InCommon®

A Welcome to Federated Identity

Nate Klingenstein, Internet2, USA

Prepared for the Matsuyama University, December 2013

www.incommon.org

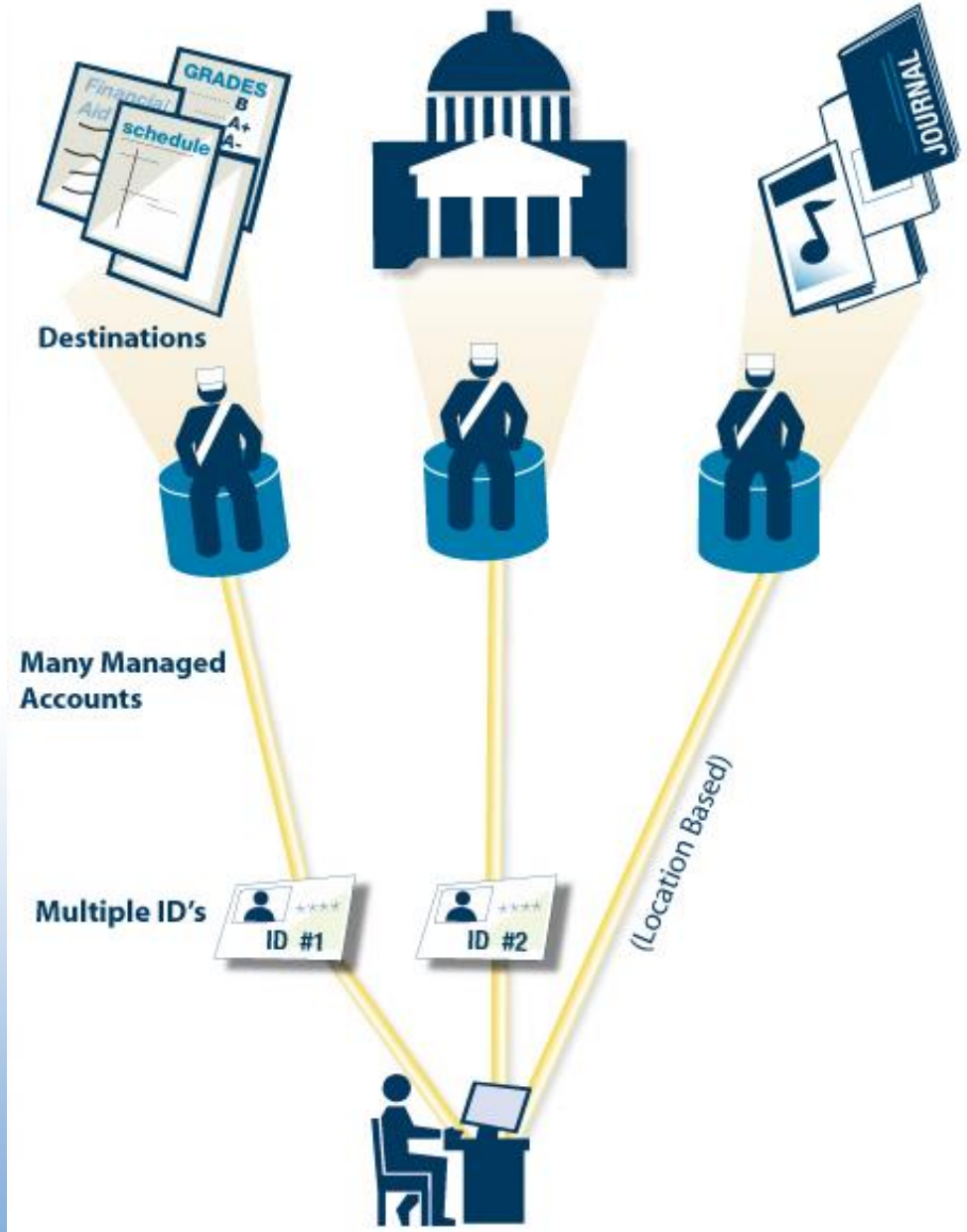
- Welcome to the presentation and thanks to our hosts
- What is Federated Identity?
- Why is Federated Identity valuable? Who is it valuable for?
- How you can get started using Federated Identity
- Challenges, especially the ones unique to libraries and Japan

Why is Shared Identity Important?

