Information technology networked system for student mobility support

Piotr Dębiec and Andrzej Materka
Institute of Electronics, Lodz University of Technology, Lodz, Poland

Abstract

Purpose – This paper presents an IT system – Student Connectivity Module (SCM) – designed to support administration of student exchange between universities in different countries, developed under the EU seventh Framework Program. The purpose of this paper is to share the acquired knowledge on existing difficulties in mobility management, propose solutions to those problems, and present results of system validation using its prototype deployed at two universities.

Design/methodology/approach – Prior to the system design, the needs, plans and expectations concerning the academic IT services were surveyed among 100 universities. On this basis, in close with prospective system users, an original peer-to-peer system was developed using top-down model-driven and agile software development techniques.

Findings – The barriers to effective interoperation of academic information systems (AIS) were revealed: first, diversity and heterogeneity of campus IT solutions; second, differences in patterns of international student mobility flow; third, diversity in national personal data protection policies; and fourth, lack of standards for e-data exchange. The SCM system overcomes these problems by adopting platform-independent IT solutions, web-services, a network of trusted authority servers, and a novel "quasi-standard" solution for e-data exchange, with the use of home university campus cards to access facilities at host institutions.

Originality/value – The management of foreign student exchange is a complicated process. It involves students, faculty, administrative staff and external institutions. To the authors knowledge, there is no other comprehensive networked IT system available to facilitate administration of student mobility, make it better controlled, less laborious and faster, in a secure way. The IT solution contributes to overcoming the current barriers to academic mobility within Europe and elsewhere.

Keywords Information systems, Campus smart card, International student exchange, Personal data security

Paper type Case study

1. Introduction

The aim of the Bologna Process is to create a European Higher Education Area based on international cooperation and academic exchange of students and staff [1]. This idea is strongly supported by the Erasmus program, which is a part of European Union's Lifelong Learning Program[2]. The program, established in 1987, offers students and universities' staff an opportunity to study or work in another European country for a period of minimum three and maximum 12 months. The program includes financial support for studying and working abroad, foreign language preparation, multilateral projects, and university cooperation. The number of students and academics benefited from the Erasmus grants increases year by year. For example, in the 2011/2012 academic

This work has been supported by the "European Education Connectivity Solution" project under European Union 7th Framework Program. The collaboration with European Campus Card Association (ECCA), in particular, the help of ECCA members, Eugene McKenna, Tor Fridell, and Sinead Nealon, in conducting the university survey, is much appreciated.

The International Journal of Information and Learning Technology
Vol. 32 No. 1, 2015
pp. 17-31

2056-4880
DOI 10.1108/IJILT-06-2014-0014

year, more than 250,000 students from 33 countries spent part of their studies abroad at around 4,000 colleges and universities.

For each education institution that takes part in the Erasmus program, the management of the student exchange is a big challenge because of significant differences in organization of study, study programs, rules and regulations existing at the cooperating institutions and concerning for example assessment rules and grades, document forms, field of study names, and academic calendars. This diversity is reflected in the European AIS which are highly incompatible and cannot directly exchange electronic data. Moreover, these systems also differ in technical details, such as data structures, text character encoding schemes, or languages supported, what sometimes precludes even manual entry of the incoming student's data. As an example, the second family name of an incoming Spanish student cannot be entered into a Polish information system because there is no such field in the database. Moreover, even the student's ID cannot be entered when it is identical with any local student ID as this would break the database integrity. As a consequence, the academic records of students coming from Spain are stored in a paper form. That raises a problem with issuing campus cards for these students what in turn can preclude them from access to the host university facilities such as library, student web portal, vending machines.

To address the above problems, in 2009, the consortium of three enterprises, OneCard Solution (Ireland), OPTeam (Poland), Mecenat (Sweden), and three universities, Waterford Institute of Technology (WIT) (Ireland), University of Zagreb (Croatia), Lodz University of Technology (TUL) (Poland), started a "European Education Connectivity Solution" (EECS) research and development project supported financially within the European Union 7th Framework Program [3]. The primary goal of the project was to develop and implement a working prototype system which would overcome the current barrier to market expansion by facilitating student information exchange, and providing mobile students with a wide range of services based on the use of campus smart card technology (Materka *et al.*, 2009). The prototype was intended for future commercialization by the cooperating enterprises.

