

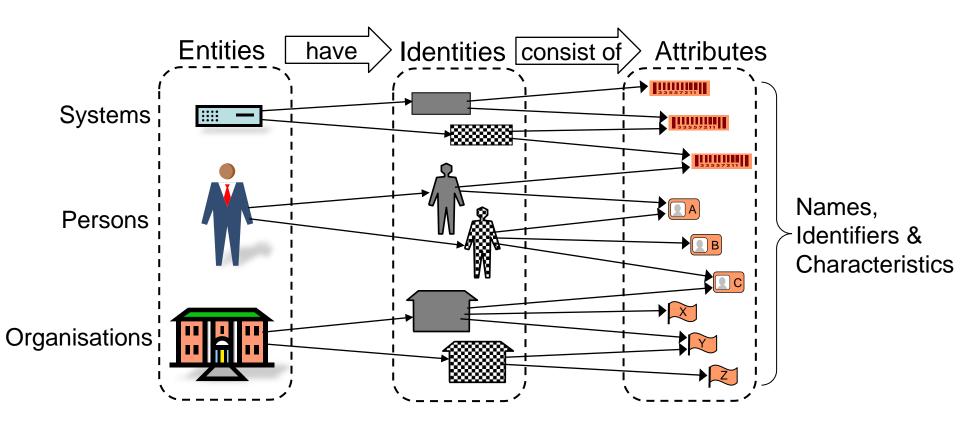
Identity Management

Prof Audun Jøsang Department of Informatics University of Oslo

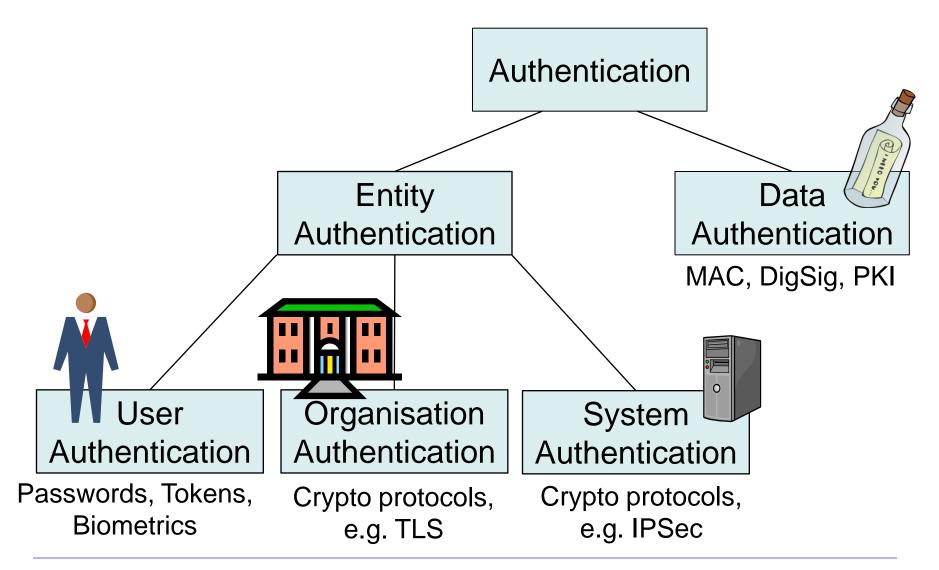


Finse May 2014

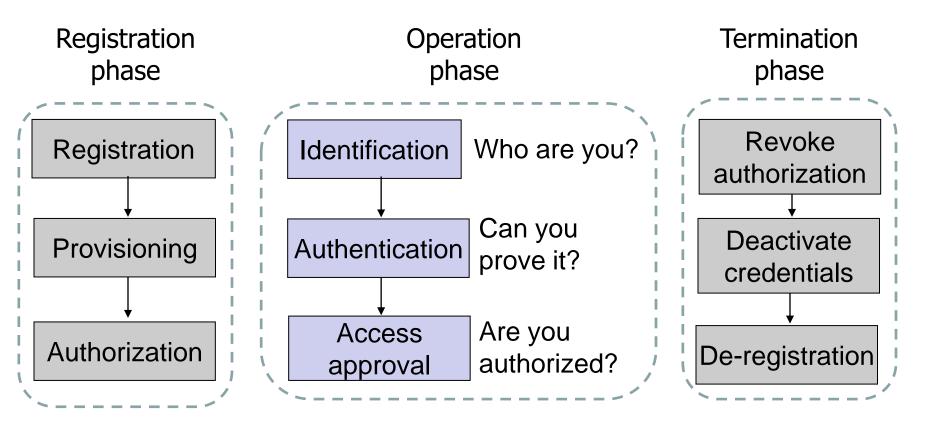
The concept of identity



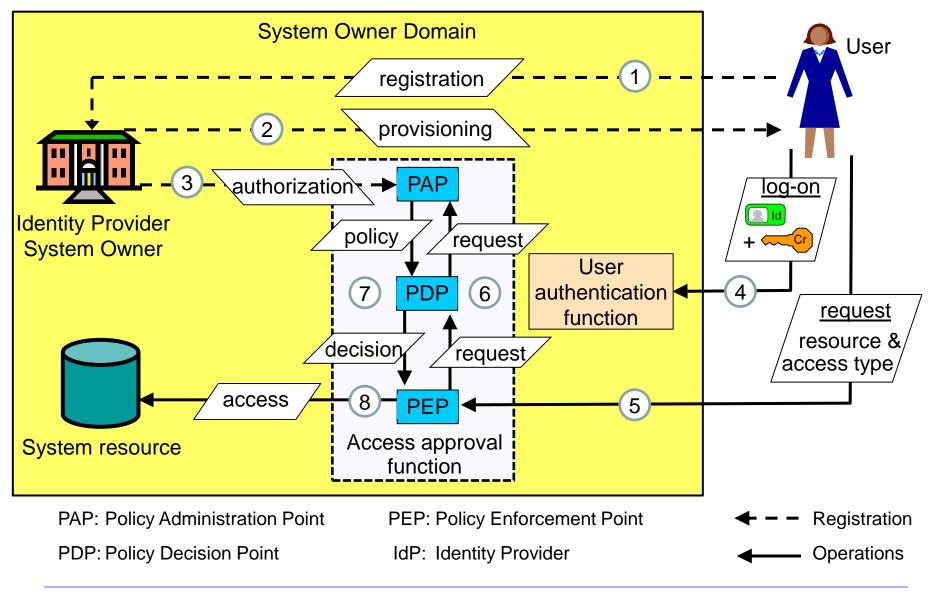
Taxonomy of Authentication



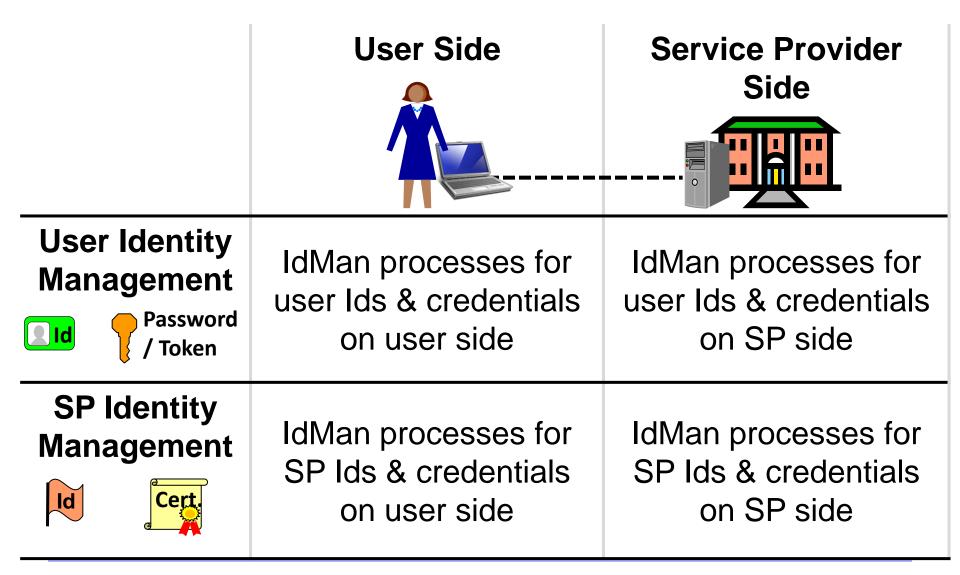
Access Control Phases



