Toward Educational Virtual Worlds: Should Identity Federation Be a Concern?

Gonçalo Cruz[1,2*], António Costa[2], Paulo Martins[1,2], Ramiro Gonçalves[1,2] and João Barroso[1,2]

[1]INESC TEC (formerly INESC Porto), 4200-465 Porto, Portugal // [2]School of Science and Technology, Universidade de Trás-os-Montes e Alto Douro, 5000-801Vila Real, Portugal // goncaloc@utad.pt // acosta@utad.pt // pmartins@utad.pt // ramiro@utad.pt // jbarroso@utad.pt

[*]Corresponding author

ABSTRACT

3D Virtual Worlds are being used for education and training purposes in a cross-disciplinary way. However, its widespread adoption, particularly in formal learning contexts, is far from being a reality due a broad range of technological challenges. In this reflection paper, our main goal is to argue why and how identity federation should be discussed and adopted as a solution to several barriers that educators and institutions face when using Virtual Worlds. By presenting a clear set of scenarios within different dimensions of the educational process, as classroom management, content reuse, learning analytics, accessibility, and research, we consider identity, traceability, privacy, accountability, and interoperability as main concerns in order to support our argument. Finally, we conclude the paper by presenting paths to a proposal for a workable solution, through the analysis and reflection of different and current efforts that has been made by other teams, towards future technological developments.

Keywords

Digital Identity, Identity Management, Federated Identity, Virtual Worlds, Education

Introduction

We live the most collaborative experience since the beginning of the World Wide Web, due to the easy manner in which one can connect with other users, resources, services and information. To attain things such as books we wish to buy, tuition fees we have to pay, or even the completion certificate of an online course we attended, we constantly face the need to use our identity, and ensure to other entities that they are indeed dealing with us. This raises ethical and legal questions about privacy, security and accountability, both for users and entities - in the use and sharing of their personal information.

Thus, it's strictly necessary to have management tools available that enable not only the certification and validation of users' identities, but also assure them that there will be a basic level of privacy when they share their personal information with other parties. This is why the existence of federations between entities, through the mutual agreement and establishment of policies, practices and common standards, proves to be of greater importance. The inherent advantages of these trust relationships are numerous and constantly cited on literature (Madsen et al., 2005; Shim et al., 2005; Smith, 2008).

In education, identity federation has also been a topic of interest for researchers (Linden, 2005; Hammerle, 2006; Aguirre et al., 2008), but it mainly addresses the use of web-based systems such as wikis, learning and content management systems, forums, academic portals, repositories, etc. Regarding 3D Virtual Worlds, some studies were developed within this field with emphasis on other perspectives, such as sociology (Lorentz, 2011), anthropology (Gabriels et al., 2011), and psychology (Aas, 2011). However, other studies show identity issues as barriers and challenges for students, staff and institutions in the adoption of Virtual Worlds for learning (Palomaki, 2009; Dalgarno et al., 2011), but we are left with a lack of clear evidence that supports the argument on why identity federation should be taken into account as one of the major concerns towards the widespread use of Virtual Worlds in education.

For that purpose, there is a need to understand in which dimensions of the educational process, identity federation technology has the potential to bring benefits. Students, teachers and institutional leaders feel somewhat unmotivated, unconfident and insecure in the development, management, support and assessment of classrooms or educational projects in Virtual Worlds due a broad range of factors related to identity issues. From time consumption (e.g., proliferation of students' and teachers' logins, passwords, roles and other data for different institutional systems, including Virtual Worlds; track, link and assess huge amounts of 3D data, as students' in-world access, classroom attendance and task progress; etc.), to costs (e.g., 3D resources development, interoperability and

reutilization, copyright policies and licensing terms, etc.) and reputation (e.g., ethical and legal questions related with avatars' problematic behaviors, as inappropriate gestures and customizations, in which privacy assurance and users' accountability are compromised).

In these and other dimensions that we will present afterwards, several identified barriers and challenges can be solved and/or minimized by identity federation technology. However, other ones will remain without a clear solution for teachers and institutions. For instance, in 3D distance learning classrooms, if on the one hand we can manage students' attendance based on their avatars' status, behavior and interaction during the class, logins' and logouts' time and zone, etc., on the other hand we can't fully ensure if the student behind the avatar is really who we think it is. That is a classical challenge, throughout the years, common to any social or group application to be implemented in the classroom, not just Virtual Worlds.

Although, besides the argument on why identity federation technology should be used towards the massive adoption of Virtual Worlds in education, we also need to discuss how the solution must be figured out. Therefore, we begin by describing the state of the art related to the digital identity topic, framing it within the e-learning and distance education fields. Subsequently, we move forward to the major contribution of our work, clearly demonstrating a set of different problematic scenarios that underlie our argument, according to the current solutions and efforts. Finally, we end the paper by proposing paths to a practicable solution, in order to guide future technological developments that can solve the different problems identified within the presented educational scenarios.