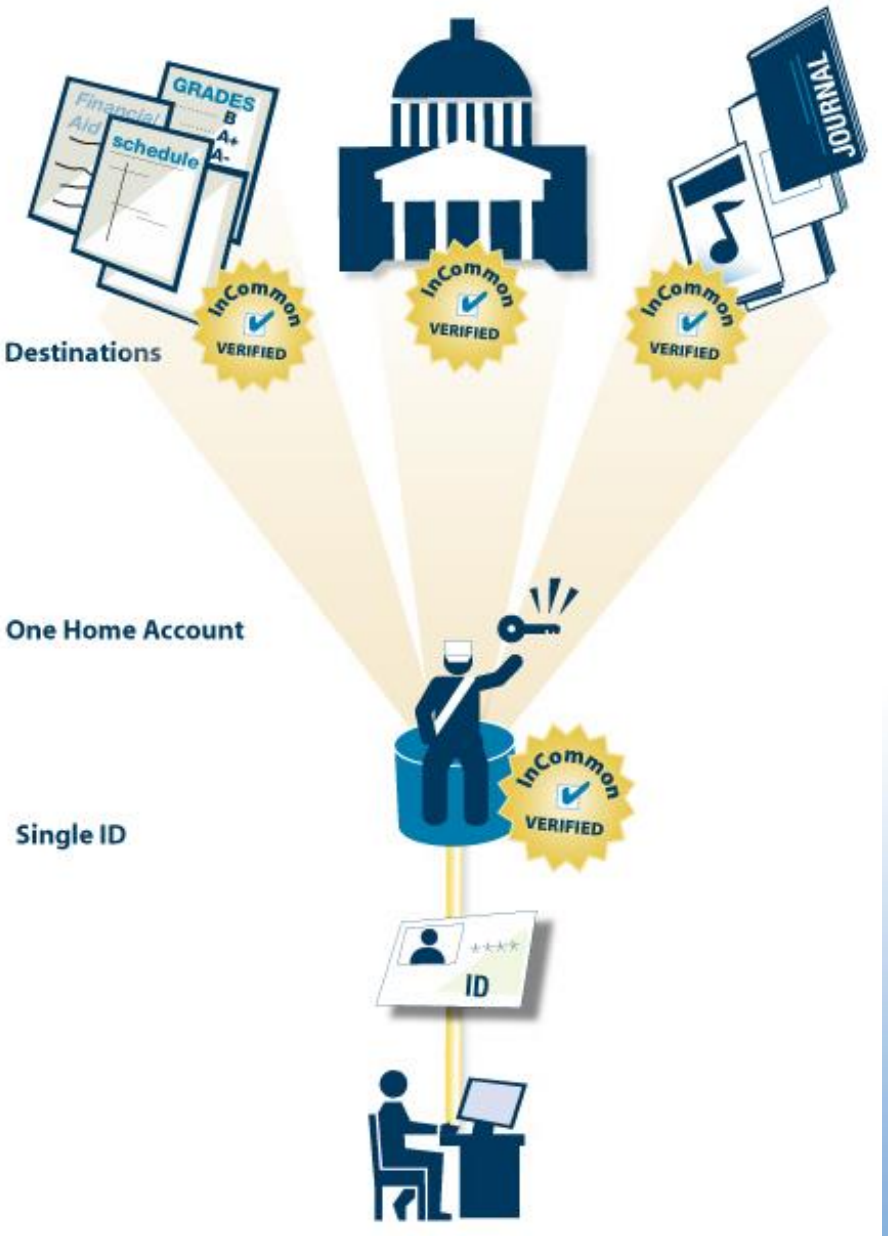
- Authoritative user data(attributes), expressed to a service
- Many applications, many users, not many credentials
  - People and applications are complicated, so any identity system that serves many of them will also be complicated
- Regulatory compliance
  - Excellent auditability of who, what, when, and how for data release
- Cloud services
  - SaaS, PaaS, IaaS, NET+

