

# Secure sharing of Higher Education Achievement Reports (HEARs) with User- Managed Access (UMA)

Maciej Machulak (Newcastle University, UK)  
maciej.machulak@ncl.ac.uk

# Outline

2

- User-Managed Access
  - ▣ Why needed
  - ▣ Architecture
  - ▣ Protocol
- SMART Project
  - ▣ Higher Education Use Case
  - ▣ Demo
- Summary
- Q&A

# The “data price” for online service is too high: typing...

3

- Provisioning by hand
- Provisioning by value
- Oversharing
- Lying!



# The “data price” for online service is too high: connecting...

4



- Meaningless consent to unfavorable terms
- Painful, inconsistent, and messy access management
- Oversharing of lots of real information

# The “data price” for online service is too high: private URLs...

5



- Handy but insecure
- Unsuitable for really sensitive data

# Privacy is not about secrecy

*The goal of a flexible, user-centric identity management infrastructure must be to allow the user to quickly determine what information will be revealed to which parties and for what purposes, how trustworthy those parties are and how they will handle the information, and what the consequences of sharing their information will be”*

– Ann Cavoukian, Ontario Information and Privacy Commissioner, **Privacy in the Clouds** paper



It's about context, control, choice, and respect























# UMA gives users a true digital footprint control console

smartam.

Welcome Lukasz Moren | Logout

-  Data
-  Contacts
-  Applications
-  History
-  Notifications

Home » History

-  **Lukasz Moren** accessed **lukaszmoren's date of birth** from  Career Monster  
 Newcastle University S3P  
28.09.2012 08:37 ([show details](#)) [modify access](#)
-  **Lukasz Moren** accessed **lukaszmoren's grades** from  Career Monster  
 Newcastle University S3P  
11.09.2012 16:50 ([show details](#)) [modify access](#)
-  **Maciej Machulak** accessed **lukaszmoren's last name** from  Vodafone  
 **lukaszmoren's last name**  
 Newcastle University S3P  
11.09.2012 16:50 ([hide details](#)) [modify access](#)
-  **Bob Umanitarian** accessed **lukaszmoren's first name** from  Vodafone  
 Newcastle University S3P  
11.09.2012 16:50 ([show details](#)) [modify access](#)
-  **Bob Umanitarian** accessed **lukaszmoren's grades** from  Lloyds TSB  
 Newcastle University S3P  
23.08.2012 13:09 ([show details](#)) [modify access](#)
-  **Bob Umanitarian** accessed **lukaszmoren's location** from  Lloyds TSB  
 Newcastle University S3P  
23.08.2012 13:09 ([show details](#)) [modify access](#)
-  **Lukasz Moren** accessed **lukaszmoren's grades** from  Career Monster  
 Newcastle University S3P  
23.08.2012 13:04 ([show details](#)) [modify access](#)

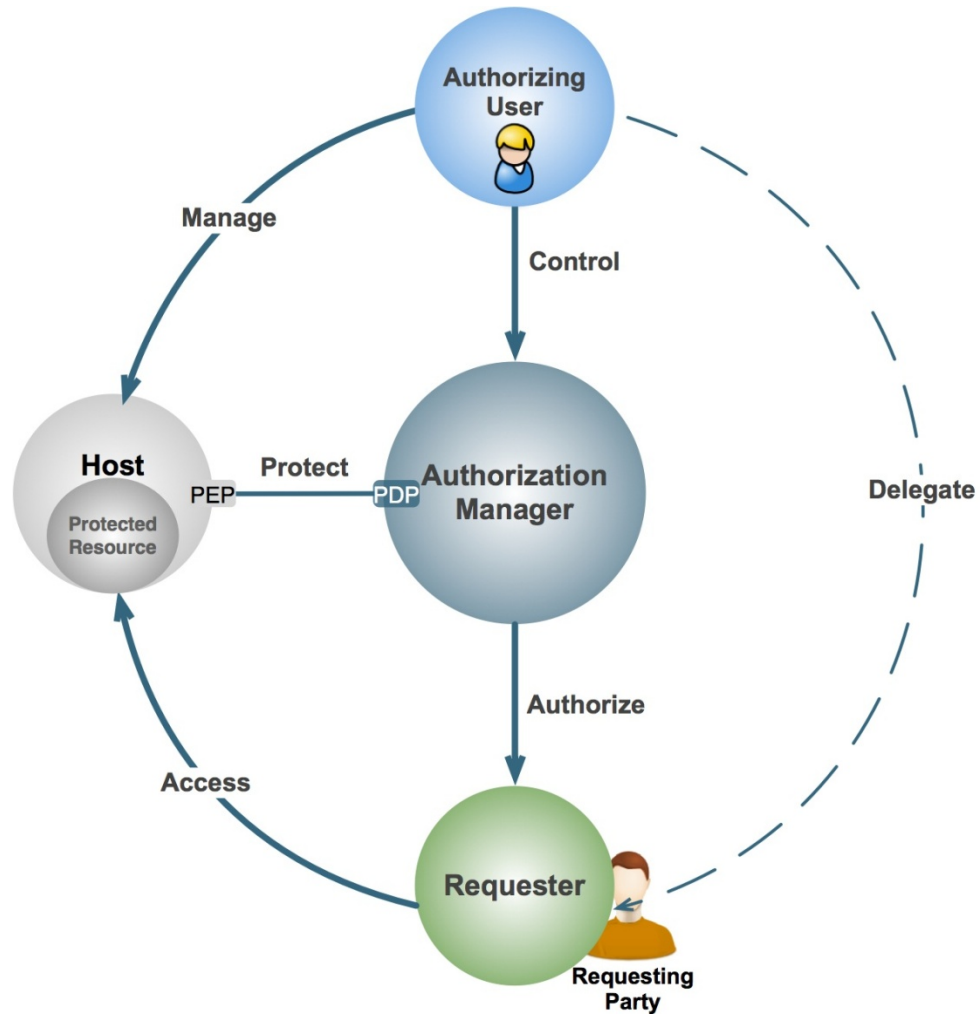
# UMA gives users a true digital footprint control console