In the first stage of the project, all the university partners did research on the current state and the needs concerning student facilities, student exchange rules and practices existing at their home institutions. Particular attention was paid to personal data protection regulations and IT solutions supporting students and staff. Additionally, the needs, plans and expectations concerning the desirable IT services were surveyed among more than 100 chief international officers and stakeholders coming from different European universities. The survey had revealed, for example, that 86 percent of the universities show moderate or strong need for direct electronic data exchange between cooperating institutions. By comparison, the need for e-learning and distance learning solutions had been 66 percent. The research and survey results were then evaluated and compared for similarities and differences existing at the universities. This in-depth analysis allowed identifying the following crucial design issues:

- personal information protection policy – most European countries do not permit personal data storage and processing on the territory of another country;
- connectivity with diverse systems – European AIS are implemented with a variety of diverse technologies and have incompatible database structures;
- interoperation between the peers – there are no formal standards defining data formats and data exchange protocols in the domain of higher education and campus card systems;

- conformance with the Erasmus program – the students' application processing procedures must be implemented in accordance with the program's rules;
- multilingualism – the system must support all the European languages;
- scalability – the system must be able to handle various student exchange traffic levels and the growing number of cooperating universities; and
- security and mutual trust – cryptographically strong and widely accepted algorithms and protocols must be used to ensure data protection and mutual trust between the cooperating institutions.

In the paper, the solutions to these problems are presented along with the results of their verification performed on the working prototype of the system with strictly defined tests, real-life trials, and validations.

2. Related works/research

The problem of standardization of the trans-national learning documents and certifications has been addressed by the European Parliament, and the Europass initiative was established in 2004 to increase mobility of citizens[4]. Within the initiative, a paper form of the Mobility Certificate has been standardized; the document certifies knowledge and skills acquired during study or work in another country. Another product of the initiative was a prototype system to exchange the electronic documents between the higher education institutions. However, that system did not support the management of student mobility process in any way – it was focused only on secure exchange of the final data concerning mobility, namely Transcript of Records and Skills and Competences acquired, necessary to issue the Europass Mobility document (Athanassios and Philippe, 2006).

In 2008, two consortia of Polish and Italian universities, MUCI and Cineca respectively, started a new project aimed at developing a prototype infrastructure to exchange data about student mobility between two universities (Mincer-Daszkiewicz *et al.*, 2009). The prototype was completed in 2009 and connected the University of Parma in Italy and the University of Warsaw in Poland. It was based on Java Web Services (WS), Glassfish application servers, and Oracle database. The experiment revealed incompatibility problems of information processing systems already in use at both institutions, and a need for standardization was concluded. The next step in the project was to start cooperation with Roman Student Systems and Standards Group (RS3G), European University Information Systems (EUNIS) which is a federation of around 150 European university directors of information technology, and companies from Europe and the USA[5].

The only existing "quasi-standard" application for European student mobility support is the moveon system developed by QS-unisolution[6] which is used by about 300 European Higher Education Institutions. Almost all the procedures required by Erasmus mobility regulations are supported by several modules of the system, such as, "Mobility grants application filling in and management", "Electronic Learning Agreements", and "Mobility Certificates". However, the system is not integrated with any of the information systems currently used at the European universities, so students' data have to be re-entered or imported manually through text files of the given, strictly defined format (direct information from Sales Department of QS-unisolution company, obtained in 2012). This is the only way of the data synchronization implemented in moveon what is its main

weakness. Despite 12 years of existence on the united European market, the use of the system is limited mainly to Germany (153 universities) and France (100 universities). The only Polish university using moveon software was Technical University of Opole which eventually abandoned its use.

Considering the lack of formal standards, we proposed a novel "quasi-standard" solution based on mutual exchange of electronic versions of the paper documents, well-defined by the Erasmus program. Within the documents, the crucial data such as names and codes of countries, universities, study levels, fields of study, have been standardized by adopting the existing ISO standards, Erasmus database, and RS3G proposals. This approach reduces the exchange of non-standardized "raw" data thus reducing the amount of work required to upgrade the system when the appropriate standards become available.

3. System architecture

System architectures with a centralized database were not considered because most European countries do not permit personal data storage and processing on the territory of another country. We proposed a peer-to-peer architecture with a network of applications and databases located at the individual universities. Each of the databases contains the information concerning only the home outgoing students but not the incoming students. Each of the applications processes only the local data but can have an indirect, read-only access to the strictly defined data of the peer databases, and can remotely trigger the strictly defined group of functions and procedures at the peer sites. The actual data processing is always performed locally and the selected results can be presented to the authorized users at the cooperating institutions.

Three software modules operate in each node (Figure 1), namely Client Application Interface (CAI), Card Application Management System (CAMS), and Student Connectivity Module (SCM). Two former modules perform student authentication and authorization and assure access to various campus facilities such as libraries,