Federated Identity

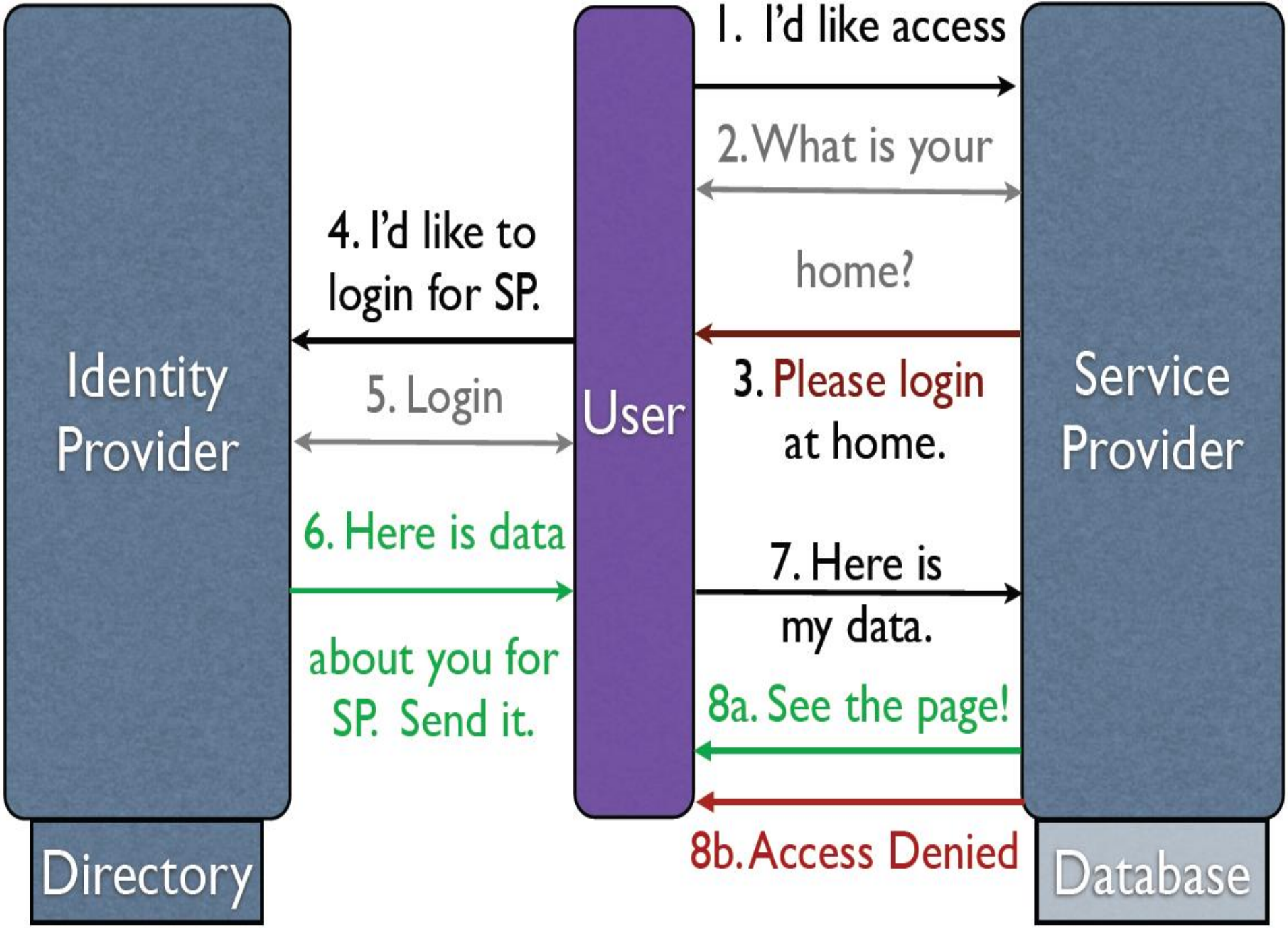
- Single Sign-On (SSO) with a variety of features added to fit a multi-domain world
  - More evolution of local SSO systems like Kerberos than innovation
- Single Log-Out(SLO)... becomes a very difficult problem
- Provisioning
  - Can be a challenge, depends on the application
- Federations scale trust and simplify operations
  - Distinct from federated identity, as you'll find out with some vendors