- *Web 2.0 access control is inconsistent and unsophisticated*
- *To share with others, you have to list them literally*
- *You have to keep rebuilding your “circles” in new apps*
- *You can’t advertise content without giving it away*
- *You can’t get a global view of who accessed what*
- You can **unify** access control under one app
- Sharing policies can test for **claims** like “over 18”
- You can **reuse** the same policies with multiple sites
- You can control access to stuff with **public** URLs
- You can **manage** and **revoke** access from one place



# UMA Players

9



# UMA - Protocol

10

**(1) Trust a Token**

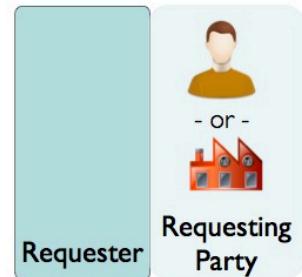
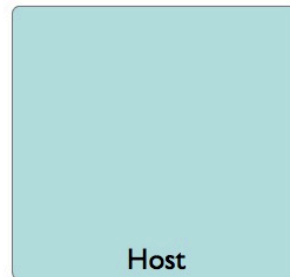
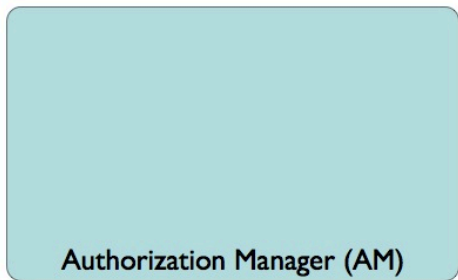
**(2) Get a Token**

