AARC

Authentication and Authorisation for Research and Collaboration

E-Resources Interoperability

Libraries moving to federated Single Sign-On (SSO)

Jos Westerbeke
Erasmus University

Peter Gietz
DAASI International

Jiří Pavlík
Moravian Library

LIBER 2018, Lille
6.7.2018

Erasmus University Library

DAASI International

MORAVSKÁ ZEMSKÁ KNIHOVNA

Library as a safe place

The library must

- provide a private (virtual) place
- protect its users

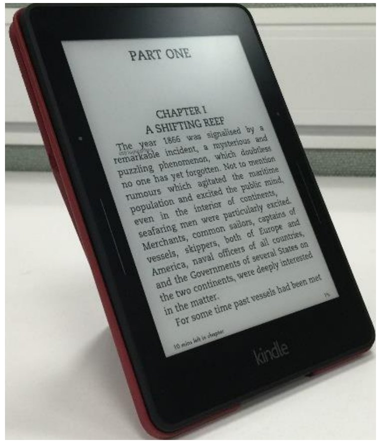
A trusted safe place with privacy

Library as digital content provider

late 20th century - early 21th century

Print -> Digital -> Remote

Remote = any time, any place, any device.



PART ONE

CHAPTER I
A SHIFTING REEF

The year 1866 was signalised by a remarkable incident, a mysterious and puzzling phenomenon, which doubtless no one has yet forgotten. Not to mention rumours which agitated the maritime population and excited the public mind, even in the interior of continents, seafaring men were particularly excited. Merchants, common sailors, captains of vessels, skippers, both of Europe and America, naval officers of all countries, and the Governments of several States on the two continents, were deeply interested in the matter.

For some time past vessels had been met

10 mins left in chapter

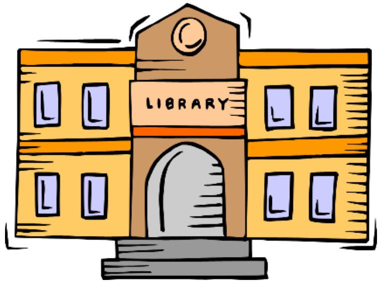
1%

We want:

authenticated and authorized access

preserving privacy

Access: from IP to SSO



IP based authentication:

location based

(Artificially adapted for any place by VPN and Proxy.)

Copyright 2013 All Rights Reserved by Ben Clay

SSO authentication:

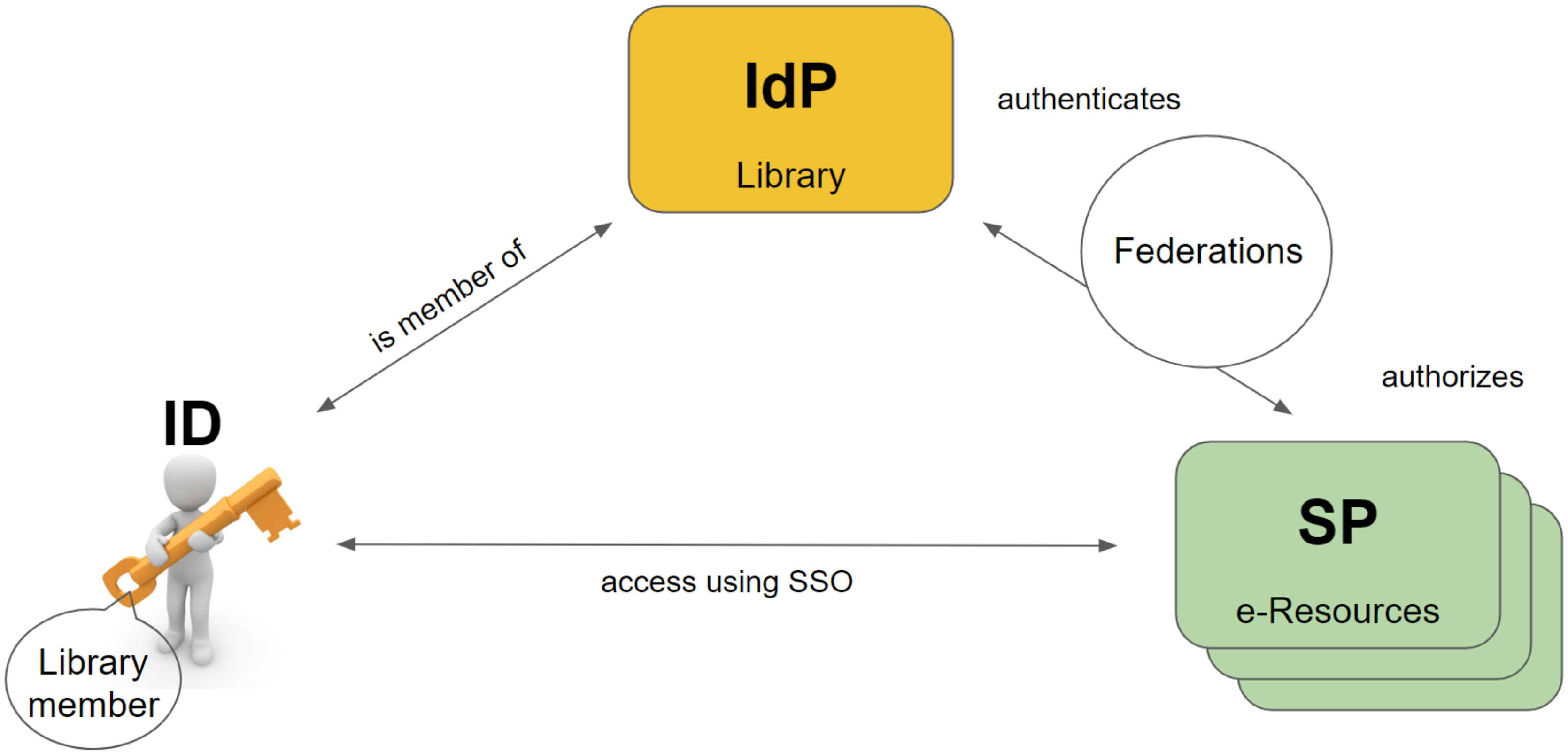
person(ID) based

(Any place, any time, any device)

SSO benefits

- tailored contracts: e.g. buy a subscription for one faculty.
- In case of abuse: just one user can be blocked, instead of all staff and students alike.
- better statistics

What is SSO?


