

Federated identity management from University to digital school, and one login to resources and services

Maria Laura Mantovani^{a,b}

^aConsortium GARR, Italy, marialaura.mantovani@garr.it, <http://orcid.org/0000-0002-2311-2924>

^bUniversity of Modena and Reggio Emilia, Italy, marialaura.mantovani@unimore.it

Abstract

Nowadays a number of resources available online can help quicken the creation and strengthening the Italian population's digital expertise, especially if the school system is ready to fully exploit them. In schools, due to the limited funds available, investments need to be channeled towards the network infrastructure and the crucial security services. This is pointed out in the call from the Ministry of Education addressed to schools in order to build, extend or upgrade their network infrastructure. The call provides access to structural funds including, in addition to the LAN / WLAN network, the federated identity management and access control to online resources. IDEM Identity Federation is operational since a decade for the Italian universities and it is now offering its quality experience to schools. IDEM allows managing and controlling user access to online services, initiated from any type of digital devices. The user connects from its personal device or from the one owned by the school, and whether he connects from school, from home, or on mobility, IDEM ensures that the digital school can fulfill its mission while ensuring the students' actions over the network are accounted and their privacy and safety is ensured.

Keywords: skill development, educational provision, structural funds, ICT equipment, teacher education.

Digital inclusion and skills

A European Commission study ("Digital inclusion and skills", 2014, p. 6) shows that 47% of the European population has insufficient digital skills and 23% has none at all. In Italy 60% of the population has insufficient digital skills, while 40% has none and this, with our large population, equates to almost 18 million people without digital skills. The school is the place where this gap can be overcome in order to gain sufficient digital skills. We are not referring to computer specialists, but to the use of digital technologies in everyday life, in the common work, in new professions. Know how to collaborate using a technology platform, how to produce an audio-video or multimedia document, how to create a website, are skills that all students could easily obtain as a part of their curricula, to be used their future working life.

Eventually, all of this has been transposed into the PON 2014-2020 call for schools: "In the European society information and knowledge are valuable resources able to change the flow of the economy; holding digital skills has become one of the minimum requirements for ensuring adequate levels of social and digital inclusion. Therefore, to improve the quality of life and sustain the Country's socio-economic development, all the citizens must be granted equal opportunities in the use of the network and in access to information, knowledge, services, education and training for employment; the organization and the quality of services provided by public administrations need to take into account the divide still existing across the country and the continuous rapid evolution of ICT technologies.

To overcome the digital gap more and more diversified investments are needed both in infrastructure - for connectivity and appropriate technological equipment availability - and for the provision of courses aimed at reducing the digital divide and for the development of specific and relevant digital skills across the population, particularly in young people, teachers and workers" ("Fondi Strutturali Europei", 2015).

PON 2014-2020 call for digital school

(20 REGIONS, 8.730 SCHOOLS, 3 BILLIONS EURO OF AVAILABLE FUNDS)

"The empowering of school environments with technologies suited to disseminate innovative teaching models" will be provided. "The Ministry of Education has stepped up measures designed to encourage school communities to rethink about spaces, time and the way of teaching and learning, just thanks to greater mediation of technologies and new languages in daily teaching practices" ("Fondi Strutturali Europei", 2015).

The first measure put out to call by the Ministry of Education gives to the schools the ability to create, expand or upgrade the LAN (Local Area Network)/WLAN (Wireless Local Area Network) infrastructure. The schools, provided with "100% wireless coverage of the school area and an Internet connection of at least 30 Mbps will ensure their students access to digital textbooks, software with exercises, broadcast and podcast lessons, simulations and digital educational games, and many opportunities for access to additional knowledge. Learning is no longer restricted to specific school time frames and the teaching methods use open and flexible times and spaces. You can learn anywhere, anytime, on any device and with the support of those who have the control of the content, the knowledge and the procedure" (Ghizzani, 2015).

