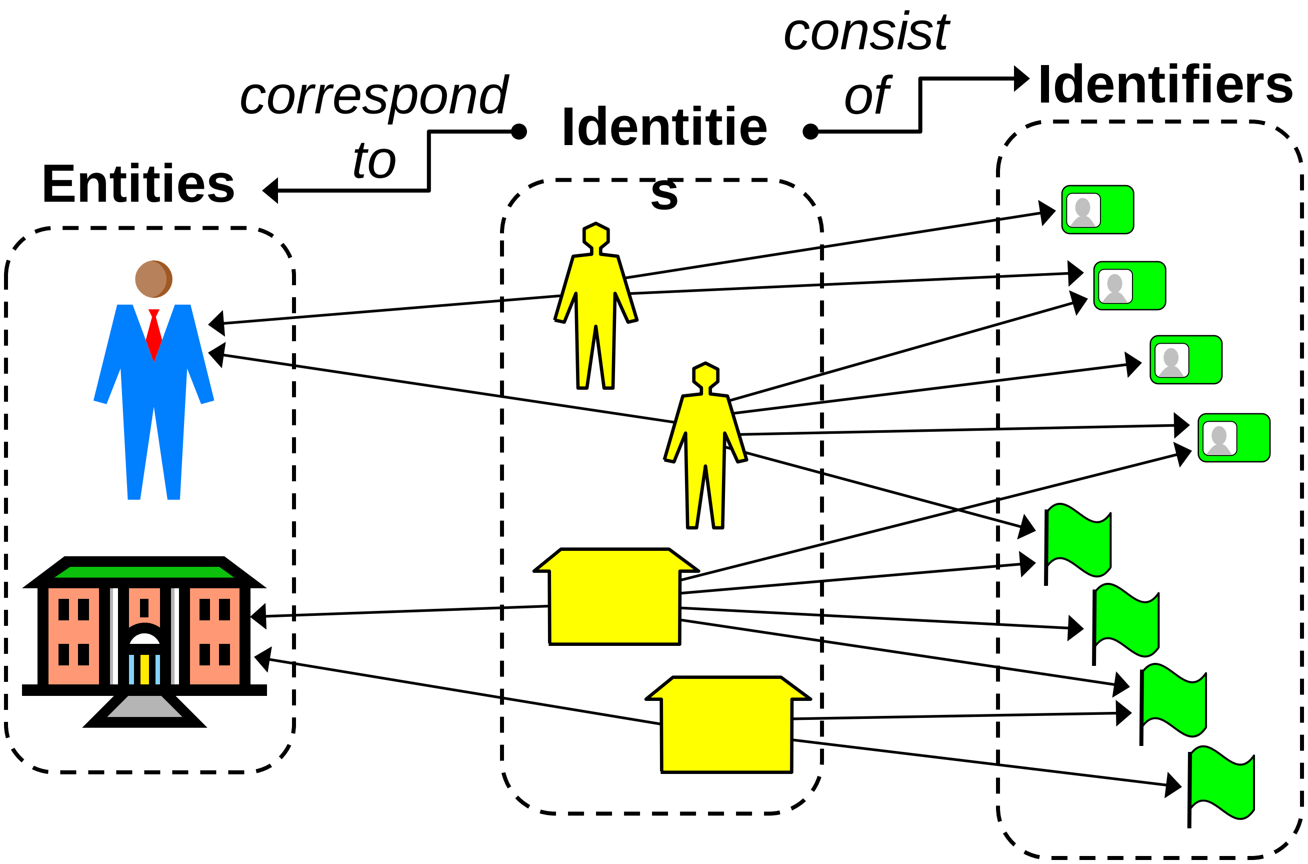
Outline

- Identity and access management concepts
- Identity management models
  - User identity management
  - Service provider identity management
- Federation implementations
- Authentication assurance

Identity related concepts

- Entity
  - A person, organisation, agent, system, etc.
- Identity
  - A set of characteristics of an entity in a specific domain
  - An entity may have multiple identities in the same domain
- Digital identity
  - Identity resulting from digital codification of characteristics in a way that is suitable for processing by computer systems
- Identifier
  - A characteristic or attribute that can be related to a specific entity
    - Can be unique or non-unique within a domain
  - Transient or permanent, self defined or by authority, suitable for interpretation by humans and/or computers, etc
  - Separation between identity and identifier is blurred in common language

Relationship between Entities, Identities and Identifiers



Identity & access management

Identity

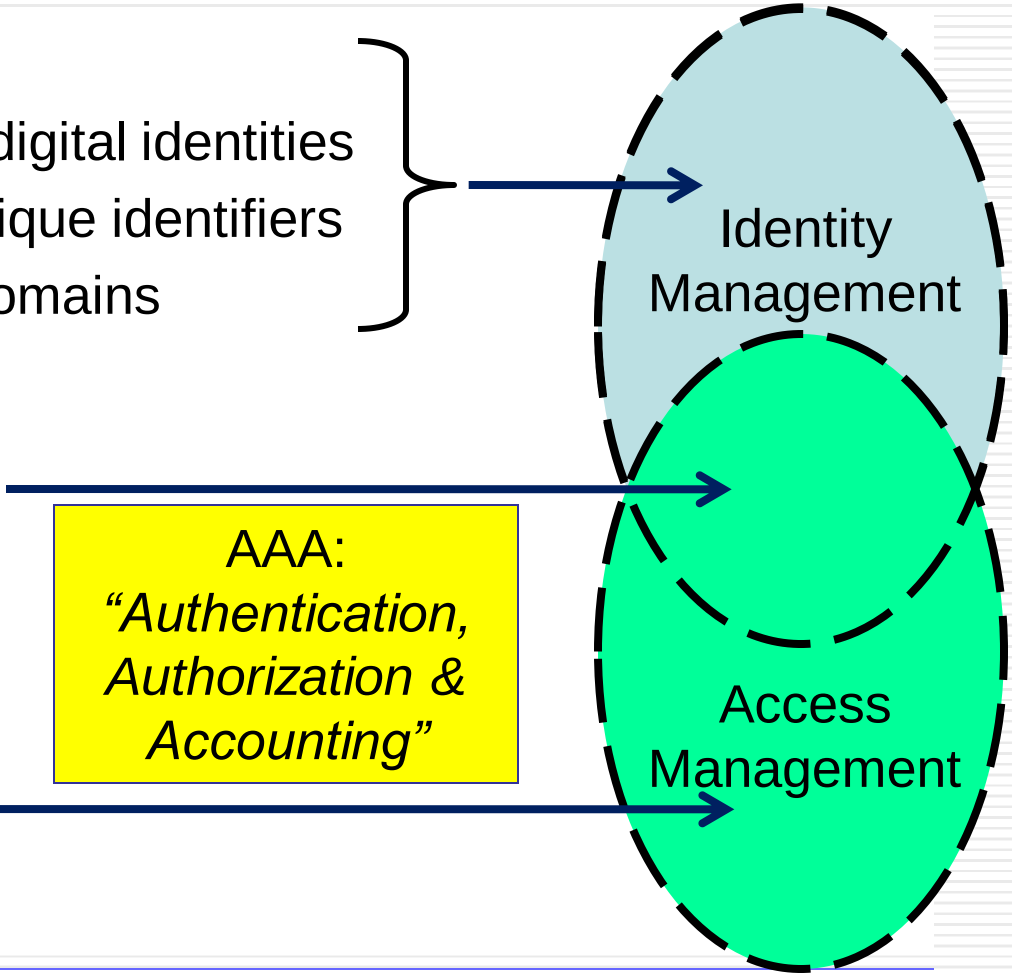
- Representing and entities as digital identities
- Managing name spaces of unique identifiers
- Mapping identities between domains

Authentication

- Registration
- Credentials management
- Entity authentication

Access

- Authorization
- Access control
- Accounting



AAA:
"Authentication, Authorization & Accounting"

Access Control Phases

Authorization

Policy definition by authority

Access rules specification

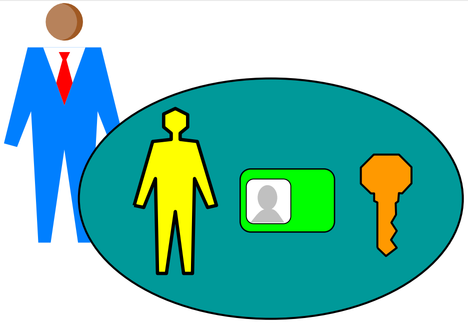
	Dev.	Prod.
John	✓	
Mary		✓

Policy encoding by custodian

Grant/reject access requests

Policy enforcement by system

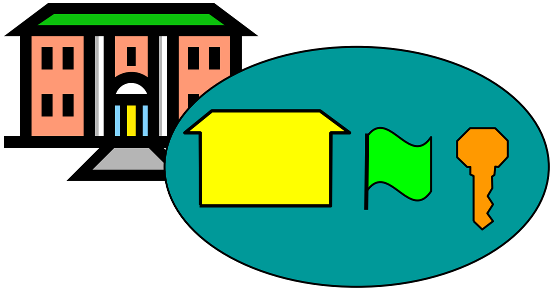
Who's identity?



User's Ids and credentials

- Issued by: SPs & IdP
- Managed by users & SPs

- Application layer authentication
- Traditional identity management



SP's Ids and credentials

- Issued by DNS registrars & CAs
- Managed by users & SPs

- Transport layer authentication
- Not traditionally part of identity management

Four types of identity management

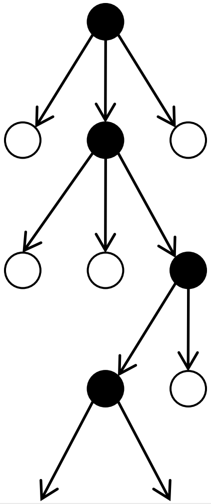
(1) Mgmt of user IDs and credentials on SP side	(2) Mgmt of user IDs and credentials on user side
(3) Mgmt of SP IDs and credentials on SP side	(4) Mgmt of SP IDs and credentials on user side

- Only type 1 is traditionally considered part of IAM
- Types 2,3,4 are equally important for security

X.500 Directory and Protocol

- Hierarchical name space
- Inspired by the postal network
- Protocol for accessing and managing the directory

Directory Information Tree



RDN of entry	Distinguished name of entry
{null}	{null}
{Country=GB}	{Country=GB}
{Organisation=BT}	{{Country=GB} Organisation=BT}
{Organisational Unit=Sales, Location=London}	{{{Country=GB} Organisation=BT} Organisational Unit=Sales, Location=London}

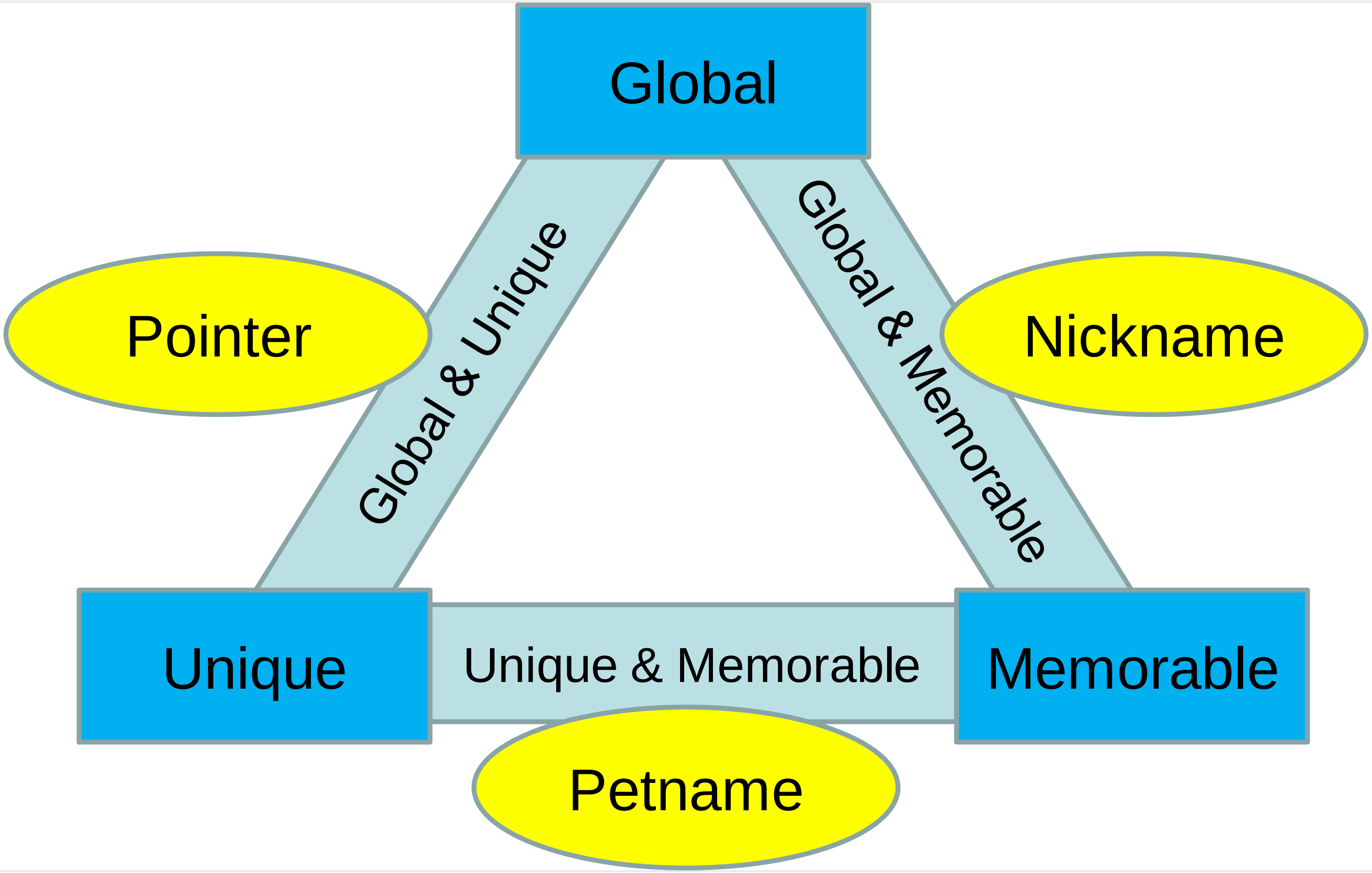
LDAP Directory and Protocol (**L**ightweight **D**irectory **A**ccess **P**rotocol)

- Light version of X.500
- LDAP protocol is used to query the an LDAP directory to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet.
- LDAP allows you to look up identity attributes of entity, e.g. for authentication and AC purposes.
- Commercial products: e.g. MS Active Directory

Identifier characteristics

- Local or global
- Unique or ambiguous
- Assigned by authority or self assigned
- Permanent or temporary
- Reassignable or not
- Persistent or not
- Human or machine readable
- Memorable or not (passing bus test)

Zooko's Triangle



Zooko’s triangle

- Desirable properties of an identifier:
  - Global
  - Unique
  - Memorable
- Identifiers can only have 2 of the properties.
  - Global & Unique: **Pointer**
    - e.g. URL: *www.pepespizza.co.nz*
  - Global & Memorable: **Nickname**
    - e.g. *Pépés Pizza*
  - Unique & Memorable: **Petname**
    - e.g.: *My Wellington Pizza*

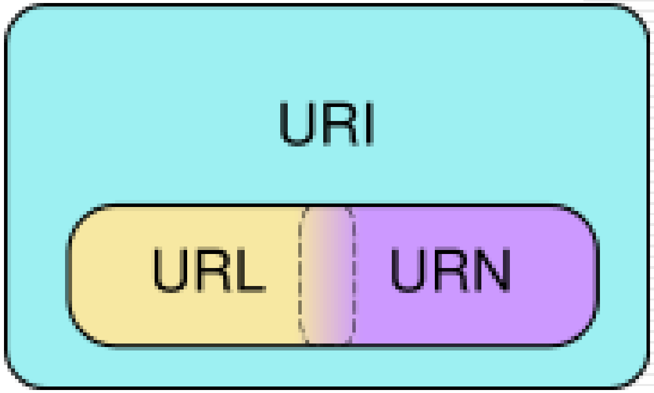
Name spaces of unique identifiers

- Local name spaces
  - Staff number
    - Within company
  - Social security number
    - Within state/country
  - Bank account number
    - Within state/country
  - Bank box number
    - Within branch office

- Global name spaces
  - Domain names
  - IP addresses
  - Telephone numbers
  - Email addresses
  - ISBN
  - X.500 Directory
  - URI and URL
  - XRI
  - DOI
  - GUID

URI: Uniform Resource Identifier

- URL: Uniform Resource Locator
  - Where is it?
  - E.g. Domain name or path
- URN: Uniform Resource Name
  - What is it?
  - E.g. ISBN or email name
- URI
  - What is it and where is it?
  - $\underbrace{\text{mailto:}}_{\text{Scheme}}\underbrace{\text{josang@}}_{\text{URN}}\underbrace{\text{unik.no}}_{\text{URL}}$



XRI: eXtensible Resource Identifier Two forms:

i-name:

- Human friendly
- Reassignable
- Example: Domain name

i-number

- Machine readable
- Human *un*-friendly
- Persistent

- Mapping between i-name and i-number
- Similar to DNS mapping between domain name and IP Address

i-number examples

1st level
Global
i-Numbers

=!1000.a1b2.93d2.8c73 (Personal)
@!1000.9554.fabd.129c (Organizational)
!!1000 (Network - reserved for XDI.org-accredited i-brokers)

2nd level
Community
i-numbers

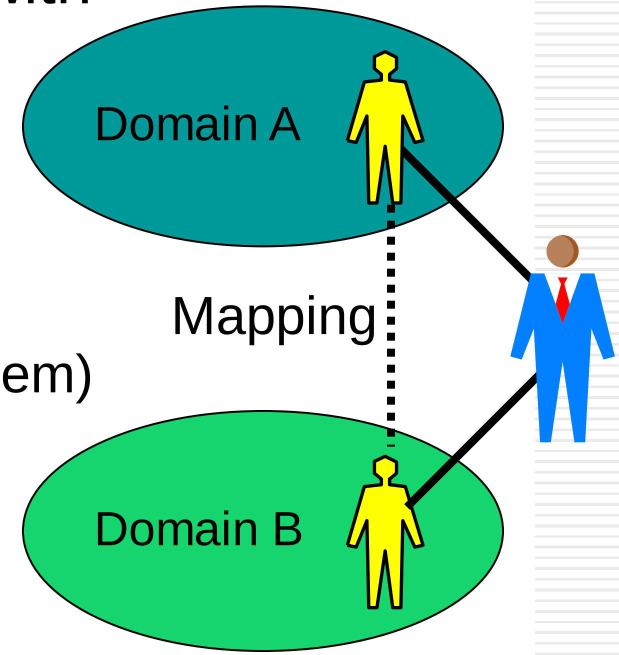
=!1000.a1b2.93d2.8c73!3ae2 (Personal)
@!1000.9554.fabd.129c!2847.df3c (Organizational)
!!1000!de21.4536.2cb2.8074 (Network)

