

Cnlab / CSI 2013

Social Business – endlich produktiv!

Social Business und Security



User name

Password

How do I log on to another domain?



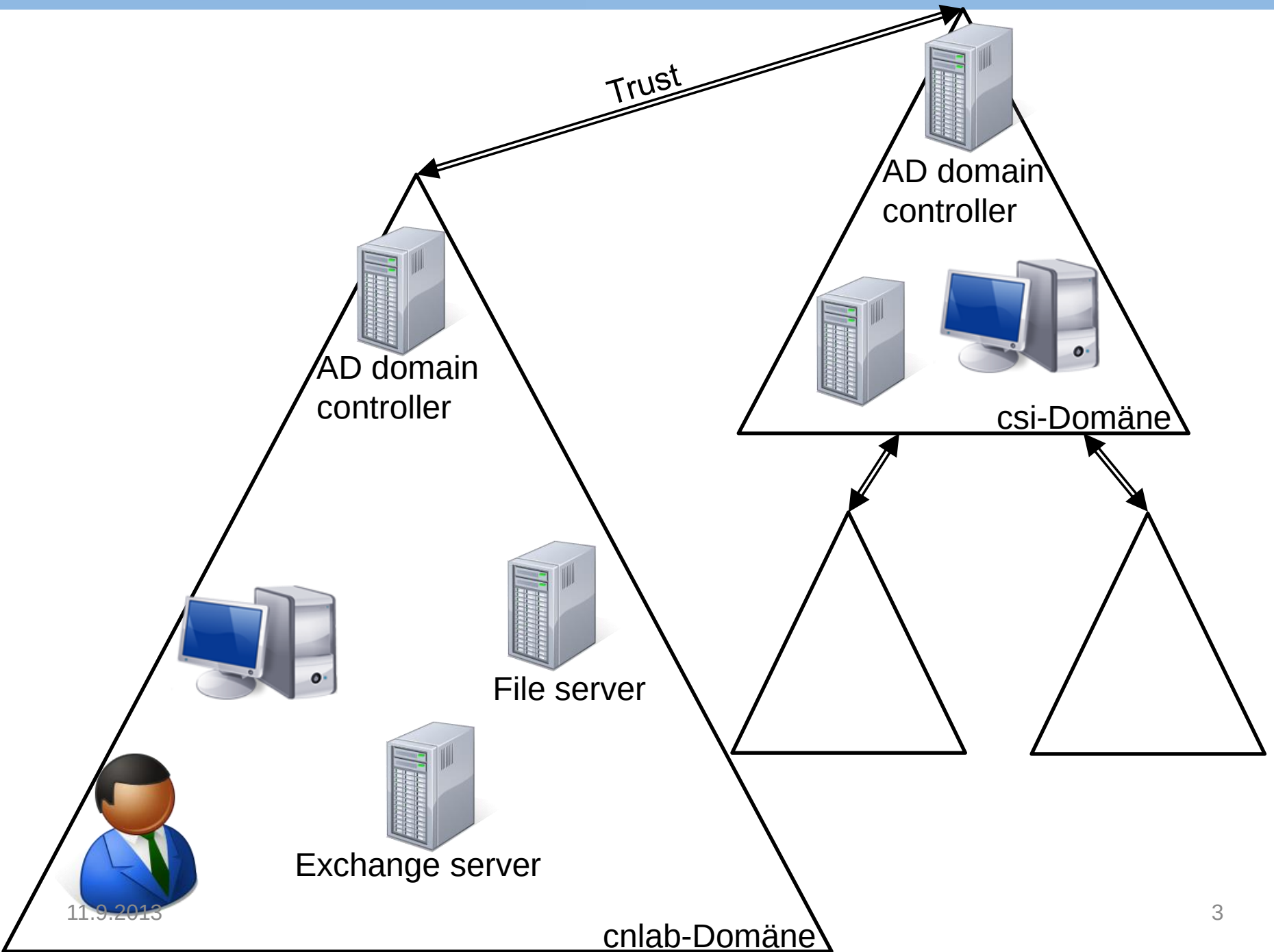
csi\

Password



Log on to: csi
How do I log on to another domain?