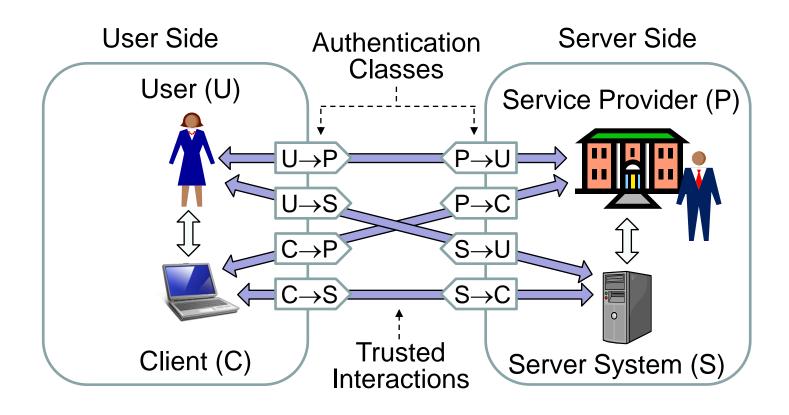
Access control concepts (abstract model)



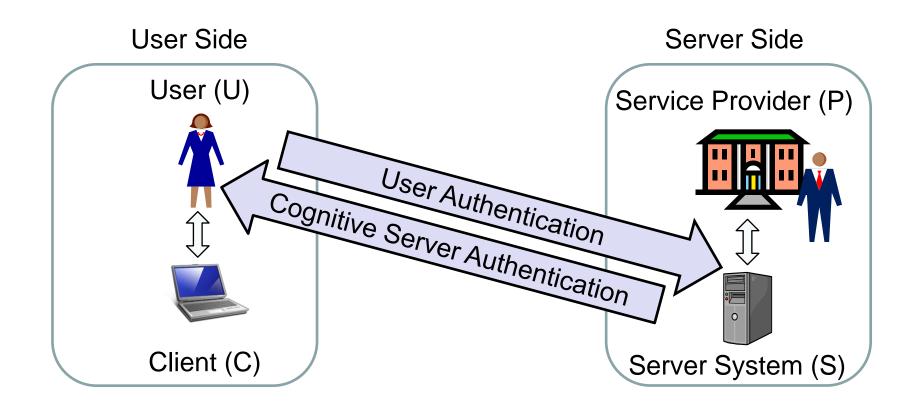
Identity management processes



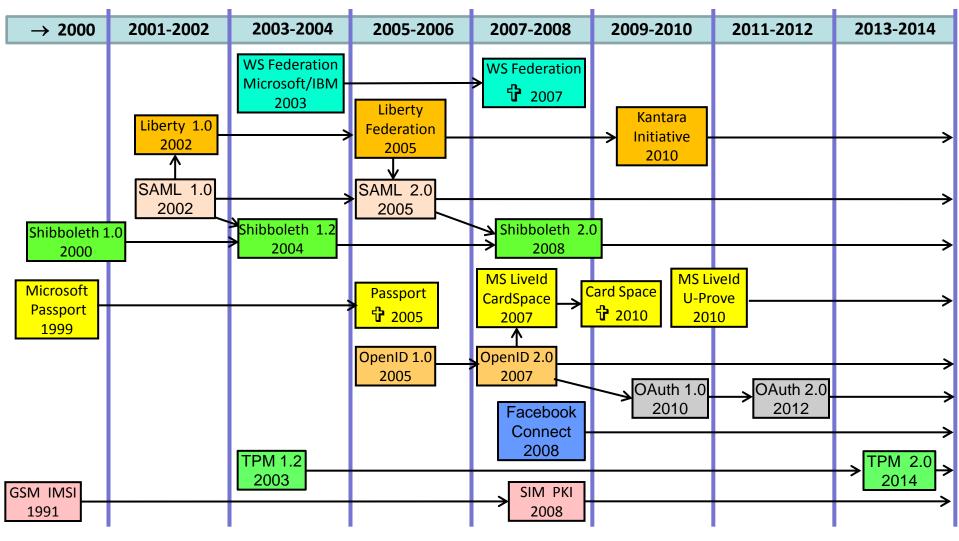
Entity authentication classes



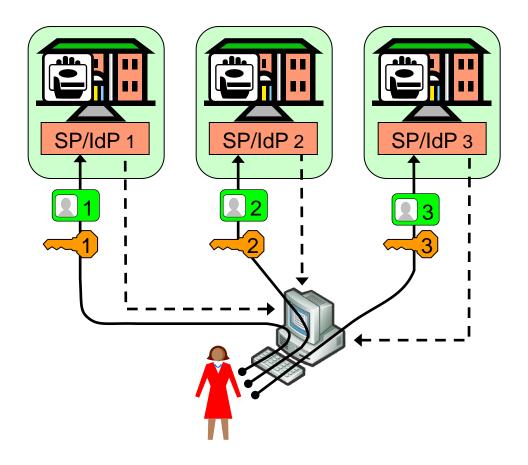
Mutual online entity authentication



Evolution of User Id Management

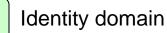


Silo domain model



Legend:





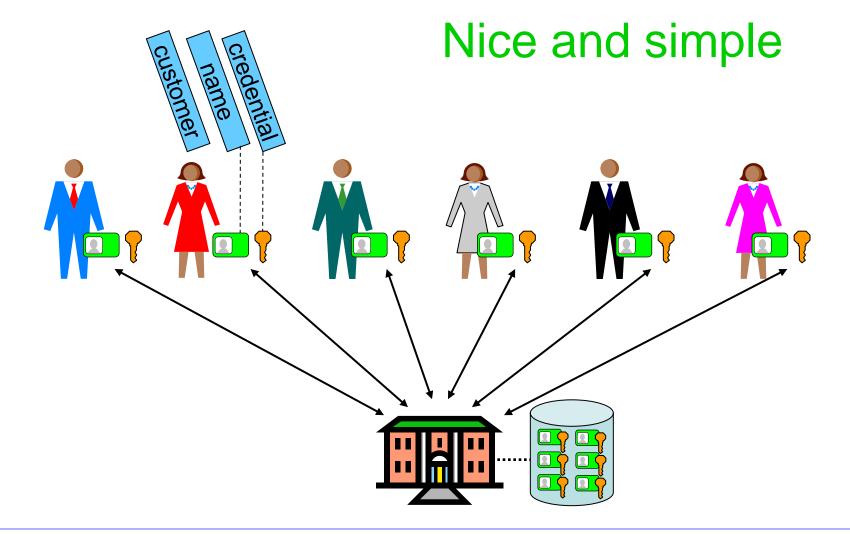


User identifier managed by IdP #



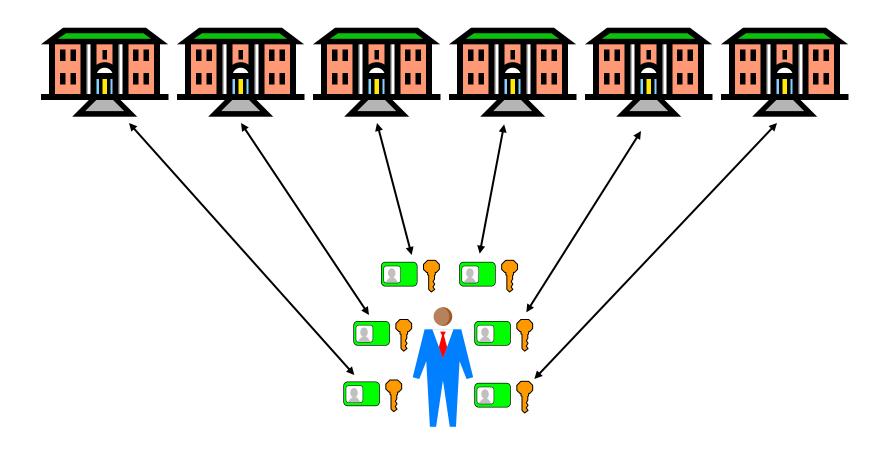
Service provision

Imagine you're a service provider

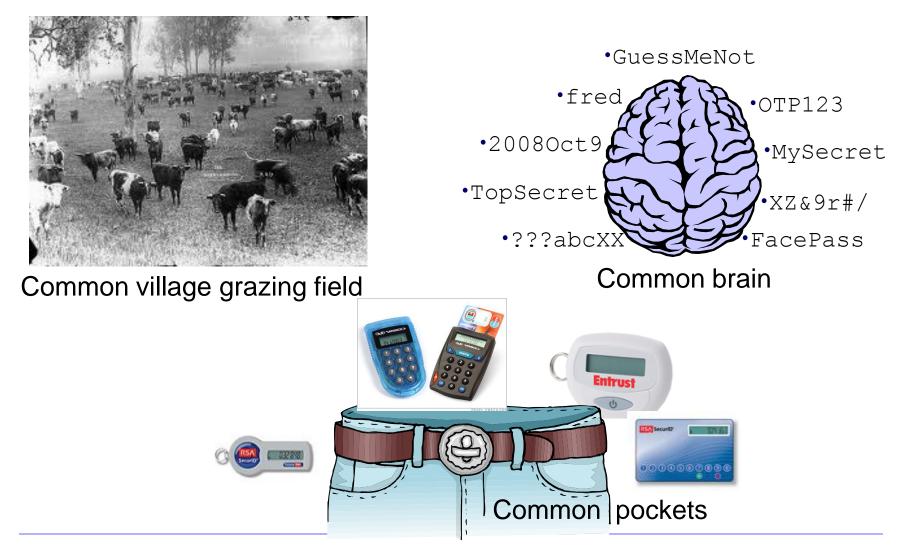


Imagine you're a customer

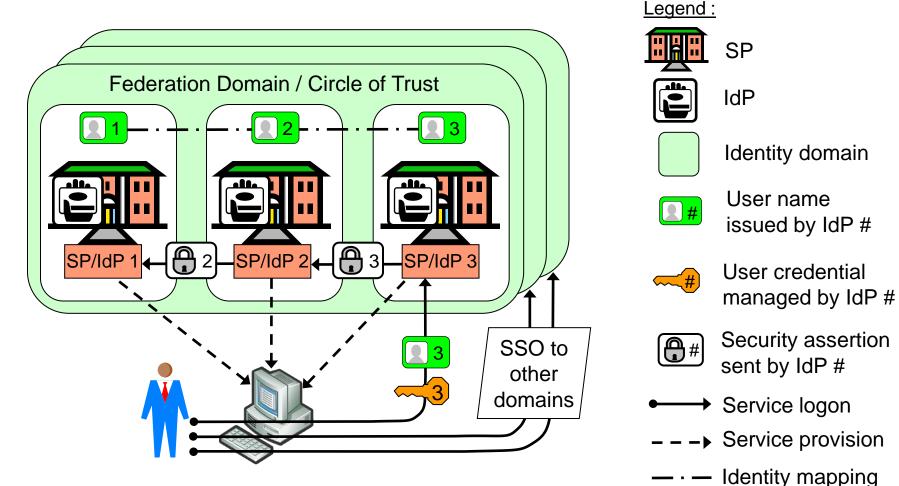
It's a nightmare



Tragedy of the Commons

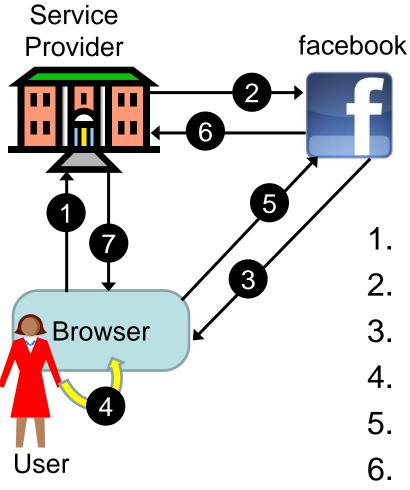


Federated SSO model



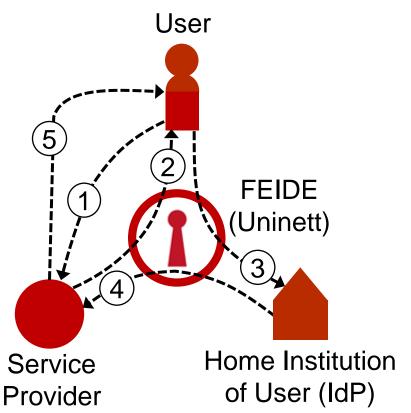
Examples: Liberty Alliance, SAML2.0, WS-Federation, Shibboleth