3rd level
Community
i-numbers

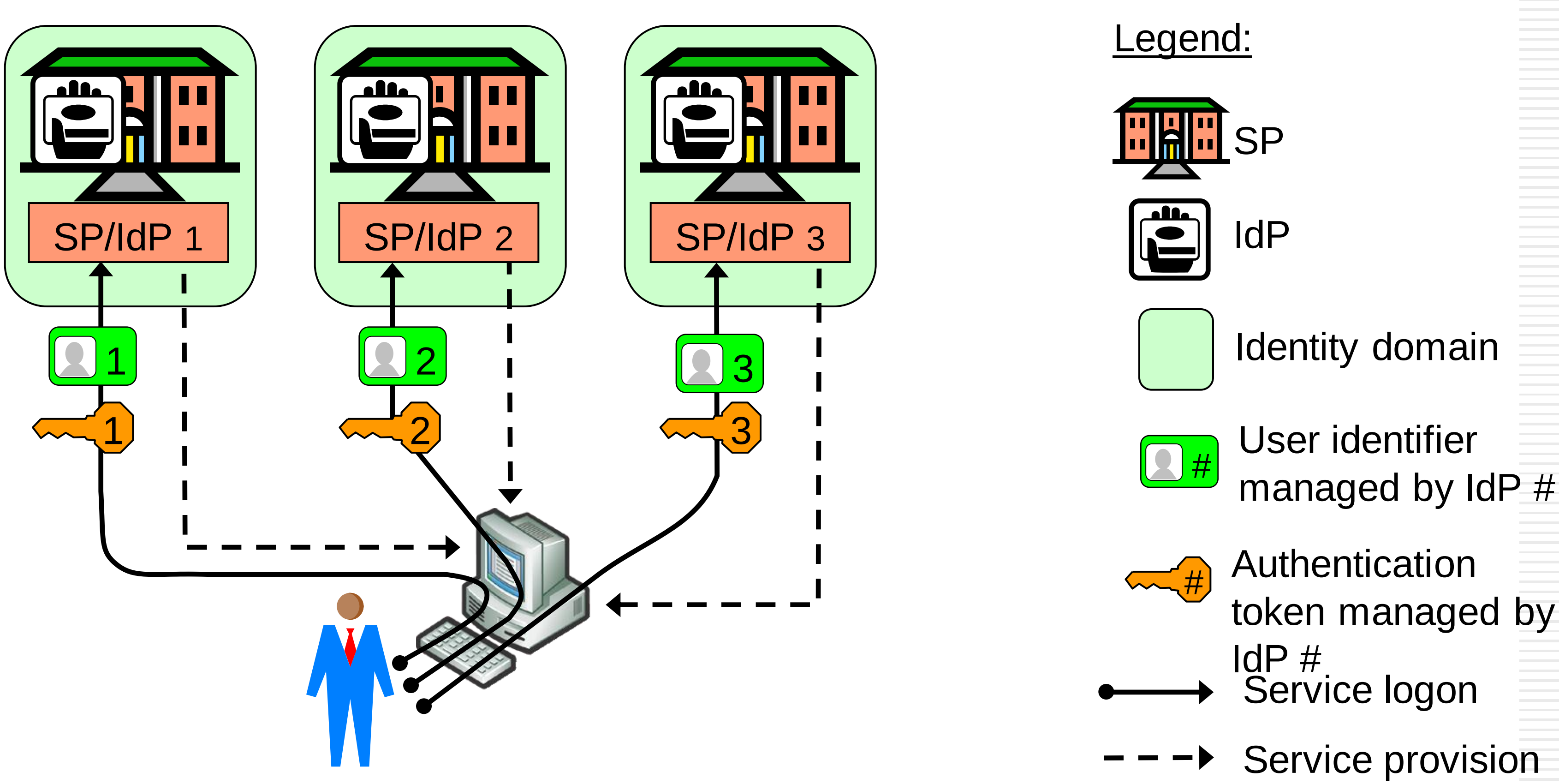
=!1000.a1b2.93d2.8c73!3ae2!1490 (Personal)
@!1000.9554.fabd.129c!2847.df3c!cfae (Organizational)
!!1000!de21.4536.2cb2.8074!9fcd (Network)

Identity Domains

- An identity domain is a network realm with a name space of unique identifiers
- Management structures:
  - Single authority, e.g. User Ids in company network
  - Hierarchical: e.g. DNS (Domain Name System)
- A single policy is normally applied in a domain
- Integration/federation of domains
  - Requires mapping of identities of same entity
  - Requires alignment of policies



Silo domain model

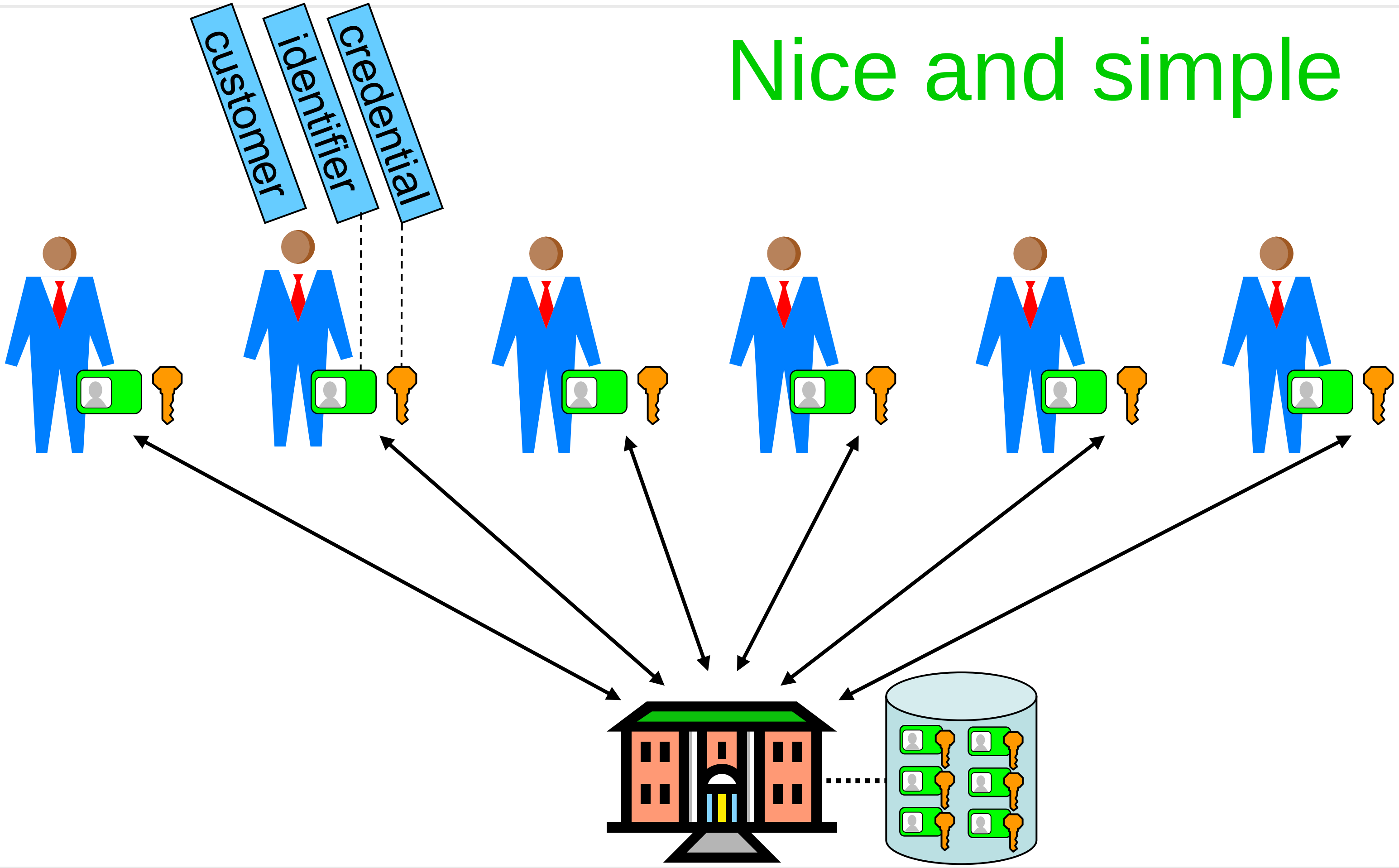


Silo user-identity domains

- SP = IdP: defines name space and provides access credentials
- Unique identifier assigned to each entity
- Advantages
  - Simple to deploy, low cost for SPs
- Disadvantages
  - Identity overload for users, poor usability

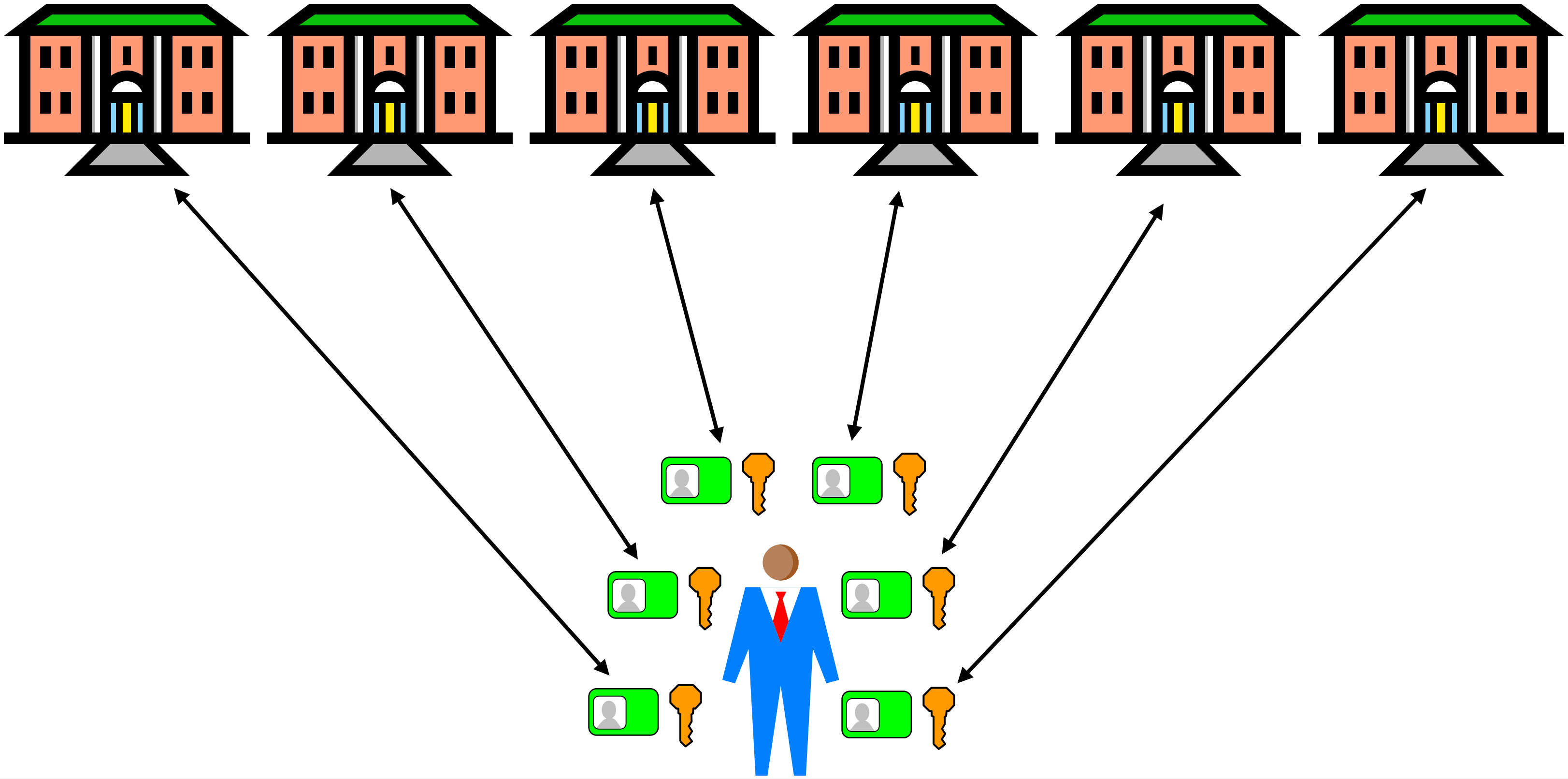
Imagine you're a service provider

Nice and simple

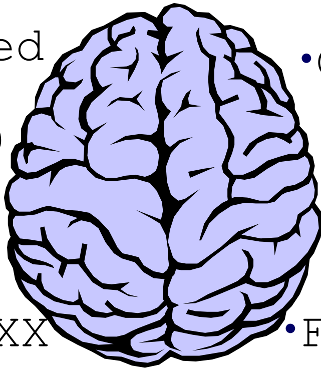


Imagine you’re a customer

It’s a nightmare



Tragedies of the Commons



- GuessMeNot
- fred
- OTP123
- 2008Oct9
- MySecret
- TopSecret
- XZ&9r#/
- ???abcXX
- FacePass

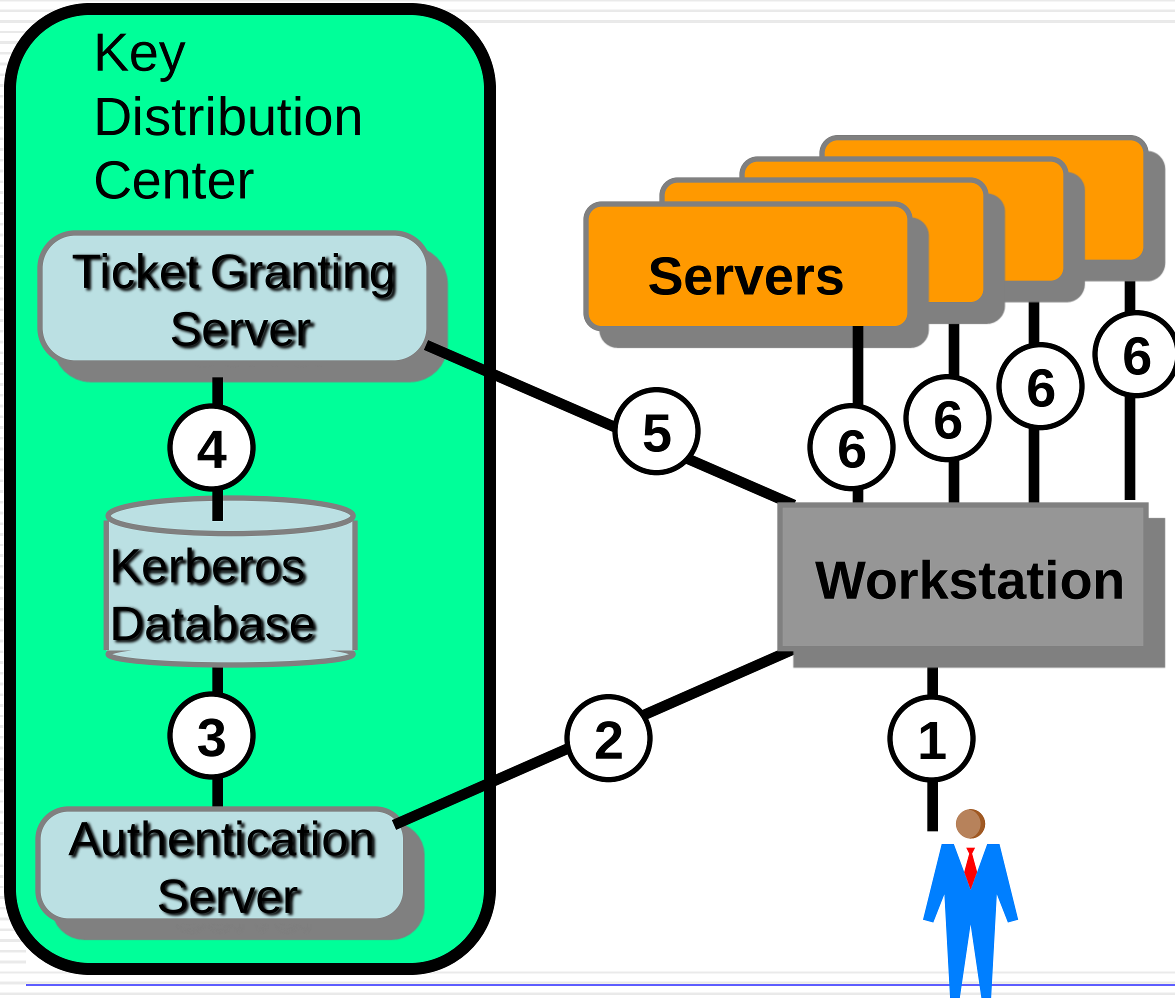
Push towards SSO (Single Sign-On)

- Users don’t want more identifiers
- Low acceptance of new services that require separate user authentication
- Silo model requires users to provide same information to many service providers
- Silo model makes it difficult to offer bundled services, i.e. from different service providers
- Service providers want better quality user information

Kerberos SSO

- Part of project Athena (MIT) in 1983.
- User must identify itself once at the beginning of a workstation session (login session).
- Does not require user to enter password every time a service is requested!
- Every user shares a password with the AS (Authentication Server)
- Every SP (service provider) shares a secret key with the TGS (Ticket Granting Server)
- Tickets are sealed (encrypted) by TGS proves to SPs that the user has been authenticated

Kerberos – simplified protocol

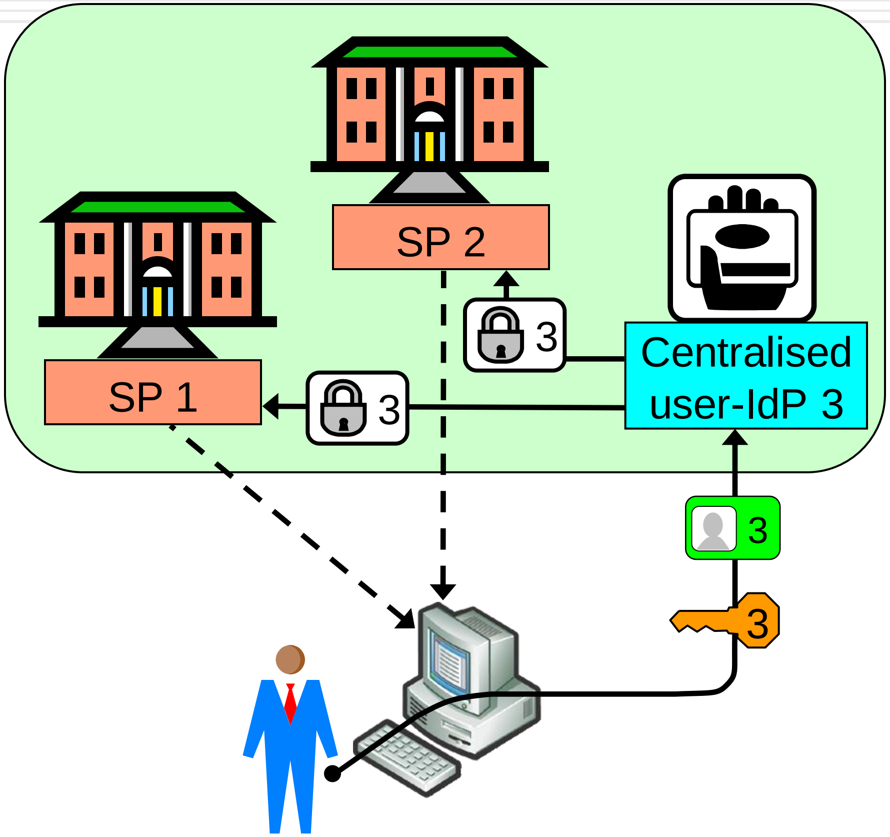


1. Request service
2. Authentication
3. Look-up user
4. Request ticket
5. Ticket
6. Service access with ticket

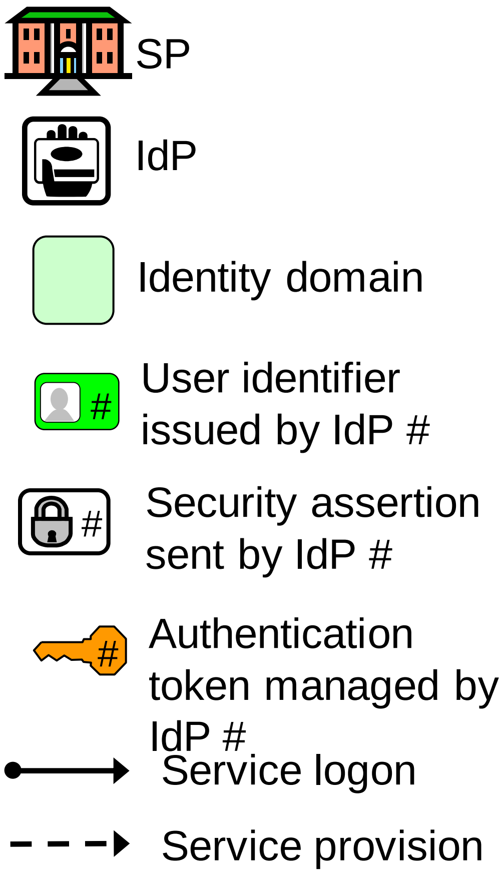
Kerberos – Advantages and limitations

- First practical SSO solution
- Centralized TTP (Trusted Third Party) model
- Uses only symmetric cryptography
- Requires Kerberos clients and servers + KDC
- Only suitable for organisations under common management (single domain)
- Does not scale to very large domains
- Not suitable for open environments (Internet)

