



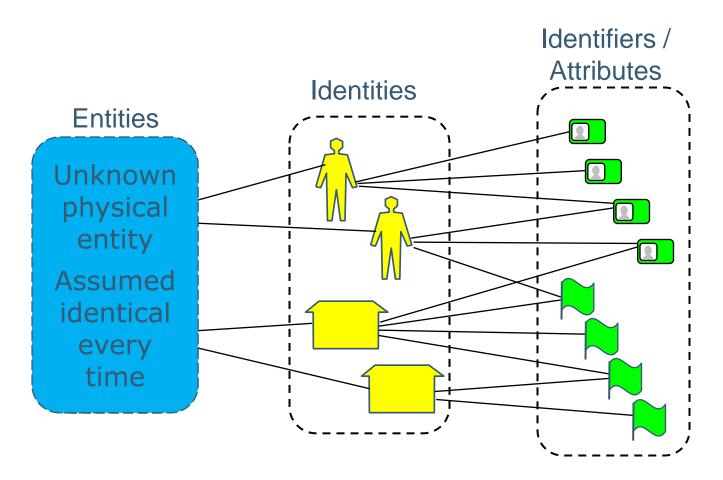
### Research Challenges in Identity Management

AF Security 14 August 2008

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

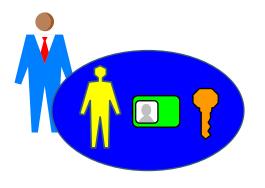
AFSecurity 14.08.2008

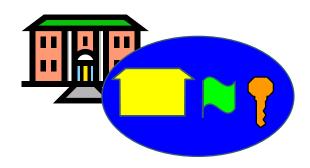
### Relationship between Entities, Identities and Identifiers





### Who's identity?





#### User Ids:

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

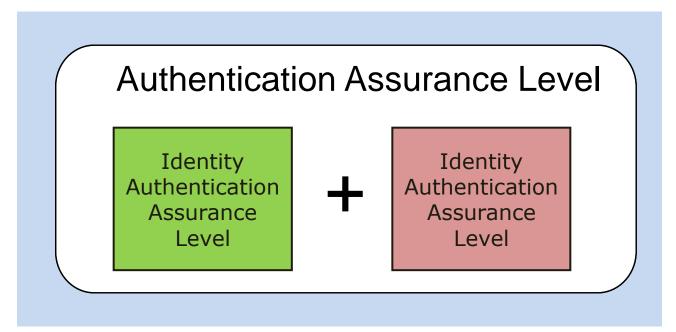
#### SP Ids:

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

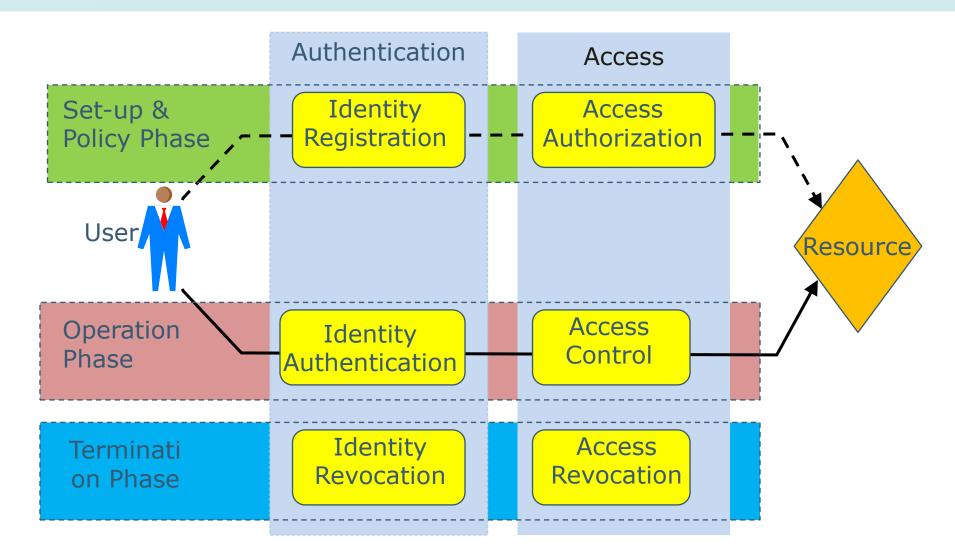


### Authentication Assurance Level (AAL)

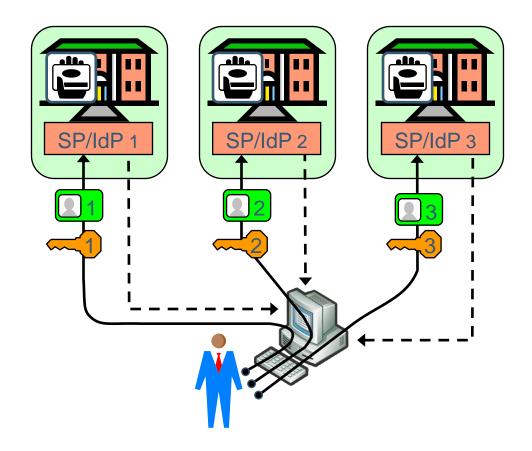
- AAL is a combination of
  - Identity Registration Assurance Level (IRAL)
  - Identity Authentication Assurance Level (IAAL)



#### Authentication and Access



### Silo domain model



Legend:





Identity domain



User identifier managed by IdP #

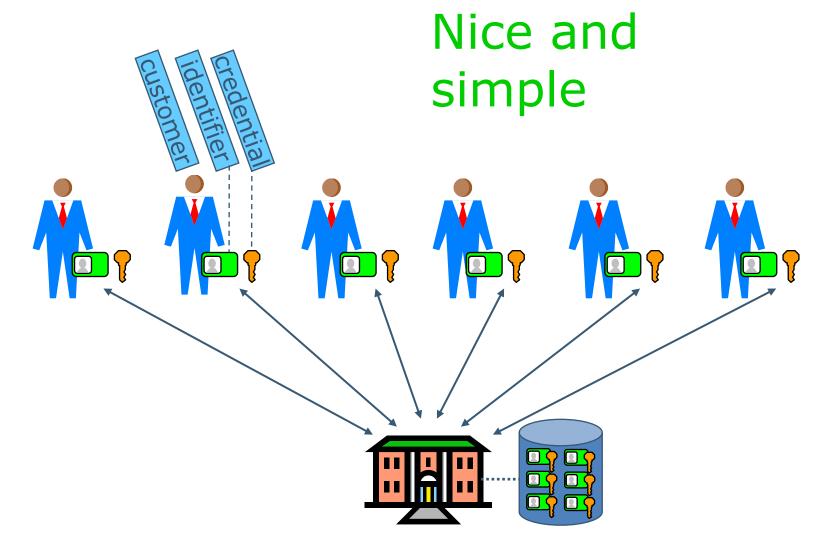


Authentication token managed by IdP #



Service provision

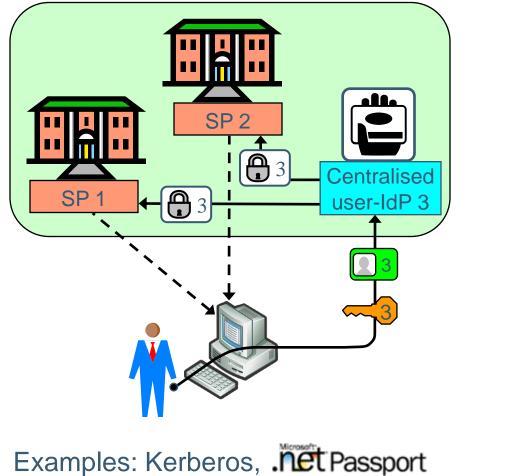
#### Imagine you're a service provider



#### Imagine you're a customer

## It's a nightmare

### Traditional Single Sign-On (SSO)



Legend:







Identity domain



User identifier issued by IdP #



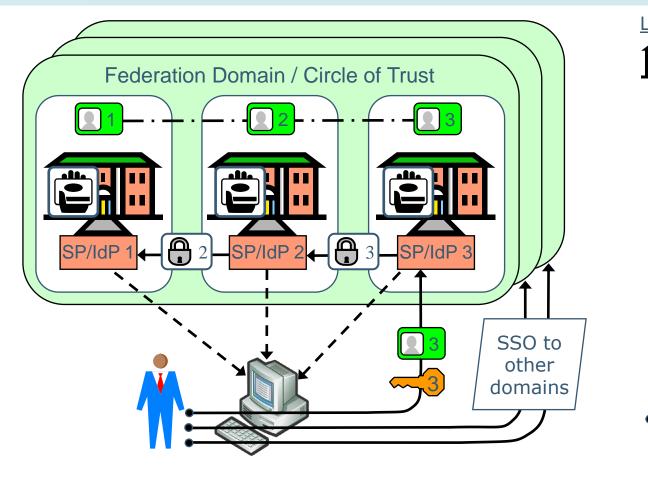
Security assertion sent by IdP #

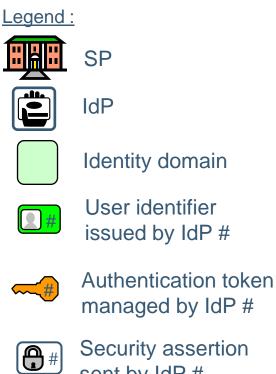
Authentication token managed by IdP #



--► Service provision

### Federated SSO model



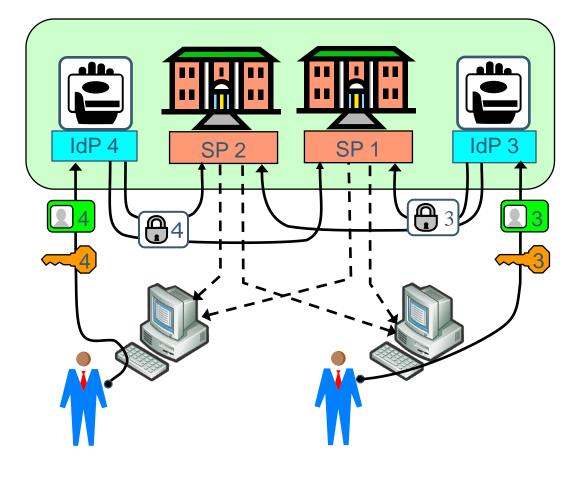


Security assertion sent by IdP #

- User logon
- -> Service provision
- Identifier mapping

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

### Distributed SSO identity model



Example: OpenID

#### Legend :









User identifier managed by IdP #



Authentication token managed by IdP #



Security assertion issued by IdP #

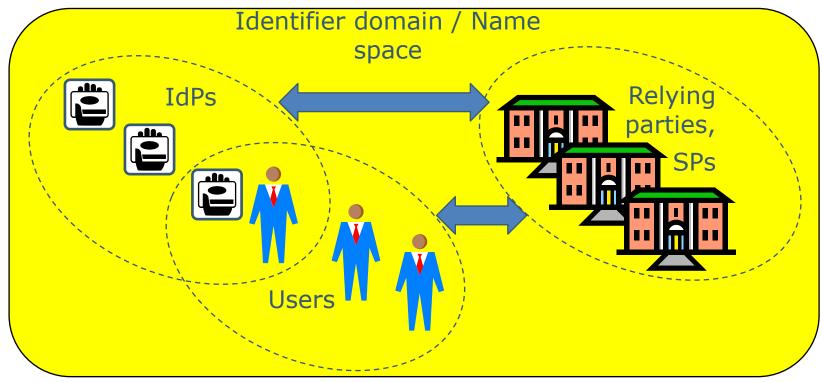
→ User logon

– – Service provision



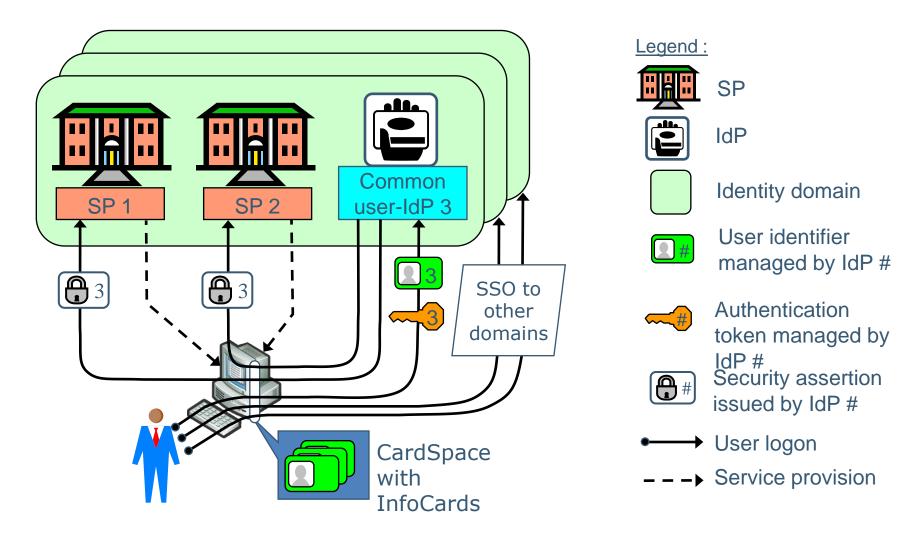
### **OpenID distributed SSO**

- Common name space
- Distributed IdPs
- No authorities

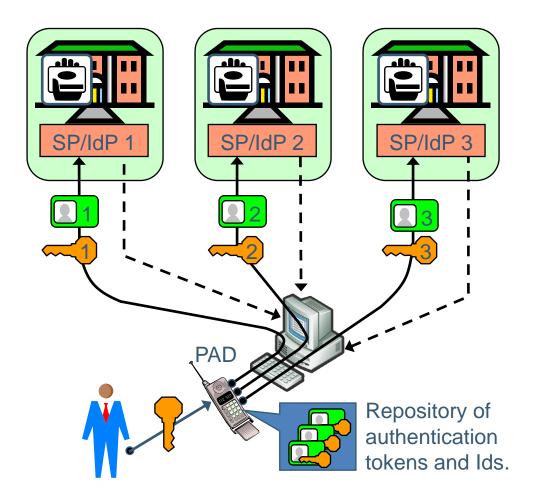




### Microsoft's InfoCard model



### User centric model



#### Legend:







User identifier managed by IdP #



Authentication token managed by IdP #

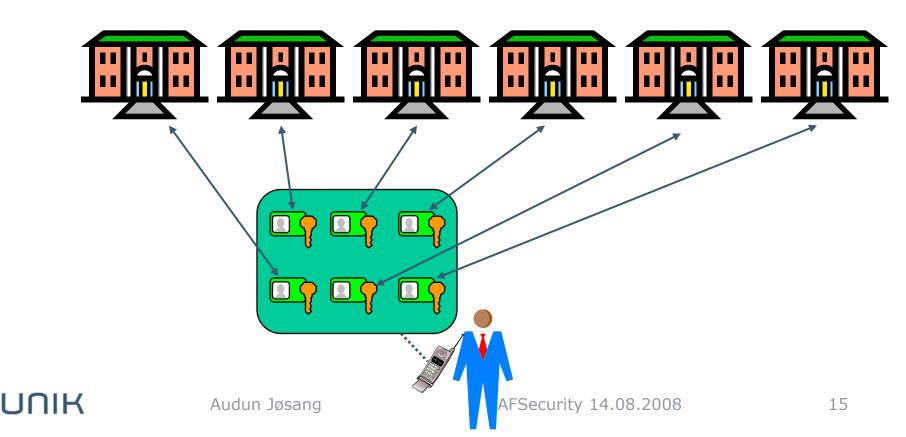
- → User logon
- --> Service provision



Personal Authentication Device

### User centric SSO: Imagine you're a customer

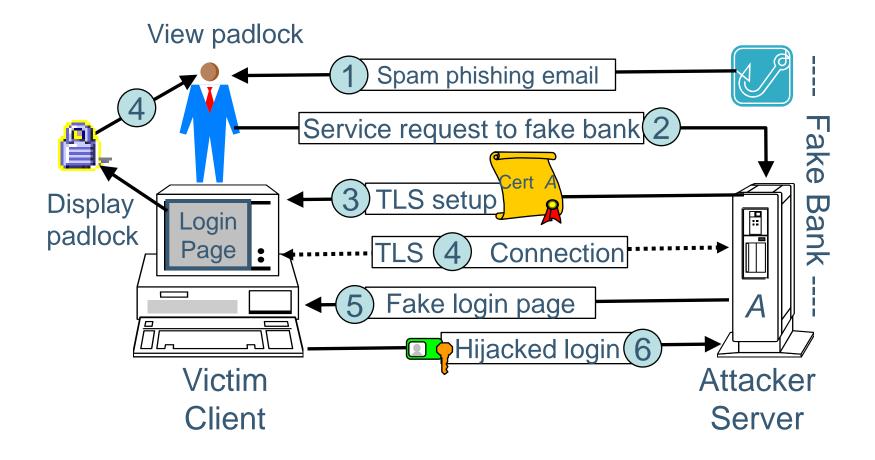