E-Learning and digital identities

Digital identities are electronic representations of known information about a specific individual or organization, such as attributes, traits or preferences (Anwar et al., 2006). In e-learning, related with the concept of telepresence and how an individual manifests electronically, digital identities are created not only by the inclusion of biographical details but also with information on how the individuals communicate and interact with others in a shared online space.

Distance education may be more conducive to academic dishonesty than face-to-face instruction (Baron & Crooks, 2005), and the large gap existing between the current generation of students and teachers may mean more opportunities for it to occur (Windham, 2005). Thus, much effort has been put into the effective verification of students' identities through online learning authentication (Bailie & Jortberg, 2009). In order to ensure academic integrity (Roberts & Hai-Jew, 2009), and prevent negative behaviors such as cheating (Bedford et al., 2009) and plagiarism (Olt, 2009), institutions need to verify if the current person that signed up for the learning is the one taking the course. Also called accountability, this is of critical importance for the reputation of the institutions, and defined as an encouraging process for students to become more involved in managing the risks they face (Whitson, 2009).

There are different types of authentication methods, depending on the data requirements used for that purpose. Some systems use only a password and others use smart cards or biometrics (physiological characteristics and behaviors), in order to link an individual with his/her own digital identity. Common biometrics measures involve the uses of fingerprints, iris scans, facial scans and voice (Ahmed & Moskowitz, 2005), and others use a combination of information, such as keystroke latencies in word-processing (Joyce & Gupta, 1990), search interests (Rowe, 2010), or even traffic-based access network (Barisch, 2009). At a very basic level, many systems use Internet Protocol (IP) address tracking to link individual users with their respective locations; IPs and real users are closely related (Clauβ & Schiffner, 2006). For instance, logging in with a particular identity from various IPs in geographically dispersed locations may be one way of identifying concerns.

Students have lots of personal information that they share in online courses or activities. They share personal information within their work and the access to that information should be protected. It may be wholly private, disseminated among a small group of learners, or published on the Web, but whatever the case, the student has intellectual property rights over his/her own work that should also be preserved. In this sense, the concepts of authoring and privacy are strictly related to the knowledge of identity and should be taken into account by educators and institutions. Sometimes, a pseudonym may be used as a unique identifier, in order to provide an anonymous

identity during specific learning activities (e.g., peer reviewing). The pseudonym is an identifier where only the entity that assigned this type of identification knows the real world identity behind it (Anwar and Greer, 2012).

In the specific case of 3D Virtual Worlds, some researchers have found a very disconnected relationship between the avatar's information and the user's real world identity (Junglas et al., 2007), which suggests a greater range of identity differentiation. Such variant identities may allow them to experiment a set of roles and opportunities for social interaction. Many authors are against this digital identity anonymity because of the fear that anonymity would result in misdeeds or other threats, especially in business and educational contexts (Adrian, 2008; Boon & Sinclair, 2009).

Identity and access management

The concept of access management is used to describe the process of allowing access to protected online information. It mainly describes the administrative procedure to allow access to online resources or services, for any individual based on the provided identity (Alves & Uhomoibhi, 2010). It includes authentication (the process of verifying the identity of any individual that is requesting access), authorization (the process of determining what kind of access that should be granted to the user based on his/her credentials), attributes (information about the user, as membership or role), and trust (the agreement between different parties and systems for sharing identity information).

There are several ways in order to control user access to resources. One of the most known is Role-Based Access Control (RBAC). A method that regulates access to computer or resources based on the roles or privileges of individual users within an institution (Onashoga et al., 2014). In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file. Roles can be defined according to the user skills, authority, and responsibility within the institution. When properly implemented, it enables users to carry out a wide range of authorized tasks by dynamically regulating their actions according to flexible functions, relationships, and constraints. Not only services based on the Web, which are frequently used in e-learning contexts (e.g., wikis, learning management systems, forums, etc.), but also 3D Virtual Worlds (e.g., Second Life and OpenSimulator) use this type of framework for access management (Allison et al., 2012).

However, much of the current services supporting e-learning require authentication, which means that the user needs to introduce his/her credentials in each one. This is a problem tackled by Single Sign-On (SSO) access control, that improves user experience and gives response to some of the issues related to identity management. With SSO systems, authentication is managed centrally and the user can navigate through different distributed applications using the same session and/or credentials (Bhatti et al., 2007). In this sense, SSO systems provide an effective way to manage authentication and authorization inside institutions, but are restricted to the administrative domain of each institution. For instance, in order to provide the mobility of users, access and exchange of contents and services across different educational institutions, the creation of federated identity management solutions is mandatory.

Federated identity management

Almost all technology-based digital identities work within particular systems and are not federated over multiple systems (Schwartz, 2010). The concept of identity federation can be understood as a group of organizations or service providers which have built trust relationships among themselves in order to enable sharing of information about the identity of its users. It returns the responsibility for authentication to a user's home institution (also known as identity provider), and establishes authorization through the secure exchange of information between the two parties. This concept allows the possibility of integration and sharing of resources in a secure and reliable way (Bhargav-Spantzel et al., 2007).