Traditional Single Sign-On (SSO) Model



Legend:

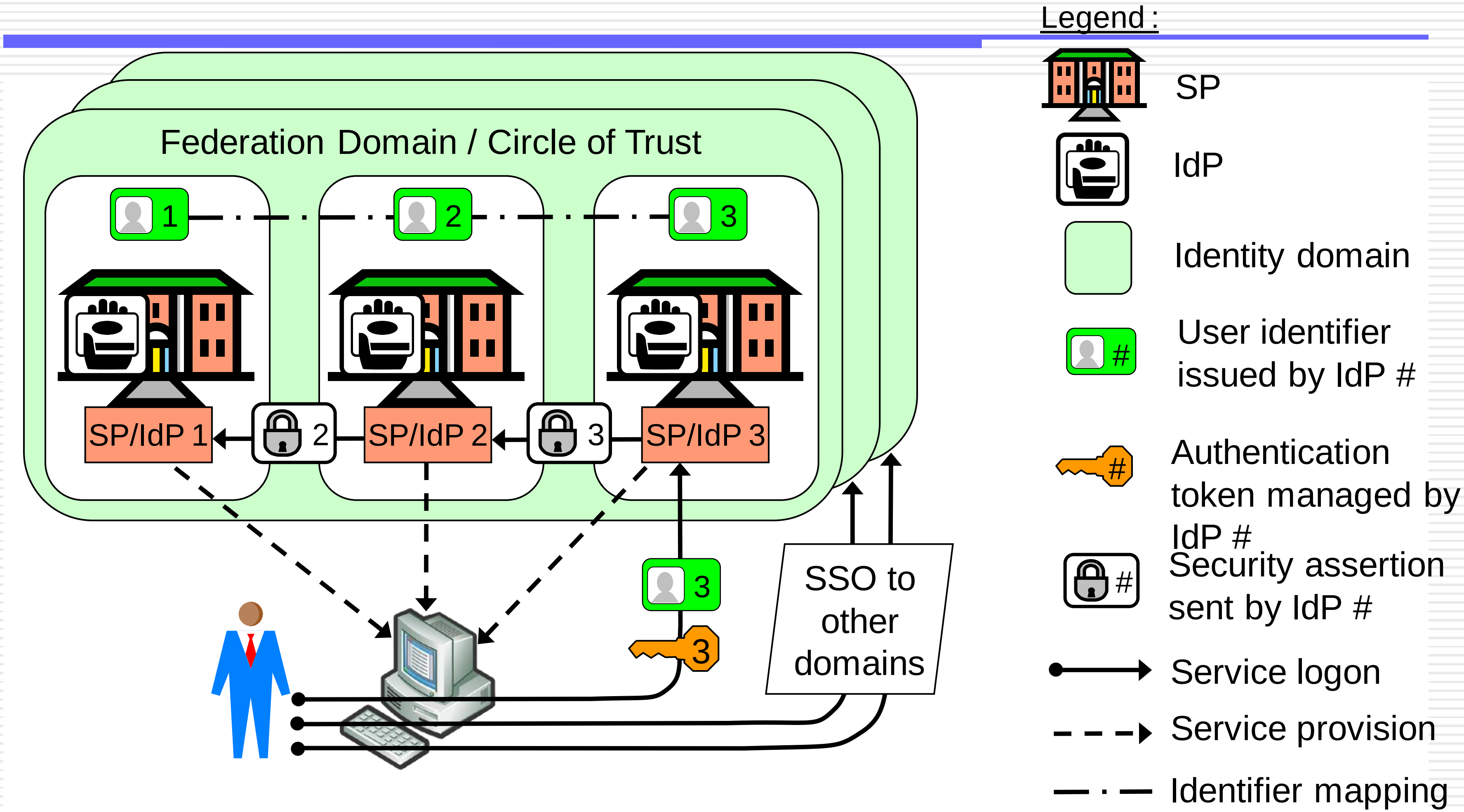

SP
IdP
Identity domain
User identifier issued by IdP #
#
Security assertion sent by IdP #
#
Authentication token managed by IdP #
#
Service logon
Service provision

Examples: Kerberos, Microsoft .net Passport

Traditional SSO

- Single authority/infrastructure that acts as identifier and credentials provider
- Single authority authenticates users on behalf of all SPs
- Advantages
  - Well suited for SPs under single management, e.g. within large private and government organisations
  - Good usability
- Disadvantages
  - Politically difficult to implement in open environments.
  - Who trusts authentication by other organisations?

Federated SSO model


Legend :
SP
IdP
Identity domain
User identifier issued by IdP #
Authentication token managed by IdP #
Security assertion sent by IdP #
Service logon
Service provision
Identifier mapping
Federation Domain / Circle of Trust
1
2
3
SP/IdP 1
SP/IdP 2
SP/IdP 3
2
3
3
3
SSO to other domains

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

Federated SSO

- Identity Federation
  - A set of agreements, standards and technologies that enable a group of SPs to recognise user identities and entitlements from other SPs
  - Identifier (and credential) issuance as for the silo model
  - **Mapping** between a user’s different unique identifiers
  - Authentication by one SP, communicated as security assertions to other SPs
  - Provides SSO in open environments

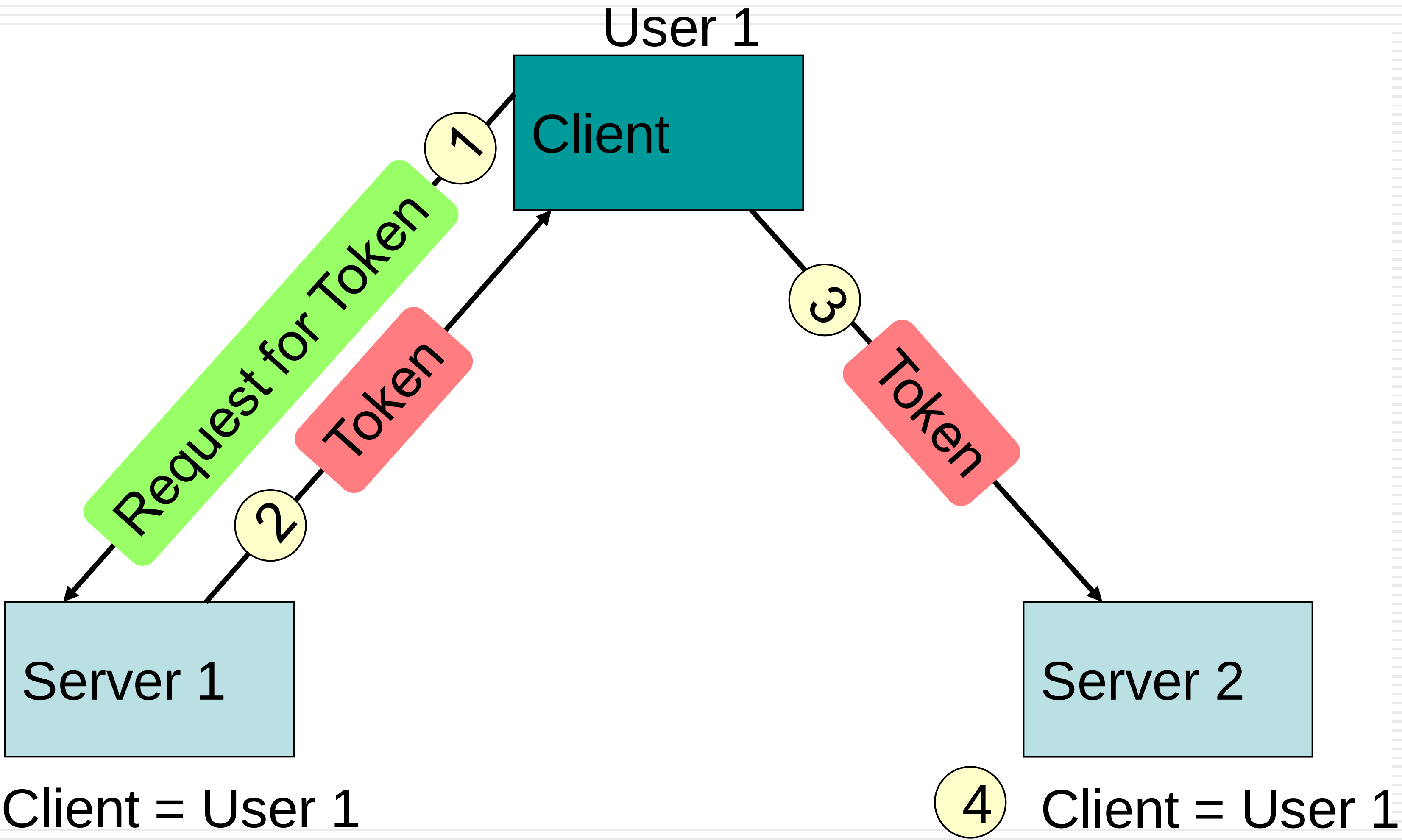
Federated SSO

- Advantages
  - Improved usability (theoretically)
  - Compatible with silo user-identity domains
  - Allows SPs to bundle services and collect user info
- Disadvantages
  - High technical and legal complexity
  - High trust requirements
    - E.g. SP1 is technically able to access SP2 on user's behalf
  - Privacy issues
  - Unimaginable for all SPs to federate,
    - multiple federated SSOs not much better than silo model

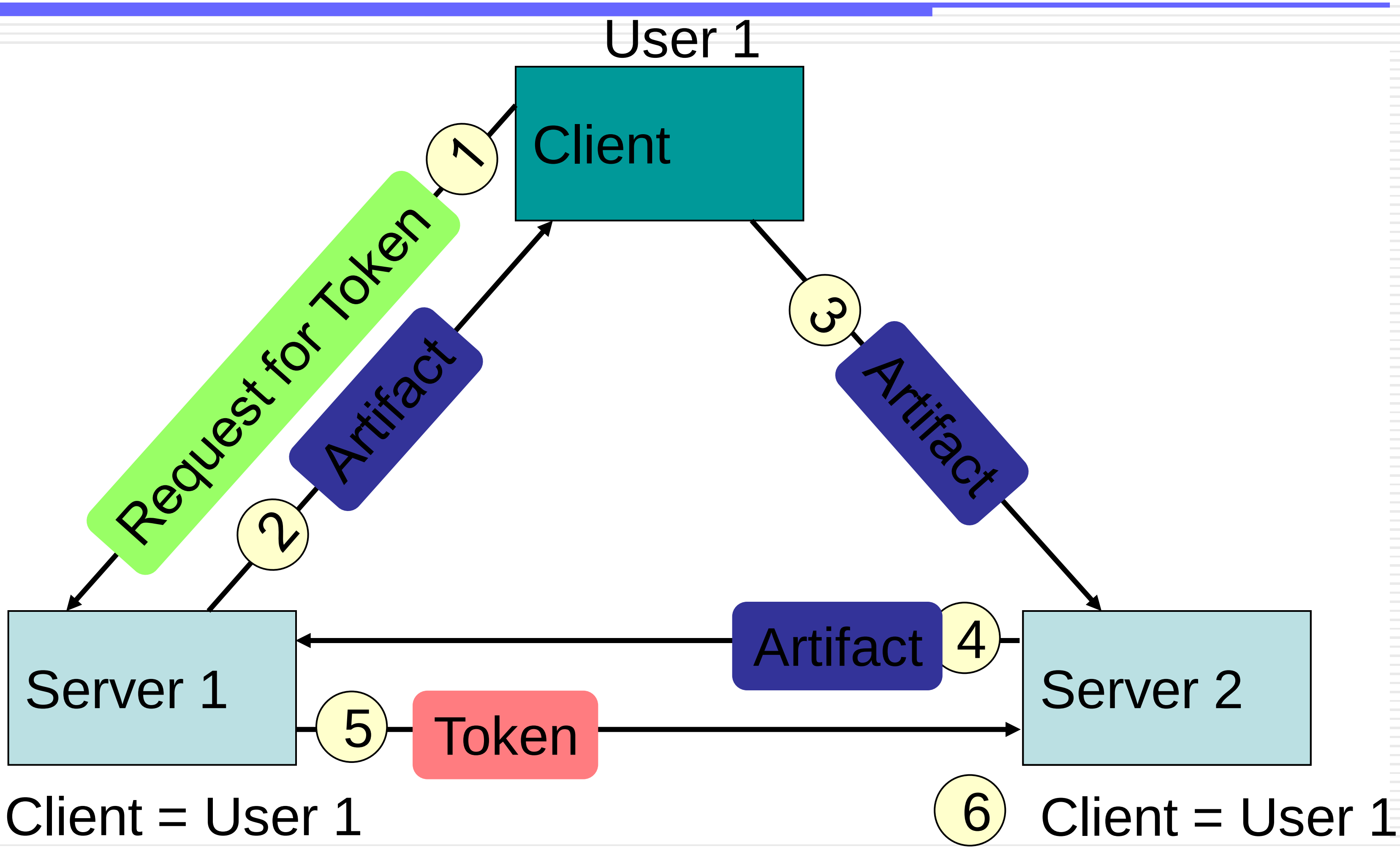
Standards for Federated SSO

- What are the “Standards”?
  - SAML (OASIS)
  - Liberty ID-FF (Liberty Alliance), merged with SAML2.0
  - WS-Federation (IBM, Microsoft) (decreasing support in industry)
- Standards based solutions make life easier
  - Multi-vendor interoperability
  - Reduced technology “lock-in”
  - Benefit from the experience of others
- Software Implementations
  - Shibboleth; Open source software that implements SAML 2.0
  - Sun, IBM, CA, Microsoft etc

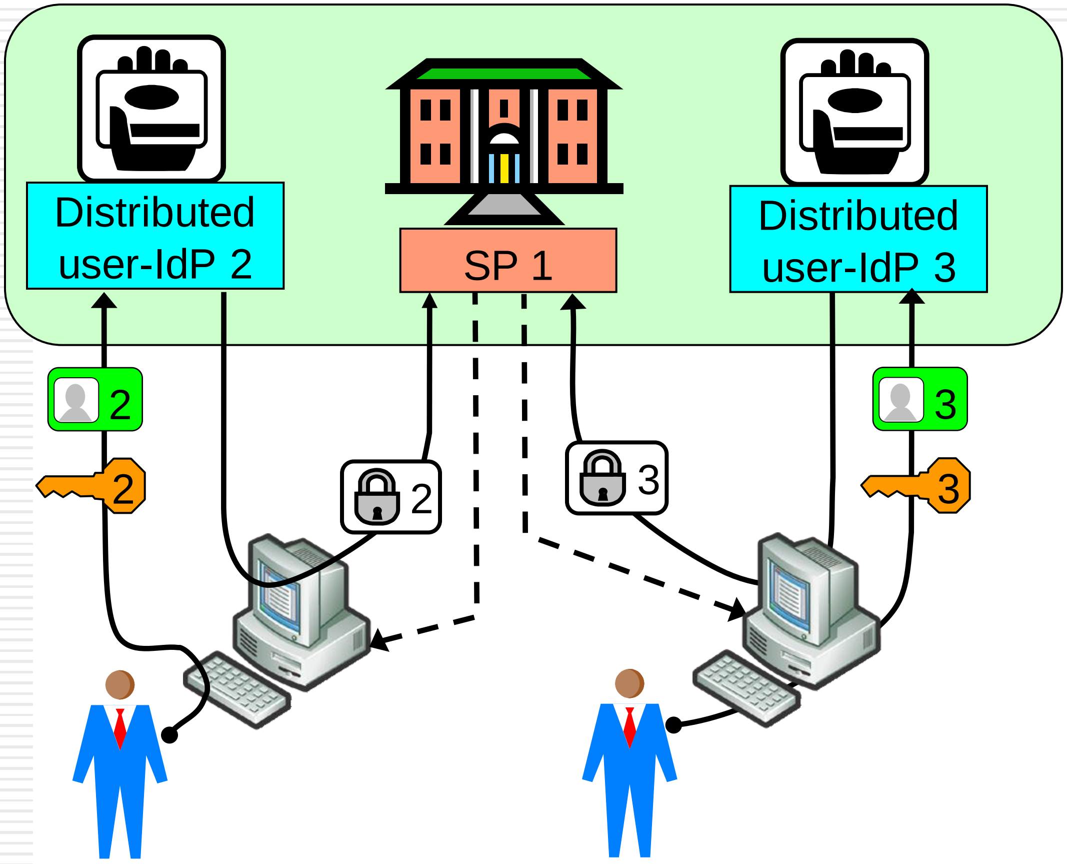
SAML identity federation protocol profile with Security Token sent as Browser Post



SAML identity federation protocol profile with Token sent through Back Channel



Common SSO identity model



Legend:

SP
IdP
Common identity domain
User identifier managed by IdP #
Authentication token managed by IdP #
Security assertion issued by IdP #
Service logon
Service provision

