Shibboleth authentication for Sync & Share - Lessons learned

Enno Gröper

Abteilung 4 - Systemsoftware und Kommunikation
Computer- und Medienservice
Humboldt-Universität zu Berlin

30 Jan 2018

Overview

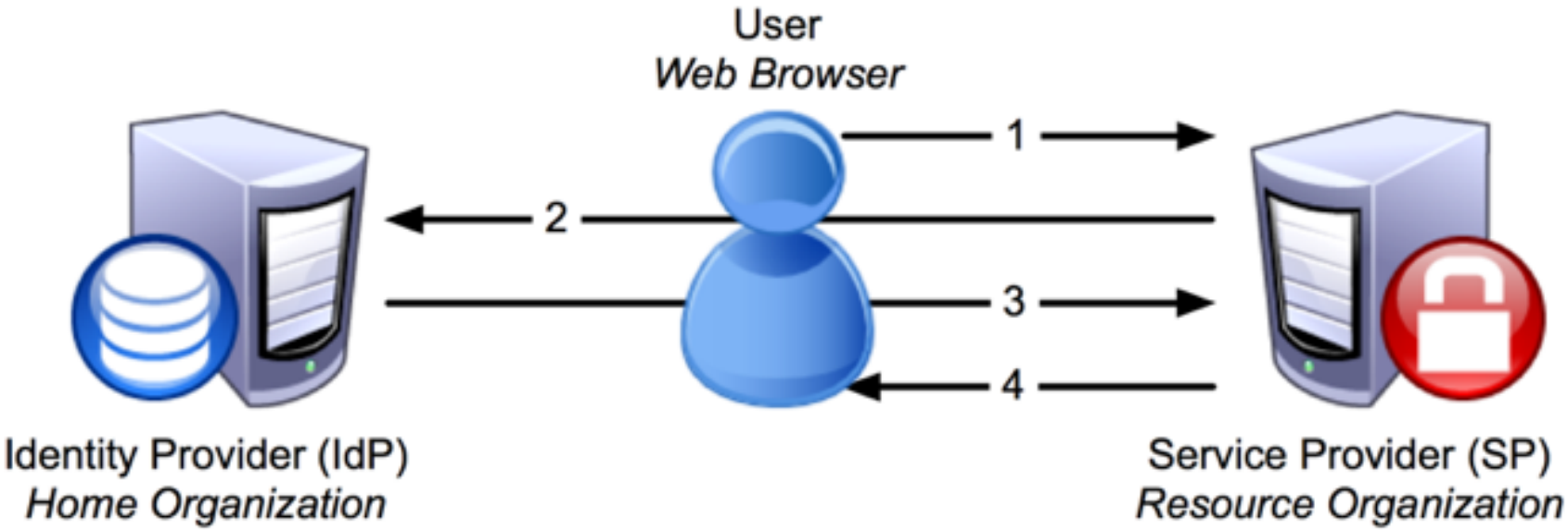
- Introduction to Shibboleth
- Integrating Shibboleth into Sync & Share service
- What about Logout?

Overview

- Introduction to Shibboleth
- Integrating Shibboleth into Sync & Share service
- What about Logout?

What is Shibboleth?

- Authentication architecture with focus on privacy
- Service provider gets only the necessary information (attributes) about the user
- No user credentials at the service provider
- Based on Security Assertion Markup Language (SAML)



source: CC BY-SA 3.0 https://wiki.shibboleth.net/confluence/display/CONCEPT

Why (not) Shibboleth?

Pro:

- Don't have to worry about the users credentials
- Possibility to reach many (university) users using federations (national like DFN-AAI and worldwide like EduGAIN)
- Single Sign On system

Contra:

- Currently no way for SP to query user status
  - Did the account get deleted?
  - Did it get locked?
- Usually needs a webbrowser (no CLI or API)

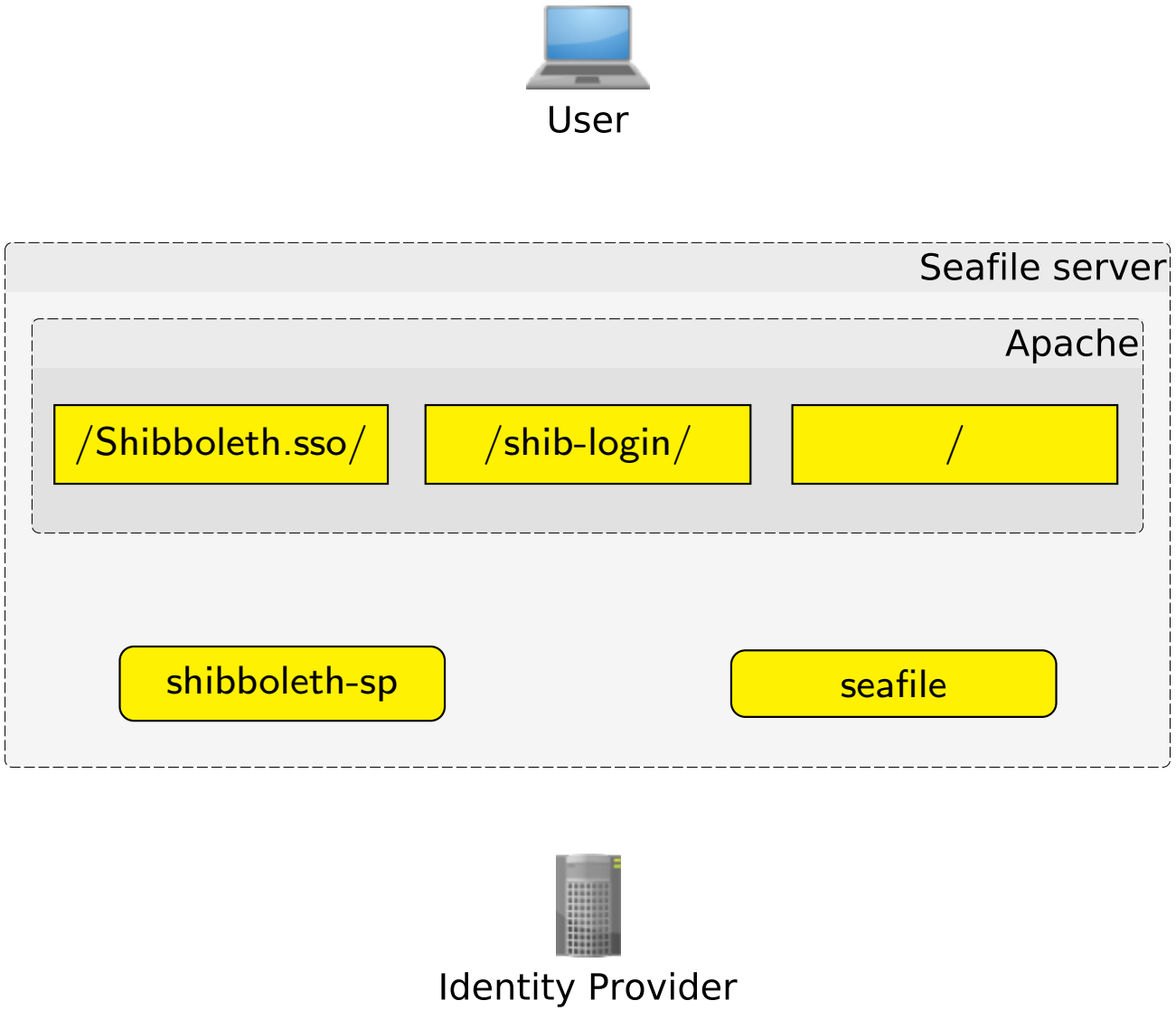
Overview

- Introduction to Shibboleth
- Integrating Shibboleth into Sync & Share service
- What about Logout?

