SUDI – Single Unified Digital Identity – A Unified Identity Life Cycle Management platform for HEI – UTAD Case Study

António Rio-Costa[1], Sílvio Capela[1], Alberto Vasconcelos[1], Frederico Branco[1], Elsa Justino[1,2]
[1] Universidade de Trás-os-Montes e Alto Douro UTAD, Quinta de Prados, 5001-801 Vila Real, Portugal, acosta@utad.pt; albertov@utad.pt; ejustino@utad.pt
[2] CAPP-Centro de Administração e Políticas Públicas da Universidade de Lisboa, Portugal.

Keywords
Identity Management, LDAP, Life Cycle Management, Machine Learning, Blockchain, Digital Identity

1. ABSTRACT

In a higher education institution, the user electronic information is usually scattered among various places and systems that provide services according to their requirements. The digital information contained in the various systems needs to be transversal to many digital identities, each one representing a user. This leads to several issues when managing the users' rights on the access to technological infrastructures and resources, mainly because users have different types of rights and restrictions according to their role in the institution.

Because of that problem, in 2007, the University of Trás-os-Montes e Alto Douro (UTAD) created an identity management system that became responsible for managment all digital identity information since creation to removal providing an Identity Management (IDM) solution, that it was at the time enough to respond to the University needs. Twelve years later the UTAD requirements, and in higher education intuitions in general, become more demanding, more mature gained importance in the information systems ecosystem. What led to a necessarily upgrade of the identity management infrastructure, to rethink and reengineer all the identity lifecycle management in the institution in the light of the best practices and standards.

The current paper, reports on an ongoing project that aims to improve the existing identity management system in UTAD and to present the basis of a proposal for a common Identity lifeclycle framework, under development, transversal to higher education institutions (HEIs) aligned with the identified best practices and standards.

2. PROJECT SCOPE

Besides the already existing identity management system at University of Trás-os-Montes e Alto Douro, the number of users and resources are growing, this requires to manage the access for each identity. The quest of this project is development of a general framework suitable to any higher education institution and implement it in the specific case of UTAD. The main objective of this framework is the definition of roles that incorporate all kinds of users (digital identities), working and accessing the system, in a higher institutions and associate them to each specifics rights and restrictions inside those same systems.

The current IDM system divides users in two groups, students and staff, this division bring issues to the institution because it not specifies the type of users inside each one of this groups and respective resources, what leads to issues like the need of system administrators to manually manage users associated resources. The framework, under development, has the goal to delivery an identity management platform based in higher education institutions generic identified roles and is being developed according to The International Organization for Standardization standard ISO 24760, 27001, the recent approved and implemented General Data Protection Regulation, respecting his private information policies, and based on the best practices currently available in this information technology area.

Another ambition of this solution is the utilization of the Blockchain concept in an IDM context. The combination of the decentralized blockchain principle and identity management, suggested that a

digital ID can be created for each digital identity to relate the respective user to all transactions carried out by him. This integration of the blockchain concept it will assure to the user the preservation of the "timeline" and it will create a history of interactions by that user.

3. TECHNICAL APPROACH

3.1. ISO 27001

The quantity of sensitive data in a higher education institution is countless, this type of organization not only contains individual personal information, like data related to employees and students, but also important organization data as financial information. So, this quantity of sensitive information leads to what is the most important point of an information security management system (ISMS) and that needs a large focus by any organizational entity that is the management of sensitive organizational information.

In order to achieve guaranteed security and integrity in an ISMS the International Organization for Standardization created the ISO 2700. The standard ISO 27001 is a specification written by the best specialists in security information which contains technical information about a methodology about how to build and implement an ISMS in an organization.

In this case scenario and in order to develop a trustworthy higher education institutional IDM framework, the attention given to this matter of work represents what should be a major target to ensure since the first product idea. By that, the implementation of the current project according with standard ISO 27001 evidence a special care with users' personal and sensitive information.

3.2. ISO 24760

One big problem when developing an information system is the definition of terms, concepts and ideas. The non-definition of this values could lead to a misunderstanding of communication, ideas and decrease the viability of the final application product. So, according to that and the current project achievement to deliver an identity management framework for higher education institutions, meaning an inclusion of a large and distinct groups of entities, the need of a universal definition of terms and concepts is an imperative requirement. The International Organization for Standardization, in order to create a universal guide containing all definitions related to identity management, developed the ISO 24760. The standard ISO 24760 specifies definitions, terms, concepts of identity, identity management and their relationships.

