EPiC Series in Computing

Volume 95, 2023, Pages 27–36

Proceedings of European University Information Systems Congress 2023

Using SaaS in a European University: Protect your Privacy and enjoy!

Georgios Roussos[1*], Dimos Charidimou[1†], Angeliki Agorogianni[1],

[1] IT Center - Aristotle University of Thessaloniki (AUTh), Greece

grou@it.auth.gr, dharidimou@it.auth.gr, aagorogi@it.auth.gr

Abstract

Using Software as a Service (SaaS) in a European university can provide many benefits, such as access to powerful tools and applications to enhance academic research and collaboration; however, it could always be a big challenge and a precarious situation. European law states that European universities are required to protect their privacy (personal & academic data, etc.), especially when using SaaS solutions. Choosing a SaaS provider isn't a simple process; it requires reviewing their privacy policies and much more (e.g., transparency about what data they collect, how they use it, and how long they retain it) to ensure compliance with General Data Protection Regulation (GDPR). This paper sheds light on Aristotle university's case, which could help universities to adopt improved methods to prevent unauthorized access or give the necessary access only to their data and protect their privacy, especially when using identity and access management (IAM) or access control solutions. By taking the above steps, European universities can enjoy the many benefits of SaaS solutions without worrying about GDPR issues but contrariwise focusing on their academic goals.

* https://orcid.org/0000-0003-2311-5196
† https://orcid.org/0000-0002-7602-3650

1 Introduction

Currently, educational methods are in a transitional state, with traditional tools giving way to entirely digitized ones driven by technological innovation (Roussos et al., 2023). European universities are increasingly adopting Software as a Service (SaaS) solutions to improve research and collaboration but must ensure compliance with the General Data Protection Regulation (GDPR) when using such services. One standard solution is Identity and Access Management (IAM) through single sign-on (SSO) access control, where employees or students can use one login for multiple applications. Security Assertion Markup Language (SAML) is a standard to securely exchange authentication and authorization information between parties, including the identity provider and service provider (Magnanini et al., 2022).

As SSO offers many benefits, organizations, and institutions often consider implementing it for SaaS applications. For example SSO helps maintain better SaaS security, as it may ensure more users adhere to password policies and make password recovery more efficient (Copeland et al., 2021). It also guides companies in observing access control requirements outlined in international standards like SOC2 or ISO27001. In response to the ever-growing need for robust and verifiable data security for sensitive research data, the IT Center of Aristotle University of Thessaloniki (AUTh) has achieved certifications like ISO 9001:2015[‡] and ISO/IEC 27001:2013[§] (Roussos et al., 2022).

This article will feature a noteworthy application of a previously established technique and delve into ways to maintain the security and compliance of university community data while utilizing SaaS. It will also put forward recommended measures for ensuring a completely secure data flow, including using SAML for data encryption to prevent unauthorized data access.

2 Ensuring Privacy and security when using SaaS – Why?

As data privacy concerns continue to mount, academic institutions must find ways to protect sensitive information without hindering academic progress (Roussos et al., 2022).

Ensuring the Privacy and security of personal and academic data is paramount for European universities. Not only is it a legal requirement under the GDPR, but it also helps to maintain the trust and confidence of students, staff, and other stakeholders in the university.

With the increasing use of cloud-based software-as-a-service solutions in academia, universities must take extra precautions to safeguard their data against unauthorized access, theft, and misuse (Sheik & Muniyandi, 2023). The consequences of failing to protect personal and academic data can be severe, both legally and reputationally. In addition to financial penalties, a data breach can damage a university's reputation and erode the trust of its stakeholders, including students, staff, and donors. This can lead to a loss of funding and a decline in European programs, among other adverse outcomes (Kaiser et al., 2022)

In light of these risks, European universities must take data protection seriously and implement robust measures to safeguard their personal and academic data. This includes carefully reviewing the privacy policies of any SaaS providers and ensuring that they meet GDPR requirements for data protection. By doing so, universities can protect their data from unauthorized access, maintain compliance with relevant regulations, and build trust with their stakeholders while enjoying the many benefits of using SaaS solutions to enhance academic research and collaboration.