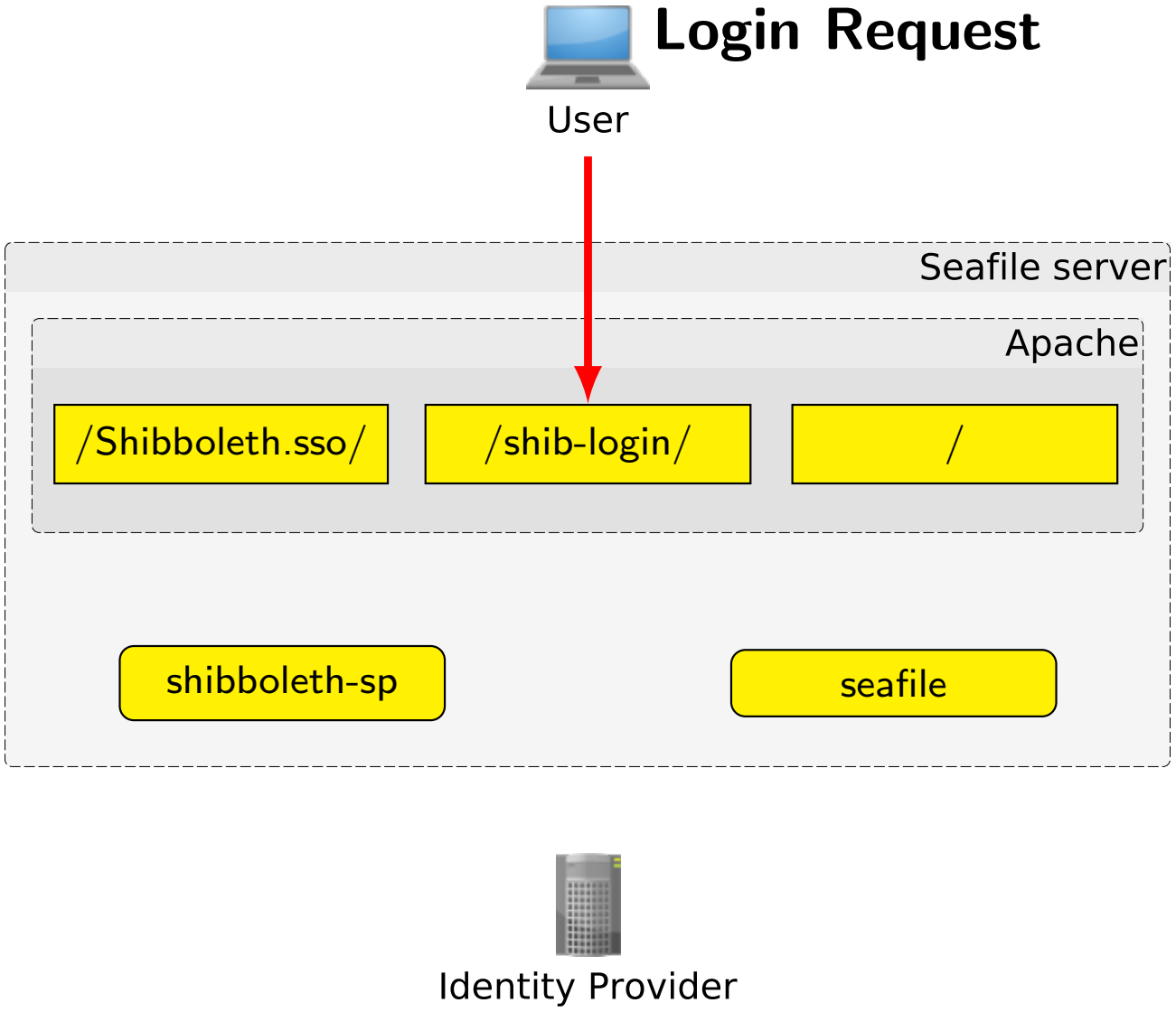
How to use Shibboleth in CSS service

- Use Shibboleth-capable Webserver (Apache preferred)
- Install and configure shibboleth-sp
- Configure shib-protection in Webserver
- Enable Shibboleth support in Webapp
- Register your SP with your IdP (send metadata to IdP admin)