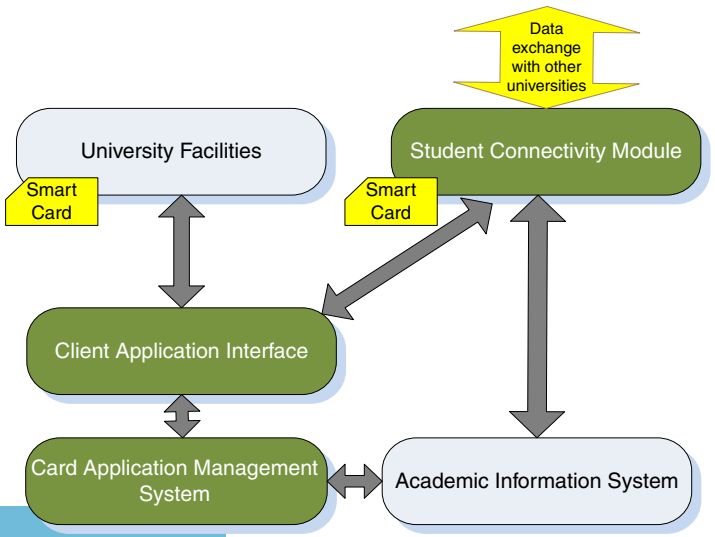

Figure 1.
Interconnections between the system modules

laboratories, or vending machines. The latter module supports all the student mobility procedures defined by the Erasmus program. The SCM utilizes the CAI module as the only trusted service for student authentication and authorization.

The modules contain three interfaces, namely the SCM-to-SCM interface, the interface to the local information system, and the interface to the university facilities. All the interfaces are implemented using open standard technologies. The interface to the information system is a preconfigured, preferable, but optional connection. Its main role is to automatically deliver to the SCM personal data and course of study details for the students who apply for mobility grants. This is to avoid retyping a huge amount of data that already exists in the local systems. The SCM-to-SCM interface is the main data exchange connection linking each pair of the cooperating higher education institutions. The peer-to-peer network of the SCMs is illustrated in Figure 2.

To deal with significant differences in the IT infrastructure existing at the universities, the proposed architecture is very flexible. The system modules can operate autonomously, without any additional elements or services. On the other hand, the system can utilize the external data sources and services, such as LDAP authentication and authorization service or academic database, if they are available at the given institution.

4. Compatibility and interoperation issues

In the target peer-to-peer system, the cooperating SCMs communicate with each other using Internet infrastructure. The communication protocol is based on a widely accepted and stable remote procedure call technology named web services, which allow for integrating diverse systems using independently developed software.

The peer-to-peer WS are used to exchange electronic versions of the Erasmus documents. Four categories of data contained in these documents have been standardized according to MUCI, Cineca, and RS3G experiences and guidelines. Language code dictionary follows ISO 639-1 standard[7], country code dictionary follows ISO 3166-1 alpha-2 standard[8], and university and subject area records come from the LLP Erasmus database. The remaining coding schemes and protocols have been decided by the project team.

Because of the international nature of the system, the database and graphical user interface are multilingual. The distributed SCM architecture ensures that not more than two languages have to be supported in each node, namely English, which is obligatory for all locations, and national language. On installation, the SCM is initialized with English support only, but the system administrator expands it by entering translated names and terms to the SCM dictionaries using the dictionary management functionality. Similarly, the data supplied by students, for example the course names, can also be entered in two languages.

As our survey shows there are universities that run courses in more than two languages. For these cases, the SCM application can be configured to support any number of languages. The strings displayed on the interface, such as labels, headers, table names, are read out from text files. These text files can be edited by system administrator to contain translations for any language. The Unicode UTF-8 character encoding standard[9] has been adopted in the whole system, i.e., for the SCM database, the application code, and the configuration text files.