The most important part of an identity management platform are the users, since they represent a large and fundamental section of any organizational system. According to the standard ISO 24760, users represent an entity which can be a person, organization or another sub-system. As stated in the same standard, a user representation in a digital system or technological infrastructure is defined as a digital identity. A digital identity contains attributes and some of them, normally an pair "Username" and respective "Password", can be used as credentials to guarantee access to the information system, identifying that user to the system.

3.3. GENERAL DATA PROTECTION REGULATION (GDPR)

In the last years, the exponential evolution of the technological systems led to a global preoccupation about how the data contained in that systems could be protected against unauthorized access or it could be protected against illegal selling. In 2016, the European Union (EU) adopted the General Data Protection Regulation, making it one of the biggest achievements in recent years. The GDPR was created in order to replace the old and out of dated 1995 Data Protection Directive, which was been created in the internet childhood. So, it was given two years to all EU member states to ensure conditions of a complete implementation in their countries of the GDPR by May 2018.

The European Union's approved General Data Protection Regulation stipulates, as an overall, the protection of personal information as a fundamental right that should be guaranteed to any citizen. In the GDPR are specified all the rules that the organizations should necessarily obey in order to guarantee the secrecy of all sensitive and personal information existing in their systems and technological infrastructures.

3.4. PRIVACY IMPACT ASSESSMENT (PIA)

Privacy Impact Assessment (PIA) concept emerged in mid-1990s and his impact in Europe gained more visibilty with the implementation in all European Union (EU) member states of the General Data Protection Regulation (Art. 35 of the GDPR). The article 35 of the GDPR denominated "*Data protection impact assessment"* it's the first article of Section 3, "*Data protection impact assessment and prior consultation"*, and it refers to an obligation by the controller to conduct an impact assessment when the data processed by his system represent, in any circumstance, *"a high risk to the rights and freedoms of natural persons"* (Art. 35(3) of the GDPR).

In order to achieve a right approach in the assessment development, the article 35 of the GDPR specifies the minimum requirements that a PIA should contain to be valid and particular case scenarios where a PIA shall be necessarily required. In a more precise way, the Privacy Impact Assessment is an analysis, made by an organizational institution to his own processes, seeing how these processes can affect or compromise the privacy of individual's sensitive and personal data, before starting processing it.

3.5. INFORMATION SECURITY POLICY – BEST PRACTICES

The management of sensitive information represents a large responsibility to any information system. Based on importance given to that matter, institutions created best practice guides in order to reduce possible risks of data violation or identity theft. These available guides provide information guides with templates that can be used to achieve an information security policy for this project framework, combining legal requirements and current best practices.

The ongoing project, besides following the International Organization for Standardization's ISO 24760, 27001, follows the best practice guides available in this scientific area, ensuring a suitable working framework capable of being adopted by any individual higher education institution improving their identity management platform without compromising the information contained in it.

4. CURRENT IDENTITY LIFECYCLE SOLUTION

The University of Trás-os-Montes e Alto Douro technological infrastructure provides a set of information systems that have as a main goal the support of administrative procedures and guarantee a series of digital services to the users which led to the IDM issue approached in this paper and to the final product solution designed in order to solve the problem.

The existing information system of UTAD, besides having some weaknesses in the identity management technological area, have some strong points that deserve to be underlined in order to understand the current context and situation of this specific higher education institution. From the strong points should be approached the solid and mature information system, the UTAD has a relevant physical infrastructure that counts with many years of updates and implementations, this gives to the university a stable environment to develop, implement and test applications/solutions without technical preoccupations. Another major point that deserve special reference is that almost every UTAD services are available in web, meaning that the current staff as experience in working with web technologies.

The IDM system available at this moment at UTAD was developed to solve the digital identities problems at that moment and designed according to the needs of that time without following any best practice rules or preparation for future certification. The UTAD's current technological infrastructure and identity management system has the following overall architecture:

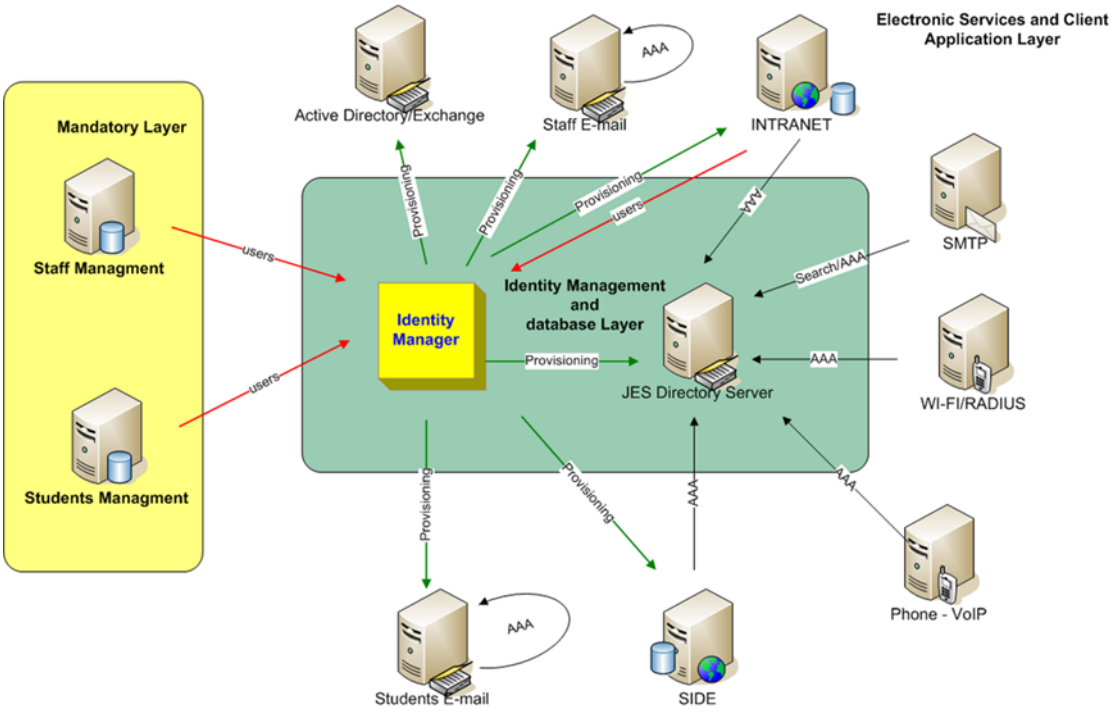

Figure 1- UTAD's current technological infrastructure and IDM system overall architecture

As seen in **Figure 2** the current identity management system isn't based in a roles management type, which means that to each digital identity (user) of the technological infrastructures the system administrator is responsible for managing user's permissions and resources what makes it non-flexible/agile for the constant needs and demands.

Another problem of the current identity management system is the non-definition of a lifecycle to each user, this means that there isn't any stipulation of when a digital identity can, or it should be denied access to University technological infrastructures. Besides the aim to cut out the need of many digital identities per user, this system didn't obliterate completely the problem, in fact, if a student becomes a collaborator with the university, which means a "Staff Member", it will need a second account that gives him access to the staff resources.

5. EXPECTED IDENTITY LIFECYCLE SOLUTION

The objective of the project in progress is the development of a framework that allows a single digital identity for all resources, thought and developed according to The International Organization for Standardization ISO 24760, 27001, respecting the recent privacy policies approved with de European Union General Data Protection Regulation and following the best practices currently available in this information technology area. The intended framework will also be capable of identifying unusual behaviors by users. In order to achieve that, it will be used machine learning technology, which will establish a standard conduct to each digital identity, according to his usual interactions. The main objective of including this technology is that it will help to identify possible attacks to the UTAD private information and users' identity theft attempt. Another technology that can be used to prevent identity theft or credentials corruption is the blockchain concept. So by that and the importance given by University of Trás-os-Montes e Alto Douro to the treatment of personal and sensitive data of users the expected identity lifecycle solution wants to be able of implementing the Blockchain concept, giving the user full control of his credentials and making available to him a personal historic which enables a complete "life report" of the digital identity, recording different interactions from that user to any system and specifying the types of interaction or transaction with historical data like related intervenient parts and date of interaction.

As seen in the previous chapter, the current system does not specify types of users (roles) besides the "Students" and "Staff" big roles. The intended of this project is an elaboration of generic and default roles, for each type of user of the UTAD technological infrastructure, which include all kind of possible users. A simple example of the need for this kind of IDM framework is a student that graduates and become teacher on the same university, by the usual procedure it will be created a new digital identity or manually modified the resources that the student, now as a teacher, can access on the technological infrastructures. This process makes what appear to be a simple transaction not efficient and take unnecessary time from both parts, student and University. The ongoing project is thought in order to simplify these tasks, in the same example, the digital identity is associated to a "student" role and when he becomes a teacher that role is simply changed to a "teacher" role, it will take no time for the user, he will keep the same credentials as before and all the resources associated to the "teacher" role will be available for him.