IdP
Library
authenticates
Federations
authorizes
is member of
ID
Library member
access using SSO
SP
e-Resources

Federated IDentity management

The library serves hundreds of publishers. A publisher like Elsevier serves thousands of institutions. They work together through federations when it comes to ID Management. (or IAM)

- **Authentication**. An IdP (library) manages authentication, and provides at least an identifier to the SP**.**
- **Provisioning.** An IdP provides attributes. These are exchanged at the first sign-on. An SP often asks for personal data such as an email address.

=> **Minimal disclosure policy:** A Persistent Identifier, Affiliations.

What can libraries expect in the coming years?

- Increasing demand by publishers for SSO access
- Increasing denial by publishers for IP based access
- More awareness by users of personal data exchange
- Recommendations from initiatives such as RA21.org
- Recommendations from Library consortia

Activities:

eduGAIN — The international interfederation of national research and education federations.

RA21 — Activity on enhancing the user experience in federated identity management (FIM).

REFEDS — The research and education federations group.

AARC — EU-funded project on FIM technologies and policies.

AARC Project

- Authentication and Authorization for Research Collaboration
- EU funded project in its second phase
- Inspired by the work from FIM4R Group (FIM for Research)
- Objectives:
  - Deliver production-ready architectural building blocks and best practices to enable research and e-infrastructures to build interoperable AAI
  - Avoid a future in which new research collaborations develop independent AAIs
- Libraries:
  - A number of AARC 1 pilots were dedicated to library use-cases
  - Dedicated training material for libraries
  - See also https://aarc-project.eu/libraries/

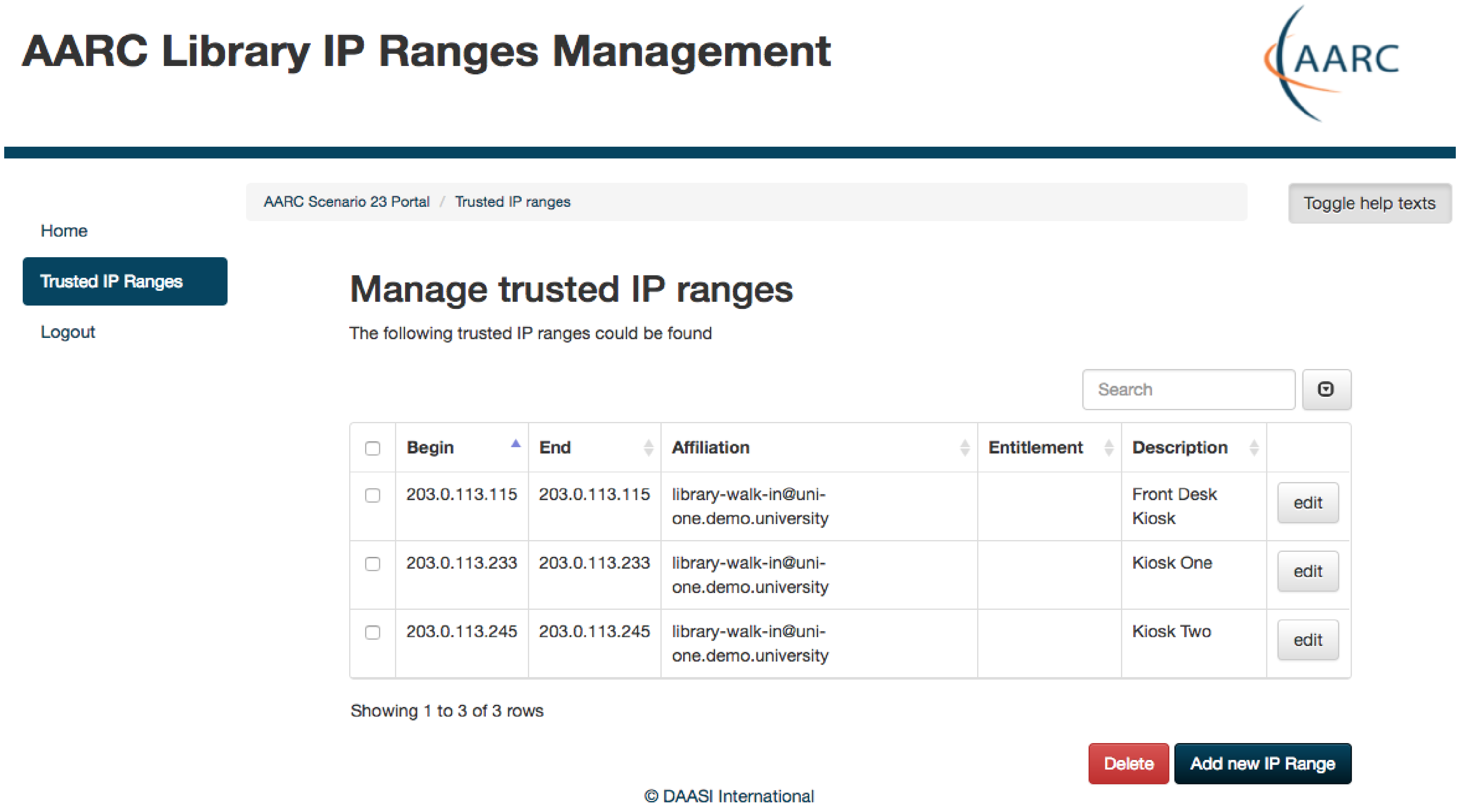
AARC Libraries walk-in-user pilot

- Reliance on using IP addresses to authenticate users prevents some university libraries from moving to federated access
- Even if a library switches to FIM, there still are needs for IP based authentication:
  - Old IP-based contracts with content providers
  - Provide access to „walk-in“ users
- Thus a solution was created that integrates IP based authentication in a federated infrastructure
  - Shibboleth IdP v3 can be configured to automatically authenticate users from defined IP addresses or ranges of IP addresses, but that is a static configuration
- See also https://wiki.geant.org/display/AARC/Libraries+walk-in-user+pilot

AARC Libraries walk-in-user pilot

- Setup:
  - Standard Shibboleth IdPv3
  - IdP extension to collect User‘s IP address
  - IdP ranges/affiliation/entitlement attributes database in LDAP directory
  - IdP Intercept filter to halt authentication if user‘s IP was not found in LDAP
  - Stand-alone administration interface for managing IP ranges in LDAP which is tenant capable so that a number of libraries can use the service