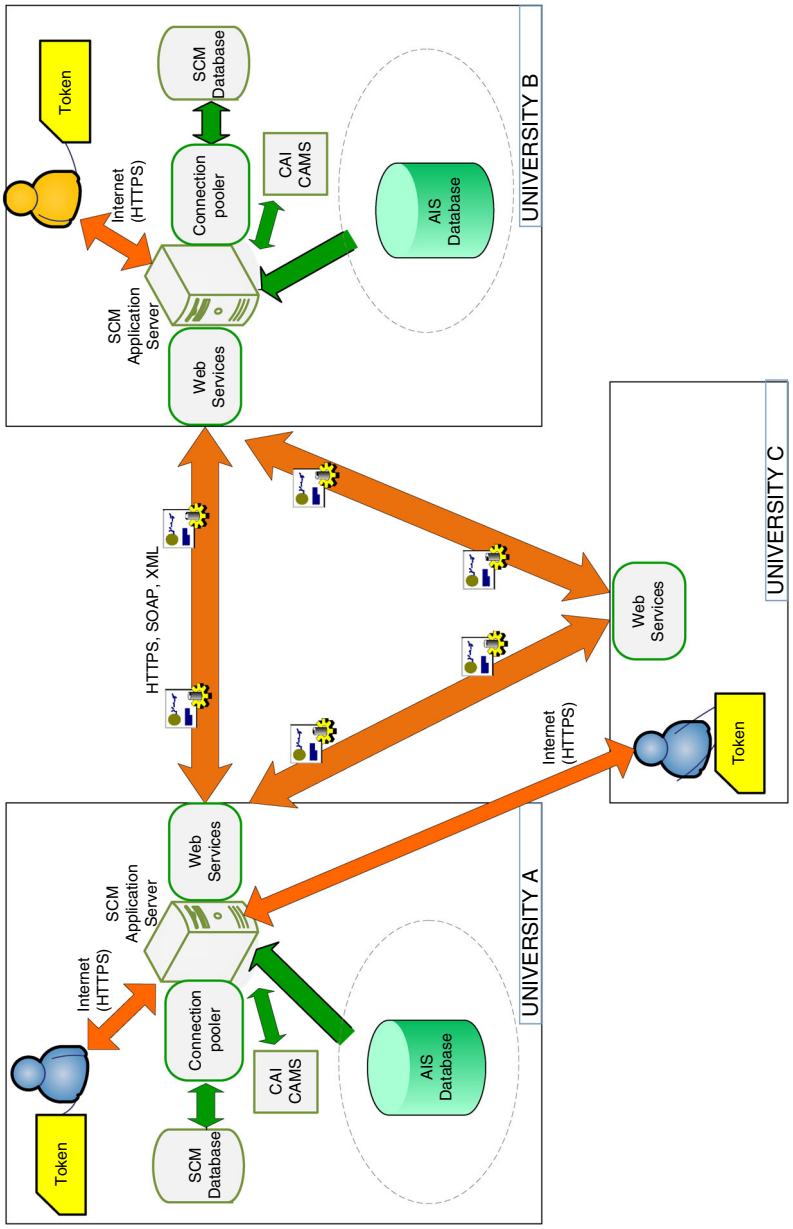

Figure 2.
Architecture of the SCM network

5. Conformance with student mobility standards

The student exchange model was derived from the Erasmus program rules and regulations. The model was further expanded in cooperation with international exchange office at the TUL to include national and university procedures. The following student exchange procedures are consistent with the Erasmus standards:

- LLP bilateral agreement;
- Student application for Mobility Grant;
- Transcript of records;
- Learning agreement;
- Changes to learning agreement;
- Prolongation of mobility period;
- Host transcript of records; and
- Stay confirmation.

The SCM module can be operated by several categories of users having different privileges in the exchange process:

- Educational program coordinator – registers university agreements concerning the student exchange; assigns coordinators to agreements; takes final decision on student Mobility Grant applications;
- Dean's officer – enters, modifies and approves data related to applicant's studies (e.g. average mark, Transcript of Records, enrollment for relevant year/semester);
- Agreement coordinator – co-ordinates actions resulting from the exchange agreement; evaluates student application for Mobility Grant, produces a ranking list of the applications; and
- Student – Mobility Grant applicant.

The data exchanged between universities are related to the information required during filling in and processing of the Erasmus forms. The important assumption is that there is only one source of primary information related to student mobility – it is his/her home university SCM database. The majority of data and decisions are entered into this database by home students and local staff. However, some data such as host Transcript of Records or decisions concerning study abroad are entered remotely by the cooperating universities.

At any time, students can view the status of their applications which can be for example: "submitted", "verified", "lacking data", "qualified", "rejected", "ready to be signed". To fulfill the Erasmus procedure the appropriate electronic PDF documents are generated, printed, signed and posted.

As an example, a student at the host university wants to change the previously accepted Learning Agreement, for example, replace one course with another. To follow the Erasmus Changes to Learning Agreement procedure, student fills in and signs an appropriate form (Figure 3). The paper document is then accepted and signed by the host Educational Program Coordinator, and sent to the home university. The home coordinator, after receiving acceptance of the new Learning Agreement from the home Dean's Officer and Agreement Coordinator, takes the final decision, and sends the signed document back to the host Educational Program Coordinator. The process is rather slow because the paper documents must be exchanged by mail.

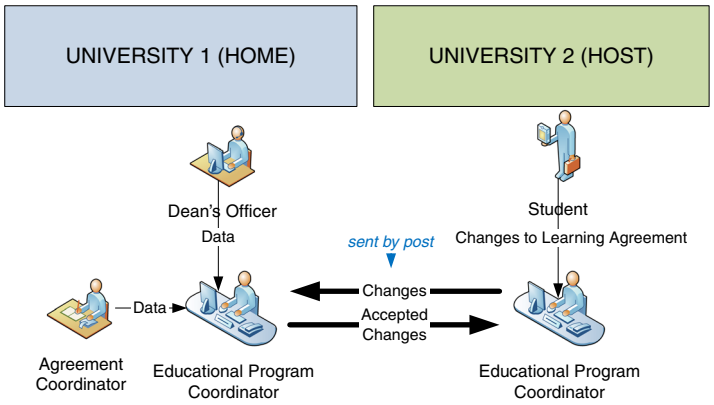

Figure 3.
Changes to learning agreement use case

In the SCM module, the decision is made without delay and is instantly accessible for the other parties involved in the procedure. The SCM implementation of the Changes to Learning Agreement is presented schematically in Figure 4. With a web browser, the student logs into his/her home university SCM and fills in the appropriate form (step 1). In step 2, the host Educational Program Coordinator logs into the host university SCM and has (indirect) access to the student's application via the SCM-to-SCM connection. The coordinator remotely confirms the application in the student's home SCM database. The confirmation makes the student application data accessible for the home Educational Program Coordinator, Dean's Officer, and Agreement Coordinator who then make their own independent decisions. Usually, the Educational Program Coordinator waits for the Dean's Officer and Agreement Coordinator acceptances (steps 3a, 3b) before making a decision (step 4). This decision is treated as final and becomes instantly visible for the student in