There are a number of advantages for educational institutions in adopting a federated access management system (Kallela, 2008; Alves & Uhomoibhi, 2010). The main advantages are:
- User experience: users only need to use their institutional username and password to access internal and external resources;
- Interoperability: most of the systems are based on international standards and implemented at national level in

several countries (e.g., UK, USA, Australia, Spain, Finland);

- Cost saving: reducing the costs of service providers for setting up and managing multiple users and passwords, as well as reducing help requests from users who forget their own credentials;
- Privacy and security: is based on federation policies and trust agreements between parties, as well as standard technology, practices, and strong authorization controls over secure access channels;
- Collaboration, sharing, and resources availability: increasing the quantity, quality and variety of users, experiences and educational resources to support learning;
- Flexibility: institutions and educators can more easily track down appropriate resources for their students and negotiate licenses only for users who will use particular resources, whatever their needs and wherever they are located;
- Assessment: allowing the traceability of data related to users' access and use of services, helping educators to adjust their instructional strategies and support to students.

In addition to e-business and e-commerce, the most common areas where these solutions are applied, federated identity management is also currently being adopted by educational institutions worldwide. These institutions have agreed in terms of policies, practices and standards in order to establish a trust relationship that allow their users to access and use services and resources provided by the partners. For example, in the European Higher Education context, eduGAIN project, from the GÉANT network, encompasses more than 40 beneficiaries, and is a service intended "[...] to enable the trustworthy exchange of information related to identity, authentication and authorisation between the GÉANT (GN3plus) Partners' federations. The eduGAIN service will deliver this through co-ordinating elements of the federations' technical infrastructure and a policy framework controlling the exchange of this information." (European Commission Communications Networks, Content and Technology, 2013). Likewise, led by the Internet2 consortium and with more than 400 Higher Education participants, the InCommon project was created in order to support "[...] a common trust framework for U.S. education and research. This includes trustworthy shared management of access to on-line resources in support of education and research in the United States. [...]" (InCommon, 2014).

Finally, there is a large diversity of identity federation systems, standards and specifications. From systems based on open standards to those based on proprietary solutions, developed by private companies. Nearly all have similar features, ranging in scope and applicability of the solution. However, some architectures and specifications stand out: the Security Assertion Markup Language (SAML - http://saml.xml.org/about-saml/) - a standard created to exchange security related information between organizations and enterprises; the Internet2 Shibboleth specification (http://shibboleth.net/about/) - an extension of the standard SAML to being an example of an identity federation system that uses Web-based implementation methodology of SAML; the Web Services Security (WS-Security, WSS: http://www.soapui.org/SOAP-and-WSDL/applying-ws-security.html) - which is an extension of the Simple Object Access Protocol (SOAP) developed according to the WS-Federation specification; the OpenID (http://openid.net/) - a Single Sign-On open standard for consumers, accepted by organizations as Google, PayPal, Yahoo!, etc.; and the OAuth (http://oauth.net/about/) - another open protocol/standard that runs an API authorization between different applications; among others.

Identified problematic scenarios and current solutions

An extensive research agenda can be found addressing Virtual Worlds technology issues and concerns (Lee & Warren, 2007; Hendaoui et al., 2008; Messinger et al., 2009; Thompson, 2011). Many areas need further exploration, but we are moving toward standardization that helps insure interoperability (Burden, 2011). However, most of the standards efforts have concentrated on the graphical aspects, neglecting other important issues that can impact its widespread adoption for education and training purposes - as identity federation.

In different dimensions of the educational process within Virtual Worlds, identity federation can impact all actors in educational institutions, such as teachers, students and staff - fostering its massive adoption. This is why the problem must be discussed by the educational technology community. In order to better explain how relevant the problem is, we present below a set of scenarios and dimensions of the educational process in Virtual Worlds, where the most cited and adopted ones (e.g., Second Life and OpenSimulator) will gain more attention - but others should also be taken into account.

Firstly, it should be possible for a teacher and/or trainer to easily create and build his/her class or team without the current administrative workload needed. This means that if a teacher desires to start running educational activities in a Virtual World, technology should automatically recognize and link their students' academic identity with the 3D avatars, giving them the permissions and attributes based on their roles. This will enable students to access the virtual spaces with a unique set of credentials that can easily identify the student in the 3D virtual space (e.g., login, password, avatar's name, profile information, etc.). Moreover, the usability related to this process should also be improved. For instance, this instantiation of roles and permissions can be available from a template on the web, without much complexity or difficulty to fill out. This is already happening for Virtual Worlds' technology such as Second Life, with the SLOODLE project. However, linking avatars with the Moodle students' mapping is needed (Sloodle, 2013).