[‡] ISO 9001:2015 - Quality management systems - Requirements
[§] ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements

2.1 The GDPR and SaaS Compliance

The GDPR is a set of privacy regulations that all businesses and organizations like European universities, must comply with when using SaaS solutions. Under the GDPR, SaaS providers must follow strict guidelines about collecting, using, and retaining personal data. They must also provide transparent information about their privacy policies and how they protect user data (Kaiser et al., 2022).

When choosing a SaaS provider, universities must review their privacy policies carefully to ensure compliance with the GDPR.It is crucial to have clear answers for at least three questions:

- what data the SaaS provider collects or states that it is important to collect,
- how they use it, and
- how long they retain it.

Additionally, European universities should investigate the measures that the SaaS provider has in place to protect data privacy and prevent data breaches.

2.2 SSO & SaaS – The process

As mentioned, an SSO system is a system that integrates several application login windows into a single one. SSO allows users to access all of their SaaS apps from a single page by inputting their login credentials (username, password, etc.) (Seta et al., 2019). SSO works on a trust relationship between an application service provider (SP) and an identity provider (IDP). When a user initiates a sign-in attempt to a SP from an IDP, the SP generates a SAML request, which is transmitted to the IDP. The IDP interprets the request based on its configuration settings. The relevant attributes are then mapped to the corresponding user attributes within the IDP. The IDP returns the response, including the mapped attributes, to the SP for verification. If the data is confirmed authentic, the user can access the SP.

2.3 SSO & SaaS - Benefits for Universities

Implementing Single Sign-On (SSO) would offer several advantages for universities with a large student body. Firstly, it would simplify the login process by allowing students to use a single set of credentials to access multiple applications and services (Magnanini et al., 2022). This would reduce the workload on IT staff, who would no longer have to manage multiple accounts for each student. SSO also enhances security by reducing the chances of weak password reuse while enabling more robust authentication measures, such as two-factor authentication, without adding user complexity. In addition, SSO grants better control over user access to applications and services, allowing organizations to manage permissions at a granular level, add or remove users quickly, and prevent unauthorized access, thereby streamlining access management processes.

However, SaaS providers may require clients, such as universities, to provide full or more user profile data than necessary. Therefore, it is essential for universities to be aware of SSO's fundamental limitations and threats, especially when using SaaS

2.4 SSO & SaaS Limitation & Threats

Despite the benefits, there are some limitations that a European university have to consider, limitations and threats including potential security vulnerabilities.

These limitations and threats are not specific to European universities and are common to any organization implementing SSO, especially with SaaS solutions. One of the primary risks is that SaaS providers may require more data than necessary, which increases the risk of data breaches. Additionally, a compromised SaaS provider could result in a widespread data breach, exposing data of multiple clients. To mitigate these risks, it is crucial for organizations to carefully assess SaaS providers' security

protocols, review and limit data access, and use encryption technologies like SAML for secure data transfer.

While SSO offers numerous advantages , European universities must also consider potential security vulnerabilities (Kumar & Goyal, 2019). One significant limitation of SSO is the high level of trust placed in both the IDP and the SPs involved. Compromising the university's IDP would provide an attacker with access to all SPs connected to the SSO system. Similarly, compromising one of the SPs could give an attacker access to all other SPs in the system. Phishing attacks also pose a threat, with attackers creating fake login pages for the university's IDP or SP to capture user credentials for accessing other SPs. Session hijacking is another attack vector, whereby an attacker intercepts a user's SSO session and takes over their access to various SPs (Copeland et al., 2021) (Westers et al., 2023). These types of attacks can be challenging to detect and prevent, especially if the attacker employs sophisticated methods. How the IT Center of AUTh managed to overcome those issues?