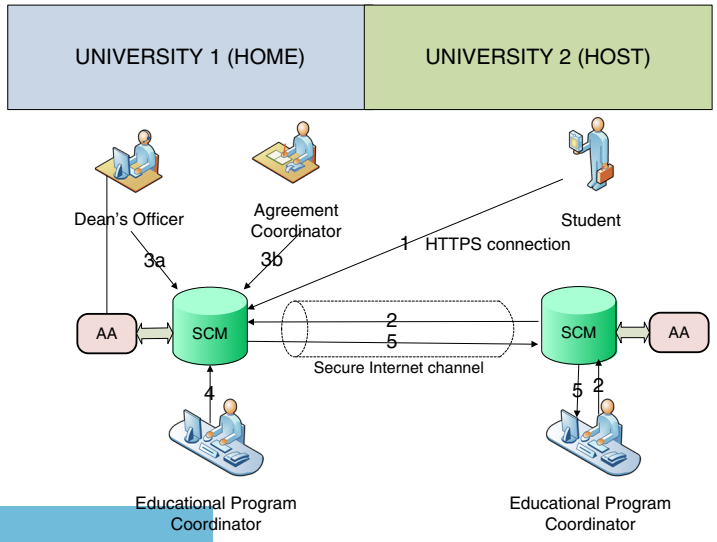

Figure 4.
Changes to learning agreement implementation

his/her home SCM application (locally) and for the cooperating coordinators in the host SCM application (remotely).

All the remaining procedures are performed similarly. The data coming from the cooperating institutions' databases are accessible remotely but they are never copied between the SCM systems. The Erasmus standard PDF documents are always generated using student's home SCM data and then can be downloaded and copied at student's host university. Such a solution has eliminated the need for automatic data synchronization which is a very complex issue in distributed systems.

6. Security and mutual trust

Security issues are very important in any public peer-to-peer network. Ideally, the node's security level should be controlled exclusively by that node and cannot be affected by any other node. In practice, this goal can be achieved to a certain extent.

In the EECS project, the most important issue was how to locally authenticate the peer systems' users without their prior registration in the local systems. Because central user management systems could not be used, we proposed an original two-phase authentication procedure. In the first phase, the user is authenticated in his/her home SCM. In the second phase, the user's identification data (first name, family name, and university code) are sent to the peer's SCM server, but this transmission is only allowed after successful SCM-to-SCM authentication.

In the first authentication phase, students use their home campus cards. The login token is read from the card with the use of a smart card reader controlled by a Java applet being an element of the SCM web application. The username and token are then encrypted and sent through the Internet link to the home SCM server. The main security issue concerns the card access keys which are sent through the Internet to read out the token. The keys must be protected from disclosure to unauthorized persons including the card owner, because the same keys are often used in other campus facilities, such as vending machines and access control systems. However, the Java applet communicating with the reader runs on the user machine, so it can be copied, disassembled and modified locally to reveal the keys. This poses a potential security problem.

To avoid this problem, we decided to use the card's Unique Identifier (UID) as the login token. This data can be read without any access keys and is unique in the local systems. The authentication is strengthened with a four-digit personal identification number (PIN), which must be entered by student during the logon process. After three failed login attempts the student's account is blocked. The authentication process is mutual – the Java applet is signed by the university's private key which is certified by the trusted, public certification authority. Otherwise, the software is considered untrusted and alerting messages are displayed in the web browser to discourage user from using it.

The staff is authenticated with usernames and passwords. The user account management is performed locally thus the cooperating peers are not mutually informed about the other party's users. To improve the mutual trust level, the system logs all the operations performed by the peers' users.

For the second phase of server authentication, the WS-Security (WSS) solution was initially considered, because it is built in the adopted WS technology. However, as our literature studies have shown, the WSS technology does not ensure enough security and is prone to dictionary, replay, and token substitution attacks (Krawczyk and Wielgus, 2006). Additionally, the weakness of the peer authentication procedure built in the public WS registries makes it possible to register and use the services by

unauthorized parties (Dai and Steele, 2005). Some research has been conducted to improve the level of trust in public Universal Description, Discovery and Integration services by the use of personal Public Key Infrastructure required by every client or provider of WS (Rekik *et al.*, 2009), but this non-standard solution would require the existence of a specialized central authority what was unacceptable.