Secondly, it should also be possible for teachers and staff to manage and track students' attendance within the classes or training sessions. This means that teachers should have tools available to track and assure students' participation in the classroom based on their identity, knowing when they login, logout or go outside the classroom space. Moreover, it would be also possible to have a report on avatars' status (e.g., if they are away or not, based on the frequency of interaction with their avatar) during the class - helping manage and register the attendance and participation of each student. Clearly this is a hard task for teachers in a random access environment such as Second Life, to identify late arrivals or early departures from his/her learners, and also is a requirement of almost of the educational institutions (Madeira et al., 2010; Kluge & Riley, 2008). However, this does not fully assure the students' participation and identity within the classes - but that is also a problem with other applications, not only with Virtual Worlds, along the years (e.g., a student can use the credential of a colleague and impersonate him; an account owner may delegate control of their attendance to a number of real life individuals who manage his/her attendance interchangeably, in order to maintain an around-the-clock in-world presence, etc.) (Lindsay et al., 2010), and even in face-to-face classes is possible to have similar problems (e.g., a student can stay in a classroom but nothing assures that he/she will not pay attention or sleep; or even in large classes with lots of students, in which is hard to manage the identities of each student during an evaluation test).

Thirdly, it should be possible to have an integrated and holistic view of students' learning patterns, due to a transparently navigation across services, with a unique credential, that quickly can occur in a multimodal enriched learning environment (SLOODLE fails in this aspect, because it only offers the connection between Moodle and Second Life - not with the different academic services and tools, such as e-mail, repositories, videoconferencing, etc.). This means that we, as teachers or faculty members, should be able to track students' behavior and activity based on a unique identity within all academic services and tools. Based on a comprehensive access tracking and log analysis, this would cause us to assess how students use the different resources and services in the learning process, helping to monitor it inside virtual classrooms, in order to better understand their difficulties and plan or provide adequate measures. Examples such as Moodog (Zhang et al., 2007), can be found concerning asynchronous learning supported by Content Management Systems.

Fourthly, although in a social Virtual World like Second Life having different accounts and avatars can be useful for a person (Lindsay et al., 2010), in an educational context that's not desired. This phenomenon of identity overlapping raises important legal and ethical questions in relation to users' rights and responsibilities in-world and ownership of avatars and their digital creations (Lindsay et al., 2010). From exploitation, to cyberbullying, sex, violence, and other problematic scenarios (Bugeja, 2007; LaChapelle, 2007), students and teachers don't have the guarantees of security and privacy that they need. It should be possible to identify who is related to a disruptive behavior. It's obvious that the concept of real privacy is still a utopia within Virtual Worlds, and on that point we agree with other researchers (Vilela et al., 2010; Freudenthaler, 2011), however this sense of accountability combined with access control promotes the compliance of rules and norms within an educational group or institution.

Fifthly, Virtual Worlds based on Second Life technology follow system and environment controls through Role Based Access Control (Allison et al., 2012), which, in turn, boil down to three categories: land related, content related, and group related. In each category there are different roles, permissions or privileges, and functions. It should be possible to delegate these roles automatically, based on the users' identity and context of the learning activity. For example, in a role play activity to simulate a refugee camp in the real world, students must follow the realistic mobility options such as walking, running or crawling. If they are given the opportunity to teleport or fly, "[...] they may not intuitively experience the time taken to resolve a dilemma situation [...]" (Perera et al., 2012). Other cases, in which some engagement functions can be an obstacle to learning, such as avatar customization or

chat conversation (Kluge & Riley, 2008; Cruz et al., 2013), it should be possible to block or prohibit students to do it. For instance, if a group of architecture students have to do a collaborative task of creating and constructing a 3D virtual space, it is not desirable that they be distracted from the main focus of the activity and start to edit their avatar's appearance. It means that they should only have access to the appropriate functions in order to complete the activity (e.g., voice, chat and build permissions).

Moreover, there are also accessibility issues related to educational scenarios in Virtual Worlds. It should be possible for the Virtual World to acknowledge if the student has any disability and adapt the 3D classroom environment for him/her (e.g., when a blind student logs in with his/her avatar in-world, the system might automatically teleport the student to the class or turn on the 'follow' mode connected to a colleague). Also, other students and the teacher should be aware of it. It means that if a blind student goes to a virtual class, a text-to-speech device ought to be available. Similarly, for deaf students, voice communication should only take place when a speech-into-text device is enabled. This already happens with some of the videoconferencing and Voice over IP (VoIP) technologies (e.g., Asterisk - http://zaf.github.io/asterisk-speech-recog/), where technology is flexible and capable to adapt to user's identity and attributes (e.g., automatic translate voice into chat for a deaf user).

Sixthly, Virtual Worlds are currently mostly isolated in restricted servers, managed by a single entity (Morgado, 2013), and there is no persistent identity that other places can detect and interact with (Clark-Casey, 2010). This may change and it should be possible to optimize the distributed learning environments and resources of different academic institutions, as well as currently happens with web-based services (Morgado, 2009). It means that if a teacher in United States has a 3D science lab in their OpenSimulator server, they should be able to give access to it to an European colleague, for use with his/her students - and also the contrary, seamlessly, without requiring creation of local identities (Hypergrid technology only provides this to a limited degree, as is mentioned below). This cooperation between institutions and staff promote a network of 3D open educational resources and spaces, with new scenarios for massive learning and research. It also promotes educational mobility across countries and cultures, that can be tracked and managed based on agreed policies, practices, standards and licenses, ensuring user's authenticity, reuse and authoring of the 3D learning objects - preventing situations like Copybot, a modified Second Life client that was able to copy illegally 3D contents (Hunt, 2007).