Authentication via Facebook Connect



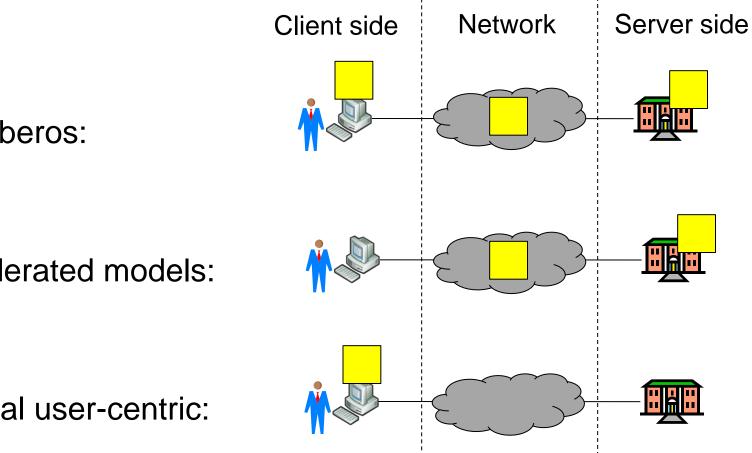
- 1. User requests service
- 2. Redirect to facebook authentication
- 3. Present facebook login form
- 4. User provides Id + credential
- 5. Credentials forwarded to facebook
- 6. Confirm authenticated user
- 7. Provide service





- 1. User requests access to service
- 2. Service Provider sends authentication request to FEIDE, and displays FEIDE login form to user.
- 3. User enters name and password in FEIDE login form, which are sent for validation to Home Institution of user.
- 4. Home Institution confirms authentic user and provides user attributes to FEIDE which forwards these to SP
- 5. Service Provider analyses user attributes and provides service according to policy

SSO technology location



Kerberos: ullet

Federated models: \bullet

Local user-centric: •

Client-side location for local user-centric identity management

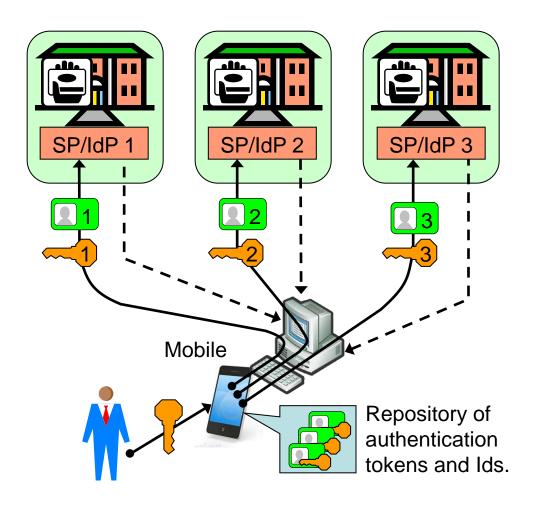
- IdM in Workstation
 - e.g. SW based password wallet

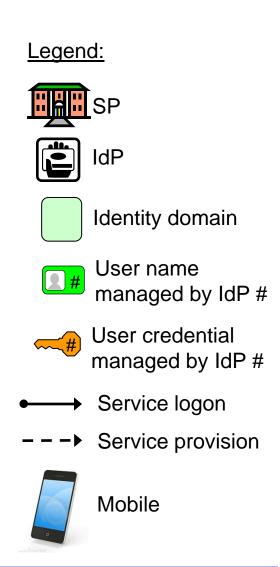


- IdM in Mobile phone
 - e.g SW/SIM based password wallet



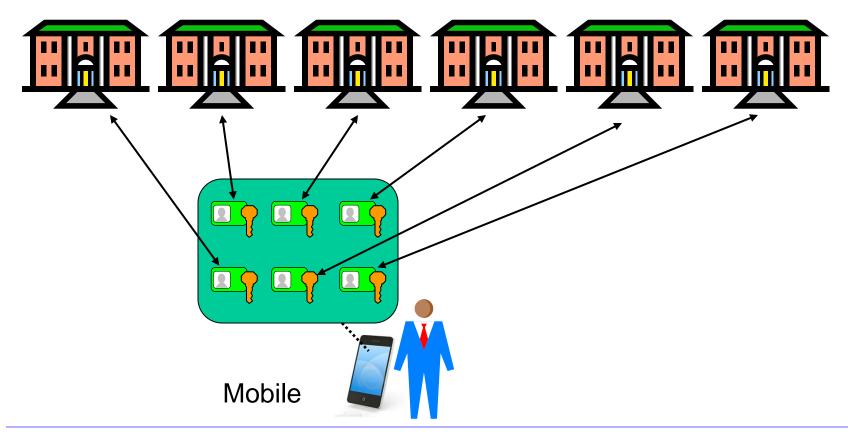
Local user-centric model





Local user-centric: Imagine you're a customer

User friendly and scalable



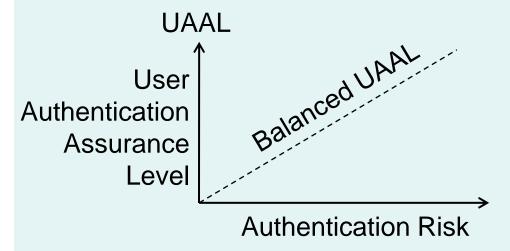
e-Authentication Frameworks for e-Gov.

- Trust in identity is a requirement for e-Government
- Authentication assurance produces identity trust.
- Authentication depends on technology, policy, standards, practice, awareness and regulation.
- Consistent frameworks allow cross-national and crossorganisational schemes that enable convenience, efficiency and cost savings.

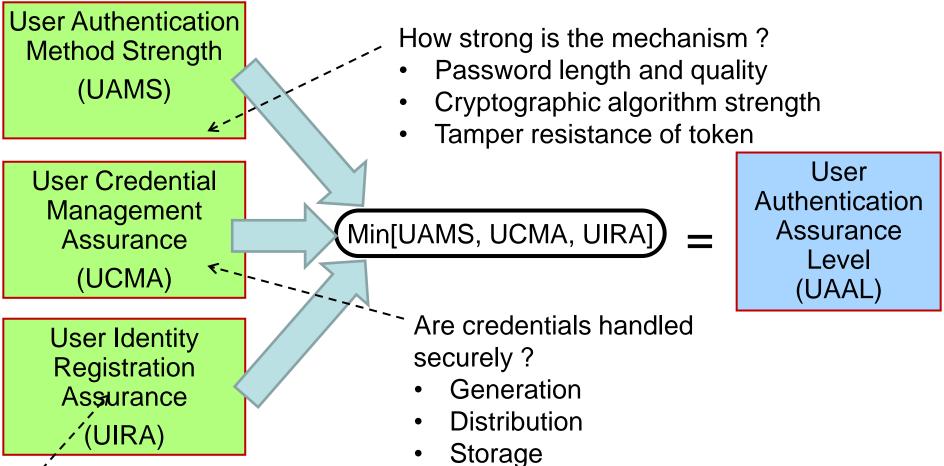


Authentication Assurance

- Authentication assurance = robustness of authentication
- Resources have different sensitivity levels
 - High sensitivity gives high risk in case of authentication failure
- Authentication has a cost
 - Unnecessary authentication assurance is a waste of money
- Authentication assurance should balance resource sensitivity



Factors for UAAL



How certain are you that the correct user was registered in the first place ?