AARC Libraries walk-in-user pilot



AARC Library IP Ranges Management

Manage trusted IP ranges

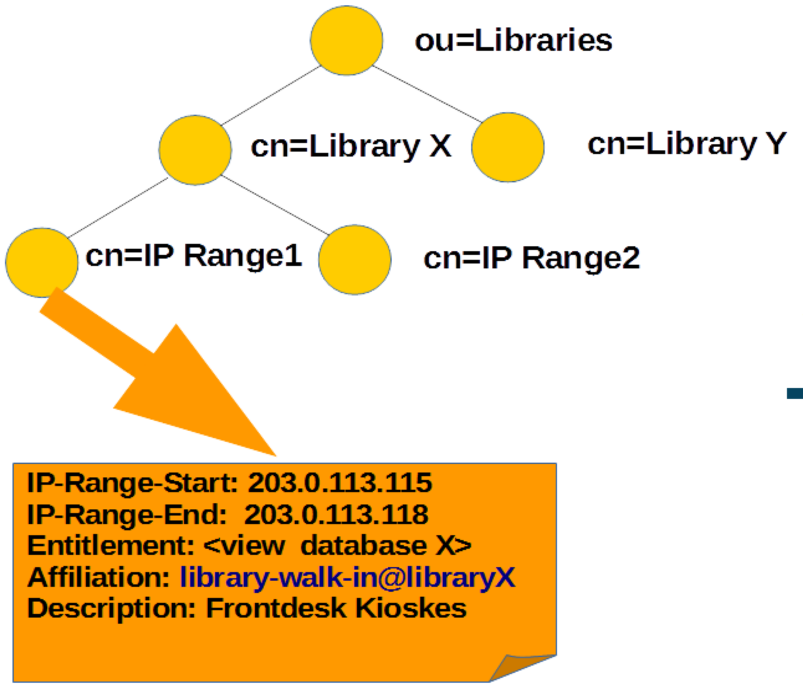
The following trusted IP ranges could be found

☐	Begin	End	Affiliation	Entitlement	Description	
☐	203.0.113.115	203.0.113.115	library-walk-in@uni-one.demo.university		Front Desk Kiosk	edit
☐	203.0.113.233	203.0.113.233	library-walk-in@uni-one.demo.university		Kiosk One	edit
☐	203.0.113.245	203.0.113.245	library-walk-in@uni-one.demo.university		Kiosk Two	edit

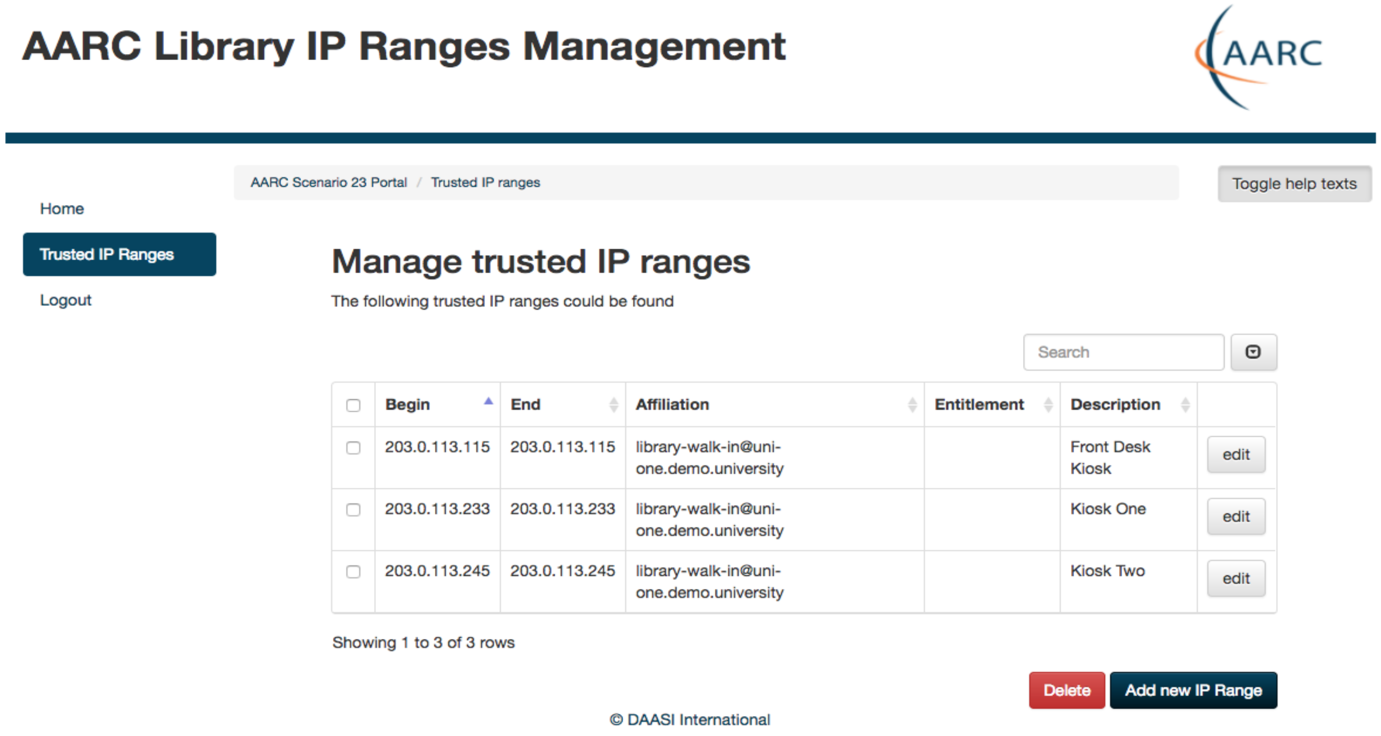
Showing 1 to 3 of 3 rows

© DAASI International

AARC Libraries walk-in-user pilot



IP-Range-Start: 203.0.113.115
IP-Range-End: 203.0.113.118
Entitlement: <view database X>
Affiliation: library-walk-in@libraryX
Description: Frontdesk Kioskes


AARC Library IP Ranges Management

Manage trusted IP ranges

The following trusted IP ranges could be found

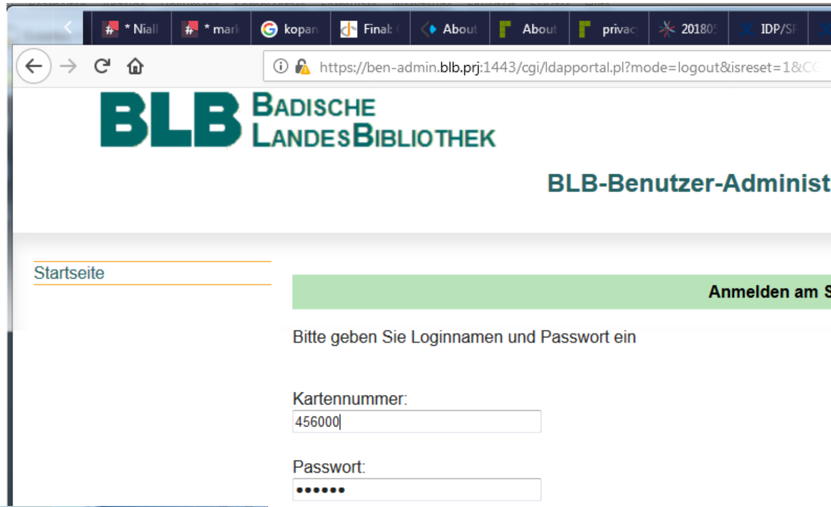
☐	Begin	End	Affiliation	Entitlement	Description	
☐	203.0.113.115	203.0.113.115	library-walk-in@uni-one.demo.university		Front Desk Kiosk	edit
☐	203.0.113.233	203.0.113.233	library-walk-in@uni-one.demo.university		Kiosk One	edit
☐	203.0.113.245	203.0.113.245	library-walk-in@uni-one.demo.university		Kiosk Two	edit