Finally, for research purposes, "[...] virtual worlds also add new ethical considerations to survey research. [...] identity in Second Life is fluid so ensuring respondent integrity is difficult." (Bell et al., 2009). Thus, if we are conducting research, in most cases we should and/or may be in our interest to know who exactly is beyond the avatar, in order to ensure the validity and reliability of the data that we are collecting - preventing biases. Moreover, the user should also know who the researcher leading the study is, in order to participate in an informed and coherent way.

Ongoing projects, such as Medulla (Fox et al., 2010) or Moonshot (Howlett & Hartman, 2010), are the proof that we are pointing to the right way by stating that identity federation is an enabler for the adoption of Virtual Worlds by the educational community, if correctly applied. On the one hand, the American project Medulla, created by the Federation of American Scientists (FAS), uses web Single Sign-On access control with Shibboleth and DSpace databases manager for identity management, team building, information sharing, project management, peer review, data versioning, data archiving, intellectual property management, and learning management in Virtual Worlds (Fox et al., 2010). This clearly shows us that we are already able to use federated identities standards to access Virtual Worlds, as well as ensure that the data and metadata related to user traceability, privacy, and authoring are interoperable within different Virtual Worlds technology. However, the Medulla team had only the concern of interconnection between Virtual Worlds, neglecting web-based systems such as learning management systems.

On the other hand, the European project Moonshot, from Janet-led in partnership with the GÉANT and other partners, aims to develop a single unifying technology for extending the benefits of SAML-based federated identity to a broad range of non-web services, including cloud infrastructures, high performance computing, grid infrastructures and other commonly deployed services including email, file store, remote access and instant messaging (Howlett & Hartman, 2010). Although the Moonshot did not focus on the same concern of Medulla, this ongoing project shows us that it should be possible to communicate between different technologies using federated identity (e.g., web-based with non-web-based).

Other efforts are already being developed, but far from support the identified problems within our scenarios. For example, Hypergrid - an architecture and protocol for securely decentralizing multiuser virtual environments, establishes an open federation of multiuser applications that can exchange user agents and assets, and can generally interoperate on several basic services. It supports the teleportation of user agents between Virtual Worlds in different administrative domains while preserving user identity, as well as the users' 3D virtual representation and connections to certain home-world services, as the users' inventory (Lopes, 2011). However, it only assures the interconnection of different grids or servers, and has several security, scalability and trustability problems (Clark-Casey, 2010).

Moreover, projects such as the aforementioned SLOODLE (Livingstone & Kemp, 2008), simply outline how it is possible to integrate Second Life Virtual World and Moodle. One of the most fundamental affordances of it is to pair Moodle users to their Virtual World avatars. When a user clicks on the Second Life registration booth, while logged in with their avatar, they are prompted to visit a Moodle registration page. This allows Moodle to verify the Second Life identity of the Moodle user, and this data is then stored in Moodle. Alternatively, a 'Login Zone' object in Second Life allows avatar registration to be driven from Moodle, followed by logging into Second Life. More similar efforts are found in the literature (Madeira et al., 2010).

Future directions

As our main goal, we have shown before a set of clear scenarios in which identity federation solutions can bring an added value, namely: classroom management, content reuse, learning analytics, accessibility, research, etc. On the one hand, identity federation can simplify the process of creation, management and monitoring of classes in 3D Virtual Worlds, by improving the usability, reducing the time and the administrative workload involved, and, in turn, the frustration and unpleasantness this may cause to educators. On the other hand, by ensuring private and secure access based on students' roles/attributes, identity federation can help somewhat to prevent surface learning, or even to guarantee the same rights and conditions to students' learning. Moreover, it can reduce and/or eliminate issues related to other technological challenges of Virtual Worlds, as cost or content production. If trust relations between institutions exist, within the use of Virtual Worlds, we are only one step behind the concept of 3D open education - by reusing shared resources and spaces, within institutional copyright policies and accountability terms.

However, the way we think and put the issue of federation must go beyond the interconnection between different Virtual Worlds using the same underlying technology (Lopes, 2011), or specific learning management systems (Livingstone & Kemp, 2008). We need to take e-learning, in a near future, as a unique shared service, independently from the platform or application in use (e.g., web or grid-based). We argue that the standardization of Virtual Worlds within themselves, without concerns of identity insurance, user traceability, privacy, accountability or interoperability with other non-virtual world systems can affect seriously the adoption of these for learning purposes. The path to interoperability and a seamless interaction between information systems, learning systems, third party applications and even devices, point out that the focus should be in the user, where the achievement and management of the correct identity is crucial to this success. The correct identity management of users, complemented with security and trust aspects, are intrinsic factors of identity federation standards, therefore should be taken into account into the technological development and standardization efforts of Virtual Worlds. As consequence of this, its adoption in academic or even non-academic learning spaces can be greatly enhanced.