Example: OpenID

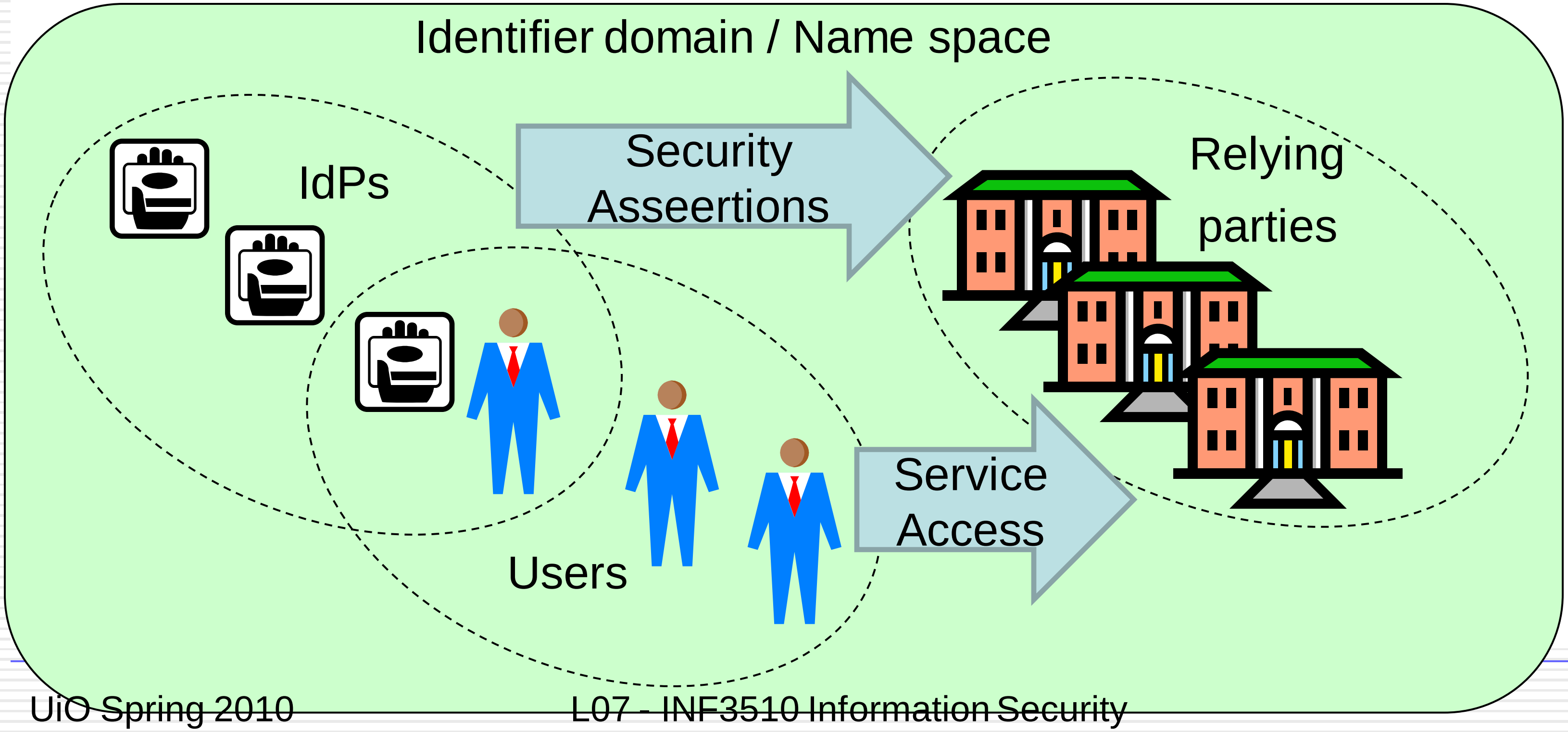
Common SSO identity model

- Single common identifier name space
  - E.g. based on URIs or XRis
- Distributed assignment of identifiers
  - Each IdP controls its own domain name
  - Registers users under domain name
- Whoever controls a domain name can be IdP

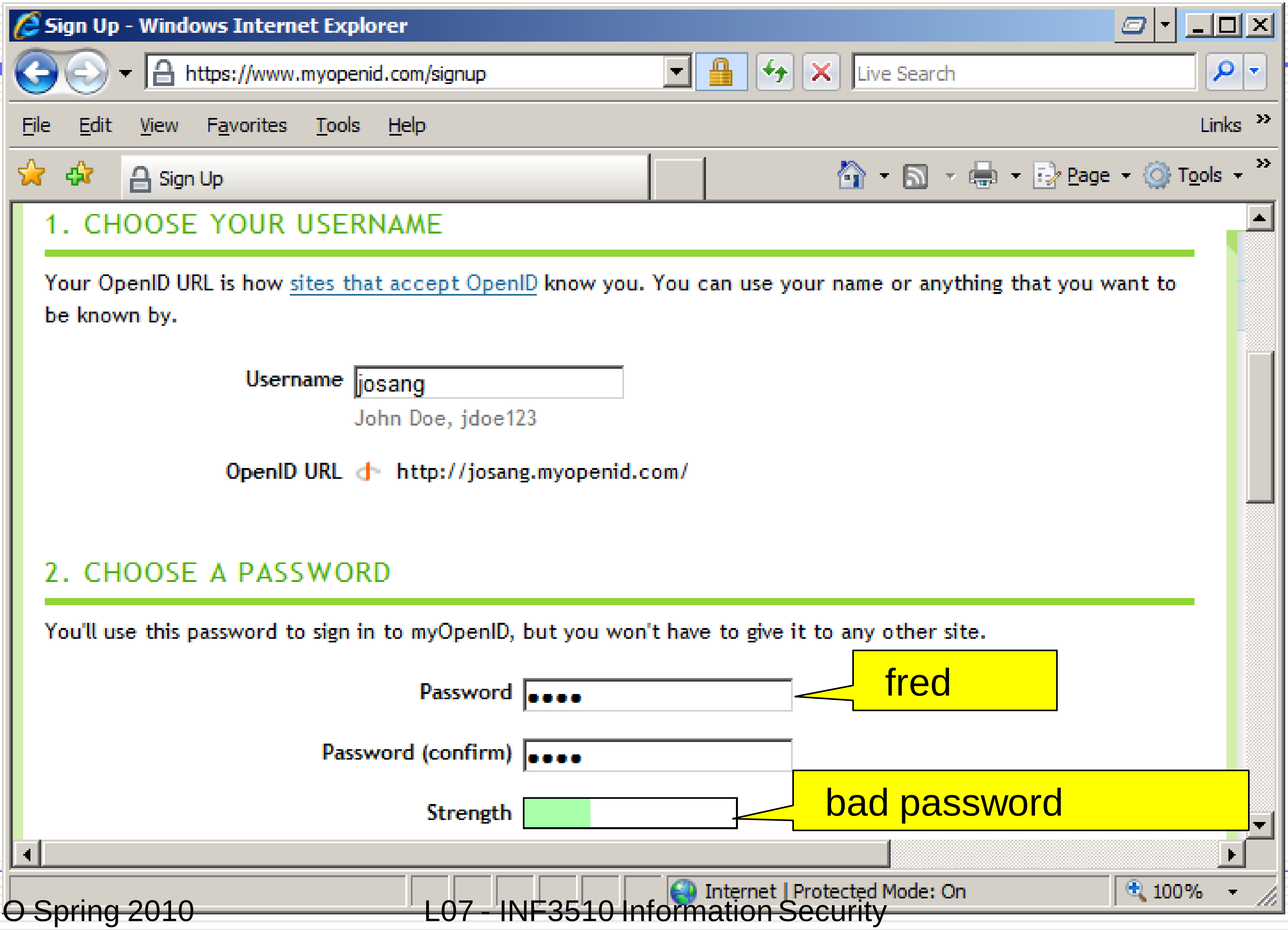
- IdPs are involved for every service access
  - Collect info about service access

The OpenID common SSO model

- Common name space
- Distributed IdPs
- No authorities



OpenID self registration



Sign Up - Windows Internet Explorer
https://www.myopenid.com/signup
Live Search
File Edit View Favorites Tools Help
Links
Sign Up
Page Tools
Internet | Protected Mode: On
100%

1. CHOOSE YOUR USERNAME

Your OpenID URL is how sites that accept OpenID know you. You can use your name or anything that you want to be known by.

Username: josang

John Doe, jdoe123

OpenID URL http://josang.myopenid.com/

2. CHOOSE A PASSWORD

You'll use this password to sign in to myOpenID, but you won't have to give it to any other site.

Password: ●●●●

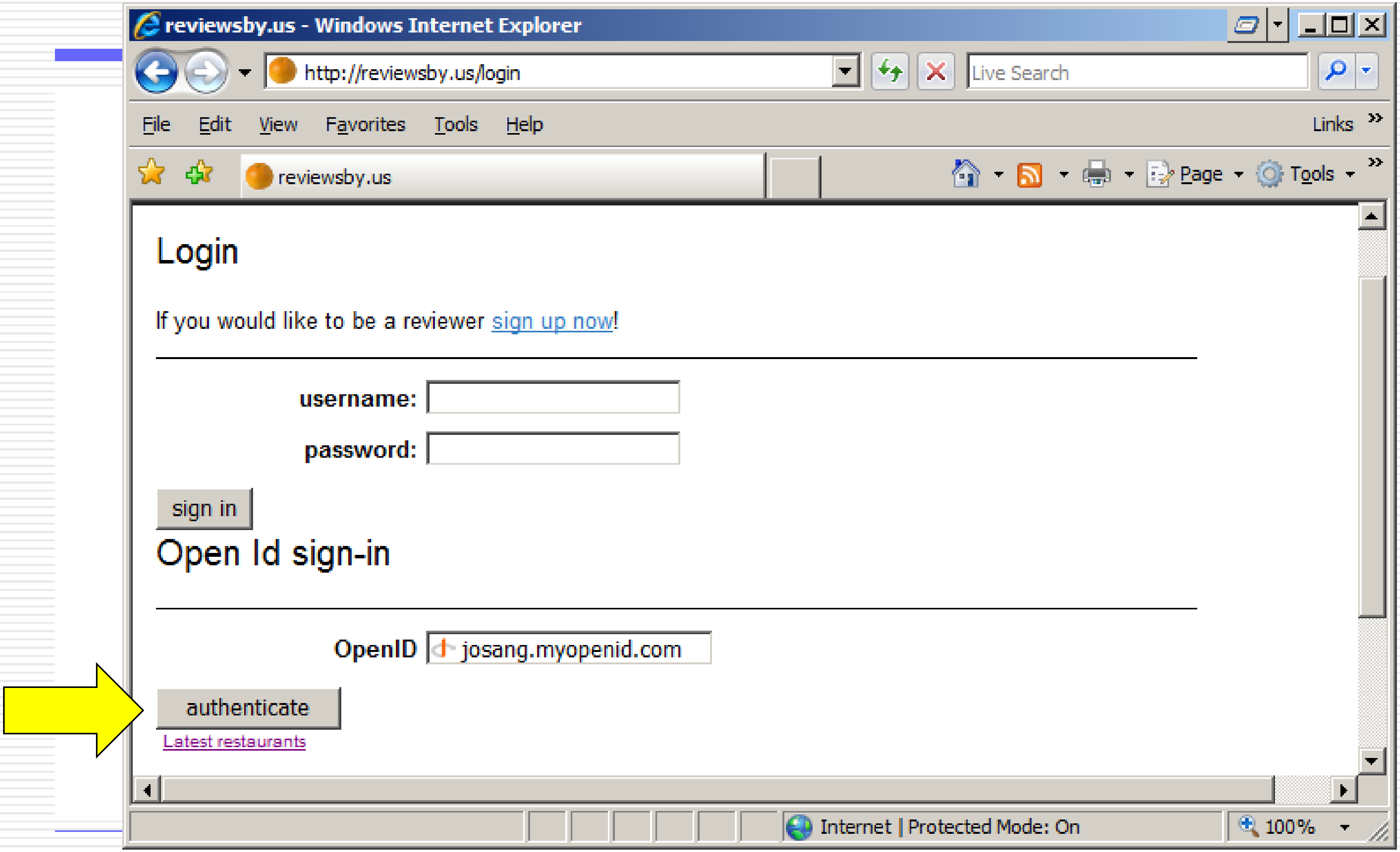
Password (confirm): ●●●●

Strength

fred

bad password

Service Access Without Password


reviewsby.us - Windows Internet Explorer
http://reviewsby.us/login
Live Search
File Edit View Favorites Tools Help
Links
reviewsby.us
Page
Tools
Internet | Protected Mode: On
100%

Login

If you would like to be a reviewer sign up now!

username:

password:

sign in

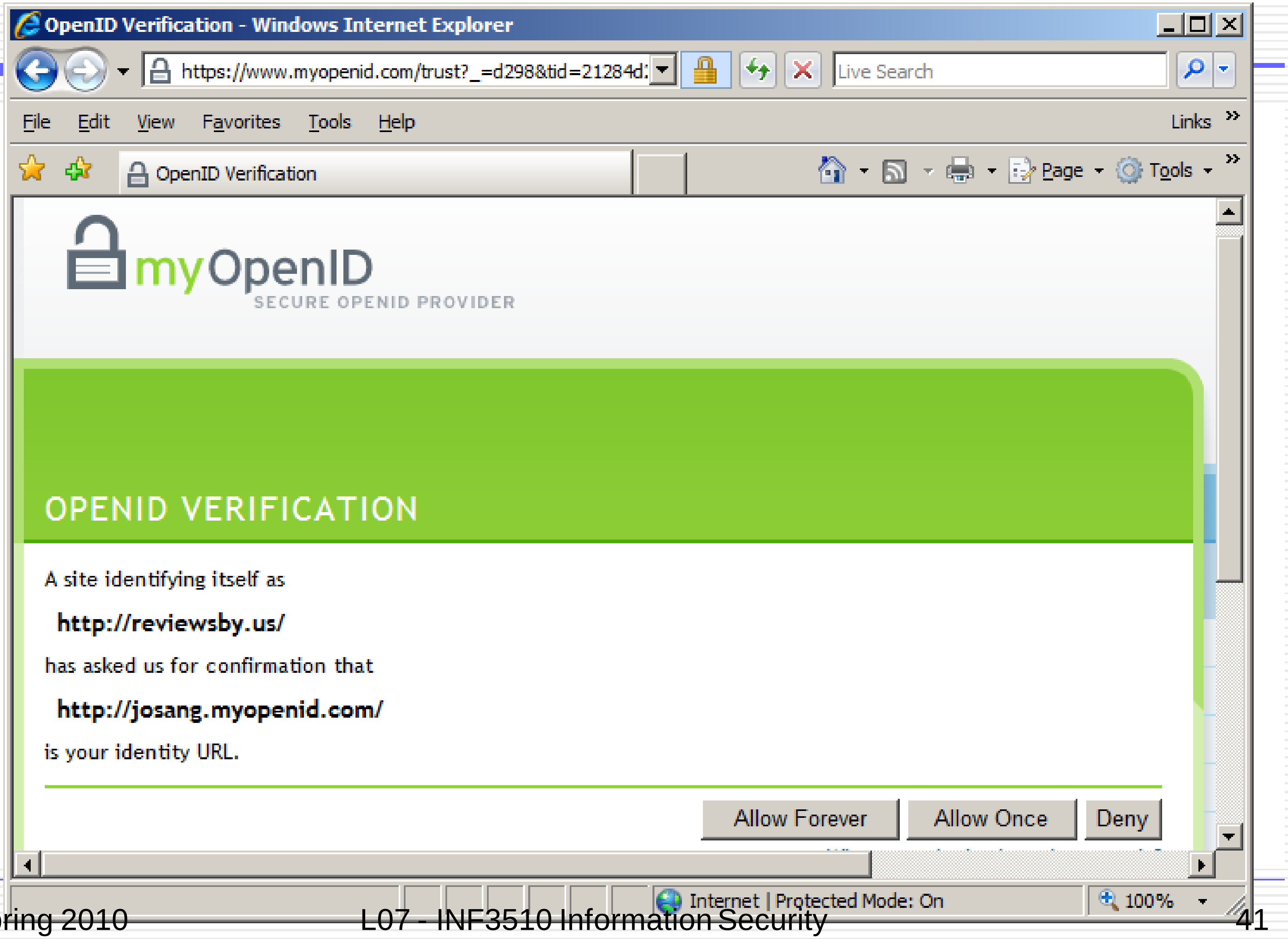
Open Id sign-in

OpenID: josang.myopenid.com

authenticate

Latest restaurants

First Time Sevice Access



OpenID Verification - Windows Internet Explorer
https://www.myopenid.com/trust?_=d298&tid=21284d:
Live Search
File
Edit
View
Favorites
Tools
Help
Links
OpenID Verification
Page
Tools
myOpenID
SECURE OPENID PROVIDER
Internet | Protected Mode: On
100%

OPENID VERIFICATION

A site identifying itself as

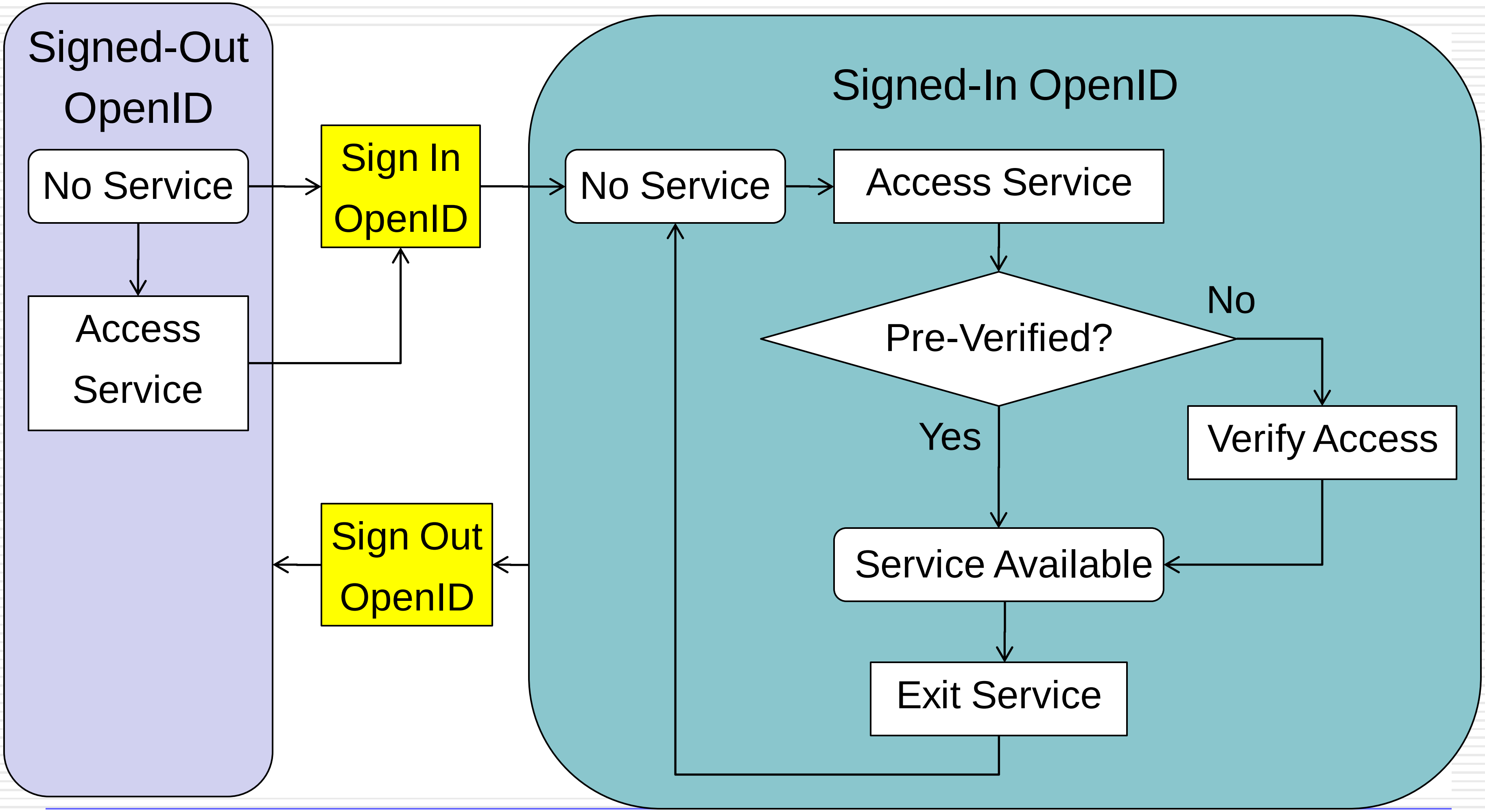
http://reviewsby.us/

has asked us for confirmation that

http://josang.myopenid.com/

is your identity URL.