Showing 1 to 3 of 3 rows

© DAASI International

Real life example

- Within a project we implemented Identity Management and SSO for a German state library, including:
  - synchronisation from library management system,
  - OpenLDAP as central authentication & attribute server
  - dedicated web interface with federated login
    - to de-/re-activate accounts
    - to manage IP-Ranges
  - Shibboleth IdP with extensions
  - Single-Log-Out feature
- Normal login but enhancing attributes based on IP



https://ben-admin.blb.prj:1443/cgi/ldapportal.pl?mode=logout&isreset=1&C

BADISCHE LANDESBIBLIOTHEK

BLB-Benutzer-Administ

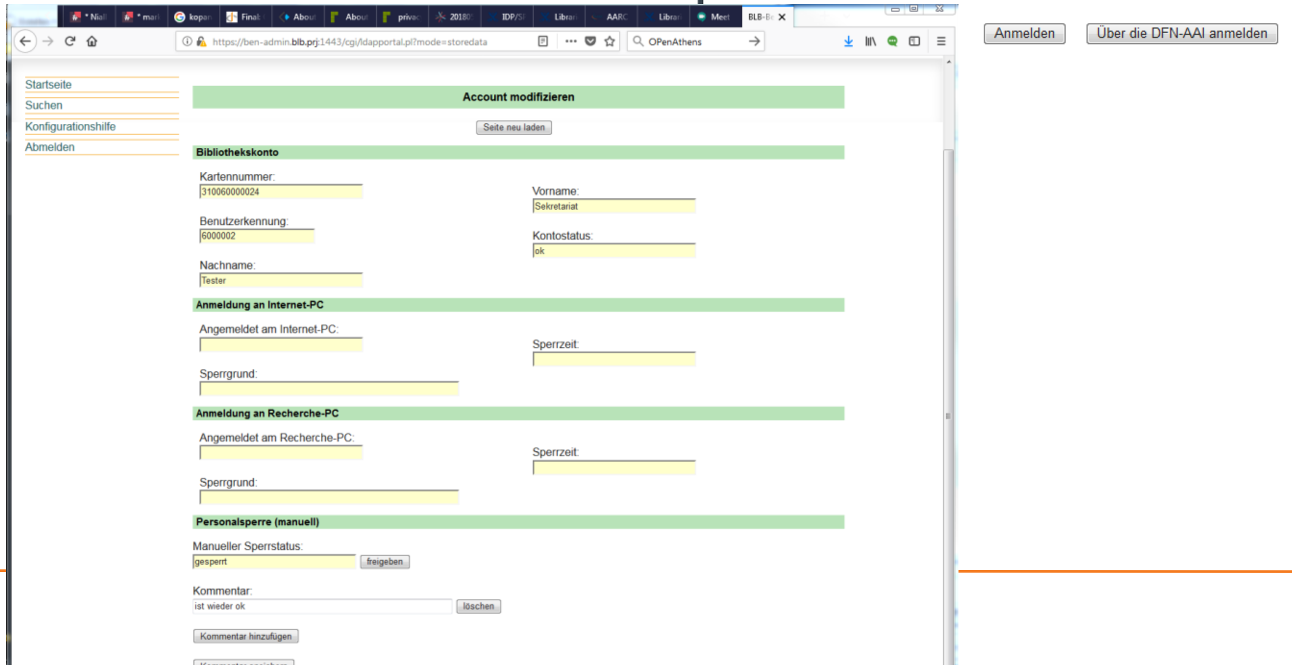
Startseite

Anmelden am S

Bitte geben Sie Loginnamen und Passwort ein

Kartennummer: 456000

Passwort: ••••••



https://ben-admin.blb.prj:1443/cgi/ldapportal.pl?mode=storedata

Account modifizieren

Bibliothekskonto

Kartennummer: 310060000024

Vorname: Sekretariat

Benutzerkennung: 6000002

Kontostatus: ok

Nachname: Tester

Anmeldung an Internet-PC

Angemeldet am Internet-PC:

Sperrzeit:

Sperrgrund:

Anmeldung an Recherche-PC

Angemeldet am Recherche-PC:

Sperrzeit:

Sperrgrund:

Personalsperre (manuell)