This vision by the Ministry of Education appears to suggest a growth of the Bring Your Own Device (BYOD) paradigm in order to encourage the use at school of mobile devices in possession of students and teachers ("Pros and Cons of Allowing Digital Devices in the Classroom", 2012). Important economic factors orienting towards BYOD are highlighted too. The school adopting BYOD does not spend any more in expensive computer labs with PCs that soon become obsolete (Menduni, 2015). The result is a significant savings that can be invested in favor of a modernization of the network infrastructure of the school and its security. The provision of a modern and technologically advanced school is important for the school itself, as students increasingly choose the school in which to enroll taking into account its technological provision (Balena, 2015).

To successfully implement BYOD at school ("The "BYOD" Debate"), few enabling factors must be in place (Delgado, 2014): 1) an adequate network capacity, both internally and externally, must be ensured. Hundreds of students should be able to access the Internet simultaneously, so network capacity is extremely important. The access link is one of the elements; on the other hand the LAN/WLAN inside the school and transmission equipment must be adequate to the expected traffic; 2) clear rules about the behavior of students, teachers and parents with digital devices must be set out and offenders must be punished ("11 Sample Education BYOT Policies To Help You Create Your Own", 2014); 3) personal security and device's security must be a subject of teaching; 4) an identity management system must be implemented to know who is doing what on the school network; 5) BYOD users should not only be enabled to use existing digital materials and services, but encouraged to become active users, with the ability of creating new digital content.

The call of the Ministry of Education focusses precisely on points 1 and 4, where infrastructure investments are needed. The remaining points will be hopefully addressed in the coming calls, which are expected to tackle the objectives of building and improving the teachers' and other school staff competences and the development of the Digital School.

Challenges in adopting Software as a Service at school

Many of the tools we already use at school today are platforms provisioned in the Software as a Service (SaaS)¹ fashion, namely they live outside the perimeter of the school, such as Google Drive², GoogleApps³, Office365⁴, the digital school record book, e-books, the school website. Also Moodle⁵ can be a service hosted outside the school. To access all these SaaS tools, each student and teacher will need a digital identity, namely a username and password for each one of the services they need to access. The school institutions wanting to promote and effectively use digital technologies, not limited to the BYOD, but also by means of computer labs or institutional workstations, must prepare to manage and control their members' access to all the services they use, both inside the school and SaaS. For services provisioned by the school, the user is no longer using different digital identities created for each service, while the school takes care of managing digital identities, one for each of its members, performing operations of creating and assigning them to the users, monitoring their usage, updating and finally disabling them at the end of their life. The effort devoted to the digital identities management is rewarded with control and security provisioned to the users. It is no more acceptable to waste the efforts of identity management scattering it on all the SaaS platforms that the school

¹ https://en.wikipedia.org/wiki/Software_as_a_service

² https://en.wikipedia.org/wiki/Google_Drive

³ https://en.wikipedia.org/wiki/Google_Apps_for_Work

⁴ https://en.wikipedia.org/wiki/Office_365

⁵ <https://en.wikipedia.org/wiki/Moodle>

decides to use. The model of centralized identity management has begun to spread in Italian universities for ten years and being now fully operational, schools can count on a consolidated working model to follow (Author, 2008).

Federated identity management: an effective tool for managing the digital school

One of the indicators for the evaluation of the proposals called in the Ministry of Education tender is having opted in to federated identity management. "With federated identity management we mean access to many resources and services through the release of unique credentials. This system makes the user's online activities easier and more secure, while at the same time reducing the credential management overload for those in charge of services, and eliminating the need to replicate credentials in a number of databases." It becomes then necessary to have tools and technologies to centralize the identity management (Author, 2015), to improve management efforts and simplify the operations the user need to do. In the identity federation management model the SaaS administrator no longer has to manage user authentication, a complex and burdensome issue for the service, which does not provide added value, but only adds security problems and takes away resources and efficiency to the main business. Removing this burden the services increase in security and efficiency. On the other hand the school has to implement a new centralized system for managing identities.

Centering the effort of identity management in one place, the school can guarantee more security to digital identities, add additional control features such as a second factor of authentication, and is provided with tools to enforce privacy, all of this with greater efficiency. In this way the school can offer many services to teachers, staff, students and their parents. The advantage for the user is obvious: a unique password for accessing all online resources. With one password to remember we gain greater ease of use accessing multiple resources and a greater security having just one password to protect, while privacy is guaranteed because it is under control of the school identity management operator, who is the data controller of personal data of students, parents and teachers.