For development and implementation of the ongoing project it will be used Midpoint, Midpoint is an opensource Identity Management system that allows defining the organizational structure, which allows the definition of roles according to departments or groups and also allows the management of users, roles and resources. The existence of an opensource solution that allows the creation, development and implementation of the intended product like Midpoint, guarantees that there isn't no technological limitation for this project in a real case as intended.

6. CONCLUSIONS AND FUTURE WORK

The needs and requirements of higher education institutions today are growing exponential which makes it a matter of concern for the years to come. The higher education institutions today must make critical adjusts to the technological infrastructures available to satisfy not only the needs of a constantly growing and changing universe of users, which includes internal users of the system and external system users, but also in certification of that infrastructures ensuring a prospect future for them.

The main goal of the ongoing project is the development of an identity management framework based on nowadays higher education institutions requirements and shape it to the specific's necessities of the University of Trás-os-Montes e Alto Douro. This project represents an ambition to deliver a pioneer and certified framework, satisfying all the current standards in this area of technological information and identity management (ISO 24760, 27001), besides that it will follow and respect all current regulation concerning privacy and sensitive/personal information treatment (GDPR).In addition to that it will includes and follow the best practices available in the identity management and information privacy areas. Furthermore, new technological concepts like Blockchain or Machine Learning it will be used in order to give the framework the intended innovative character in protection and preservation of personal and sensitive users' digital information, being that the main current concerns in identity management systems.

By all that, the final project product it will be an innovating framework that can be easily shaped to individual higher education institutions, in this case scenario the University of Trás-os-Montes e Alto Douro, making it a long-term framework solution in the area of identity management and upgradable worthy for the years to come.

7. REFERENCES

GÉANT website (2010). *Information Security Policy - Best Practice Document*. Retrieved February 11, 2019, from: https://services.geant.net/sites/cbp/Knowledge_Base/Security/Documents/gn3-na3-t4-ufs126.pdf.

Evolveum website (2018). *Why is midPoint the Best Identity Management and Identity Governance platform?*. Retrieved February 12, 2019, from: https://evolveum.com/midpoint/

Oracle website (2018). *Best Practices for Identity and Access Management (IAM) in Oracle Cloud Infrastructure*. Retrieved February 14, 2019, from: https://cloud.oracle.com/iaas/whitepapers/best-practices-for-iam-on-oci.pdf.

EUR-Lex Access to European Union law website (2016). *Official Journal of the European Union*. Retrieved February 15, 2019 from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

International Organization for Standardization website (2011). *ISO/IEC 24760-1:2011(en) Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts*. Retrieved February 15, 2019 from: https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-1:v1:en

Forbes website (2018). *How Blockchain Can Solve Identity Management Problems*. Retrieved February 17, 2019, from: https://www.forbes.com/sites/forbestechcouncil/2018/07/27/how-blockchain-can-solve-identity-management-problems/#470a57ed13f5

Arsénio Reis, Glória Fraga, Jorge Godinho Santos, Jorge Borges, Fernando Rodrigues, António Costa, Luis Barbosa, João Barroso, José Bulas Cruz, (2006)," Providing services for students - a project report". EUNIS – (European University Information Sytems), Tartu.

Costa António, Reis Arsénio, Vasconcelos Alberto, Santos Jorge, Borges Jorge , Barroso João, Cruz Bulas(2007)," University of Trás-os-Montes e Alto Douro Digital Identity Management – Project Report", EUNIS – (European University Information Sytems) Grenoble.

Rio-Costa A., Reis A., Borges J., Vasconcelos A., Santos J , Barroso J., Bulas-Cruz J (2009). "Providing Lifetime Services to Students – The case of the University of Trás-os-Montes e Alt Douro", EUNIS – (European University Information Sytems), Santiago de Compostela.

Rio-Costa A., Borges J., Reis A., Gonçalves R., Barroso J., (2011). "Providing University Federated Services at UTAD – A Project Report", EUNIS – (European University Information Sytems), Dublin.

Rio-Costa A., Borges J., Reis A., Vasconcelos A., Gonçalves R., Barroso J., (2011). "The University of Trás-os-Montes and Alto Douro e-learning shared federated services - A project report", EUNIS – (European University Information Sytems), Dublin.

