Identity Management

NISNET Winter School
Finse, April 2008

Audun Jøsang <josang @ unik.no>

UNIK

UNIVERSITY GRADUATE CENTER

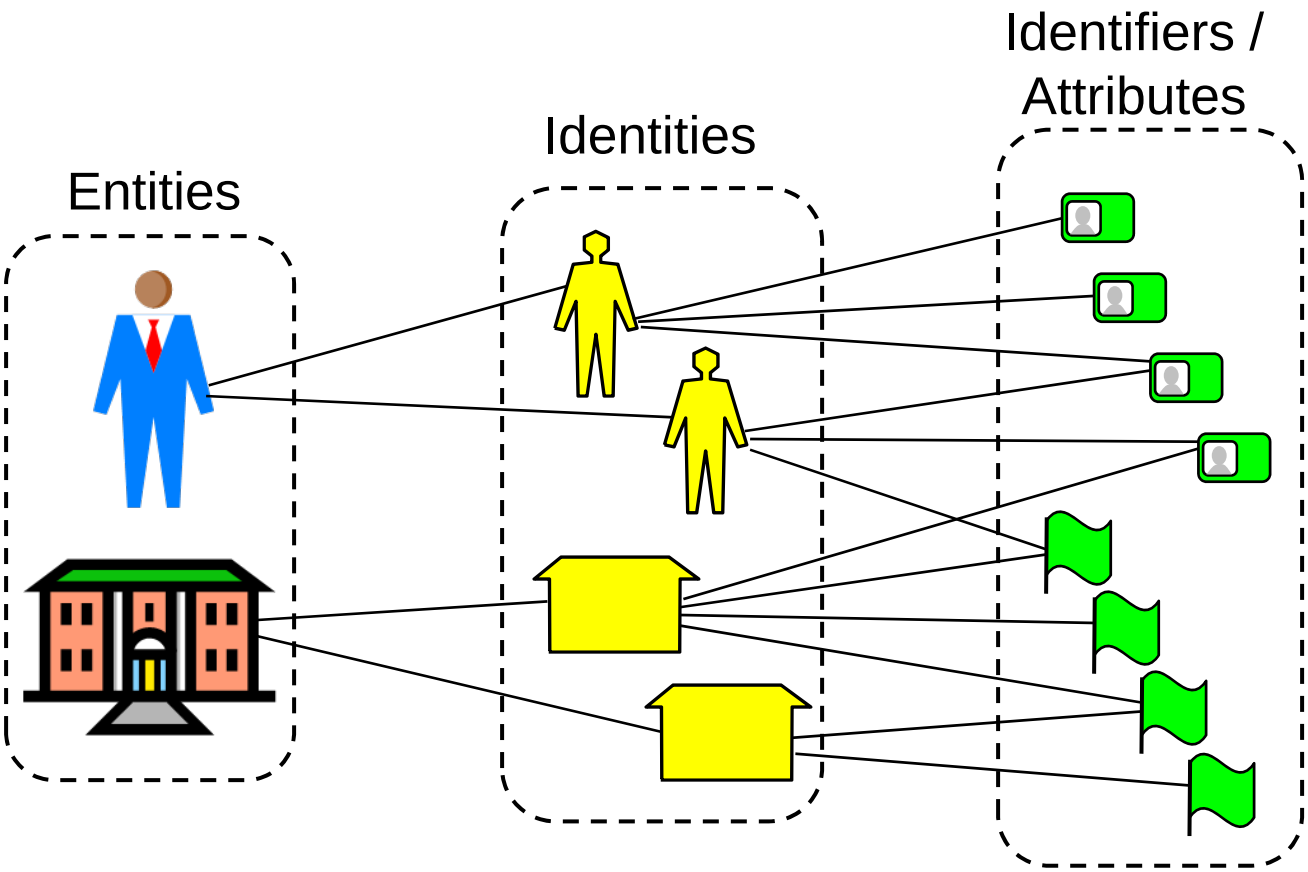
This talk

- Identity and identity management concepts
- Identity management models
- Service provider identities
- Authentication assurance
- Security Usability
- Research challenges

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
    - Unique identifiers within a domain
    - Non-unique identifiers 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



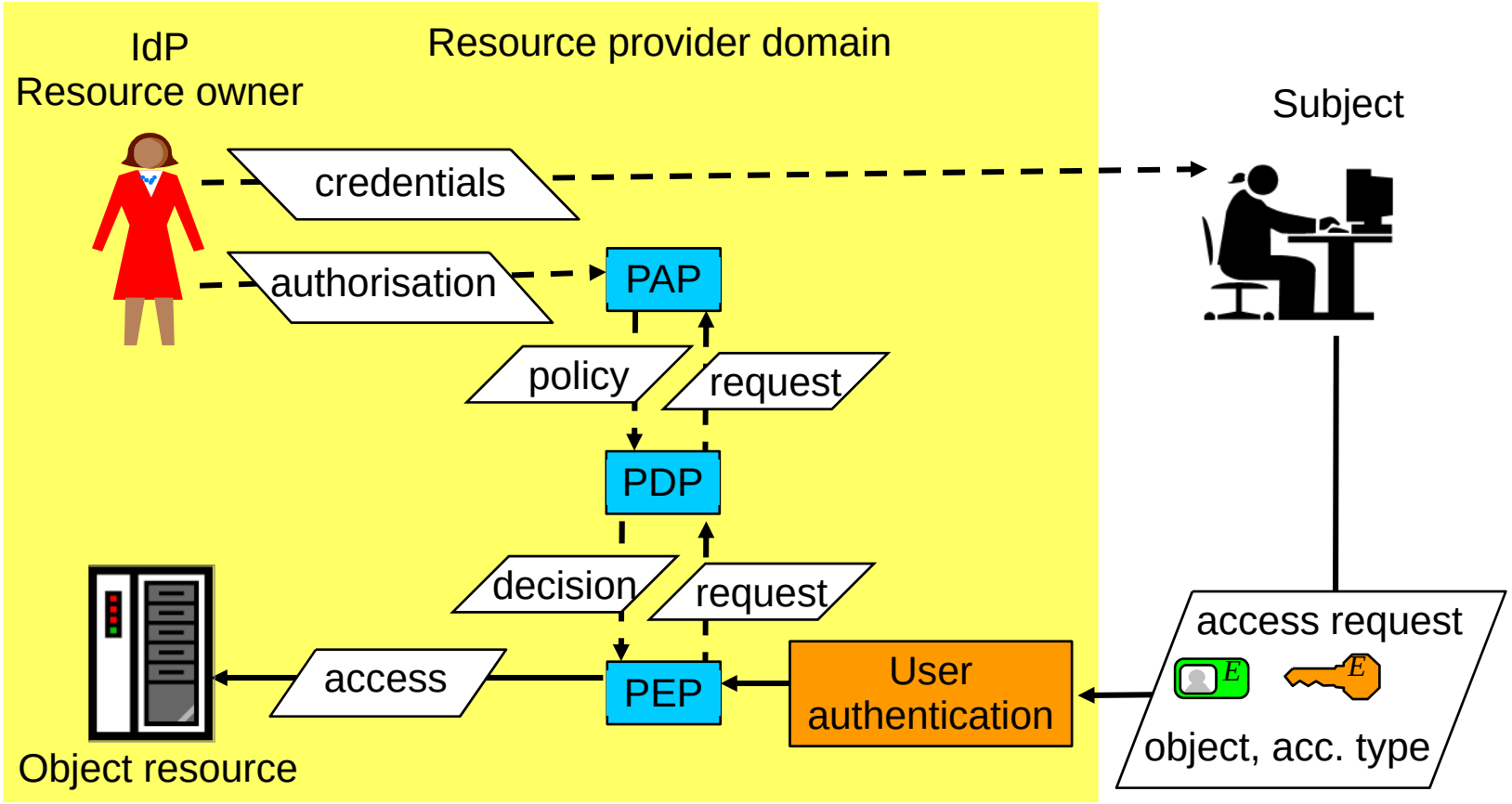
What is identity management?

- Representing and recognising entities as digital identities
- Managing name spaces of unique identifiers
- Managing access credentials/tokens to entities
- Covers AAA
  - (Authentication, Access Control and Accounting)
  - First identify, then authenticate, finally control access

Comment about AAA and Authorization

- Traditionally AAA stands for ”Authentication, *Authorization* and Accounting”
  - ”Authorization” is here interpreted as access control
  - Leads to absurd conclusions
- Authorization is to set access policy
  - E.g. Definition of ”Confidentiality” is that only ”authorized” entities shall have read access to info.
- Attackers who access info with stolen passwords are not authorized
  - Accoording to the traditional AAA terminology the attackers would be authorized
  - In reality it is a case of a false positive access decision

Access control conceptual diagram



Legend

PAP: Policy Administration Point

PEP: Policy Enforcement Point

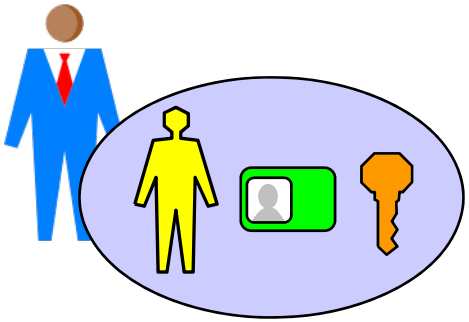
PDP: Policy Decision Point

IdP: Identity Provider

(WS-Security terminology and architecture)

http://www.oasis-open.org/specs/index.php

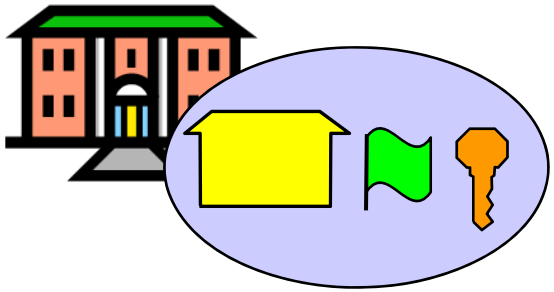
Who's identity?



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

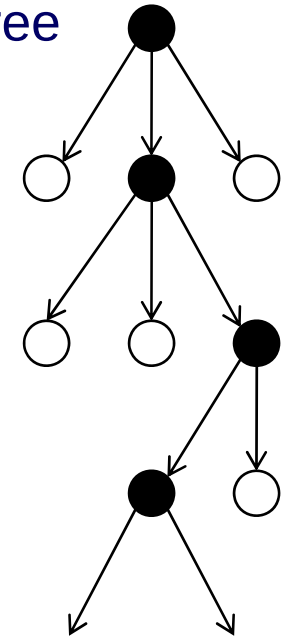
Name spaces of unique identifiers

- 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

X.500 Directory

- Hierarchical name space
- Inspired by the postal network
- Defunct when X.400 mail became defunct

Directory Information Tree



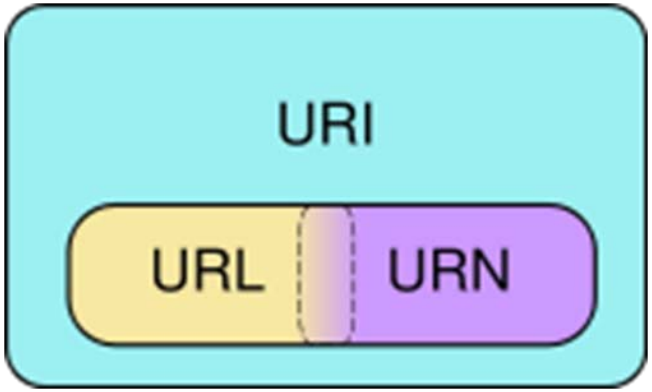
RDN of entry	Distinguished name of entry
{null}	{null}
{Country=GB}	{Country=GB}
{Organisation=BT}	{{Country=GB} Organisation=BT}
{Organisational Unit=Sales, Location=London}	{{{Country=GB} Organisation=BT} Organisational Unit=Sales, Location=London}

UNIK UNIVERSITY GRADUATE CENTER

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?
  - mailto:josang@unik.no

Scheme URN 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

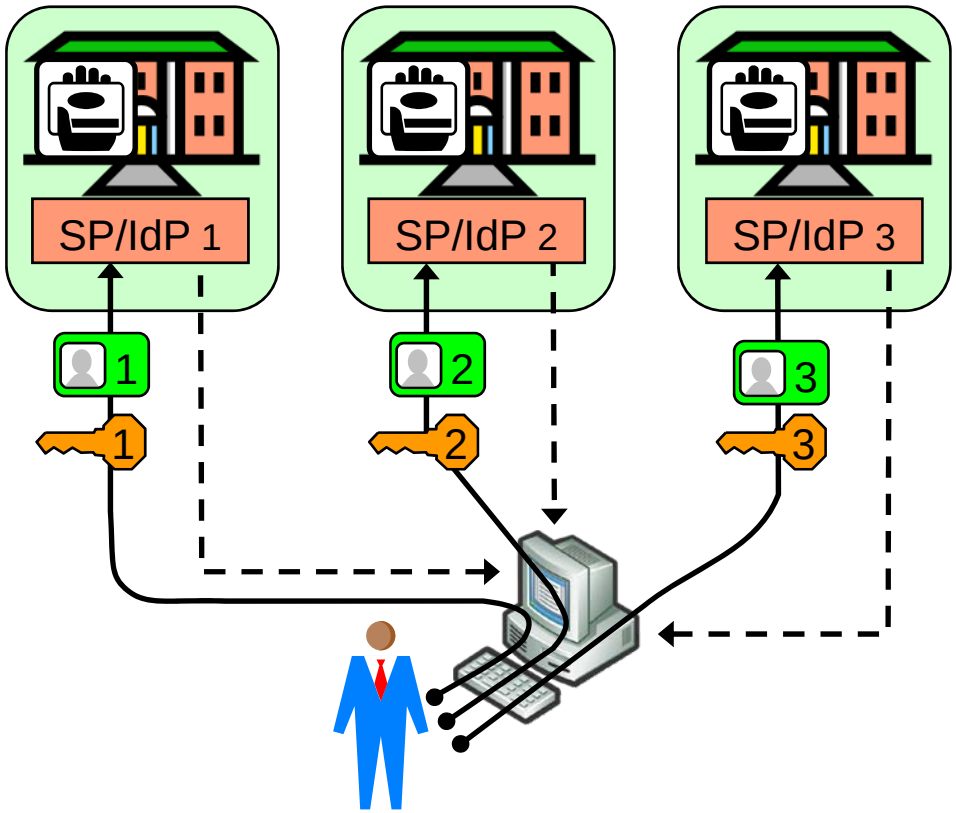
Community i-numbers

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

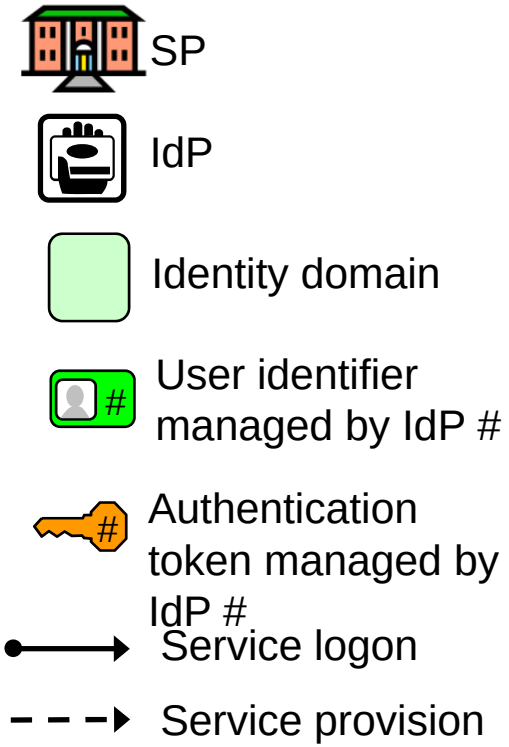
Identifier characteristics

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

Silo domain model



Legend:

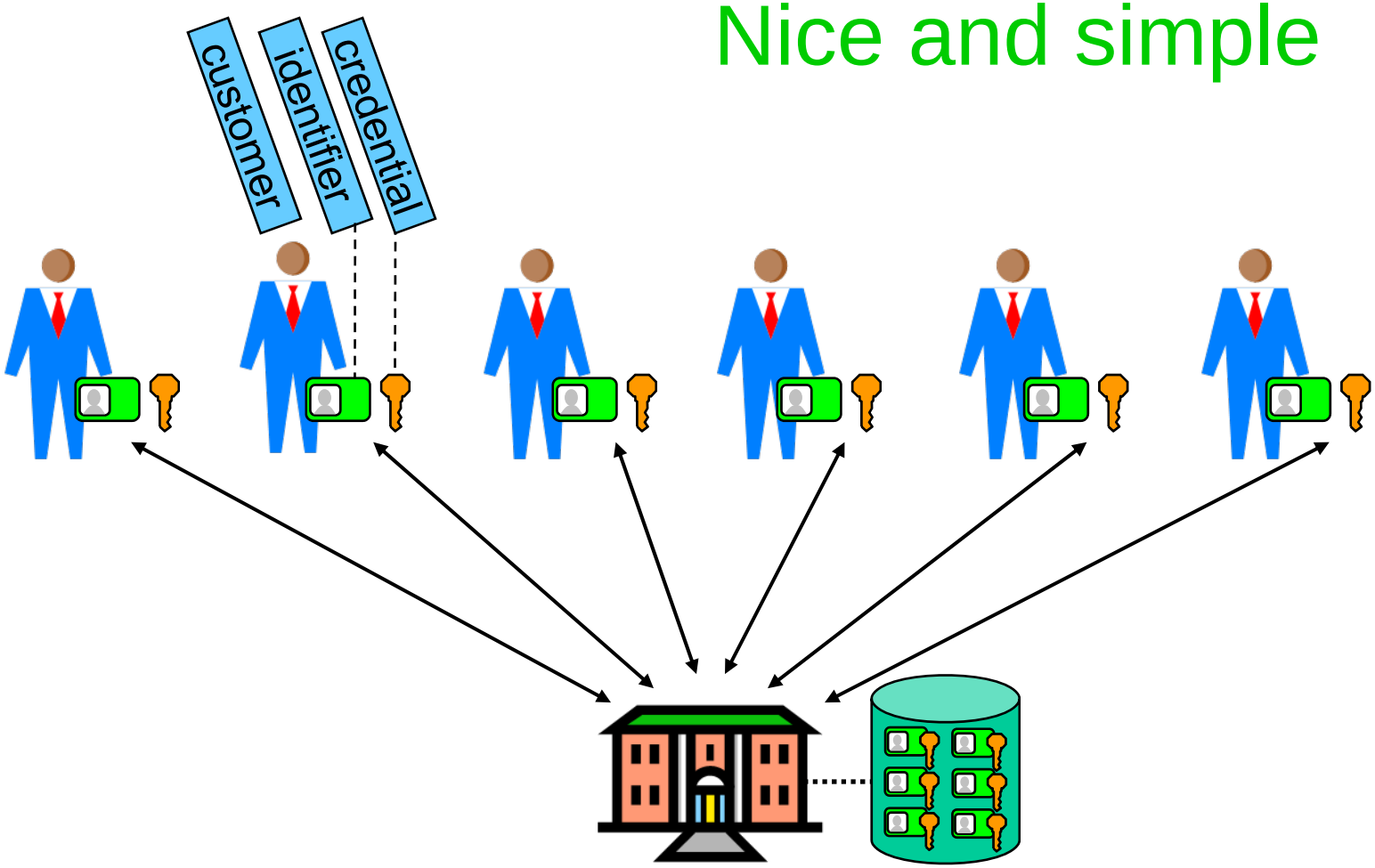


Silo user-identity domains

- 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

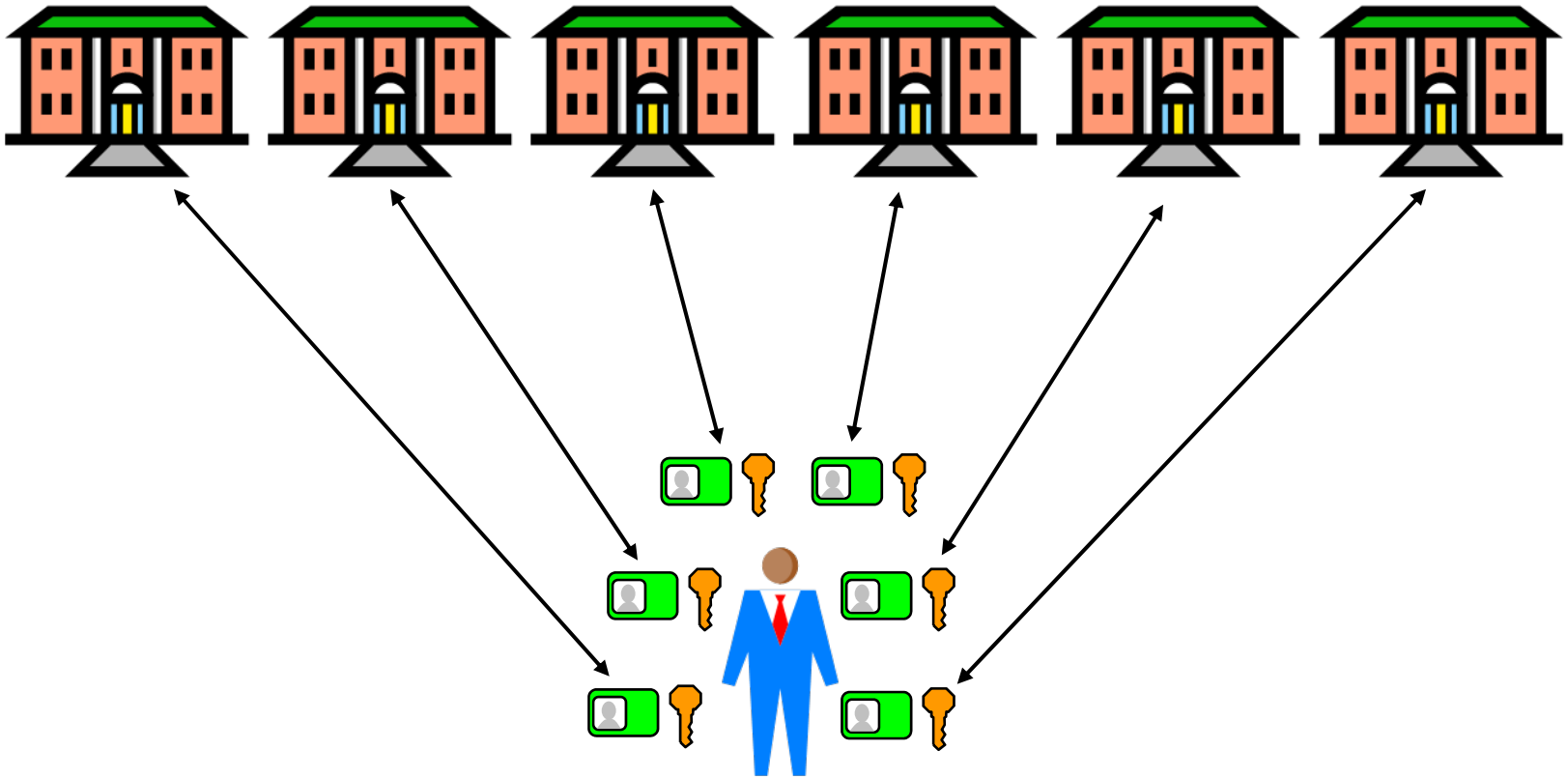
Imagine you're a service provider

Nice and simple

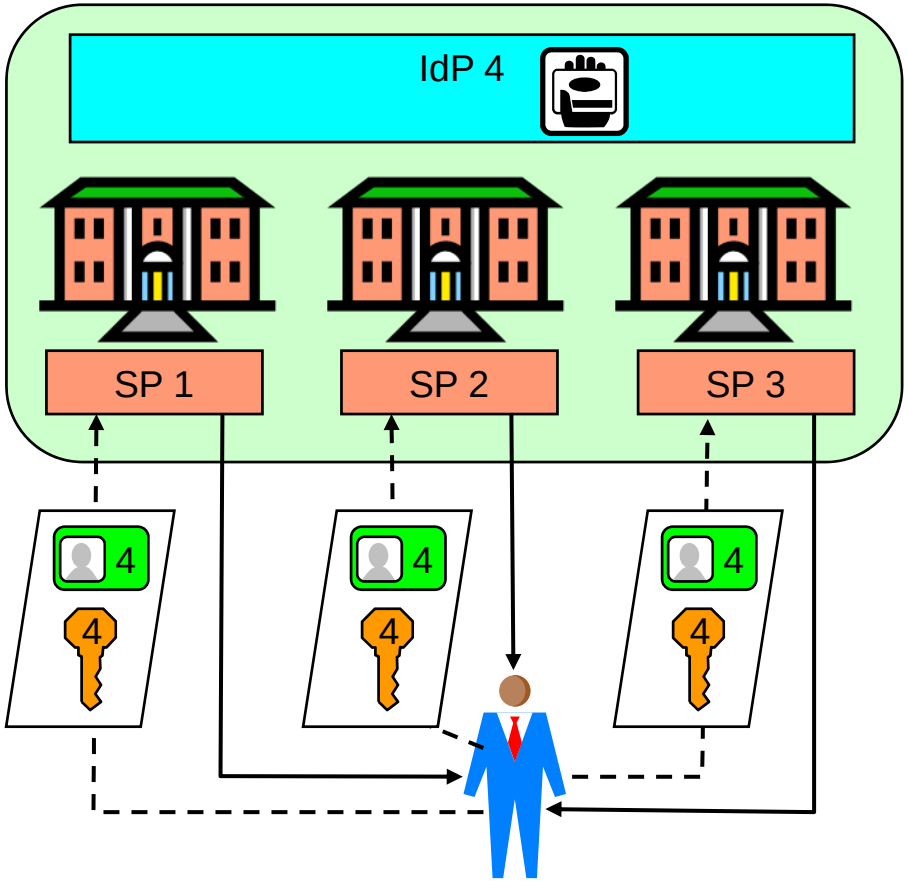


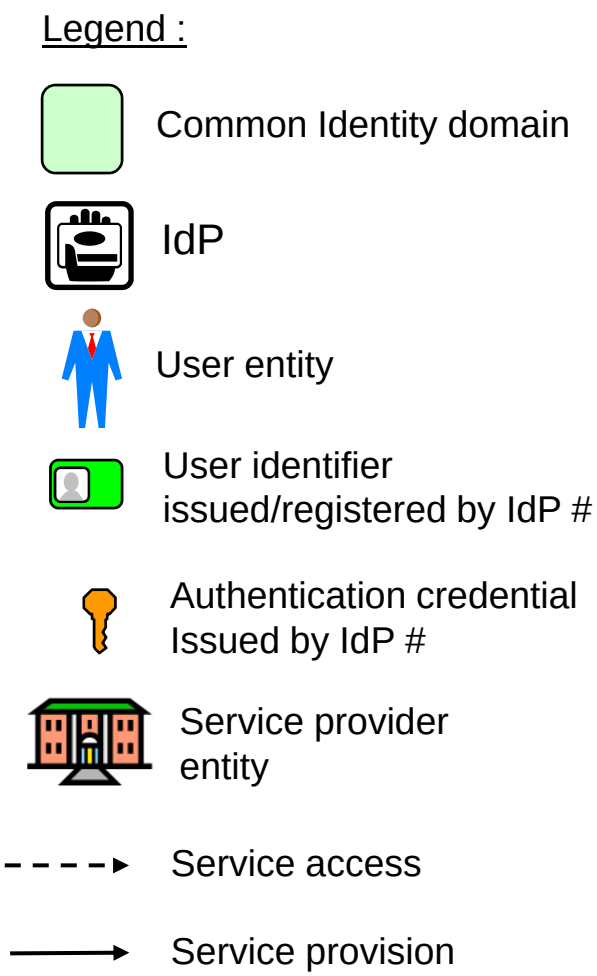
Imagine you're a customer

It's a nightmare



Common user identity domain





Example: PKI with user certificates

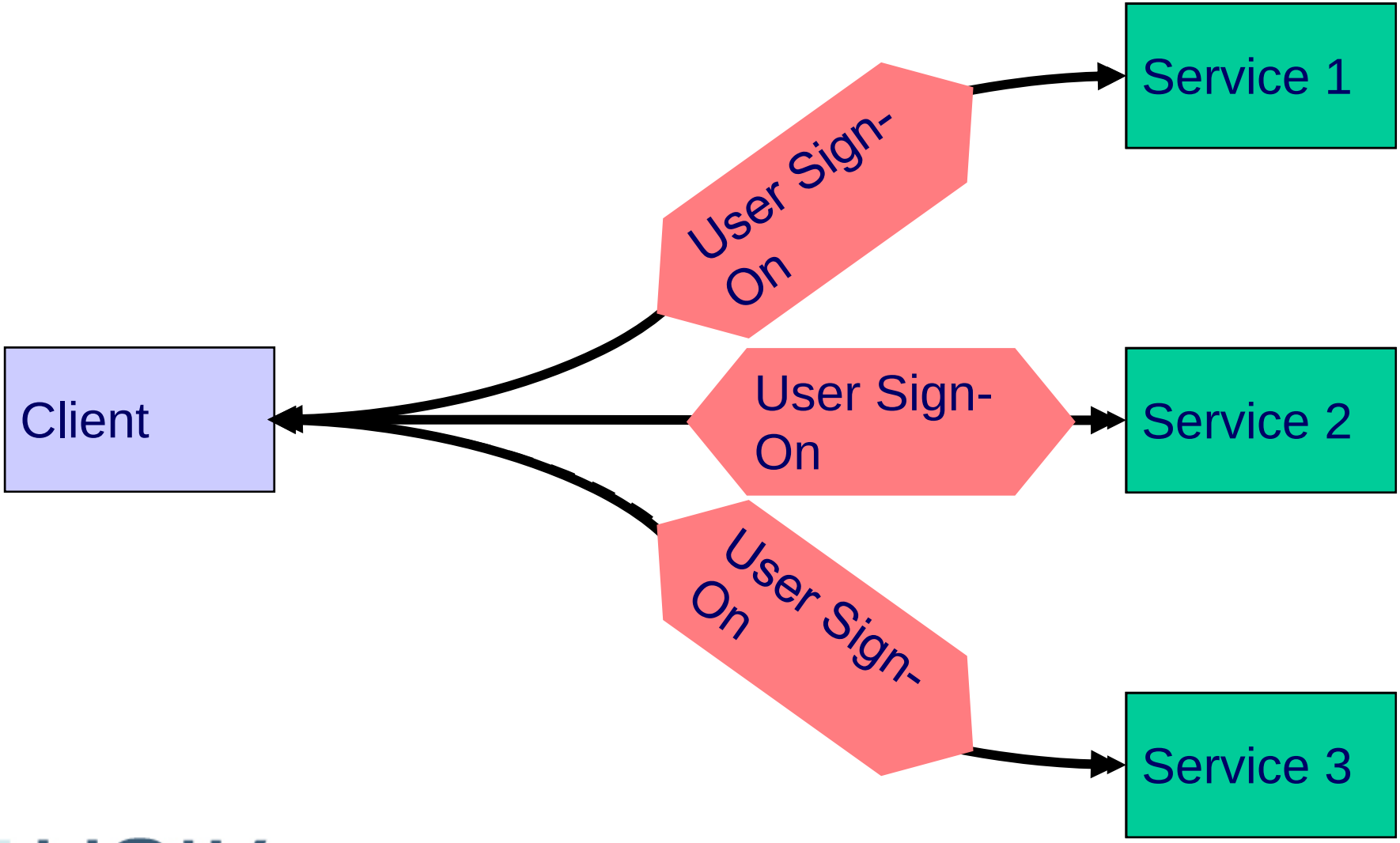
Common user identity domain

- 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

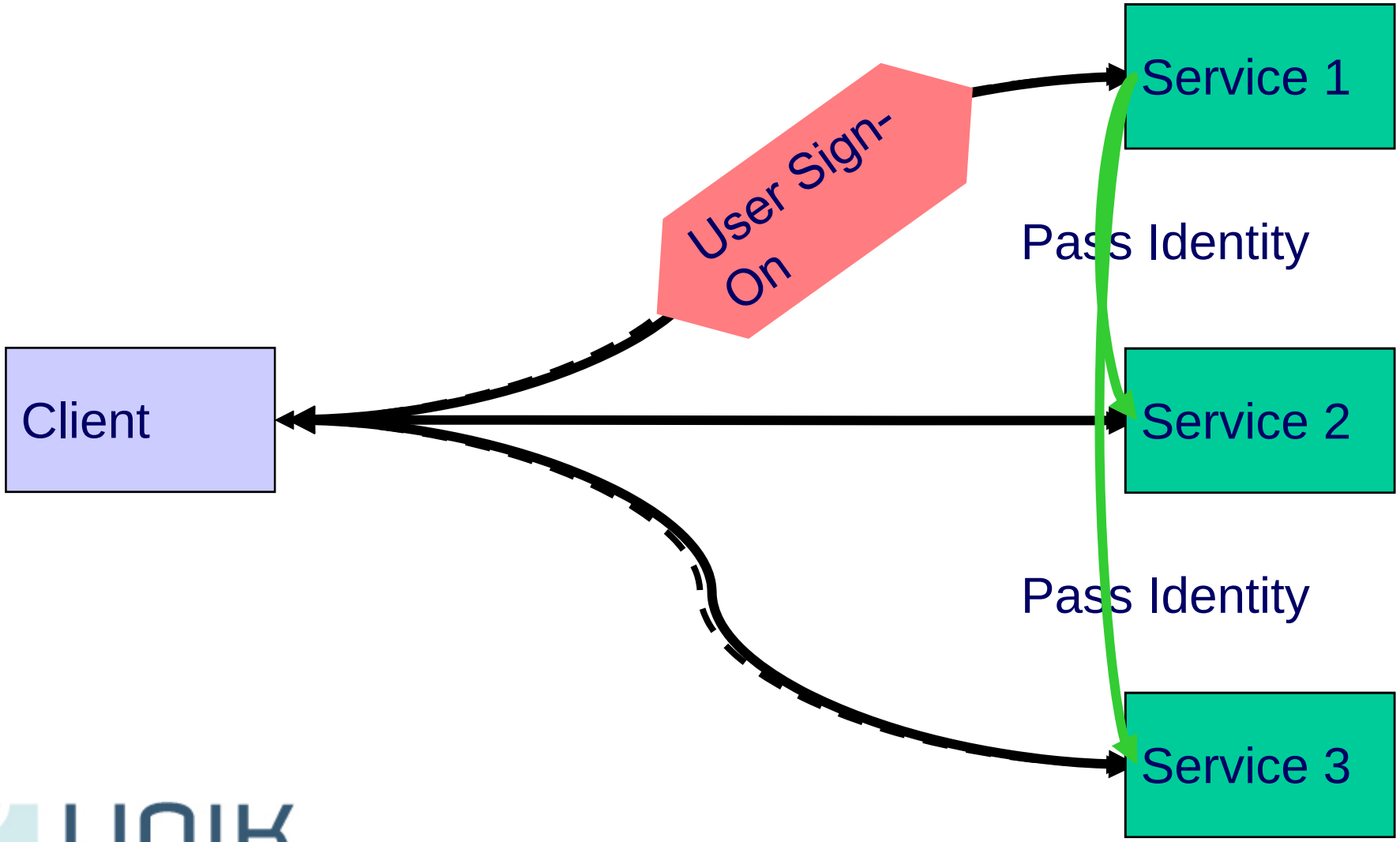
Push towards Single Sign-On

- 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

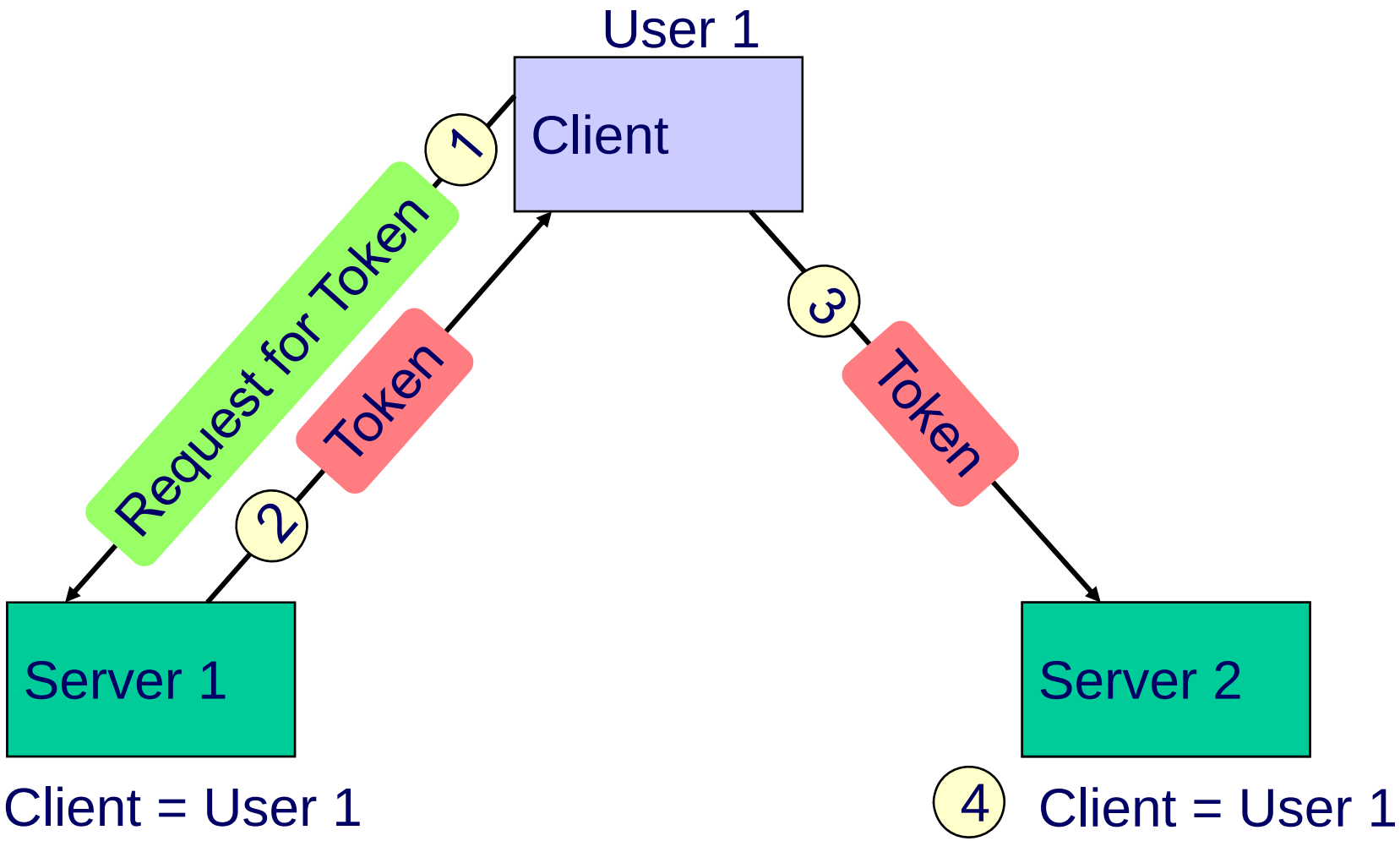
Multiple Sign-On to Multiple Servers



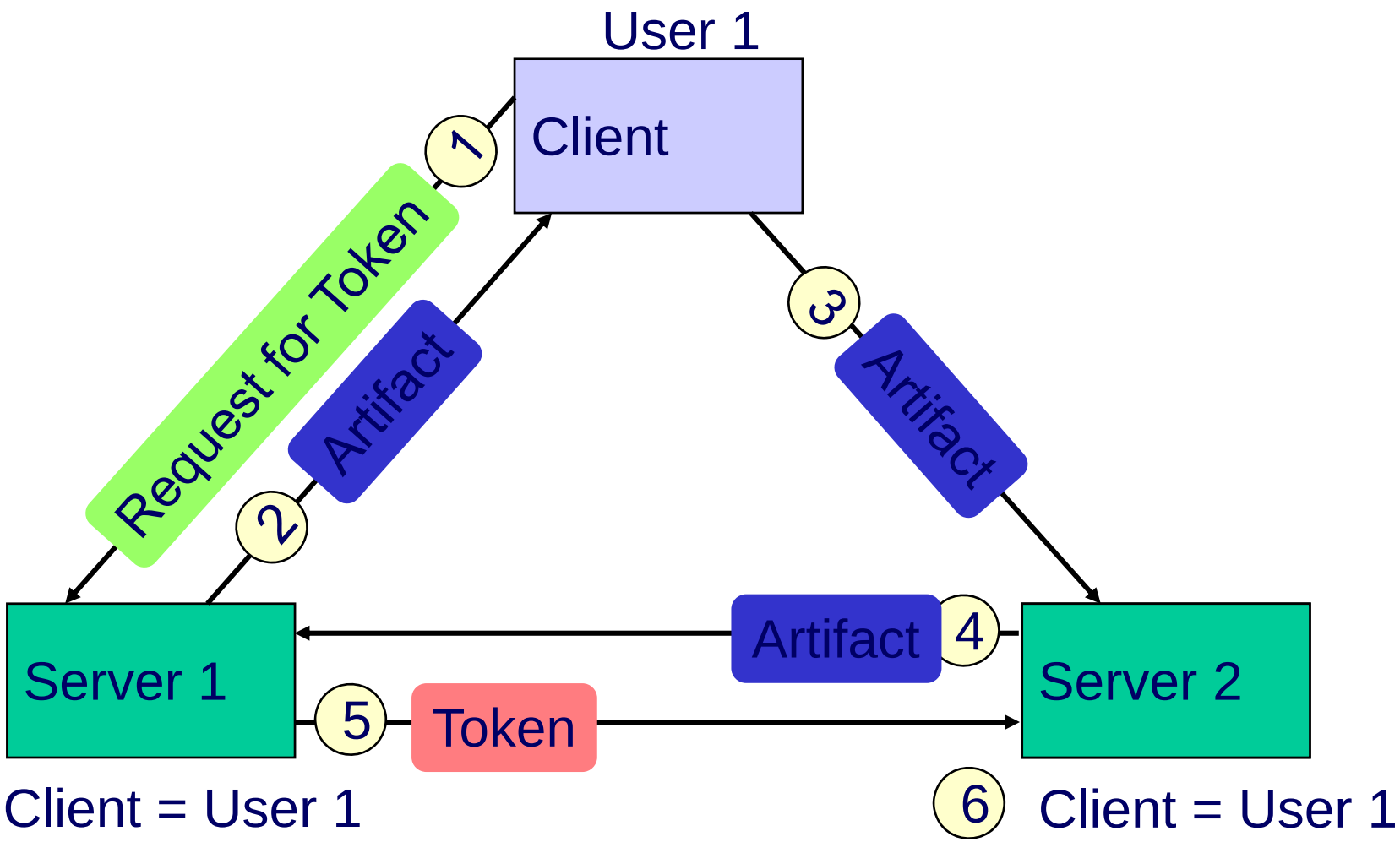
Single Sign-On to Multiple Servers



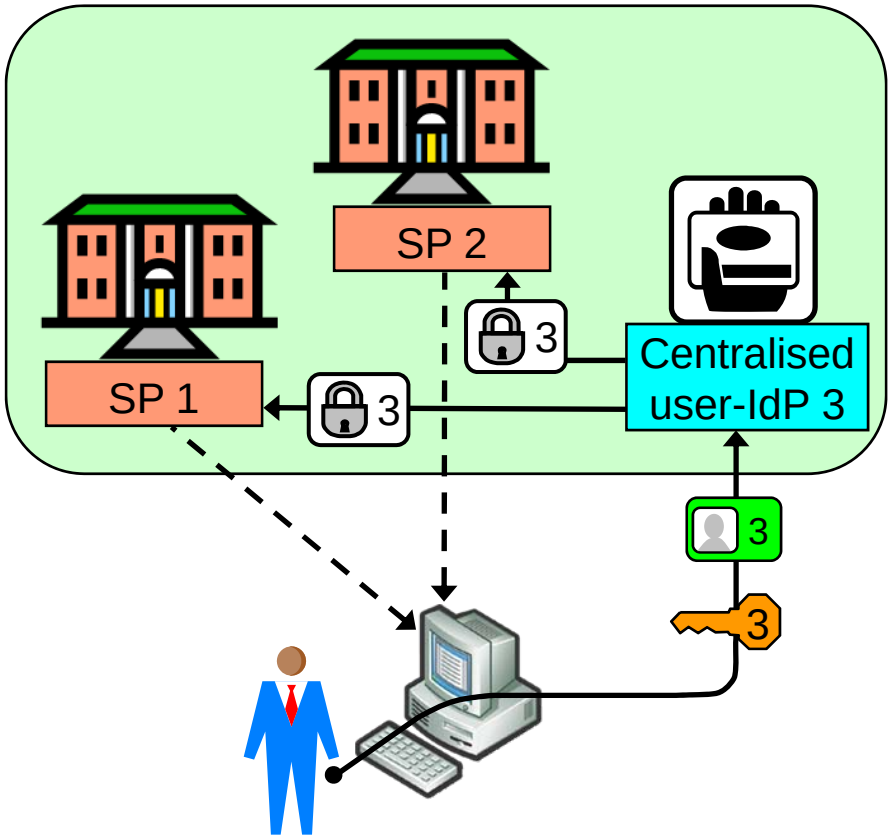
Token from Server 1 allows login at Server 2



Token exchanged over back-channel



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

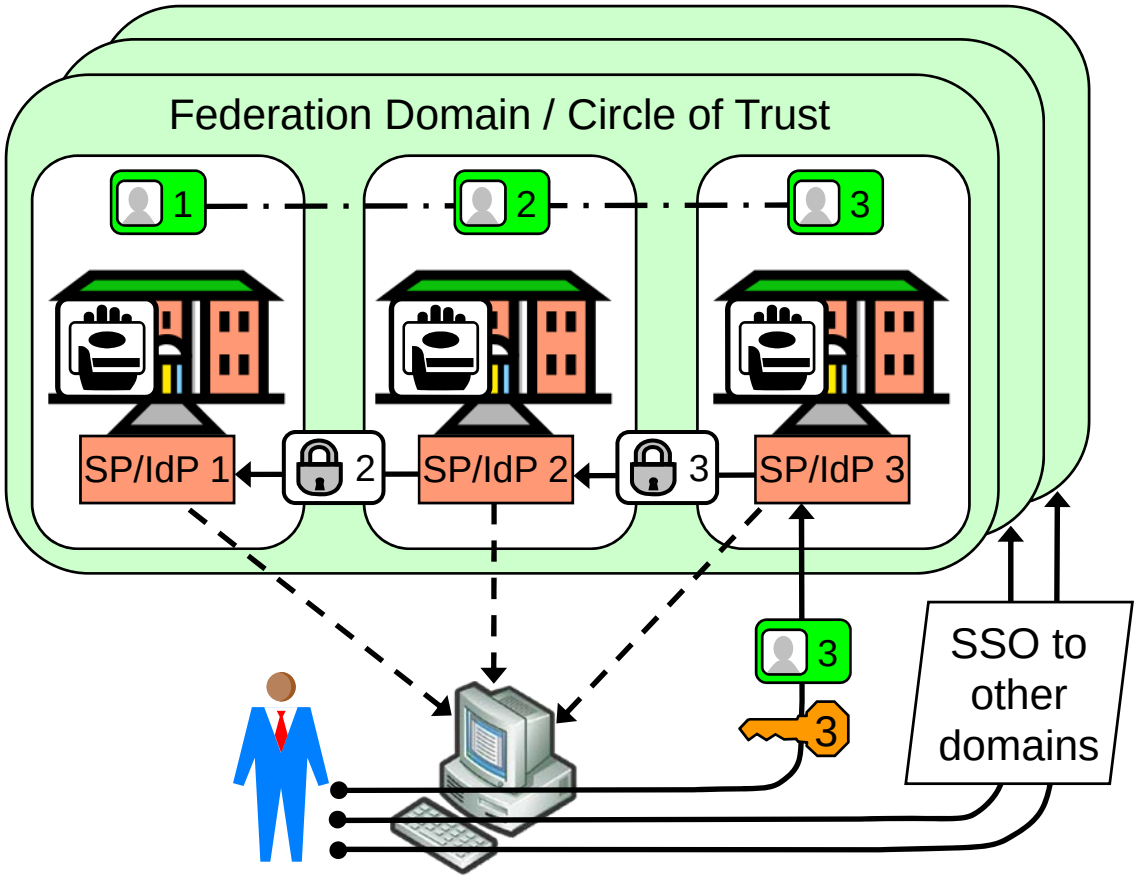
Service provision

Examples: Kerberos, .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

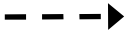

Identity domain


User identifier issued by IdP #


Authentication token managed by IdP #


Security assertion sent by IdP #


Service logon


Service provision

Identifier mapping

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