- Pre-authentication credentials, e.g. birth certificate
- Biometrics

UAAL: User 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 in the identity assertion	Low confidence in the identity assertion	Moderate confidence in the identity assertion	High confidence in the identity assertion

Example taken from Australian NeAF 2009

Alignment of e-Authentication Frameworks

Authentication Framework	User Authentication Assurance Levels				
EAG	Little or no assurance		Some	High	Very High
(USA) 2006	(1)		(2)	(3)	(4)
IDABC		Minimal	Low	Substantial	High
(EU) 2007	X	(1)	(2)	(3)	(4)
FANR	Little or no assurance		Low	Moderate	High
(Norway) 2008	(1)		(2)	(3)	(4)
NeAF	None	Minimal	Low	Moderate	High
(Australia) 2009	(0)	(1)	(2)	(3)	(4)
ePramaan	None	Minimal	Moderate	Strong	Very Strong
(India) 2013	(0)	(1)	(2)	(3)	(4)

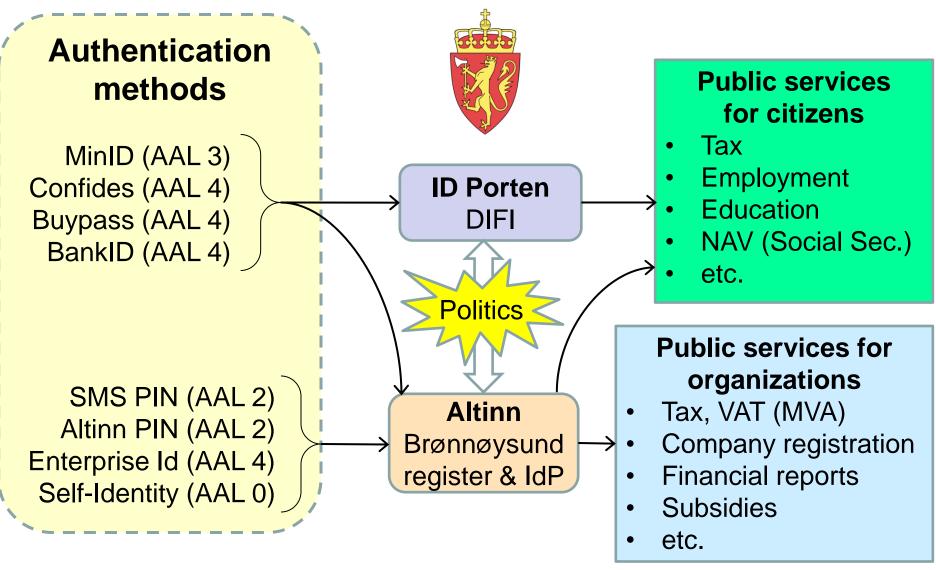
Risk Analysis for Authentication

Determining the appropriate UAAL for an application

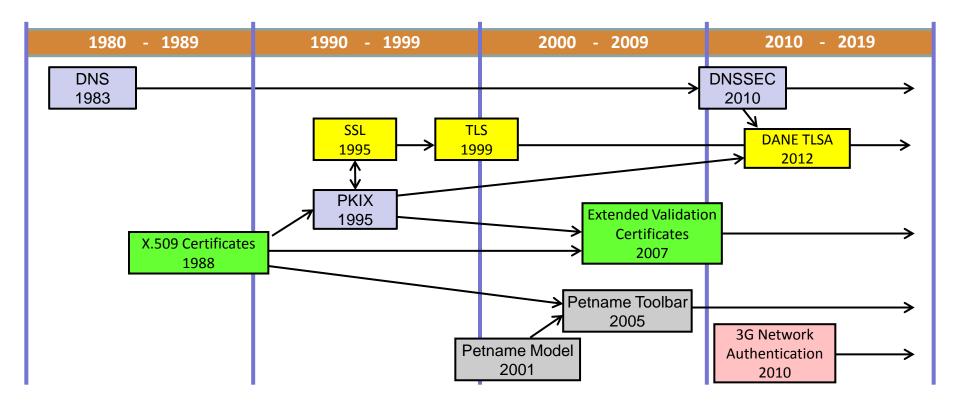
		Impact of e-Authentication failure				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	None (0)	Low (2)	Moderate (3)	High (4)	High (4)
	Likely	None (0)	Low (2)	Moderate (3)	High (4)	High (4)
	Possible	None (0)	Minimal (1)	Low (2)	Moderate (3)	High (4)
	Unlikely	None (0)	Minimal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

JAAL

Id Management for Norwegian e-Gov.



Evolution of SP Id Management



Public-Key Certificates

- A public-key certificate is simply a public key with a digital signature
- Binds name to public key
- Certification Authorities (CA) sign public keys.
- An authentic copy of CA's public key is needed in order to validate certificate
- Relying party validates the certificate (i.e. verifies that user public key is authentic)

X.509 Digital Certificate

- Version
- Serial Number
- Algorithm Identifier
- CA Name
- CA Unique Identifier
- User Name
 - User Unique Name
- User Public Key

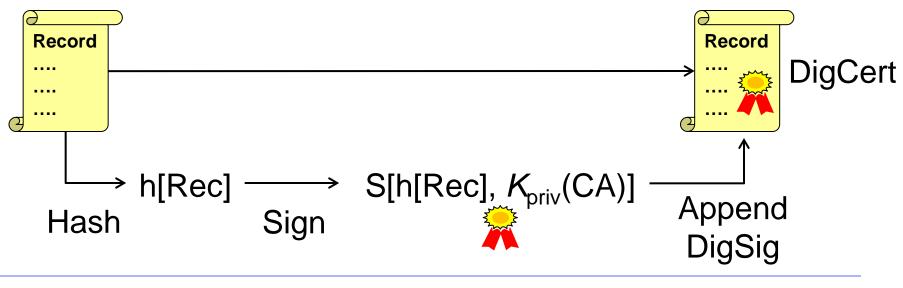
CA DigSig

- Validity Period
- Extensions

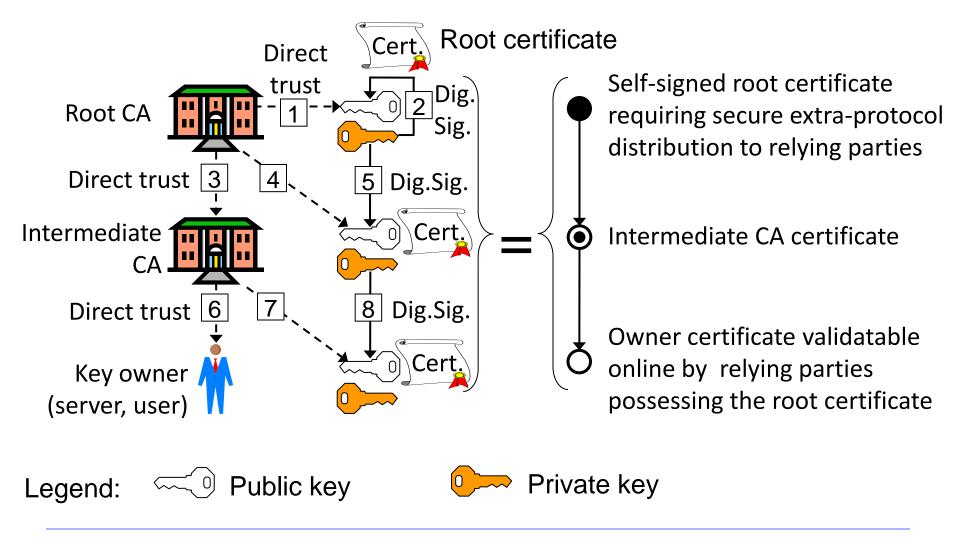
(Tryv)

How to generate a digital certificate?