We clearly need to interconnect digital identities with physical identities, thus creating a unique federated identity system that can act independently from the Virtual World in use. Instead of the need to adapt Virtual Worlds to the federation systems, we need an open agreement with basic federated and interoperable standards that should be capable to adapt within the broad range of available services on the Internet. This way, Virtual Worlds are able to scale and evolve independently within the different research areas, without compromising the users' identity. Our proposal remains on the convergence of the Medulla (Fox et al., 2010) and Moonshoot (Howlett & Hartman, 2010) federation efforts that can be achieved by the development of new technological solutions or readapting the current ones. As seen before, we know that many educational institutions worldwide have agreed to the adoption of the same policies, practices and standards that allow users' authentication and authorization while protecting their privacy. In this sense, we can straightforwardly reach and simplify the widespread adoption of Virtual Worlds by the educational community worldwide: implementing a unified solution for cross-compatible federations, that can not only federate and manage identities between 3D Virtual Worlds, but also within different systems and applications (independently from the platform in use).

Acknowledgements

References

Aas, B. (2011). What's real? Presence, personality and identity in the real and online virtual world. In N. Zagalo et al. (Eds.), *Virtual worlds and metaverse platforms: New communication and identity paradigms* (pp. 88-99). Hershey, PA: IGI Global.

Adrian, A. (2008). No one knows you are a dog: Identity and reputation in virtual worlds. *The Computer Law and Security Report*, *24*(4), 366-374.

Aguirre, S., Quemandaq, J., & Salvachúa, J. (2008). Work in progress - developing joint degrees through e-learning systems. *Proceedings of the 38th Annual Frontiers in Education Conference (FIE 2008)* (pp. F4D19-F4D20). Washington, DC: IEEE Computer Society. Retrieved September 11, 2013, from http://dx.doi.org/10.1109/FIE.2008.4720474

Ahmed, F., & Moskowitz, I. (2005). Composite signature based watermarking for fingerprint authentication. In A. Eskicioglu et al. (Eds.), *Proceedings of the 7th Workshop on Multimedia and Security* (pp. 137-142). New York, NY: ACM Press.

Allison, C., Campbell, A., Davies, C., Dow, L., Kennedy, S., McCaffery, J., Miller, A., Oliver, I., & Perera, G. (2012). Growing the use of virtual worlds in education: An opensim perspective. In M. Gardner et al. (Eds.), *Proceedings of the 2nd European Immersive Education Summit* (pp. 1-13). Paris, France: Universidad Carlos III de Madrid, Departamento de Ingeniería Telemática.

Alves, P., & Uhomoibhi, J. (2010). Issues of e-learning standards and identity management for mobility and collaboration in higher education. *Campus-Wide Information Systems, 27*(1), 79-90.

Anwar, M., Greer, J., & Brooks, C. (2006). Privacy enhanced personalization in e-learning. In G. Sprague et al. (Eds.), *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services (PST2006)* (pp. 1-4). New York, NY: ACM Press.

Anwar, M., & Greer, J. (2012). Facilitating trust in privacy-preserving e-learning environments. *IEEE Transactions on Learning Technologies*, 5(1), 62-73.

Bailie, J., & Jortberg, M. (2009). Online learner authentication: verifying the identity of online users. *Journal of Online Learning and Teaching, 5*(2), 230-238.

Barisch, M. (2009). Modelling the impact of virtual identities on communication infrastructures. In E. Bertino et al. (Eds.), *Proceedings of the 2009 5th Workshop on Digital Identity Management (DIM'09)* (pp. 45-52). New York, NY: ACM Press.

Baron, J., & Crooks, S. (2005). Academic integrity in web based distance education. *TechTrends, 49*(2), 40-45.

Bedford, W.,Gregg, J., & Clinton, S. (2009). Implementing technology to prevent online cheating: A case study at a small southern regional university (SSRU). *Journal of Online Learning and Teaching, 5*(2), 197-207.

Bell, M., Castronova, E., & Wagner, G. (2009). Surveying the virtual world: A large scale survey in second life using the virtual data collection interface (VDCI). *German Council for Social and Economic Data (RatSWD) Research Notes, 40.* Retrieved September 11, 2013, from http://dx.doi.org/10.2139/ssrn.1480254

Bhargav-Spantzel, A., Squicciarini, A., & Bertino, E. (2007). Trust negotiation in identity management. *IEEE Security & Privacy, 5*(2), 55-63.

Bhatti, R.,Bertino, E., & Ghafoor, A. (2007). An integrated approach to federated identity and privilege management in open systems. *Communications of the ACM, 50*(2), 81-87.

Boon, S., & Sinclair, C. (2009). A world I don't inhabit: Disquiet and identity in second life and facebook. *Educational Media International*, *46*(2), 99-110.

Bugeja, M. (2007, September). Second thoughts about second life. *The Chronicle of Higher Education.* Retrieved September 11, 2013. http://chronicle.com/article/Second-Thoughts-About-Second/46636

Burden, D. (2011). A semantic approach to virtual world standards. *IEEE Internet Computing, 15*(6), 40-43.