The proposed solution is to combine WS with the proven public key infrastructure built into the Secure Socket Layer protocol, and utilize the existing trusted public network of X.509 certificate authorities such as VeriSign or Thawte. In the proposed scenario, the strong authentication is combined with strong confidentiality of the exchanged data.

The user authorization is strictly defined and controlled in two layers of the SCM. The WS layer does not allow for direct access to the partner's database – only the operations implemented in the WS procedures are available for the peer. In the application, each logged user is assigned a role (e.g. Educational Program Coordinator, Dean's Officer) that allows calling strictly defined subset of the WS procedures.

7. Testing, validation and trials

Because of the practical context of the project, the system testing and validation were being performed constantly by all the consortium members. The cooperation within the consortium in this area can be summarized as follows. The research teams were producing the project's deliverables to a specified quality level, within the acceptance criteria formally defined in the project documentation. The enterprise parties were responsible for the final acceptance of all deliverables and then took up and exploited the results to their own advantage.

The methodology used during the SCM design and testing was a combination of top-down model-driven and agile software development techniques (Martin, 2002), enabling evolutionary development and delivery. The successive, enhanced versions of the student mobility module were instantly implemented, tested and enhanced, starting from early stages. Each of the SCM versions was subject to standard unit tests performed by programmers and a series of functional tests performed by a group of teachers according to the previously defined scenarios. The teachers were instantly passing the test results to the programmers who in turn were delivering the next version of the system. The milestone versions of the SCM were subject to additional tests performed by the staff of the International Exchange Office to validate that the implemented functions and electronic documents are in compliance with the Erasmus rules and regulations.

The presented testing and validation procedure was conducted on the system of two SCM instances installed at WIT, Ireland, and TUL, Poland. In the former location, the SCM was integrated with the local campus card system. In the latter location, the SCM was additionally integrated with the local AIS. The test and validation results confirmed that important design problems had been solved – the SCM is capable of exchanging information with other SCMs and the local AIS, supports multiple languages and conforms to the Erasmus standards.

The solutions concerning the system security and, consequently, the mutual trust between the cooperating nodes, were more difficult to be verified, mainly because there are no widely accepted tests or tools that can be used to assess the security level of networked information systems. Moreover, none of the cryptographic algorithms used to protect these systems has been scientifically proved to be unconditionally secure. The strength of these algorithms, for the given secret key length, can only be roughly

estimated using complexity theory (Schneier, 1996). Thus the ultimate security test is to implement the system, publish the whole system documentation and source codes, and wait for the results of cracking trials performed by professional cryptanalysts, researchers or hackers. However, this approach could not be used because the time frame of the project was too short, and the substantial part of the documentation had to be kept confidential according to the consortium agreement.

Despite this, to achieve high security standards, we used a kind of "security by design" approach to discover potential vulnerabilities of the security measures proposed for the system. This approach was based on a critical peer review of each of the proposed solutions concerning the system security. All the project teams were involved in the process, and the proposals were implemented if no vulnerabilities were found.

The personal data protection policy problem is solved by the distributed architecture of the system – all the students' personal data are stored and processed in their home countries. Similarly, the peer-to-peer communication scheme along with peer-to-peer SCM database architecture mitigate the global scalability issue – the bandwidth demand on each node is independent of the total number of cooperating peers. In other words, adding a new bilateral connection to the SCM network has no influence on the remaining nodes. However, as some research has showed (Hales and Edmonds, 2005; Vakili *et al.*, 2013), the overall performance of large-scale peer-to-peer systems can be highly variable and unpredictable, and a significant improvement of the cooperation quality is a difficult scientific challenge on its own.

The local scalability issue is mainly connected with the limited database resources that can be assigned to the SCM by university administrators. Setting database quotas is a common solution in the case when the same database server is used by many applications. Although the quotas can affect various system resources such as disk space, memory usage, or processor time, our experience shows that bottleneck problems mainly result from the limitation of the number of concurrent sessions. To overcome the problem, a connection pooler has been designed to manage a large number of concurrent incoming peer requests using a small number of shared database connections (Figure 2). The operation of the pooler was tested with an artificially generated traffic pattern emulating 100 concurrent peer-to-peer requests serviced using five database sessions. The results showed that each of the requests was serviced within 30 seconds, and 30 percent of the requests were serviced within two seconds. None of the connections had been timed out.

Apart from the presented tests and validations, the following three cross-platform features of the SCM were tested according to the requirements of the cooperating enterprises:

- Web browser independence was tested using Internet Explorer, Firefox, Opera, and Chrome;
- Operating system independence was tested under Linux and Windows; and
- Database independence was tested with Oracle and MS SQL database management systems.

During the cross-platform tests, a series of system refinements were made mainly to address the database independence issues. The final version of the SCM operated properly in various configurations of the operating systems, database technologies, and web browsers.

