

Identity Management with x-services in Aleph

Gerard Bennett, University of Westminster

IGeLU – Budapest - Session 11.42

Thursday 3rd Sept 2015

The University

- Central London mainly: Regent; Marylebone; Cavendish and Harrow (15 km north-west)
- Public university, teaching and research
- Started in 1837: antecedent institutions
- Faculties:
 - Faculty of Science and Technology (Cavendish)
 - Faculty of Media, Arts and Design (Harrow)
 - Faculty of Social Sciences and Humanities (Regent)
 - Faculty of Architecture and the Built Environment (Marylebone)
 - Westminster Law School (Regent)
 - Westminster Business School (Marylebone)
- 20,000+ students; 1000+ staff. User groups, including ‘others’

Overview

- University of Westminster context
- Identity Management (IDM) at Westminster
- Use of IDM to provision Aleph accounts
 - Version 1 – to Spring 2015
 - Version 2 – since Spring 2015
- X-service at the heart of this: ‘update-bor’
- X-services security
- Tools for monitoring

Identity Manager (IDM)

- Use of Identity Manager to provision accounts for many systems
- Authoritative sources feeding an Identity Vault (database + drivers)
- Main authoritative sources: Student record management system SITS; Staff DB (SAP); Record management for 'Others'
- Identity Vault driver feeds going to many different systems, to create, update and delete account information
- Functions for both Authentication and Authorisation

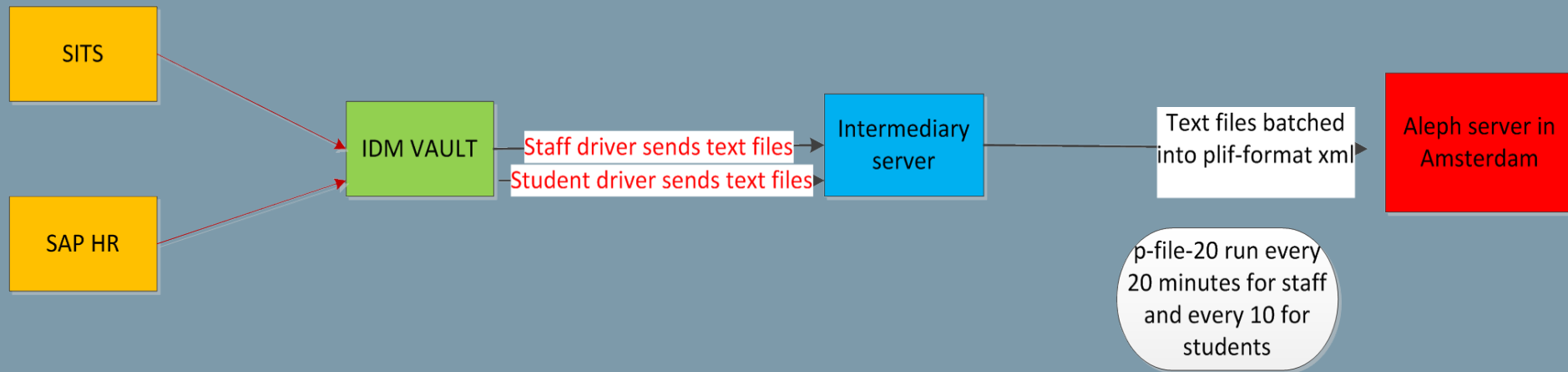
IDM and Library

- IDM in use is NetIQ Identity Manager
- IDM driver controlling creation, updating and deletion of Aleph users since 2006
- A separate IDM driver for Shibboleth attributes also. Sends to Shibboleth IdP
- Outsourcing of IDM in Spring 2014
- Review > Decision to re-write the driver.

