LESSONS LEARNED FROM THE DEPLOYMENT OF A STUDENT/INSTRUCTOR INFORMATION SYSTEM IN ARISTOTLE UNIVERSITY OF THESSALONIKI

Ioannis Salmatzidis[1], George Pangalos[2]

[1] Information Technology Center (ITC), Aristotle University of Thessaloniki, P.O. Box 888, Thessaloniki 54124, Greece, jsal@auth.gr – [2] School of Technology, Aristotle University of Thessaloniki, Thessaloniki 54124, Greece, pangalos@auth.gr

Keywords
Student Information Systems (SIS), system architecture, web services, Single-Sign-On (SSO), PKI, student smart cards (SC), Hardware Security Modules (HSMs).

1. EXECUTIVE SUMMARY

Aristotle University of Thessaloniki (AUTH) is the largest Greek university with 86,000 undergraduate and 9,000 postgraduate students. In order to support student services, disparate, non-homogeneous IT systems were established during the past with no campus-wide coordination in mind.

1.1. Background

In 2005 Aristotle University considered the deployment of a SIS solution in order to harmonize and consolidate its distributed campus operations. The AUTH IT Center elaborated a strategic plan which identified the groups of stakeholders, the needs of each identified group and the project objectives.

1.2. Alternatives

The AUTH IT Center evaluated in consultation with the affected users the pros/cons and risks regarding 3 alternatives, namely the use of commercial SIS software, the in-house development and the adoption of some community Open Source SIS. AUTH opted for a mixture of the first two. Objectives suggested the need of a standards based, modular architecture that would allow a commercial SIS to work with the existing infrastructure and also allow in-house developed applications to be used in place or on top of vendor modules, by making use of web-services with no additional loyalties. The security framework had to be established with internal resources so that vendor applications could focus on business requirements. All users own a single account across applications, the same used in PC labs, or central computing facilities, based on pubcookie SSO and openLDAP. Students are offered typical SIS services (records, course registration, transcript requests) over SSL, with no requirements on soft/hard X.509 certificates, trying to keep things easy for them. In contrast, instructor services require HSMs that establish openVPN connections. Through the portal instructors are offered typical SIS services and may also submit digitally signed grades.

1.3. Conclusions

Both quantitative indicators (number of users, served transactions, portal visits) and qualitative instruments reflected positive user acceptance. The services are used currently by more than 30% of students and 20% of instructors. Evaluation figures are promising, but there is still a long way ahead towards global acceptance. Among lessons learned we should stress the underestimated migration issues, time and cost-wise. Students and instructors involved were quite enthusiastic and receptive, whereas a large number of admin staff expressed the typical resistance to change. Constantly along the course of the project we reconsidered business processes, in an effort to keep them simple. Security is still perceived by some users as complexity. But on the whole, the consolidated SIS services really revolutionized operations and gave a boost to similar ICT services across campus.

2. BACKGROUND

Aristotle University of Thessaloniki (AUTH) is the largest Greek university with 86,000 undergraduate and 9,000 postgraduate students. It comprises 42 departments organized in 9 faculties. AUTH, among other universities, requires effective Student Information Systems (SIS) to manage its academic operations such as course management, student records, student and teaching administrative processes, etc. Even though budget and technical resources are limited, while stakeholders' objectives are sometimes contradictory to each other, IT Centers need to be responsive to these needs, since students and faculty are the key resource in the learning chain. Administrative staff plays also an important role towards higher productivity in universities.

During the 90s the 1st generation of SIS in AUTH were usually limited at departmental level. Paper forms were in decline. However student records where only available on-line in the local LAN. Around year 2000 2nd generation SIS implemented core business processes but still processes didn't cross departments or faculties. Currently, students and teachers perceive on-line SIS services fundamental to learning, teaching and research.

2.1. The situation before

In recent years disparate, non-homogeneous IT systems were established in AUTH, with no campus-wide coordination in mind, not to mention interoperability with external eGovernment applications. Departmental registration offices scattered across or off-campus made their own choices and put individual effort to support local systems for student and faculty information services. Investments were fragmented, taking place in different periods under different specifications. Moreover, departments signed out-of-sync dissimilar annual support contracts. In the meantime user expectations for on-line services kept increasing, while enhancements and modifications were in constant need. Even though a common commercial SIS software was used by more than two thirds of the departments, different versions and configurations rendered the support of this infrastructure complicated and expensive. A fraction of needed SIS procedures were available online for some departments.