1. Tedious user registration at all resources
2. Unreliable and outdated user data at resources
3. Different login process at each resource
4. Many different passwords
5. Identity provider may need to support multiple custom authentication methods and/or be asked for access to its identity database



1. Single sign on
2. Services no longer manage user accounts & personal data stores
3. Reduced help-desk load
4. Standards-based technology
5. Home organization and user controls privacy


1. I'd like access
2. What is your
home?
3. Please login
at home.
4. I'd like to
login for SP.
5. Login
6. Here is data
about you for
SP. Send it.
7. Here is
my data.
8a. See the page!
8b. Access Denied
Identity
Provider
User
Service
Provider
Directory
Database

Federated Identity Protocols

- We don't want applications or users to know anything about federated identity protocols
  - Implementations of security software by non-specialists almost always has vulnerabilities, sometimes serious vulnerabilities
  - Hardwiring an application to a protocol means the application must change every time the protocol changes
  - Users want it to “just work”
- SAML 2.0, OAuth 2.0, legacy SAML 1.1/Shibboleth 1.x, some legacy OpenID, eventually OpenID Connect
- Many dead federated identity protocols like IMI/Infocards, WS-*(except for ADFS), Liberty Alliance, etc.

Federations

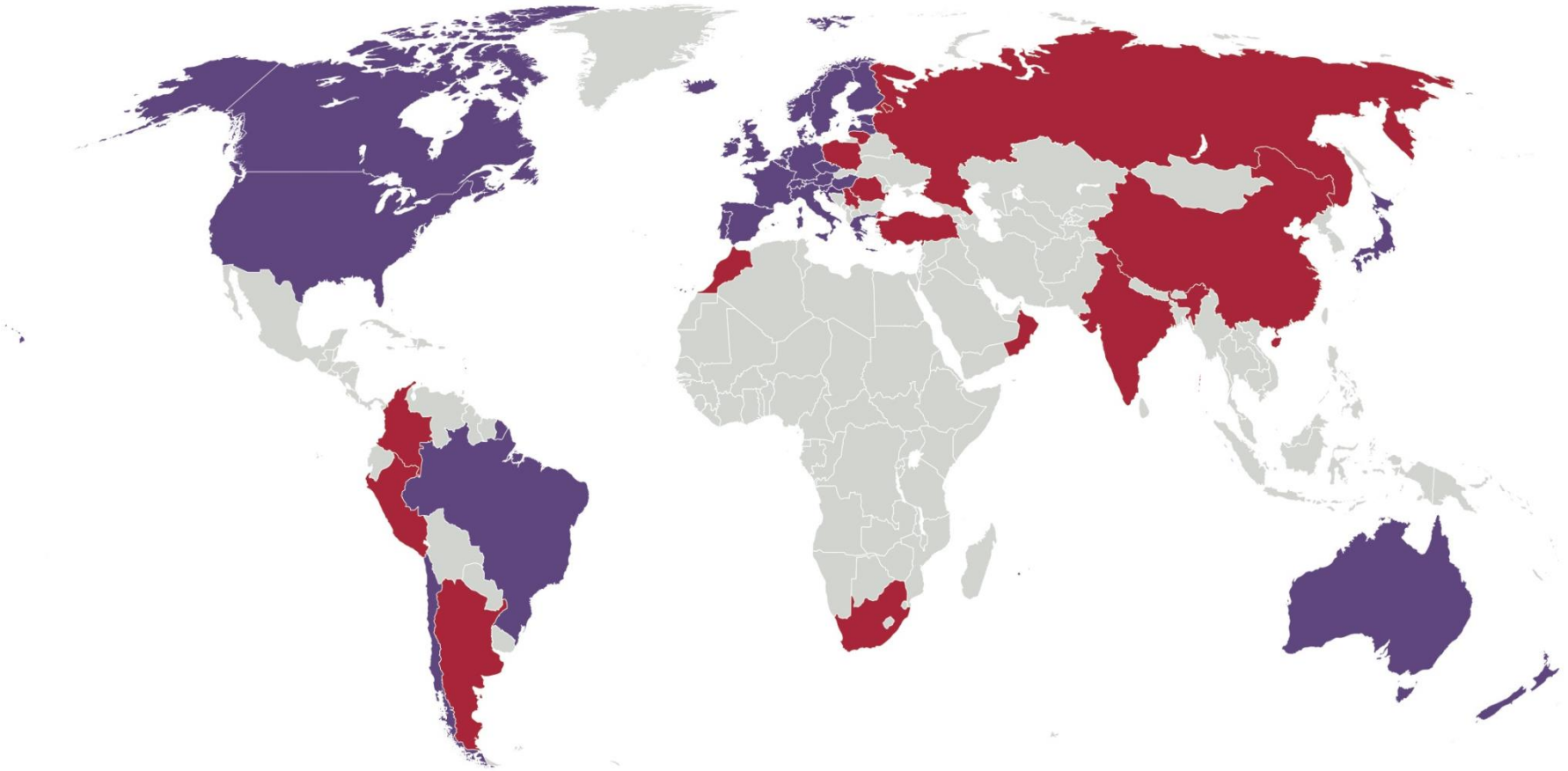
- A federation is not necessary for federated identity