Manueller Sperrstatus: gesperrt

Kommentar: ist wieder ok

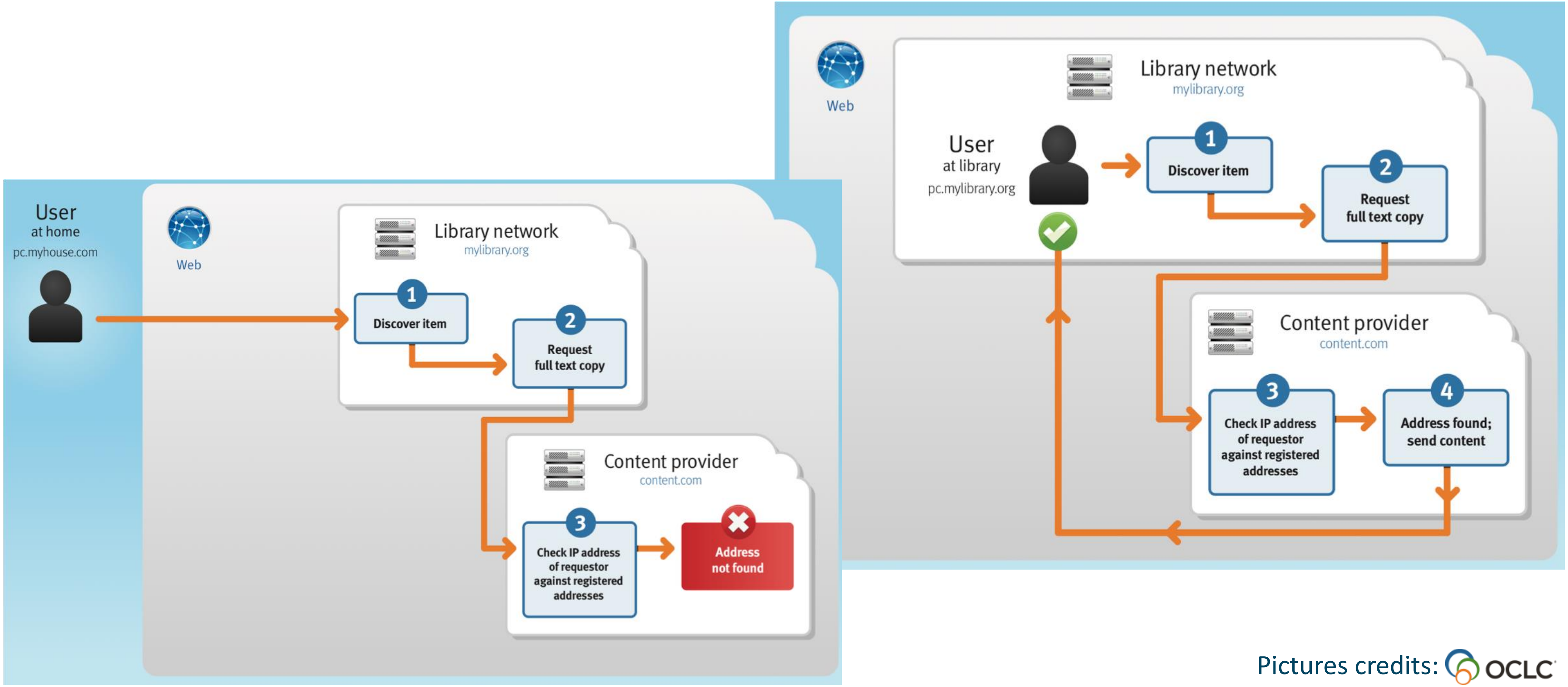
Real life example

- Shibboleth IdP extensions:
  - Login Handler that
    - respects the deactivation flag
    - Enforces a captcha after 3 wrong password inputs
    - Collects IP address of user
- Data Connector that enhances the user attributes based on IP address and IP range configuration in LDAP server (Range → Entitlement)
- Data Connector that adds additional entitlements based on group memberships of the user

AARC EZproxy pilot

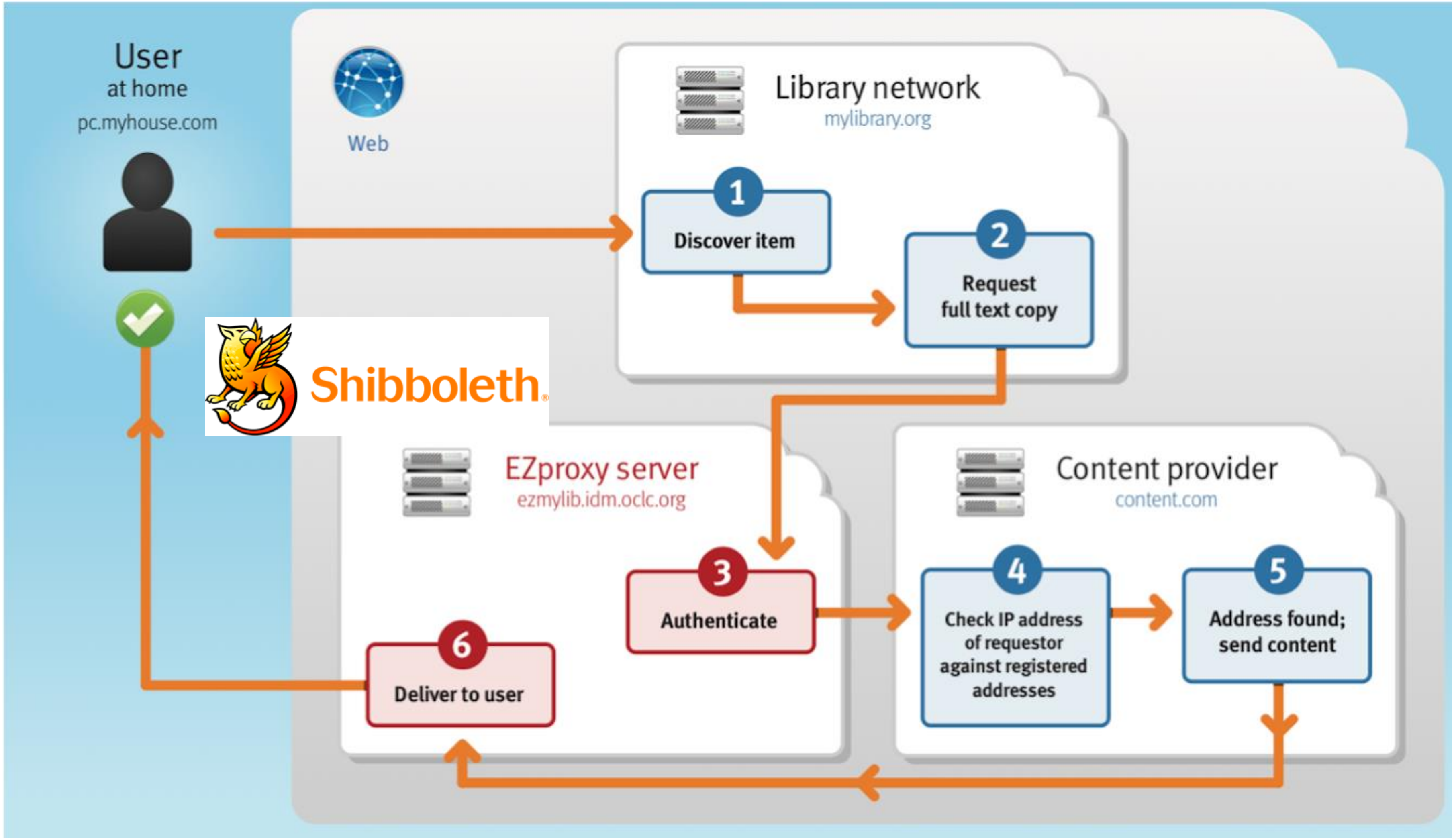
- EZproxy could bring e-resources without native federative authentication support into SSO environment
- Appropriate EZproxy configuration described at the pilot
  - https://aarc-project.eu/libraries/
  - https://wiki.geant.org/display/AARC/Libraries+EZproxy+access+mode+switch+pilot
- Production implementation at Erasmus University
  - Hosted version by OCLC, easy to set-up and maintain
- Production implementation at Moravian Library
  - Local version, https://www.mzk.cz/en/catalogues-and-databases/databases
  - Access via EZproxy to: eLibraryUSA, Naxos Music Library
  - SSO native: EBSCOhost, ProQuest Central, SpringerLink, Web Of Knowledge, Oxford Music Online