Aleph IDM version 1

- Two drivers: staff & student
- Provides data to p-file-20 in plif format
- Data : z303; z304; z305; z308
- Processing stages. Batch files; Intermediary servers (to run processes that could not be run on hosted Aleph; additional processing; PLIF file; scheduling p-file-20 at frequent intervals
- Unnecessary complexity & error prone

Aleph Identity & Data Exchange Version 1 using text files and intermediary server

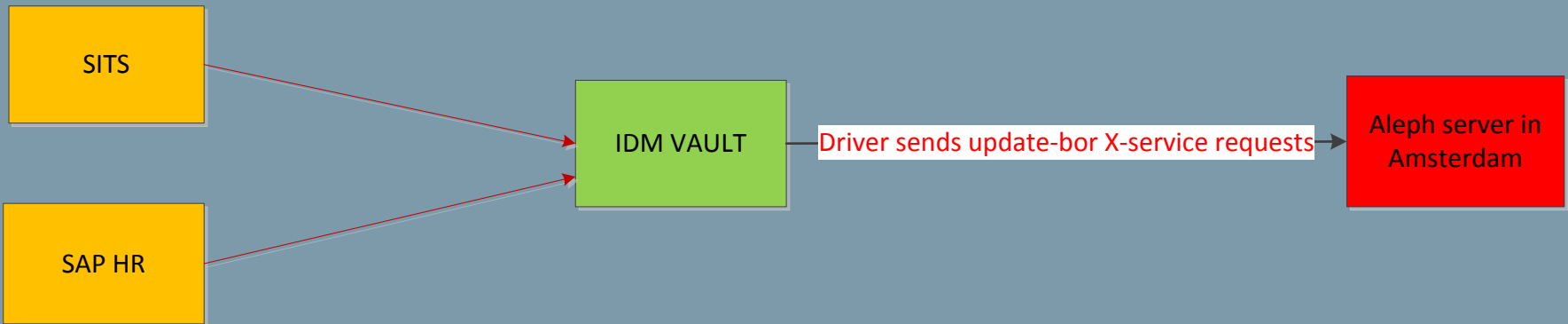


Aleph IDM version 2

- One driver for staff and students
- A single update in Identity vault triggers an update in Aleph.
- Using X-service: update-bor
- PLIF format for data
- Post not Get
- No scheduling; no batching; no intermediary servers; no p-file-20 post-processing
- Failures or problems at the level of single transactions not batch files
- Logging is found in www server logs /apache logs

Aleph Identity & Data Exchange

Version 2 with single driver for staff and students;
X-service update-bor; No scheduling; no batching;
no intermediary servers; no p-file-20



Update-bor

- https://developers.exlibrisgroup.com/aleph/apis/Aleph-X-Services/update_bor for documentation
- Driver is only sending the specific data for the update / insert etc. Documentation suggests that the whole record, z303 etc, is sent each time.
- Some mandatory fields, but not well-documented
- Operations permitted are Insert; Update; Delete and Add.
- ‘Add’ does not care whether there is already a record present or not, but requires the full data of an Insert to be sent each time

```
request: "/X?op=update-  
bor&library=WST50&update-  
flag=Y&xml_full_req=<?xml  
version="1.0"?><p-file-20><patron-  
record><z303><match-id-type>00</match-  
id-type><match-id>227038</match-  
id><record-action>U</record-  
action></z303><z305><record-  
action>U</record-action><z305-  
id>227038</z305-id><z305-sub-  
library>WST50</z305-sub-  
library></z305><z308><record-  
action>A</record-action><z308-key-  
type>01</z308-key-type><z308-  
id>227038</z308-id><z308-key-  
data>2270381</z308-key-data><z308-  
user-library>WST50</z308-user-  
library><z308-verification-type>00</z308-  
verification-type><z308-  
encryption>N</z308-encryption><z308-  
status>AC</z308-status></z308></patron-  
record></p-file-20>"
```

