**D1.2 State of the Art MOOC, Tablet, Security and Identity Management (V1)**

•••••••••••••••••••••••••••••••••••••••••••••

Edited by: Antoine Garnier

Date: December 02nd,2015

Table of Contents

1. Introduction 4

2. LMS 5

2.1. Presentations of the main existing LMS on the market 5

2.1.1. Open EdX 5

2.1.2. Canvas 6

2.1.3. Moodle 7

2.1.4. Blackboard 8

2.1.5. Desire2Learn 8

2.2. Technical description and comparison 8

3. Authoring tools 13

3.1. What does an authoring tool permit to create? 13

3.1.1. Your MOOC with EdX, Coursera or Udemy… 13

3.2. Operation of the tool 16

3.2.1. Description of SCORM 16

3.2.2. Operation of an integrated authoring tool 17

3.3. Comparisons of the main integrated solutions 21

4. Contents 22

4.1. Description of the various contents in a MOOC 22

4.1.1. A massive use of videos 22

4.1.2. Images and text 24

4.1.3. 3D, AR 25

4.2. Standards for contents 26

4.2.1. Online standards 26

4.2.2. Coming offline standard: edupub 27

5. Learning Analytics 28

5.1. Presentations of the subject 28

5.1.1. Definition 28

5.1.2. Data retrieved 28

5.1.3. Aim of LA 28

5.1.4. Use case 28

5.1.5. Utilizations 28

5.1.6. Materialization 29

5.1.7. First users 29

5.1.8. LA Methods 29

5.2. Presentations of the different standards 30

5.2.1. edX Insights 30

5.2.2. xAPI 31

5.2.3. Caliper Analytics 32

5.3. Presentations of different software 34

5.3.1. Brightspace : LeaP 34

5.3.2. SNAPP 36

5.3.3. LOCO-Analyst 38

6. Security and Authentication 41

6.1. Roles and Use cases 41

6.1.1. Content Creators 41

6.1.2. Content Consumers 41

6.2. Information Security Key Concepts 41

6.2.1. Availability 41

6.2.2. Confidentiality & Integrity 41

6.2.3. Authentication & Non-repudiation 42

6.2.4. Digital Rights Management 42

6.3. Mobile Security 42

6.3.1. Device Security and TEE 42

6.3.2. Application Security 43

6.3.3. Digital Identities (device & user) 43

6.4. User Authentication Methods 43

6.4.1. 3-factor Authentication 43

6.4.2. One-time-passwords vs Public Key Infrastructures 43

6.4.3. Biometry on the rise 44

6.4.4. Software vs. Hardware Tokens 44

6.4.5. Federated Identity (OpenID, SAML, OAuth) 45

6.5. Security Implementation Approaches 45

6.5.1. Standards 45

6.5.2. Best Practices 45

6.5.3. Security through Obscurity 46

6.6. Solution Recommendations 46

6.6.1. NFC & Contactless Cards 46

6.6.2. Application Security & Virtual Smart Cards 46

6.6.3. DRM Solutions 46

# Introduction

# LMS

## Presentations of the main existing LMS on the market

### Open EdX

#### History

EdX is a nonprofit offering the highest quality education, both online and in the classroom. Founded by the Massachusetts Institute of Technology (MIT) and Harvard University, edX offers online learning to on-campus students and people around the world. EdX is building an open-source online learning platform and hosts a web portal for online education.

EdX was founded in May 2012 after OpenCourseWare, its ancestor created in 2001 by the MIT alone. This first attempt was described by then president, Charles Vest in the words:

*“It expresses our belief in the way that education can be advanced by constantly widening access to knowledge and information, and by inspiring others to participate. Simply put, OpenCourseWare is a natural marriage of American higher education and the capabilities of the World Wide Web.”*

Tis definition of OpenCourseWare could have been applied to EdX directly. But EdX presents an enhanced experience with more interactions, discussions forums, grades and a university-sanctioned certificate upon completion. OpenCourseWare was more a platform with contents (that were used by students to revise and improve what they learn during classroom time. At this time OpenCourseWare counted over 2,000 published courses. Over time, however, more and more independent learners emerged, becoming the primary users of MIT’s OCW. To date, there have been 122 million views by 87 million visitors from nearly every country across the globe. The program has reached students from Nigeria, Mexico, Ghana and Zambia, in places where higher education isn’t readily available nor necessarily emphasized.

EdX could be more presented as the next step for online education at the MIT.

EdX serves three main missions:

* Expand access to education for everyone
* Enhance teaching and learning on campus and online
* Advance teaching and learning through research

Practically EdX delivers courses from universities worldwide. They also present their goals, however, as going beyond with a goal of research that will allow the platform to understand how students learn, how technology can transform learning, and the ways teachers teach on campus and outside.

#### Business Model

More than 60 schools, nonprofits, corporations, and international organizations offer or plan to offer courses on the edX website[[1]](#footnote-1). As of 22 October 2014[[2]](#footnote-2), edX has more than 3 million users taking over 300 courses online.

If the access to the contents remains free, it costs for colleges and universities to host their courses on edX. And it’s not very affordable… A simple hosting of the courses would cost $50,000, and $10,000 the second year, plus 50% of the revenues of the courses over these amounts. If EdX participates in the creation of the course, it would costs $250,000 the first year and $50,000 the year after, plus 50% of the revenues over these amounts.

Although edX has substantial resources, questions arise about its business model. For three years, Harvard and MIT have put on the table $60 million to launch the platform, which currently employs 140 people. The start-up has also raised over $ 30 million from the various institutions with which it works. At the time of its accession, each university negotiates its financial contribution or not. Access to the course is free for students, but for the institutions, the entry ticket to edX consortium remains very high as we see above.

To continue its growth, edX is now focusing on continuing education. Several members of edX (University of British Columbia, Rice, Google, etc.) offer paid since October 2014 online courses towards professionals from several days to several weeks. "*We conducted some experiments at MIT. Our first Mooc on big data ($ 500) was a success and attracted 3,000 students. It is also a very promising market for most of our partners*," said Johannes Heinlein, Vice President Strategic Partnerships of edX.

The other major project is that of certification. Students who have access to free courses can now punish their success by an authenticated certificate issued by the home institution. It takes between 25 and $ 100 depending on the institution. At least half of that amount back to the university, the other goes into the pocket of edX, which could be a promising niche : "Between 1 and 5% of learners are willing to pay for a certificate," as said by Johannes Heinlein.

The platform can also rely on the income from the sale of content licenses to other institutions (eg Crown sites in Saudi Arabia, etc.) or services to users of the platform.

At the opposite the code of edX platform is available as open source. It empowers an important number of players to build their own platforms. EdX was used in France ofr example to build FUN (France Université Numérique), the national platform for MOOCs.

### Canvas

#### History

Canvas is learning management system, which is a comprehensive cloud-native software package developed by Instructure an educational technology company based in Salt Lake City, Utah. Instructure also developed Canvas Network, a massive open online course platform.

The Utah-based company tested the LMS at several local schools including Utah State University and Brigham Young University before officially launching Canvas.

Instructure also owned an LMS platform designed for the specific needs of elementary and secondary schools: Canvas K-12. The LMS also enrolls parents to provide greater visibility into their children's learning experience and provides actionable analytics to teachers and administrators.

The company also owned a corporate LMS with Bridge launched in 2015.

#### Business Model

Canvas is an open-source LMS that Instructure for itself in various institutions and companies (higher education, K-12 and corporate). Since its launch, Instructure has attracted more than 6 million teachers and students from 425 institutions and booked more than $90 million in contracts.

Instructure Canvas Network, the company’s answer to MOOC platforms like Coursera, Udacity or edX, has delivered more than 40 online courses by partner universities since its launch in November 2012. Other than MOOC platforms like Udacity or Coursera, Canvas Network allows institutions to define the structure of their courses and how to teach these themselves which has resulted in various different formats ranging from a smaller online course format with more interaction to really massive video lecture based courses.

### Moodle

#### History

Moodle is software learning management system. Developed on pedagogical principles, Moodle is used for blended learning, distance education, flipped classroom and other e-learning projects in schools, universities, workplaces and other sectors.

At the beginning, Moodle was developed by Martin Dougiamas to help educators to create online courses with a focus on interaction and collaborative construction of content, and it is in continual evolution. The first version of Moodle was released on 20 August 2002.

In the higher education market as of fall 2013, Moodle is the second largest provider with 23% market share, following Blackboard (41%) and Desire2Learn (11%) and Instructure as number three and four providers[[3]](#footnote-3).

#### Business Model

Moodle is a free and open-source software distributed under the GNU General Public License.

Nowadays the Moodle Project is led and coordinated by Moodle HQ, an Australian company of 30 developers which is financially supported by a network of sixty Moodle Partner service companies worldwide. Moodle's development has also been assisted by the work of open-source programmers.

### Blackboard

#### History

The Blackboard Learning Management System, or Blackboard Learn, is a virtual learning environment and course management system developed by Blackboard Inc. It is Web-based server software which features course management, customizable open architecture, and scalable design that allows integration with student information systems and authentication protocols.

In 1997, Stephen Gilfus and Dan Cane started a company called CourseInfo and were developing a software product that would power online education and be scalable for wider institutional application. At the same time, Matthew Pittinsky and Michael Chasen formed Blackboard LLC and were contracted to help lead the formation of the Educause IMS standards group for online education technology. The two groups merged to form Blackboard Inc., which then developed the Blackboard Learning System.

Blackboard is particularly implicated in the development and the implantation of IMS standards such as Caliper for the analysis of the uses of students.

#### Business model

Blackboard is a for-profit company that sells its LMS to K-12, Higher Education, Government and Corporate.

### Desire2Learn

#### History

D2L Corporation (previously known as Desire2Learn) and commonly referred to as “D2L”, is a provider of eLearning solutions. It is the developer of the Brightspace integrated learning platform which is used by higher education institutions, K-12 school districts and corporate and government customers.

D2L Corporation was founded in 1999.

Brightspace is the brand used to describe D2L’s integrated learning platform. The Brightspace platform’s core learning products include D2L Learning Environment, D2L ePortfolio and D2L Learning Repository. The platform also offers analytics products such as D2L Insights, D2L Degree Compass and D2L LeaP.