In 2003 the Information technology Center (ITC) received an order from upper management to establish a single annual support contract covering all faculties and departments in a voluntary basis. It was then thought that a single contract may offer economy of scale. As one might guess, this turned out as a quite successful scenario and in a 3 years time only 4 departments had been left out of the common annual support contract.

But this was not enough. The gaps and disparities between departmental processes had not been tackled yet. As a result, it was practically impossible to provide modern e-services and a smooth transition to an e-University environment. Since ITC got involved with the support of SIS along with the rest educational IT infrastructure, it had to initiate its own planning in order to enhance its internal productivity. The Center elaborated a strategic plan which identified:

- The groups of stakeholders
- The user needs of each identified group and the university's objectives
- The alternative actions to achieve the wished results
- The evaluation of the alternatives and the risks involved.

The groups of potential users were undergraduate, graduate, PhD and exchange programs students, alumni, faculty teachers, administrative staff, system administrators at faculty node level, central ITC administrators, external users e.g. applicants and Publishing Houses involved in study material distribution.

2.2. General project objectives and vision

A broad set of objectives per affected group was necessary to ensure that the new consolidated (at the faculty level) SIS delivers potential benefits. The objectives intended to achieve the following:

1. Meet the requirements of all end users and most particularly the ones identified by students and teachers, with regard to usability and ease of use

2. Support diverse educational models in order to cover all departments of AUTH and a wide range of academic activities
3. Handle a wide range of academic business processes, especially those that require central coordination or those that cross departments
4. Homogenize business processes and apply simplification as needed in order to minimize technical support and maintenance effort
5. Avoid implementing business processes directly into source code so that changes are easier and more efficient
6. Ensure interoperability with other in-campus systems such as elearning and in-house developed systems/modules, or even eGovernment services off-campus
7. Follow standardized and proven technologies whenever feasible
8. Opt for modular and scalable SIS software in order to easily add new functionality and meet future needs with low incremental costs.

2.3. The recorded user needs

The user needs of each identified group are predominantly relevant to end-user simplicity. The web interface should be simple and self-explanatory. Training to use the interface shouldn't be necessary for the majority of students and faculty. On the other hand administrative staff has more complicated tasks to perform, thus training is inevitable but simplicity is still essential. As far as privacy is concerned, the absolutely minimal personal information should be collected to complete a transaction.

In terms of user accessibility requirements, the content should be accessed and understood by as many people as possible without discrimination. Under the project funding terms, all official websites of EU institutions should follow international guidelines for accessible web content. The guidelines to be followed are the Web Content Accessibility (WCAG) guidelines (ver. 1.0) issued by the World Wide Web Consortium (W3C) as part of the Web accessibility initiative. Applying the principles of W3C/WAI was considered particularly important for the on-line user interface to be developed.

2.4. Technical architecture requirements

Additionally to the general project objectives and user needs, the IT Center came up with a list of technical, lower level requirements that support the accomplishment of the abstracted needs:

1. Ensure that the SIS to be established is hardware technology agnostic
2. Achieve economy of scale and maintenance simplification by consolidating infrastructure from the departmental level to the faculty level, (e.g. Faculty of Engineering node, Faculty of Philosophy node, etc.), or even better, achieve a completely centralized system
3. Upgrade the old departmental databases (OMNIS) to ANSI SQL compliant ones
4. Establish a primary key which uniquely identifies all students (student registration number)
5. Deploy a fault tolerant and reliable architecture. System failures in a faculty node shouldn't affect operations of all other nodes
6. Prefer web services since they are simple and platform neutral. This directly implies the employment of SOAP, WSDL and above all, XML. Standards compliance is a key issue in order to achieve interoperability with the existing university infrastructure or future augmentation
7. Access is only permissible to authorized users. Certificate authentication should be employed for critical processes
8. Separate Identity Management from core SIS. Authentication and authorization functions in individual applications shouldn't be duplicated. Aristotle University happens to have an existing framework, namely OpenLDAP (www.openldap.org) and Pubcookie (www.pubcookie.org) and SIS is required to interoperate with. In terms of federation support, Shibboleth is currently under consideration (but not during project implementation)