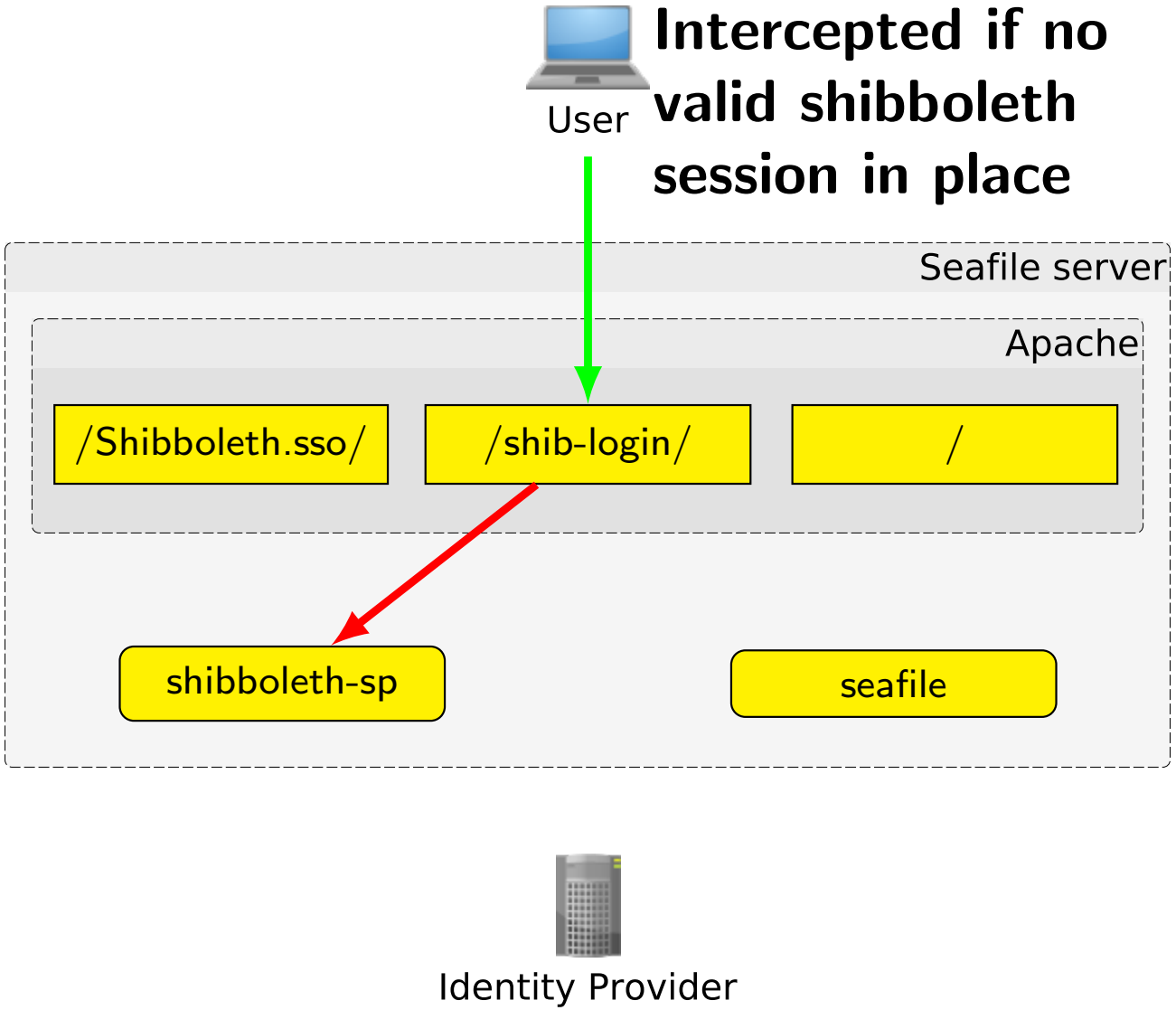
Shibboleth login flow



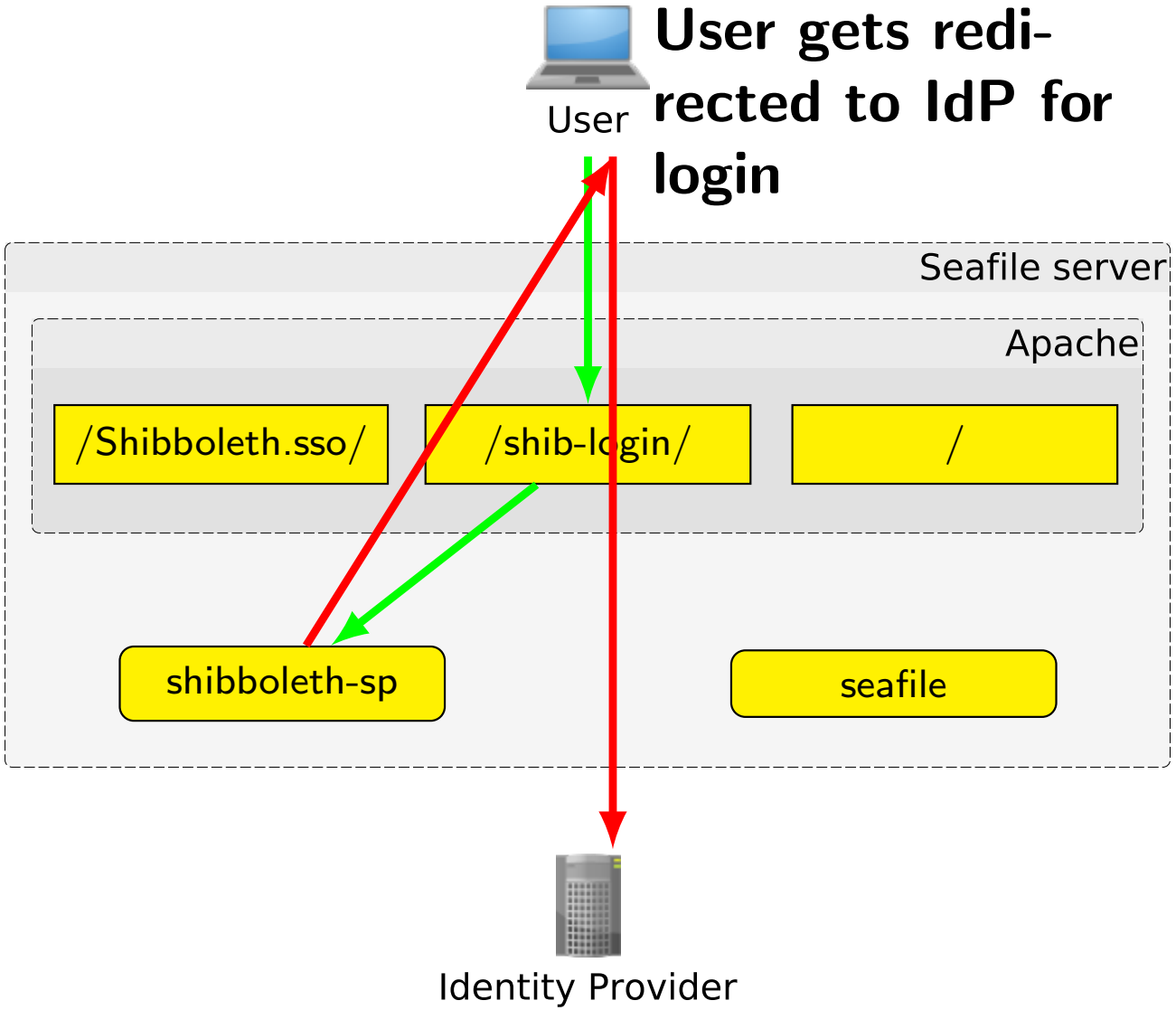
Shibboleth login flow



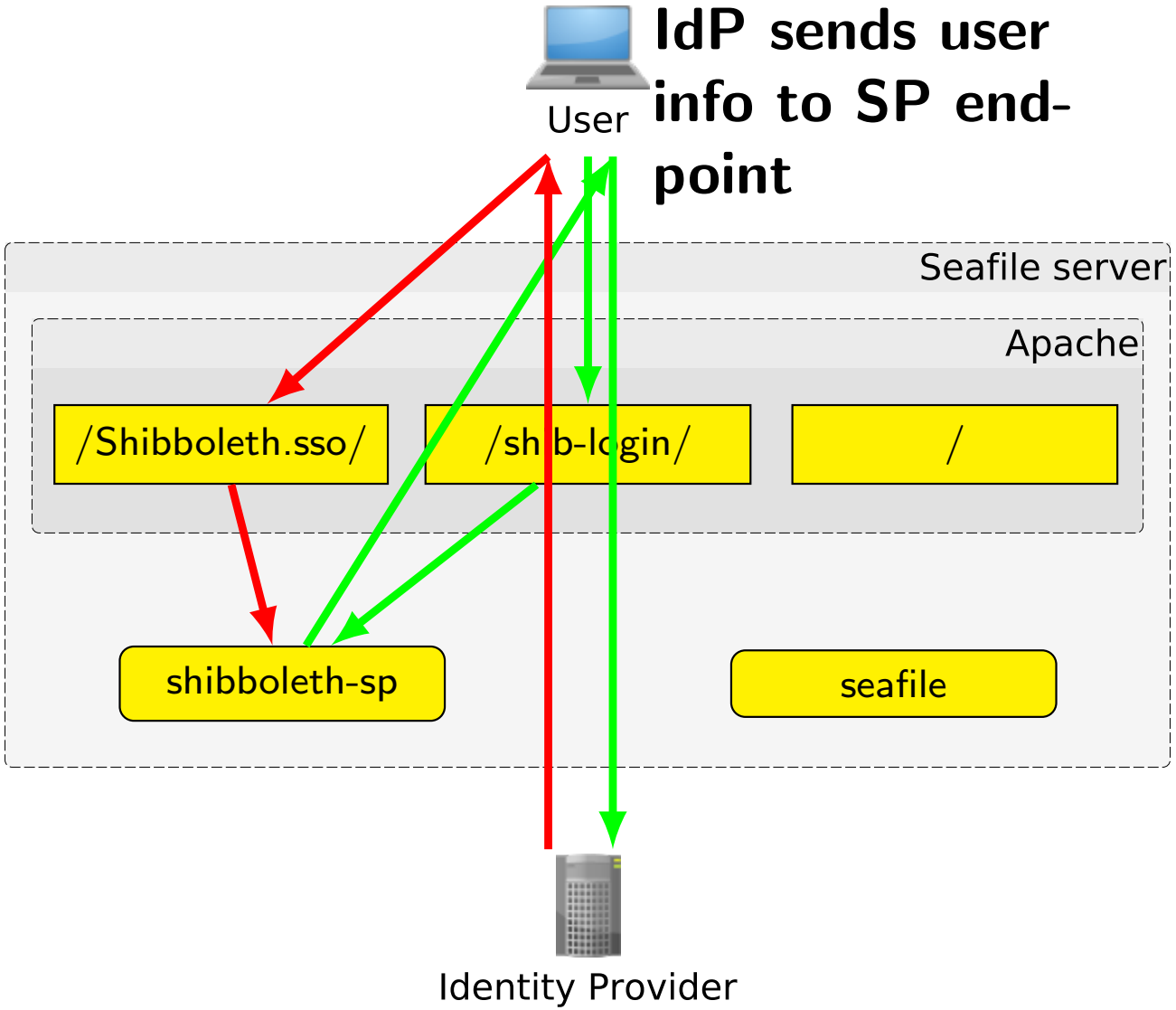
Shibboleth login flow



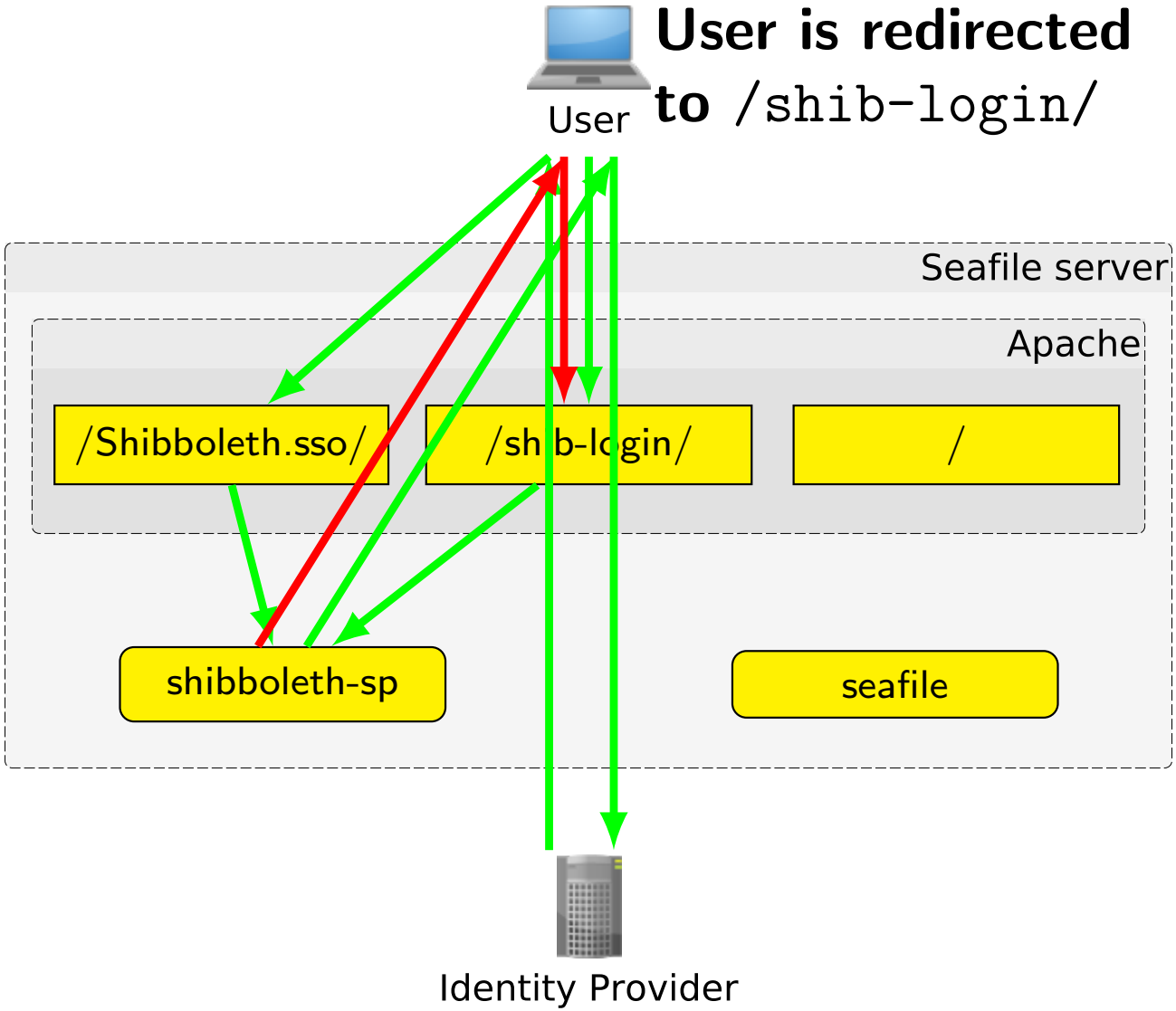
Shibboleth login flow



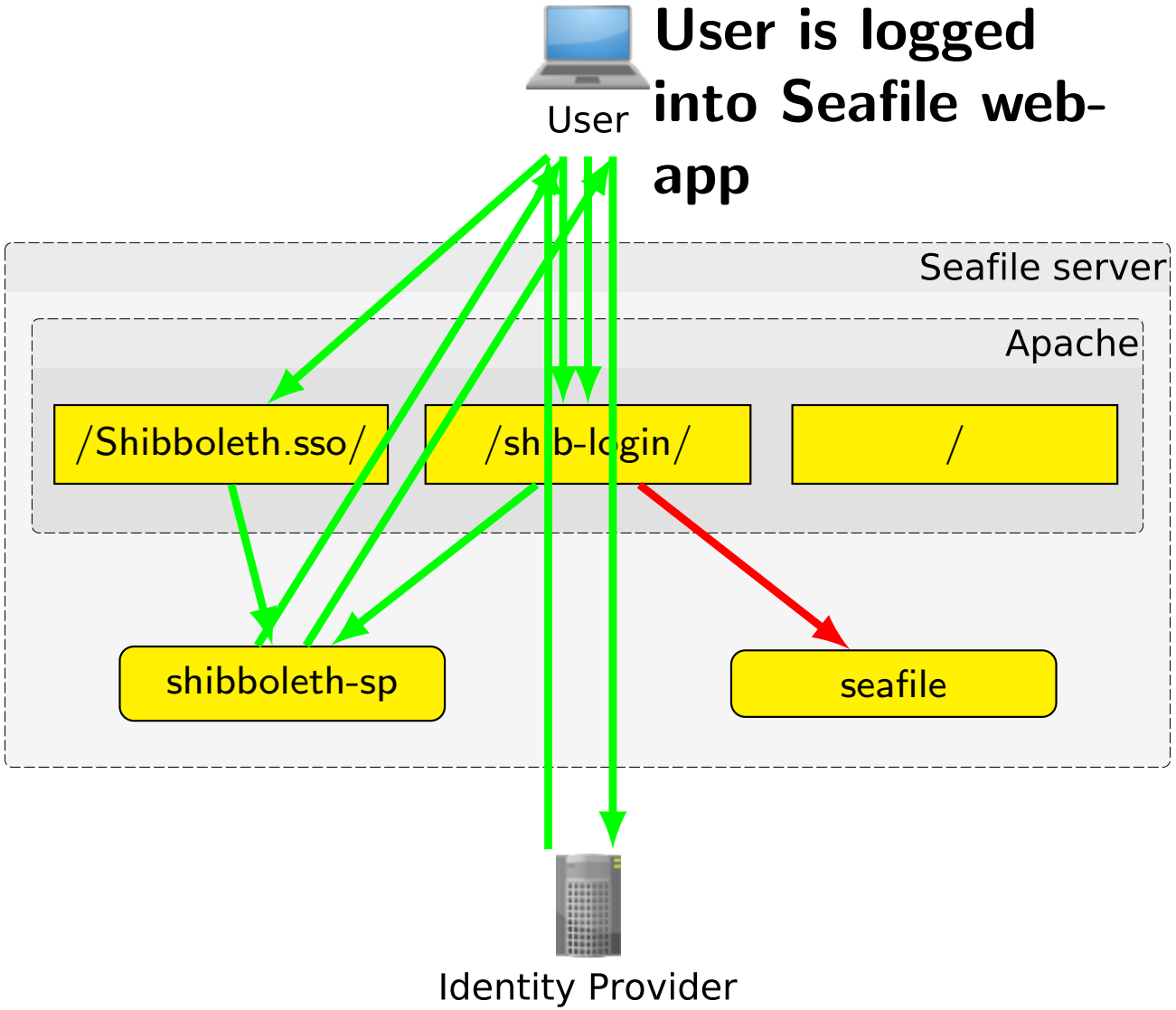
Shibboleth login flow



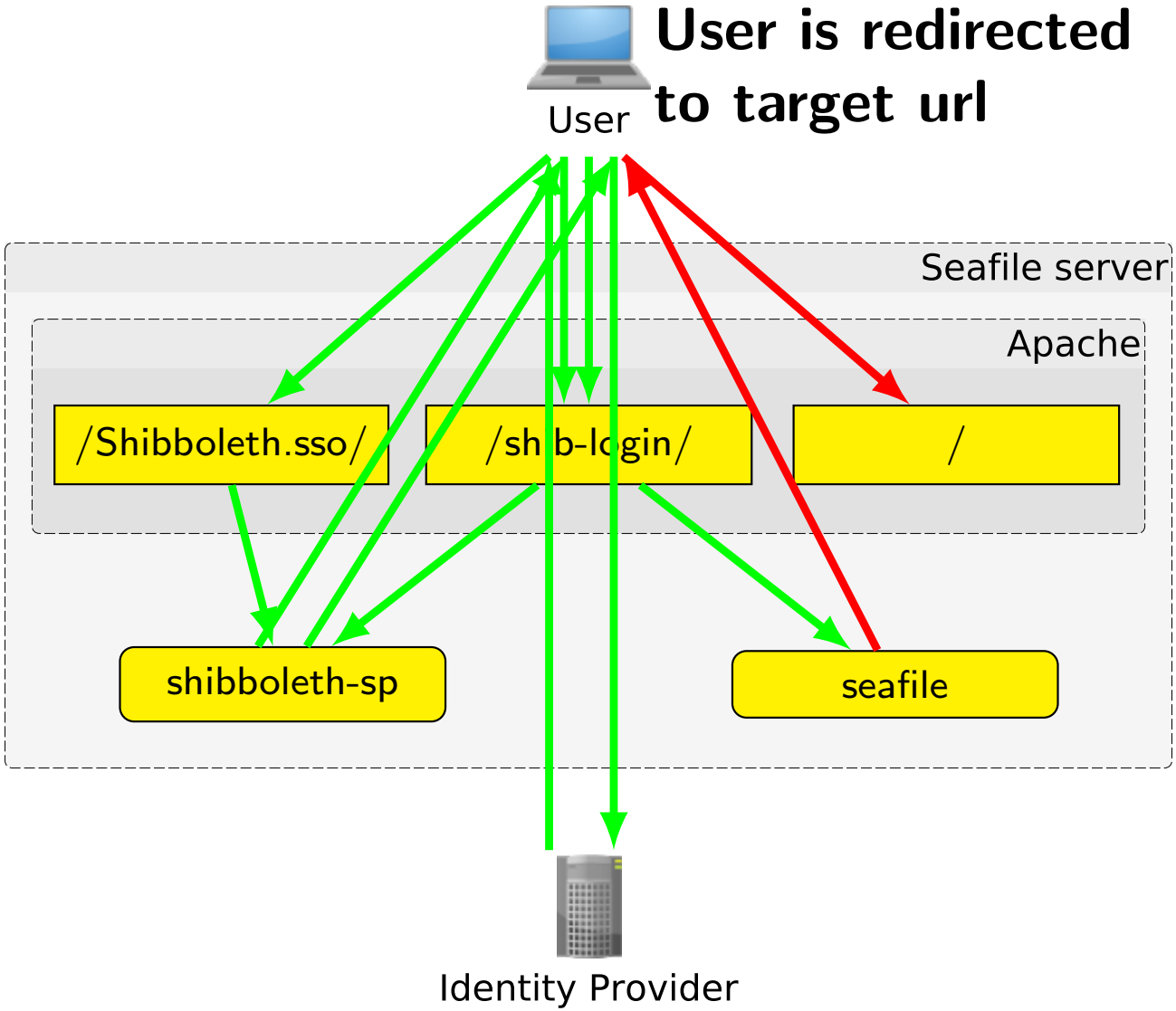
Shibboleth login flow



Shibboleth login flow



Shibboleth login flow



Login summary

- Apache / webserver
  - Manages / distributes requests
  - Handles SSL
- Sync & Share webapp (i.e. Seafile)
  - Transfers shibboleth login on specific endpoint into normal webapp session
- Shibboleth-sp
  - Talks to IdP
  - Provides endpoints for IdP
  - Validates attributes

Metadata - Describing your service

- Description of service
- Api (SAML) endpoints
- SP certificate
  - May be the same as https server certificate
  - Need to care about this in case of rollover!
  - SP acts as client and server, needs matching extensions!
- Needed user data (attributes), required or optional
  - Required state of an attribute is only informational and may be ignored by IdP!
  - No complex logic possible (each attribute is either required or not)
  - relevant standard: eduPerson Object Class Specification

Metadata - What attributes are needed?

- Service needs to uniquely identify the user
  - Need to ensure noone else gets access to the (shared) data
  - Need to ensure the user retains control of his data
- Other users need to uniquely identify the user
  - Whom am I sharing data with / giving access to my files?