D2L offers Brightspace solutions for the higher education and K-12 education markets. These solutions include online and blended learning, curriculum management, content management and analytics. Brightspace is also offered to corporate and government customers, with field and channel enablement and employee learning and development solutions.

The D2L Partner Network includes organizations with a focus on education markets, including content publishers, independent software vendors and service providers. D2L has partnerships with Ceridian, IBM, McGraw Hill Education, and SoftChalk.

#### Business Model

D2L is a for-profit company. It sells its LMS.

## Technical description and comparison

|  |  |  |  |
| --- | --- | --- | --- |
|  | Blackboard | Moodle | D2L |
| ****Administration**** | Administrative Reporting  Course Catalog  Custom Reporting  Data Import/Export  Grading  Individual Plans  Legacy System  Resource Management  Student Portal | Administrative Reporting  Course Catalog  Custom Reporting  Data Import/Export  Email Integration  Grading  Individual Plans  Mobile Access  Training Workflow |  |
| ****Tracking and Reporting**** | Skills Tracking | Skills Tracking |  |
| ****Assessment & Testing Tools**** | Goal Setting  Testing  Training Metrics | Quiz or Survey  Custom Templates  Custom question and answer library  Can accept some test banks  Multiple feedback options  Multiple feedback options  Publication options include time limits, multiple takes, delays between takes, and custom audiences |  |
| ****Compatibility and Supported Devices**** | browser | browser | browser |
| ****Customization and Branding**** | Custom Branding  Custom Fields  Custom Functionality  Custom User Interface Exam Engine  Multiple Delivery Formats | Course Authoring  Custom Branding  Custom Fields  Custom Functionality  Custom User Interface  Exam Engine |  |
| ****Course Interactivity**** | AICC, SCORM | Blogs  Collaboration Management  Discussion Forum  File Exchange  Internal Messaging  Live Chat  Wikis  AICC, IMS, SCORM |  |
| ****User Registration**** | Registration Management  User Access Controls | Defined User Roles  Registration Management |  |
| ****Technologies**** |  | PHP |  |

|  |  |  |
| --- | --- | --- |
|  | Edx | Canvas (Instructure) |
| **Administration** |  | Administrative Reporting  Course Catalog  Data Import/Export  Grading  Mobile Access  Roster Processing  Unlimited Users |
| **Tracking and Reporting** |  | Skills Tracking |
| **Assessment & Testing Tools** |  | Quiz (graded or ungraded)  Custom Templates  Custom question and answer library  Can accept some test banks  Multiple feedback options  Multiple feedback options  Publication options include time limits, multiple takes, and custom audiences |
| **Compatibility and Supported Devices** | Browser |  |
| **Customization and Branding** | Course Authoring  Custom Branding | Course Authoring  Custom Branding  Custom Fields  Exam Engine |
| **Course Interactivity** | Discussion Forum  Internal Messaging  Live Chat  AICC, SCORM | Discussion Forum  Internal Messaging  Live Chat  AICC, SCORM |
| **User Registration** | User Access Controls | Defined User Roles  User Access Controls |
| **Technologies** | Written almost entirely in Python for the server and Javascript for the browser | Canvas was built using Ruby on Rails as the web application framework backed by a PostgreSQL database. It incorporates JQuery, HTML5, and CSS3 to provide a modern user interface. OAuth is used to provide limited access to a user's information on certain social media sites like Facebook and Twitter to allow for collaboration between sites. Canvas operates as a software as a service using Amazon Web Services in the "Cloud". |
|  |  |  |
|  |  |  |

1. **Administration –** This includes the number of course administrators and all of the tools and features available to you – including tracking and reporting, content management, notifications, single sign-on, API, and more.
2. **Tracking and Reporting –**There are a number of different ways to track your LMS data within an LMS. With these tools, guide student progress via prerequisites and learning paths, export user data and create real-time reports, and deliver timed courses and inactivity timeouts.
3. **Assessment & Testing Tools** – Most learning management systems have some sort of online exam system with various testing tools. A few features that may be a bonus are question pooling, question randomization, required responses, and automated self-grading.
4. **Compatibility and Supported Devices** – Many LMSs have an HTML 5-based user interface that adapts to different hardware devices, including desktops, laptops, and tablets. Specific platforms that may be supported are PC, Mac, Linux, iOS (iPads/iPhones), Andriod, Blackberry, and more.
5. **Customization and Branding** – It is important that your online courses can be identified as your own. Be sure you have the abilities to brand courses with your logo and colors, customize groups and terms of use, create custom certifications of completion, and create custom email notifications.
6. **Integration** – Does your learning management system have any integration tools such as API? With this, you can integrate with talent management systems, CRMs, back-office systems, and more.
7. **eCommerce** – If you plan on selling your courses online, these are the must-have features for you: integrated shopping cart, emailed receipts/notifications, and various payment gateways including Authorize.NET and PayPal.
8. **Course Interactivity** – Levels of interactivity can vary among LMSs. Interactive features that may be important are: HD streaming video, audio, images, SCORM presentations, assignments, and tests.
9. **User Registration** – How easy can you register your students? Be sure you can import students via mass uploads, automate uploads, and/or enable students to self-register quickly.

# Authoring tools

## What does an authoring tool permit to create?

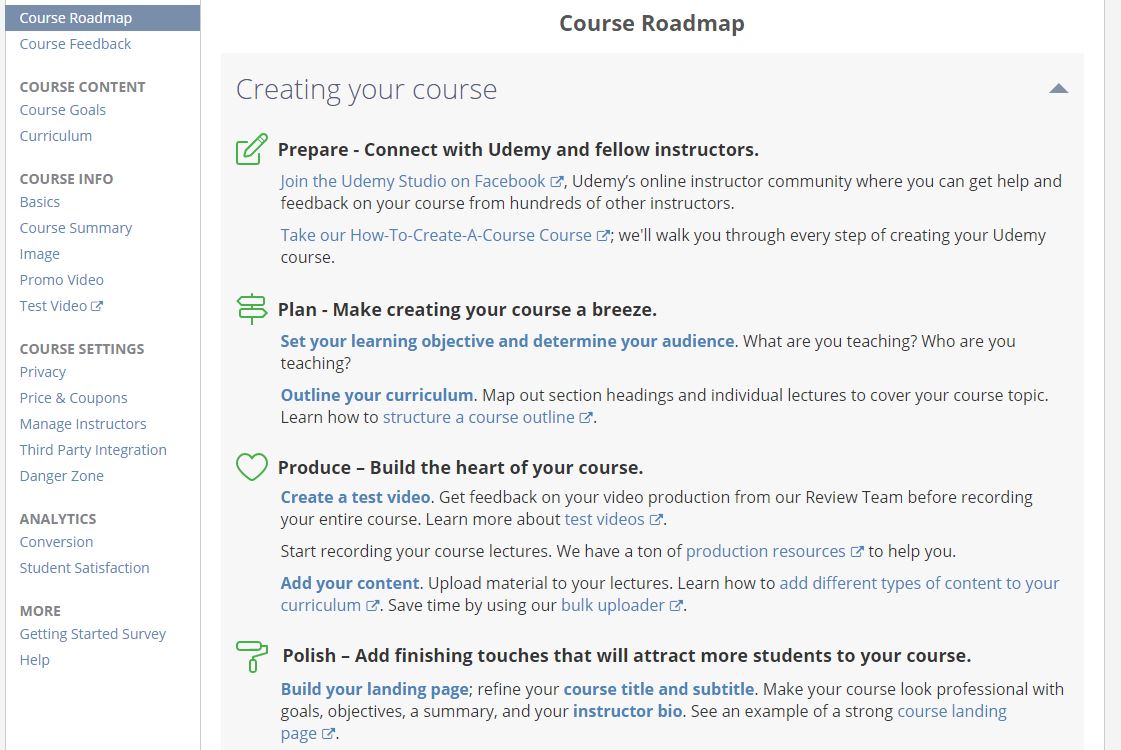
Depending of the platform you’re targeting, you could build course with various authoring tools. Either you’re creating a MOOC for some of the main platform such as EdX, Coursera, Udemy… and you will use a basic tool for the construction of your course or you want it on Moodle or Blackboard of example and you will use more complex authoring tool compliant with international standards (SCORM, IMS-QTI…).

### Your MOOC with EdX, Coursera or Udemy…

Still here you’ve got two options, either you make the videos and the content yourself or you ask the EdX support – but this assistance has an expensive price – several thousand dollars will be needed.

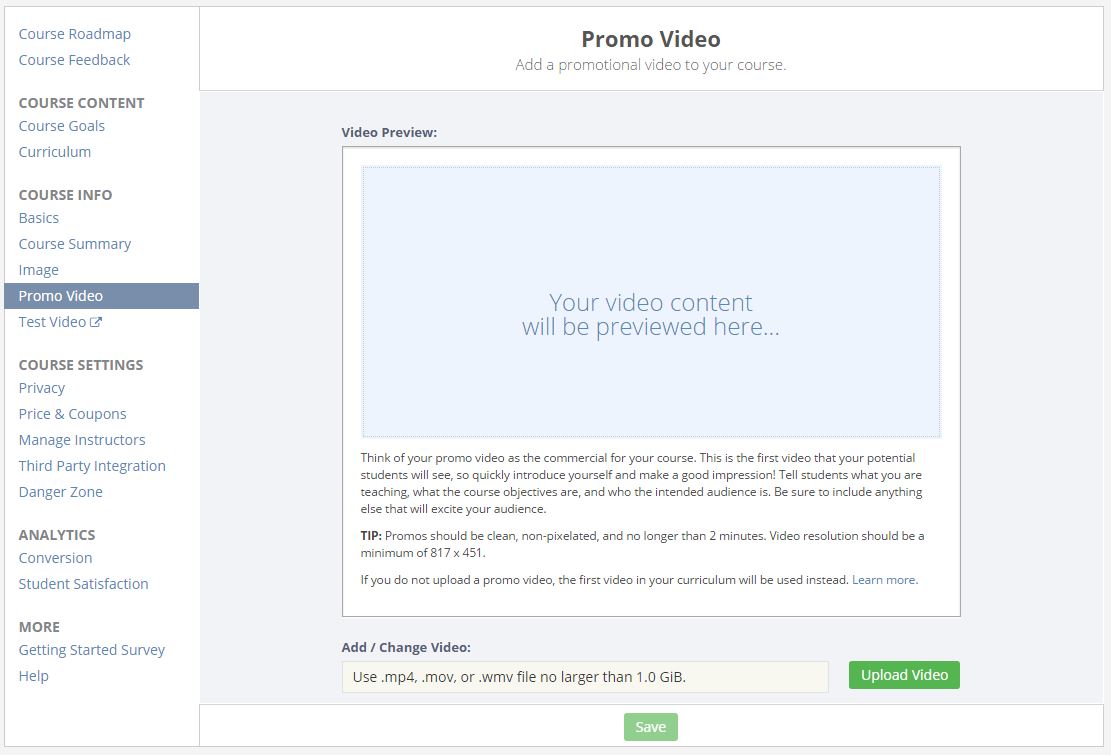
#### With your own content

Take an example with Udemy. After subscribing, you’ll see this kind of interface:



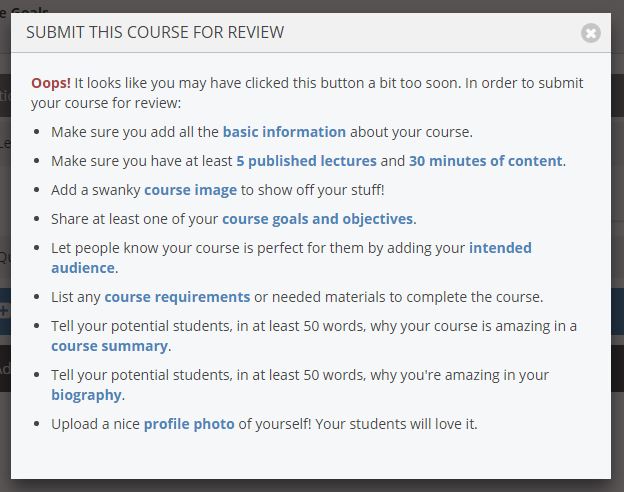
*Preparing the course with Udemy platform*

On the right, you’ll find all the instructions to build the course from the Promo video to the Privacy settings.



*Uploading a promo video – Udemy platform*

With your own content - your videos filmed on your own – you will just have to upload it where it is necessary. As soon as your content is ready and every section of this curriculum filled, your course could be launched. But it has to be reviewed before. The platform checks that the course has the necessary components before the publication.



*Submitting a course - Udemy platform*

Once accepted, the course could start – for free or payable depending on the platform and the business model you chose for your course.

#### With the platform assistance

As we saw above, platforms like EdX or Coursera can help to build courses. These are payable services – sometimes very expensive.

EDX offers two types of partnership to suppliers of MOOCs:

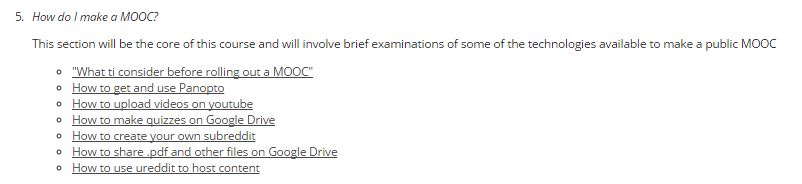
- A "self-service" system, in which the supplier arrives with his own contents. When the course will generate revenue, EDX take 50,000 dollars the first year, $ 10 000 the following years, plus 50% of revenues in excess of these thresholds.

- An "accompanied" service, the teaching staff and technical EDX helping the provider to create its course. In this case, EDX takes $ 250 000 the first year, $ 50 000 the following years, and still 50% of revenues in excess of these thresholds.

Coursera offers a simpler device:

Coursera returns between 6 and 15% of revenues generated by each MOOC, plus 20% on the "licenses" being sold. We can assume that the revenue generated by the courses translated at the initiative of Coursera (who complete authority over the decision) will be distributed in the same way. The provider thus affects earnings from the first penny of revenue generated, but in small quantities.

#### Bootstrapping your MOOC

Several tutorials on the web offer help to build a MOOC without any assistance of the main platforms but instead with a panel of free tools available on the Web such as YouTube, Google Drive or Reddit.

*Bootstrapping method for MOOCs*

It doesn’t offer any assistance for the most problematic point in a MOOC yet: filming your videos.

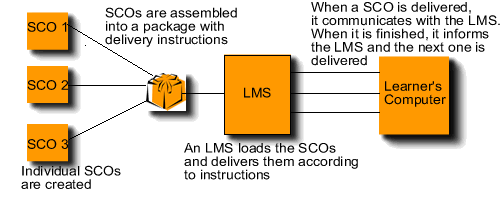
## Operation of the tool

Several authoring tools on the market offer to create contents that can be used directly in LMS. In these cases they are respecting international standards and especially SCORM (Sharable Content Object Reference Model) that defines how content may be packaged into a transferable ZIP file called "Package Interchange Format”. Before seeing the operation of an authoring tool, we will focus on the SCORM standard.

### Description of SCORM

#### The main features

So what are the features of the standard defined by the SCORM LMS platform material and e-learning design?

* The use of XML;
* Training courses are formed of several autonomous educational grains called "SCO" (Sharable Content Object). These learning units are autonomous and can be composed of various resources: texts, videos, sounds, animations, HTML pages etc.);
* Informative metadata describes the e-learning content (general, technical, educational, etc.) and allow classifying to find them more easily later.

*How SCO are delivered to learners*

#### SCORM, what benefits?

The size argument SCORM is the guarantee of interoperability between e-learning content and learning management platforms. LMS platforms that meet the SCORM model can incorporate any e-learning content and conversely, badged SCORM modules are usable on all platforms LMS market. This ensures the sustainability of e-learning SCORM content, since they will be used with all existing development tools and does not suffer from any technological developments on the platform or LMS LMS platform change for dissemination.

SCORM guarantees a good communication between e-learning content and LMS platforms that use the standard. Most distance learning market players are now following this model. It almost became difficult to do without it and take the risk of being marginalized or losing potential market share.

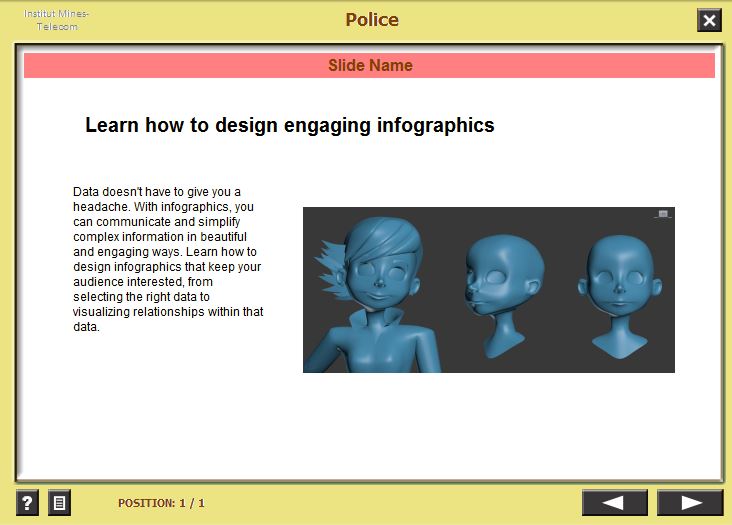
#### SCORM, what control?

The ADL (Advanced Distributed Learning), in collaboration with other organizations specialized in the technologies of distance training, determines the specifications of SCORM model. Created in 1997 by the Department of Defense, the association's mission is to identify and classify learning objects that will then be used by the masses. These must be available and shareable on the web. The essential concept is to make the SCORM learning objects produced on different tools, usable and editable by all other applications.

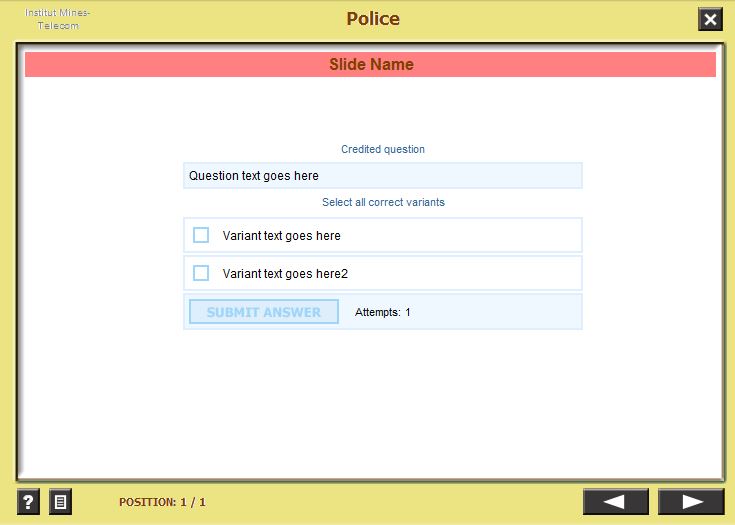
### Operation of an integrated authoring tool

We choose to present a tool that could be used for Moodle called CourseLab. It allows to build a course with various media and quizzes.

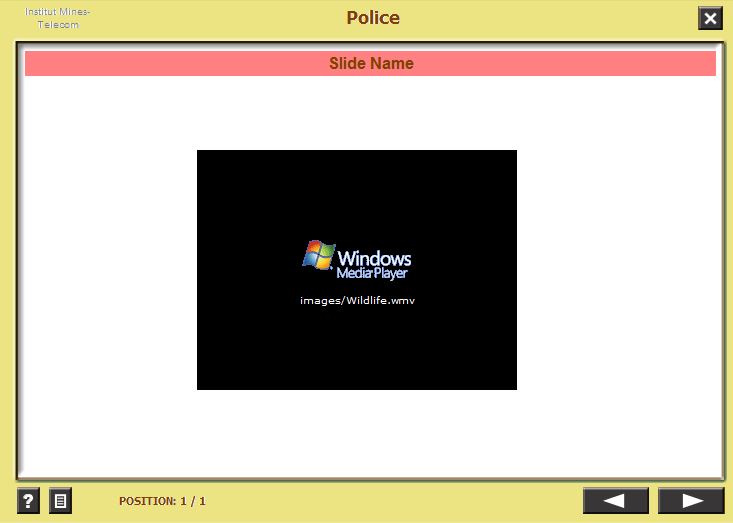
As it is presented below, you could add various media to your production.