9. Achieve confidentiality by ensuring that data exchanged between user and system are not read by unauthorized persons
10. Secure sensitive data by ensuring that data exchanged between user and system are not modified by third person (integrity). Sensitive data such as grades and graduation announcements should be hashed. Modifications to sensitive data destroy original hashes and should trigger alerts
11. Implement non-repudiation by ensuring that a user, e.g. staff or a faculty member, can not deny at a later date, a committed data submission
12. Ensure that every user is responsible for operations performed. This can be achieved by logging of operations performed, along with time, location (IP address) of transactions (accountability).

Since this was an IT project, the ITC got this excellent opportunity and suggested that the project had to go beyond serving pure Registration/Administration issues. The SIS had to be integrated with other similar university IT services e.g. IT services that the Center already provides to end-users.

2.5. Security concerns

Security is an upfront design parameter rather than a delayed addition. However, traditional security challenges are more complicated within a distributed architecture. Of paramount importance is the fact that the level of security and availability of the new distributed environment should be similar, if not higher than the level provided by the previous fragmented infrastructure. Having said that, it becomes necessary to restrict the interactions that users and applications may carry out with the central infrastructure or neighbouring faculty nodes. Thus the existing private VLANs inside registrations offices had to be preserved.

Among the security issues addressed was that conventional firewalls do not help at protecting web services, since such services operate on standard http and https ports (80 and 443). Moreover, due to the distributed architecture, latency is an important issue. Digital signing and encryption (VPNs, SSL) add additional performance burdens that had to be tackled.

2.6. Interoperability requirements

The technical specifications ensuring interoperability are prescribed by the Greek eGovernment Interoperability Framework (Greek e-GIF). Under this framework, web services are required to implement the SOAP protocol for data transfer, the WSDL service description and the UDDI standard for listing what services are available. Also data transferred between systems should follow specific standards, namely XML and XML Schemas. The transformation of data should be done using XSL and all XML implementations will be developed to meet the W3C guidelines. In general, all outputs should be XML under the W3C guidelines. In terms of Directory Services these should be based on some LDAP compatible protocol.

3. ALTERNATIVES CONSIDERED

The University IT Center considered in consultation with the affected users the pros/cons and risks regarding 3 alternatives:

1. The use of some commercial SIS software localized for the national legislation and the Greek language. A possible alternative would be the software already used at that time by the majority of departments. A couple other alternatives with smaller installation basis existed in the Greek market; international software could also be an option. In any case this had to go with major upgrade of the existing functionality in order to support new needs, along with major Business Process Re-engineering, which meant basically simplification and homogenization across campus. Security procedures were also an issue for upgrade and integration
2. The in-house development of a SIS
3. The adoption of some community Open Source SIS.

The selection was based mainly on the following criteria:

- Commercial SIS are not that flexible to adapt rapidly to new requirements (e.g. new business processes) and demanding user expectations. These systems are quite expensive to implement or maintain
- Development of in-house systems is challenging since funding is limited and deadlines are frequently not met in such deployments. Moreover, it requires technical and project management skills, which are not always available
- Open Source communities may constantly contribute to enhancements and ensure sustained development.

At that time, no significant resources could be allocated for in-house development. Moreover, due to the high risks in terms of time planning and budgetary issues, the 2nd alternative had to be postponed if not cancelled.

AUTH was not aware at that time of any complete Community Open Source Student SIS such as Kuali Student (it was actually in the launching phase), thus we had to exclude this alternative, at least for that time being. The Feasibility Study funded by the Andrew W. Mellon Foundation to assess college and university interest in a next generation, open source SIS, which actually led to the Kuali Student project, was only available in July 2006.

On the other hand vendor supplied systems impose a lot of risks as well. Depending on how closed and non-standardized they are, future development is either limited or costly. Further in-house development is difficult in case interoperability issues are overlooked.

AUTH finally opted for a mixture of the first two alternatives, that is the supply of a standards based, modular, commercial SIS that interoperates with the existing infrastructure and also allows in-house developed applications to be used in place or on top of the vendor modules, by making use of web-services with no additional loyalties.