3 A Case Study: Aristotle University of Thessaloniki & Zoom as SaaS

Aristotle University, located in Thessaloniki, Greece, is an example of a European University that has implemented effective measures to protect its data privacy when using SaaS solutions. From the period of the Covid-19 pandemic (Kalfa et al., 2021), AUTh turned to Zoom[**] as an extra SaaS solution to support online or hybrid learning for the academic community.

3.1 The Background – Challenges

The IT Center of AUTh faced a significant challenge in protecting sensitive data, such as emails, usernames, and passwords, from being compromised, as universities and SaaS providers like Zoom are prime targets for hackers (Wilson & Hingnikar, 2023). To comply with GDPR, AUTh had to prohibit the transmission of this data to unknown data centers worldwide, which posed a challenge in using Zoom as a SaaS solution.

The IT Center of AUTh worked to find a solution that allowed them to use Zoom while still maintaining the security and privacy of sensitive data[††]. This required a careful evaluation of Zoom's security protocols and the implementation of additional security measures, including the use of SSO with SAML and encryption technologies to secure data transfer (Westers et al., 2023). Despite the challenges, the IT Center of AUTh's solution proved successful, and their case is now considered a unique example of how universities can safely and effectively use SaaS solutions while complying with GDPR.

3.2 The Solution – Best Practices

The IT Center of AUTh tried a lot of advanced settings based on SAML Response Mapping configuration to finally ensure compliance with GDPR while using Zoom as a SaaS solution.

Finally the adopted configuration (Figure 1 – An improved process on SAML Communication (university IDP & SaaS SP) allowed only the user's name or surname to be read and stored by Zoom, while all other data was encrypted and hashed using values that made no sense, such as hashed email addresses for each user. The SAML Response Mapping configuration between the Identity Provider and the Service Provider was set up only to allow necessary values to be transferred and no additional

[**] Except Zoom, AUTh use various cloud service providers like Amazon, Google, Microsoft etc. As Zoom alternative, except Google Meet, Microsoft Teams etc, AUTh use the BigBlueButton (BBB) which is running on-premises using the SSO method.

[††] Specifically, those data regard credentials and personal data of 54.720 active users.

information. Currently, IT Center of AUTh applies this improved process to all SaaS providers and as always our goal is the slogan: "Let's digital transform our EUni[‡‡] by keeping data privacy and security first.", also, “First protect, then enjoy!”.