**(3) Use a Token**

# UMA - Protocol

11

## □ Trust a Token

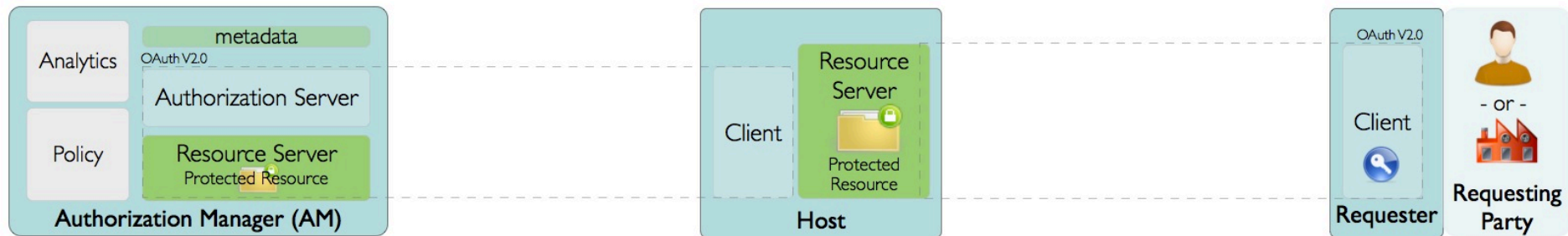


**Authorizing User** (user at browser or other user agent)

# UMA - Protocol

12

## □ Trust a Token

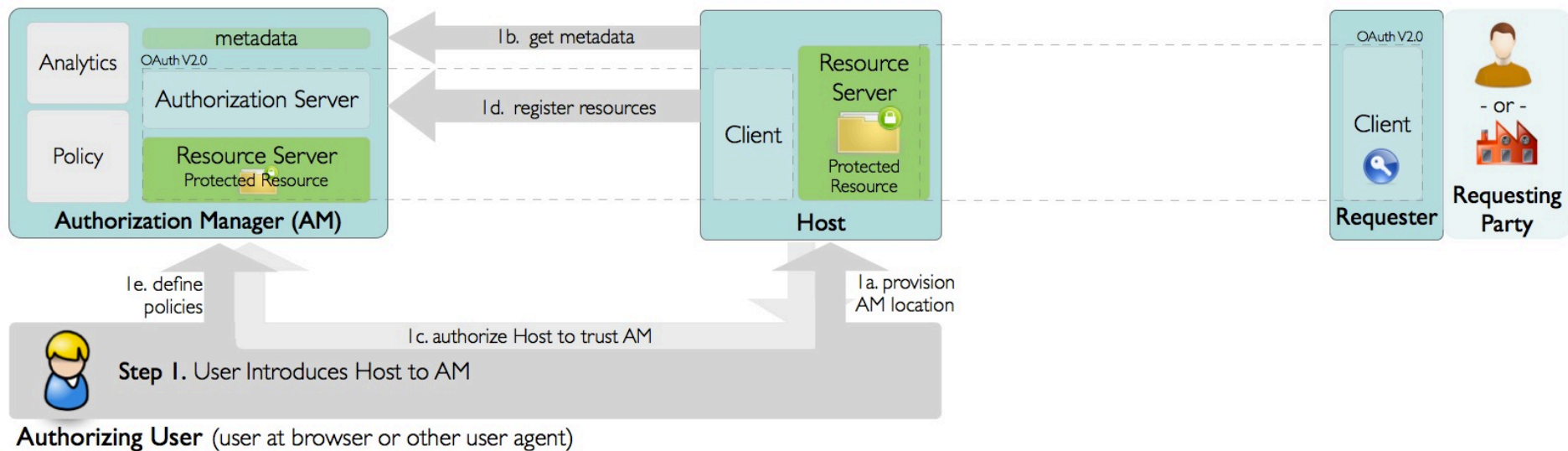


**Authorizing User** (user at browser or other user agent)

# UMA - Protocol

13

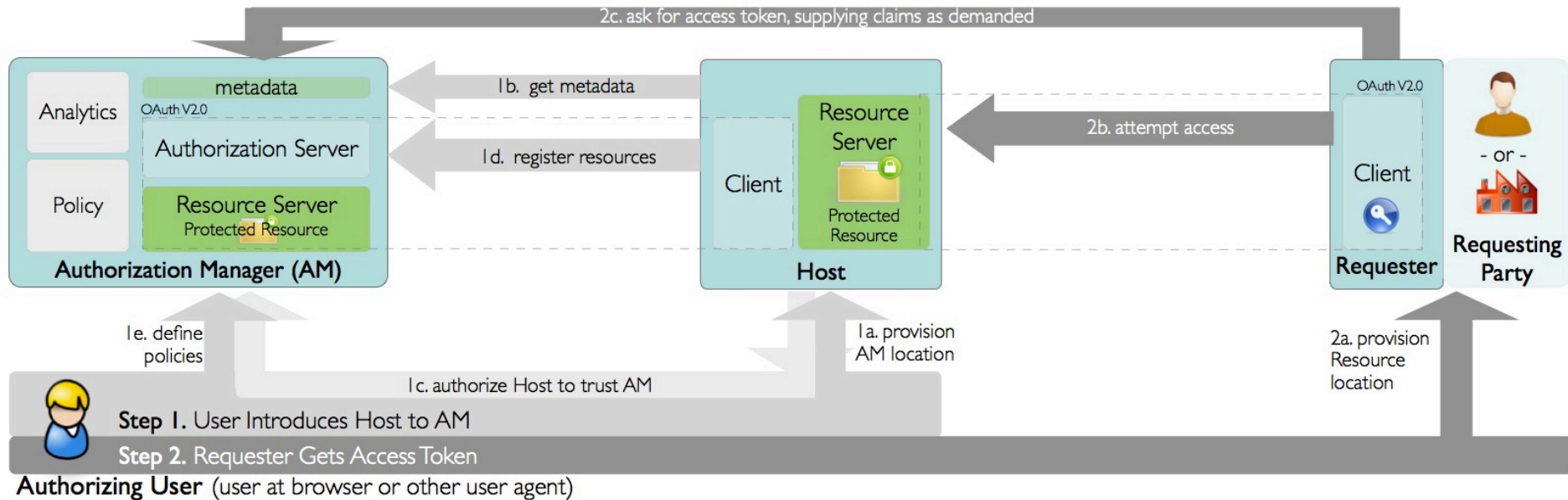
## □ Trust a Token



# UMA - Protocol

14

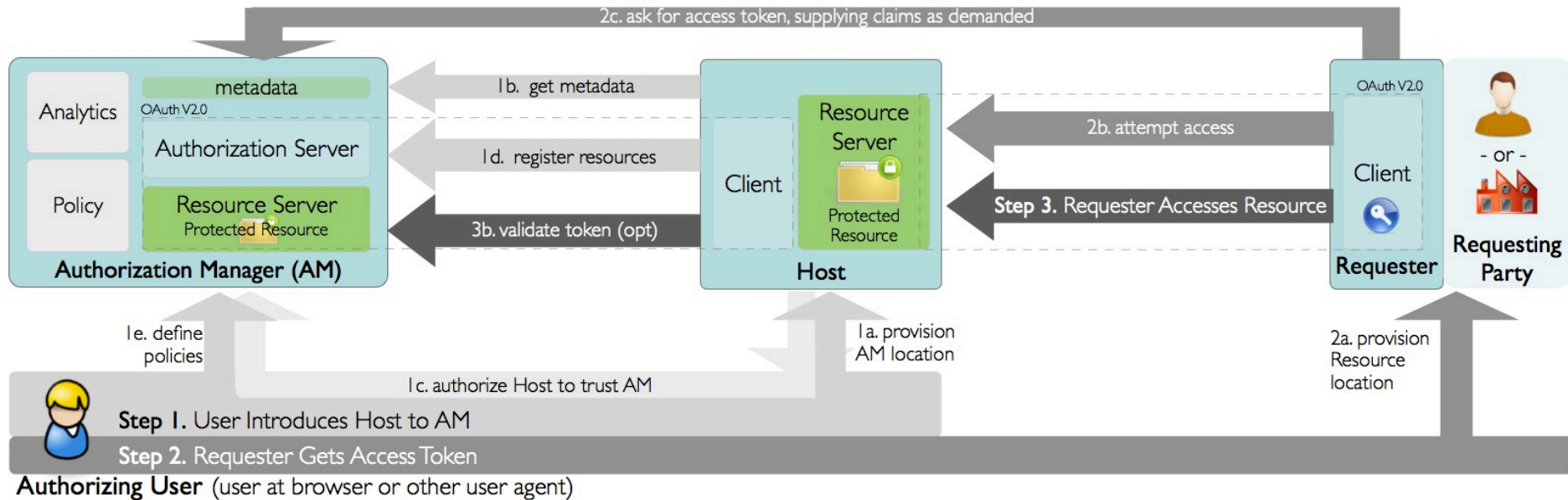
## □ Get a Token



# UMA - Protocol

15

## □ Use a Token



# SMART

16

## SMART Project

### Newcastle University, UK



# The SMARTAM.org project

17

**smartam.org**  
your one place to share your data, securely.

1. Register your data  
personal data, photos, documents
2. Set permissions  
to read or manage
3. Choose contacts  
friends, family, colleagues
4. Share your data  
maintaining your privacy