Rio-Costa A., Ramiro G. (2011), "Serviços Federados em B2B -Uma proposta de investigação", CISTI'2011 - 6ª Conferência Ibérica de Sistemas e Tecnologias de Informação, Chaves, Portugal.

Gonçalo Cruz, Antonio Costa, Paulo Martins, Ramiro Gonçalves, Joao Barroso (2013); "Federation technology and Virtual Worlds for Learning: Research trends and opportunities towards identity federation"- 5th International Conference on Games and Virtual Worlds for Serious Applications (VS-GAMES), VS-GAMES. IEEE.

Goncalo Cruz, Antonio Costa, Paulo Martins, Ramiro Gonçalves, Joao Barroso (2015); "Toward Educational Virtual Worlds: Should Identity Federation Be a Concern?", Educations Technology Society, volume 18.

Frederico Branco; José Martins ; Ramiro Gonçalves ; Jose Bessa; Antonio Costa (2015), "A Decision Support Platform for IT Infrastructure Management The University of Tras-os-Montes e Alto Douro Services of Information and Communications Case Study"- 10Th Iberian Conference on Information Systems and Technologies (CISTI), Iberian Conference on Information Systems and Technologies. IEEE.

Jose Bessa, Frederico Branco, Antonio Costa, Jose Martins, Ramiro Goncalves (2016). "A Multidimensional Information System Architecture Proposal for Management Support in Portuguese Higher Education The University of Tras-os-Montes and Alto Douro Case Study". 11TH IBERIAN CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGIES (CISTI), Iberian Conference on Information Systems and Technologies.

Jose Bessa, Frederico Branco, Antonio Rio Costa, Jose Martins,Ramiro Goncalves (2017). " Information Management Through a Multidimensional Information Systems Architecture: A University of Tras-os-Montes e Alto Douro Case Study". INTERNATIONAL JOURNAL OF TECHNOLOGY AND HUMAN INTERACTION.

8. AUTHORS' BIOGRAPHIES

António Costa – Is an ICT specialist at (UTAD), Vila Real, Portugal, and is responsible for the coordination the areas of core infrastructure and communications, computer security areas, datacentre, VoIP and communications networks. He collaborates in teaching on different degrees of computer courses, as well as in research, extension and development projects. Holds a degree in Electrical Engineering (specialization in Electronics, Instrumentation and Computation) and a post-graduate degree in engineering area. Currently, he is in the final research stage to complete the PhD

in Computer Sciences. He made several made courses or specializations which includes the Upper Course Director for Public Administration; Diploma of specialization of the Information Society for Public Administration, SIP Masterclasses, OpenStack and Data protection Security specialization.

Silvio Capela - Current attending the last year of the Information and Communication Technology course in University of Trás-os-Montes e Alto Douro (UTAD) where acquired competencies related to the Information Technologies (IT), Information Systems, Software Engineering, System Analysis and Networking and currently is researching in an Identity Management (IDM) Project in UTAD's ICT services and wants to acquire the master's degree in Computer Engineering in the next two years.

Alberto Vasconcelos - Senior network/Linux/security integrator/consultant working in UTAD with more than 20 years of experience. His specialties are Linux architectures/server security/database admin coupled with associated support services/automation and monitoring with a heavy use of open source software, and a strong inclination to mix network concepts with open source-based Unix technology.

Frederico Branco – Holds as PhD in Computer Science from the University of Trás-os-Montes and Alto Douro in 2014. He is an Assistant Professor at the University of Trás-os-Montes and Alto Douro. He has published 2 articles in specialized magazines and 8 papers in events proceedings. Received 3 awards and/or honors and currently coordinates 1 research project. He works in the areas of Engineering and Technology with emphasis on Information Systems and Technologies. In his professional activities he interacted with 13 collaborators in co-authorship of scientific works. is an Information Systems completed his Master from the University of Trás-os-Montes e Alto Douro (UTAD), Vila Real, Portugal. He is currently researching Information Systems Architectures and Network Communications aiming the to complete his PhD. Besides this, implements Business Intelligence (BI) and Self- Service BI solutions.

Elsa Justino – Holds a PhD in Social Work. The professional experience includes the positions held in the service commission as Vice-President of the Student Support Fund, Deputy Director General of the General Directorate of Higher Education and Head of the Office of the Secretary of State for Employment and Vocational Training. She is currently Administrator of the University of Trás-os-Montes and Alto Douro and of the Social Action Services. In the field of higher education he has regularly participated in studies, communications and scientific articles on students, social action and higher education.