Metadata - attributes to identify a person

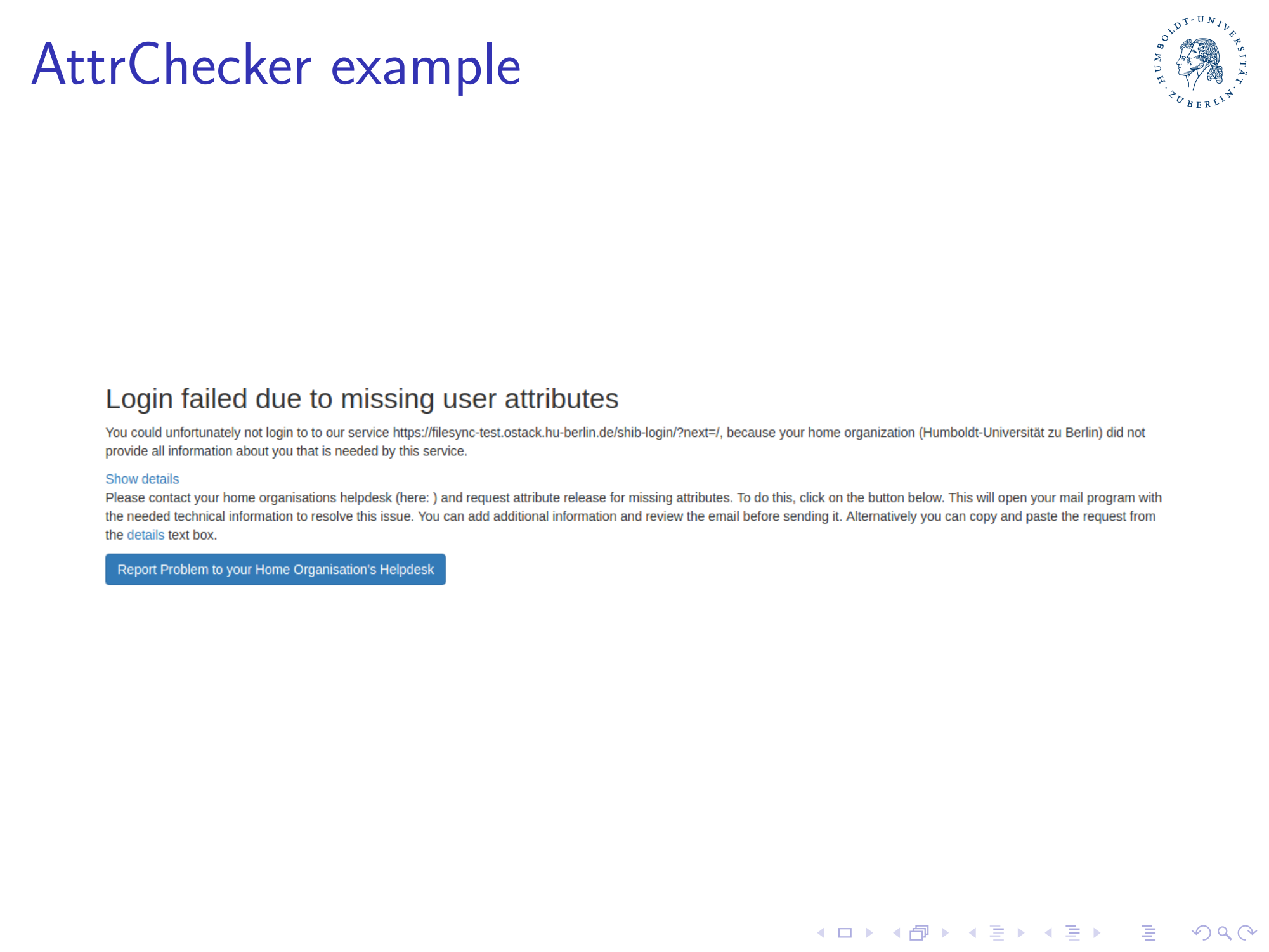
	eduPerson-PrincipalName	eduPersonTargetedID	eduPersonUniqueId
format	<account>@home.edu	https://idp.home.edu/shibboleth!http://box.hu-berlin.de/<uuid>	<hash>@home.edu
uniqueness	per person	per person and service	per person
human-friendly	yes	no	no
persistence	may be reassigned after locally defined period of dormancy, or even changed	no required lifetime ("should be longer than a single user interaction")	yes (may never be reused)
remarks	some institutions don't like to share account names (privacy, attack vector)	best for privacy, in practice usually longer lifetimes?	relatively new, in eduPerson specification since 10/2013, not widely adopted yet?

Metadata - which attributes used in Seafile?

- Checking attributes in SP using AttrChecker:
  `https://github.com/CSCfi/shibboleth-attrchecker`

```
<Handler type="AttributeChecker" Location="/AttrChecker" [...]>
<AND>
  <OR>
    <Rule require="displayName"/>
    <AND>
      <Rule require="sn"/>
      <Rule require="givenName"/>
    </AND>
  </OR>
  <OR>
    <Rule require="eppn"/>
    <AND>
      <Rule require="eduPersonUniqueId"/>
      <Rule require="mail"/>
    </AND>
  </OR>
</AND>
</Handler>
```

AttrChecker example



AttrChecker example

Login failed due to missing user attributes

You could unfortunately not login to to our service https://filesync-test.ostack.hu-berlin.de/shib-login/?next=/, because your home organization (Humboldt-Universität zu Berlin) did not provide all information about you that is needed by this service.

Show details

"The following user information in form of SAML attributes is needed by this service. Required but missing attribute values are marked in red."

Connection summary	
IdP	Humboldt-Universität zu Berlin
entityId	https://shib-idp.cms.hu-berlin.de/idp/shibboleth
SP	https://filesync-test.ostack.hu-berlin.de/shib-login/?next=/
Time	Thu Oct 19 16:50:16 2017
Contact	

Attribute	Value
eduPersonPrincipalName	
displayName	Enno Gröper

Email template for your IdP Administrator

Identity Provider releases my user attributes to https://filesync-test.ostack.hu-berlin.de/shib-login/?next=/. Please find a summary of the login attempt below.

The attributes that were not released to the service are:

Connection summary:

Please contact your home organisations helpdesk (here:) and request attribute release for missing attributes. To do this, click on the button below. This will open your mail program with the needed technical information to resolve this issue. You can add additional information and review the email before sending it. Alternatively you can copy and paste the request from the details text box.