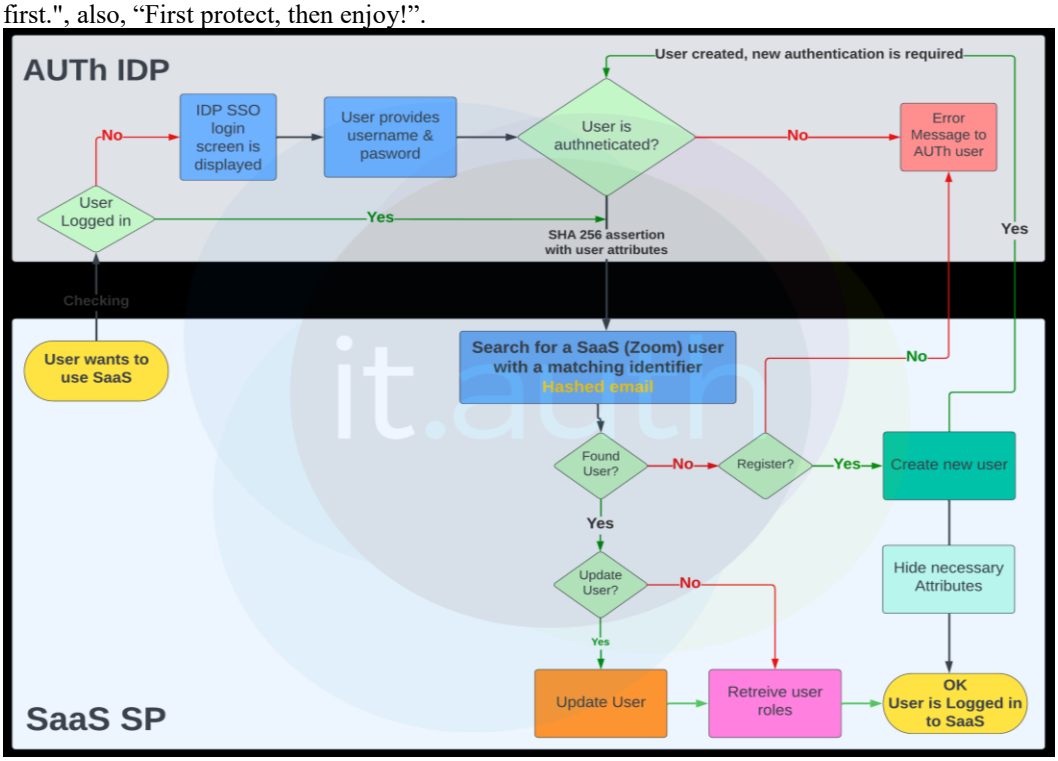

Figure 1 – An improved process on SAML Communication (university IDP & SaaS SP)

After implementing the security measures mentioned by controlling IdP’s attributes, Zoom only collects and stores the first name, last name, and a long-length hashed email address with the prefix "authgr_" in their Data Center worldwide. The hashed email address adds an extra layer of security, as it makes it more difficult for an attacker to retrieve the original email address from the stored data. (Figure 2)

[‡‡] EUni: European University

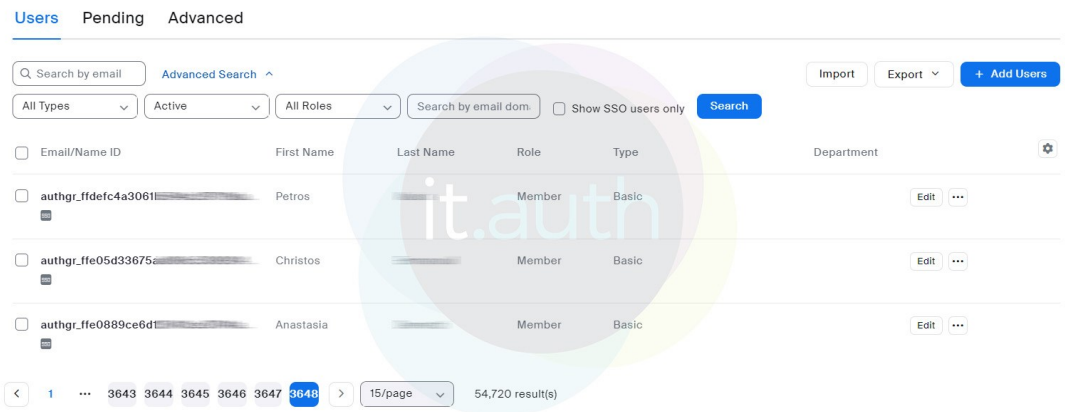

Figure 2 - 54.720 Hashed emails (not reals email addresses) on Zoom Dashboard.

This approach ensured that academic, and personal data remained securely stored within AUTh's data centers and was not shared with Zoom or any third party. It also protects user emails from spamming and passwords or usernames from potential leakage.

In this case, AUTh enjoys Privacy and GDPR compliance. But is there any additional proof of tansfered and stored data? The following figure (Figure 3) shows the SAML Response Logs having succeeded in responding and next figure (Figure 4) a view in detail.