### It's a dream



### Closer look at SSO

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

### Phishing: Failed server authentication





### A phishing example: Hawaii Federal Credit Union

🗿 Web Site Login - Microsoft Internet I	Explorer		DirectLink • Internet Banking - Microsoft Internet Explorer			
<u>File E</u> dit <u>Vi</u> ew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		<u></u>	ile Edit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		<b>A</b> *	
Address 🕘 https://hcd.usersonlnet.com/asp/USERS/Common/Login/NetLogin.asp		ddress 👸 https://www.hawaiiusafcuhb.com/cgi-bin/mcw000.cgi?MCWSTART	💌 🄁 Go 🛛 Links			
New Security Feature	LOG IN		FEDERAL CREDIT UNION	credit union Visa card	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 important to us. We have added a new security feature called			Login Register-General f	I Membership Register-Business Members I I	Demo	
PassMark. PassMark will help protect you from fraudulent online activities like phishing, ID theft, and spoofed web sites. Everyone enrolled in Online		=	Accour Passwo	word:		
Banking is required to enroll in PassMark. Follow the instructions on each screen to	Please enter your Account Number to log in to our services. Services through a secured connection. If you have difficulty logging in, please call Hawaii Federal Credit Ur		Phis	Continue Reset		
complete this one-time enrollment.	847-1371 or email us at <u>memberservice@hawaiifcu.org</u>		2/28/07 - It i phishing emails Credit Union. Tl	t has been brought to our attention that various s have been sent referencing HawaiiUSA Federal The recent email states that multiple computers to loa into your HawaiIUSA account and failure to		
Where is the Password box? The Password box will appear on the next screen. This is another change we/ve applied to enhance	Log In Home		respond to the email will result in a suspension of your HawailUSA account. It contains spelling errors, invalid links, and unfamiliar phone number amongst many erroneous statements.			
your security.	<u>Sign Up Now!</u> Not a member? <u>Click here to apply for a loan.</u>	V4.14.7.0 <b>v</b>	ANY PART OF TH website at www	such an email, <b>DO NOT REPLY TO OR CLICK ON</b> <b>IFIE EMAIL</b> . For more information, please visit our w.hawaiiusafcu.com or call our Member Service 4300 (Oahu) or full free 800-379-1300 (neighbor islands and mainland).	~	
e	🗎 🕘 🕥	Internet			🔒 🧇 Internet 🛒	