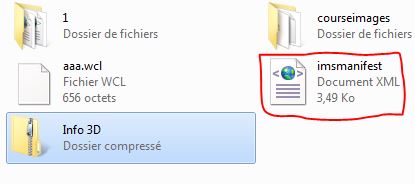
*Texts and images*

**

*Quizz*

**

*Video*

Once your course is ready you can publish it and choose the SCORM compliance.

## Comparisons of the main integrated solutions

Several hundreds of authoring tools can be counted on the market more or less focused on some aspects of the content creation (video, features, metadata, standard compliance…). The license could be different as well (free, free trial, open source or paid) and the installation can vary from hosted or local.

# Contents

## Description of the various contents in a MOOC

A MOOC could include a great diversity of contents (video, image, text, 3D, AR, interactive quiz…). We will try to describe them so as to have a global overview of the composition of a MOOC.

### A massive use of videos

#### Video as forms of knowledge transmission

In the context of digital infrastructure open to innovation, the Internet is full of innovative experiments and teaching formats. All the potential of the Internet is used, such as hypertext resources and multimedia files: tutorials that are a hybrid of texts and commentary video screens and infographics; conferences in short format and recorded lectures widely disseminated. Ted Talks, developed by Chris Anderson, are free diffusions of the best conferences on “Ideas worth spreading”, which are new forms of knowledge dissemination. These are “performances” made by experts in short and lively formats. The use of video as a means of transmission of knowledge has exploded in recent years –expertise, lectures hybridizing speech, text, graphics and animated media become the norm for educational transmission. And finally, what Khan Academy has done is to acknowledge these changes by offering digital spaces of learning through play and video.

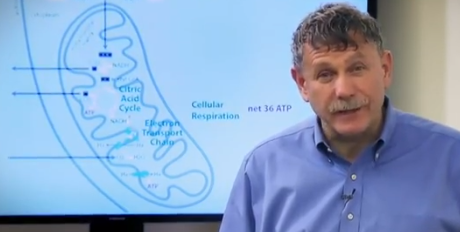
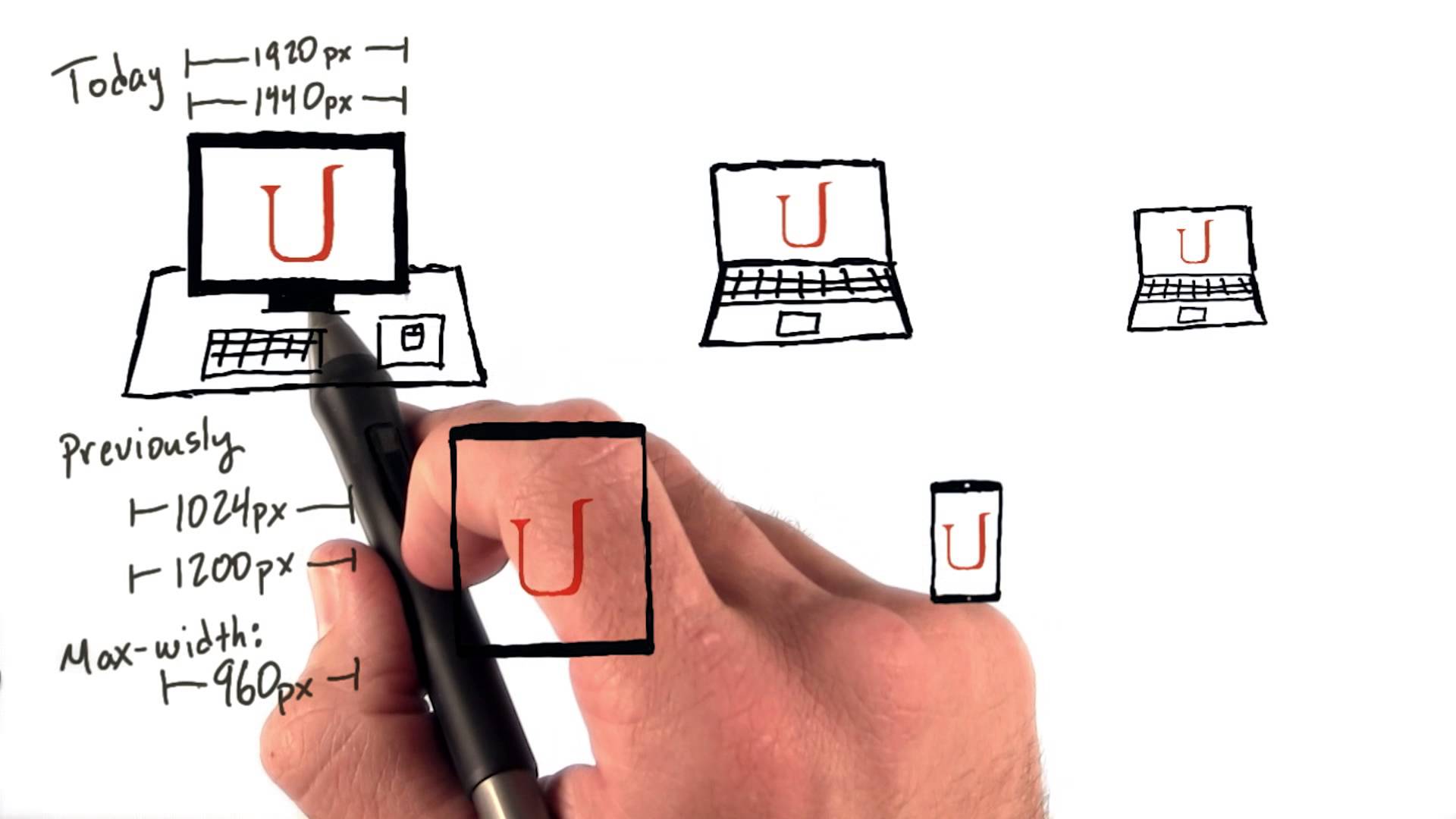
Video formats, too, are changing. It is now typical for videos proposed within MOOCs to be interrupted by in-video quizzes, or are synchronized with html content, maps or other components in the web page.

#### The good video: short and straight

An important report released by edX in April 2014 gave design teams some concrete data to examine. You’ll find below the recommendations and practical application points from the paper.

##### Videos Types for MOOCs

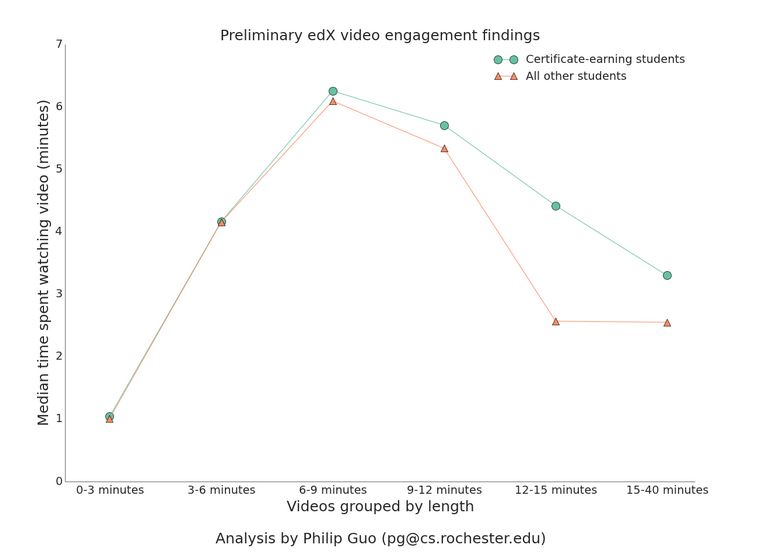
Lectures are divided into two primary types for the study, [which mirrors most MOOCs]: 1) lecture videos for content delivery—presented via an instructor/professor (‘talking head’ is the term used in the paper), and 2) a tutorial/demonstration, a step-by-step problem solving walk-through, common in computer science courses, courses featuring mathematical concepts or science courses featuring lab demonstrations.

*Type 1: lecture video*

*Type 2: Tutorial video*

##### Key Findings of Study

* Shorter videos are more engaging. Student engagement levels drop sharply after 6 minutes



*Video engagement on EdX platform*

* Engagement patterns differ between the two video formats; engagement higher with the lecture style videos (‘talking head’) which researchers suggest is due to more “intimate and personal feel”
* Several MOOC instructors interviewed for study felt more comfortable with the classroom lecture format, however this format did not translate well online, even with much editing in production studio
* For tutorial videos, the Khan-style format where teacher draws on tablet and talks, was found to engage students more effectively than screen casts. A contributing factor—instructors ability to situate themselves “on the same level” as student
* Video producers determined that pre-production planning had the largest impact on the engagement effect of the videos. Researchers used a data set within the study to test this idea

### Images and text

Images and texts are largely used in MOOCS especially to bring additional materials with the video (exercise, tutorial…). Pdf format is the most used; sometimes documents can be opened directly in the browser and written in HTML5.

### 3D, AR

#### Is learning a pleasure or an effort?

The culture of the screen allowing access to content generates immediate pleasure and it leads to reinvent new ways to motivate and create the desire to learn, and practice critical thinking. It was pointed out that tension can arise between the *exopedia* (education outside the school via the screens) and the *endopedia* (education at school) based on thinking and aptitudes of critical distance[[4]](#footnote-4). How to recreate the *libido sciendi*? Are serious games the way to learn? These debates merely reproduce the tension between an immediate and misleading, substantial world and the world of knowledge and ideas that forces to make an effort…

Thus, long before MOOCs were serious games (1970). At present, health education is one of the teaching areas were there exists numerous simulation games. It is, for instance, possible to train medical students in surgery without hurting patients, to teach them emergency gestures in stressful situations that cannot be replicated every day, or to train medical assistants to detect hazards in apartments for the elderly.