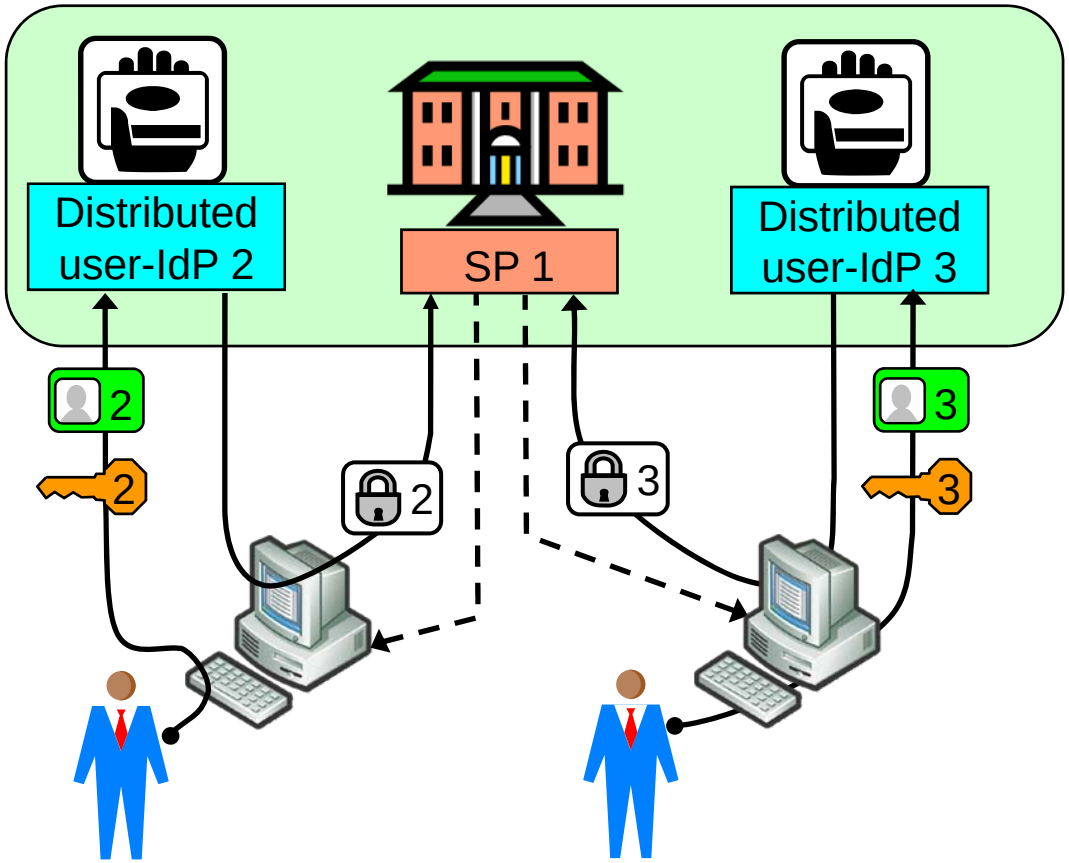
Federated SSO

- Advantages
  - Improved usability (theoretically)
  - Compatible with silo user-identity domains
  - Allows SPs to bundle services
  - Allows SPs to collect user information
- 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

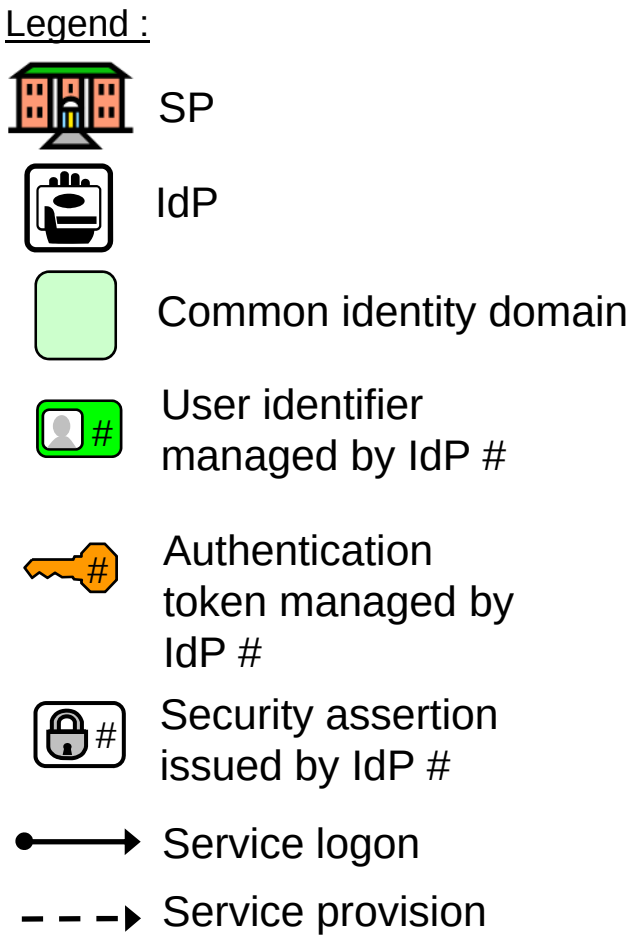
Standards for Federated SSO

- What are the “Standards”?
  - SAML (OASIS)
  - Liberty ID-FF (Liberty Alliance), merged with SAML2.0
  - WS-Federation (IBM, Microsoft)
- Standards based solutions make life easier
  - Multi-vendor interoperability
  - Reduced technology “lock-in”
  - Benefit from the experience of others

Common SSO identity model



Example: OpenID

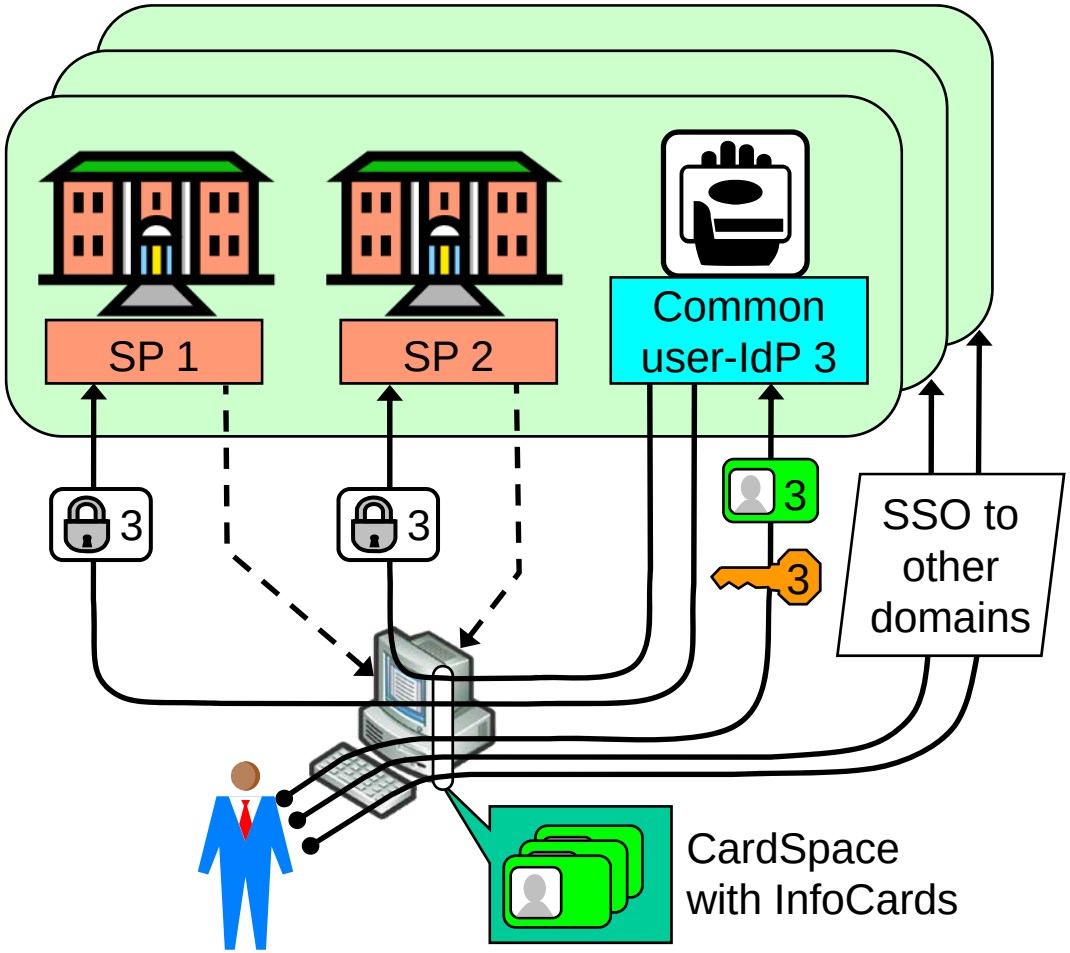


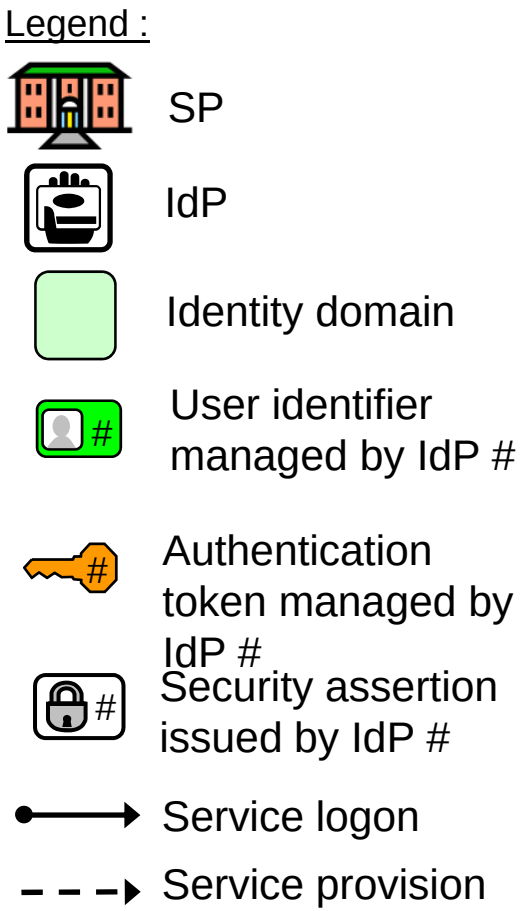
Common SSO identity model

- 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

Microsoft's InfoCard model





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

A closer look at 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

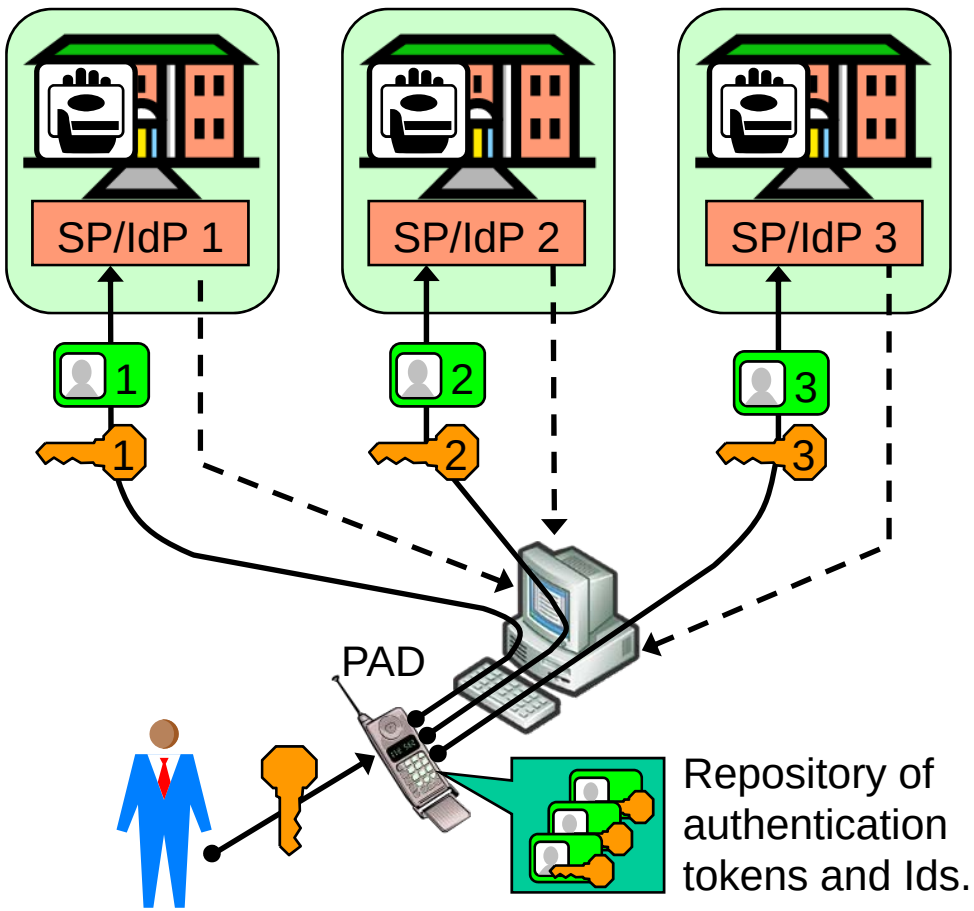
- Buzzword with positive connotation
- Seems to promise a solution to users' problems
  - Scaleability for the user
- Possible interpretations:
  - Any architecture that improves the user experience
  - Putting the users in control of their identities
  - Solutions that preserve privacy
  - SSO technology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