#### Genuine bank login

https://hcd.usersonlnet.com/asp/US ERS/Common/Login/NettLogin.asp

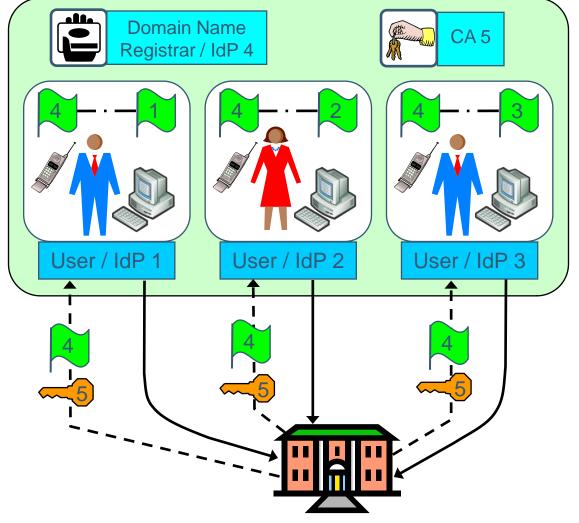
#### Fake bank login

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

#### **Identifier characteristics**

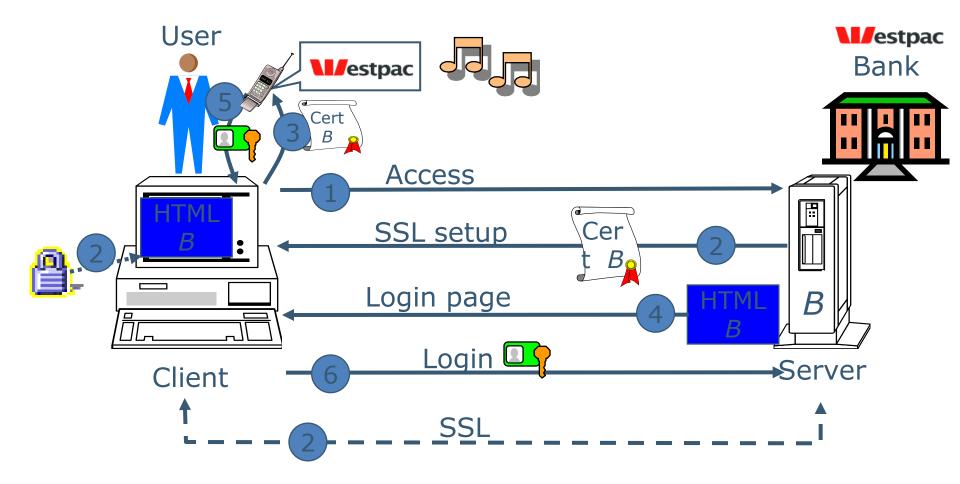
- Local or global
- Assigned by authority or self assigned
- Permanent or temporary
- Reassignable or not
- Persistent or not
- Human or machine readable

#### SP identity management User Centric model





# User-centric server authentication



### Unintended vulnerability

					_			
	🚰 Nordea - Betali	ng - Logg i	nn - Microsoft In	ternet Explorer				
	<u>Fil R</u> ediger <u>V</u> is	Favoritter	V <u>e</u> rktøy Hielp					
	Adresse Anttps://n	ettbetaling.bb	🖌 🄁 Gå til					
	Nordea	N	lettbank	/		<u>^</u>		
					? <u>Hielp</u>   @ <u>Kont</u>	<u>akt</u>   🖾 <u>E-po</u>		
	🔂 Daglig	Betaling	Aksjehandel	Betaling Utland	Fondshandel	Investortjen		
	Logg	Lo	ogg inn	≣				
A 11 A 1		N	ettbetaling					
All Norwegian banks have the same URL			Kontonummer:					
			Sikkerhe	tskode:				
			Husk å logge deg ut når du er ferdig. Hvis du er inaktiv i en					
		p	periode, vil du etter en tid automatisk bli logget ut.					
	<	,				>		
	ど Fullført			<u></u>	🥥 Internett	.::		
	Audun .	Jøsang		AFSecurity 14.08	.2008	22		

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

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



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



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