Example of insert

```
<p-file-20>
<patron-record>
<z303>
<match-id-type>00</match-id-type>
<match-id>999999999</match-id>
<record-action>I</record-action>
<z303-name>Smith,John</z303-name>
<z303-birth-date>19950803</z303-birth-date>
<z303-delinq-1>00</z303-delinq-1>
<z303-delinq-3>00</z303-delinq-3>
<z303-delinq-n-3>%</z303-delinq-n-3>
<z303-ill-library>MRD</z303-ill-library>
<z303-home-library>REG</z303-home-library>
<z303-ill-total-limit>0010</z303-ill-total-limit>
<z303-ill-active-limit>9999</z303-ill-active-limit>
<z303-send-all-letters>Y</z303-send-all-letters>
<z303-send-con-Ing>ENG</z303-send-con-Ing>
<z303-plain-html>P</z303-plain-html>
<z303-field-1>NEXRSSL</z303-field-1>
<z303-profile-id>STUDENT1</z303-profile-id>
</z303>

<z304>
<record-action>I</record-action>
<z304-id>999999999</z304-id>
<z304-sequence>01</z304-sequence>
<z304-address-type>21</z304-address-type>
<z304-email-address>w999999999@noreply.westminster.ac.uk</z304-email-
address>
</z304>

<z305>
<record-action>I</record-action>
<z305-id>999999999</z305-id>
<z305-sub-library>WST50</z305-sub-library>
<z305-bor-type>UG</z305-bor-type>
<z305-bor-status>05</z305-bor-status>
<z305-expiry-date>20500101</z305-expiry-date>
</z305>

<z308>
<record-action>I</record-action>
<z308-key-type>00</z308-key-type>
<z308-id>999999999</z308-id>
<z308-key-data>999999999</z308-key-data>
<z308-verification-type>00</z308-verification-type>
<z308-verification>03081995</z308-verification>
<z308-encryption>N</z308-encryption>
<z308-status>AC</z308-status>
```

Example 2 of update

```
<p-file-20>
<patron-record>
<z303>
<match-id-type>00</match-id-type>
<match-id>13784098</match-id>
<record-action>U</record-action>
<z303-delinq-3>00</z303-delinq-3>
<z303-delinq-n-3>%</z303-delinq-n-3>
<z303-ill-total-limit>0010</z303-ill-total-limit>
<z303-ill-active-limit>9999</z303-ill-active-limit>
<z303-field-1>BBUSWIT</z303-field-1>
</z303>

<z304>
<record-action>U</record-action>
<z304-id>13784098</z304-id>
<z304-address-type>21</z304-address-type>
</z304>

<z305>
<record-action>U</record-action>
<z305-id>13784098</z305-id>
<z305-sub-library>WST50</z305-sub-library>
<z305-bor-type>UG</z305-bor-type>
<z305-bor-status>05</z305-bor-status>
<z305-expiry-date>20500101</z305-expiry-date>
</z305>
</patron-record>
</p-file-20>
```

Example of deletion

```
<p-file-20>  
<patron-record>  
<z303>  
<match-id-type>00</match-id-type>  
<match-id>225765</match-id>  
<record-action>D</record-action>  
<z303-birth-date></z303-birth-date>  
<z303-ill-library>MRD</z303-ill-library>  
</z303>  
  
<z305>  
<record-action>D</record-action>  
<z305-id></z305-id>  
<z305-sub-library>WTS50</z305-sub-library>  
</z305>  
</patron-record>  
</p-file-20>
```

X-services security

- https for transmission of data via x-services between IDM vault and Aleph
- server-ip-allowed in alephe/tab for restrictions on IPs that can access Aleph via x-server
- www-x user has permissions on what actions the default x-server user can execute

Other considerations

- Working with a remote IDM supplier
- Test and live vaults
- Notion of associating IDM record with Aleph record
- Need to ensure that vault has the correct associations for the records in Aleph
- Migration of users from live vault to test Aleph

Tools for monitoring

- Log monitor checking for errors
 - Emails of errors detected
- Real-time monitor of IDM – Aleph interactions
- Also tool to input xml. Useful for trouble-shooting IDM problems

Real-time monitoring tool

- Display of real-time data from Aleph DB alongside data sent by IDM
- File column displays data sent
- Using X-services to retrieve data from Aleph, not SQL
- Filters: Type of operation; User status; Library; Environment; Errors only, or all transactions
- Final column: 'File' the update-bor request sent