User centric SSO

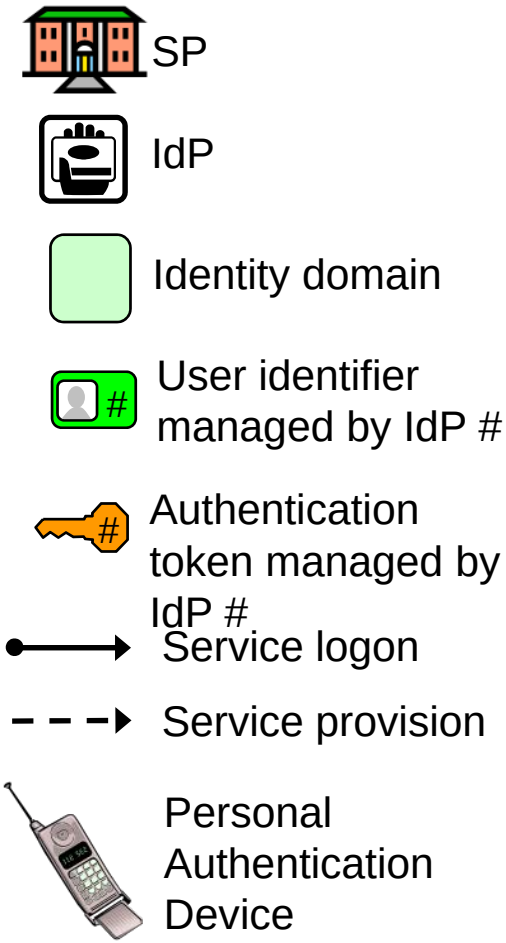
- User side technology for efficient management of identifiers and credentials
- Implementation
  - Software based
  - Hardware based: Personal Authentication Device (PAD)
- General purpose
- Assumed to be secure

Solves user side scalability problem

User Centric model

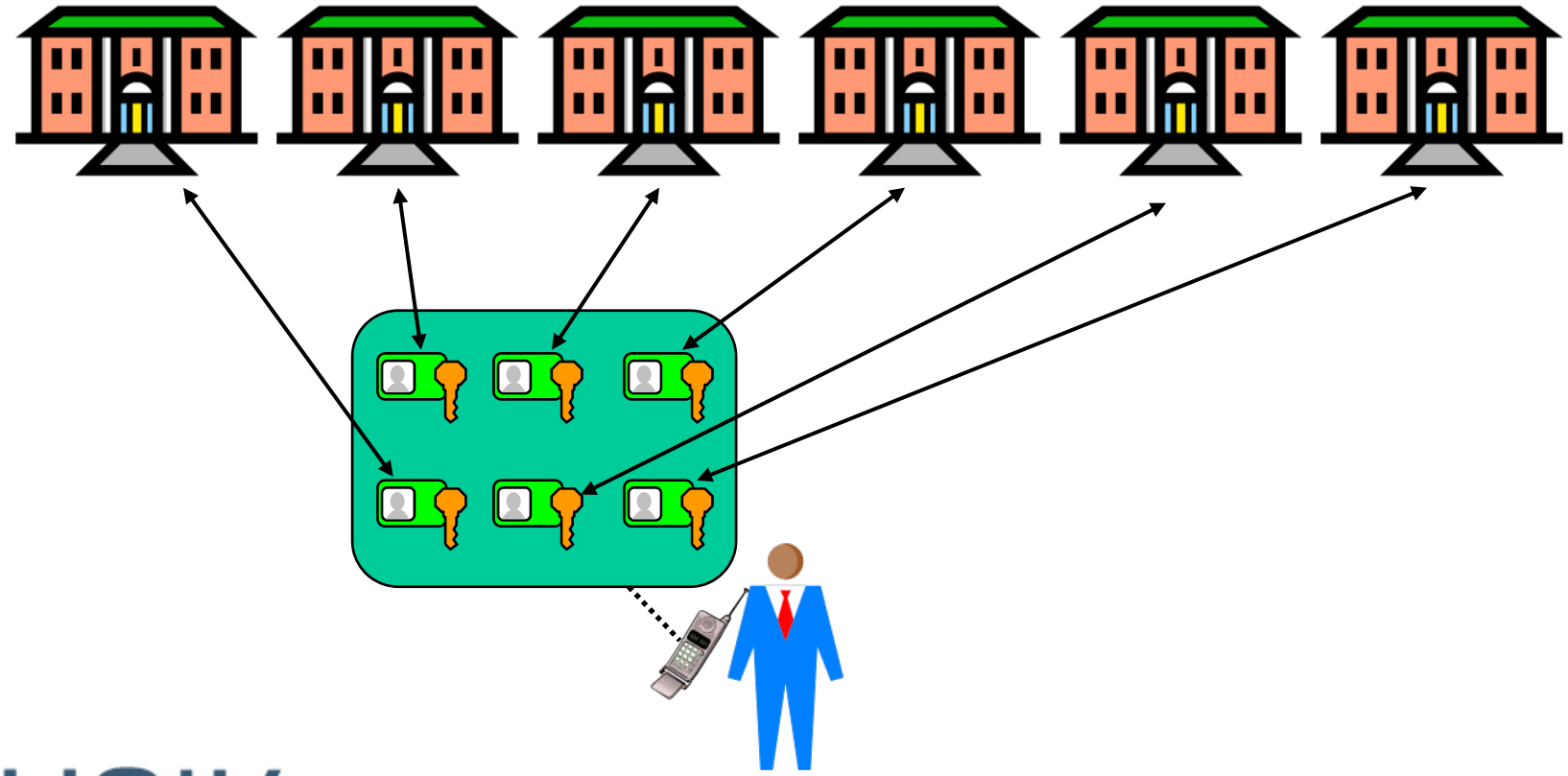


Legend:



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

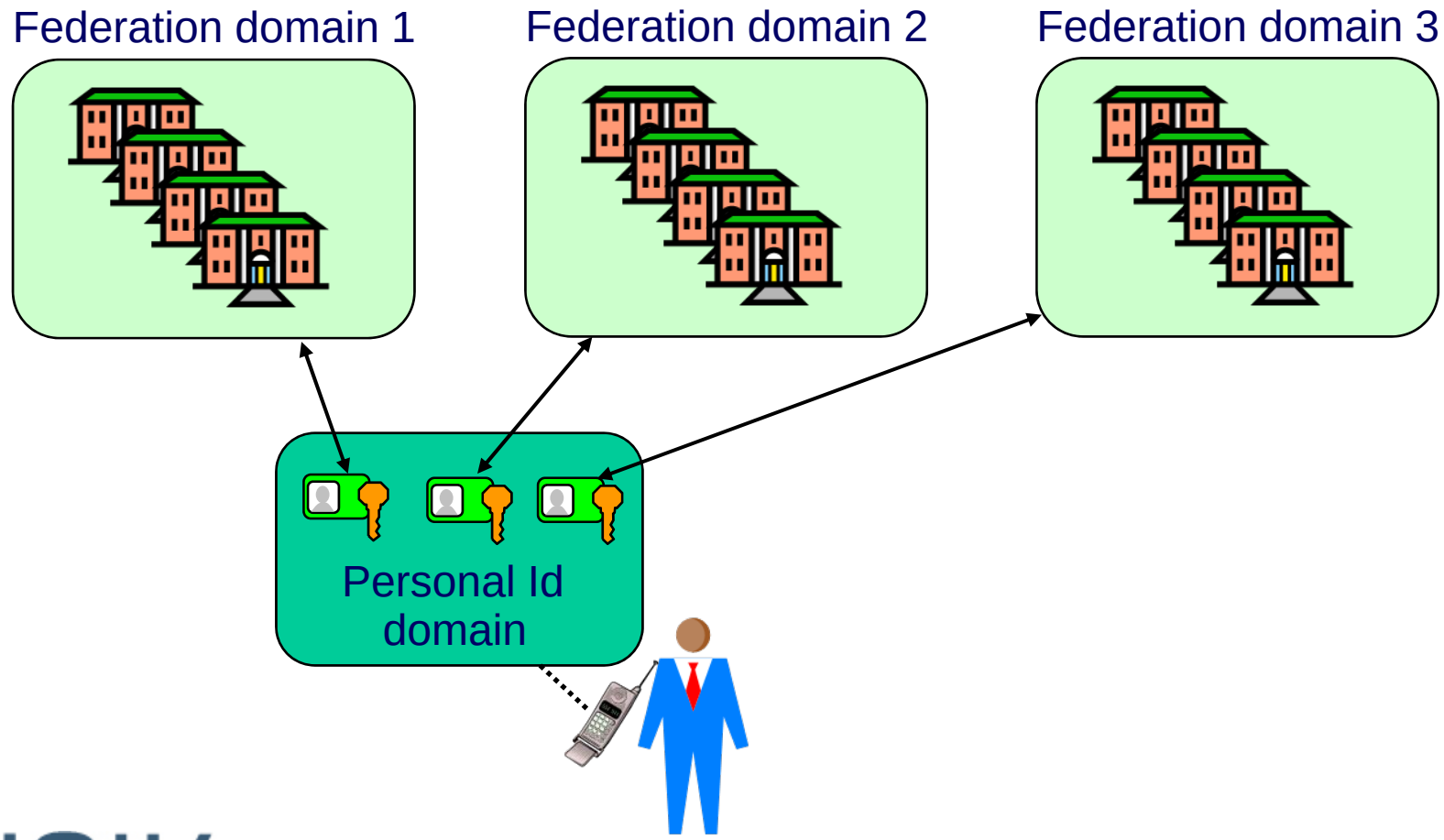
Combined Federated and User-Centric

- 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.

Federation technology resources

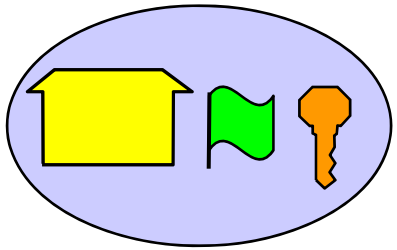
- Shibboleth
  - Open source software
  - http://shibboleth.internet2.edu/
- Liberty Alliance
  - Industry consortium
  - Provides specifications and white papers
  - http://www.projectliberty.org/
- SAML 2.0
  - OASIS XML format standards for exchanging authentication info
  - http://www.oasis-open.org/
- WS-Federation
  - IBM, Microsoft *et al.*
  - Specification based on the WS-Security roadmap (OASIS standards)
  - http://www-128.ibm.com/developerworks/library/specification/ws-fedworld/

Combining federated and user centric identity management

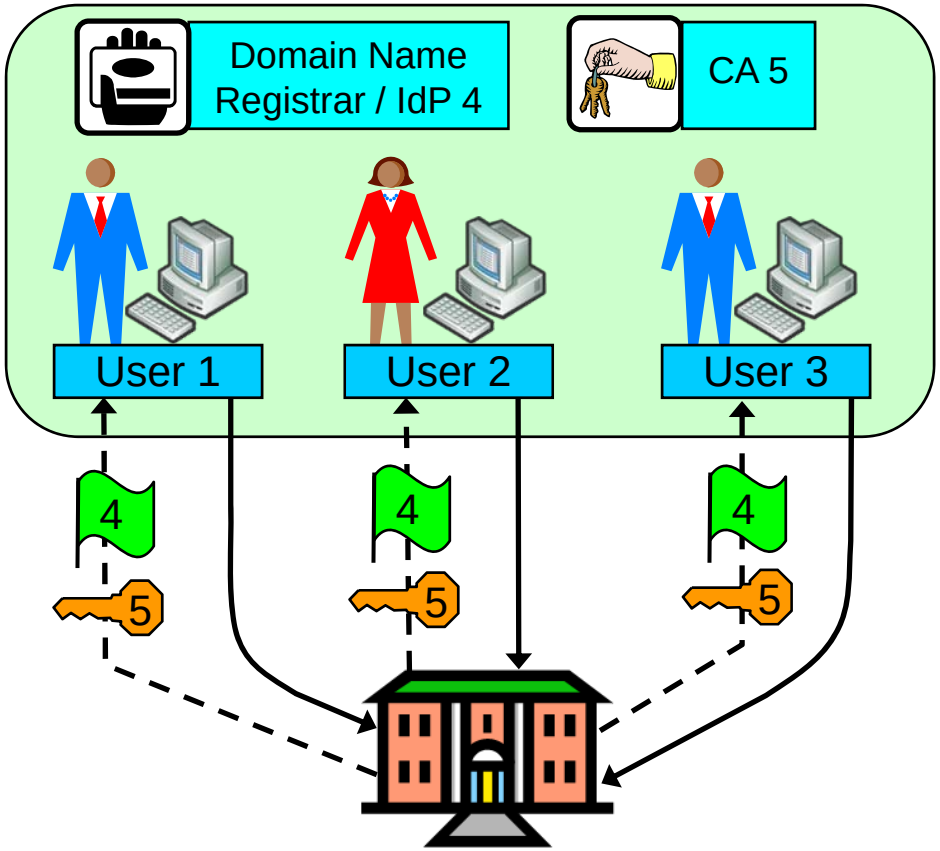


SP identity management

- 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:

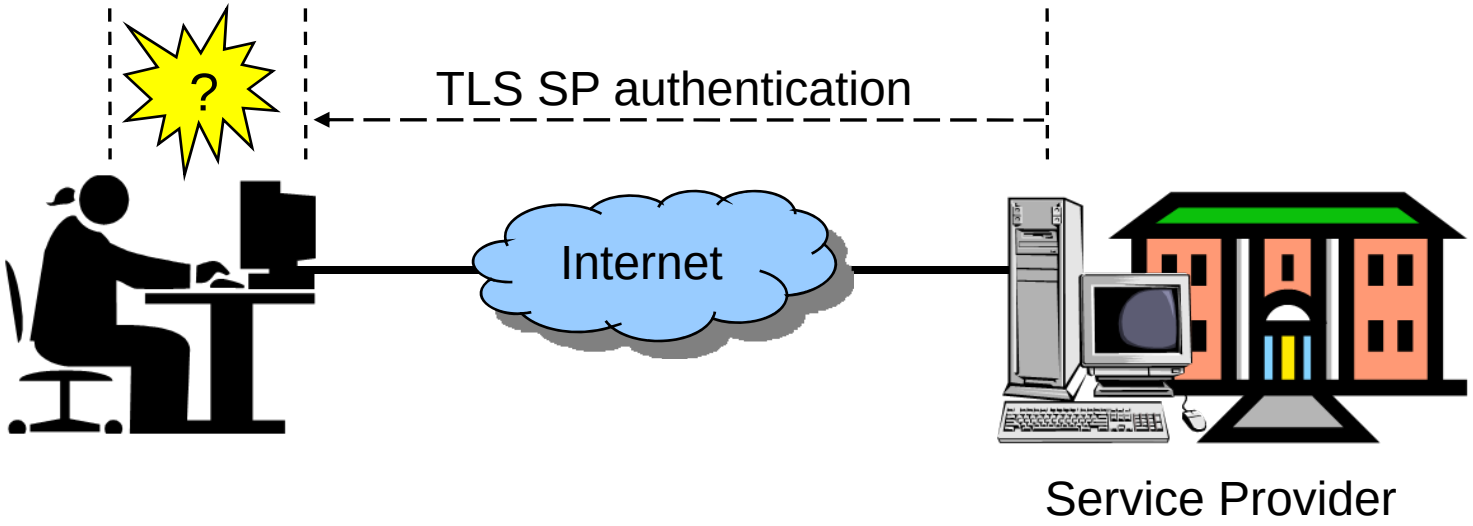
- SP Identity domain
- Domain name issued by IdP #
- SP entity
- Domain name registrar / IdP
- Certificate Authority
- Auth. token issued by CA #
- Service access
- SP authentication

Example: Browser PKI

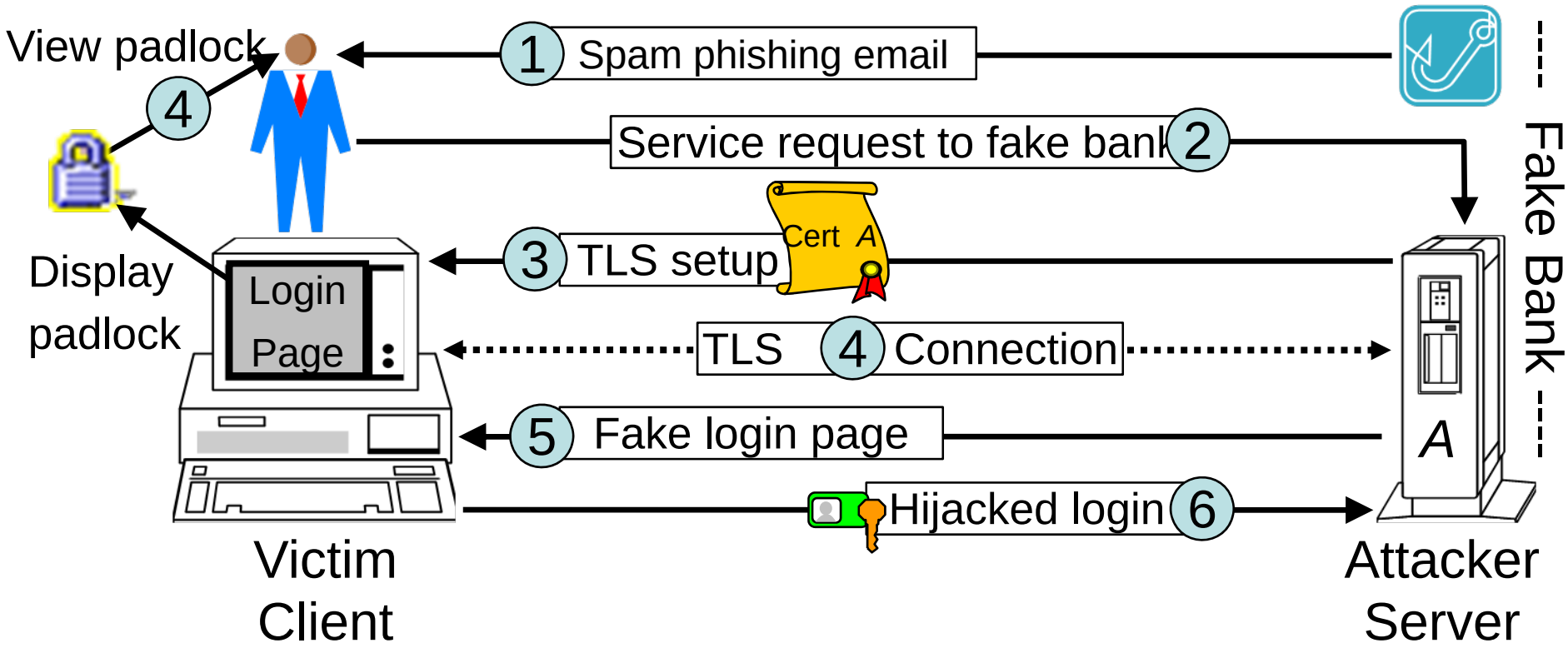
Common SP identity domain

- 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 SP authentication with SSL