Clark-Casey, J. (2010). *Scaling opensimulator: An examination of possible architectures for an internet-scale virtual environment network* (Unpublished master's thesis). Oxford, England: University of Oxford. Retrieved September 7, 2013, from http://justincc.org/downloads/docs/justincc-dissertation.pdf

Clauβ, S., & Schiffner, S. (2006). Structuring anonymity metrics. In A. Juels et al. (Eds.), *Proceedings of the 2006 2nd ACM workshop on Digital Identity Management (DIM'06)*(pp. 55-62). New York, NY: ACM Press.

Cruz, G., Maia, A., Morgado, L., Fonseca, B., Paredes, H., Bessa, F., Rodrigues, C., & Martins, P. (2013). Designing user learning experience in virtual worlds: The young europeans for democracy serious application. In A. Rocha et al. (Eds.), *Advances in Information Systems and Technologies* (pp. 1117-1128). Berlin, Germany: Springer-Verlag.

Dalgarno, B., Lee, M., Carlson, L., Gregory, S., & Tynan, B. (2011). Institutional support for and barriers of the use of 3D immersive virtual worlds in higher education. In G. Williams et al. (Eds.), *Proceedings of the 2011 Ascilite Conference: Changing demands, changing directions* (pp. 316-330). Hobart, Australia: University of Tasmania.

European Commission Communications Networks, Content and Technology (2013). *eduGAIN service*. Retrieved September 11, 2013, from http://www.geant.net/service/eduGAIN/Pages/home.aspx

Fox, M., Kelly, H., & Patil, S. (2010). Medulla: A cyberinfrastructure-enabled framework for research, teaching, and learning with virtual worlds. In W. Bainbridge (Ed.), *Online Worlds: Convergence of the Real and the Virtual* (pp. 87–100). London, England: Springer-Verlag.

Freudenthaler, S. (2011). *Flexible learning settings in second life* (Unpublished master's thesis). Graz University of Technology, Graz, Austria.

Gabriels, K.; Bauwens, J., & Verstrynge, K. (2011). Second Life, second Morality? In N. Zagalo et al. (Eds.), *Virtual worlds and metaverse platforms: New communication and identity paradigms* (pp. 306-320). Hershey, PA: IGI Global.

Hammerle, L. (2006). SWITCHaai: Shibboleth-based federated identity management in switzerland. In G. Krčmařová, & P. Sojka (Eds.), *Proceedings of the 2006 1st CESNET Conference on Advanced Communications and Grids (CESNET 2006)*(pp. 1-12). Prague, Czech Republic: CESNET.

Hendaoui, A., Limayem, M., & Thompson, C. (2008). 3D Social virtual worlds: Research issues and challenges. *IEEE Internet Computing, 12*(1), 88-92.

Howlett, J., & Hartman, S. (2010, March). *Project moonshot*. Paper presented at the IETF 77 Meeting, Anaheim, CA. Retrieved October 11, 2013, from http://www.painless-security.com/wp/wp-content/uploads/2010/03/moonshot-ietf-77-briefing-paper.pdf

Hunt, K. (2007). This land is not your land: Second Life, copybot and the looking question of virtual property rights. *Texas Review of Entertainment & Sports Law, 9*(1)*,* 141-172.

InCommon (2013). *About incommon*. Retrieved September 11, 2013, from htps://www.incommonfederation.org/about.

Joyce, R., & Gupta, G. (1990). Identity authentication based on keystroke latencies. *Communications of the ACM, 33*(2), 168-176.

Junglas, I., Johnson, N., Steel, D., Abraham, D., & Louglin, P. (2007). Identity formation, learning styles and trust in virtual worlds. *The Database for Advances in Information Systems, 38*(4), 90-96.

Kallela, J. (2008). *Federated identity management solutions* (Technical report). Helsinki University of Technology, Helsinki, Finland. Retrieved October 10, 2013, from http://www.cse.hut.fi/en/publications/B/1/papers/Kallela_final.pdf

Kluge, S., & Riley, E. (2008). Teaching in virtual worlds: Opportunities and challenges. *Issues in Informing Science and Information Technology, 5*(1), 127–135.

LaChapelle, N. (2007, July 18). Some foundations for second life pedagogy. *Educause connect*. Retrieved September 10, 2013, from http://connect.educause.edu/blog/HiredEd/somefoundationsforse/44785

Lee, C., & Warren, M. (2007). Security issues within virtual worlds such as second life. In C. Valli, & A. Woodward (Eds.), *Proceedings of the 5th Australian Information Security Management Conference* (pp. 142-152). Perth, Australia: Edith Cowan University.

Linden, M. (2005). Organising federated identity in Finnish higher education. *Computational Methods in Science and Technology, 11*(2), 109-117.

Lindsay, D., Zwart, M., & Collins, F. (2010). My self, my avatar, my rights: Rights of avatar identity and integrity in virtual worlds. In D. Riha (Ed.), *Humanity in Cybernetic Environments* (pp 147-158). Oxford, England: Inter-Disciplinary Press.