Report Problem to your Home Organisation's Helpdesk

Integration into federations

- National federations (DFN-AAI) - contract between institution and federation operator
- eduGAIN
  - Least common denominator of all connected national federations (if you obey the rules of your national federation, you are fine)
- Data protection code of conduct
  - Defines behavioral rules for SPs which want to receive user attributes from IdPs
  - Standardized privacy statement in English
  - Better chance to get user attributes, if conformance with CoC assured?
- Need to integrate federation metadata

Statistics

- Supporting DFN-AAI federation for nine month
- Around 70 external users (of 3200)
- Contact with 21 home institutions, four in the area of Berlin
- 25 tickets about needed attributes, that were not provided
- Two failed negotiations about attribute transfer
- One time we had to fill and sign a form
- Four institutions worked out-of-the-box

min	max	#	$\# \leq 3$	$\# > 3 \leq 10$	$\# \geq 14$
0	51	16	8	1	7

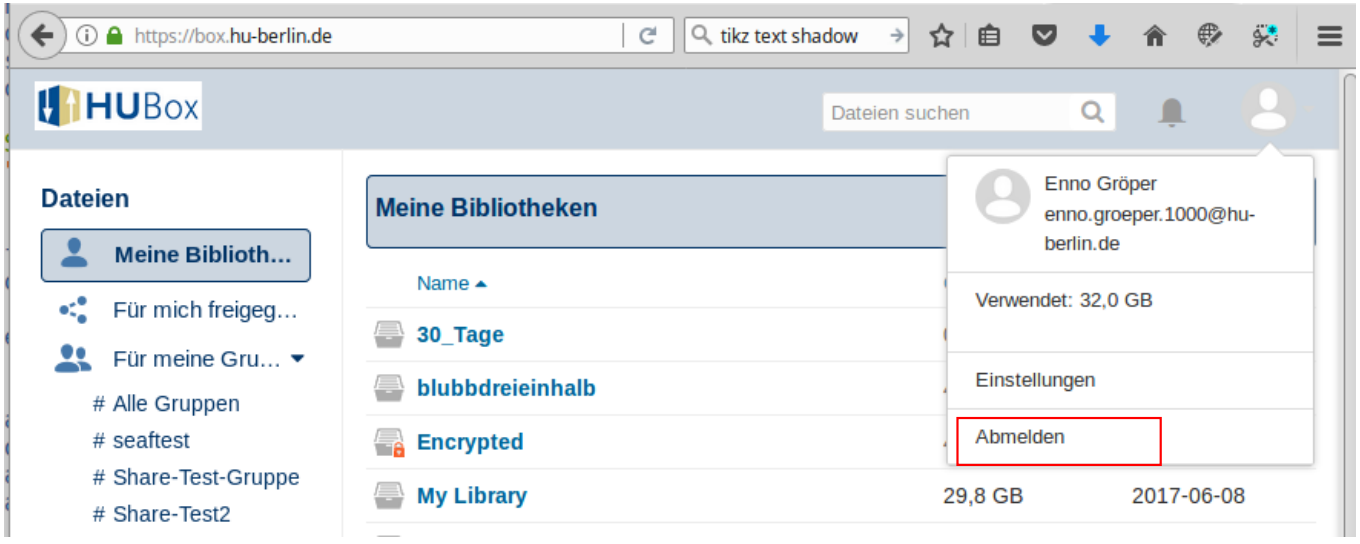
Table: duration for successful attribute transfer in days

Overview

- Introduction to Shibboleth
- Integrating Shibboleth into Sync & Share service
- What about Logout?

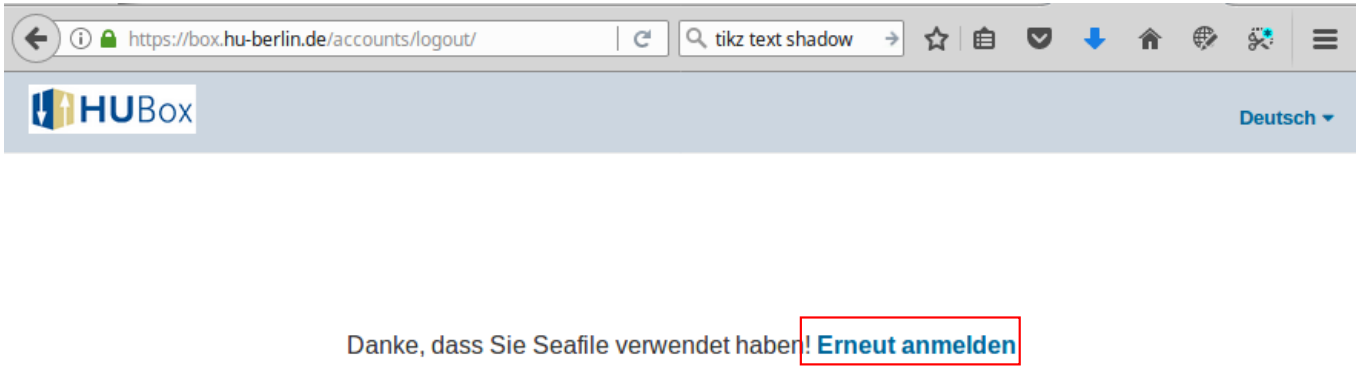
What's the problem?

Doing logout...



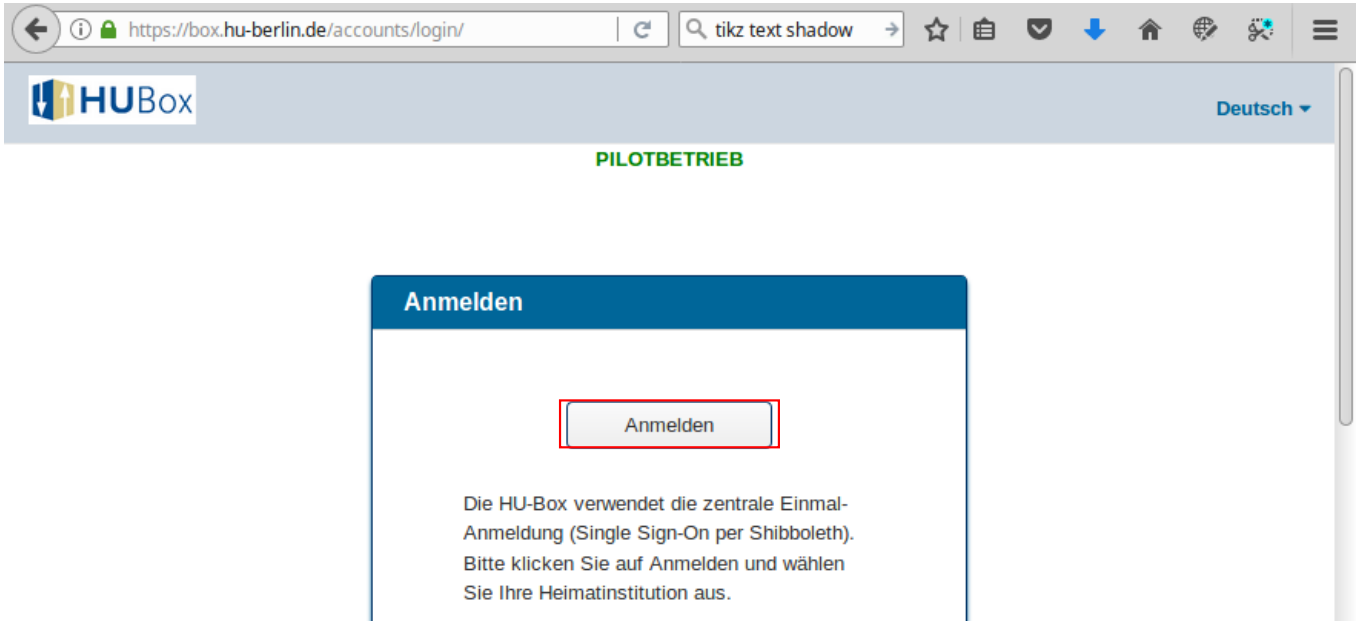
What's the problem?

Back to login...