Phishing and spoofing

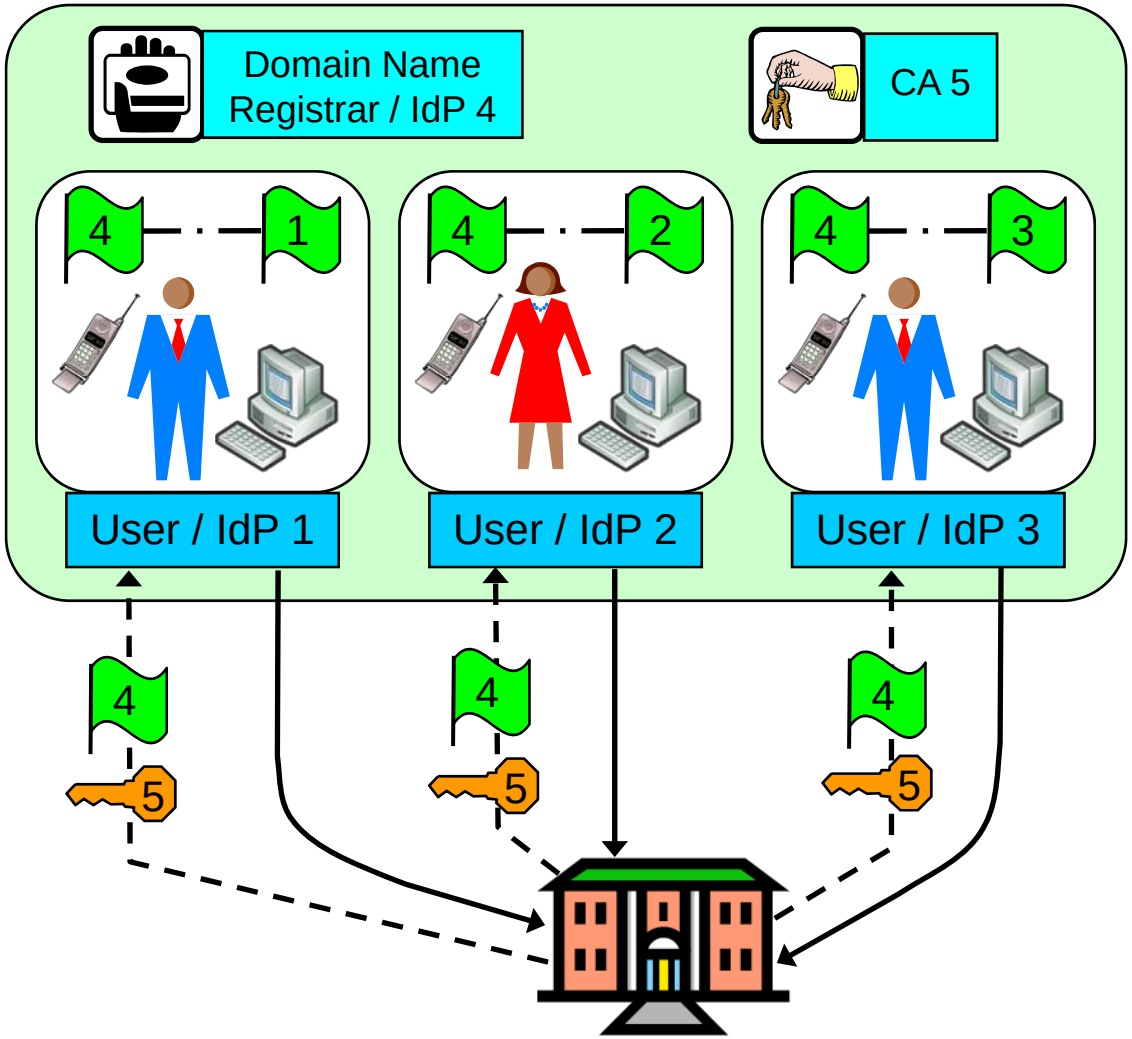


The great server certificate swindle

- 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 model



Legend :

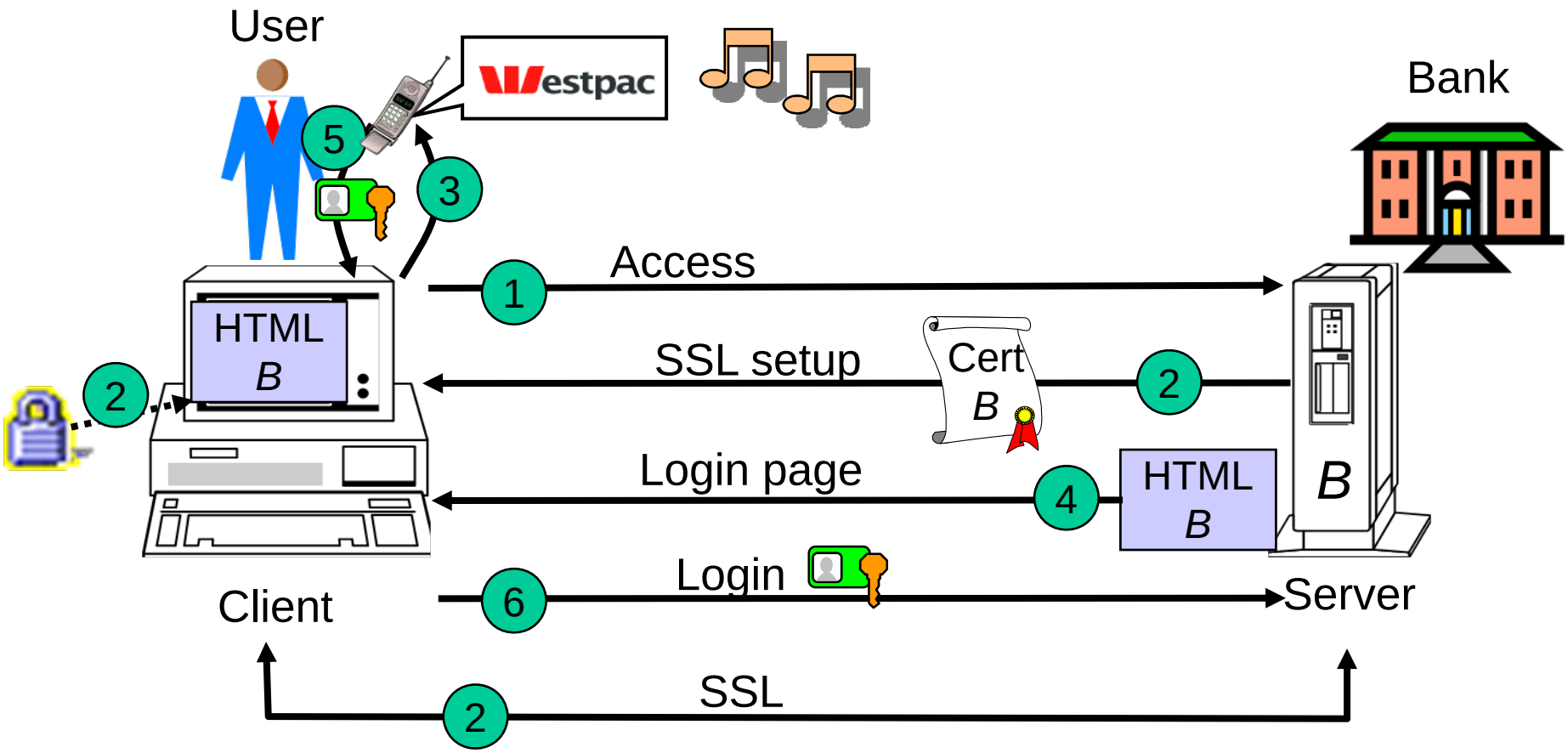
- SP Identity domain
- Domain name issued by IdP #
- PAD
- SP entity
- Domain name registrar / IdP
- CA
- Auth. token issued by CA #
- Service access
- SP authentication
- Identifier mapping

User-Centric 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

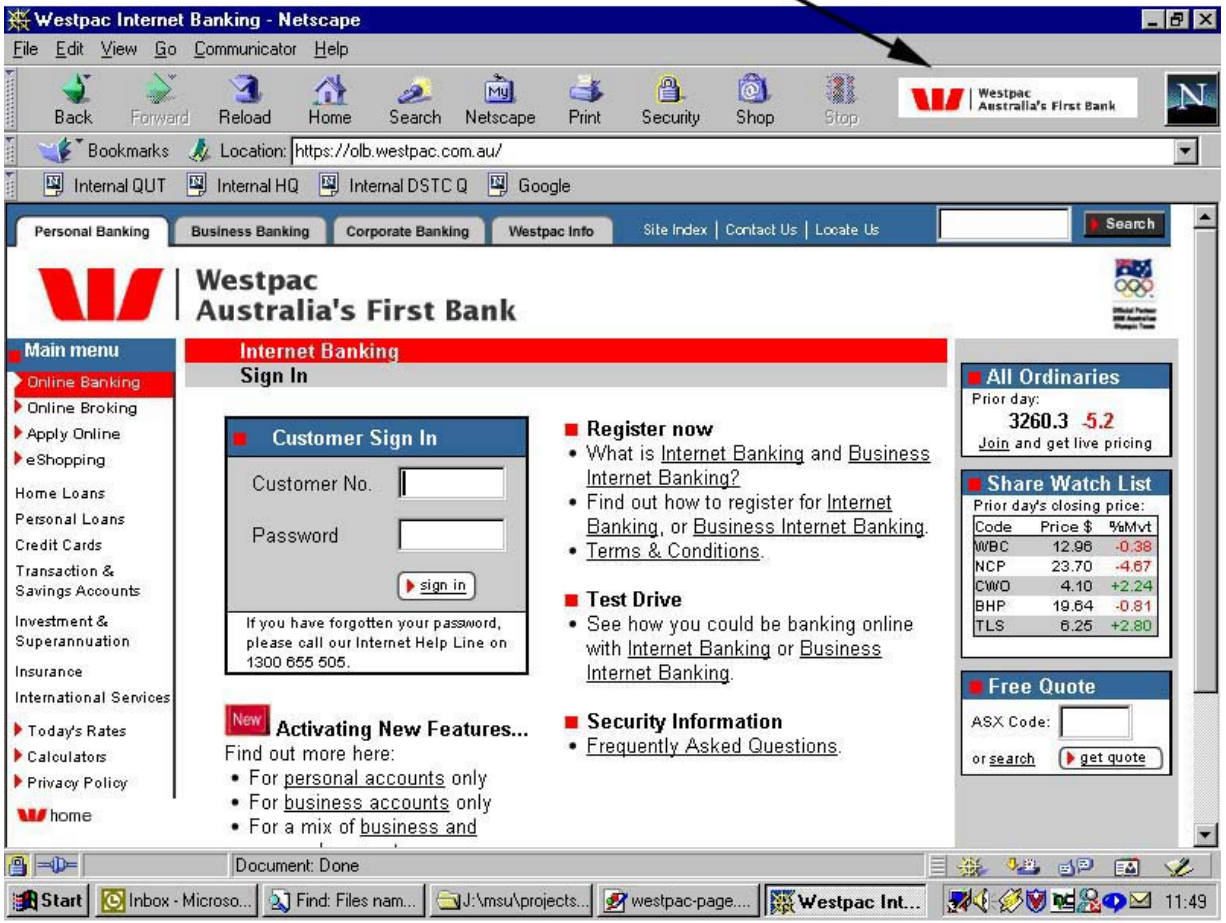


SP identity management

Principle of Mozilla TrustBar

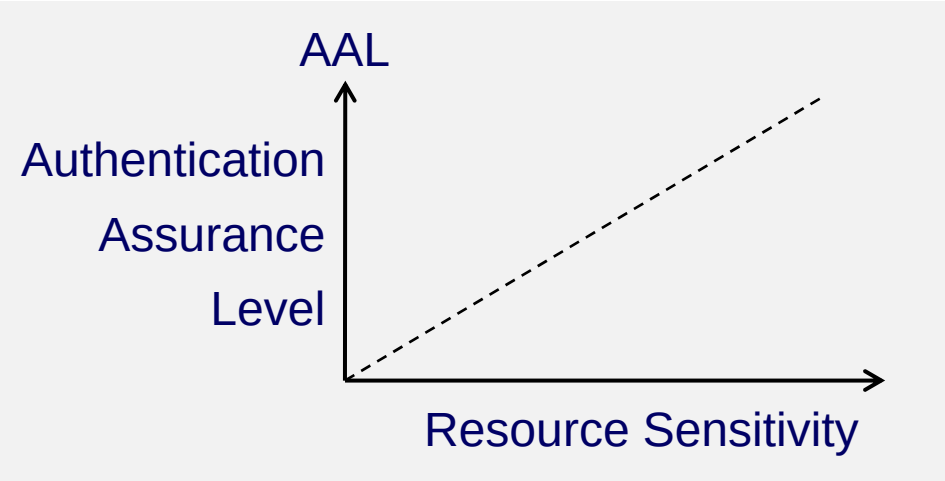
Personalised graphical logo and/or sound as site identifier

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

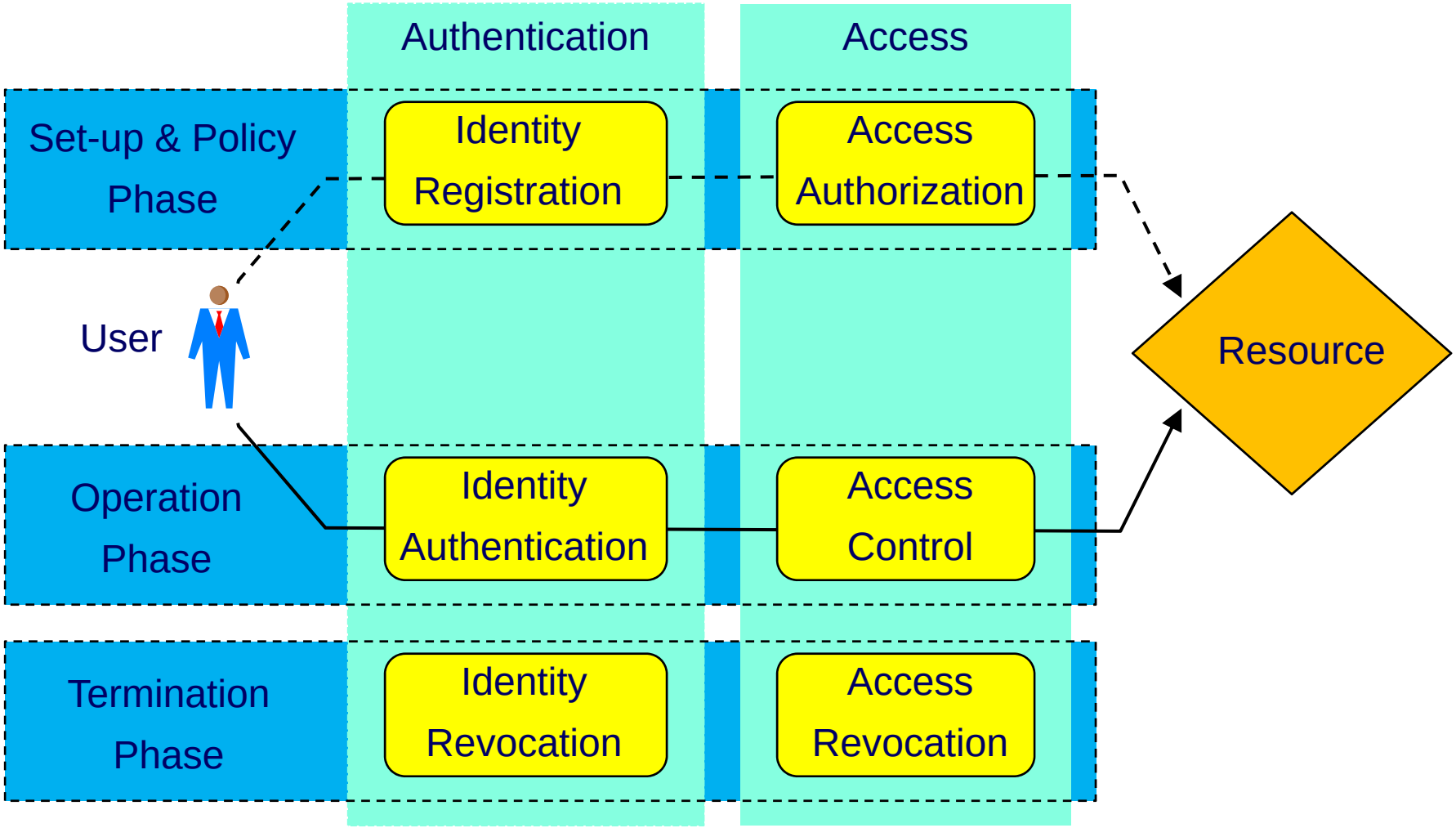


Authentication Assurance

- 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

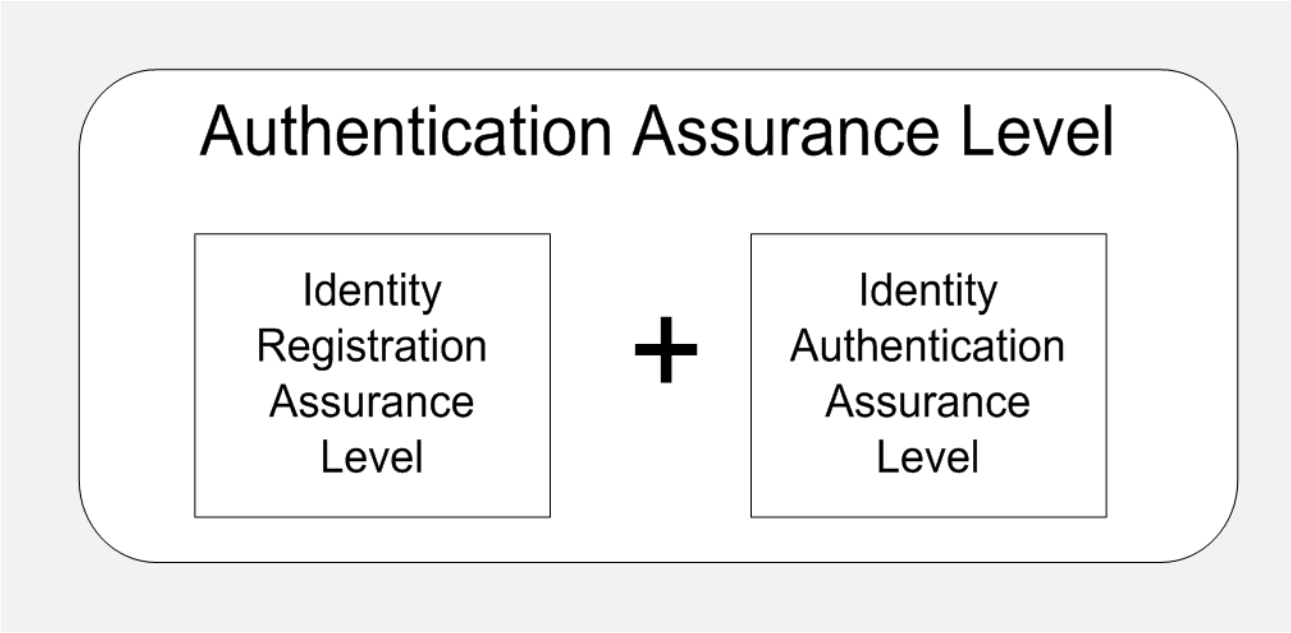


Authentication and Access



Authentication Assurance Level (AAL)

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



Identity Registration

- Pre-Authentication of new entity
  - Physical world credentials, e.g. driver licence, passport, utility bills etc.
- Registration of new identity
  - Assigning new unique identifier
  - Registration of identity details
- Issuing authentication credentials
  - Password, access cards, hardware tokens etc.