OpenID flow chart (user perspective)



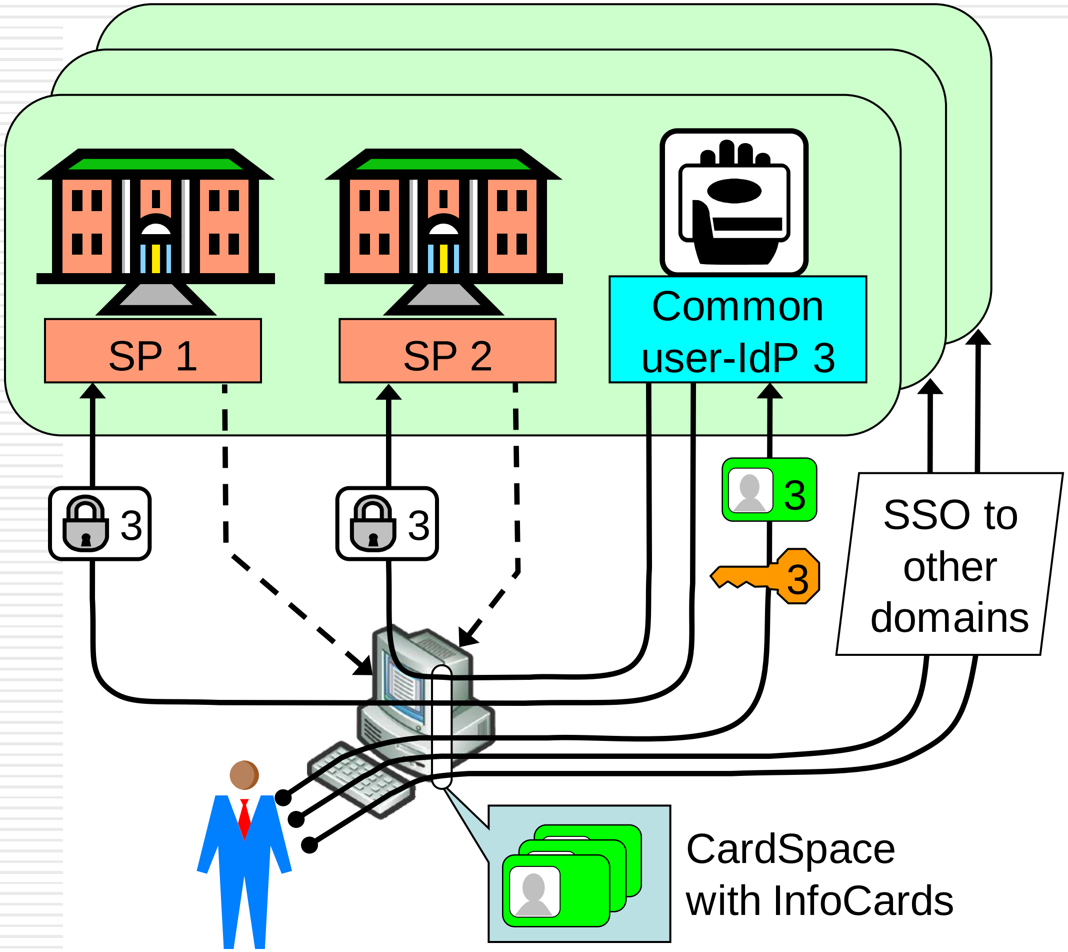
OpenID Characteristics

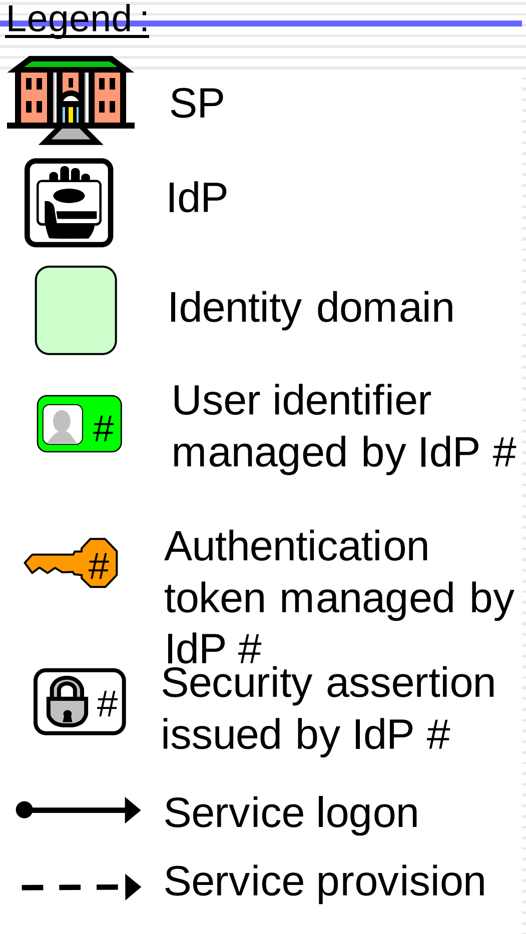
- Self registration
- ID Providers are not ”authorities”
- You can be your own ID Provider and Server
- Only supports AAL-1
- Not suitable for sensitive services
- Targets online services with AAL-1
- Open to multiple forms of abuse

OpenID Business Model

- For ID Providers
  - Collection of market data
  - Knows who uses which service
  - Fragmentation of ID Provider market is a threat
- For Service Providers (Relying Party)
  - Potentially more traffic and business
- For users
  - Avoid multiple identities
  - Avoids typing passwords
  - (Must still type OpenID identifier)

Microsoft’s InfoCard model



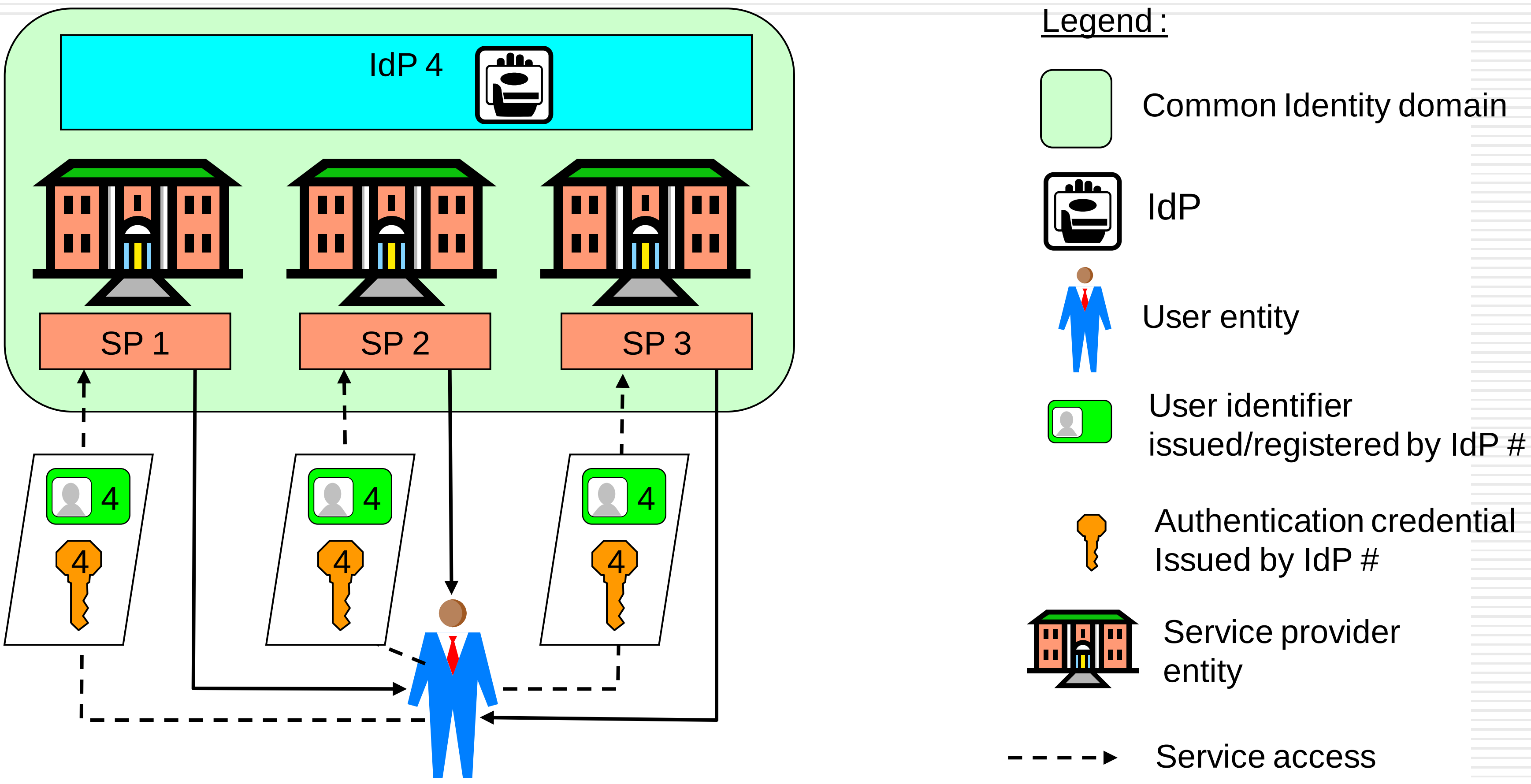


Legend :
SP
IdP
Identity domain
User identifier managed by IdP #
Authentication token managed by IdP #
Security assertion issued by IdP #
Service logon
Service provision
#
#
#

InfoCard Model

- Requires intelligent browser
- Identities called ”InfoCard” stored in the browser’s ”CardSpace”
- Browser automatically relays security assertions
- SignOn to IdP subject to phising
- Supports multiple IdPs
- ”MS.Net Passport” renamed ”MS Live Space”
- CardSpace is compatible with dstributed common identity models, e.g. OpenID

Global user identity domain



Legend :

Common Identity domain

IdP

User entity

User identifier issued/registered by IdP #

Authentication credential Issued by IdP #

Service provider entity

Service access

Service provision

Example: PKI with user certificates

Global user identity domain

- IdPs define/register identifiers and issue/record credentials
- All SPs recognise and authenticate the same user by the same identifier
- Advantages
  - Simple to manage for users and for SPs
- Disadvantages
  - Politically difficult to define name space
  - SPs will not trust identifiers/credentials issued by third party
- <u>Utopic solution</u>

Server or Client side Automation in SSO

- Single **manual** authentication
- Repeated **automated** authentications
- SSO is simply an automation mechanism
- Where to put the automation?
  - – Both on server and client side: **Traditional SSO**
    - Kerberos, InfoCard
  - – On server side only: **Federated SSO**
  - – On client side only: **User Centric SSO**

User-centric identity manageent

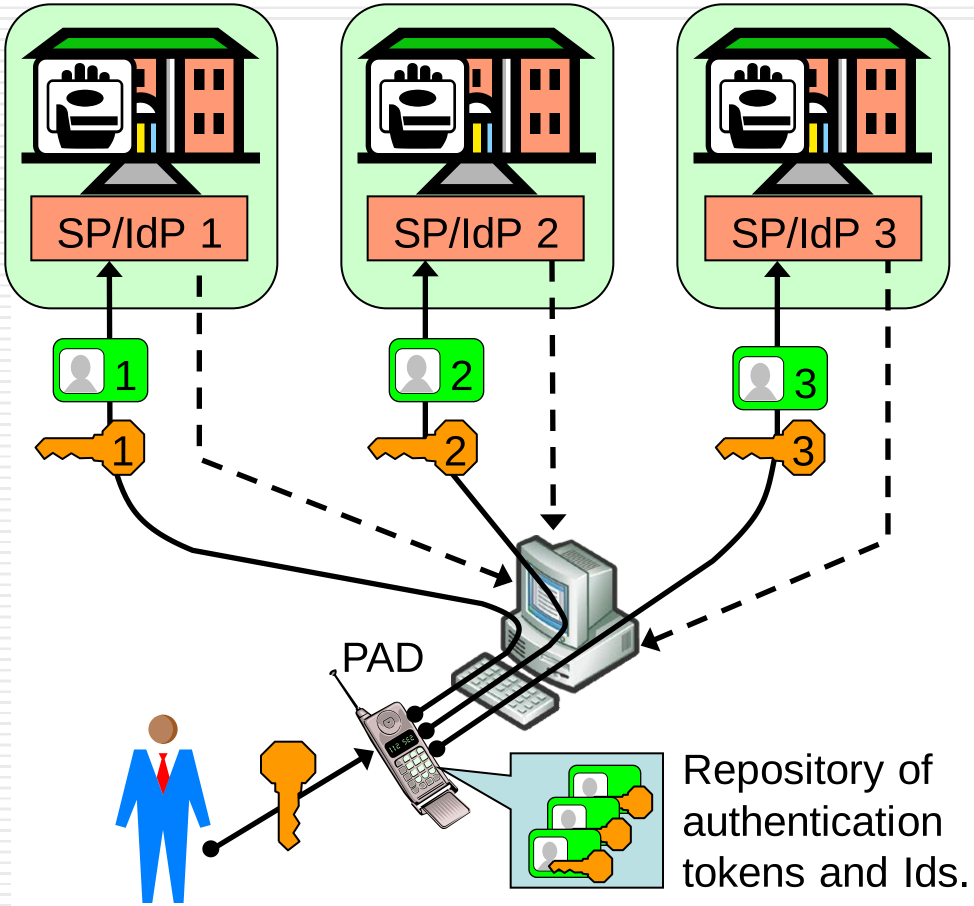
- Buzzword with positive connotation
- Seems to promise a solution to users' problems
  - Scaleability for the user
- Possible interpretations:
  - Any architecture that improves the user experience
  - Putting the users in control of their identities
  - Solutions that preserve privacy
  - SSO technology implemented on the user side

User centric SSO – Client side automation

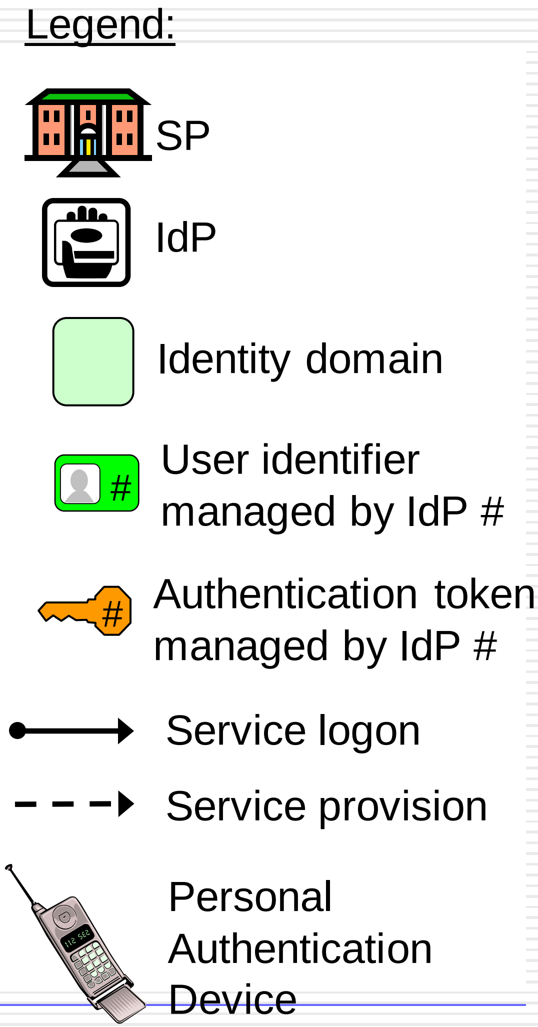
- User side technology for efficient management of identifiers and credentials
- Implementation
  - Software based
  - Hardware based: Personal Authentication Device (PAD)
- General purpose
- Assumed to be secure

Solves user side scalability problem

User Centric model

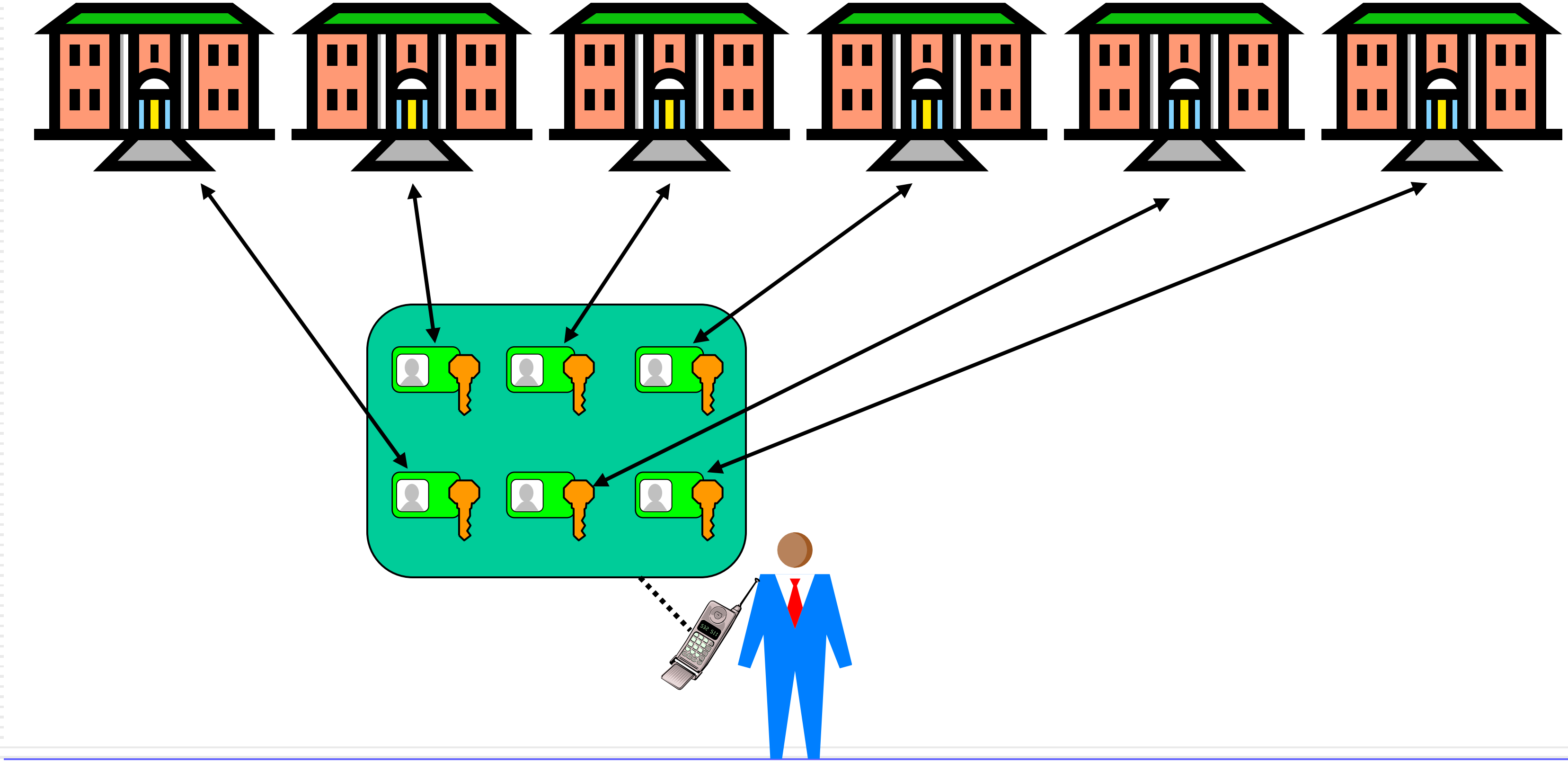


Repository of authentication tokens and Ids.