Switch User



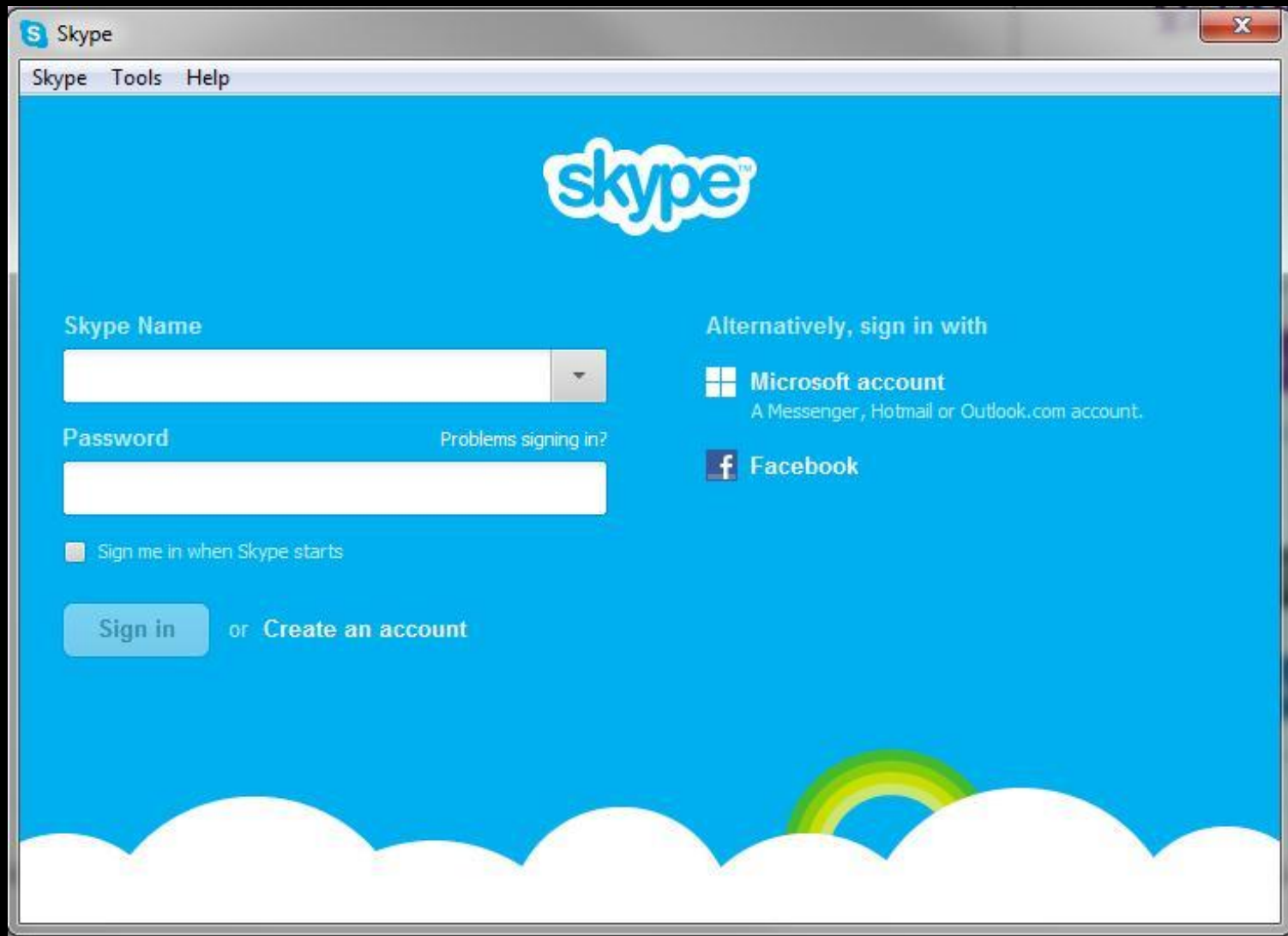
Yahoo! makes it easy to enjoy what matters most in your world.

Best in class Yahoo! Mail, breaking local, national and global news, finance, sports, music, movies and more. You get more out of the web, you get more out of life.

☐ Keep me signed in[Sign In](#)[I can't access my account](#)
[Help](#)

OR

[Facebook](#)[Google](#)[Create New Account](#)



Funding longer lives 

Food security 

Climate/natural disasters 

Sustainable energy 

Other 

[+ Add story](#)

Login

E-mail

Password

[Go](#)

Create user profile

Display name*

Email address*

Password*

Your password must be at least 8 characters long and contain both upper and lower case letters and at least 1 number

Confirm password*

Enter your password again

☐ Please tick to confirm you have read and agreed to the [Legal Notice](#) and [Privacy Policy](#)

Captcha*



[Go](#)

* Mandatory field



Sign in with Facebook



Sign in with Twitter



Sign in with LinkedIn



Sign in with Google

- Alle diese Beispiele zeigen «Federations»
- Was ist Federation?
- Wie funktioniert Federation?