Login with your existing account:



[about smartam.](#) | [about uma](#) | [about us](#) | [terms and conditions](#) | [privacy policy](#) |



The “Polish Gang of Four” ...plus one

See also the SMARTAM implementation FAQ  
at <http://tinyurl.com/umafaq>

# The SMART project is...

18

- About “Student-Managed Access to Online Resources” with UMA
- At the School of Computing Science, Newcastle University, UK
  - ▣ Affiliated with the Centre for Cybercrime and Computer Security
  - ▣ The team Prof. Aad Van Moorsel, Maciej Machulak, Łukasz Moreń
    - Alumni: Maciej Wolniak, Chris Franks, Jacek Szpot, and Domenico Catalano (Oracle)
  - ▣ A product of HEFCE/JISC funding (Jan '10–Aug '12)
  - ▣ Developing SMARTAM, UMA/i, Puma, and Apache Amber
- Blogging at <http://smartjisc.wordpress.com> and tweeting @smartproject

# One of the SMART use cases: Transcript of Records sharing

19

- Based on “Sharing Trustworthy Personal Data with Future Employers” scenario\* submitted to UMA WG
  - ▣ Students interact with online job application systems
  - ▣ Share their exam marks, certificates, references, etc.
  - ▣ Data is stored at their various home Higher Education institutions
- See “Secure sharing of Higher Education Achievement Reports (HEARs) at Newcastle University using SMART” case study\*\*

\* [http://kantarainitiative.org/confluence/display/uma/cv\\_sharing\\_scenario](http://kantarainitiative.org/confluence/display/uma/cv_sharing_scenario)

\*\* [http://smartjisc.files.wordpress.com/2012/10/smart\\_hears\\_draft012.pdf](http://smartjisc.files.wordpress.com/2012/10/smart_hears_draft012.pdf)

# HEAR Documents

20

- Electronic document that provides a single comprehensive record of a learner's achievement at a HE institution.
- Contains information:
  - ▣ identifying the holder of the qualification;
  - ▣ on the HE institution and the national higher education system;
  - ▣ on the qualification, its level, and details of each of the modules or units studied
  - ▣ on the form of assessment (timed examination, essay, project, dissertation),
  - ▣ on marks awarded, and their relative weighting towards the final summary mark or grade, etc.
  - ▣ ...

# Problem scenario

21



Bob

# Problem scenario

22



Bob



# Problem scenario

23

The diagram illustrates a job application process. On the left, the CareerMonster logo is shown above a stack of documents labeled "job positions". On the right, the Newcastle University S<sup>3</sup>P logo is shown above a stack of documents labeled "personal information (incl. name, academic records, etc.)". In the center, a modal window titled "Applying for Junior Database Architect" is displayed. The modal contains the following text and form elements:

**Applying for Junior Database Architect**

In order to apply, you need to provide the following information:

**Full name** · incomplete

Please provide your first, second, and last name:

**Grades** · incomplete

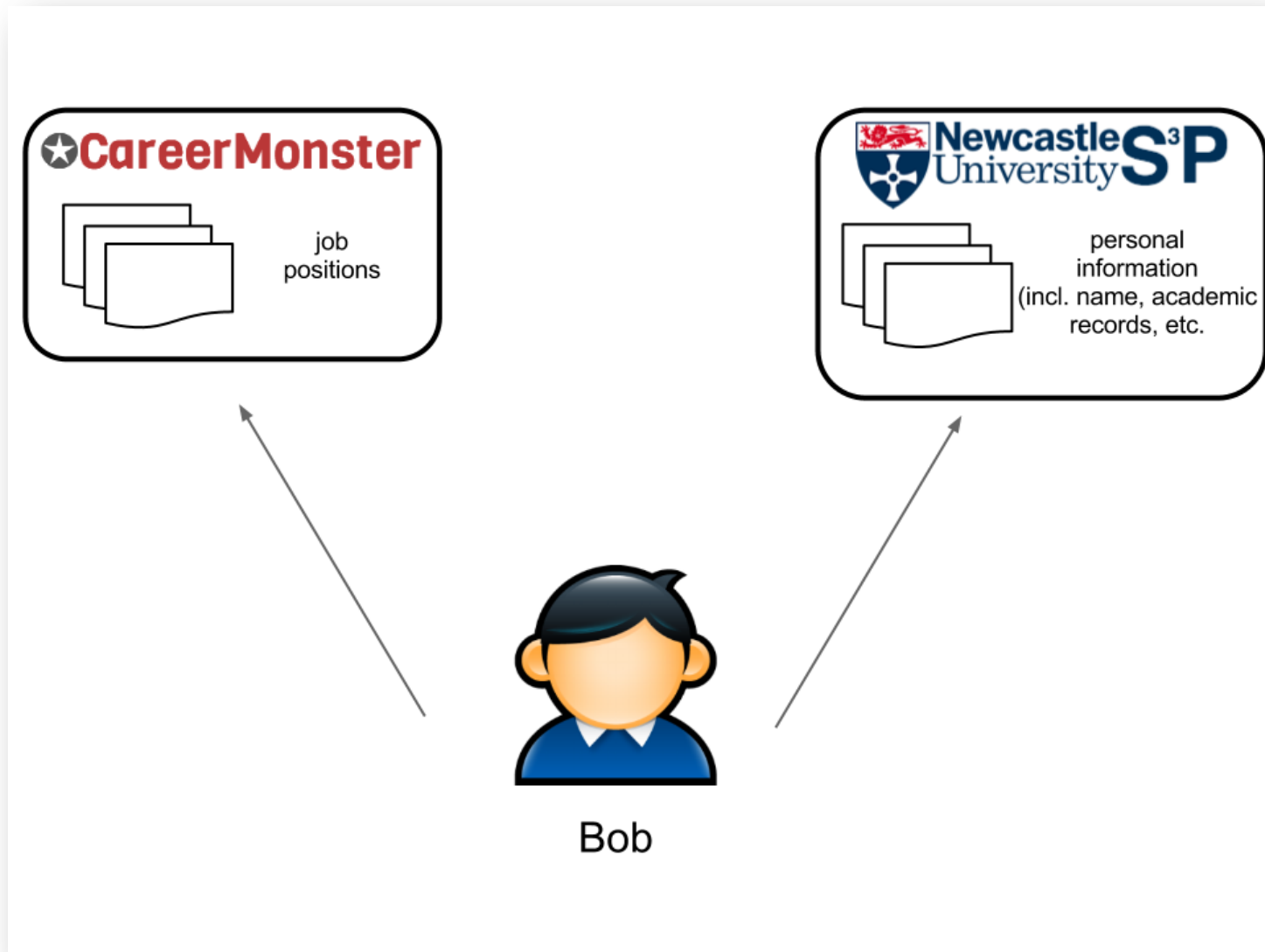
Upload your Transcript of Records:

No file chosen

An arrow points from the "job positions" stack to the modal window.

# Problem scenario

24

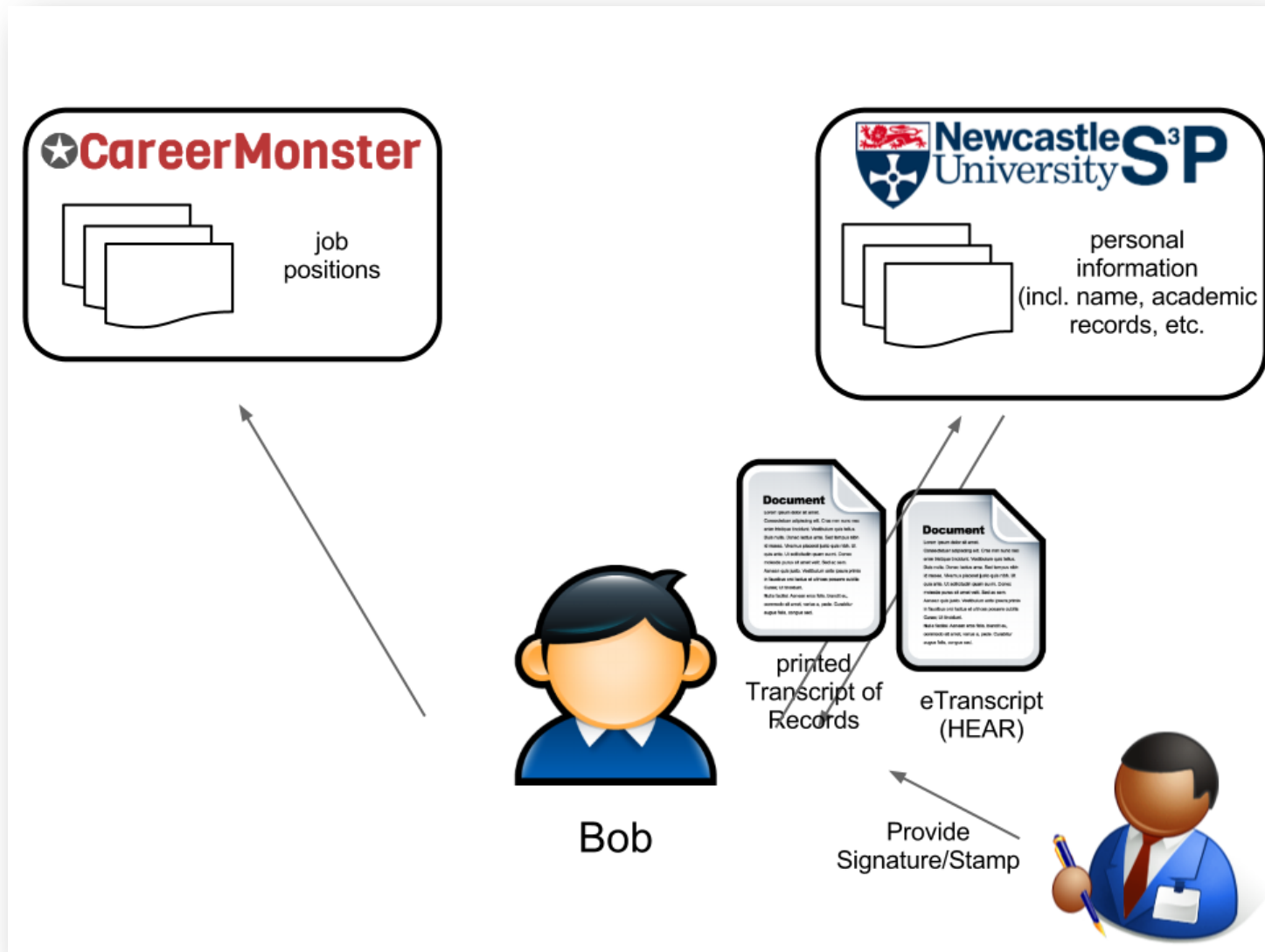






# Problem scenario

26



# Problem scenario



**CareerMonster**  
job positions



**Newcastle University S<sup>3</sup>P**  
personal information  
(incl. name, academic records, etc.)

Signed,  
Stamped &  
Scanned  
Transcript of  
Records  
/  
eTranscript  
(HEAR)