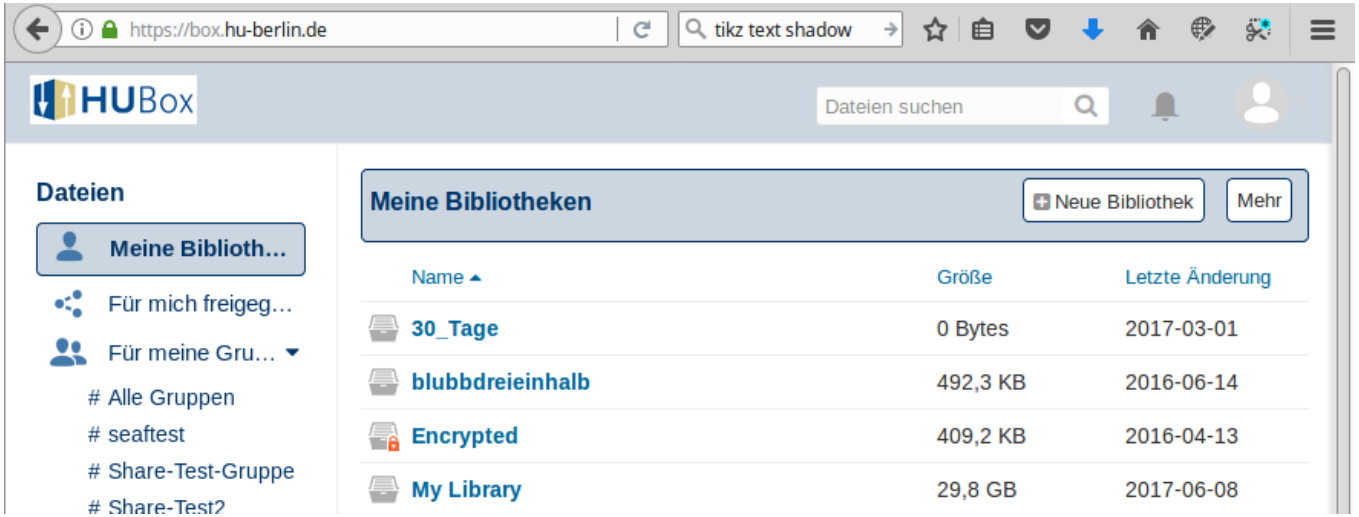
What's the problem?

Starting relogin...



What's the problem?

Back in without providing any credentials!



How to solve it?

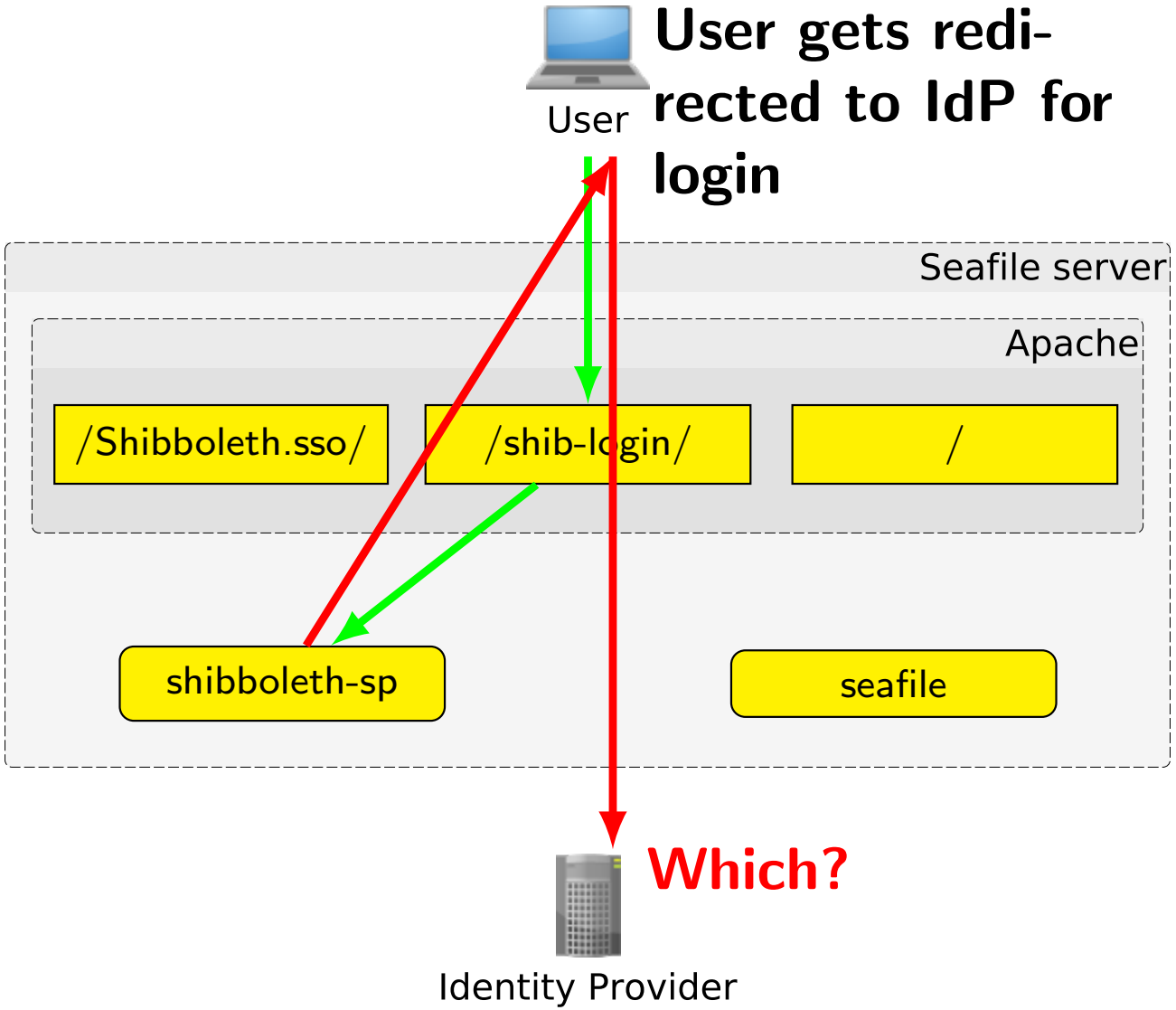
- Close browser (and cross fingers!)?
  - Not very convenient, some users use multiple tabs nowadays
  - Some browsers don't honor the 'end of session' setting of cookie (or never end their session)
- Delete session cookies by hand?
  - Inconvenient
  - Too complex for most users

Implementing Single Logout

- Sessions we need to care about
  - Webapp session
  - Shibboleth SP session
  - Shibboleth IdP session
- Types of logout
  - Front channel
    - Like login using user session and redirects
    - Easy to implement
  - Back channel
    - No user session, IdP contacts SP and requests logout
    - Needed if logout is initiated by another service
    - Needs mapping of shibboleth SP session to webapp session
    - Webapp doesn't do logout, but requests logout from shibboleth-sp

Thank you for your attention!

Shibboleth login flow



Connecting to the home organization

- Central Discovery Service (formerly WAY-F)
  - Service of federation operator
  - Easy to use
  - Can't be customized or controlled
  - Multiple federations only possible, if supported by federation operator
- Embedded Discovery Service (EDS)
  - Webapp running inside your server
  - A little bit harder to deploy
  - Customizable and configurable
  - Example:
    `https://wiki.shibboleth.net/confluence/display/EDS10/Embedded+Discovery+Service`