Identity Authentication

- User actions:
  - Claim identity by presenting unique identifier
  - Provide credentials
- System action:
  - Verify that credentials correspond to claimed identity
  - Login/reject the user depending on verification result

Queensland Government Authentication Framework

Define business requirements and sensitivity/risk levels

↓

Determine Authentication Assurance Level

↓

Determine Identity Registration Assurance Level

↓

Determine Identity Authentication Assurance Level

↓

Implement registration and authentication mechanisms

QGAF AAL Scale

Authentication Assurance Level (AAL)				
Level 0	**Level 1**	**Level 2**	**Level 3**	**Level 4**
No Assurance	Minimal Assurance	Low Assurance	Moderate Assurance	High Assurance
No confidence is required in the client's identity	Minimal confidence is required in the client's identity	Low confidence is required in the client's identity	Moderate confidence is required in the client's identity	High confidence is required in the client's identity

Source: Queensland Government Authentication Framework

From Classification Level to AAL

Highest Information Security Classification Level				
Public	Unclassified	In Confidence	Protected	Highly Protected
↓	↓	↓	↓	↓
AAL-0	AAL-1	AAL-2	AAL-3	AAL-4
Authentication Assurance Level (AAL)				

Source: Queensland Government Authentication Framework

From Impact of Authentication Failure to AAL

- Resources are not only information
  - Classification level of resources not always meaningful
- AAL can be determined as a function of the risk of authentication failure
- Authentication failure = false positive

- Authentication Risk = Impact Severity * Probability

Determining Impact Severity

IMPACT Type	Severity Lowest				Highest
	None	Minimal	Minor	Moderate	Substantial
	↓	↓	↓	↓	↓
Risk to any party's safety	None			Any risk to personal safety	Threaten life directly
Distress caused to any party	None		Minor - Short term distress	Limited long term distress	Substantial long term distress
Damage to any party's standing or reputation	None		Minor - Short term damage	Limited long term damage	Substantial long term damage
Inconvenience to any party	None	Minimal inconvenience	Minor inconvenience	Significant inconvenience	Substantial inconvenience

Source: Queensland Government Authentication Framework (extract)

Impact Probability

Probability Rating	Definition	Guideline Percentage
Almost Certain	It is almost certain that an impact will occur from a failure in authentication	**95-100%**
Likely	It is likely that an impact will occur from a failure in authentication.	**50-95%**
Possible	It is possible that an impact will occur from a failure in authentication.	**10-49%**
Unlikely	It is unlikely that an impact will occur from a failure in authentication.	**1-9%**
Rare	It would be rare that an impact will occur from a failure in authentication.	**<1%**

Source: Queensland Government Authentication Framework

Determining Authentication Risk

		Impact Severity				
		None	**Minimal**	**Minor**	**Moderate**	**Substantial**
Probability	**Almost Certain**	Negligible	Minimal	Low	Moderate	High
	Likely	Negligible	Minimal	Low	Moderate	High
	Possible	Negligible	Minimal	Low	Moderate	High
	Unlikely	Negligible	Minimal	Minimal	Low	Moderate
	Rare	Negligible	Minimal	Minimal	Low	Moderate

Source: Queensland Government Authentication Framework

From Authentication Risk to AAL

Authentication Risk Level				
Negligible	Minimal	Low	Moderate	High
↓	↓	↓	↓	↓
AAL-0	AAL-1	AAL-2	AAL-3	AAL-4
Authentication Assurance Level				

Source: Queensland Government Authentication Framework

Types of identity registration

- No registration
  - Service will not remember user in future access
- Automatic registration
  - Using anonymous system data, e.g. cookies
- Self registration without proof of identity
  - Using real name
  - Using false name or pseudonym
- Registration with proof of identity
  - Using real or easily traceable name
  - Using escrow pseudonym

IRAL Properties

Identity Registration Assurance Level (IRAL)	Client Anonymity Maintained	Allows Contactability and Service History and Personalisation	Real World Identity link, service delivery non-repudiation	Supports overall AAL > 2	Supports Non-repudiation of registration
IRAL-4 High	No	Yes	Yes	Yes	Yes
IRAL-3 Moderate	No	Yes	Yes	Yes	No
IRAL-2 Low / Basic	No	Yes	Yes	No	No
IRAL-1 Pseudonymous or Self Registered	Yes by Pseudonym	Yes	No	No	No
IRAL-0 No registration	Yes	No	No	No	No

Source: Queensland Government Authentication Framework

Identity Authentication Assurance Levels

Identity Authentication Assurance Level	Confidence Provided	Description
IAAL-4	**High confidence**	The highest practical authentication assurance is required. Strong cryptographic authentication mechanisms must be used and authentication will require at least two factors.
IAAL-3	**Moderate confidence**	A moderate level of confidence in the authentication mechanism is required. Strong cryptographic authentication mechanisms must be used. Generally speaking this level of authentication will require two factors.
IAAL-2	**Low confidence**	A low level of confidence in the authentication mechanism is required. The mechanism needs to prevent common forms of attack, such as: eavesdropper, replay, and online guessing attacks. For example, a password over an encrypted link. However, strong cryptographic authentication is not mandatory.
IAAL-1	**Minimal confidence**	Authentication is performed, but there is little assurance placed upon it. For example, a challenge-response password mechanism.
IAAL-0	**No confidence**	No authentication is performed. Included for completeness only, but does not represent any authentication process.

Source: Queensland Government Authentication Framework

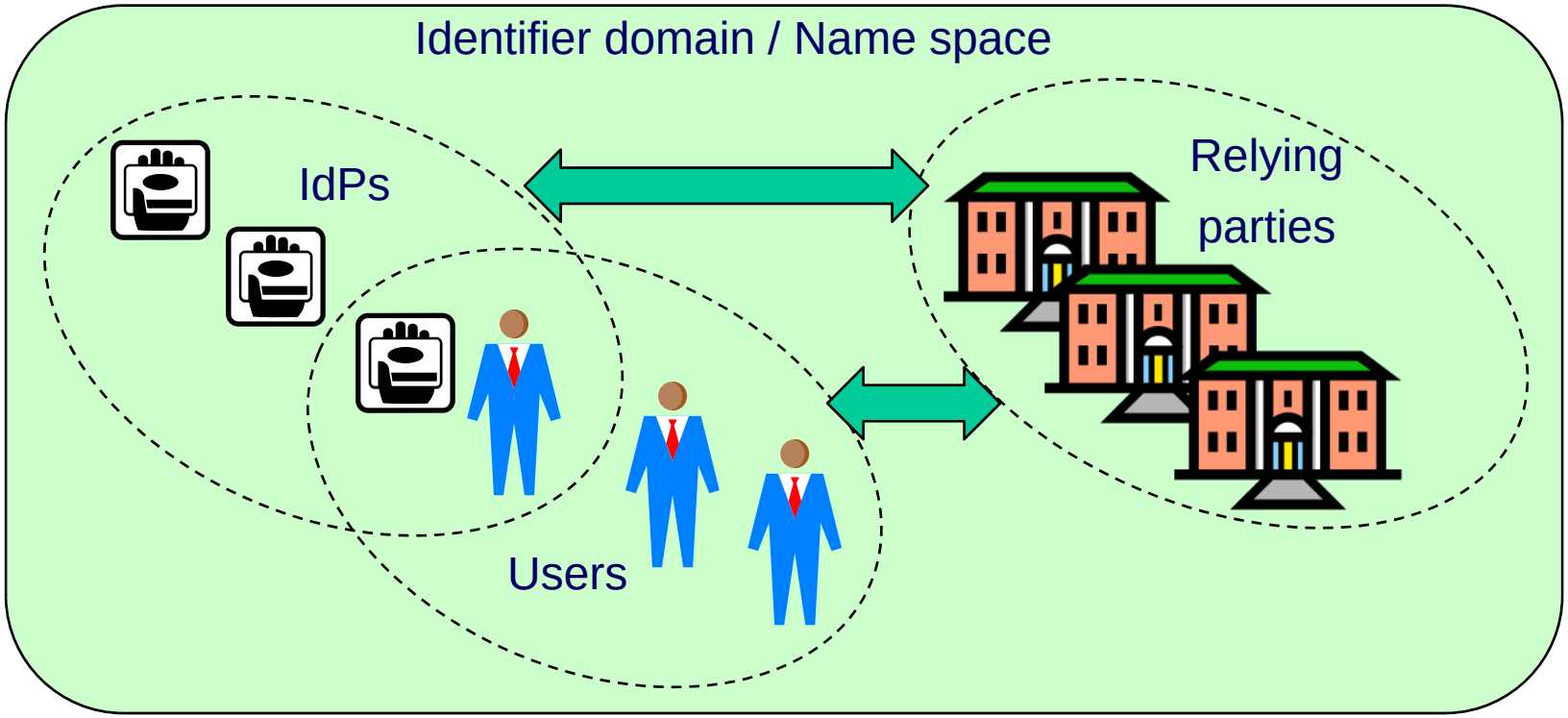
Determining IAAL from AAL and IRAL

	Required Authentication Assurance Level				
Registration Assurance Level	AAL-0 None	AAL-1 Minimal	AAL-2 Low	AAL-3 Moderate	AAL-4 High
IRAL-0 - None	IAAL-0	N/A	N/A	N/A	N/A
IRAL-1 - Minimal	IAAL-0 (1)	IAAL-1	(IAAL-3)	(IAAL-4)	N/A
IRAL-2 - Low	IAAL-0 (1)	IAAL-1	IAAL-2	N/A	N/A
IRAL-3 - Moderate	IAAL-0 (1)	IAAL-1	IAAL-2	IAAL-3	N/A
IRAL-4 - High	IAAL-0 (1)	IAAL-1	IAAL- 2	IAAL-3	IAAL-4

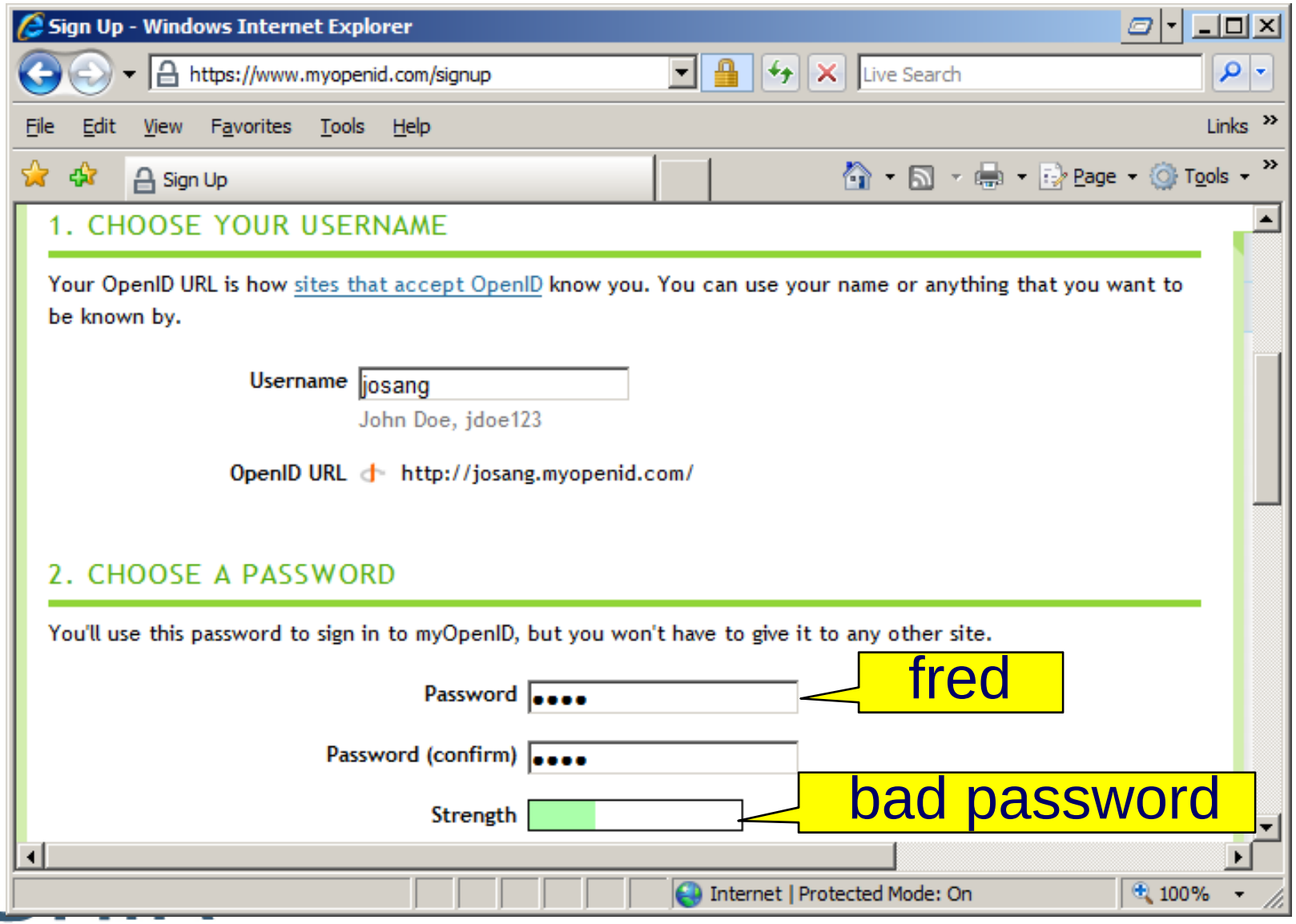
Source: Queensland Government Authentication Framework

The OpenID common SSO model

- Common name space
- Distributed IdPs
- No authorities



OpenID self registration



Service Access Without Password

reviewsby.us - Windows Internet Explorer

http://reviewsby.us/login

File Edit View Favorites Tools Help

reviewsby.us

Login

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

username:

password:

sign in

Open Id sign-in

OpenID josang.myopenid.com

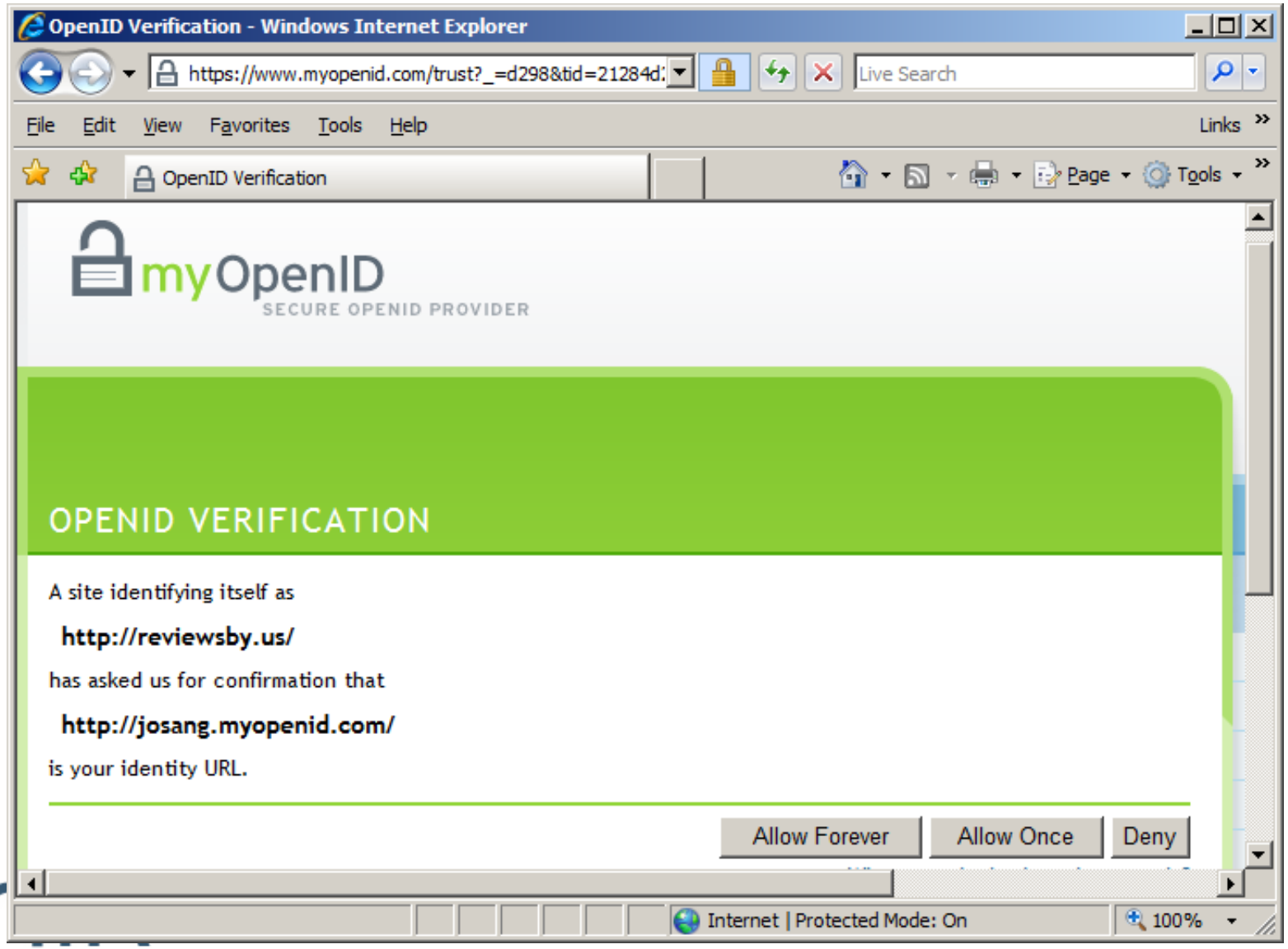
authenticate

Latest restaurants

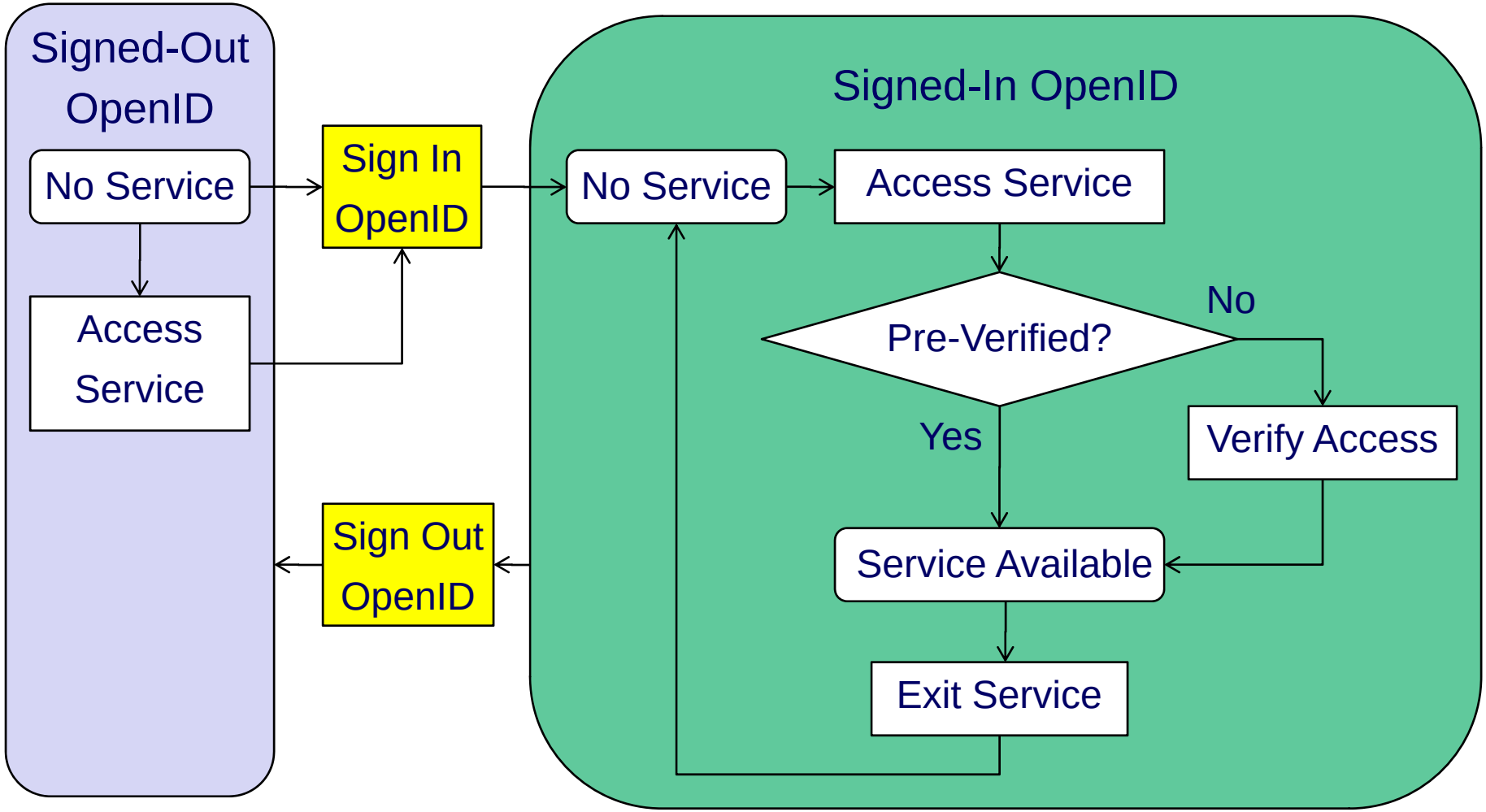
Internet | Protected Mode: On

100%

First Time Sevice Access



OpenID flow chart (user perspective)