  - It makes federated identity easier, more scalable, and more maintainable
- Typically one federation per sector, per country
  - This is usually because of different privacy and data protection laws
  - There are also cultural differences
  - We're working hard on connecting countries, too
- InCommon in the USA
- GakuNin in Japan
- 7125 Entities registered in 35 Federations

Federations

- Federated identity is happening everywhere – business to business, business to consumer, medical, defense, aerospace, etc.
- But federations are only really happening in academia
- Business and consumer federated identity tend to use bilateral relationships
  - Both of these are smaller scale than academic federation
  - Consumer world: only a few IdP's(Facebook and Twitter and Google)
    - We already have many thousands
  - Business world: tight business relationships and contracts already exist

Research and Education Identity Federations

REFEDS



Identity Federations in production

AT	ACOnet Identity Federation	ES	SIR	NL	SURFconext		
AU	Australian Access Federation AAF	FI	Haka	NO	FEIDE		
BE	Belnet R&E Federation	FR	Fédération Éducation-Recherche	NZ	Tuakiri New Zealand Access Federation		
BR	CAFe	GR	GRNET	PT	RCTSaai		
CA	Canadian Access Federation CAF	HR	AAI@EduHr	SE	SWAMID		
CH	SWITCHaai	HU	eduID.hu	SI	ArnesAAI Slovenska		
CL	COFRe	IE	Edugate	UK	UK Access Management Federation for Education and Research		
CZ	eduID.cz	IT	IDEM	US	InCommon		
DE	DFN-AAI	JP	GakuNin	int	IGTF		
DK	WAYF	LV	LAIFE				
EE	TAAT						