#### When the lab became a game

Gamification is also used as another way to retain students within online course. Studies show that persistence is encouraged by introducing elements of game mechanics into the course. For example, interactive challenges ( such as 3D lab reproducing experiments) introduced intermittently during the course will unlock the next step. This can be closely associated with badging as it is now prevalent for people to have a profile or an avatar.

Mobile devices also help to develop gamification and professional mobile video games are already successful in the educational world. Users can unlock additional content pays offs – the model of the in-app purchase – which is a well-known and remunerative model in the mobile and Facebook worlds.

gMOOC (game-based MOOC) are one of the numerous variations of MOOCs. The course is done in a virtual world where it is possible to interact with other avatars and acquire social skills. This is also a unique opportunity to meet people not involved in the course.

Serious games and game-based online courses allow teaching disciplines where it is mandatory to manipulate costly objects or meet external people. This allows MOOCs in the physics, chemistry or biology disciplines. The virtual laboratory below is such an interactive environment developed for creating and conducting simulated experiments.

*Reducing the cost of manipulation with a virtual laboratory*

## Standards for contents

### Online standards

#### SCORM

SCORM ("Sharable Content Object Reference Model") enables dynamic sharing of educational content by defining a model for structuring such content and an API model: compatible Learning Management Systems can thus recover on the fly from bases learning objects data sources. The structuring of the contents is a tree, with high-level aggregates (courses) composed of smaller reusable blocks, Sharable Content Objects (SCO), which are themselves composed of basic resources (text, images).

#### Tin Can CAP

The Experience API (Tin Can API) is commonly considered the successor to SCORM. The Experience API allows for several new capabilities that SCORM didn't, such as:

* Taking e-learning outside of the web browser
* E-learning in native mobile applications
* More control over learning content
* Solid security using Oauth
* Platform transition; e.g. start e-learning on a mobile device, finish it on a computer
* The ability to track games and simulations
* The ability to track real-world performance
* Team-based e-learning
* Tracking learning plans and goals

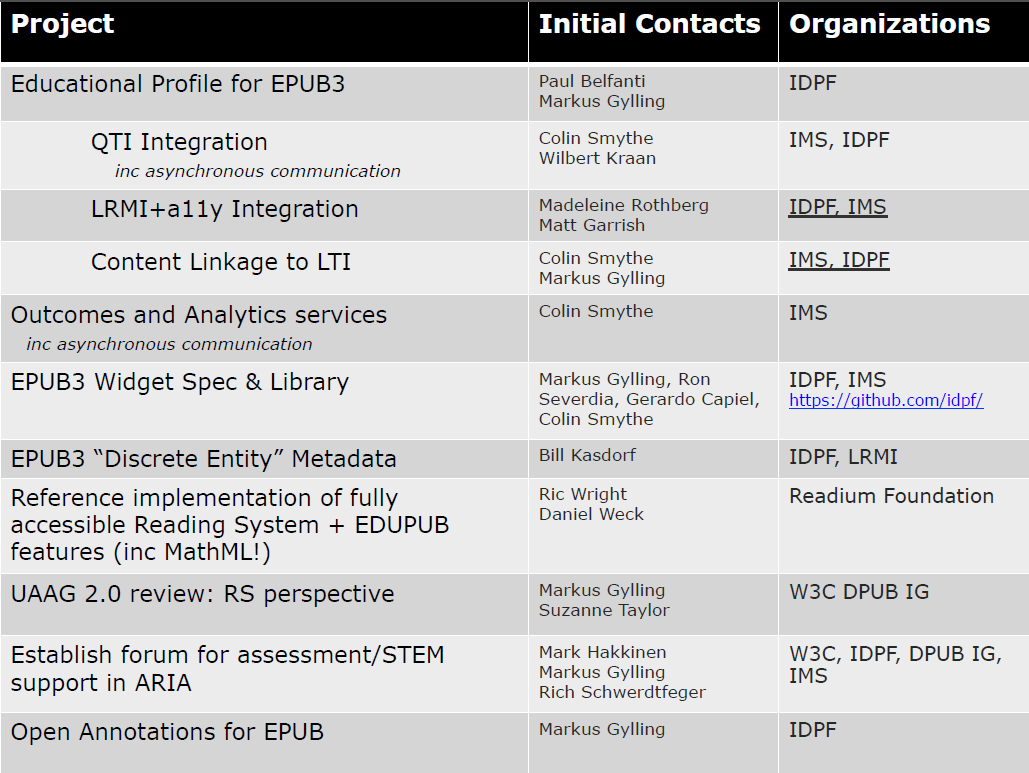
#### LOM

Learning Object Metadata is a data model, usually encoded in XML, used to describe a learning object and similar digital resources used to support learning. The purpose of learning object metadata is to support the reusability of learning objects, to aid discoverability, and to facilitate their interoperability, usually in the context of online learning management systems (LMS).

This model has been adopted by countries and adapted, like in France with SCOLOM for K-12 and SUPLOM for Higher Education.

### Coming offline standard: edupub

A standard of education is under development within the IDPF. Its aim is to make online resources available offline. Several tasks are under paralleled developments.



*IDPF working groups for EDUPUB standard*

As the forseen tasks showed it

# Learning Analytics

## Presentations of the subject

### Definition

Learning analytics is the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimising learning and the environments in which it occurs (LMS, MOOC platforms…).

### Data retrieved

The type of data gathered varies by institution and by application, but in general it includes information about the frequency with which students access online materials or the results of assessments from student exercises and activities conducted online. Usual types of data are :

* log-in information
* rates of participation in specific activities
* time students spend interacting with online resources or others in the class
* grades

### Aim of LA

Learning analytics tools can track far more data than an instructor can alone, and at their best, LA applications can identify factors that are unexpectedly associated with student learning and course completion.

Analytics programs evaluate large data sets to provide decision makers with information that can help determine the best course of action for an organization. Learning analytics (LA) takes this same approach but with the specific goal of improving learning outcomes, which could be measured by grades, retention, or completion.

### Use case

With more than 100 students in his intro to psychology course, Dr. Delgado is unable to provide the level of individual attention for each student that he would prefer. Inevitably, some highly capable students drop out or do poorly, in part, he believes, because they simply need extra guidance. The course progresses, and the amount of data collected balloons. The LA system runs weekly analyses, looking for associations between the variables and outcomes. When it spots students whose activity suggests a low likelihood of success, it automatically notifies them and suggests steps they could take to increase their odds of success in the course. Delgado also receives notifications, and he personally contacts several students identified as at-risk. These students appreciate the extra attention and make changes to their level of participation and activity in the course.

### Utilizations

The most common use of learning analytics

• for individual learners to reflect on their achievements and patterns of behaviour in relation to other

• identify students who appear less likely to succeed academically and to enable—or even initiate—targeted interventions to help them achieve better outcomes.

• some faculty employ LA tools to identify specific units of study or assignments in a course that cause students difficulty generally

• Instructors can then make curricular changes or modify learning activities to improve learning on the part of all students.

• for institutional administrators taking decisions on matters such as marketing and recruitment

### Materialization

• Reports can take various forms

• most feature data visualizations designed to facilitate quick understanding of which students are likely to succeed

### First users

First implementations were made by for-profit institutions (University of Phoenix, Capella University, and the American Public University System (APUS).

Traditional higher education institutions like Rio Salado College in Arizona have also begun to implement LA and predictive modeling. Because the college found that early grades in coursework were not a reliable factor in predicting student success, its LA software focuses on information such as log-in frequency, the pace of a student’s work in the first eight days of class, and student involvement in discussion forums. In other LA systems, grades are part of the analysis:

At Louisiana State University, LA tools factor in grade data; where grades are high but a student’s participation is low, the software ignores the concern, sending out a caution only when both are low.

### LA Methods

Methods for learning analytics include:

• Content analysis - particularly of resources which students create (such as essays)

• Discourse Analytics Discourse analytics aims to capture meaningful data on student interactions which (unlike 'social network analytics') aims to explore the properties of the language used, as opposed to just the network of interactions, or forum-post counts, etc.

• Social Learning Analytics [18] which is aimed at exploring the role of social interaction in learning, the importance of learning networks, discourse used to sensemake, etc.

• Disposition Analytics which seeks to capture data regarding student's dispositions to their own learning, and the relationship of these to their learning. For example, "curious" learners may be more inclined to ask questions - and this data can be captured and analysed for learning analytics.ontext (what?), stakeholders (who?), objectives (why?), and methods (how?).

## Presentations of the different standards

### edX Insights

#### An ongoing construction

edX Insights was launched in oct 2014. Prior to this development several companies developed tools to offer this feature in edX (e.g. Extension Engine). edX Insights is the tool for data & analytics of edX. It will address course teams, instructors, and researchers. Currently it tracks basics indicators for them such as the number of students enrolled, their age, gender of geographical distribution

*Geographical distribution for given MOOC*

These first features were released back in 2014. In 2015, edX development team added more details data. It introduced some tools to interpret the graded submissions and the description between assignment type and students answers.

The graded submissions analysis enable to;

• assess how difficult the problem is for students to answer correctly;

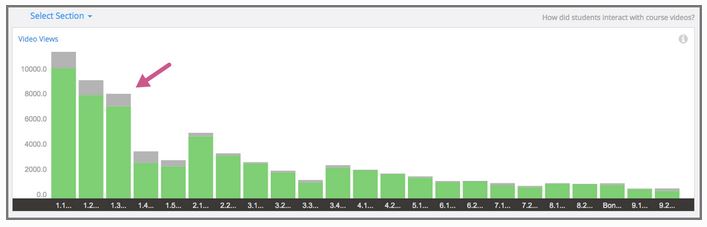
• detect common mistakes;

• understand student misconceptions;

• find errors in problem components.

edX Insights also offers to investigate your assignment choices and review the student answers tye by type. It could hep instructors to improve their grading policy.