- 1. Assemble the information (name and public key) in single record Rec
- 2. Hash the record
- 3. Sign the hashed record
- 4. Append the digital signature to the record



PKI certificate generation



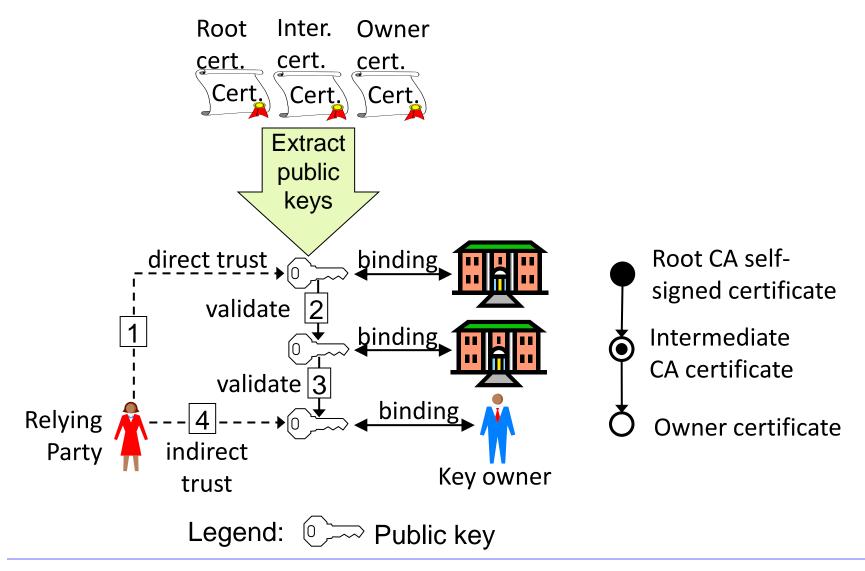
Self-signed root keys: Why?

- Many people think a root public key is authentic just because it is self-signed
- Can be deceptive
 - Gives impression of assurance
 - Disguises insecure practice
 - Gives false trust

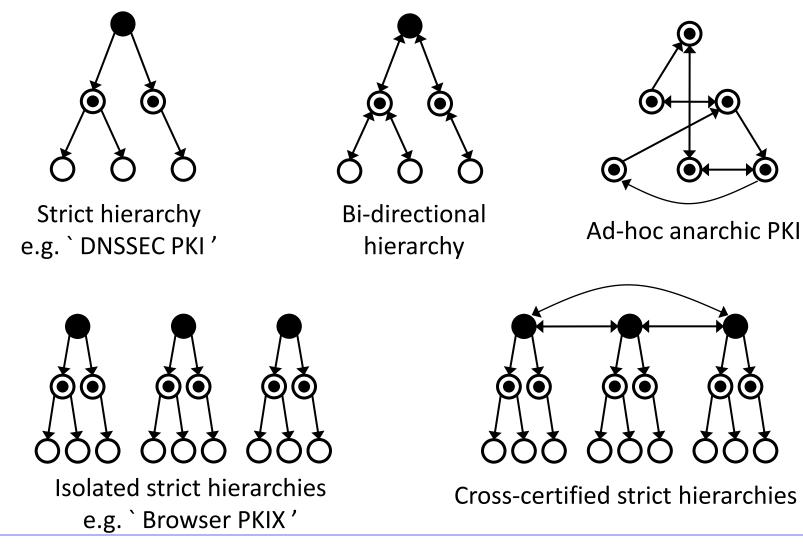


- Self-signing provides <u>absolutely no security</u>
- Useful purpose of self-signing
 - X.509 certificates have a field for digital signature, so an empty field might cause applications to malfunction. A self-signature is a way to fill the empty field
 - Self-signature can be used to specify a cert as a root

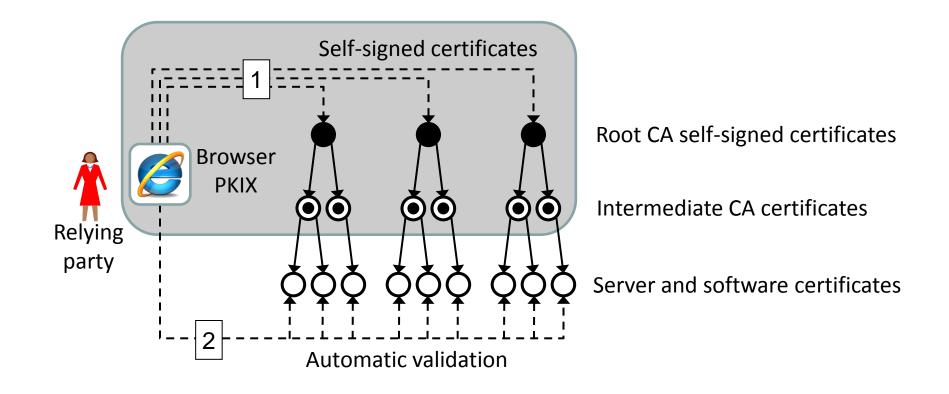
Certificate and public key validation



PKI Trust Models



Browser PKIX



A phishing example: Hawaii Federal Credit Union

🗿 Web Site Login - Microsoft Internet Explo	rer		DirectLink • Internet Banking - Microsoft Internet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		A	Elle Edit View Favorites Iools Help	
Address 💩 https://hcd.usersoninet.com/asp/USERS/C	ommon/Login/NetLogin.asp	Go Links	Address 🕘 https://www.hawaiiusafcuhb.com/cgi-bin/mcw000.cgi?MCWSTART	💌 🄁 Go 🛛 Links
New Security Feature	LOG IN		FEDERAL CREDIT UNION	This credit union is federally insured by the National Credit Union Administration
The protection of your financial information and the security of your online transactions are very				Demo
important to us. We have added a new security feature called PassMark. PassMark will help			DirectLink • Internet Banking	
protect you from fraudulent online activities like phishing, ID theft, and spooled view sites.		=	Password:	
PassMark. Follow the	lease enter your Account Number to log in to our services. Service through a secured connection.		Continue Reset	
complete this one-time enrollment.	f you have difficulty logging in, please call Hawaii Federal Credit U 847-1371 or email us at <u>memberservice@hawaiifcu.or</u>		Phishing Alert Update! 2/28/07 - It has been brought to our attention that various phishing emails have been sent referencing Hawai/USA Federal	
Where is the Password box? The Password box will appear on the next screen. This is another	Acct. Number:		Credit Union. The recent email states that multiple computers have attempted to log into your Hawaii/SA account and failure to respond to the email will result in a suspension of your Hawaii/SA account. It contains spelling errors, invalid links, and unfamiliar	
change we've applied to enhance your security.	Log In Home		accounts a contains appening en one, investment an insistements. phone number amongst many encoded statements. If you receive such an email, DO NOT REPLY TO OR CLICK ON	
	<u>gn Up Now!</u> at a member? <u>Click here to apply for a loan.</u>	V4.14.7.0	ANY PART OF THE EMAIL. For more information, please visit our website at www.hawailusafcu.com or call our Member Service Center at 534-4300 (oalu) or toll free 800-379-1300 (neighbor islands and mainland).	
ê)		Internet	istanius and maintainu).	🞽 🔮 Internet .:

Genuine bank login

https://hcd.usersonInet.com/asp/USE RS/Common/Login/NettLogin.asp

Fake bank login

https://hawaiiusafcuhb.com/cgibin/mcw00.cgi?MCWSTART

Certificate comparison 1

-	
Certificate 🛛 🕐 🔀	Certificate ? 🔀
General Details Certification Path	General Details Certification Path
Certificate Information This certificate is intended for the following purpose(s):	Certificate Information This certificate is intended for the following purpose(s):
•Ensures the identity of a remote computer	•Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.	* Refer to the certification authority's statement for details.
Issued to. Inclusersonniet.com	Issued to: www.nawaiiusarcund.com
Issued by: Class 3 Open Financial Exchange CA - G2	Issued by: VeriSign Class 3 Secure Server CA
Valid from 19/08/2006 to 13/09/2007	Valid from 29/11/2006 to 15/12/2009
Install Certificate Issuer Statement	Install Certificate Issuer Statement
ОК	ОК
Genuine certificate	Fake certificate

Certificate comparison 2

Certificate		?×
General Details Certification Path		
Show: <all></all>	~	
Field	Value	
 Version Serial number Signature algorithm Issuer Valid from Valid to Subject Public key 	V3 2f 2f 73 0a d1 f2 f6 cd ba 2f 6 md5R5A Class 3 Open Financial Exchan Saturday, 19 August 2006 10: Thursday, 13 September 2007 hcd.usersonInet.com, HCD, H R5A (1024 Bits)	
Ed	it Properties Copy to File.	
		ж

Genuine certificate

Certifica	te				?	×
General	Details	Certification F	Path			
Show:	<all></all>			~		
Field				Value	^	
Sign Sign Vali Sub	ial numbe nature ale			V3 1c 53 d7 13 2d c6 3f df a0 ca sha1RSA VeriSign Class 3 Secure Server Wednesday, 29 November 20 Tuesday, 15 December 2009 9 www.hawaiiusafcuhb.com, Te RSA (1024 Bits)		
			Edi	t Properties		
			_			
					Ж	

Fake certificate

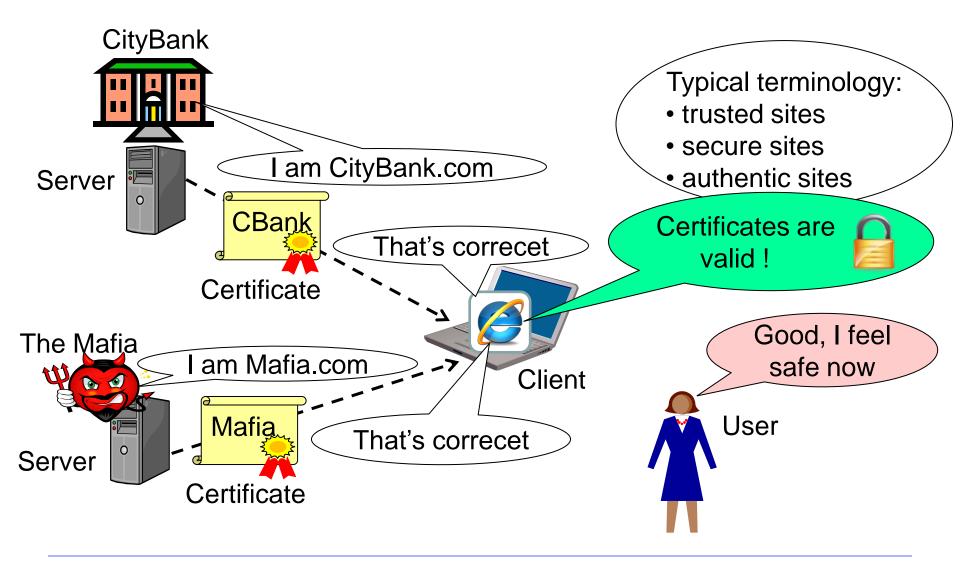
Certificate comparison 3

Certificate	Certificate	? 🗙
General Details Certification Path Certification path VeriSign Class 3 Public Primary CA Class 3 Open Financial Exchange CA - G2 Class 1 Open Financial Exchange CA - G2 Class 1 Open Financial Exchange CA - G2	General Details Certification Path Certification path VeriSign Class 3 Public Primary CA VeriSign Class 3 Secure Server CA Www.hawaiiusafcuhb.com	
View Certificate Certificate status: This certificate is OK.	Certificate status: This certificate is OK.	/iew Certificate
	ок	ОК

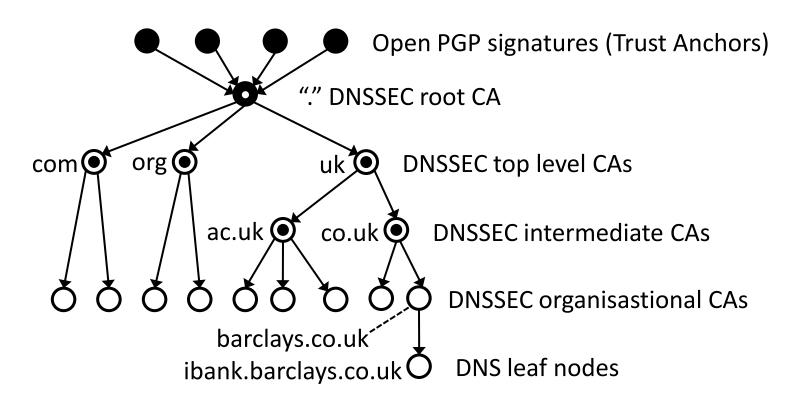
Genuine certificate

Fake certificate

Meaningless PKIX Server Authentication

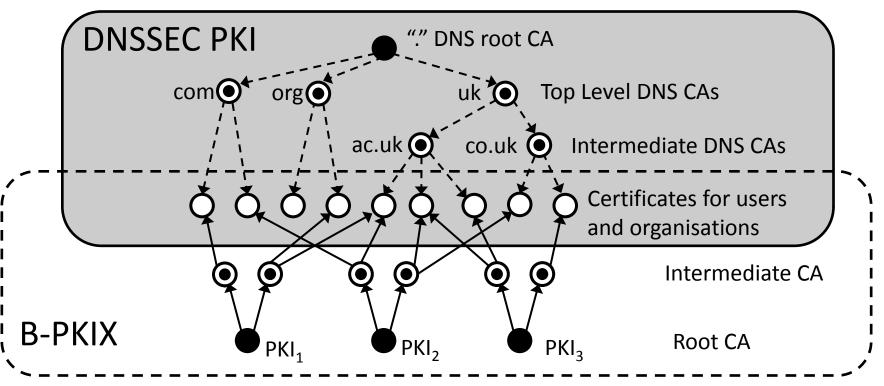


DNSSEC PKI



- The DNS (Domain Name System) is vulnerable to e.g. cache poisoning attacks resulting in wrong IP addresses being returned.
- DNSSEC designed to provide digital signature on every DNS reply
- Based on PKI with a single root.