AARC EZproxy pilot



Pictures credits: OCLC

AARC EZproxy pilot



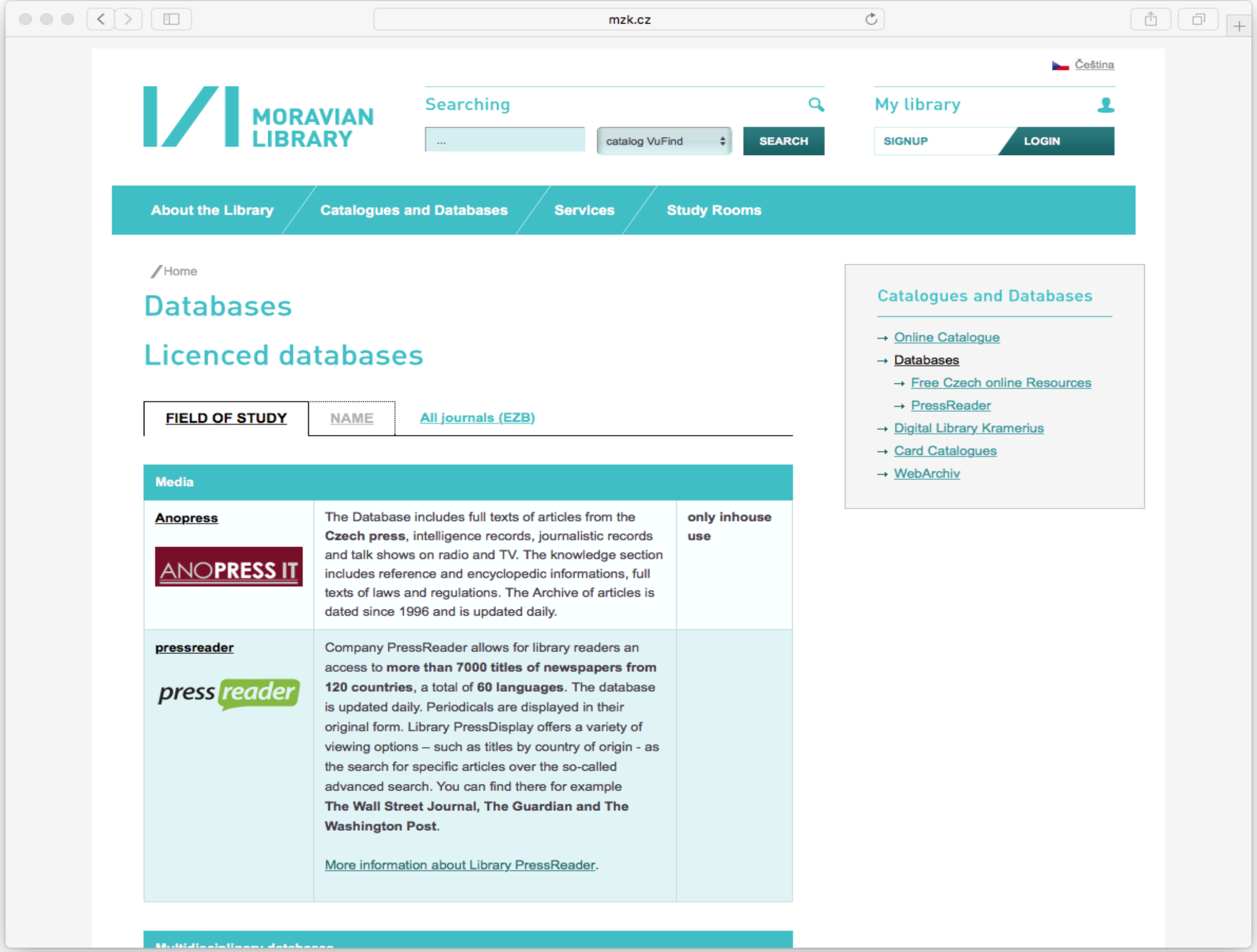
Picture credits: OCLC

AARC EZproxy pilot - Moravian Library

Licensed resources

SSO for users

- EZproxy links
- WAYFless links



Databases

Licenced databases

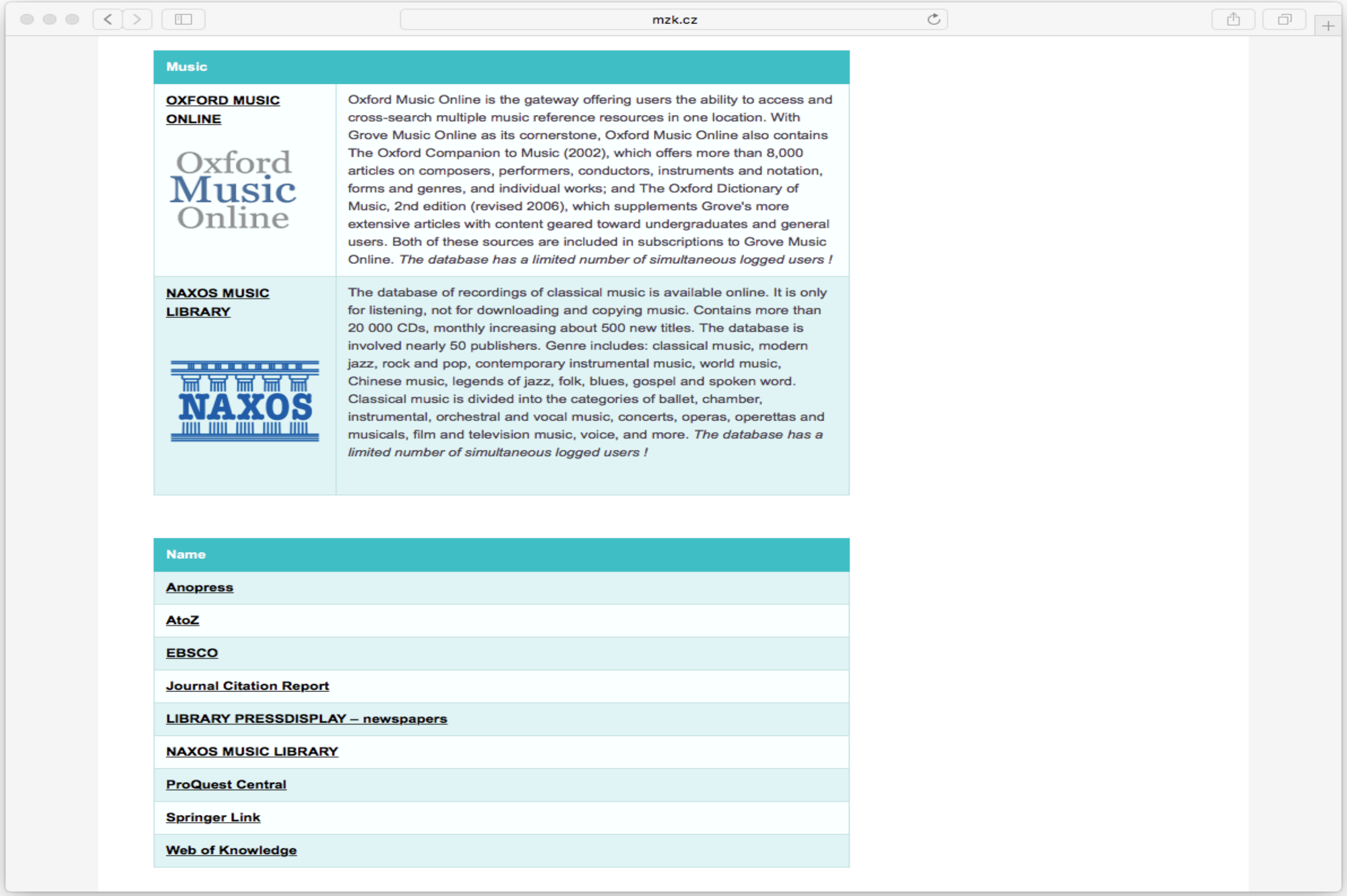
Media		
Anopress ANOPRESS IT	The Database includes full texts of articles from the **Czech press**, intelligence records, journalistic records and talk shows on radio and TV. The knowledge section includes reference and encyclopedic informations, full texts of laws and regulations. The Archive of articles is dated since 1996 and is updated daily.	**only inhouse use**
pressreader press reader	Company PressReader allows for library readers an access to **more than 7000 titles of newspapers from 120 countries**, a total of **60 languages**. The database is updated daily. Periodicals are displayed in their original form. Library PressDisplay offers a variety of viewing options – such as titles by country of origin - as the search for specific articles over the so-called advanced search. You can find there for example **The Wall Street Journal, The Guardian and The Washington Post**. More information about Library PressReader.	

Multidisciplinary databases

Catalogues and Databases

- → Online Catalogue
- → Databases
  - → Free Czech online Resources
  - → PressReader
- → Digital Library Kramerius
- → Card Catalogues
- → WebArchiv

AARC EZproxy pilot - Moravian Library