Identity Federation

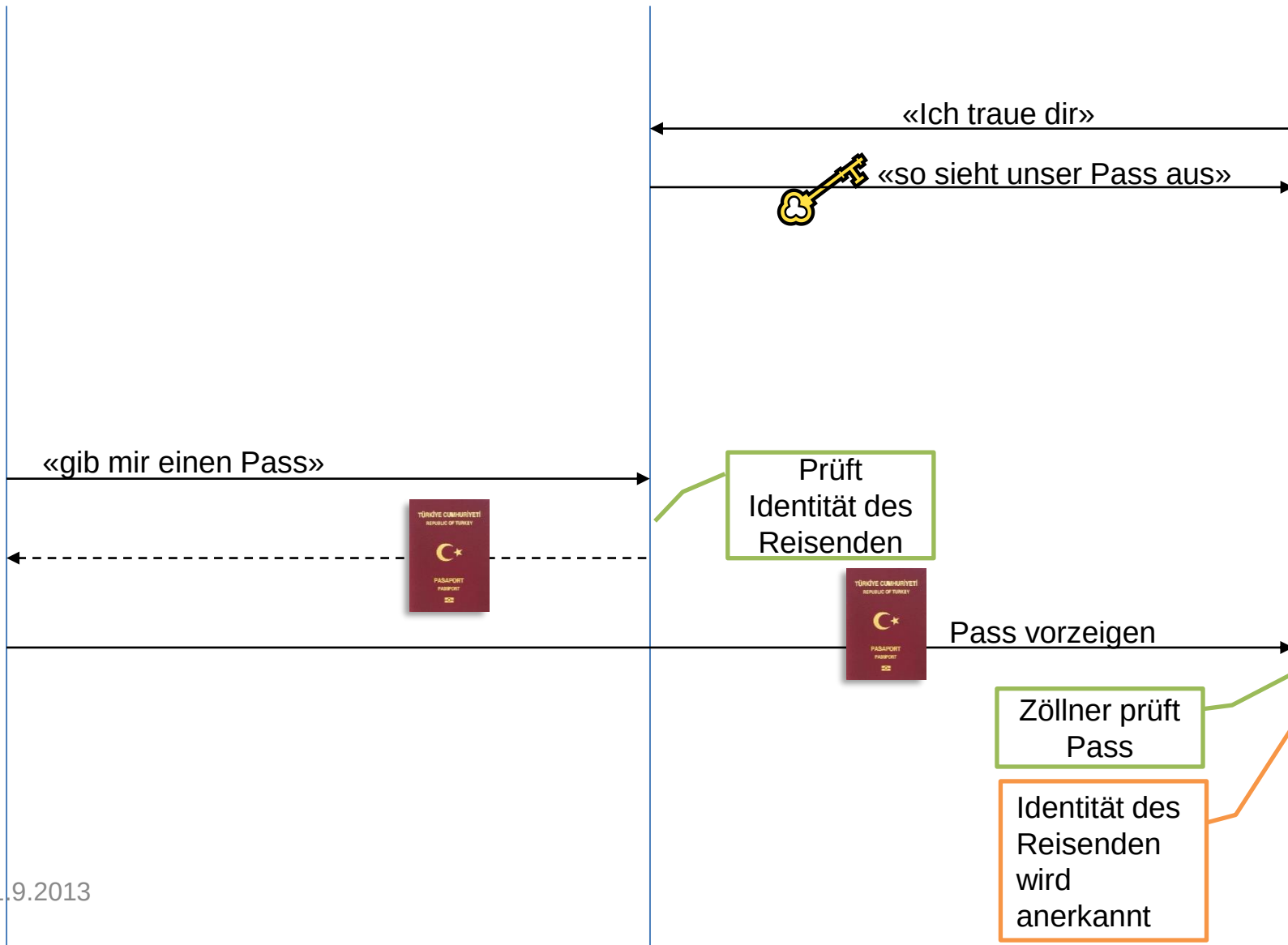


Authentisierung mittels Pass

Reisender

Türkische Passbehörde

Schweizer Zoll

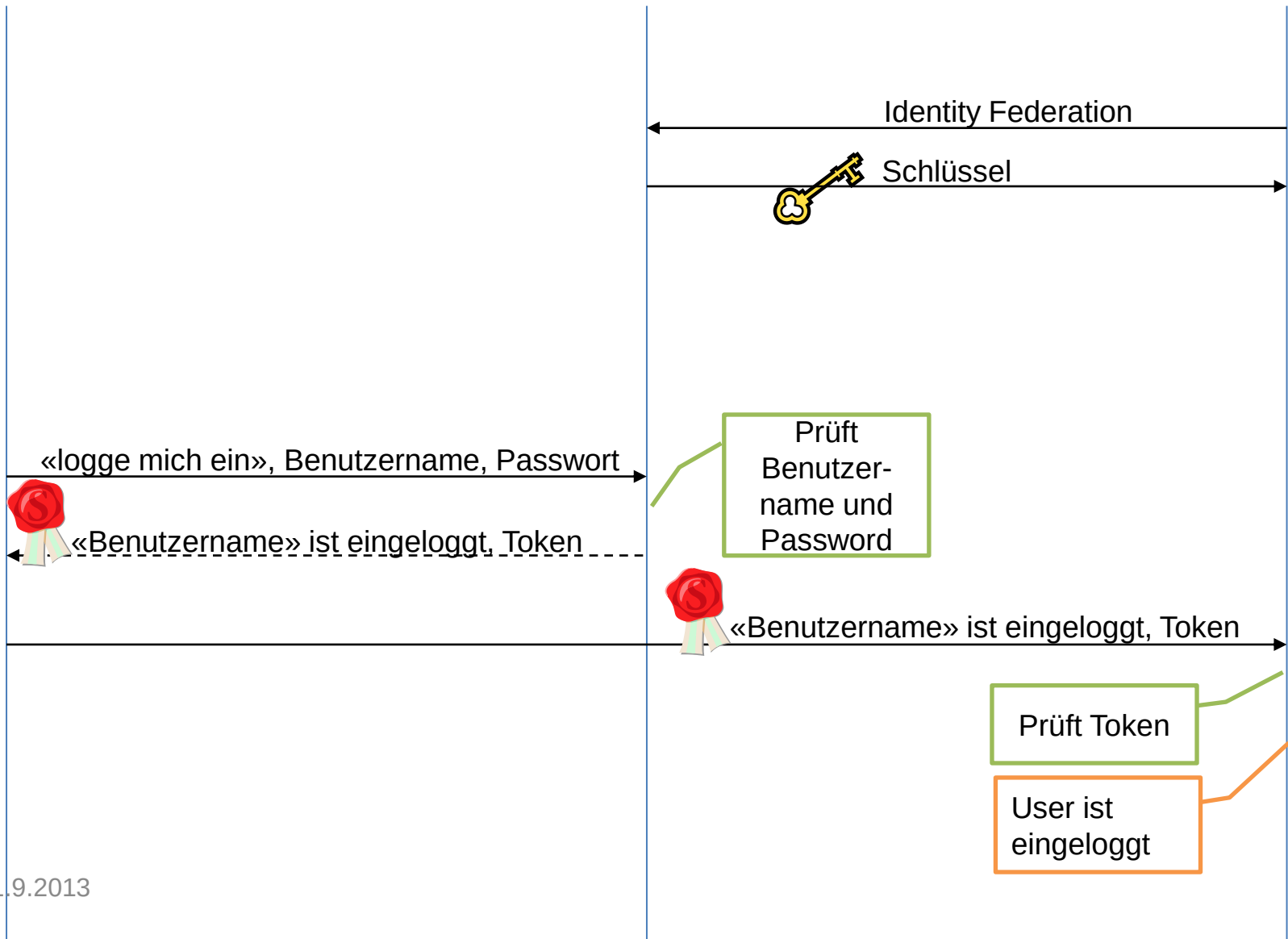


Authentisierung mittels SAML

User

Identity Provider

Service Provider



The screenshot shows a web browser window with the URL <https://idp.hslu.ch/idp/Authn/UserPassword>. The page header includes the Lucerne University of Applied Sciences and Arts logo, the text "HOCHSCHULE LUZERN", and the "SWITCHaai" logo. Below the header are links for "About AAI", "FAQ", "Help", and "Privacy". The main section is titled "SWITCHaai Login" and contains a login form. The form instructs the user to "Enter your username and password below, then click on the Login button to continue." It features two input fields: "Username:" and "Password:". Below the password field is a "Login" button. At the bottom of the form, there are two links: "Lost your password?" and "Change your password".

Lucerne University of Applied Sciences and Arts

HOCHSCHULE LUZERN

SWITCHaai

[About AAI](#) | [FAQ](#) | [Help](#) | [Privacy](#)

SWITCHaai Login

Enter your username and password below, then click on the **Login** button to continue.

Username:

Password:

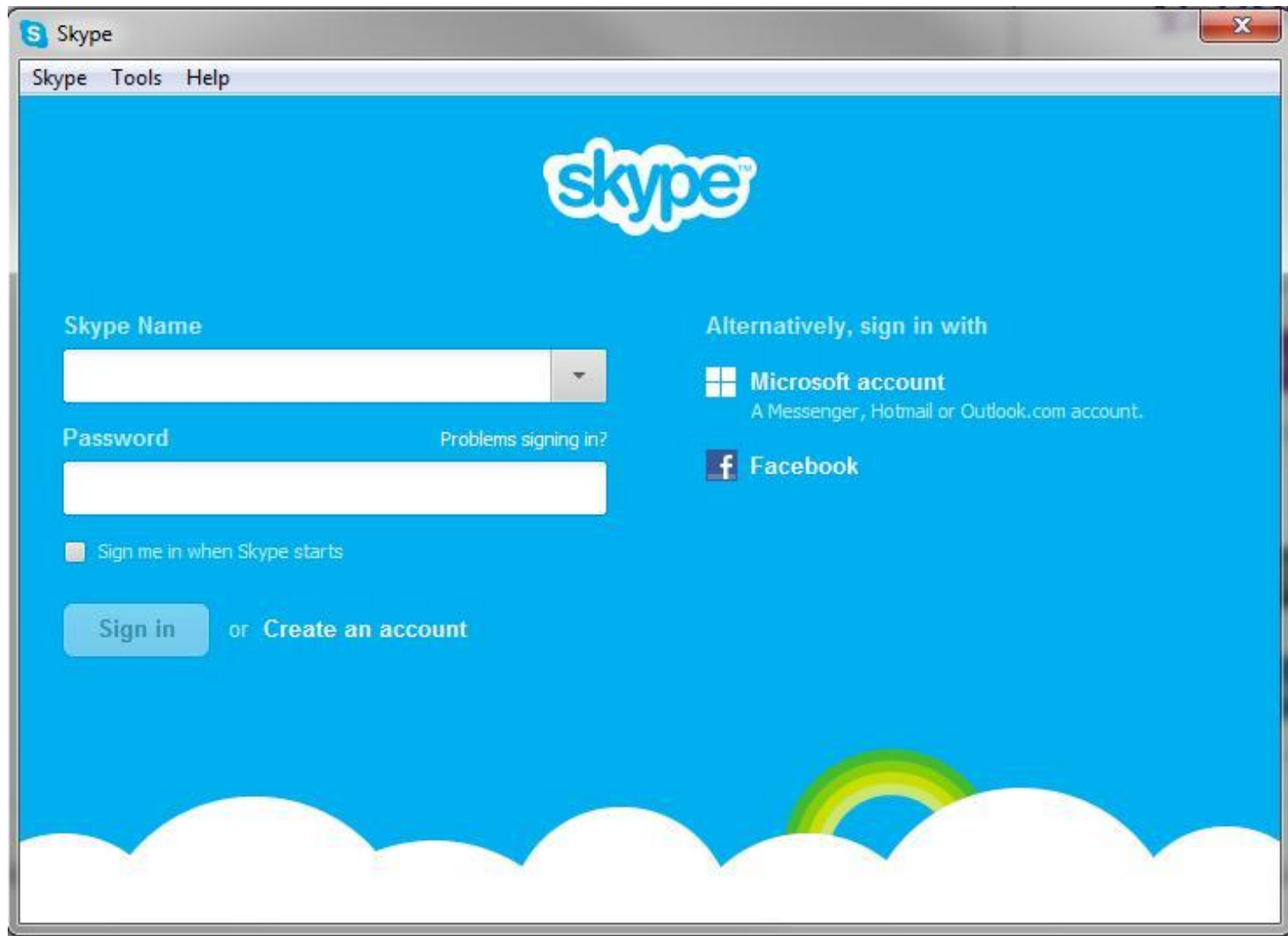
Login

[Lost your password?](#) | [Change your password](#)