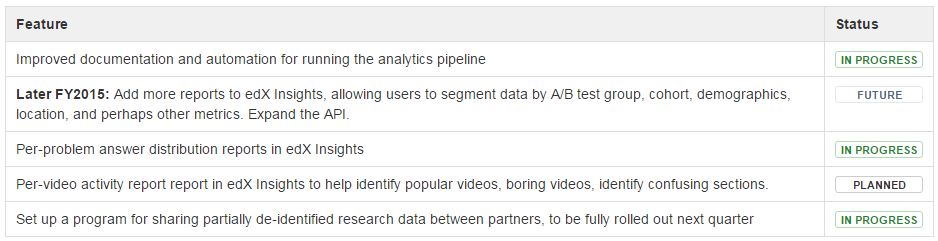
edX Insights also helps to analyze the video engagement that can give information to gain perspective on learners’ viewing patterns.

*Number of views of videos by sub-section *

It’s also possible to search for replayed segments in each video underlying or not a difficult that met students.

#### Roadmap

It will enhance data visibility and analysis capability for course teams, instructors, and researchers. For course teams and instructors, a specific focus will be given to student demographics, behavior, and performance. For researchers, the tool will retrieve a trackable and queryable data.



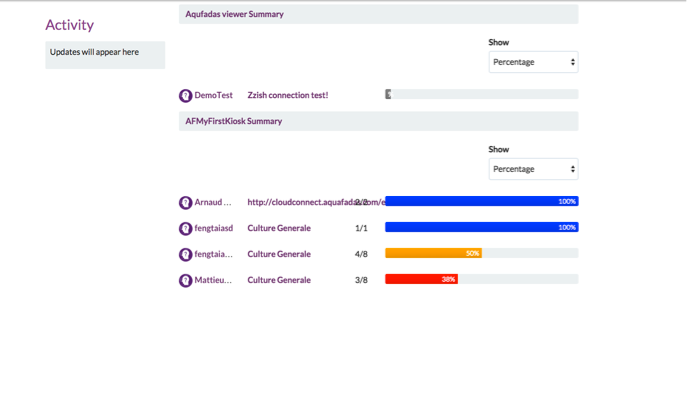
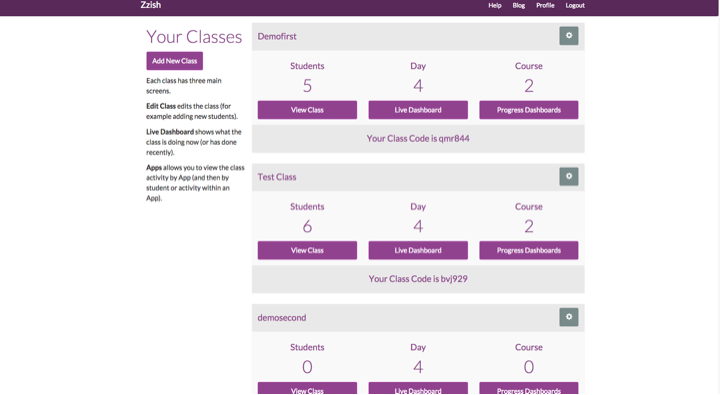
*edX roadmap for Data & Analytics*

### xAPI

The Experience API (xAPI), also known as the Tin Can API, is an e-learning software specification that allows learning content and learning systems to speak to each other in a manner that records and tracks all types of learning experiences. Learning experiences are recorded in a Learning Record Store (LRS). LRSs can exist within traditional Learning Management Systems (LMSs) or on their own.

It’s also known as the successor of SCORM, an e-learning standard for packaging e-learning content to be delivered to LMSs.

XAPI is particularly focused on data tracking (games and simulations, real-world performance, learning plans and goals).

A Learning Record Store (LRS) is a data store system that serves as a repository for learning records necessary for using the xAPI that can be retrieved in bar charts of various diagrams developed by companies.

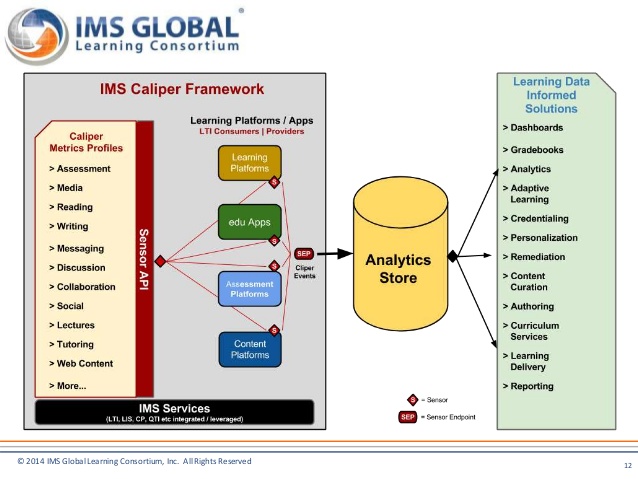
*Data & analysis tool using xAPI by Aquafadas*

xAPI-enabled learning activities generate statements, or records of e-learning in the form of "I did this" or "Actor verb object." These statements are transmitted over HTTP or HTTPS to an LRS. The main function of an LRS is to store and retrieve the data that's generated from Experience API statements.

### Caliper Analytics

IMS will include a standard that:

* creates IMS Learning Metric Profiles to establish a basic, and extensible, common format for presenting learning activity data gathered from learner activity across multiple learning environments. Metric Profiles provide a common language for describing student activity. By establishing a set of common labels for learning activity data, the metric profiles greatly simplify exchange of this data across multiple platforms. While Metric Profiles provide a standard, they do not in and of themselves provide a product or specify how to provide a product. Many different products can be created using the same labels established by the standard.
* creates the IMS Learning Sensor API to define basic learning events and to standardize and simplify the gathering of learning metrics across learning environments.
* leverages and extends the IMS LTI/ QTI standards thus enhancing and integrating granular, standardized learning measurement with tools interoperability and the underlying learning information models, inclusive of course, learner, outcomes and other critical associated context.



*Caliper: retrieving data in an analytics store through various tools*

The Caliper Sensor API and Metric Profiles have been tested across a wide range of products over the past 18 months, and they are now operational in several well-known educational products. The Caliper workgroup is led by D2L, Elsevier, Intellify Learning, Learning Objects, McGraw-Hill Education, Penn State University and the University of Michigan. The specification has achieved a “candidate final release” status[[5]](#footnote-5). First implementations have been seen recently by Brightspace.



Sakai, another LMS we examine earlier plan in its roadmap support for IMS Caliper.

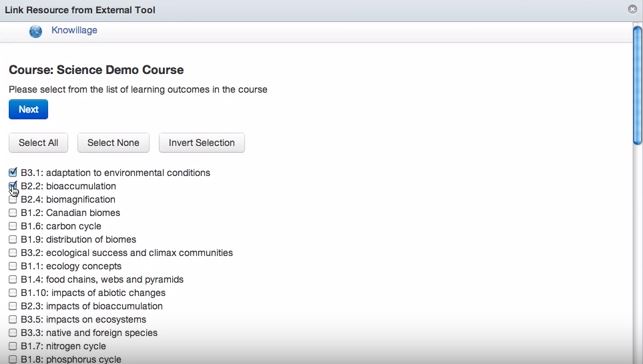
## Presentations of different software

Much of the software that is currently used for learning analytics duplicates functionality of web analytics software, but applies it to learner interactions with content. Social network analysis tools are commonly used to map social connections and discussions. LA software are more a combination of various tools used to track and analyze students work.

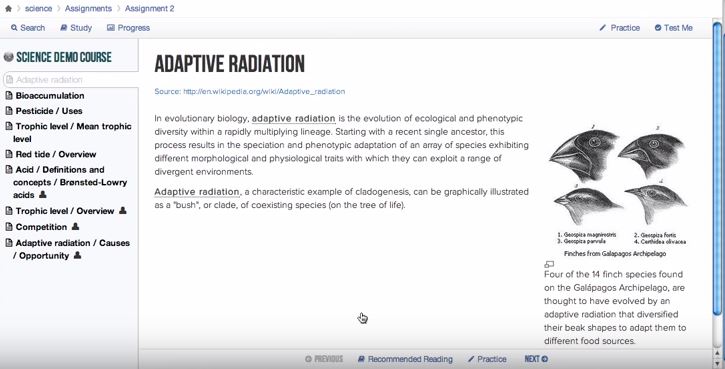
### Brightspace : LeaP

Brightspace (D2L) develops specific tools of learning analytics. After acquiring Knowillage and its LeaP product in 2012, they integrate the technology of the startup directly in their LMS. Leap enables to create personal paths for students. The LA module aims at measuring, optimizing, and demonstrating, progress and achievement for each student. It also gives teachers the robust analytics tools and actionable insights they need to track student engagement, offer support, personalize and improve instruction.

But they don’t really offer any kind of knowledge map. They offer adaptive paths for students built by instructors. From a semi-automatic built pre-show test, LeaP assesses the level of each student et proposes pieces of knowledge to improve.



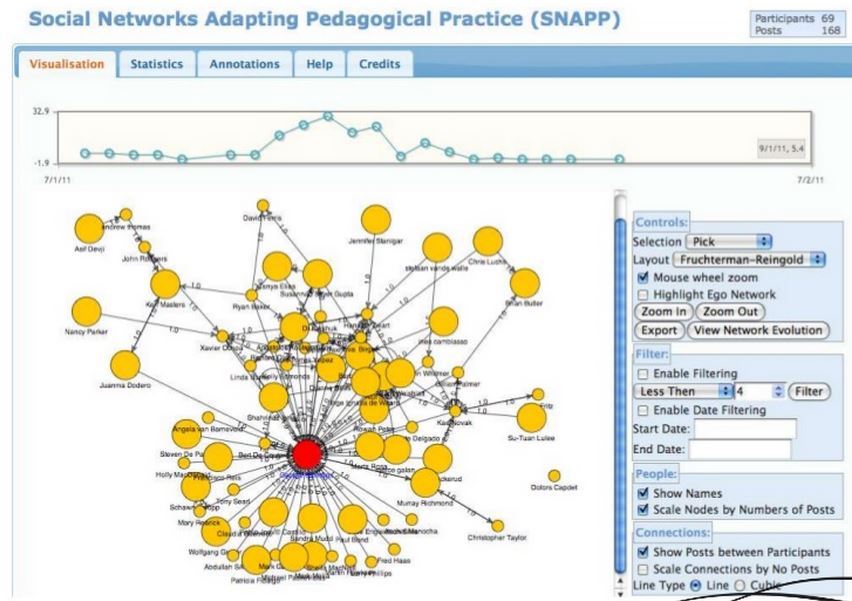
*Construction of the pre-show test*



*Learning object to improve*

### SNAPP

SNAPP for Social Networks Adapting Pedagogical Practice is a tool designed to evaluate student behavioral patterns against learning activity design objectives and intervene as required in a timely manner.