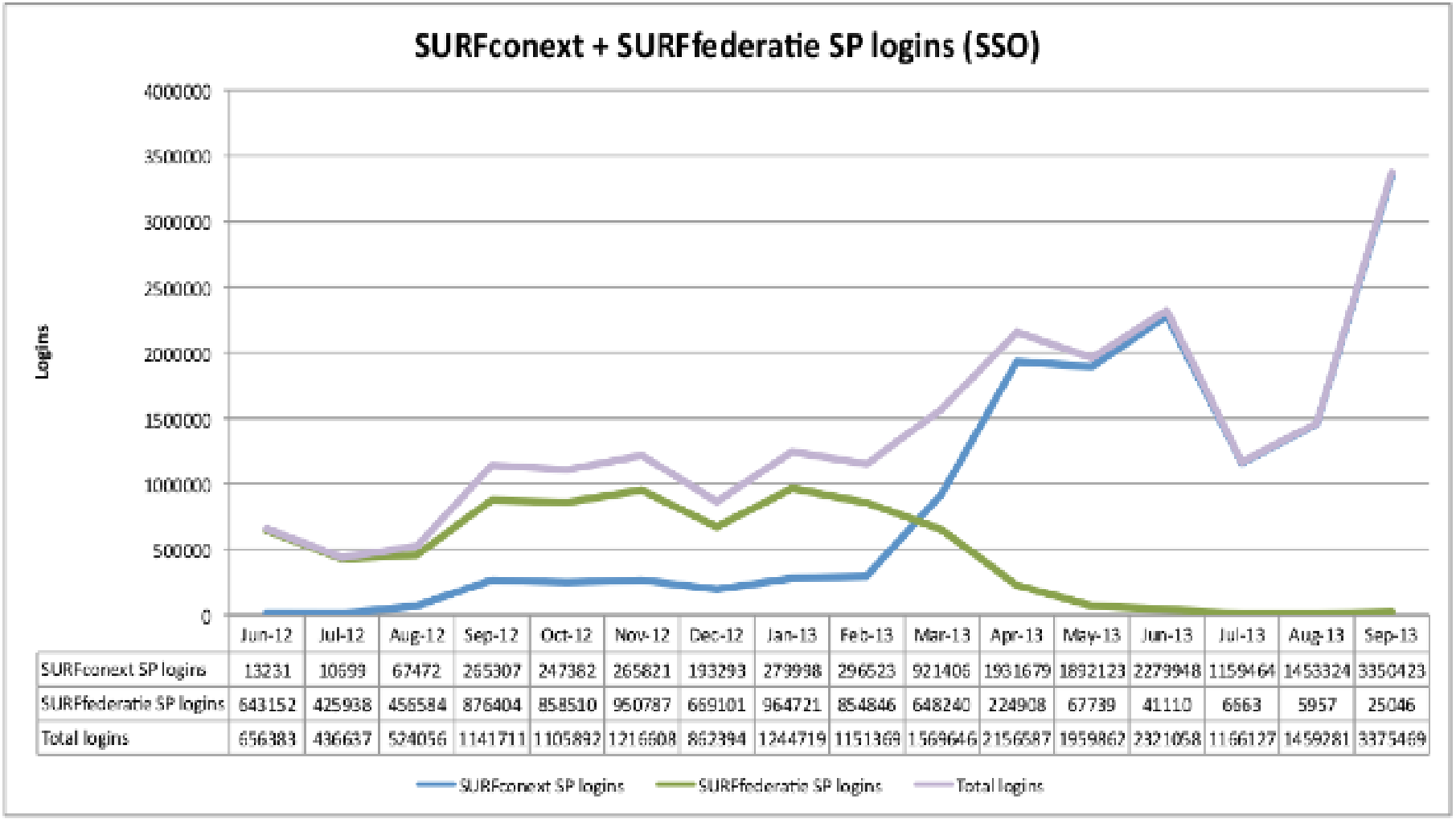
Identity Federations in pilot

AR	MATE	PL	PIONIERId
CN	CARSI	RO	RoEduNet Federation
COL	COLFIRE	RS	iAMRES
IN	INFED	RU	ΦEDUrus AAI
LT	LEFT	TR	YETKİM
PE	INCA	ZA	SAIF
MA	eduIDM		
OM	Oman Knowledge ID Federation		

This map is intended to provide a high-level overview of countries with identity federations.