refresh		show last records		10	30	50	100	200	500	Operation type	PU	I	U	D	ALL	Only show Errors	E										
Borrow Status		all	01	02	03	04	05	06	10	11	14	29	Library				ALL	CAV	HRW	MRD	REG	Servers			LIVE	TEST	BOTH
Patron	Operation		Home Library			Changes no./Error no.			Date			Server															
15663500	I		Regent			17/0			[2015-04-17 15:55:15]			TEST															
15663483	I		Cavendish			17/0			[2015-04-17 15:55:14]			TEST															
15663476	I		Regent			17/0			[2015-04-17 15:55:13]			TEST															
15663452	I		Regent			17/0			[2015-04-17 15:55:12]			TEST															
15663421	I		Regent			17/0			[2015-04-17 15:55:11]			TEST															
13784098	U		Harrov			10/0			[2015-04-17 15:24:47]			TEST															
14726738	U		Regent			10/0			[2015-04-17 15:10:46]			TEST															
14804182	U		Harrov			3/0			[2015-04-17 15:07:22]			TEST															
13822233	U		Cavendish			3/0			[2015-04-17 15:07:06]			TEST															
15002462	U		Marylebone			8/0			[2015-04-17 14:26:46]			TEST															
227415	U		NotFound			ERROR			[2015-04-17 14:21:11]			TEST															
13787929	U		Marylebone			7/0			[2015-04-17 14:11:18]			TEST															
13787929	U		Marylebone			9/0			[2015-04-17 14:10:45]			TEST															
14095195	U		NotFound			ERROR			[2015-04-17 14:01:40]			TEST															
14680210	U		Cavendish			3/0			[2015-04-17 13:57:48]			TEST															
15663225	I		Regent			17/0			[2015-04-17 13:41:52]			TEST															
14921108	U		Marylebone			3/0			[2015-04-17 13:41:42]			TEST															
14921108	U		Marylebone			3/0			[2015-04-17 13:39:41]			TEST															
15422248	U		Marylebone			8/0			[2015-04-17 13:24:42]			TEST															
14549230	U		Marylebone			3/0			[2015-04-17 13:13:15]			TEST															
14759367	U		Marylebone			3/0			[2015-04-17 12:31:06]			TEST															
14759367	U		Marylebone			3/0			[2015-04-17 12:29:06]			TEST															
14286562	U		Regent			3/0			[2015-04-17 12:02:37]			TEST															

Field Name	Aleph Value	IDM Request
ref	999999999.1.1429198060.000.31	999999999.1.1429198060.000.31
timestamp	2015-04-17 15:20:02	2015-04-17 15:20:02
z303-id	999999999	N/A
z303-name-key	smith john 999999999	N/A
z303-user-library	WST50	N/A
z303-open-date	17/04/2015	N/A
z303-update-date	17/04/2015	N/A
z303-con-Ing	ENG	N/A
z303-name	Smith,John	Smith,John
z303-delinq-1	00	00
z303-delinq-n-1		N/A
z303-delinq-1-update-date	00000000	N/A
z303-delinq-2	00	N/A
z303-delinq-n-2		N/A
z303-delinq-2-update-date	00000000	N/A
z303-delinq-3	00	00
z303-delinq-n-3	%	%
z303-delinq-3-update-date	00000000	N/A
z303-profile-id	STUDENT1	STUDENT1
z303-ill-library	Marylebone	MRD
z303-home-library	Regent	REG
z303-field-1	NEXRSSL	NEXRSSL
z303-note-1		N/A
z303-note-2		N/A
z303-ill-total-limit	0010	0010
z303-ill-active-limit	9999	9999

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://library-mon...are.php?&limit=30 x http://library-mon...1429198060.000.31 x

library-monitor.cloudapp.net/aleph/compare.php?ref=99999999.11429198060.000.31

Most Visited Getting Started Save to Mendeley Accounts Reading list bookmark... Add to My Bookmarks

z303-delinq-n-3	%	%
z303-delinq-3-update-date	00000000	N/A
z303-profile-id	STUDENT1	STUDENT1
z303-ill-library	Marylebone	MRD
z303-home-library	Regent	REG
z303-field-1	NEXRSSL	NEXRSSL
z303-note-1		N/A
z303-note-2		N/A
z303-ill-total-limit	0010	0010
z303-ill-active-limit	9999	9999
z303-send-all-letters	Y	Y
z303-send-con-Ing		ENG
z303-plain-html	P	P
z303-birth-date	10/01/1970	19950803
z303-title		N/A
z303-upd-time-stamp	201504171657014	N/A
z304-id	999999999	999999999
z304-sequence	01	01
z304-email-address	w999999999@my.westminster.ac.uk	w999999999@noreply.westminster.ac.uk
z304-date-from	00000000	N/A
z304-date-to	00000000	N/A
z304-address-type	21	21
z304-update-date	20150417	N/A
z304-upd-time-stamp	201504171657015	N/A
z305-id	999999999	999999999
z305-sub-library	WST50	WST50
z305-open-date	17/04/2015	N/A