The communication protocol between federated identities and online services is SAML (Simple Assertion Markup Language)⁶ (Cantor et al, 2005). SAML decouples the user authentication from the access to a resource. The identity management and authentication are executed by a component called Identity Provider (IdP) located at the school, while access control (authorization) to the resource is done by a component called the Service Provider (SP). The SP, in order to decide if the user can log in, evaluates the assertion sent by the IdP to the SP. The IdP is the sole online service that receives the user's credentials. Each other service, whether internal to the school, or in the cloud, receives only the SAML assertion assumed necessary to decide whether the user can access or not.

The benefits introduced with federated identity management are: for the user, the Single Sign On (SSO) in accessing many services both internal and external to the organisation (Landau & Moore, 2012); for the school, a unified identity management, by means of which you can control who does what. All users who bring their laptops or devices at school (BYOD), while they access online resources, will be under control of the IdP, a system managed by the school. Clearly, organisations that do not have implemented their own IdP, entrust privacy and users' monitoring to external services. A third benefit is for the resource provider, for which the management of its application is simplified.

Privacy in the digital school

Schools must take the responsibility of the personal data protection of people working, studying, or in any case having to do with the school. The Italian Privacy Act (Italian Legislative Decree no. 196/2003) establishes the "data minimisation principle: information systems and programs are configured to minimise the use of personal and identification data, so as to exclude the processing if the purposes sought in the individual cases can be achieved by using either anonymous data or mechanisms that allow identification of the individual only in case of need." With SAML, we have the technological tools to enforce the provisions of the Privacy Act and the school can transfer to providers only those personal data that are strictly necessary to provide the requested service. This means freeing the user from providing data in excess, avoiding to accept a treatment too invasive of privacy.

The IdP handles all the personal data of users (teachers, students, parents), organising them into homogeneous profiles in order to create and manage digital identities. The IdP, within its capabilities, can appropriately create the assertions intended for each service so that each assertion, directed to a specific service is built for each specific user, and contains only the strictly necessary information in order to allow the access and deliver the service. Each assertion is encrypted and signed to ensure confidentiality, integrity and non-repudiation during online transmission stages and reception by the recipient.

⁶ The Security Assertion Markup Language (SAML) 2.0 is an XML-based framework that allows identity and security information to be shared across security domains. The SAML specification, while primarily targeted at providing cross domain Web browser single sign-on (SSO), was also designed to be modular and extensible to facilitate use in other contexts.

One identity federation for universities and schools and the available services

Similarly to what was done since last 7 years for universities and research institutions, for whom IDEM Federation⁷, coordinated and managed by the Consortium GARR⁸, has been set up, it might be useful to start organizing an identity federation for schools. The identity federation aims to ensure confidence among the participating organizations: the organizations, registering their Identity Provider and Service Provider in the federation, certify that the systems are under their control and responsibility. In the federation, communication between participants can only happen if the trust is maintained and actors communicate through encrypted and certified statements. In this way the transit online of personal data and digital identities is certified. The IDEM Federation nowadays counts over seventy Identity Providers in Italy delivering to date about 4 million digital identities to students, researchers, faculties, staff and alumni of Italian universities. These end users can now gain access to about 1000 protected resources available in the world.

Already available in the IDEM Federation are some services useful to SAML enabled schools: Wifi access throughout the national territory, videoconferencing GARR Vconf, mega-file sharing with Filesender, Le@rning-GARR, Terena Certificate Service, EduOpen, Dreamspark, Knodium. Other services are immediately configurable: for example any Moodle service, Wiki and CMS on various platforms, Google Apps, Office365, Box, Media Library On Line, Sebina Open Library, social learning platforms. Other services such as e-books and school record book platforms could be available if there was a critical mass making the request, as shown by the successful use case related to publishers in the US and Britain (Landau & Moore, 2012).