Given the national and European Commission financing possibilities, the Centre applied for funding, which was approved in 2005 (Greek Information Society Framework Program). The biding procedures and evaluation awarded Cardisoft e-University solution from a local vendor as the favourable SIS software, whereas ITC had to establish the elaborated security framework with internal resources so that vendor applications could focus on business requirements. The chosen SIS had just to fit to this security framework.

3.1. Definition of project success

The following key success indicators had been defined in order to measure the success of the project:

1. All departments sign some Memorandum of Understanding accepting centrally imposed terms and participate in the project
2. The core SIS Services have been successfully developed and released across departments
3. Migration of all student records and registration offices historical data have been transferred to the new SIS
4. The project is completed in a timely manner and services are deployed
5. The project budget was within initial expectations
6. Positive qualitative feedback is returned from students, faculty and staff on system experience (through surveys/questionnaires). According to this feedback the implemented SIS enables users to perform efficiently their day-to-day operations
7. Interoperability mechanisms (web services) are in place so that in-house developed modules can communicate with the vendor SIS.

4. OBJECTIVES ACHIEVED AND REALIZED SERVICES

Departments had to accept an internal MoU and immediately afterwards could exploit the project infrastructure, the software licenses and the migration/training man-hours. With the completion of the project the following objectives were achieved efficiently:

- The adoption of harmonized and homogenized business processes, especially the ones related to a common security policy across departments and faculties
- The consolidation of nodes at the faculty level so that economy of scale could be achieved along with maintenance simplicity, along with the upgrade to ANSI SQL databases (MS SQL)
- The increase of security level by establishing encrypted server to server communications (e.g. DB replication) through VPNs. Use of digital certificates by teachers in order to perform critical tasks (e.g. grades upload) and administrative operations
- The simplification of the user interface (with no training). With the deployment of SSO users don't have to retype passwords when moving around multiple university portals.

Supplementary to the security framework, rigid Terms of Use were diligently considered so that liabilities are clearly defined and academic authorities are well protected. The SIS was finally integrated with other similar university IT services such as synchronous and asynchronous learning systems. All users own a single user account across all web applications, based on pubcookie Single-Sign-On authentication and openLDAP. The same account is used for campus wireless network access, computer labs, portals offering software distribution, IT Helpdesk access, as well as access to central computer facilities (Terminal servers, Unix servers, personal disk space). Currently there are considerations to upgrade this infrastructure to Shibboleth in order to support federation.

4.1. Services offered

The project accomplished typical eUniversity services over a single portal http://web.itc.auth.gr in a one stop shop. Some of the services available per user group are shown in the following table. Please note that staff is served through fat clients that are confined in private faculty VLANs, which are manually synchronized with the external web applications on a daily schedule.

Table 1 Services per user group

User group	Undergraduate, graduate, PhD, exchange students	Access	SIS web portal
Read personal records and learning unit details such as syllabus and educational resources, Read recent or historical learning unit results, Receive alerts (email, SMS) when new learning unit results are available, Submit learning unit registration, Submit study material declarations per learning unit (a single book of choice free of charge), Apply for transcripts and get notifications on when to pick them up at the desk, or get notification on the date of mail dispatch, Read Course Timetable and Exam Calendar, Submit evaluation questionnaires, Read personalized messages.			
User group	Faculty teachers	Access	SIS web portal
Read historical taught learning unit instances, Get statistics on learning unit instances (participants, distributions, averages, deviations), Submit leaning unit details (e.g. course objectives, communication, office hours, syllabus), Submit digitally signed grades using HSMs, Receive alerts when committed learning unit results are modified for any reason, Read Course Timetable and Exam Calendar, Design, deploy and get feedback on student evaluation questionnaires, Read personalized messages or send personalized or team messages to students, Manage student absences.			
User group	Administrative staff	Access	Fat client
Manage students' enrolment, Manage Educational Programs (curricula), Learning Units and Learning Unit instances that form Educational Programs, Manage registration of Learning Units and study material declarations, Issue transcripts for students / alumni, Produce statistics / reports, Check and accept digitally signed scores sent from faculty through portals, Manage Course and Exam Calendar, Send messages to groups of students or teachers, Design, deploy and get feedback on student evaluation questionnaires, Receive alerts when learning unit results are modified for any reason.			