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://library-mon...are.php?&limit=30 x http://library-mon...1429198062.000.31 x http://library-mon...9198060.000.31.xml x +

library-monitor.cloudapp.net/aleph/compare.php?ref=999999999.U.1429198062.000.31

Most Visited Getting Started Save to Mendeley Accounts Reading list bookmark... Add to My Bookmarks

z303-field-1	NEXRSSL	N/A
z303-note-1		N/A
z303-note-2		N/A
z303-ill-total-limit	0010	N/A
z303-ill-active-limit	9999	N/A
z303-send-all-letters	Y	N/A
z303-send-con-Ing		N/A
z303-plain-html	P	N/A
z303-birth-date	10/01/1970	N/A
z303-title		N/A
z303-upd-time-stamp	201504171657014	N/A
z304-id	999999999	999999999
z304-sequence	01	01
z304-email-address	w999999999@my.westminster.ac.uk	w999999999@my.westminster.ac.uk
z304-date-from	00000000	N/A
z304-date-to	00000000	N/A
z304-address-type	21	21
z304-update-date	20150417	N/A
z304-upd-time-stamp	201504171657015	N/A
z305-id	999999999	999999999
z305-sub-library	WST50	WST50
z305-open-date	17/04/2015	N/A
z305-update-date	17/04/2015	N/A
z305-bor-type	Undergraduate	N/A
z305-bor-status	F/T Undergrad.	N/A
z305-expiry-date	01/01/2050	20500101
z305-loan-permission	Y	N/A

z303-delinq-n-3	%	%
z303-delinq-3-update-date	00000000	N/A
z303-profile-id	STUDENT1	STUDENT1
z303-ill-library	Marylebone	MRD
z303-home-library	Regent	REG
z303-field-1	NEXRSSL	NEXRSSL
z303-note-1		N/A
z303-note-2		N/A
z303-ill-total-limit	0010	0010
z303-ill-active-limit	9999	9999
z303-send-all-letters	Y	Y
z303-send-con-lng		ENG
z303-plain-html	P	P
z303-birth-date	10/01/1970	19950803
z303-title		N/A
z303-upd-time-stamp	201504171657014	N/A
z304-id	999999999	999999999
z304-sequence	01	01
z304-email-address	w999999999@my.westminster.ac.uk	w999999999@noreply.westminster.ac.uk
z304-date-from	00000000	N/A
z304-date-to	00000000	N/A
z304-address-type	21	21
z304-update-date	20150417	N/A
z304-upd-time-stamp	201504171657015	N/A
z305-id	999999999	999999999
z305-sub-library	WST50	WST50
z305-open-date	17/04/2015	N/A

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://library-mon...are.php?&limit=30 x http://library-mon...1429198062.000.31 x http://library-mon...9198060.000.31.xml x +

library-monitor.cloudapp.net/aleph/compare.php?ref=999999999.U.1429198062.000.31

Most Visited Getting Started Save to Mendeley Accounts Reading list bookmark... Add to My Bookmarks

z303-field-1	NEXRSSL	N/A
z303-note-1		N/A
z303-note-2		N/A
z303-ill-total-limit	0010	N/A
z303-ill-active-limit	9999	N/A
z303-send-all-letters	Y	N/A
z303-send-con-Ing		N/A
z303-plain-html	P	N/A
z303-birth-date	10/01/1970	N/A
z303-title		N/A
z303-upd-time-stamp	201504171657014	N/A
z304-id	999999999	999999999
z304-sequence	01	01
z304-email-address	w999999999@my.westminster.ac.uk	w999999999@my.westminster.ac.uk
z304-date-from	00000000	N/A
z304-date-to	00000000	N/A
z304-address-type	21	21
z304-update-date	20150417	N/A
z304-upd-time-stamp	201504171657015	N/A
z305-id	999999999	999999999
z305-sub-library	WST50	WST50
z305-open-date	17/04/2015	N/A
z305-update-date	17/04/2015	N/A
z305-bor-type	Undergraduate	N/A
z305-bor-status	F/T Undergrad.	N/A
z305-expiry-date	01/01/2050	20500101
z305-loan-permission	Y	N/A

And finally

- Questions?
- Email: g.j.bennett@westminster.ac.uk