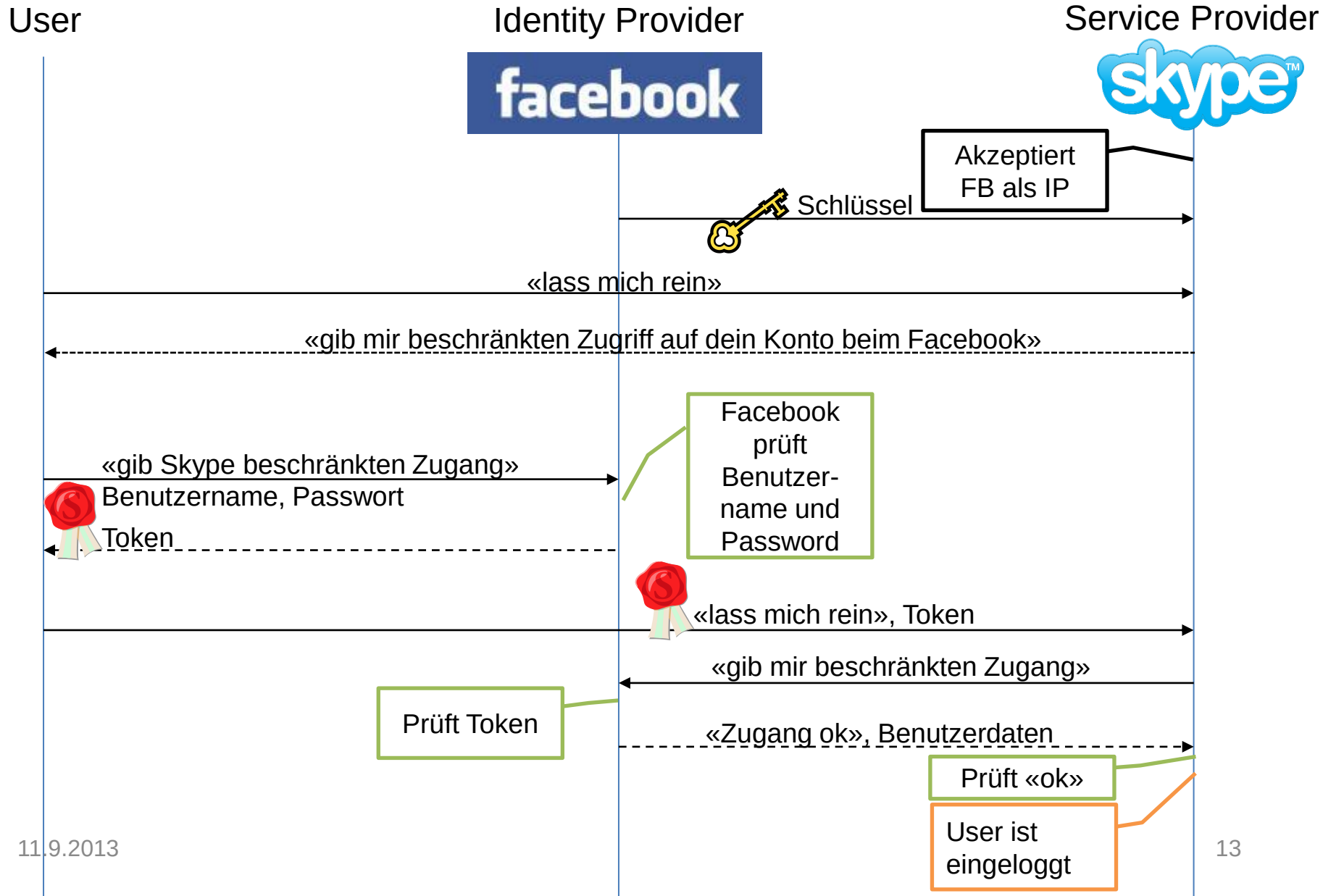
Auch verwendet für

- Bibliotheken
- Zugang zu Journals
- Wohnungsvermittlungen
- e-Learning Plattformen
- Stellen- /Praktikavermittlung
- etc.

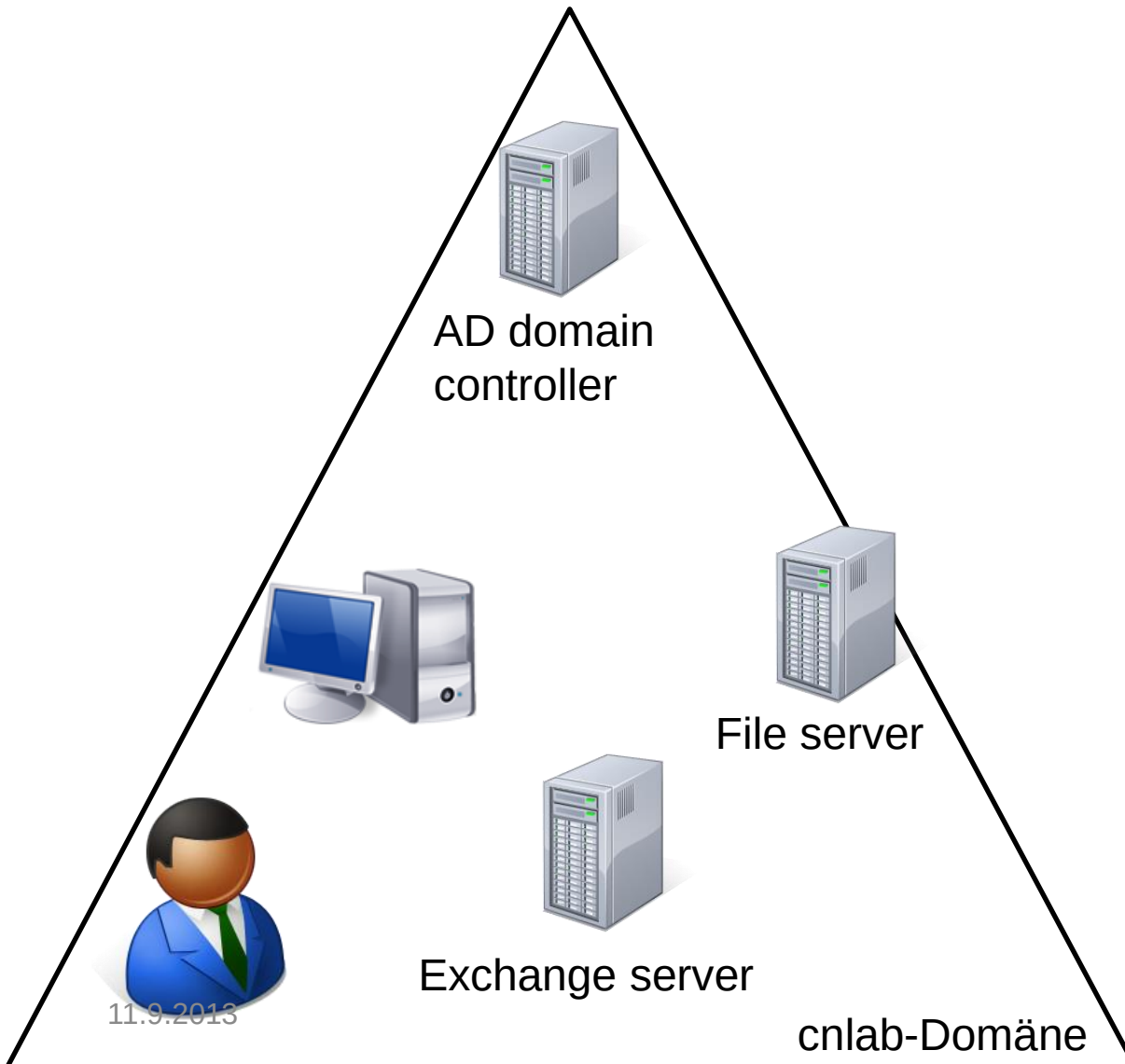
der Hochschulen.