4.2. The established technical architecture

The vendor supplied SIS has a 3-tier architecture supporting both thin and fat clients based on Microsoft SQL Server. The application server (AS) uses DCOM objects that are responsible for

exchanging data with the database (DB). As planned, although core applications are commercial off-the-shelf, the architecture is open so that new applications could be developed in-house.

Web applications serving students and teachers are installed on distributed IIS web servers. The web servers use dynamic pages that take data from a source, transform them into HTML format and send them to the user's web browser. The technology of dynamic pages used by the vendor is Active Server Pages (ASP). As it is depicted in the following figure of system topology, the central portal server redirects (distributes) web traffic to the responsible faculty web servers and in that sense it also performs load balancing.

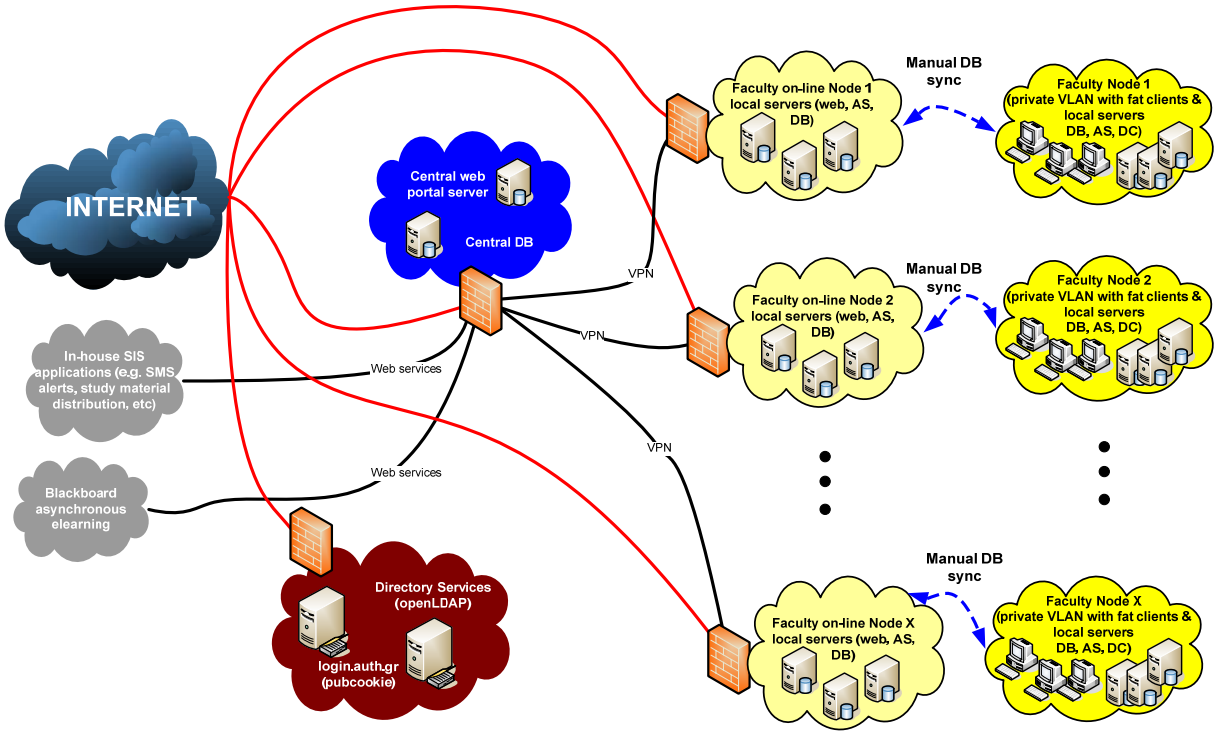

Figure 1 Architectural Topology

As seen from the figure above, in order to achieve the project objectives a central database that is synchronized with the distributed faculty databases was in need. Private faculty VLANs synchronize manually with on-line faculty databases under a daily schedule. In sequence on-line faculty databases are synchronized with the central DB. During working days only specific tables are replicated, whereas full database replication occurs during weekends. The technology used is Transact-SQL jobs. Local Domain Controllers (DC) take care of HSM certificate authentication for Windows Login.