OpenID Association Protocol
Relying Party ↔ ID Server

Relying Party R | ID Server S

Choose random x

$$\boxed{p, g, X := g^x}$$

Choose random y, k

$$\boxed{h, t, Y := g^y, K := \mathrm{H}(g^{xy}) \oplus k}$$

$$g^{xy} := X^y$$

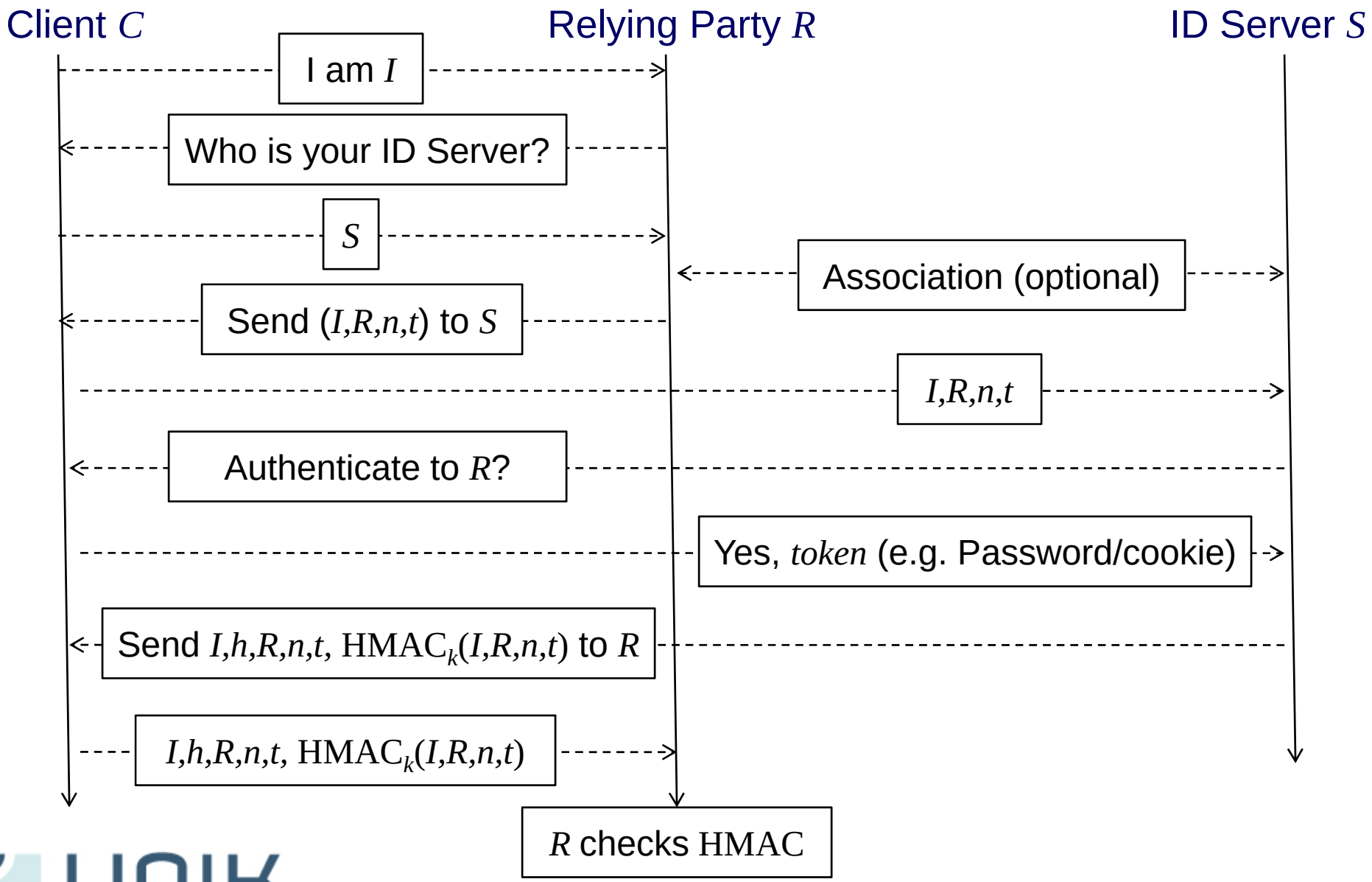
$$g^{xy} := X^y$$

$$k := \mathrm{H}(g^{xy}) \oplus K$$

Conclusion: R and S share key k

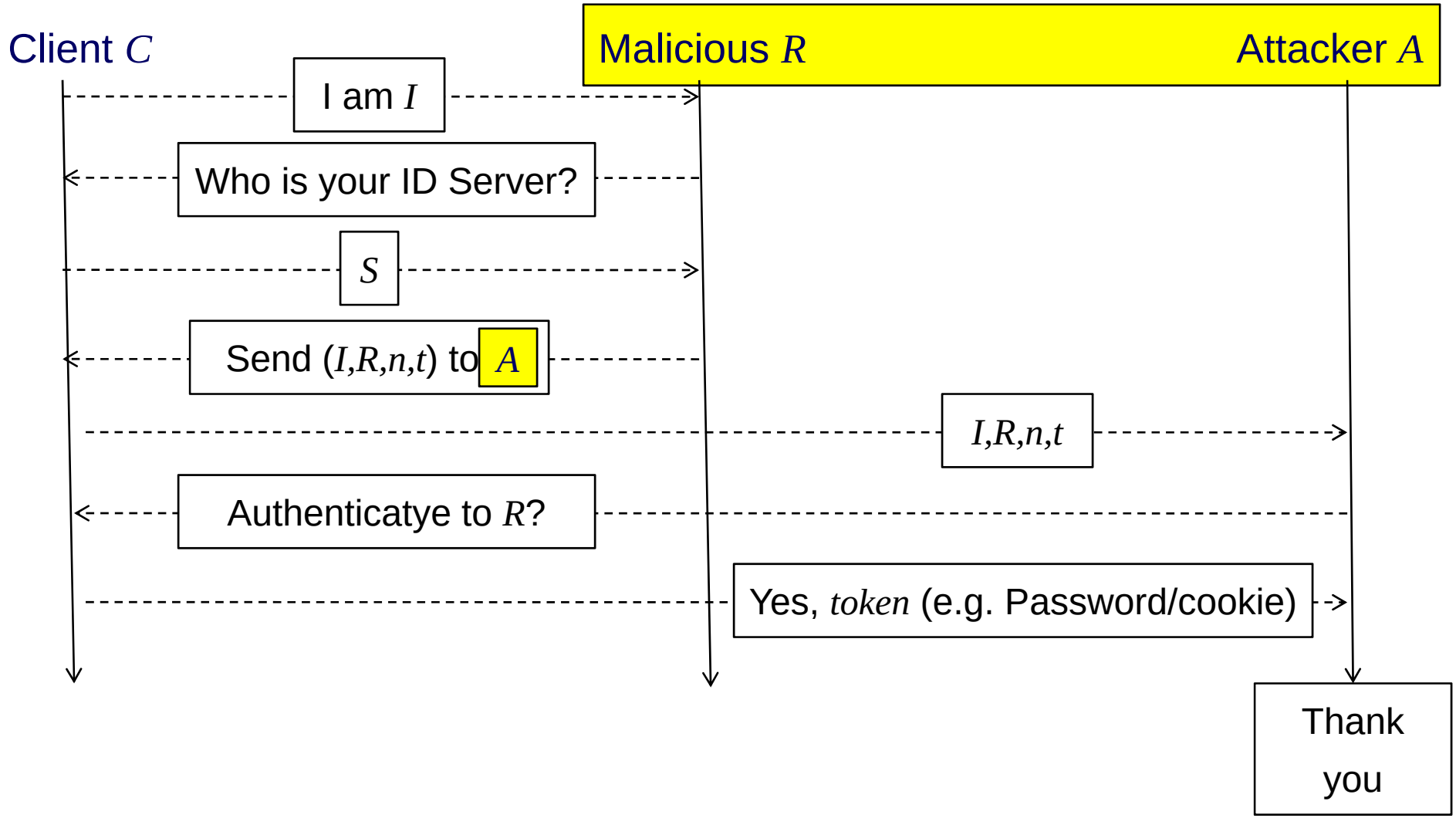
	Legend		
p	Diffie-Hellman prime	x, y	Private keys of R and S
g	Diffie-Hellman generator	X, Y	Public keys of R and S
h	Session handle	t	Validity time
K	Encrypted session MAC key	k	Shared session key
I	User OpenID	R, S	Reling party and ID Server

OpenID Protocol



UNIK UNIVERSITY GRADUATE CENTER

OpenID Phishing Protocol



Things You Can Do With OpenID

reviewsby.us - Windows Internet Explorer

http://reviewsby.us/

File Edit View Favorites Tools Help

reviewsby.us

welcome josang.myopenid.com

logout | add restaurant | search

=)

reviews of dishes and restaurants by you and me

Restaurants // Freshest

near Anywhere

Firehouse Subs
176 Tom Hill Sr Blvd,
Macon, GA, 31210-1814

Fuki Sushi
4119 El Camino Real,
Palo Alto, CA, 94306

Chicken Pasta Salad with poppy seeds
Gigi's Cafe

I don't remember what this was called, but it was a pasta salad with chicken, grapes, and poppy seeds.

Tags // Restaurants

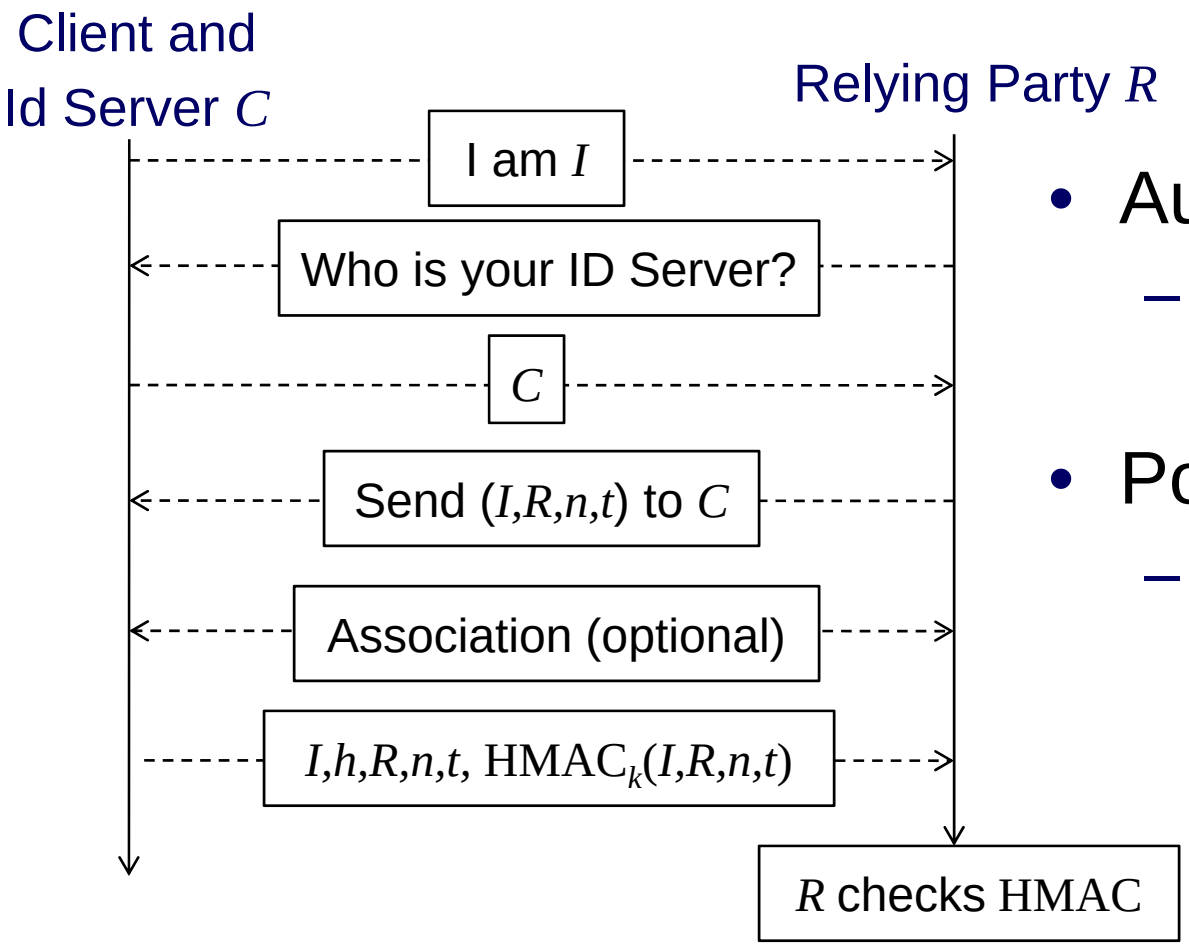
affordable asian bakery bar breakfast cafe chain cheap cheese chicken chinese coffee cute dessert espresso familyowned fastfood fish indian italian japanese mexican middleeastern oregon pizza quick salad sandwich sandwiches seafood

Done | Internet | Protected Mode: On | 100%

OpenID Characteristics

- Self registration
- ID Providers are not ”authorities”
- You can be your own ID Provider and Server
  - Personal SSO, see next slide
- Only supports AAL-1
- Not suitable for sensitive services
- Targets online services with AAL-1
- Open to abuse
- Attack multiplication factor when using OpenID is problematic

Personal SSO with the OpenID protocol



- Authentication farce
  - Asks me if I am me
- Possible prevention
  - Use of XRI requires approved IdPs

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)

Identity management security problems

- People are the weakest link
- Poor security usability creates vulnerabilities
- Main security problems are usability problems
- Password fatigue leads to password re-use
- SSO aimed at improving usability, but
  - System complexity
  - Privacy threats
  - Requires trust between many parties

Kerckhoffs' security principles (1883)

1. The system must be substantially, if not mathematically, undecipherable;
2. The system must not require secrecy and can be stolen by the enemy without causing trouble;
3. It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants;
4. The system ought to be compatible with telegraph communication;
5. The system must be portable, and its use must not require more than one person;
6. Finally, regarding the circumstances in which such a system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.

Security actions and conclusions

- A ***security action*** is when users are required to produce information and security tokens, or to trigger some security relevant mechanism.
  - For example, typing and submitting a password is a security action.
- A ***security conclusion*** is when users observe and assess security relevant evidence in order to derive the security state of systems.
  - For example, observing a closed padlock on a browser, and concluding that the communication is protected by TLS is a security conclusion.

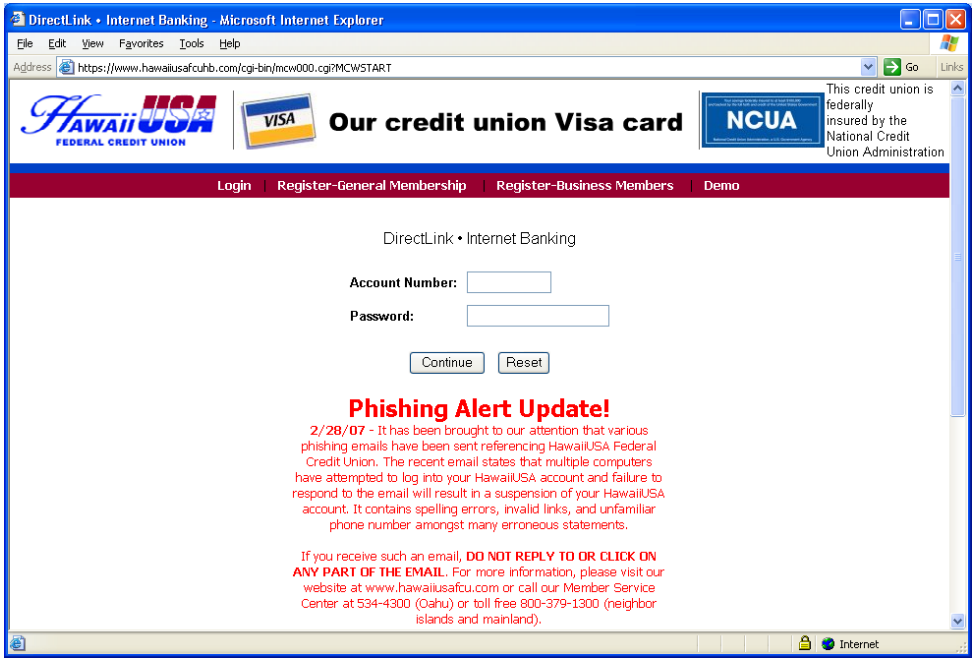
Security <u>action</u> usability principles

1. Users must understand which security actions are required of them.
2. Users must have sufficient knowledge and the ability to take the correct security action.
3. The mental and physical load of a security action must be tolerable.
4. The mental and physical load of making repeated security actions for any practical number of instances must be tolerable.

Security <u>conclusion</u> usability principles

1. Users must understand the security conclusion that is required for making an informed decision.
2. The system must provide the user with sufficient information for deriving the security conclusion.
3. The mental load of deriving the security conclusion must be tolerable.
4. The mental load of deriving security conclusions for any practical number of instances must be tolerable.