Bob



printed  
Transcript of  
Records

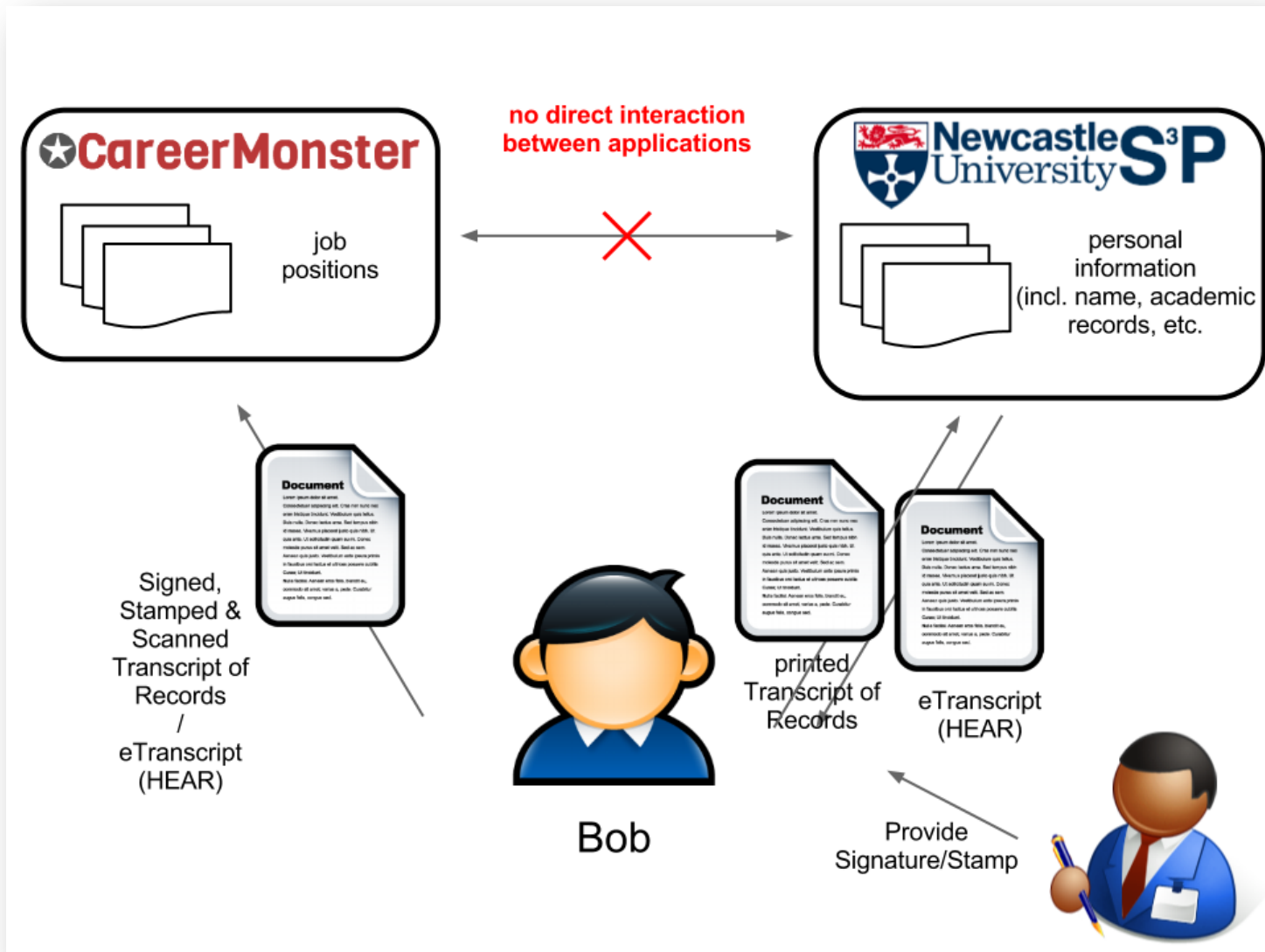


eTranscript  
(HEAR)

Provide  
Signature/Stamp



# Problem scenario



# Problems

29

- Getting the “Transcript of Records” document:
  - Engaging University staff to obtain a signed/ stamped version of the document, or...
  - Printing out the document from an online system provided by a higher-education institution, such as the S3P Portal\* at Newcastle University, or...
  - Obtaining an eTranscript document, digitally signed by a higher-ed institution, e.g. in HEAR form.
- Going through this process every time the document changes