Last update: 14 October 2013

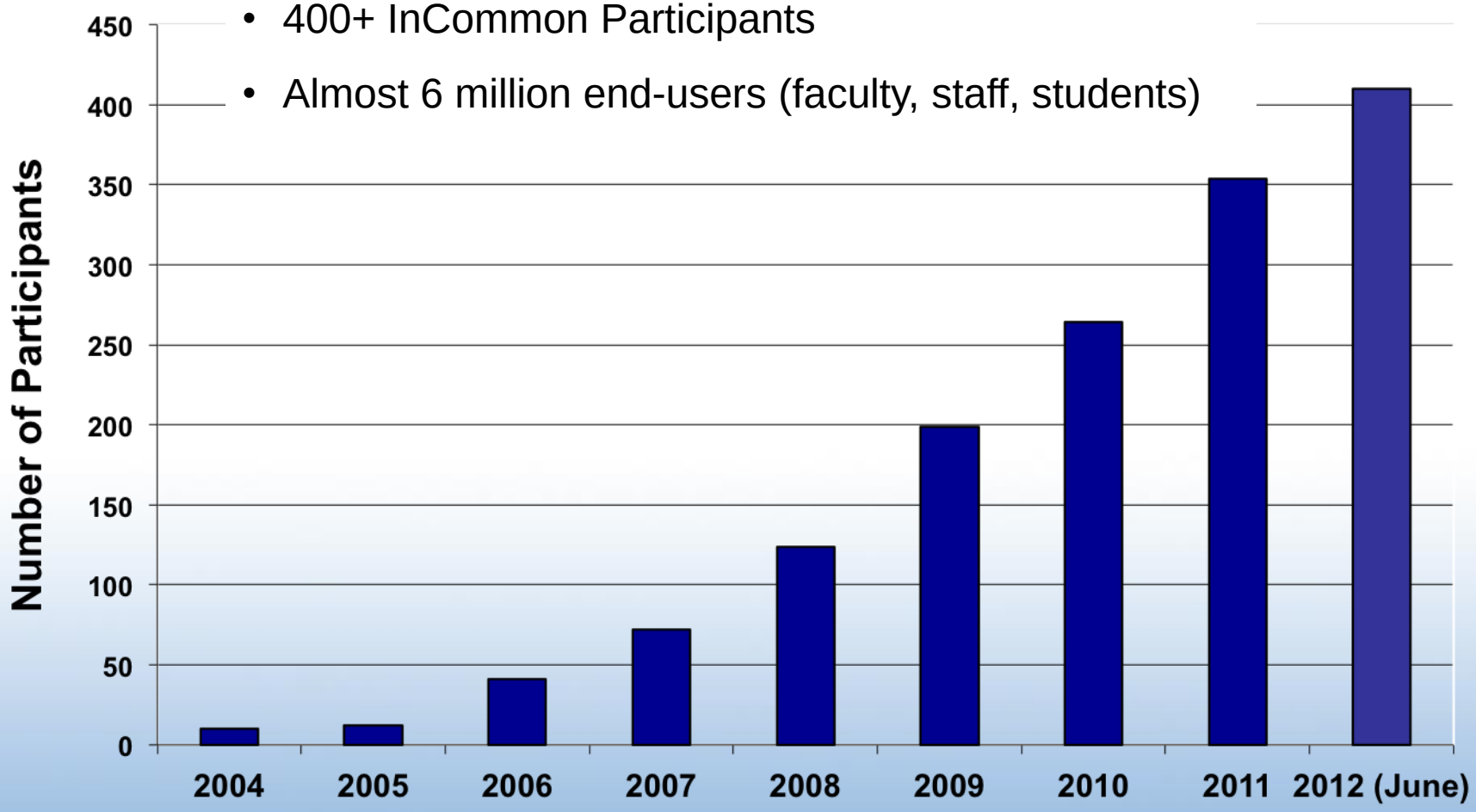
Really Growing!