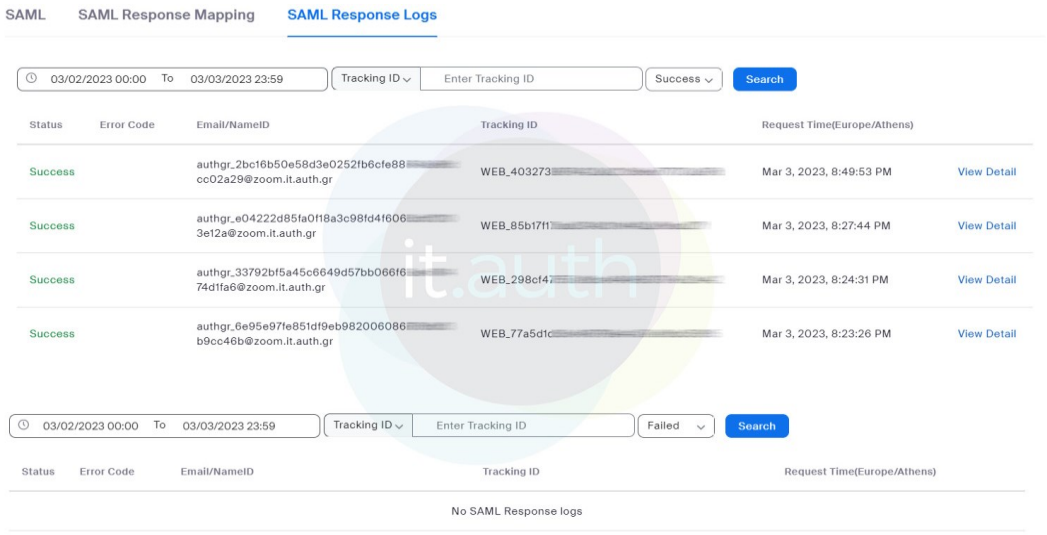

Figure 3 - SSO, SAML Response Logs - AUTh & SaaS Zoom

Figure 4 - SSO, SAML Response Logs, View Sing-in Log in Detail - AUTh & SaaS Zoom

3.3 Additional steps – Protecting data when combining SaaS and On-premise services (Zoom & Moodle)

Aristotle University uses Zoom as SaaS and Moodle LMS platform as an on-premise service to cover the needs of approximately 50k active students and academic staff. To safeguard user privacy, users typically receive different anonymized identities from the OAuth IdP when using multiple Service Providers. However, Zoom and Moodle needed a common identifier to enable internal AUTh Moodle to utilize SaaS Zoom functionalities. Due to the specific Zoom and Moodle code requirements, this identifier must be in the form of an email address.

As a result, we had to modify our IdP to generate a custom "*authZoomId*" attribute resembling an email address, which would be released to both Zoom and Moodle Service Providers. Conversely, Moodle[§§] is always informed of the same user's anonymized identity in Zoom. This allows it to utilize Zoom features for the benefit of the user and the instructor, such as scheduling and managing meetings on behalf of the user, without sharing any Moodle identity data (like Moodle Id or email addresses) with Zoom (Table1)

SP	IdP	Username	Email Attribute	Crafted released attribute for Zoom
Zoom	https://login.auth.gr	-	-	authgr_gabcdef86ff2fc0fa5eddc9420e035c3b28146528@zoom.it.auth.gr
AUTh Moodle	https://login.auth.gr	grou	grou@it.auth.gr	authgr_gabcdef86ff2fc0fa5eddc9420e035c3b28146528@zoom.it.auth.gr

[§§] Through LTI Pro, a Zoom app that integrates Zoom Video Conferencing into learning management systems (LMS).

Table 1 – Attributes shared during sign-in

Below is the code (Table2) demonstrating the synthesis of the crafted anonymized email identifier, which is always prepended with the "*authgr_*" prefix and appended with the "*@zoom.it.auth.gr*" suffix.

```
authZoomId = "authgr_" + sha1(someLocalIdpSecret, IdPname, SPname, uid) + "@zoom.it.auth.gr"
```

Table 2 – Applied custom code to anonymize the identity

This approach ensures a consistent, email-like identifier for both Moodle and Zoom while maintaining user privacy[***] (LTI Pro Application, n.d.).