\* <https://s3p.ncl.ac.uk>

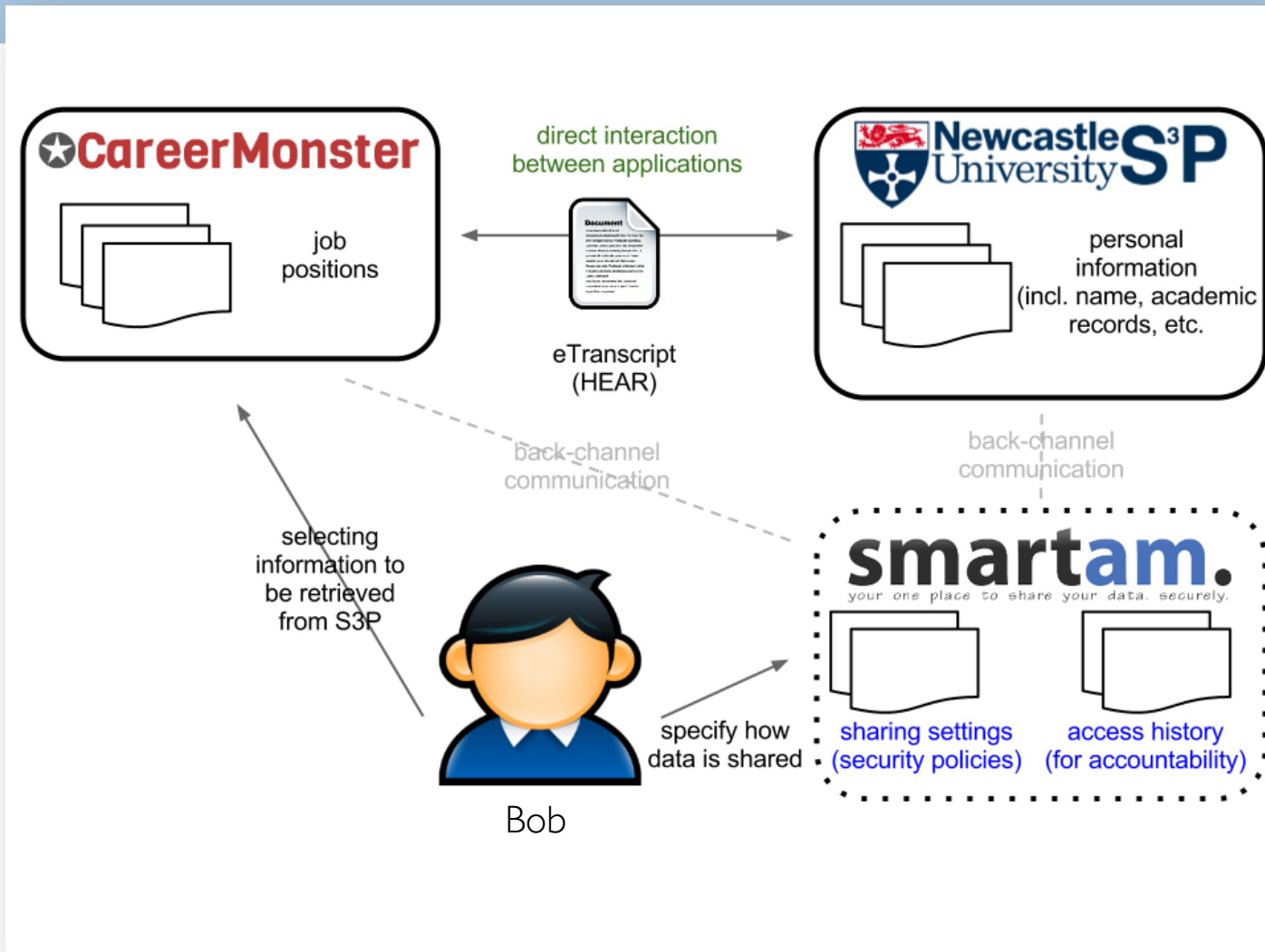
# Improvements

30

- Allow students and graduates to easily establish access to their educational data:
  - ▣ Without having to engage University staff
- Give third-party web apps, such as career services and other universities, access to current student data:
  - ▣ Continuous access to academic records during (often long) job application processes
- Give students full control over sharing of their personal information stored at Higher Education institutions
  - ▣ Access authorization
  - ▣ Insight into access requests