*Example of SNAPP pattern*

SNA has been used to assist educators in identifying instances for learner isolation[[6]](#footnote-6), creativity[[7]](#footnote-7) and community formation[[8]](#footnote-8). It also could be used as an educational evaluative tool in order to monitor group cohesion. It gives the big picture of the social interactions between students (interesting for big groups). It helps the understanding of the social relationships between learners.

The use of this academic software showed up the interest of visualization in education to explain the relations between students.

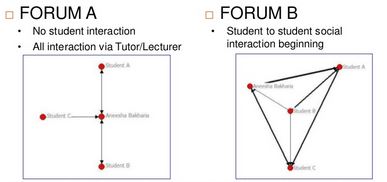
SNAPP analyses the forum postings to provide information on:

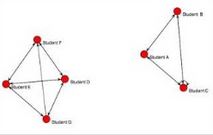
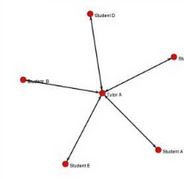
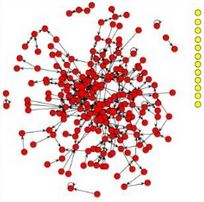
* The total number of posts (displayed at the top right of the SNAPP report);
* The number of posts per user;
* Posting frequency table – lists the number of posts and replies to posts made by each individual;
* Who has been interacting with whom and who is connecting various groups via an embedded network diagram.

Future forum statistics planned include a measure of community, thread depth (i.e. the amount of messages responding to an original posting, or “thread”), the average number of posts and social networking centrality measures;

Ex:

Comparison between two forums, both forum A and B have 14 messages posted by 4 participants:

*Comparison between two student forums*

There are available integration with various LMS such as Blackboard, Moodle or Desire2Learn. SNAPP is particularly efficient to present early warning for teaching staff investigate lack of interactions and track isolated learners or centric patterns that underline lack of communication between participants (and only with instructor). That former pattern could indicate knowledge sharing and collaboration are not occurring. Small nodes of few learners indicate the formation of groups and a potential diminution of diversity and increase of group think.

*Isolated learner, centric pattern and in-class “under construction” groups*

Future directions of development for the software are:

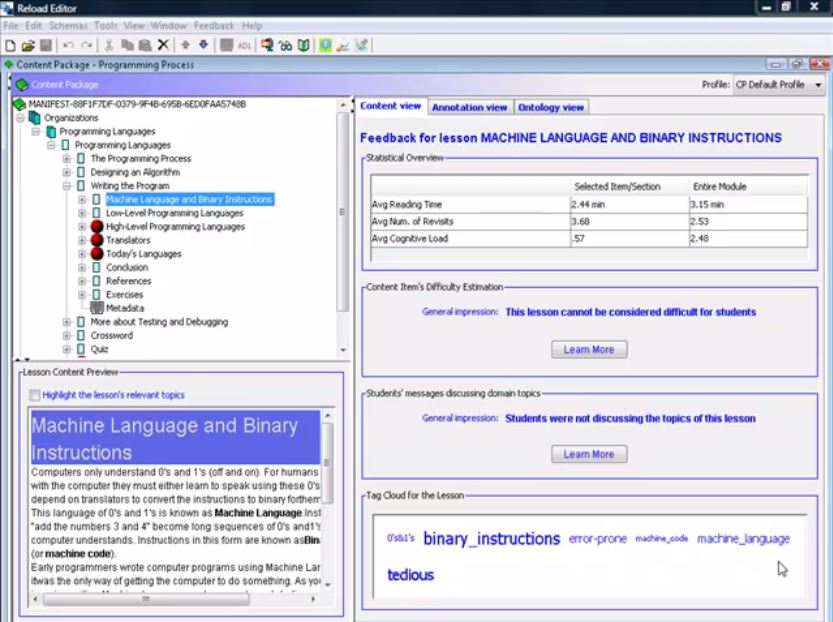
* Behavioral coding: classifying student messages to a coding scheme to speed up the analysis.
* Convert texts to term-document matrix

### LOCO-Analyst

LOCO-Analyst is an open-source tool aimed at providing teachers with feedback on the relevant aspects of the learning process taking place in a web-based learning environment. LOCO-Analyst aims at providing teachers with feedback regarding:

* All kinds of activities their students performed and/or took part in during the learning process;
* The usage and the comprehensibility of the learning content they had prepared and deployed in the LCMS;
* Contextualized social interactions among students (i.e., social networking) in the virtual learning environment.

LOCO-Analyst mixes various sources of such as user tracking data or students annotations. These analyses are based on the notion of Learning Object Context (LOC) which is about a student (or a group of students) interacting with a learning content by performing certain activity (e.g. reading, quizzing, chatting). It is built on top of the LOCO (Learning Object Context Ontologies) ontological framework, which is developed to enable formal representation of the LOC data. Furthermore, it exploits semantic annotation to interrelate diverse learning artifacts such as lessons, tests, messages exchanged during online interactions.



5

1

2

3

4

*Data retrieved by LOCO-Analyst*

1: Index of courses

2: Data on learning objects

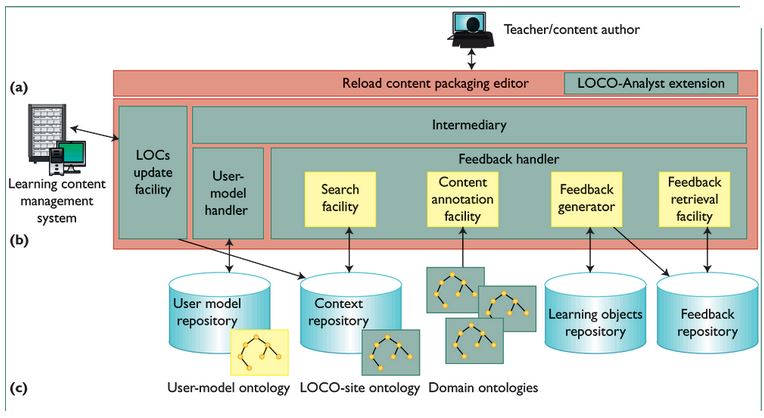
3: Average mood of students concerning the course

4: Students annotation

5: Tags of the lesson

LOCO-Analyst is implemented as an extension of an authoring tool (Reload Content Packaging Editor), an open-source tool for creating courses compliant with the IMS Content Packaging (IMS CP) specification.

LOCO-Analyst has been tested with the user tracking data of the iHelp Courses, an open-source standards-compliant LCMS developed and deployed at the University of Saskatchewan, Canada.

*LOCO-Analyst operating scheme *

# Security and Authentication

## Roles and Use cases

In MOOCTAB platform, there will be mainly 2 types of user roles; content creators and content consumers. The security requirements and security levels may differ for different roles and use cases.

### Content Creators

Content creators, mainly teachers, professionals and administrators will use authoring tools to create online course materials, exams and/or manage lessons with write permissions. Since they can modify the content, there is a need for strong authentication to access to the online materials and tools. Malicious people should not be able to modify the contents and/or add their own contents into existing course materials.

### Content Consumers

Content consumers, mainly students and corporate employees and trainees will view and/or download course materials from/into their tablets and/or web browsers. For securing subscription income, there is a need for secure authentication of consumers, but with a convenient way. Additionally, viewed and/or downloaded course materials (e-books, video contents, PDFs, etc.) must be secured for digital rights, so that they might not be easily copied and re-distributed without permission of the content owner.

## Information Security Key Concepts

In MOOCTAB system, we may consider to cover the following key security concepts.

### Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

### Confidentiality & Integrity

In information security, Confidentiality is a set of rules or a promise that limits access or places restrictions on certain types of information. Data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. Information security systems typically provide message integrity in addition to data confidentiality. For the mobility and tablet world, we should also consider App integrity, so that a malicious person should not be able to create fake apps as course viewers and/or inject malicious codes into existing Apps. The confidentiality of exams and their answers are also important.

### Authentication & Non-repudiation

Authentication is the act of confirming the truth of an attribute of a single piece of data (datum) or entity. Authentication often involves verifying the validity of at least one form of identification. In law, non-repudiation implies one's intention to fulfil their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Electronic commerce uses technology such as digital signatures and public key encryption to establish authenticity and non-repudiation.

### Digital Rights Management

Digital rights management (DRM) is a class of copy protection technologies that are used by hardware and software manufacturers, publishers, copyright holders, and individuals with the intent to control the use of digital content and devices after sale; there are, however, many competing definitions. With first-generation DRM software, the intent is to control copying; with second-generation DRM, the intent is to control executing, viewing, copying, printing, and altering of works or devices. The term is also sometimes referred to as copy protection, copy prevention, and copy control, although the correctness of doing so is disputed. DRM is a set of access control technologies. Those opposed to DRM contend there is no evidence that DRM helps prevent copyright infringement, arguing instead that it serves only to inconvenience legitimate customers, and that DRM helps big business stifle innovation and competition.

## Mobile Security

Smart phones and tablets have taken the benefits from decades of experience about the security hazards of the desktop environments. Mobile device manufacturers and mobile OS providers build an entirely new architecture and established a new approach to security in the design. On the other hand, jail-break and rooted tablets lead to download and execute Apps from unknown sources. Especially on Android mobile devices, users have more control on their devices to modify and lower security levels.