For the user acceptance verification, end-user trials were performed within the following experiment. The system was tested during a real-life exchange of student groups between two universities – TUL, Poland, and WIT, Ireland. Two WIT students

came to Lodz for a week in March 2011, and three TUL students went to Waterford for the same time period. The students and staff members of the two universities went through the Erasmus-comply procedures ;and were guided by the SCM interfaces. Every aspect of the exchange was in agreement with the Erasmus rules, except of the period of study which was shorter for economic reasons. Being at the home university, the students applied for the exchange grant and selected classes they wanted to attend abroad. After arrival to the host university, the students attended classes, received marks and, at the end of the exchange period, were issued confirmations of stay.

During the stay, the students were using their ID cards to access the selected facilities, such as library, vending machines, and class attendance service. The students' activity tested under the trial period was described in detail in the appropriate test scenarios. At the end of the exchange, each of the students had to fill in and deliver a strictly defined report. The report contained the details, results, observations, and remarks concerning the performed trials. The students detected the following issues:

- Several minor errors in the SCM instances (fixed immediately after their detection);
- Problem with opening the WIT library door using the TUL campus cards (solved during the exchange period); and
- No possibility to transfer money back from electronic purse to the bank account (this was "normal" behavior of the system agreed with the cooperating bank).

The user acceptance trials have confirmed that the SCM works as expected and the campus cards are properly recognized by the cooperating systems (WIT cards at TUL and TUL cards at WIT).

After proving that all the system requirements are met, according to the consortium agreement, the ownership of the SCM, the system prototype, source codes, and documentation has been transferred to the cooperating enterprises for commercialization purposes. Transfer of the SCM prototype was associated with its launching at the office of one of the cooperating enterprises, namely OPTeam, giving yet another test. The conclusion from the test was that the system installation and configuration is too difficult and time consuming. Consequently, the research group had to develop a software installer supporting the system deployment.

8. Summary and conclusions

The SCM has been designed as a part the EECS system to support the international student exchange process. The system architecture is a combination of an original network of nodes cooperating using WS, and the existing network of certification authorities working within the trusted and commonly used Public Key Infrastructure. This approach solves the technical and legal problems identified during the first phase of the project. The peer-to-peer distributed database structure ensures that the information protection rules being in force in many European countries are obeyed. The SCM software, run at the educational institutions, enables their cooperation across the Internet. The built-in interfaces allow for communication with any AIS. The use of the trusted PKI solution along with strong cryptographic algorithms delivers a high level of security and mutual trust. Lastly, the system architecture along with the database connection pooler, mitigate considerably the system scalability issues.

The system prototype was evaluated with extensive testing performed at unit, integration, system, and acceptance levels. Apart from the system designers and

programmers, the tests involved selected groups of students, teachers, and administrative staff. The test results allowed for consecutive refinements of the system. The ultimate conformance of the SCM with the Erasmus program has been validated by the staff of the International Office at Lodz University of Technology (TUL), Poland. The ultimate proof-of-concept trials were carried out at two universities in different IT environments. The SCM administrative scalability has been achieved by design, and the load scalability has been validated experimentally using artificially generated peer-to-peer traffic patterns.

The system security is based on advanced and mature cryptographic technologies, and each of the implemented security solutions has been reviewed and accepted by all the project teams. However, the SCM security has not been validated because there are no standardized methods that could be used to objectively assess and compare the information systems security levels. Moreover, security of every system degrades over time because more and more computing power becomes available at a lower cost and can be used to break the system that was previously considered secure. Therefore, a continuous process of third-party security assessment and auditing should be performed in the target environments. As a research team we did not have access to the production system – the ownership of the whole system has been transferred to the cooperating enterprises.

The three modules of the EECS system (CAI, CAMS, and SCM) form a unique, innovative solution that supports management of student mobility and makes the campus card services seamlessly available to students visiting foreign universities. In 2012, the EECS project won the prestigious European University Information Systems Organization (EUNIS) Elite Award [10][11].

The SCM has been built as a flexible information technology system, easy to integrate with existing solutions. However, there is still a need for extensive work on setting standards for mobility information exchange.

Notes

1. The Bologna Process – Towards the European Higher Education Area (2013), http://ec.europa.eu/education/higher-education/bologna_en.htm (accessed June 12, 2014).
2. The Lifelong Learning Programme: education and training opportunities for all (2013), http://ec.europa.eu/education/lifelong-learning-programme/doc78_en.htm (accessed June 12, 2014).
3. European Education Connectivity Solution, EECS (2013), www.eecscard.eu/index.php (accessed June 12, 2014).
4. Five documents to make your skills and qualifications clearly and easily understood in Europe (2013), http://europass.cedefop.europa.eu/en/home
5. RS3G – Rome Student Systems and Standards Group (2013), http://rs3g.sci.uma.es/drupal7/ (accessed June 12, 2014).
6. Unisolution moveon 4 – a Global Standard Software (2013), www.qs-unisolution.com/en/portfolio/moveon/about.html (accessed June 12, 2014).
7. Language codes – ISO 639 (2013), www.iso.org/iso/home/standards/language_codes.htm (accessed June 12, 2014).
8. Country Codes – ISO 3166 (2013), www.iso.org/iso/country_codes (accessed June 12, 2014).
9. Unicode Resources (2013), www.unicode.org/resources/utf8.html (accessed June 12, 2014).