At this point, it is crucial to understand that no security system is 100% secure (Copeland et al., 2021), even with measures like those taken by the IT Center of AUTh to protect sensitive data. Organizations need to continuously evaluate their security measures and stay vigilant against new threats and vulnerabilities. Users should also be educated about best practices for maintaining security and privacy, including using strong passwords and enabling two-factor authentication.

In addition to the measures already mentioned, AUTh's IT Center has implemented automatic logout after a certain period to prevent unauthorized access to sensitive data and systems. The system also recognizes suspicious IPs quickly to provide an additional layer of protection (Roussos et al., 2022). Using encrypted assertions with hash algorithms like MD5 or better SHA-256 can also verify message integrity and further enhance security (Suruse et al.)

Overall, a multi-layered approach that combines technical solutions with user education and awareness is essential to maintaining the security and privacy of university data when using SaaS solutions like Zoom. European universities should focus on building digital and secure environments that are GDPR-compliant while providing a seamless user experience. Implementing SaaS applications while keeping the Privacy and security of the academic community data intact is a challenge that requires adopting best practices.

4 Discussion

Digital transformation has become essential for European universities to keep up with the constantly evolving technological landscape. However, using Software as a Service (SaaS) applications in universities can pose significant data protection and privacy concerns.

The case of AUTh highlights the importance of balancing the benefits of SaaS solutions like Zoom with the need to protect sensitive data and comply with data privacy regulations. By implementing strong security measures and continually evaluating and improving their approach, universities and other organizations can leverage the power of SaaS solutions while keeping their data secure. In practice, universities must ensure their SaaS providers meet the highest data protection standards while providing a user-friendly interface. This includes adopting a privacy-first approach while implementing SaaS applications to avoid data breaches or privacy violations. Protecting personal data and compliance with GDPR is a top priority for all European universities, like Aristotle university.

5 References / Citations

[***] AUTh, by maintaining security at a high level and being the only case of an educational institution worldwide that asked for specific security criteria, pushed and helped Zoom developing team to find a way to apply the necessary changes and improvements so that the LTI Pro application meets the required standards concerning security needs.

Copeland, M., Jacobs, M., Copeland, M., & Jacobs, M. (2021). Reduce Cyber Security Vulnerabilities: Identity Layer. Cyber Security on Azure: An IT Professional's Guide to Microsoft Azure Security. 3–35. Retrieved from https://ebin.pub/cyber-security-on-azure-an-it-professionals-guide-to-microsoft-azure-security-2nd-ed-9781484265307-9781484265314.html

Kaiser, T., Siddiqua, R., Hasan, M., & Uddin, M. (2022). *A multi-layer security system for data access control, authentication, and authorization (Doctoral dissertation).*

Kalfa, V., Roussos, G., Charidimou, D., & Agorogianni, A. (2021). Coping with the COVID-19 challenges in a comprehensive university: learning tools and procedures adopted by Aristotle University of Thessaloniki. *EPiC Series in Computing.* EasyChair. https://doi.org/10.29007/hhvq

Kumar, R., & Goyal, R. (2019, August). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *33*, pp. 1–48. https://doi.org/10.1016/j.cosrev.2019.05.002

LTI Pro Application. (n.d.). Retrieved from Zoom App Marketplace: https://marketplace.zoom.us/apps/f8JUB3eeQv2lXsjKq5B2FA

Magnanini, F., Ferretti, L., & Colajanni, M. (2022). Flexible and Survivable Single Sign-On. In *Cyberspace Safety and Security* (pp. 182–197). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-94029-4_13