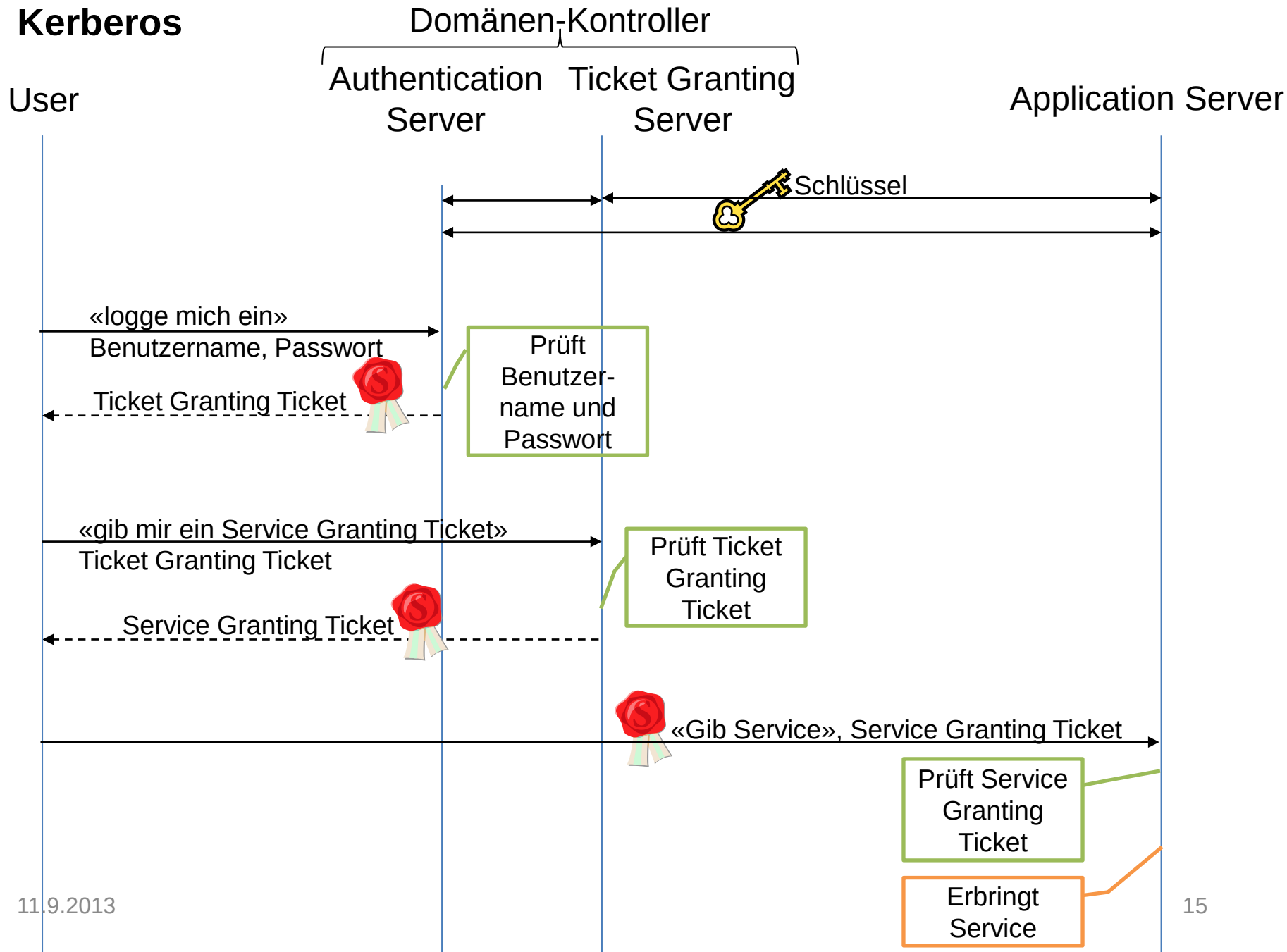
Authentisierung mittels OAuth



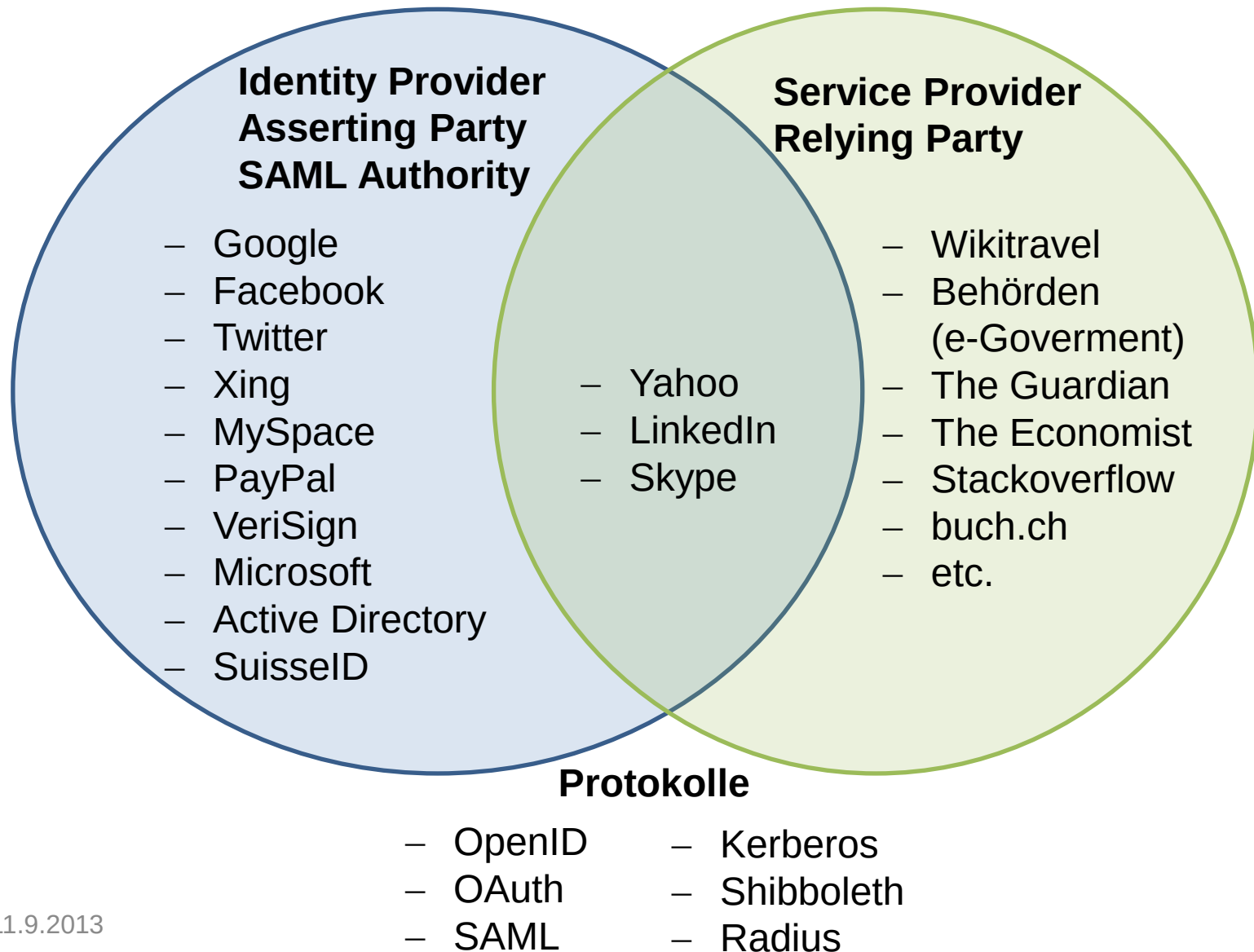
Kerberos: eine Art Federation innerhalb der Domäne



Kerberos



Begriffe zu Identity Federation



Wer bietet was im Internet?

Service Provider	Google	YAHOO!	facebook	twitter	LinkedIn	XING	Apple ID	skype	Microsoft Account	The Economist	Stackoverflow	The Guardian	PC Advisor	Open Minds (Swiss Re)
------------------	--------	--------	----------	---------	----------	------	----------	-------	-------------------	---------------	---------------	--------------	------------	-----------------------

Identity Provider

Google	✓	✓								✓	✓	✓	✓	✓
YAHOO!		✓								✓	✓		✓	
facebook		✓	✓		✓			✓		✓	✓	✓	✓	✓
twitter				✓						✓		✓	✓	✓
LinkedIn					✓					✓			✓	✓
XING						✓								
Apple ID							(✓)							
skype								✓						
Microsoft Account								✓	✓	✓			✓	

✓	✓									✓	✓	✓	✓	✓
	✓									✓	✓		✓	
	✓	✓		✓				✓		✓	✓	✓	✓	✓
				✓						✓		✓	✓	✓
					✓					✓			✓	✓
						✓								
							(✓)							
								✓						
								✓	✓	✓			✓	

SuisseID als Identity Provider



- E-Portal verschiedener Gemeinden (Aesch, Altstätten, Amden, Amriswil, Andwil, Arbon, Au, B...)
- Behörden
- Brack Electronics
- buch.ch
- Post
- KPT
- SECO

Wird normalerweise nicht als Federation betrachtet, ist aber sehr ähnlich (vergleiche Pass).

Chancen

- Vereinfachtes ID-Management für den User
- Vereinfachtes Authentisierungsverfahren für den Service Provider
- Komfort durch SSO

Risiken

- Sicherheitsmängel beim IP geben Zugang zum Service Provider
- Missbrauch von verwaisten Zugängen
 - Fehlende Sperrung
 - Fehlender Passwortwechsel
- Unerwünschtes Verhalten des Identity Provider:
 - muss mich korrekt authentisieren
 - darf nicht auf meine Service Provider zugreifen
 - darf Dritten keinen Zugang auf meine Service Provider geben
- Problem der Verkettung
 - mit einem erfolgreichen Angriff erlangt der Angreifer Zugang zu diversen Diensten

Danke

Esther Hänggi
esther.haenggi@cnlab.ch
+41 55 214 33 36

Zürich, 11. September 2013