Legend:
SP
IdP
Identity domain
#
User identifier managed by IdP #
#
Authentication token managed by IdP #
Service logon
Service provision
Personal Authentication Device

User centric SSO: Imagine you’re a customer

It’s a dream



User-Centric SSO

- Advantages
  - Improved usability
  - Compatible with silo identity domains
  - Low trust requirements
  - Good privacy protection
- Disadvantages
  - Does not allows SPs to control service bundling
  - Does not allow SPs to collect user information
  - Requires user-side software or hardware
  - Requires user education

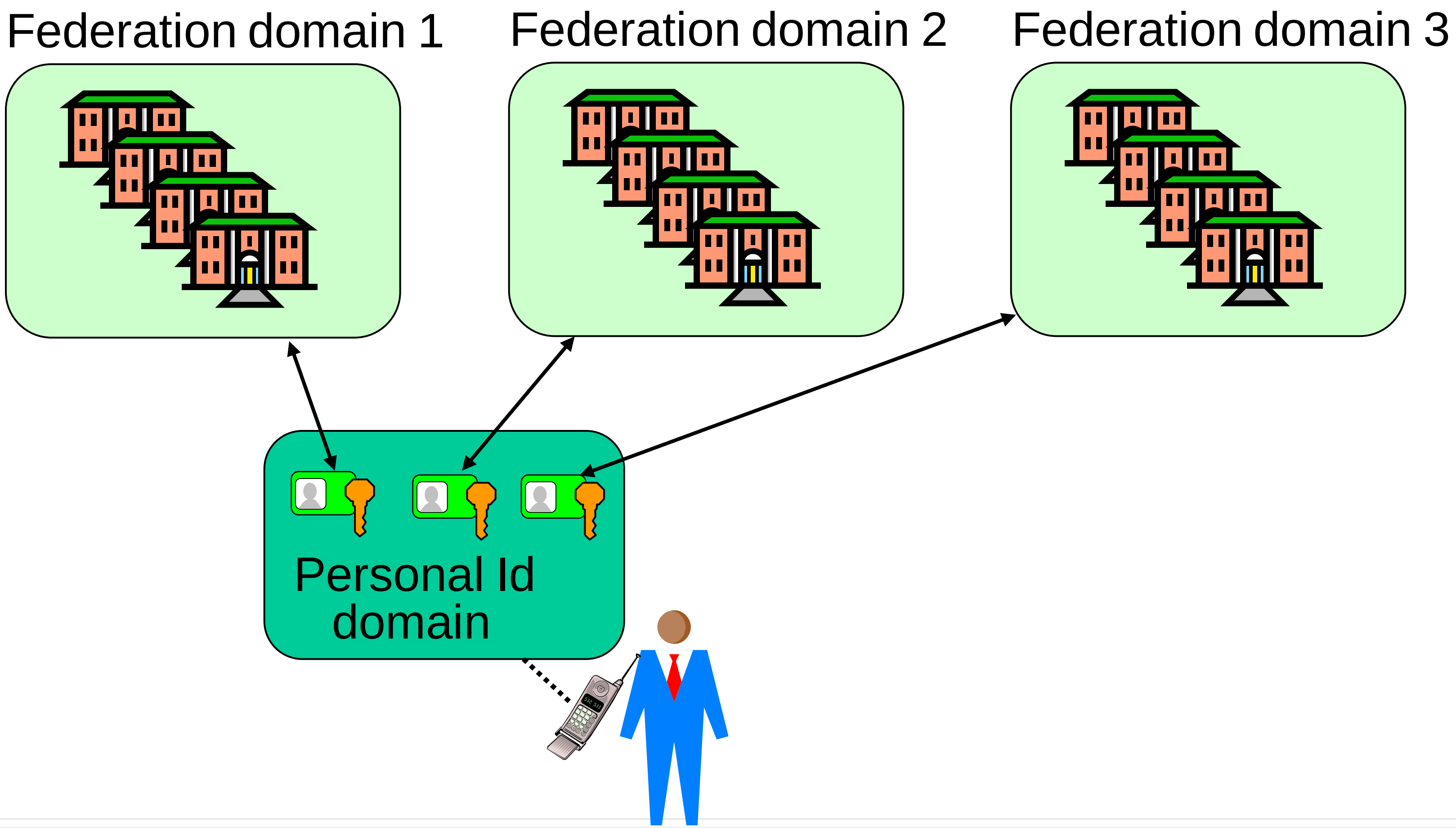
SSO model suitability

- Federated SSO, well suited for
  - Large organisations
  - Government organisations
  - Closely associated organisations
  - Related Web service providers
- User-centric SSO, well suited for
  - Open networks
  - e-commerce
  - Unrelated Web services

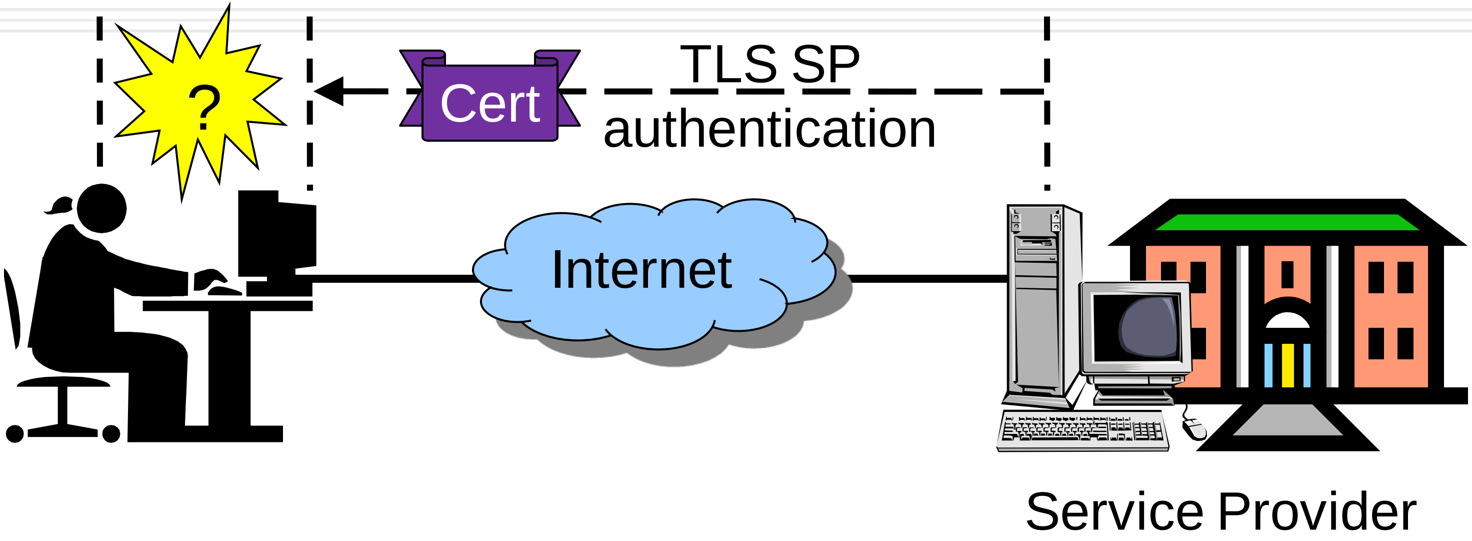
Combined Federated and User-Centric

- It is a myth that identity federation will eliminate multiple identifiers and passwords for users.
- Identity federation will be used to bundle new services that users previously did not access.
- The problem of multiple user identifiers and passwords for unrelated services can only be solved by user-centric methods.
- User-centric methods and federation are perfectly compatible.

Combining federated and user centric identity management



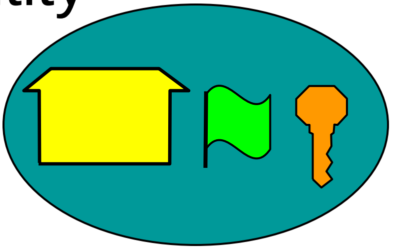
Service Provider Identity Authentication



- Authentication of business and government websites
- Mostly ignored in identity management discussions
- PKI is not enough
- Extremely important!!!

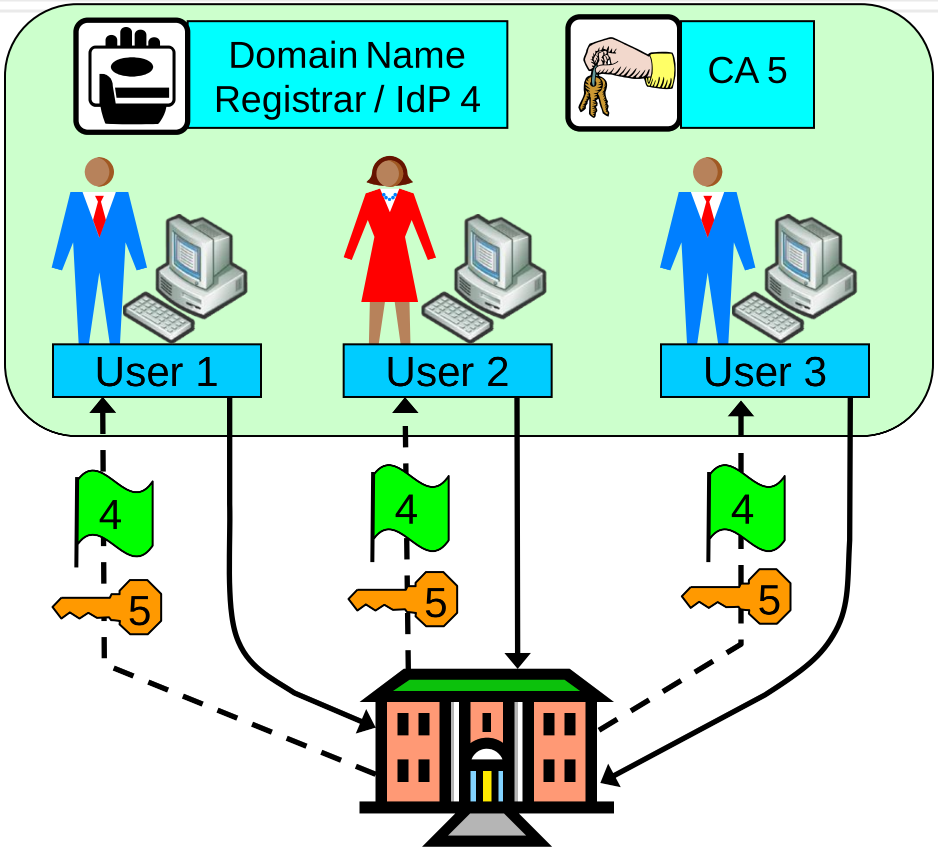
SP identity management

- Traditionally not considered as part of identity management
- No clear unique SP identifier
- Currently a major problem
  - Phishing attacks
  - Virus, Trojan attacks
  - GUI attacks
- Security fails despite strong crypto.
  - Poor usability
  - Poor platform security
- Identity federation and SSO no solution to SP identity management problems.



SP identity management

Common domain model



Legend:

🟩 SP Identity domain

Domain name issued by IdP #

SP entity

Domain name registrar / IdP

Certificate Authority

Auth. token issued by CA #

→ Service access

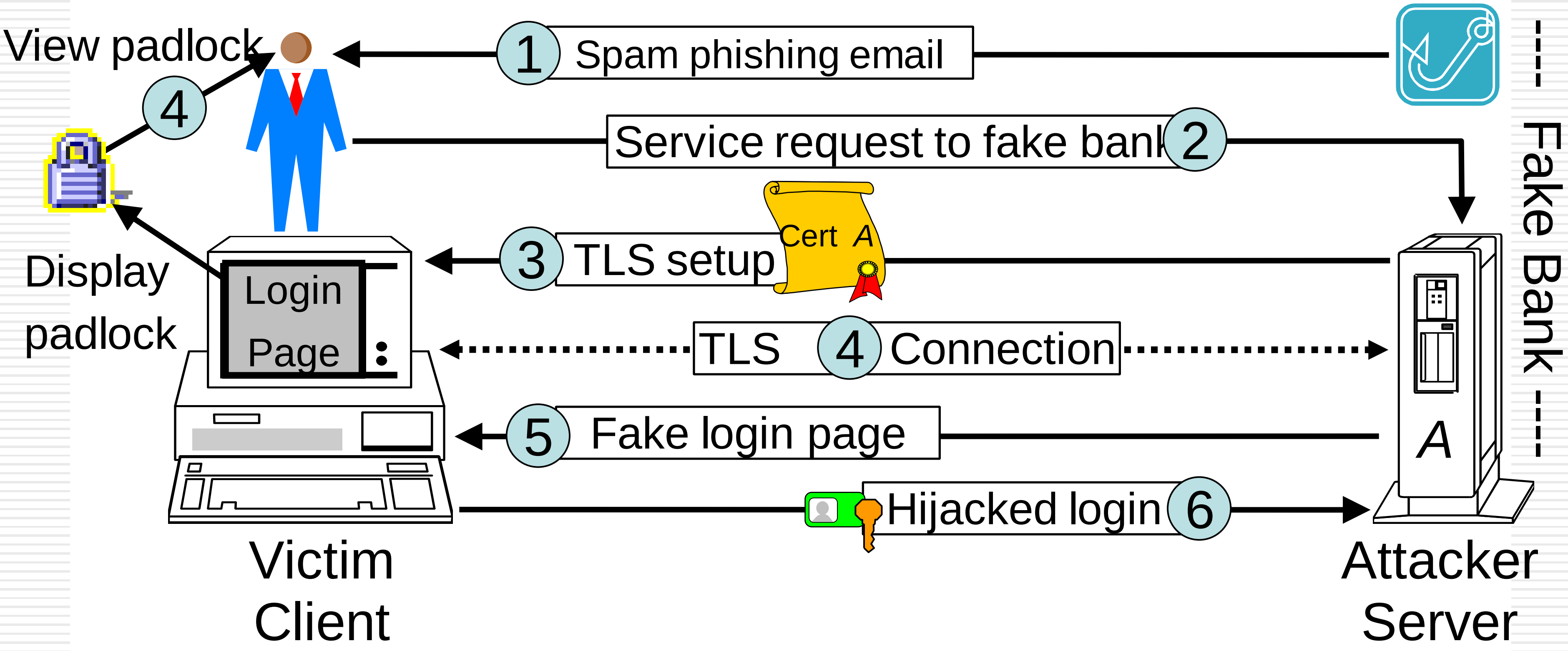
- - → SP authentication

Example: Browser PKI

Common SP identity domain

- Global name space for identifiers: URIs
- Multiple authorities acting as IdP and credentials provider
- All users/clients authenticate the same SP by the same identifier and credential
- Advantages
  - Simple model (PKI in practice), technology exists
  - Good usability possible when well implemented
- Disadvantages
  - Hard to implement well

Meaningless authentication with TLS

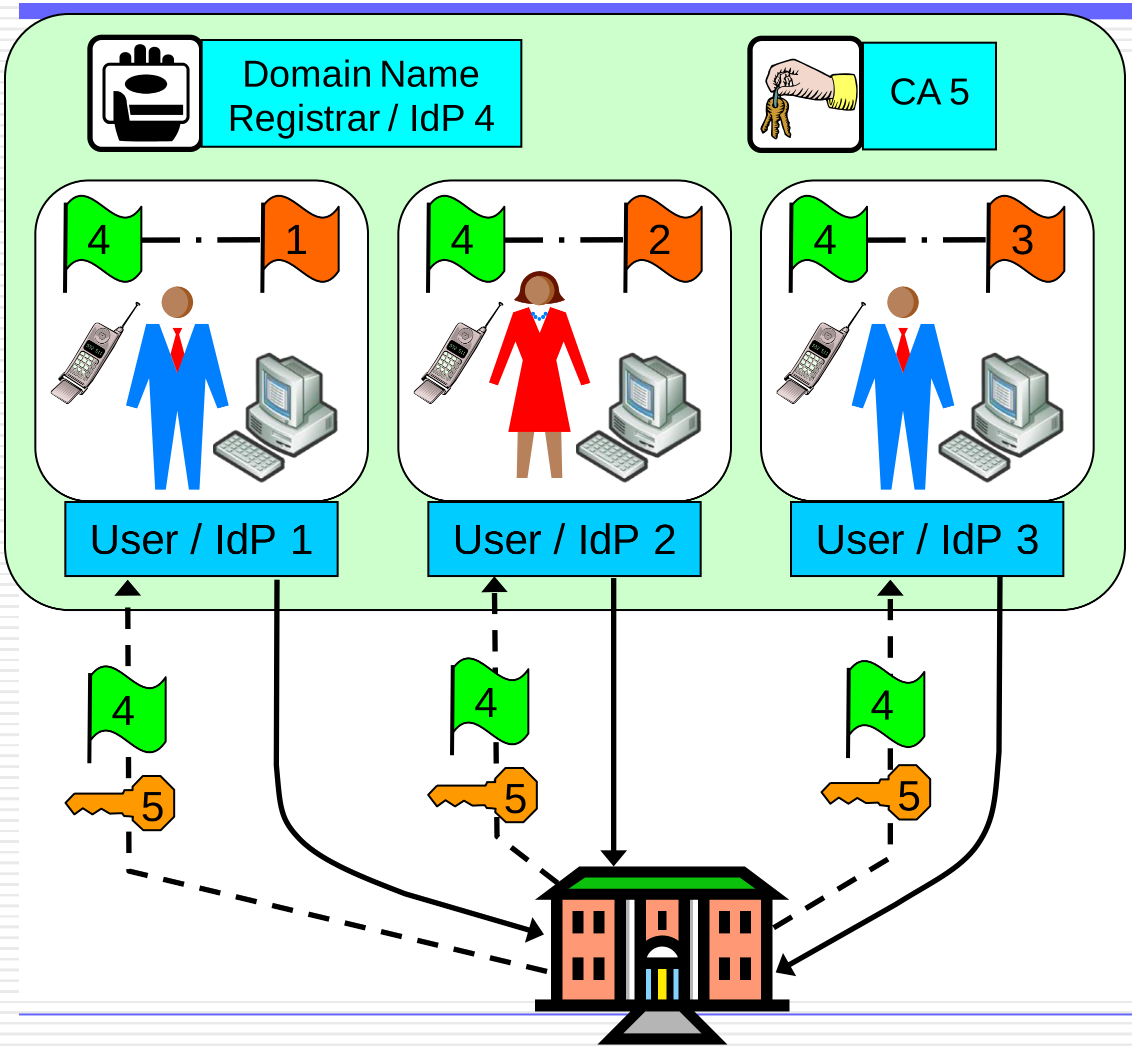


The great server certificate swindle

- SSL designed to provide:
  - Confidentiality, possible with RSA or Diffie-Hellman
  - Authentication, possible with RSA only
- RSA requires certifcitates, Diffie-Hellman not
- In practice, SSL does not provide authentication
  - Only confidentiality
  - RSA not needed
- Conclusion: Certificates worthless for SSL
  - Only valuable for marketing to stimulate (false) trust