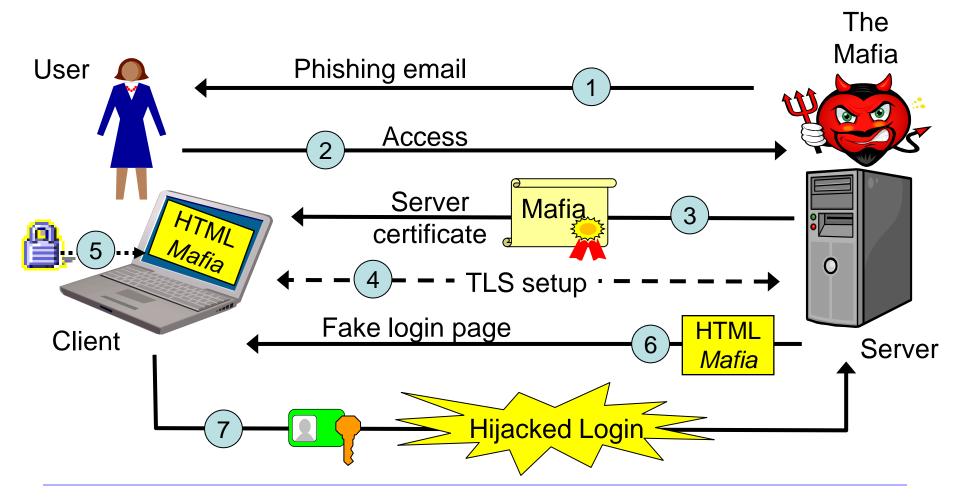
DNSSEC PKI vs. Browser PKIX



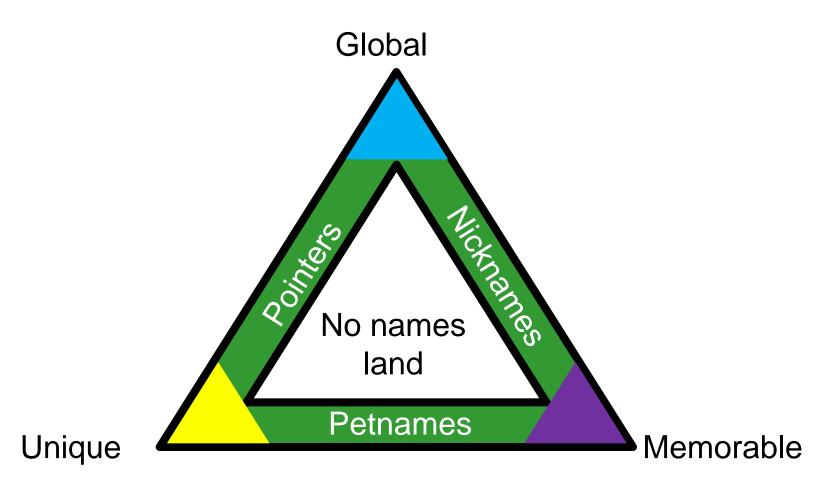
- In B-PKIX, any CA can issue certs for any domain \rightarrow problematic
- CAs under the DNSSEC PKI can only issue certificates for own domain
- The DNSSEC PKI and the B-PKI both target the same user/org nodes
- DANE: DNSSEC-based Authentication of Named Entities

Finse, 20 Alternative to B-PKIX, stationarce exist, not deployed, complex 42

Phishing and failed authentication

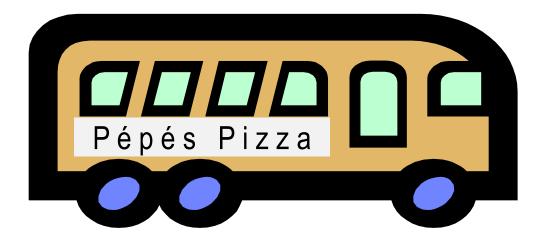


Zooko's Triangle of Id Properties



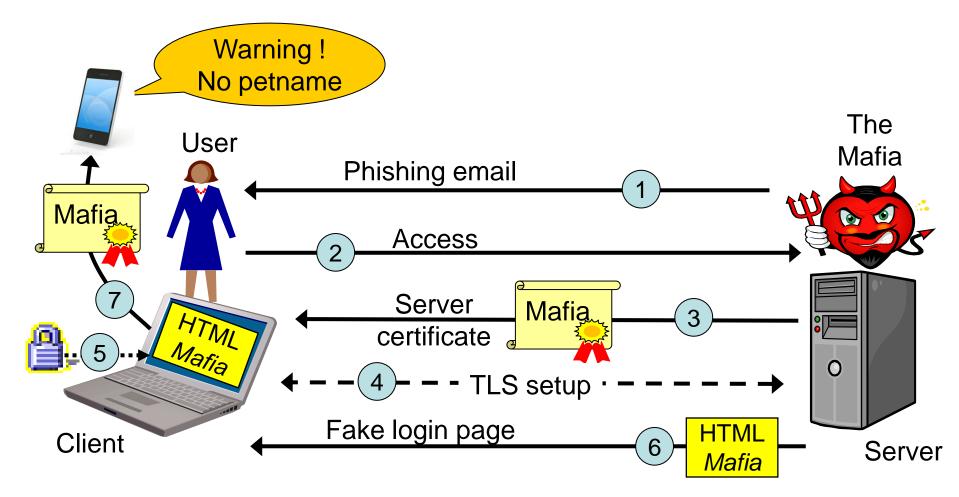
No identifier can be at the same time global, unique and memorable

Passing bus test for memorability

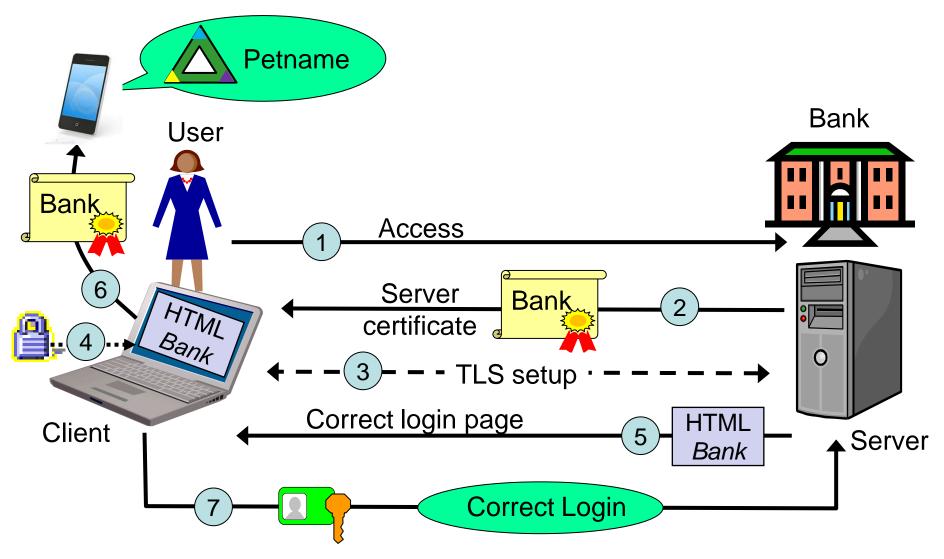


 If you see a name written on a passing bus, and you can remember the name after 5 minutes, then the name is memorable

Phishing detection with user-centric IdMan



User-centric server authentication



Thank you for your attention



Questions?