### Device Security and TEE

Device hardware layer and operating system security are at the core of any mobile device security. In the context of the overall security infrastructure of a mobile device, secure element and Trusted Execution Environment (TEE) take an important role. The TEE is a secure area that resides in the main processor of a smart phone (or any mobile device) and ensures that sensitive data is stored, processed and protected in a trusted environment. The TEE's ability to offer safe execution of authorized security software, known as 'trusted applications', enables it to provide end-to-end security by enforcing protection, confidentiality, integrity and data access rights. Handset manufacturers or chip manufacturer have developed versions of this technology in the past years and included them in their devices as a part of their proprietary solution. GlobalPlatform is a cross industry, non-profit association which identifies, develops and publishes specifications that promote the secure and interoperable deployment and management of multiple applications on secure chip technology.

### Application Security

For App integrity and securing App execution, there is no standard. The most popular methods to protect Apps are the use of App signatures and App hardening. Even there are some well known methods for software hardening; different vendors keep developing many new proprietary hardening techniques. Since this is a race between security vendors and hackers, App hardening is a continuous process and requires online controls and regular updates. Code obfuscation, anti-debugging, anti-reverse engineering, memory protection, secure storage, secure communication, code integrity are some key areas to be addressed by App hardening mechanisms and tools.

### Digital Identities (device & user)

Digital identity is the data that uniquely describes a person or a thing and contains information about the subject's relationships. A critical problem in cyberspace is knowing with whom one is interacting. Currently there are no ways to precisely determine the identity of a person in digital space. Even though there are attributes associated to a person's digital identity, these attributes or even identities can be changed, masked or dumped and new ones created. Even secure elements in tablets are considered highly secure to save and secure use of user or device identities, not all tablets have such a secure element and there is no well established standard to use secure elements from different vendors.

## User Authentication Methods

User authentication methods may be differently categorised depending on different contexts.

### 3-factor Authentication

The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something the user *knows (password, PIN, etc.)*, something the user *has (token, device, tablet, etc.)*, and something the user *is (biometry)*. Many existing MOOC systems heavily use 1-factor authentication which is typically a username and a static password to login. A common approach in online banking security, 2-factor authentication is in use; which may be an additional token (hardware or software) that generates one-time-use passwords besides username and static password. 3-factor authentication is in use in government institutions; which may include ownership of a smart card and knowing its PIN and using finger print to access doors or systems.

### One-time-passwords vs Public Key Infrastructures

Two widely used 2-factor authentication methods are one-time-passwords (OTP) and public key infrastructures (PKI). Both methods may also be used to secure data integrity. PKI can also be used for end-to-end encryption to provide confidentiality. OTP solutions are considered easy to implement, easy to operate, easy to use, less costly than KI solutions and that’s why OTP solutions are more in common usage for online service logins, VPN logins, etc. PKI solutions are more complex and costly to install and operate. Usability of PKI is also a great concern when massive online users are considered. On the other hand, PKI is considered much more secure than OTP solutions and PKI is based on well-known standards while many OTP solutions are based on proprietary algorithms. OATH organization tries to specify a standard OTP method. There are 3 different OTP generation methods; basic OTP with no input, challenge & response OTP with a server random input and transaction-data-signing OTP with transaction input. OTP generation may also use time as an input (time-based vs event-based OTPs). OTP may be sent via SMS or generated by hardware tokens or an App on a mobile device. PKI is still the only method which is accepted by digital signature acts in many countries and also in European Union.

### Biometry on the rise

In the recent years, biometry is becoming a favourite authentication method since finger print sensors are becoming smaller to be placed on mobile devices. It is also possible to use mobile device camera for iris recognition and/or to use mobile device microphone for voice recognition. Yet these technologies are still in early days since accuracy of the biometric recognition is not good enough. For example, Apple still backups Touch ID login with a static password, so that in case of fingerprint login does not work, user may switch back to a static password login. Another problem with biometry is that your biometric data may be copied and/or reproduced and replayed to access systems in behalf of you. German hackers prepared a video that shows how to by-pass Touch ID of iPhones on the next day after it is introduced to the market. This demonstration showcase how to copy finger prints from an iPhone screen, how to use this data to produce silicon finger prints and how to use those silicon films to unlock iPhone.

### Software vs. Hardware Tokens

Either OTP or PKI methods is used, the main concern stays as where OTP key or PKI private key is stored and where it is executed for cryptographic operations. The same question exists for biometric data. The most secure way is to use hardware (Smart card, offline device, USB dongles, secure elements, processors, TEE, etc.) to store and use cryptographic keys and/or biometric data. In hardware usage, those cryptographic keys should never leave hardware since the same hardware can also make necessary cryptographic operations internally with those keys. How those keys are produced and stored in hardware is also a critical point to consider for the entire chain of security. In PKI solutions, private key is generated inside hardware and never leave that hardware. Tamper resistance is also very important for that secure hardware. There is Common Criteria evaluations (from EAL1 to EAL6) which show the level of security for hardware. On the other hand, not every tablet and PC has such a secure hardware inside. Distributing an additional security device is also very costly and hard to operate. Carrying and using an additional device is also considered as not user friendly. A contactless smart card with a NFC-enabled tablet may be acceptable for end users. When a software token is considered to store and use cryptographic keys, it can never rich the level of security of any physical security hardware. But on the other hand, implementation, deployment, operation and usage of software tokens are much easier and less costly than hardware solutions. Software tokens can be used on any tablet without any special hardware requirement. Software tokens can also be secured by hardening techniques and online controls. For massive online users, software tokens may be considered good enough.

### Federated Identity (OpenID, SAML, OAuth)

Service providers may prefer to use 3rd party identity providers for user authentication. In this case, users may choose a different identity provider which may offer 1-factor or 2-facor or 3-factor authentication and it may be OTP or PKI and/or biometry. Federated identity means linking and using the electronic identities a user has across several identity management systems. In simpler terms, an application does not necessarily need to obtain and store users’ credentials in order to authenticate them. Instead, the application can use an identity management system that is already storing a user’s electronic identity to authenticate the user—given, of course, that the application trusts that identity management system. There are three major protocols for federated identity: OpenID, SAML, and OAuth. Security Assertion Markup Language (SAML) is an XML standard that allows a user to log on once to the log on site for all the trusted websites. OAuth is access granting protocol and provides authorization to APIs. OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

## Security Implementation Approaches

In security implantations, mainly there are 3 different approaches; using standard algorithms and protocols, using best practices and implementing proprietary methods and techniques. Even there is big dispute which one is better than the other; the best approach may be to use all 3 approaches in a system implementation.

### Standards

Especially in PKI systems, there are many standards like PKCS#1 to PKCS#15, X509 certificates, SSL, TLS, standard symmetric algorithms (3DES, AES…), standard asymmetric algorithms (RSA, ECC,...), standard hash algorithms (SHA1, SHA256,…), SMIME, etc. The approach of using standard algorithms and protocols brings many advantages; use of public methods allows knowing all details of algorithms and protocols publicly by everyone. This means that more scientists, more test labs, more security institutions can test and attack to these algorithms and protocols; which proves how strong those algorithms and protocols are. On the other hand, if a weakness appears in these standard methods, any solutions that use them will be affected immediately (as experienced with DES and SSL recently). The security of standard algorithms is provided with the secret key of that algorithm. That’s why storing and using that secret key is the most critical part of the whole security.

### Best Practices

Even there is no unique standard how to implement and use PKI solutions, there are many best practices to follow. If any weakness occurs in implementation of key generation, key distribution, key management, then there may be always a point of attack in such PKI system. The rule in security systems is that the system can be as secure as its weakest link in the chain.

### Security through Obscurity

In this approach, proprietary and secret designs and methods are used and such information is never shared with the outside world. An attacker needs to reverse engineer such systems and must initiate a targeted attack. This means that cracking a standard algorithm or protocol will not be enough to hack into such systems. Since the proprietary and secret security designs are tested by only designers and/or with a few testers, it is very important to use 3rd party independent security labs to attack those systems with a claimed security level in hand. Developers must use complex obfuscation techniques and implement anti-reverse engineering and anti-debugging to hide design secrets. Since no one can hide a design secret forever, such systems require regular updates and changes in security mechanisms. Because of updates, hackers will have a limited time to crack the system. Otherwise, hacker should start from scratch with every update.

## Solution Recommendations

For MOOCTAB security and authentication, 3 main works may be researched and developed in parallel. Even these works may run isolated from each other; a service provider may use all together. These works may also have overlapping tasks.

### NFC & Contactless Cards

In the consortium, NXP and Gemalto may implement together contactless card and NFC authentication for students and teachers. (*NXP and Gemalto may add more comments to here*)

### Application Security & Virtual Smart Cards

Kobil will implement a software only solution for App security, device-app-user binding and user authentication with soft-PKI-tokens (virtual smart cards). The solution will consist of a security server to be placed by either a MOOCTAB service provider or an identity provider. App developers and web portal developers will be provided by SDKs to integrate this solution. Kobil plans to use both standard algorithms and protocols (with all best practices) and many proprietary methods like software hardening. By doing this, we will benefit the advantages of all different approaches for security implementations. To make PKI deployment and management and its usage very easy, Kobil plans to use anonymous device certificates and auto enrolment within Apps. Digital signature generation and verification will be all seamless to end users and service providers. The solution should have regular updates to give hackers limited time to attack to the system. App integrity and App-device binding must be controlled by the online server.

### DRM Solutions

Besides Kobil’s App-device binding solution, Viaccess-Orca may also develop a DRM system to secure online (and downloaded?) content. (*Viaccess-Orca may add more comments to here*)

1. "Schools and Partners". edX [↑](#footnote-ref-1)
2. "Courses - edX". edX. [↑](#footnote-ref-2)
3. A Profile of the LMS Market (page 23) (PDF), CampusComputing, 2013. [↑](#footnote-ref-3)
4. [Simone, 2012] [↑](#footnote-ref-4)
5. http://www.imsglobal.org/pressreleases/pr150506.html [↑](#footnote-ref-5)
6. Mc Donald, Stuckey, Noakes and Nyrop, 2005 [↑](#footnote-ref-6)
7. Burt, 2004 & McWilliam & Dawson, 2009 [↑](#footnote-ref-7)
8. Dawson, 2008, Lally, Lipponen and Simons, 2007 [↑](#footnote-ref-8)