SP identity management

User Centric Petname Model



Legend :

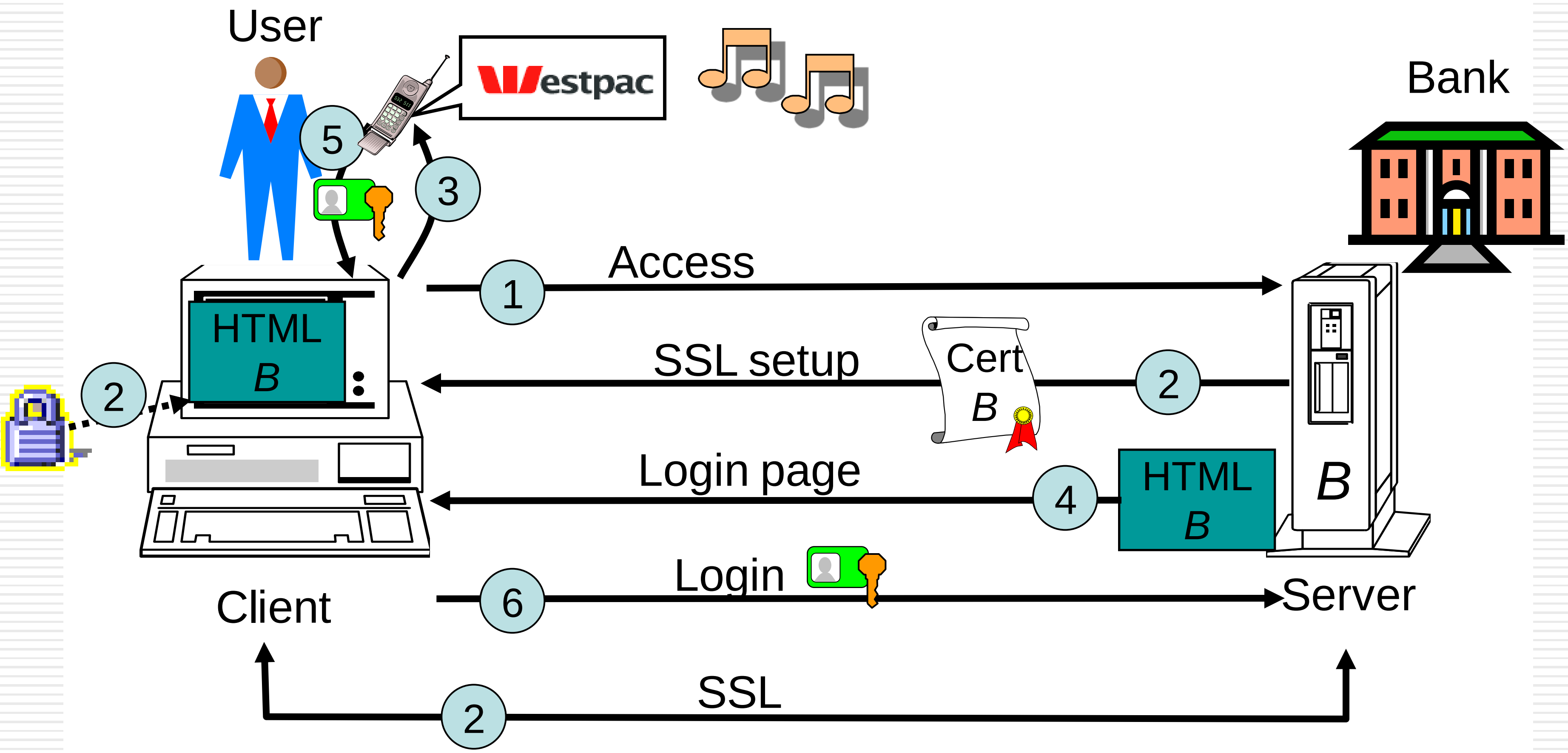
- 🟩 SP Identity domain
- # Domain name issued by IdP #
- # Petname issued by IdP #
- PAD
- SP entity
- Domain name registrar / IdP
- CA
- # Auth. token issued by CA #
- ——→ Service access
- - - -→ SP authentication
- — · — Identifier mapping

User-Centric SP identity domains

- Users create personal unique identifier for each SP they interact with
- Personal identifiers can be names, graphics or sound
- Personal identifiers are mapped to global common identifiers
- Advantages
  - Improved usability
- Disadvantages
  - Requires additional technology for managing SP identities, e.g Mozilla TrustBar

User-centric identity management

Mutual authentication scenario with petnames

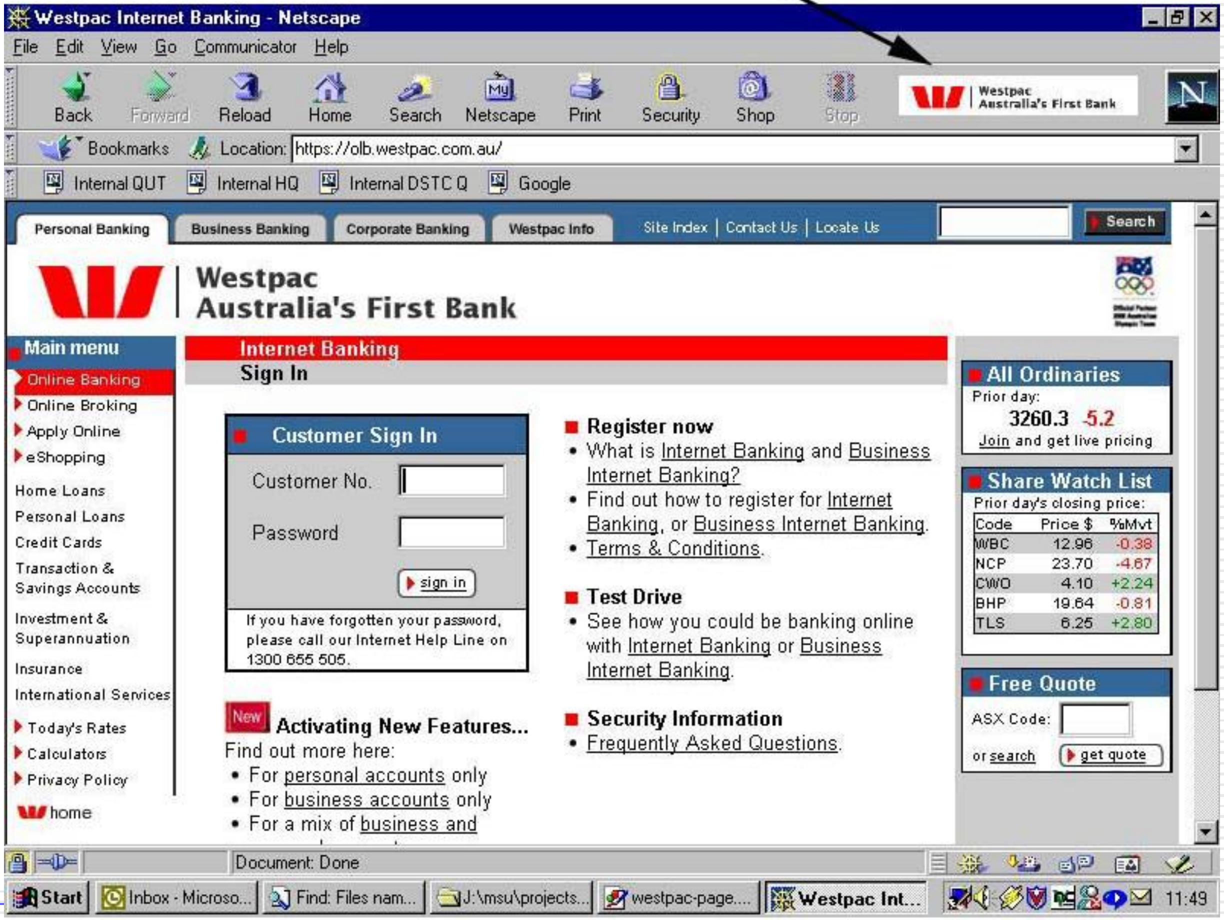


SP identity management with Petnames

Principle of Mozilla TrustBar

Personalised graphical logo and/or sound as site identifier

- Toolbar for the Mozilla and Firefox browsers
- Server certificates personalised by user
- Personal graphics or sound played when SP certificate recognised by browser


Westpac Internet Banking - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Westpac Australia's First Bank
Bookmarks Location: https://olb.westpac.com.au/
Internal QUT Internal HQ Internal DSTC Q Google
Personal Banking Business Banking Corporate Banking Westpac Info Site Index | Contact Us | Locate Us Search

Westpac
Australia's First Bank

Main menu
- Online Banking
- Online Broking
- Apply Online
- eShopping

Home Loans
Personal Loans
Credit Cards
Transaction & Savings Accounts
Investment & Superannuation
Insurance
International Services

- Today's Rates
- Calculators
- Privacy Policy

home

Internet Banking
Sign In

Customer Sign In
Customer No.
Password
sign in

If you have forgotten your password, please call our Internet Help Line on 1300 655 505.

New Activating New Features...
Find out more here:
- For personal accounts only
- For business accounts only
- For a mix of business and

Register now
- What is Internet Banking and Business Internet Banking?
- Find out how to register for Internet Banking, or Business Internet Banking.
- Terms & Conditions.

Test Drive
- See how you could be banking online with Internet Banking or Business Internet Banking.

Security Information
- Frequently Asked Questions.

All Ordinaries
Prior day:
3260.3 -5.2
Join and get live pricing

Share Watch List
Prior day's closing price:

Code	Price $	%Mvt
WBC	12.96	-0.38
NCP	23.70	-4.67
CWO	4.10	+2.24
BHP	19.64	-0.81
TLS	6.25	+2.80

Free Quote
ASX Code:
or search get quote

Document: Done

Start Inbox - Microso... Find: Files nam... J:\msu\projects... westpac-page... Westpac Int... 11:49

The European IDA → IDABC → ISA

- IDA: *Interchange of Data between Administrations*
  - EU Work Programme 2000 – 2004
- IBAC: *Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens*
  - EU Work Programme 2005 – 2009
- ISA: *Interoperable Solutions for European Public Administrations*
  - EU Work Programme 2010 – 2015

- Assurance Levels 1-4 defined in IDA auth. policy of 2004.
- Should include Level 0 to cover non-authenticating services and anonymous authentication

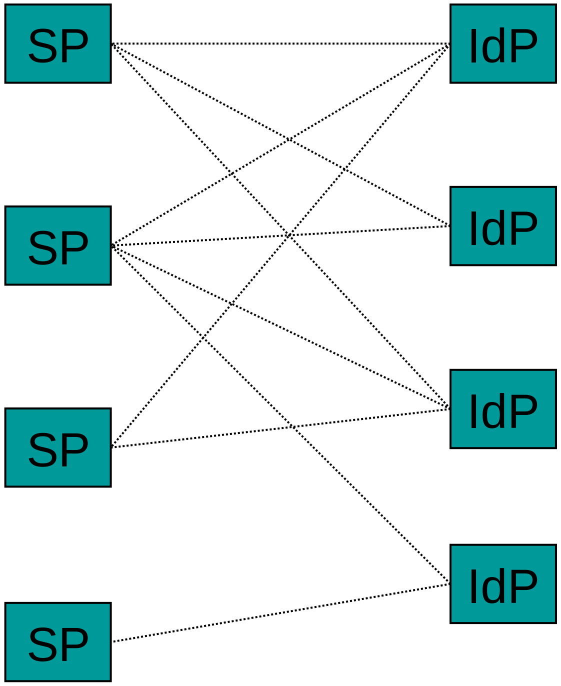
The STORK Project 2009 - 2011

- **S**ecure iden**T**ity acr**O**ss bo**R**ders lin**K**ed
- Cross-border recognition of eID
- Supports mobility of citizens
- Pilots:
  - Cross-border authentication platform
  - Safe use of the Internet for children using eID
  - Cross-border student mobility
  - Cross-border online delivery of documents
  - Change of address with eID

Four national identity federations

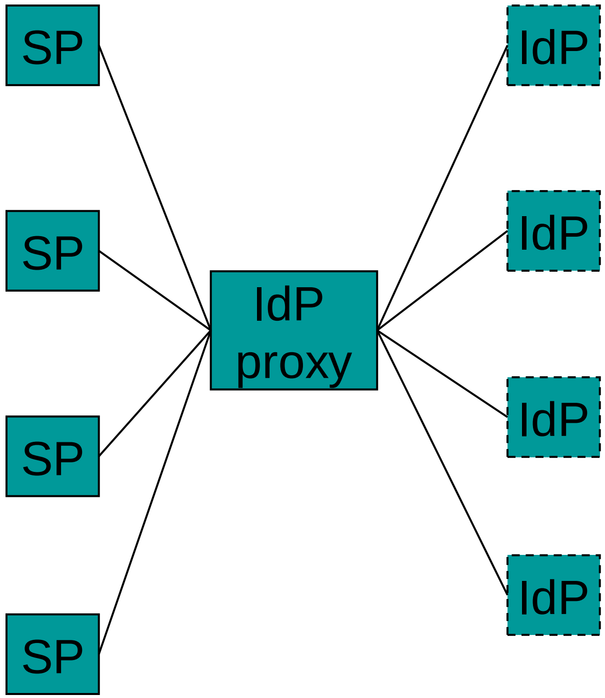
Haka (Finland):	Operational (Shibboleth)
FEIDE (Norway):	Operational (Moria, SAML2.0)
DK-AAI (Denmark):	Piloting (A-Select)
SWAMID (Sweden):	Piloting (Shibboleth)

Technical shape of a federation: Distributed



- Model deployed by Haka (.fi), SWAMID (.se) and several other federations
- Pros
  - No single point of failure in the message flow
  - Costs of federation management low
- Cons
  - Hard to track errors and
  - Not well supported by commercial products

Technical shape of a federation: Centralized



- Model deployed by FEIDE (.no) and WAYF (.dk)
- Pros
  - A single point where to locate problems and introduce new features
  - Economics of scale
- Cons
  - A single point of failure
  - Everyone needs to trust the IdP in the middle

FEIDE (Felles Elektronisk Identitet)

- FEIDE is a system for Id management within the Norwegian national education sector.
- Users have only one username and password
- Users access web-services via a central log-in service
- Services are given what they need to know about the user
- Services are not given the users password/credential, only information about the user

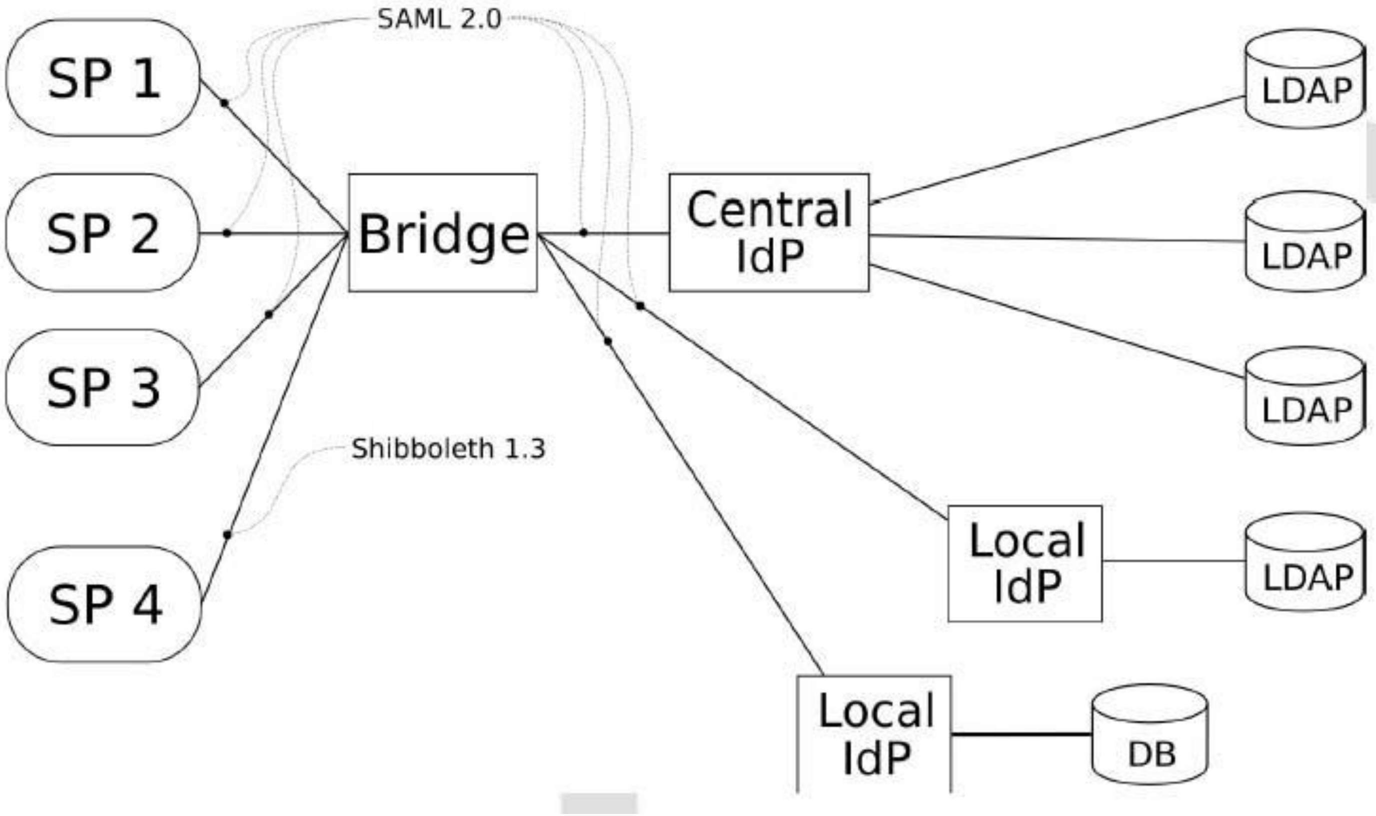
FEIDE (continued)

- FEIDE have formal agreements with the schools before they are connected
- The home organizations (schools) are responsible for the data about the users (correct and up-to-date)
- Home organizations decide themselves what services their users should be able to access via the central log-in service

FEIDE Technical Aspects

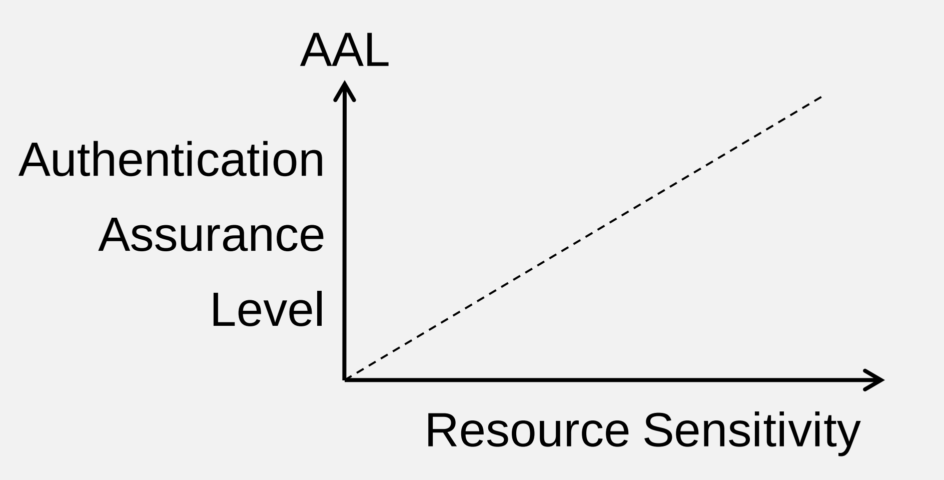
- Based on SAML 2.0
- Backend authenticate users by using LDAP
- One central identity provider (IdP) where service providers (SPs) are connected
- Single Sign On when going between services
- Single Log Out when logging out from a service