10. EUNIS Elite Award 2012 (2013), www.eunis.org/wp-content/uploads/2013/11/EECS-2013-Elite-Award-Submission-1.pdf (accessed June 12, 2014).

11. European Campus Card Association (2013), ECCA News, http://ecca.ie/news-details/items/eunis-award-2012.html (accessed February 7, 2012).

References

Athanassios, S. and Philippe, T. (2006), *A Distributed System for Issuing Europass Mobility Documents*, European Centre for the Development of Vocational Training, Cedefop.

Dai, J. and Steele, R. (2005), "UDDI access control", *Proceedings of the International Conference on Information Technology and Applications*, *ICITA*, Sydney, July 4-7.

Hales, D., and Edmonds, B. (2005), "Applying a socially inspired technique (tags) to improve cooperation in P2P networks", *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, Vol. 35 No. 3, pp. 385-395.

Krawczyk, H. and Wielgus, M. (2006), "Security of web services", *Proceedings of the International Conference on Dependability of Computer Systems*, *DEPCOS*, Szklarska Poręba, pp. 183-190.

Martin, R.C. (2002), *Agile Software Development, Principles, Patterns, and Practices*, Prentice Hall, Englewood Cliffs, NJ.

Materka A., Strzelecki M. and Dębiec P. (2009), "Student's electronic card: a secure internet database system for university management support", in Kacprzyk, J. (Ed), *Advances in Intelligent and Soft Computing*, Vol. 64 No. 64, pp. 59-72.

Mincer-Daszkiewicz, J., Arcella, F. and Ravaioli, S. (2009), "Web-services for exchange of data on cooperation and mobility between higher education institutions", paper presented at the 15th International Conference of European University Information Systems, June 23-26, Santiago de Compostela, available at: www.usos.edu.pl/node/929 (accessed June 12, 2014).

Mincer-Daszkiewicz, J. (2010). "The mobility project – building network of web-servers for exchange of data on student mobility", paper presented at the 16th International Conference of European University Information Systems, June 23-25, Warsaw, available at: www.usos.edu.pl/node/377 (accessed June 12, 2014).

Rekik, W., Khemakhem, M., Belghith, A. and Fayolle, J. (2009), "PKI and UDDI based trust centre: an attempt to improve web service security", *Internet Technology and Secured Transactions 2009 Proceedings of the International Conference ICITST, November 9-12, IEEE, London*, pp. 1-4.

Schneier, B. (1996), *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc., New York, NY.

Vakili, G., Tabatabaee, F. and Khorsandi, S. (2013). "Emergence of cooperation in peer-to-peer systems: a complex adaptive system approach", *Systems Engineering*, Vol. 16 No. 2, pp. 213-223.

About the authors

Dr Piotr Dębiec was born in Poland in 1964. He received his MSc and PhD Degrees in Electronics Engineering from the Faculty of Electrical, Electronic, Computer and Control Engineering (EECCE), Lodz University of Technology (TUL), Poland, in 1989 and 1999, respectively. He is currently an Assistant Professor at TUL. His teaching interests include digital systems, hardware description languages, computer networks, and databases. His research interests include cellular neural networks, image processing, digital design, and integration of academic information systems. He is the head of academic information system development team at TUL. He has published 20 technical articles. Dr Piotr Dębiec is the corresponding author and can be contacted at: pdebiec@p.lodz.pl

Professor Andrzej Materka was born in Poland, in 1949. He received the MSc Degree in Radio Engineering from the Warsaw University of Technology in 1972, the PhD Degree in Technical Sciences from the Lodz University of Technology (TUL) in 1979, the DSc Degree (Habilitation) in Electronics from the Technical University of Wroclaw in 1985, and the title of Professor in technical sciences (electronics, computer engineering) from the President of Poland in 1996. Since 1974 he has been with the Institute of Electronics, TUL, being its director since 1995. His research interests include analog circuit design and testing, semiconductor device modeling, medical electronics, digital signal and image analysis, pattern recognition, artificial neural networks, secure database information systems design, electronic smart cards applications, as well as human-computer computer interfaces and aids for the visually impaired. In 1980-1982 he was with the Research Institute of Electronics, the Shizuoka University, Hamamatsu, Japan, where he worked on microwave MESFET multiple-device oscillators. In 1992-1994 he was a Senior Lecturer at the Department of Electrical and Computer Systems Engineering, the Monash University, Melbourne (Caulfield), Australia, where he taught electronics and digital signal processing. Professor Materka has published 250 technical articles and six books. He has supervised 18 PhD candidates. He was a co-founder of European Campus Card Association (www.ecca.ie) and was elected its Vice-President (2004-2006) and President (2009-2011).