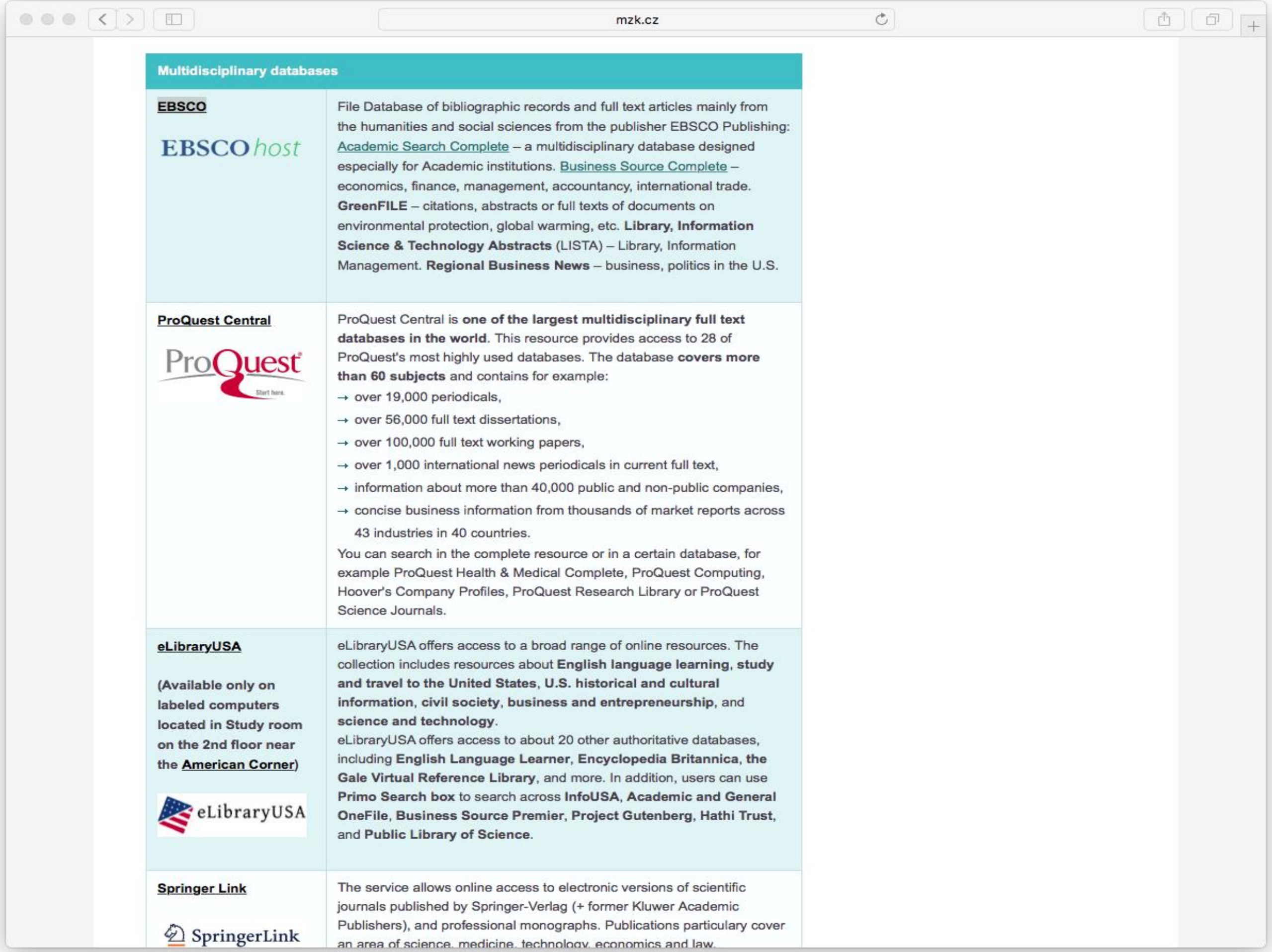
Music	
OXFORD MUSIC ONLINE Oxford Music Online	Oxford Music Online is the gateway offering users the ability to access and cross-search multiple music reference resources in one location. With Grove Music Online as its cornerstone, Oxford Music Online also contains The Oxford Companion to Music (2002), which offers more than 8,000 articles on composers, performers, conductors, instruments and notation, forms and genres, and individual works; and The Oxford Dictionary of Music, 2nd edition (revised 2006), which supplements Grove's more extensive articles with content geared toward undergraduates and general users. Both of these sources are included in subscriptions to Grove Music Online. *The database has a limited number of simultaneous logged users !*
NAXOS MUSIC LIBRARY NAXOS	The database of recordings of classical music is available online. It is only for listening, not for downloading and copying music. Contains more than 20 000 CDs, monthly increasing about 500 new titles. The database is involved nearly 50 publishers. Genre includes: classical music, modern jazz, rock and pop, contemporary instrumental music, world music, Chinese music, legends of jazz, folk, blues, gospel and spoken word. Classical music is divided into the categories of ballet, chamber, instrumental, orchestral and vocal music, concerts, operas, operettas and musicals, film and television music, voice, and more. *The database has a limited number of simultaneous logged users !*