Livingstone, D., & Kemp, J. (2008). Integrating web-based and 3D learning environments: Second life meets moodle. *European Journal for the Informatics Professional, 9*(3), 8-14.

Lopes, C. (2011). Hypergrid: Architecture and protocol for virtual world interoperability. *IEEE Internet Computing, 15*(5), 22-29.

Lorentz, P. (2011). Is there a virtual socialization by acting virtual identities?: Case study: The sims® . In N. Zagalo et al. (Eds.), *Virtual worlds and metaverse platforms: New communication and identity paradigms* (pp. 206-218). Hershey, PA: IGI Global.

Madeira, A., Sequeira, P., Morgado, L., & Gonzaga, L. (2010). Controlo da assiduidade em aulas efectuadas no second life. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *5*(1), 87-100.

Madsen, P., Koga, Y., & Takahashi, K. (2005). Federated identity management for protecting users from ID theft. In V. Atluri et al. (Eds.), *Proceedings of the 2005 1st Workshop on Digital Identity Management (DIM'05)* (pp. 77-83). New York, NY: ACM Press.

Messinger, P., Stroulia, E., Lyons, K., Bone, M., Niu, A., Smirnov, K., & Perelgut, S. (2009). Virtual worlds - past, present, and future: New directions in social computing. *Decision Support Systems, 47*(3), 204-228.

Morgado, L. (2009). Interconnecting virtual worlds. *Journal of Virtual Worlds Research, 3*(1), 4-7.

Morgado, L. (2013). Technology challenges of virtual worlds in education & training - research directions. In C. Gatzidis, & E. Anderson (Eds.), *Proceedings of the 2013 5th International Conference on Games and Virtual Worlds for Serious Applications (VS-GAMES 2013)* (pp. 1-5). Washington, DC: IEEE Computer Society.

Olt, M. (2009). Seven strategies for plagiarism-proofing discussion threads in online courses. *Journal of Online Learning and Teaching, 5*(2), 222-229.

Onashoga, A., Abayomi-Alli, A., & Ogunseye, T. (2014). Enhanced role based access control mechanism for electronic examination system. *International Journal of Computer Network and Information Security, 3*(1), 1-9.

Palomaki, E. (2009). *Applying 3D virtual worlds to higher education* (Unpublished master's thesis). Helsinki University of Technology, Helsinki, Finland. Retrieved September 7, 2013, from http://lib.tkk.fi/Dipl/2009/urn100120.pdf

Perera, I., Allison, C., Ajinomoh, O., & Miller, A. (2012). Managing 3D multi user learning environments - a case study on training disaster management. *International Journal of Emerging Technologies in Learning, 7*(3), 25-34.

Roberts, C., & Hai-Jew, S. (2009). Issues of academic integrity: An online course for students addressing academic dishonesty. *Journal of Online Learning and Teaching, 5*(2), 182-196.

Rowe, M. (2010). The credibility of digital identity information on the social web: A user study. In K. Tanaka et al. (Eds.), *Proceedings of the 4th Workshop on Information Credibility on the Web (WICOW'10)*(pp. 35-42). New York, NY: ACM Press.

Schwartz, M. (2010). Federated identity: A recipe for higher education. *Educause Quarterly, 33*(2). Retrieved from http://www.educause.edu/ero/article/federated-identity-recipe-higher-education

Shim, S., Bhalla, G., & Pendyala, V. (2005). Federated identity management. *Computer, 38*(12), 120-122.

Sloodle (2013). *Registration and enrolment*. Retrieved September 9, 2013, from https://www.sloodle.org/docs/Registration_and_Enrolment

Smith, D. (2008). The challenge of federated identity management. *Network Security, 2008*(4), 7-9.

Thompson, C. (2011). Next-Generation virtual worlds: Architecture, status, and directions. *IEEE Internet Computing, 15*(1), 60-65.

Vilela, A., Cardoso, M., Martins, D., Santos, A., Moreira, L., Paredes, H., Martins, P., & Morgado, L. (2010). Privacy challenges and methods for virtual classrooms in second life grid and opensimulator. In K. Debattista et al. (Eds.), *Proceedings of the 2010 2nd International Conference on Games and Virtual Worlds for Serious Applications (VS-GAMES 2010)* (pp. 167-174). Washington, DC: IEEE Computer Society.

Whitson, J. (2009). Identity theft and the challenges of caring for your virtual self. *Interactions, 16*(2), 41-45.

Windham, C. (2005). Father google and mother IM: Confessions of a net gen learner. *Educause Review, 40*(5), 42-59.

Zhang, H., Almeroth, K., Knight, A., Bulger, M., & Mayer, R. (2007). Moodog: Tracking students' online learning activities. In C. Montgomerie & J. Seale (Eds.), *Proceedings of the World Conference on Educational Multimedia, Hypermedia and Telecommunications (EdMedia 2007)* (pp. 4415-4422). Chesapeake, VA: AACE.