FEIDE Architecture



Authentication Assurance

- Resources have different sensitivity levels
  - Higher sensitivity requires stronger authentication
- Authentication has a cost
  - Stronger authentication costs more
- Authentication assurence should be adapted to the sensitivity level

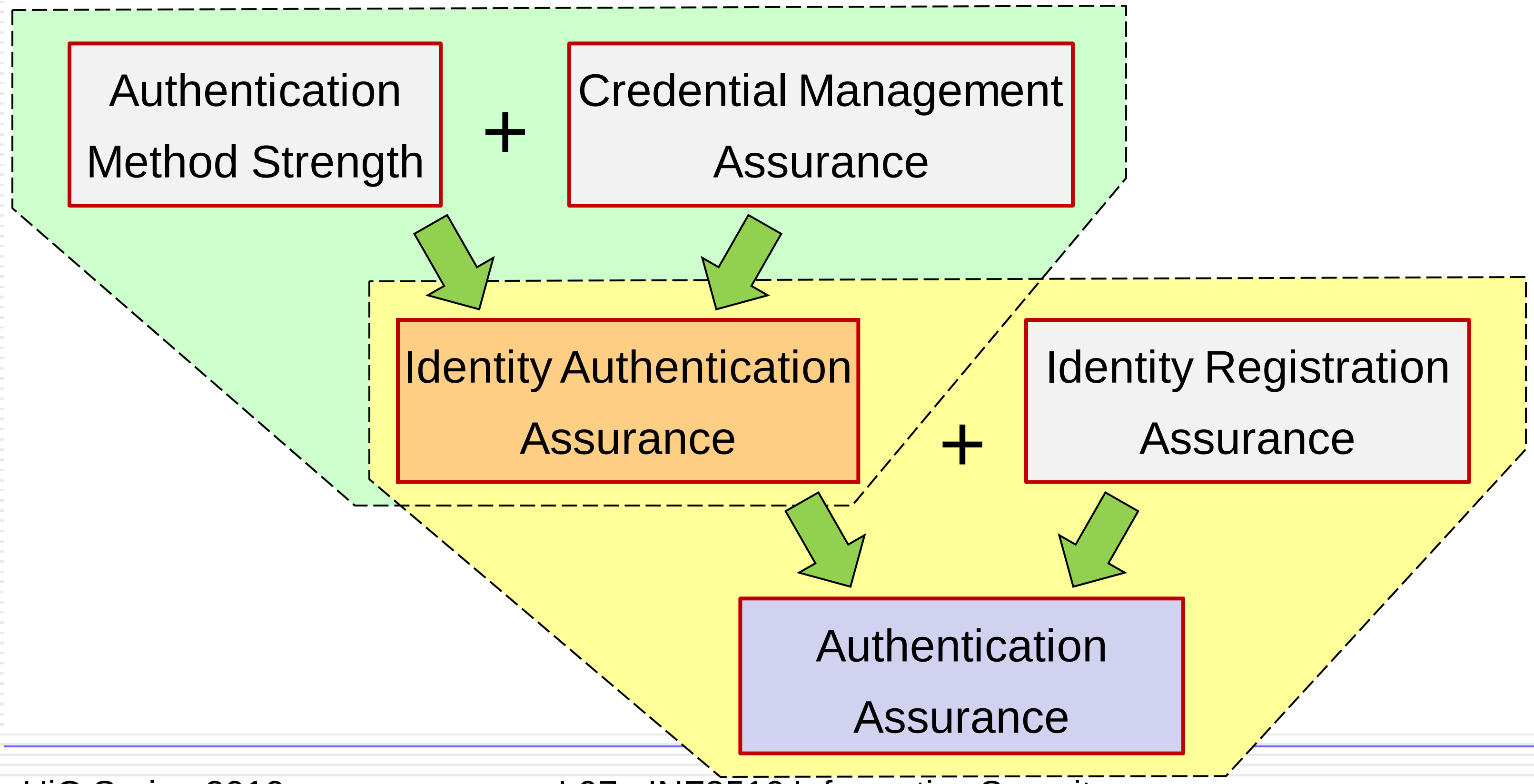


Why authentication frameworks?

- Trust in identity is a requirement for e-business.
- Authentication assurance produces identity trust.
- Authentication depends on technology, policy, standards, practice, behaviour and regulation.
- Consistency of approach allows cross-national and cross-organisational schemes that enable convenience, efficiency and cost savings.

Authentication Assurance

- Do we have the correct party at the other end of the line?
- Authentication assurance through the combination of:


Authentication Method Strength
+
Credential Management Assurance
Identity Authentication Assurance
+
Identity Registration Assurance
Authentication Assurance

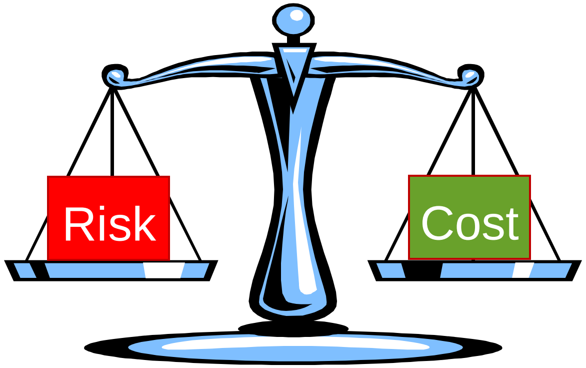
Authentication Assurance Requirement

- Application sensitivity

  Higher Sensitivity
  → Higher Risk

- Authentication cost

  Stronger Authentication
  → Higher Cost



- Authentication assurance should reflect application sensitivity.
- Risk of getting e-Authentication wrong must balance the cost.

AAL: Authentication Assurance Levels

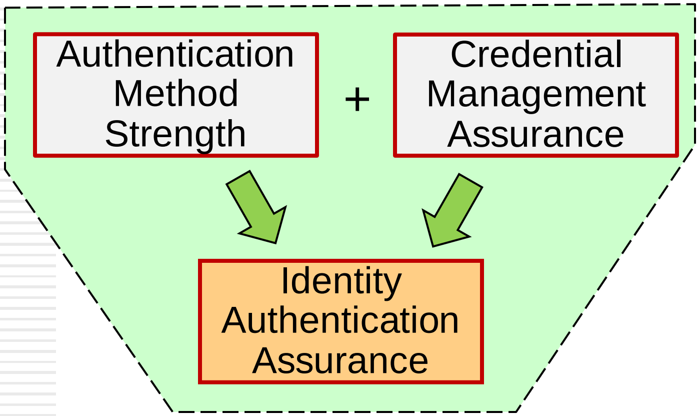
No Assurance	Minimal Assurance	Low Assurance	Moderate Assurance	High Assurance
Level 0	Level 1	Level 2	Level 3	Level 4
No registration of identity required	Minimal confidence is required in the identity assertion	Low confidence is required in the identity assertion	Moderate confidence is required in the identity assertion	High confidence is required in the identity assertion

Example taken from Australian NeAF 2009

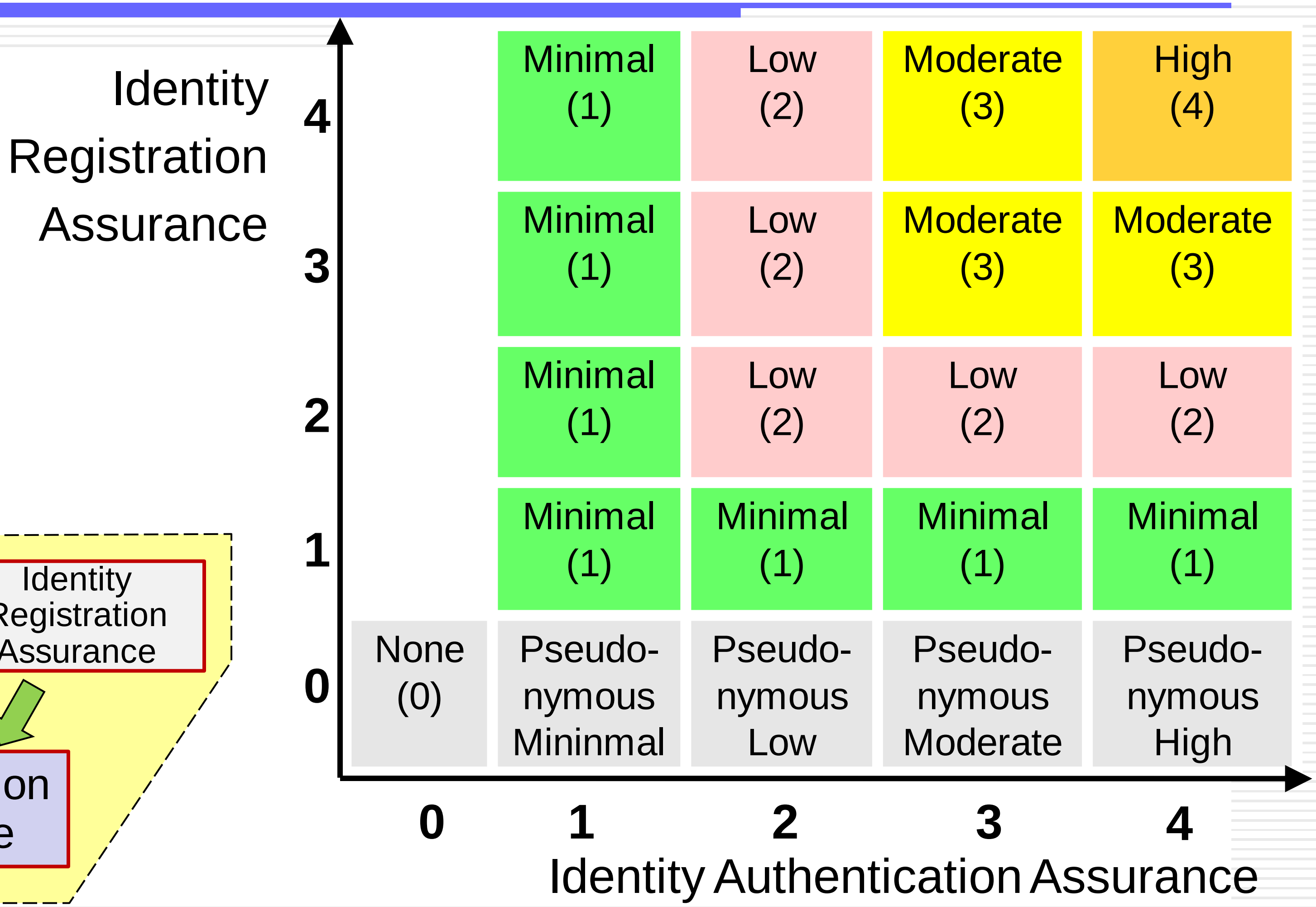
Identity Authentication Assurance Levels

Credential Management Assurance	1	2	3	4
4	Low (2)	Moderate (3)	High (4)	High (4)
3	Low (2)	Moderate (3)	Moderate (3)	High (4)
2	Low (2)	Low (2)	Moderate (3)	Moderate (3)
1	Minimal (1)	Low (2)	Low (2)	Low (2)

Authentication Method Strength


Authentication Method Strength
+
Credential Management Assurance
Identity Authentication Assurance

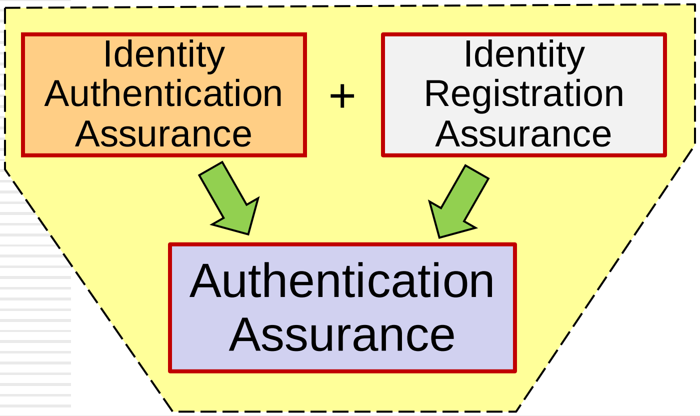
Authentication Assurance Levels



Identity Registration Assurance

	0	1	2	3	4
4		Minimal (1)	Low (2)	Moderate (3)	High (4)
3		Minimal (1)	Low (2)	Moderate (3)	Moderate (3)
2		Minimal (1)	Low (2)	Low (2)	Low (2)
1		Minimal (1)	Minimal (1)	Minimal (1)	Minimal (1)
0	None (0)	Pseudo-nymous Mininmal	Pseudo-nymous Low	Pseudo-nymous Moderate	Pseudo-nymous High

Identity Authentication Assurance



Identity Authentication Assurance + Identity Registration Assurance

Authentication Assurance

Comparison of Assurance Levels

<table>
<tr><th></th><th colspan="20">Assurance Levels</th></tr>
<tr><th>IDA (EU)</th><td colspan="4">N/A</td><td colspan="4">Minimal
(1)</td><td colspan="4">Low
(2)</td><td colspan="4">Substantial
(3)</td><td colspan="4">High
(4)</td></tr>
<tr><th>NeAF (Au)</th><td colspan="4">None
(0)</td><td colspan="4">Minimal
(1)</td><td colspan="4">Low
(2)</td><td colspan="4">Moderate
(3)</td><td colspan="4">High
(4)</td></tr>
<tr><th>NIST (US)
FADS (Norw.)</th><td colspan="8">Little or None
(1)</td><td colspan="4">Some
(2)</td><td colspan="4">High
(3)</td><td colspan="4">Very High
(4)</td></tr>
<tr><th>UKOnline</th><td colspan="5">Minimal
(0)</td><td colspan="5">Minor
(1)</td><td colspan="5">Significant
(2)</td><td colspan="5">Substantial
(3)</td></tr>
</table>

- IDA: Interchange of Data between Administrations
- NeAF: National e-Authentication framework
- NIST: National Institute of Standards and Technology
- FADS: Framework for Authentication and Digital Signatures

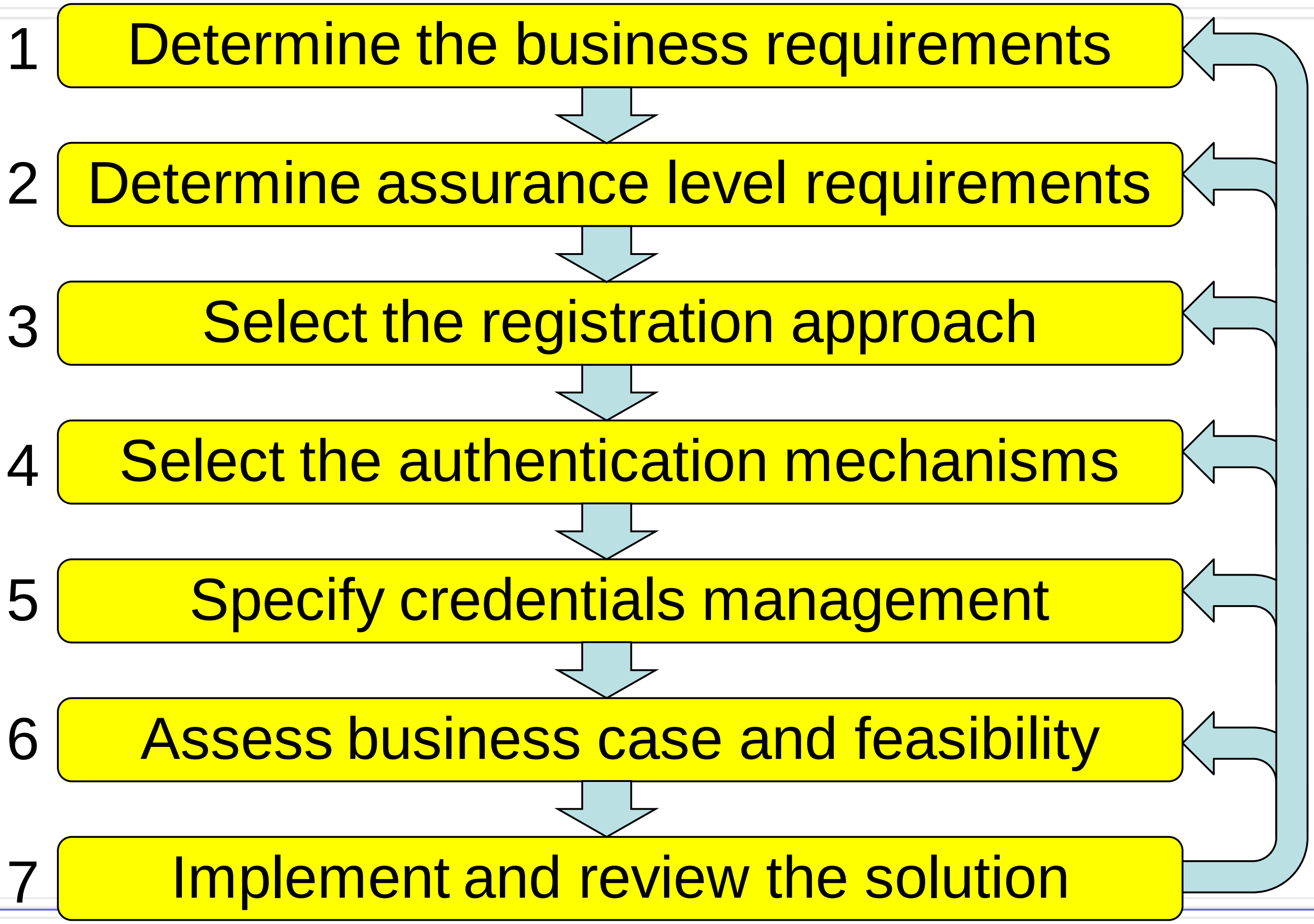
Risk Analysis for Authentication

Determines required Authentication Assurance Level

		Impact of e-Authentication failure				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	None (0)	Low (2)	Moderate (3)	High (4)	High (4)
	Likely	None (0)	Low (2)	Moderate (3)	High (4)	High (4)
	Possible	None (0)	Minimal (1)	Low (2)	Moderate (3)	High (4)
	Unlikely	None (0)	Minimal (1)	Low (2)	Moderate (3)	Moderate (3)
	Rare	None (0)	Minimal (1)	Low (2)	Moderate (3)	Moderate (3)

Example: NeAF Australia

Steps of an Authentication Framework



1 Determine the business requirements

2 Determine assurance level requirements

3 Select the registration approach

4 Select the authentication mechanisms

5 Specify credentials management

6 Assess business case and feasibility

7 Implement and review the solution

Conclusion

- Shared identity and access management requires compatible technologies, policies and assurance levels
- Many projects focus on technical solutions for cross-national/organisational integration
- Full integration requires
  - Compatible identity registration policies,
  - Accepted credentials management (distribution, storage)
  - Compatible authentication assurance levels
  - Mutual trust and political support
- Integration of identity and access solutions is challenging!