Name
Anopress
AtoZ
EBSCO
Journal Citation Report
LIBRARY PRESSDISPLAY – newspapers
NAXOS MUSIC LIBRARY
ProQuest Central
Springer Link
Web of Knowledge

Naxos EZproxy link:

- https://proxy.mzk.cz/login?auth=shibboleth&url=http://Moravska.NaxosMusicLibrary.com

AARC EZproxy pilot - Moravian Library



Multidisciplinary databases	
EBSCO EBSCO*host*	File Database of bibliographic records and full text articles mainly from the humanities and social sciences from the publisher EBSCO Publishing: Academic Search Complete – a multidisciplinary database designed especially for Academic institutions. Business Source Complete – economics, finance, management, accountancy, international trade. **GreenFILE** – citations, abstracts or full texts of documents on environmental protection, global warming, etc. **Library, Information Science & Technology Abstracts** (LISTA) – Library, Information Management. **Regional Business News** – business, politics in the U.S.
ProQuest Central ProQuest Start here.	ProQuest Central is **one of the largest multidisciplinary full text databases in the world**. This resource provides access to 28 of ProQuest's most highly used databases. The database **covers more than 60 subjects** and contains for example: → over 19,000 periodicals, → over 56,000 full text dissertations, → over 100,000 full text working papers, → over 1,000 international news periodicals in current full text, → information about more than 40,000 public and non-public companies, → concise business information from thousands of market reports across 43 industries in 40 countries. You can search in the complete resource or in a certain database, for example ProQuest Health & Medical Complete, ProQuest Computing, Hoover's Company Profiles, ProQuest Research Library or ProQuest Science Journals.
eLibraryUSA **(Available only on labeled computers located in Study room on the 2nd floor near the American Corner)** eLibraryUSA	eLibraryUSA offers access to a broad range of online resources. The collection includes resources about **English language learning, study and travel to the United States, U.S. historical and cultural information, civil society, business and entrepreneurship**, and **science and technology**. eLibraryUSA offers access to about 20 other authoritative databases, including **English Language Learner, Encyclopedia Britannica, the Gale Virtual Reference Library**, and more. In addition, users can use **Primo Search box** to search across **InfoUSA, Academic and General OneFile, Business Source Premier, Project Gutenberg, Hathi Trust**, and **Public Library of Science**.
Springer Link SpringerLink	The service allows online access to electronic versions of scientific journals published by Springer-Verlag (+ former Kluwer Academic Publishers), and professional monographs. Publications particulary cover an area of science, medicine, technology, economics and law.

EBSCOhost WAYFLess link:

- http://search.ebscohost.com/login.aspx?authtype=ip,shib&custid=s4992271&profile=ehost

What libraries have to do

- ➢create **awareness** by setting up SSO
- ➢make a policy as a consortium, using the principle: *Minimal disclosure* of information to publishers. Only a persistent ID and affiliations would be sufficient. (No *Personally Identifiable Information* by default. Personal information if based on user consent or for services of research communities.)
- ➢use eduGAIN interfederation via appropriate national federation such as Dutch SURFConex*t*

Furthermore:

- ✓help develop a user consent screen with optional sharing of more user attributes
- ✓support AARC guidelines: Research&Scholarship, GÉANT's Data Protection Code of Conduct, SIRTFI, ...
- ✓support RA21 guidelines (coming soon) for better user experience
- ✓use browser extensions which guide users, like Lean Library (library e-resource guide) and Kopernio (PDF finder)
- ✓in case of research infrastructures: deploy other policies

FEDERATED SINGLE SIGN-ON: MADE EASY!

Want to learn more about how federated access can help your library and your researchers?

The AARC project offers solutions and training for library staff.

1. WHAT'S THE PROBLEM?

There are actually several problems with IP-based authentication.

- For libraries, it's expensive and difficult to manage.
- Publishers increasingly demand SSO-based authentication.
- It's also annoying for off-campus researchers who can't benefit from a seamless solution to access library resources.

2. WHAT'S THE ALTERNATIVE?

Single Sign-On with Federated Identity Management!

3. HOW WOULD MY LIBRARY BENEFIT?

With SSO everyone (even 'walk in' guest users) gets a unique seamless solution to access to federated e-resources easily and securely.

Libraries can also save money by tailoring licenses and contracts to actual usage by discipline and you can access accurate statistics.

4. DOES IT HELP RESEARCHERS TOO?

Yes! Researchers today work from many different locations, and increasingly use research services and databases of many kinds. SSO gives researchers more opportunities to personalise services and to control the personal data sent to providers.

SSO also means that researchers only need one account, instead of a different login for each service.

5. SOUNDS GREAT, TELL ME MORE!

We've developed three pilots for the library community, and published a Libraries Toolkit. See our website for more information.

www.aarc-project.eu/libraries

6. ANY OTHER TIPS?

Global initiatives such as Resource Access for the 21st Century (RA21.org) are working to bring together publishers and libraries to improve SSO user experience.

AARC is funded by the European Union's Horizon 2020 research and innovation programme under grant agreements 653965 & 730941.
This poster relates to talk 11.2 E-resource Interoperability.

More informations at the poster stand and Project AARC web site.

Thank you

Any Questions?

http://aarc-project.eu/libraries/

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).