Roussos, G., Aliprantis, J., Alexandridis, G., & Caridakis, G. (2023). Augmented Reality in Primary Education: Adopting the New Normal in Learning by Easily Using AR-Based Android Applications. *Proceedings of the 26th Pan-Hellenic Conference on Informatics* (pp. 347–354). New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3575879.3576016

Roussos, G., Charidimou, D., Kalfa, V., Petalotis, A., & Agorogianni, A. (2022). Deliver knowledge in a Digital World: Successfully Livestream In-Person, Virtual or Hybrid large-scale educational events - Challenges and best practices. *European Journal of Higher Education IT*. Retrieved from https://www.eunis.org/erai/2022-1/

Seta, H., Wati, T., & Kusuma, I. C. (2019, October). Implement time based one time password and secure hash algorithm 1 for security of website Login authentication. *2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS).* Jakarta: IEEE. https://doi.org/10.1109/icimcis48181.2019.8985196

Sheik, S. A., & Muniyandi, A. P. (2023, December). Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review. *Cyber Security and Applications, 1*, 100002. https://doi.org/10.1016/j.csa.2022.100002

Suruse, A., Udmale, S., Doifode, V., & Waghade, A. (n.d.). *Applying a Single Sign-On Algorithm Based On Cloud Computing Concepts for SaaS Applications Using MD5 Encryption.*

Westers, M., Wich, T., Jannett, L., Mladenov, V., Mainka, C., & Mayer, A. (2023, February). SSO-monitor: Fully-automatic large-scale landscape, security, and privacy analyses of single Sign-on in the wild. https://doi.org/arxiv-2302.01024

Wilson, Y., & Hingnikar, A. (2023). Using modern identity to build applications. In *Solving Identity Management in Modern Applications* (pp. 171–197). Berkeley, CA: Apress. Retrieved from https://link.springer.com/book/10.1007/978-1-4842-5095-2

Author Biographies

Georgios Roussos is the IT System Administrator, AV Project Manager, and Zoom expert at the Academic Technology Support Office within the Digital Learning and Support Department of the Information Technology Centre (ICT) at Aristotle University of Thessaloniki (AUTh). He holds a Bachelor's degree in Informatics and Computer Technology, as well as two Master's degrees in Communication Networks and Systems Security and Intelligent Information Systems. Georgios is responsible for overseeing AV, Video Conferencing, Web Conferencing, and Live Streaming operations, as well as coordinating the university's relevant initiatives. His research interests encompass sustainable e-learning technologies, AR/VR/MR/XR technologies, wireless technologies, and information security. Since 2014, Georgios has been an active member of the Google Developers Group (GDG).

Dimos Charidimou is the Head of the Academic Technology Support Office at Digital Learning and Support Department of Information Technology Centre (ICT) of Aristotle University of Thessaloniki (AUTh), one of the biggest educational institutions in Greece. He is engaged in a wide range of issues in the field of image-audio and eLearning technologies. He has experience in the fields of videoconference services, live event broadcasting and eLearning administration. He graduated from the Department of Electronic Engineering at Alexandreio Technological Educational Institute of Thessaloniki. He holds a Master's Degree in ICT in education and a Master's Degree in Education Administration and Management. He is also a PhD candidate. His main research field is in synchronous / asynchronous distance eLearning services and platforms.

Angeliki Agorogianni is the Vice Technical Manager for Services at the IT Center of Aristotle University of Thessaloniki and the IT Center's Quality Assurance Manager. She leads a team of more than 30 members to deliver end- user services and support effectively in a high-pressure IT environment for a wide range of IT services acting mainly as user representative. She has a vast experience in the field of synchronous and asynchronous distance learning, planning and implementing solutions for Aristotle University for over a decade. She graduated from the Department of Electrical Engineering (integrated master) at Aristotle University of Thessaloniki, Greece. She holds a Master's Degree in Business Administration from the University of Macedonia, Greece. She is also involved in various European Organizations (EPICUR, EUNIS) in the field of eLearning and IT benchmarking.