References

c) *Article From an Online Periodical with DOI Assigned:*

Landau, S. & Moore, T. (2012, October). Economic tussles in federated identity management. *First Monday*, Volume 17, Number 10 <http://dx.doi.org/10.5210/fm.v17i10.4254>

i) *Quotes from web sites:*

11 Sample Education BYOT Policies To Help You Create Your Own (2014). [html] Retrieved from <http://www.teachthought.com/uncategorized/11-sample-education-byot-policies-to-help-you-create-your-own/>

Balena, C. (2015). Da Mantova al Majorana di Brindisi, [html]. Retrieved from <http://ischool.startupitalia.eu/ischool-2/35246-20150418-da-mantova-al-majorana-di-brindisi-sognando-astrosamantha>

Cantor, S., Kemp, J., Philpott, R., & Maler E. (2005, March). Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, [pdf]. Retrieved from <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

Delgado, R. (2014). 5 Successful BYOD Practices and Policies for Schools, [html]. Retrieved from <http://www.emergingedtech.com/2014/07/5-successful-byod-practices-and-policies-for-the-schools/>

Digital inclusion and skills in the EU 2014 (2014). European Commission. [pdf] Retrieved from http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5809

Fondi Strutturali Europei – Programma Operativo Nazionale “Per la scuola – Competenze e ambienti per l’apprendimento” 2014-2020. Avviso pubblico rivolto alle Istituzioni scolastiche statali per la realizzazione, l’ampliamento o l’adeguamento delle infrastrutture di rete LAN/WLAN. Asse II Infrastrutture per l’istruzione – Fondo Europeo di Sviluppo Regionale (FESR) - Obiettivo specifico – 10.8 – “Diffusione della società della conoscenza nel mondo della scuola e della formazione e adozione di approcci didattici innovativi” – Azione 10.8.1 Interventi infrastrutturali per l’innovazione tecnologica, laboratori di settore e per l’apprendimento delle competenze chiave. (2015). Ministero dell’Istruzione, dell’Università e della Ricerca, Dipartimento per la Programmazione e la gestione delle risorse umane, finanziarie e strumentali, Direzione Generale per interventi in materia di edilizia scolastica, per la gestione dei fondi strutturali per l’istruzione e per l’innovazione digitale. [zip] Retrieved from http://hubmiur.pubblica.istruzione.it/alfresco/d/d/workspace/SpacesStore/1cfc6449-c47c-481d-8dd8-00c473f13584/prot9035_15.zip

⁷ IDEM Federation official website <https://www.idem.garr.it>

⁸ Consortium GARR official website <http://www.garr.it>

Ghizzani, G. (2015). Pon 2014-2020, nuove opportunità dall'Europa. Oltre 3 miliardi di euro per la scuola [html] Retrieved from <http://blog.tecnosistemi.com/posts/2015/aprile-2015/pon-2014-2020,-nuove-opportunit%C3%A0-dalleuropa-oltre-3-miliardi-di-euro-per-la-scuola/>

Author, (2008). IDEntity Management federato per l'accesso ai servizi, [pdf]. Retrieved from http://www.garr.it/eventiGARR/ws08/presentazioni/Tutorial%20-%20IDEM/Mantovani_WSGARR08.pdf

Author, (2015). Infrastrutture di autenticazione e autorizzazione - La federazione IDEM, [zip]. Retrieved from <http://www.progressintraining.it/files-bandi-di-gara/intensivi-apm-download/151-percorso-2-mantovani-infrastrutture-di-autenticazione-e-autorizzazione-la-federazione-idem>

Menduni, G. (2015). Rassegniamoci, gli insegnanti non capiranno mai che lo smartphone a scuola non è il demonio, [html]. Retrieved from <http://www.chefuturo.it/2015/04/smartphone-scuola-insegnanti-digitale/>

Pros and Cons of Allowing Digital Devices in the Classroom (2010). [html] Retrieved from <http://education.cu-portland.edu/blog/tech-ed/pros-and-cons-of-allowing-digital-devices-in-the-classroom/>

The "BYOD" Debate, [html]. Retrieved from <https://sites.google.com/site/vcuadms647/weekly-sessions/module-4/w12-week-twelve-week-of-november-14/the-byod-debate>