For a student (either a freshman or senior) it is quite simple to activate access. Students just need a visit to the local faculty registration office in order to get a print-out with a one-time password. They simply visit a web page in order to negotiate either a new account or re-activate an existing one (e.g. forgotten password).

For the design and implementation of the security framework of the project, the following were put into practice. Based on qualitative measures and given that students are roaming across PC labs or internet cafes (a personal laptop is not always used), soft personal certificates would be at great exposure. Although PKI has already been deployed across campus since 2002, it was decided that student applications should solely be served over SSL, with no requirements on soft or hard X.509 certificates, trying to keep things easy for them.

In contrast, instructor services require HSMs (SCs with USB interface) used only from registered IPs over openVPN connections. Teachers may submit online grades which are digitally signed for authentication, confidentiality, integrity and non-repudiation reasons. Security policy demands that

online infrastructure is protected by firewalls offering stateful packet filtering. In short, among the realized security mechanisms are the following:

- User authentication with passwords for students and HSMs/PIN for faculty members, administrators and administrative staff (two-factor authentication)
- Web transactions are protected by traditional SSL over https
- Private VLANs per faculty node
- Certain transactions require point-to-point security (openVPN for server to server connections)
- The policy enforces event logging, both at the operating system as well as the SIS application level that allows the investigation of incidents
- Personal privacy is applied by implementing the institutional and national legal framework (2472/97, privacy issues of N.2774/99).

Furthermore a student smart card pilot was also implemented. The smart card (AUTH eKey) contains the cardholder's certificate issued by the Certification Authority of Aristotle University. AUTH eKey offered the following additional features for interested students:

- Use of eKey as a Student ID within campus (as an alternative to Photo IDs)
- Use of eKey as a library card for specific campus libraries (as an alternative to barcode library cards)
- Digital signing and encryption of emails or files supporting this feature (MS Word, Acrobat PDF)
- Login in Windows Domains by simply keying-in the SC PIN in specific computer labs
- Establishing secure VPN connections with campus network when off-campus
- Physical Zone Access Control in specific computer labs.

Both smart cards and HSMs chosen support RSA and are FIPS-140-1 L2 validated. Asymmetric key pairs are created on the SC or the HSM. They support a list of APIs: Microsoft CAPI, PKCS # 11 and Microsoft PC/SC through which applications can access the crypto store of the SC, support S/MIME, SSL client authentication and smart card login.

Given that the cost of such a smart card is not trivial for mass deployment, a simplistic cost-benefit analysis based on the pilot suggested that there is no significant benefit from such deployment if there are no substantial services to be covered by the card. Thus the campus-wide eKey deployment should come after service augmentation, say by electronic purse applications, charge management of photocopying machines/ printing, etc.

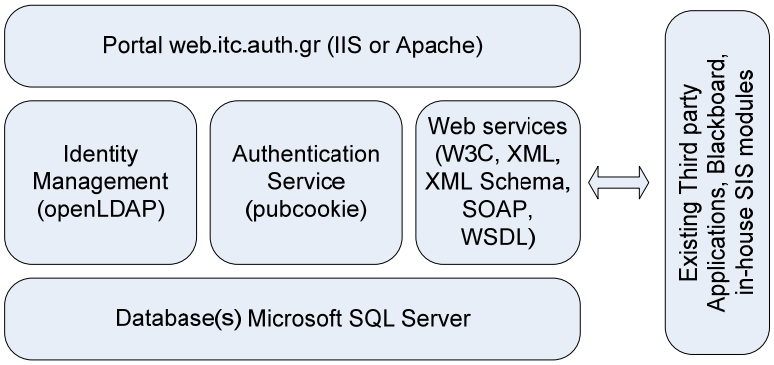

Figure 2 Technologies used

4.3. Level of interoperability achieved

As far as interoperability with other systems in campus and off campus is concerned, effort was put to achieve the maximum degree of compatibility and connectivity with existing ICT services. By using web services, in cooperation with the AUTH Library System it was possible to activate new

users in the Blackboard asynchronous elearning system. Course registration is readily available to Blackboard in the beginning of each semester, in a semi-automatic way; however the registration offices are not disturbed and data re-entry is eliminated.