# Improved scenario

31



# Benefits

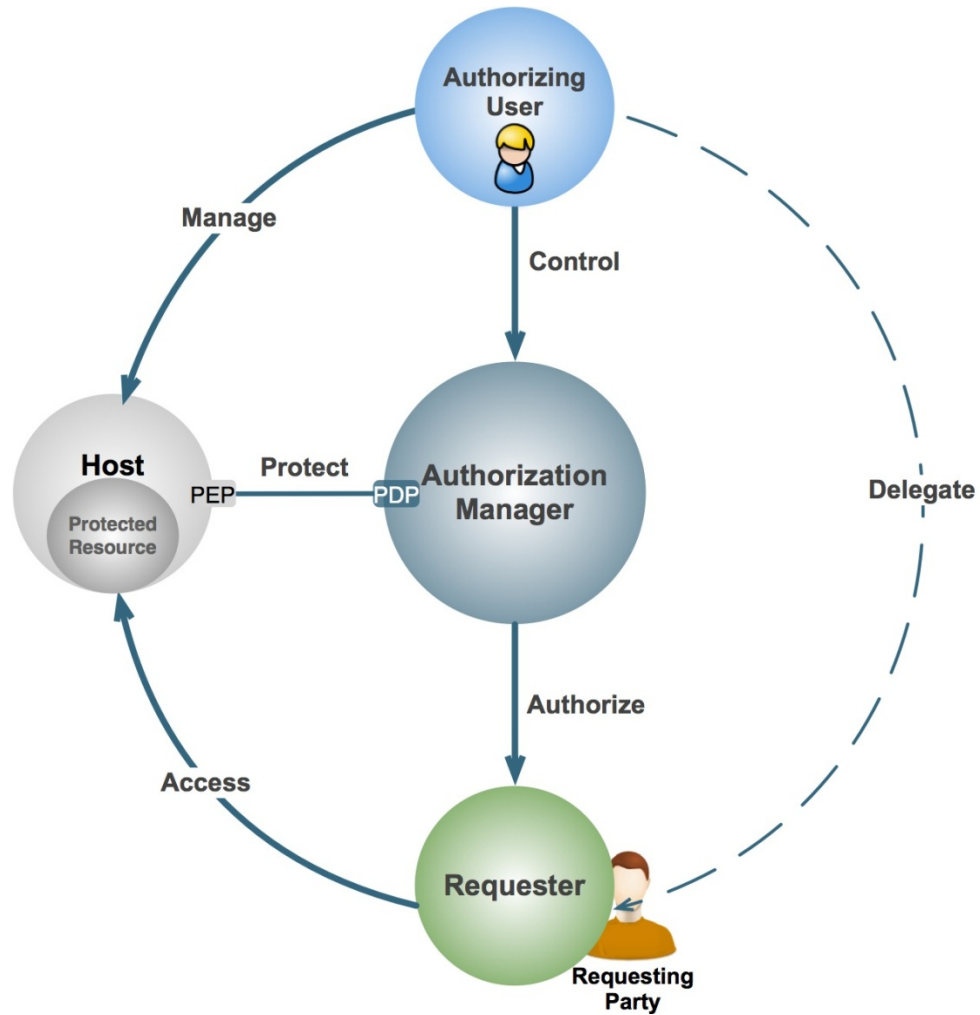
32

- Apps access data directly from trustworthy sources:
  - ▣ Simplified trust path;
  - ▣ Possibly continuous access to “fresh” data;
- Access does not require manual processes (signining, uploading, etc.) to take place;
- Authorization to access distributed data using a central component:
  - ▣ Unified UI for setting access control permissions
  - ▣ Authorization stored centrally - can be easily managed and revoked by the end-user;
- Centrally-located dashboard provides insight into how information is shared and handled;



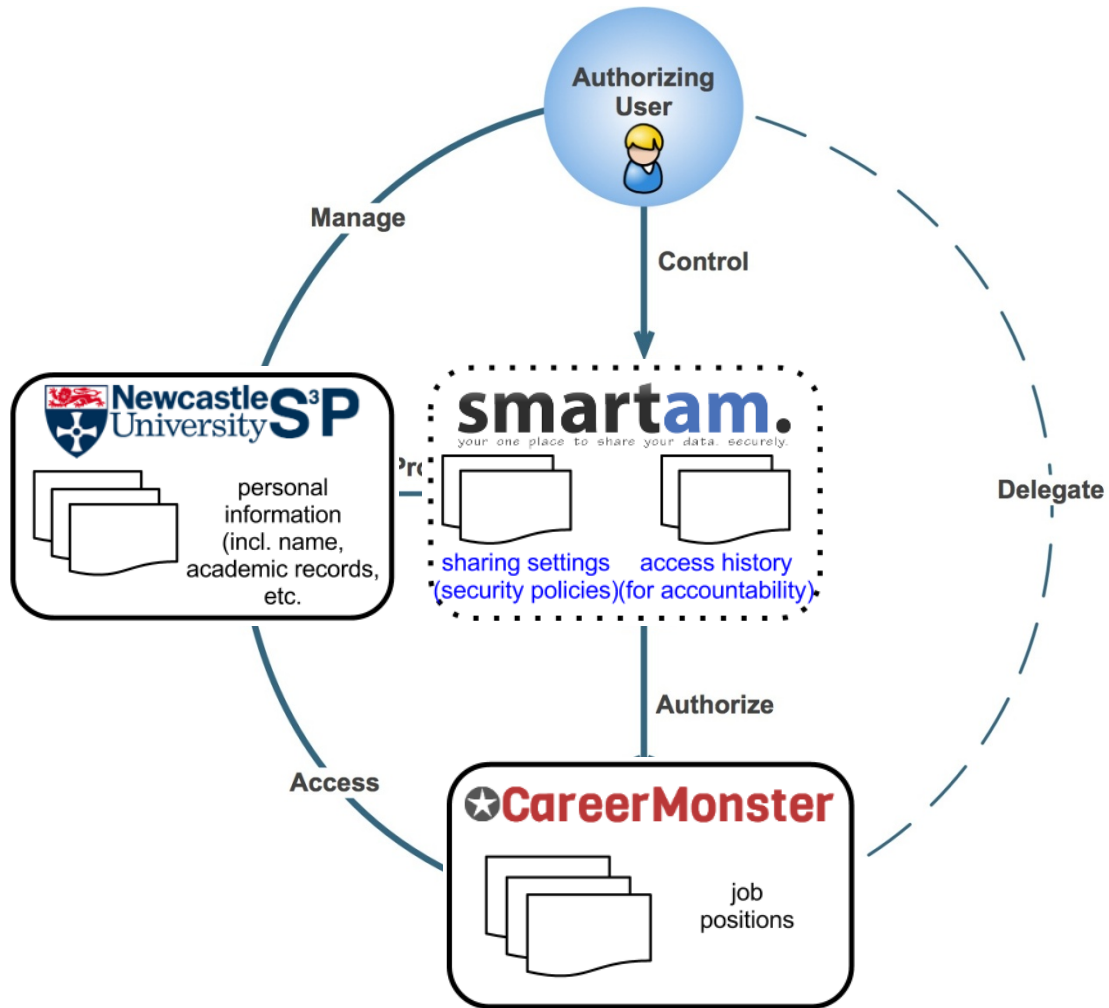
# Demo

33



# Demo

34



# The SMART demo

35

- “Newcastle S3P” demo host app:  
<https://pumahostone.appspot.com>
- “CareerMonster” demo requester app:  
<https://pumarequesterone.appspot.com>
- SMARTAM.org authorization manager  
<https://www.smartam.org>

# Questions and Discussion

36



# Acknowledgements

37

**Eve L. Maler**

UMA WG Chair

emaler@forrester.com

**Thomas Hardjono**

UMA WG Specification Editor

hardjono@mit.edu

**Domenico Catalano**

UX/Graphics Designer

domenico.catalano@oracle.com

**Members of the UMA WG**