Kennisnet UMA Case Study: How to give K-12 students control of their data

Homework Assistance

Erwin Bomas, M. Dobrinic
September 2014

See also the associated slides.

Introduction

The ecosystem of K-12 education is very dynamic and the number of cloud based services that support education is expanding rapidly. This results in more and more student data being created at many different locations. In order to make maximum use of existing data while respecting privacy and creating end user transparency in who is using what, the UMA specification offers the tools for implementing such an environment. Kennisnet is the public educational organization which supports and inspires Dutch primary, secondary and vocational institutions in the effective use of ict a.o. by offering public online services and platforms. Kennisnet investigates the user-centric approach of data management for education using UMA. Kennisnet created a mock-up of an UMA based dashboard for end users.

Problem Scenario

The case study zooms in on sharing data between an Electronic Learning Environment (ELE) and a Homework Institute (HI). The HI wants to help a student on those subjects that need extra attention. It only seems natural that this is different for every student, so this follows the Personalized Learning [http://en.wikipedia.org/wiki/Personalized_learning] principle. To be able to do so, it somehow needs to know what those subjects are. The best way to find this information, is to get to the ELE and get the progress of the student on a particularsubject. This requires the exchange of student data between different organizations, which is a challenging exercise in many ways.

The Privacy subject also becomes more and more important. An example is the InBloom initiative, that was a well-funded project to help exchanging student data in the United States. Because of major privacy concerns of parents and the resulting lack of confidence in their approach, the InBloom operation was shut down early 2014, before it had the chance to establish itself.

European legislation regarding the use of Personal Data has created a renewed spotlight on how storing as well as exchanging personal data is done. In particular, this relates to how information is disclosed, the means that a user has the ability to provide consent for exchanging information, as well as the purpose for which actual data is being requested by each organization. These regulations look like they make it inevitable to make the user play a more active role in data exchange.

While there are Identity Federations (like the Kennisnet Federation) to decentralize identity management, the most commonly applied solution when multiple organizations want to share personal data among each other is a systemic approach: a set of agreements is established, and organizations that want to join in the exchange must conform to these agreements. After which account linking between organizations can take place. While there are usecases in which this solves the actual problem, it has serious scalability issues (governance, user transparancy, etc.) and can become a large hurdle for smaller parties to be able to conform to.

When the (adolescent) user or its custodian becomes a participant in data exchange, there is common fear that existing processes will be disturbed. Also, the matter of being over-asked to provide consent for everything that is happening can create a bad experience. This doesn't even mention the situation that all users actually understand the questions that they are being asked to make the right decision These are just some of the usability challenges that, if unaddressed, can work out pretty bad for actually helping education.

Proposed Improvements

Kennisnet has taken the User Experience as the leading factor in mapping out a possible solution. By building a mock-up, possible usability issues can be addressed. The mock-up is not just a set of screens, but is backed up by the UMA specification. [slides 3-6]

Cental to the mock-up (as well as to the user) is the Kennisnet Dashboard, that could be operated by the Kennisnet organization. The Dashboard is a service at which users can log in to manage access policies. The Dashboard can also provide an overview of the shared resources, with whom they are shared and for what purpose the data is being requested. The Kennisnet Dashboard is an Authorization Server.

The Electronic Learning Environment acts as a Resource Server, such that it interacts with the Dashboard to register resources of the student for sharing, and offers an API to other Services to expose the student's resources. The relationship between the ELE and a school can be preconfigured in the Dashboard (by the school), such that it becomes possible to include this relationship in access policies when specific permission are requested and consent requests are required. This way, there is no user interaction required when (the custodian of) the student chooses to activate these policies.

The Homework Institute will access data through an API at the Electronic Learning Environment where a user is taking a course. As such, it acts as a Client, that seeks authorization at the Dashboard, and references the resource by requesting it from the source. The process of getting authorization can include the purpose for which the Client seeks access. This purpose is stored by the Dashboard, but it can also be a parameter in a Dashboard-managed access policy that can lead to the automatic granting of authorization to the resource.

While UMA creates an excellent framework to build a solution for the problem, there are still some issues to address. One is how to set up the rules for purpose-binding, the legal obligation to make explicit the purpose of use of the personal data that is to be collected. While the technical flows leave room for a possible solution, there are also many legal issues regarding this subject. More work needs to be done here to find the right answers. Another issue is a Resource Discovery facility, that helps to make the flows work seamlessly. A possible solution is for the Education domain to specify rules (or something of a resource schema) such that the Dashboard can include a (user consented) service for Resource Discovery. This particular problem is not solved in this case study though.

Solution Specifics

In the Dashboard, the main screen involves providing an overview of the state of data sharing. The main screen provides an overview of Clients for which access requests are pending authorization of the user, the resources being shared and with whom, as well as a timeline that gives feedback on client seeking (authorized) access to resources. [slide 8]

The categorized data overview actually shows all the resources that different Resource Servers have registered with the Dashboard for the logged in user. There is an overview by data category/ recource type and one by service supplier. Note that this access also accompanies the sharing purpose, as well as an expiration to the authorization. Using expirations here increases the maintainability of managing all permissions. [slides 9-11]

Because UMA is an open standard, it is also possible to incorporate public services that are not specific to the educational domain, such as social media services like Twitter or even Fitbit. [slide 12-13]

From a Dashboard-user perspective, Access Policies are means to implement Privacy. To make it easier to work with, multiple privacy levels are introduced. Each level represents (an incremental) pre-set authorizations to consent questions. [slide 14]

Deliverable

The accompanying presentation shows the screens, as well as the swimlanes that represent the UMA protocol flows as they are being used. [slide 15-36]