A phishing example
Hawaii Federal Credit Union



Genuine bank login

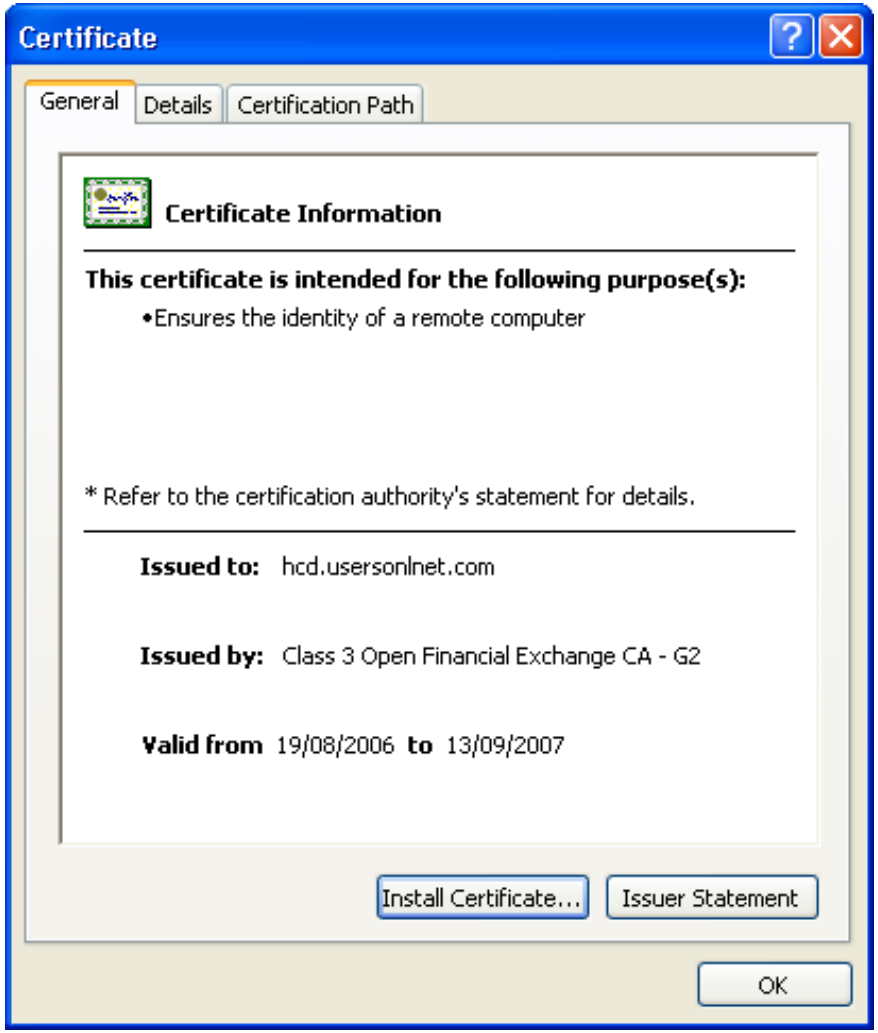
https://hcd.usersonlnet.com/asp/USERS/Common/Login/NettLogin.asp

Fake bank login

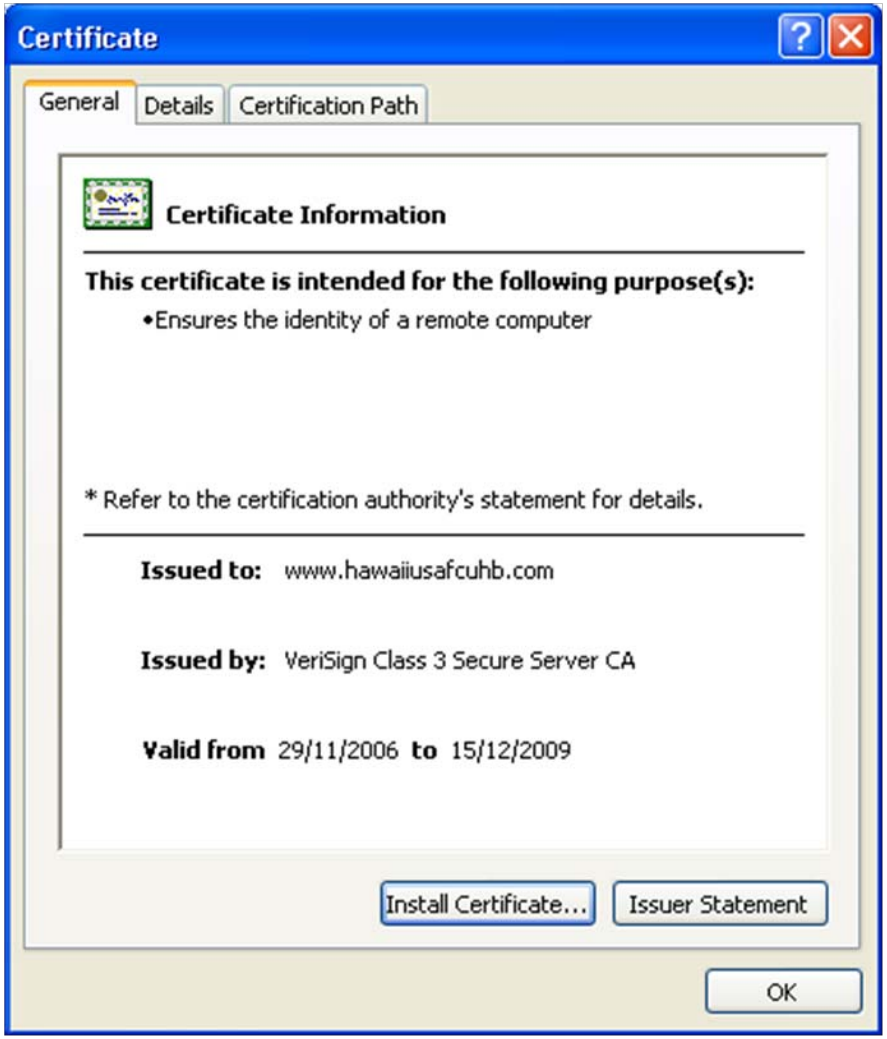
https://hawaiiusafcuhb.com/cgi-bin/mcw00.cgi?MCWSTART

UNIVERSITY GRADUATE CENTER

Certificate comparison 1

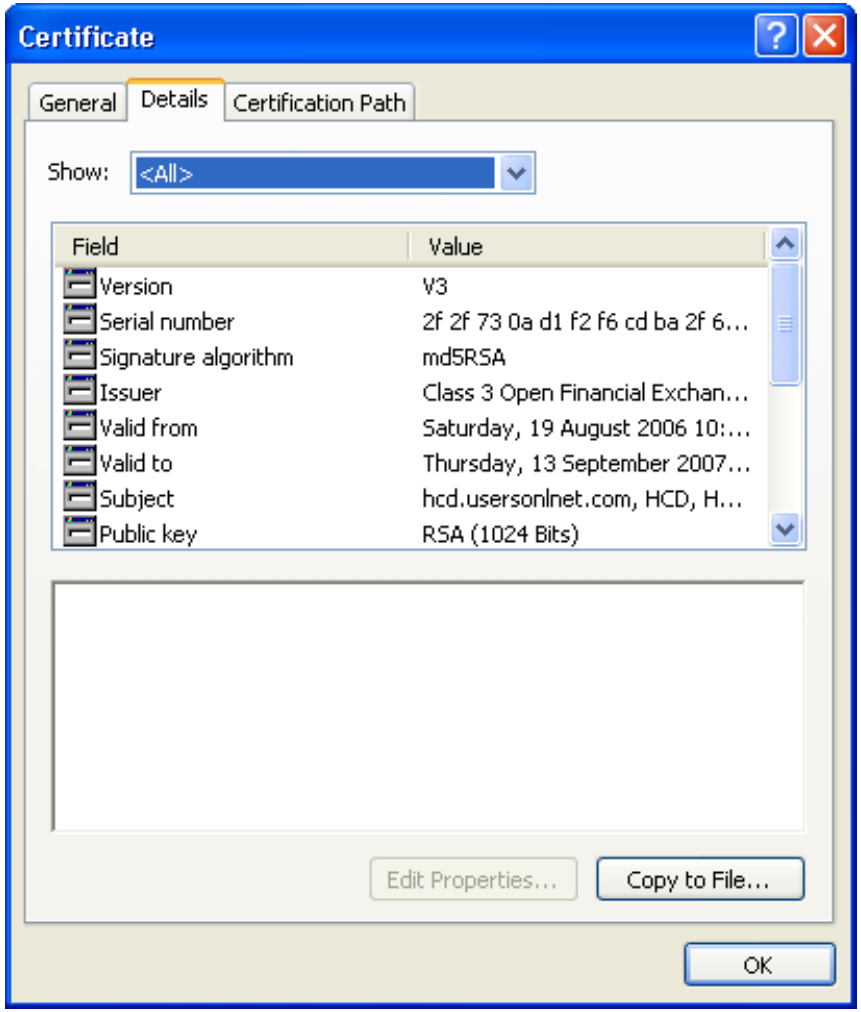


Genuine certificate

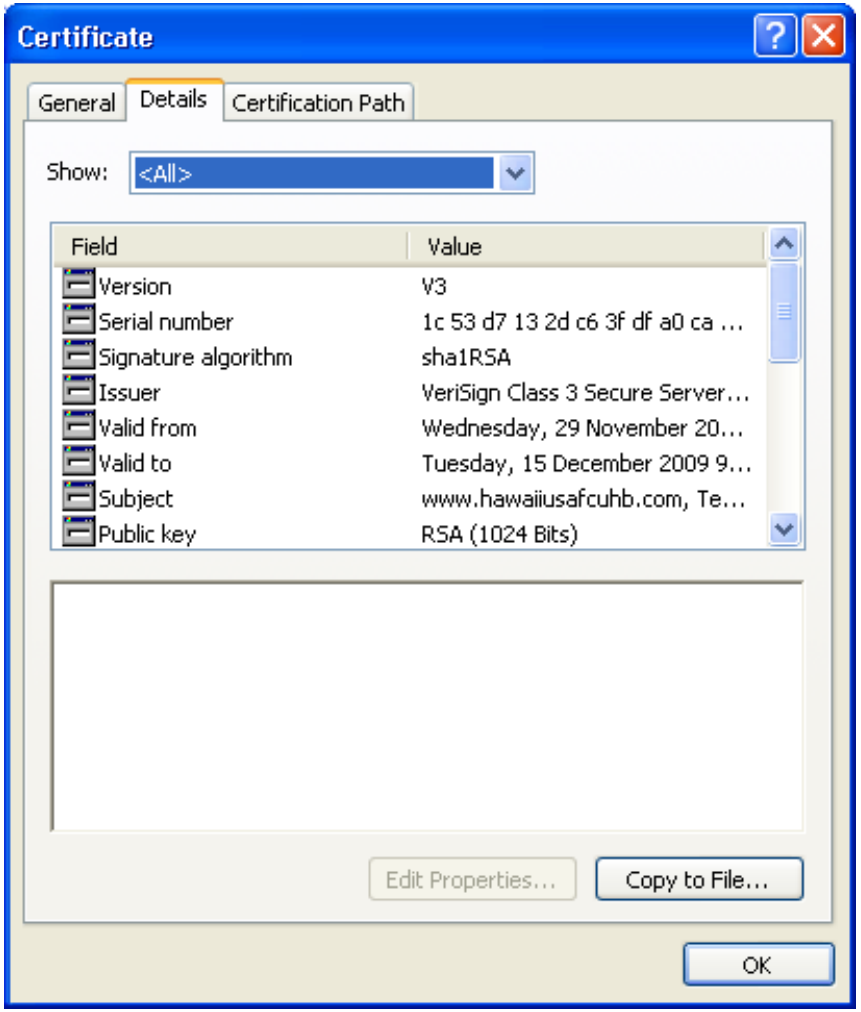


Fake certificate

Certificate comparison 2

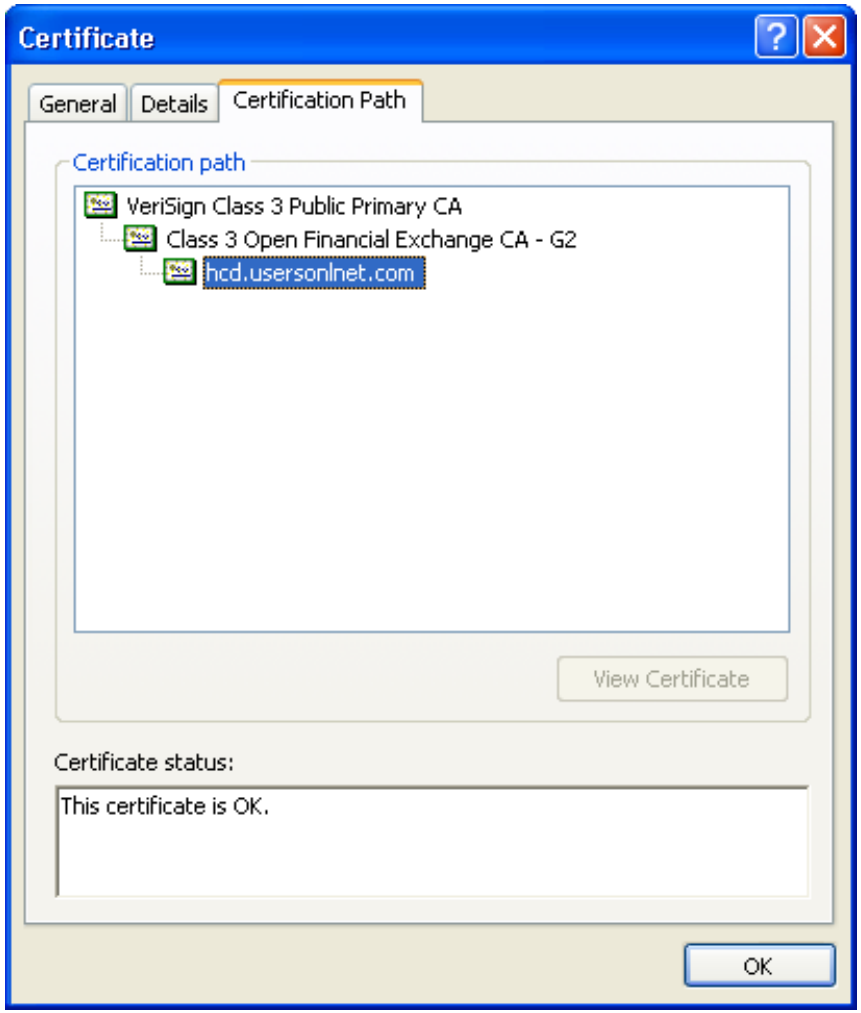


Genuine certificate

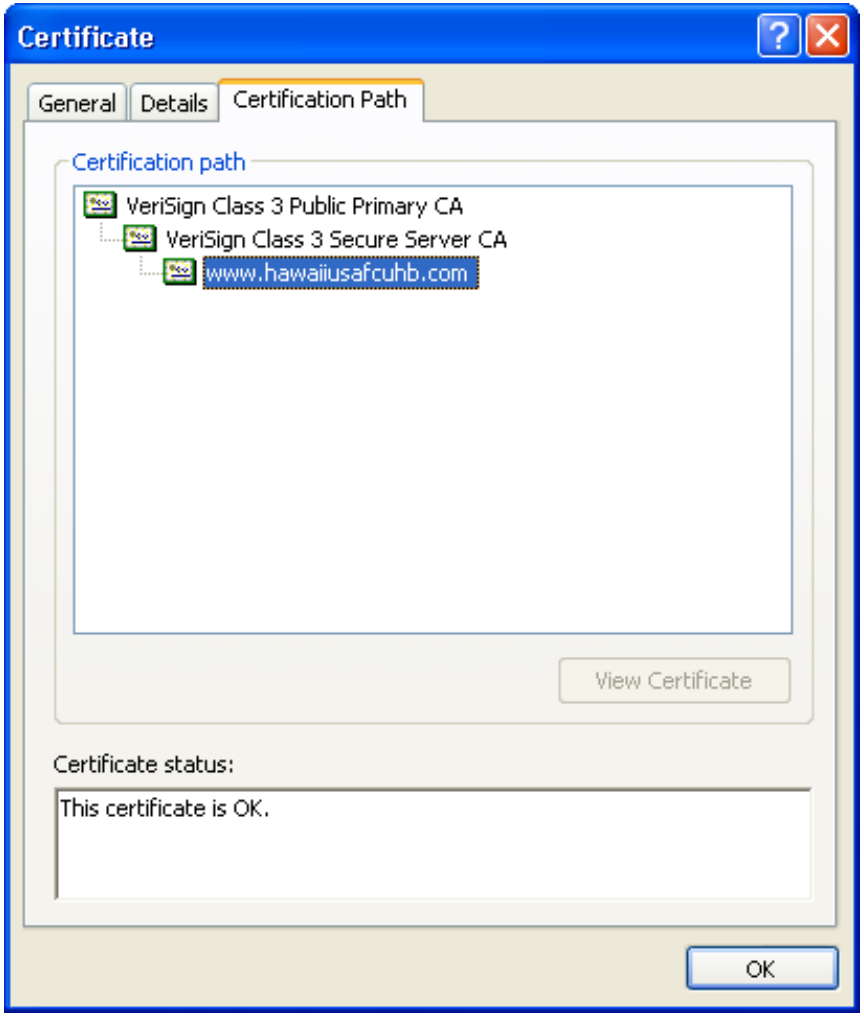


Fake certificate

Certificate comparison 3

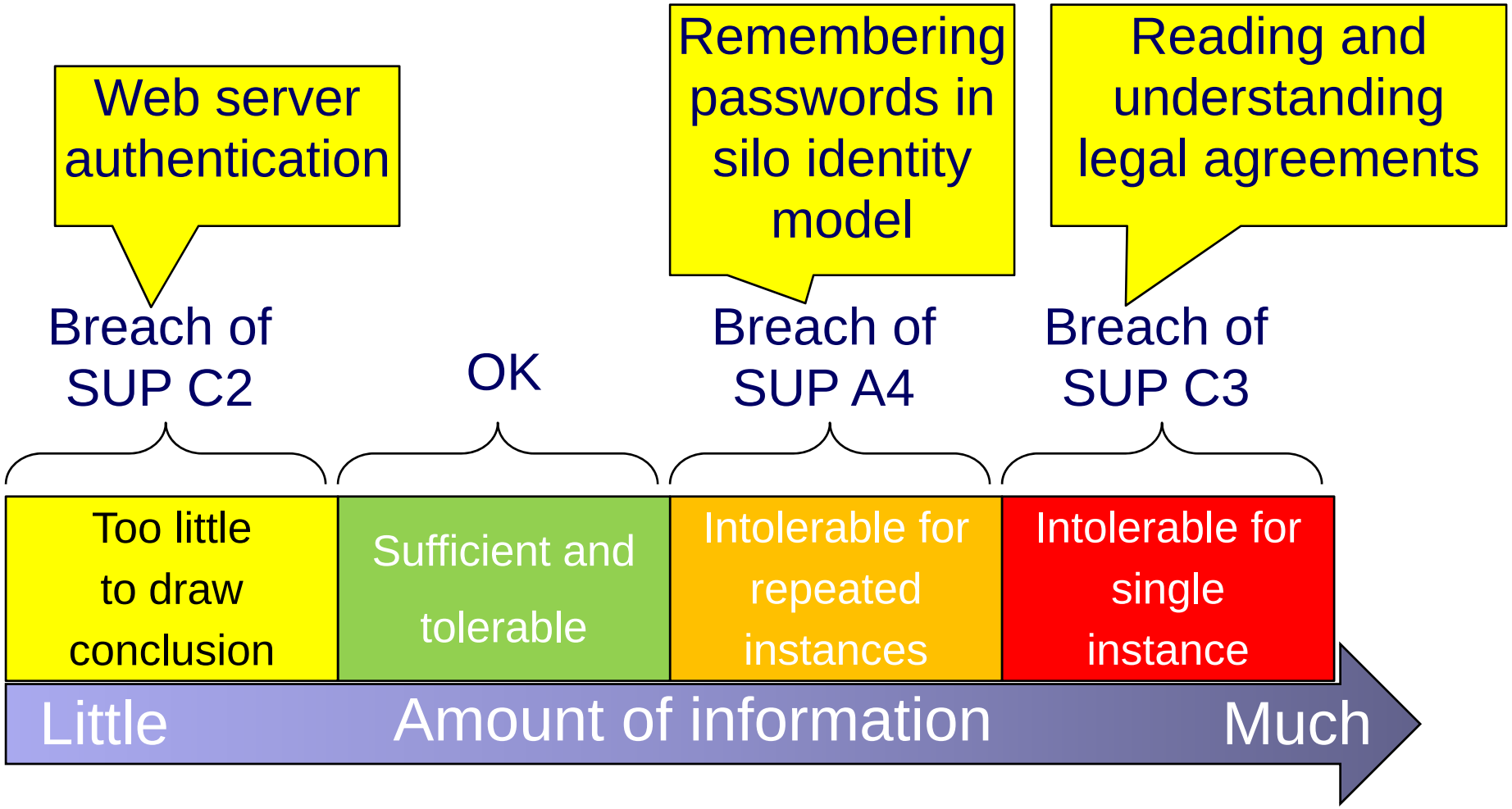


Genuine certificate



Fake certificate

Security Usability Principles for Conclusions and Actions



Research challenges

- Usability of security
- Seamless integration of user-centric and other models
- Protocols
  - Mobile integration
  - Dual channel authentication protocols
- Trusted platforms
- Privacy
- Personalisation of SP identities
- Name spaces
- Governance
- Standardisation

Questions ?