	Jun-12	Jul-12	Aug-12	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13
SURFconext SP logins	13231	10699	67472	265307	247382	265821	193293	279938	296523	921406	1931679	1892123	2279948	1159464	1453324	3350423
SURFfederatie SP logins	643152	425938	456584	876404	858510	950787	669101	964721	854846	648240	224908	67739	41110	6663	5957	25046
Total logins	656383	436637	524056	1141711	1105892	1216608	862394	1244719	1151369	1569646	2156587	1959862	2321058	1166127	1459281	3375469

InCommon Participants Year-by-Year

- 400+ InCommon Participants
- Almost 6 million end-users (faculty, staff, students)



More Recent InCommon Numbers

Now almost 600 participants

Now has 400+ university members from the USA

More than 7.5 million users(staff, students, faculty)

29 Government agencies, labs, research centers

156 Corporate Sponsored Partners

http://www.incommon.org/participants/

Federated Identity Benefits: Users

- Fewer credentials
- Single sign-on
- Privacy and control over identity data release(when appropriate)
- Access to services from anywhere, on any device, on any network
- A more consistent experience for services hosted by the organization or in the cloud

Federated Identity Benefits: Application

- Applications no longer need to authenticate users themselves
  - Saves time, especially with password resets, which means it saves money
  - Better access control than, for example, IP addresses
- Applications hosted anywhere are better integrated with the organization
  - Great for cloud services, or online library services
- Applications can get trusted user attributes too
  - You know who's really a student, or who's really a graduate
- If a user does something bad, you can always work with the school to figure out exactly whose account it was

Federated Identity Benefits: School

- The university can choose to use a wide variety of cloud services not directly owned or hosted by the university
  - All services can be connected through a single point that has been designed for diverse services, reducing the amount of infrastructure you must run
    - IP address ranges, VPN's, etc. become more flexible and disconnected from service authentication
- A very good idea of which user data is going where
  - Makes audits much less painful
- Positions you to support bring-your-own-device and bring-your-own-credential

How can I get started using federated identity?

- This used to be a very difficult question because there were few partners to talk to
  - The “chicken and egg” problem – which comes first
  - Network effect: your implementation becomes more and more useful as you can talk to more and more partners
- Today, there are thousands of services offered with federated identity that are interesting
  - Office 365, Google Apps
  - Canvas, Moodle, BlackBoard, Desire2Learn, Webassign
  - Elsevier, Ezproxy, Ex Libris, HighWire Press, JSTOR, ProQuest

Getting Started with Federated Identity

- Get engaged with GakuNin
- Set up your own identity provider
  - A variety of free open-source software can help you do this
  - simpleSAMLphp, Shibboleth
- Get connected with some applications
  - The “killer” application will be different everywhere
    - It's cloud applications in most countries today

Some Examples from the User Perspective

- The hardest part of federated identity is building a good user experience
- From small to large:

https://staff.internet2.edu/communications/ (and internet2.box.com)

https://shibtest.hampshire.edu/shibtest/

http://www.sciencedirect.com/ and http://onlinelibrary.wiley.com/

https://wiki.shibboleth.net/

http://www.cartoonnetwork.com

https://login.microsoftonline.com/

Challenges

- Finding the staff and money to run an identity provider
  - In Japan, researchers and staff are often conflated
    - Staff members are measured by research publication
      - Nowhere else in the world
  - Universities have little money for staff and services
- Building the user database that powers federated identity
  - LDAP, SQL
    - Building it centrally for an entire university
  - Universities in the Americas, Europe, and Australia already had this done, which made our job much easier

Challenges

- Adding SSO to local applications
  - Many of these applications already have integration code written by other people, but they haven't been deployed with an SSO system
- Finding the right partner applications for your university
  - Many great cloud applications exist for other countries, and probably for Japan too
- User experience
  - This is mostly a problem for the service

Thank you!

Nate Klingenstein
ndk@internet2.edu