Popular in-house developed applications and modules on top of the vendor SIS are already in pilot phase or production:

- Student SMS alerting in the event of "new grades available in the web portal" and
- A module for the Management of Study Material declarations and distribution

The established SIS followed the open standards stated in the design phase such as the accessibility guidelines WCAG and WAI by W3C and the interoperability standards recommended by the Greek eGovernment Interoperability Framework (SOAP, UDDI, WSDL, XML). In so doing, it is now feasible, although not implemented yet, to accomplish interconnection with the Greek National eGovernment Portal HERMES that serves citizens and businesses.

4.4. User acceptance

Impact can be speculated by the use of SIS services and also by qualitative instruments such as questionnaires. Currently, the services are used by more than 30% of the students and 20% of the instructors. In absolute numbers more than 20,000 users performed at least one transaction during last year and more than 10,000 student course registrations were served. Web servers experience a daily average of 5,000 distinct visits and more than 15,000 visits on peak days. There are still open requests towards improving the web interface, but in general questionnaires reflected positive user acceptance.

4.5. Objectives left for 2010+

Some of the identified objectives were impossible to meet due to budgetary reasons, or due to non available technologies. Some others were contradictory to each other, i.e. the political ones stemming from departmental views and the ones expressed by IT professionals. ITC implied that the integration had to be completely central, whereas departments suggested consolidation at the faculty level. It was then decided, as a compromise, to postpone the completely centralized system for 2010+. Among objectives which are still active but not yet accomplished under the current project is that university business logic should be gradually removed from the application code and workflow tools for conceptualizing processes should be preferred instead.

Moreover, in terms of security a significant issue remains – the conventional HTTP firewalls do not help at protecting web services. One should employ XML/SOAP firewalls, capable of conducting filtering at the application level of web server traffic and make smart decisions about letting SOAP messages through. All users wish for completely real-time on-line transactions, but this will only happen under conditions. Private VLANs and manual database synchronization could be eliminated as soon as some steady security best practices such as OWASP Web Services Security Project mitigate security risks by protecting web services and XML based SOAP messages in a distributed environment.

5. CONCLUSIONS

This paper explored lessons learned from the deployment of a student/instructor information system in Aristotle University of Thessaloniki. Both quantitative indicators (number of users, served transactions, portal visits, etc.) and qualitative instruments such as questionnaires reflected positive user acceptance. Currently, the services are used by more than 30% of the students and 20% of the instructors. Having in mind the low internet acceptance figures in Greece and given that a substantial student majority is feeling uncomfortable with performing online transactions, evaluation figures are promising, but there is still a long way ahead towards global acceptance. Among lessons learned, we want to note the migration issues that were underestimated (both time-wise and cost-wise), since in the past each department had invested in various non-homogeneous and non-standardized technologies. Both students and instructors involved were quite enthusiastic and receptive, whereas a large number of administrative staff expressed the typical resistance to change, especially the less computer-literate ones. The only risk mitigating action was to have these people involved in the early stages of the project, to train them, to make them feel part of the

project and shareholders of the credit. Actually administrative people had to realize that the plan is not to reduce the number of staff; to the contrary, it is to make them more productive by letting them do more in less time.

Constantly along the course of the project we felt the need of reconsidering business processes, in an effort to keep them simple. Security has also been and still is perceived by some users as complexity. On the whole, the SIS services really revolutionized the university operations and also gave a boost to other similar ICT services across campus such as asynchronous e-learning.

6. REFERENCES

Cardisoft website (2009). *Cardisoft e-University Technical Architecture*. Retrieved May 20, 2009, from: http://www.cardisoft.gr/en/eUni/ .

Hawkins, B. L., Rudy, J. A., Nicolich, R. (2005). *EDUCAUSE Core Data Service Fiscal Year 2004 Summary Report.* Retrieved May 20, 2009, from: http://net.educause.edu/ir/library/pdf/PUB8002.pdf .

Hossler, D. (2006). *Building a Student Information System: Strategies for Success and Implications for Campus Policy Makers. New Directions for Higher Education, No. 136*. San Francisco: Jossey-Bass, 2007. 88 pp.

Wheeler, B. (2006). *Open Source Student Services System, Report on the planning grant from the Andrew W. Mellon Foundation*. Retrieved May 20, 2009, from: http://update.estrategy.ubc.ca/wp-content/assets/Mellon-Wheeler.pdf .