A secure Internet database system for teaching and research information management at the Technical University of Łódź

A. Materka, P. Dębiec, M. Strzelecki, S. Hausman & S. Wiak

Technical University of Łódź
Łódź, Poland

ABSTRACT: A concise description of an Internet database system for teaching and research information management, for historical reasons known as *Student's Electronic Card*, is presented in this paper. The system was developed between 1998 and 2007 and successfully deployed at the Faculty of Electrical, Electronic, Computer and Control Engineering at the Technical University of Łódź, Poland. The system facilitates the most important activities of the community of 4,500 students and 450 faculty staff members. The core elements of the system are an Internet database and a number of specialised computer programs (terminals) with diverse functionality (teaching assignments, marking, student portal, cost analysis, etc). These terminals are used to enter, edit and retrieve data related to teaching, research and other activities at the faculty, and aids funds allocation, cost analysis and quality assurance. To achieve data security, smart cards are issued to staff members. They provide storage of personal secret keys for data encryption and electronic signature generation while communicating with the database. The system has been updated and expanded for more than 10 years.

INTRODUCTION

In recent years, we have observed a paradigm shift from university as a place of intellectual challenge to university as a complex enterprise – competitive, cost-effective, agile and responsive to the changing needs and expectations of society. Universities have to provide diverse academic services to a large number of people who are involved in a variety of activities (teaching/learning, curricula development, research), as well as non-academic campus services and facilities. Operation control of such enterprise requires efficient management of extensive organisational knowledge and information. This would be unthinkable nowadays without a database system or a network of local databases (more or less) seamlessly connected to each other. Much of the information stored includes users' individual data, such as personal information, marks acquired by students or staff salaries. Such sensitive information should not be disclosed to unauthorised persons. Thus users transfer the information to the database and read it from the database through secure communication channels. To make the channel secure, the user must be identified by a unique ID code, used e.g. to encrypt the information and/or attach an electronic signature to the data chunks [1][2]. These days typically authorisation is carried out with the use of a plastic smart card which provides suitable storage and cryptographic support.

This paper provides information about the architecture, functions and implementation issues of the Students' Electronic Card system developed at the Faculty of Electrical, Electronic, Computer and Control Engineering at the Technical University of Łódź (EECCE-TUL), Poland. The system is an extensively verified working example of a vital, widespread and still growing application of its type designed for the support of management of a very complex enterprise – a university.

PROJECT BACKGROUND

The need to introduce electronic documentation was already well-recognised at the Faculty in the mid-nineties. The four-fold increase in the number of students in just a few years (to about 4,500 students, which made the EECCE the largest TUL faculty) posed many organisational problems for academic and administrative staff. The first attempt to aid the management of teaching information at the Faculty was the idea of issuing an *electronic academic record book* to each student in the form of a plastic card with her/his photo for visual identification, and a digital memory of capacity sufficient to store all necessary data for the duration of the study period. At the beginning of each semester, the card would be loaded at the dean's office with a list of courses to be completed by a student and at the end of the semester, corresponding marks would be entered by teachers. This concept was first considered in 1996 to 1998 and, it was hoped, it would break a data transfer bottleneck happening at the turn of any two semesters. This card was to be carried in a pocket of the paper *academic record book* (which cannot be eliminated due to Polish national regulations). Teachers were required to write the marks both into the paper book and the card memory, the latter with the use of a

card reader connected to a computer. Prototype card readers and software modules were designed, developed and used for tests which confirmed the technical feasibility of the system. After assessment of the investment, material and exploitation costs of the solution, accounting for the size of the Faculty (4,500 students and more than 450 faculty and administrative/technical staff), the basic assumptions concerning the system concept were modified [3]. A decision was made that marks would be stored in a common Internet database accessed by teachers and administrative staff, and microprocessor cards would be issued to them only. Main function of the card was the storage of user identification data, and private keys used for the encryption and digital signature of the data exchanged between the Internet database and the system terminals [4]. Based on this concept, a complex faculty information processing system was developed and expanded, which now involves students (with no authorisation to write the crucial data into the database, yet). It is envisaged that wide introduction of electronic student ID cards will allow the granting of students the right to enter various data, make payments, etc, while maintaining data security.

SYSTEM ARCHITECTURE

The architecture of the system, with teaching information flow, is illustrated in Figure 1. All the information collected in the Faculty is stored in a single Internet database. The Oracle 10g database management system was selected for the TUL EECCE computer *Students' Electronic Card* (SEC) system design [5]. The SEC system users save the information to, and retrieve it from, the database by means of terminals – computers equipped with a card reader and specialised software. In the case of the management of information related to teaching, as illustrated in Figure 1, there are 4 types of terminals – study programs terminal, dean office terminal, teaching unit (i.e. department or institute) terminal and teacher terminal. Other terminal types are used to collect and/or process information related to research, cost analysis of the Faculty's activities, card management, etc, as will be discussed shortly.

A student portal, which is in fact a web application, is also integrated with the system, as shown in Figure 1. Two secure interfaces/channels that synchronise two separate data sets have been developed. A set of data which is frequently updated (e.g. lists of obligatory and elective courses, partial and final marks, dean's decisions, financial data) is fetched online directly from the central Oracle database.

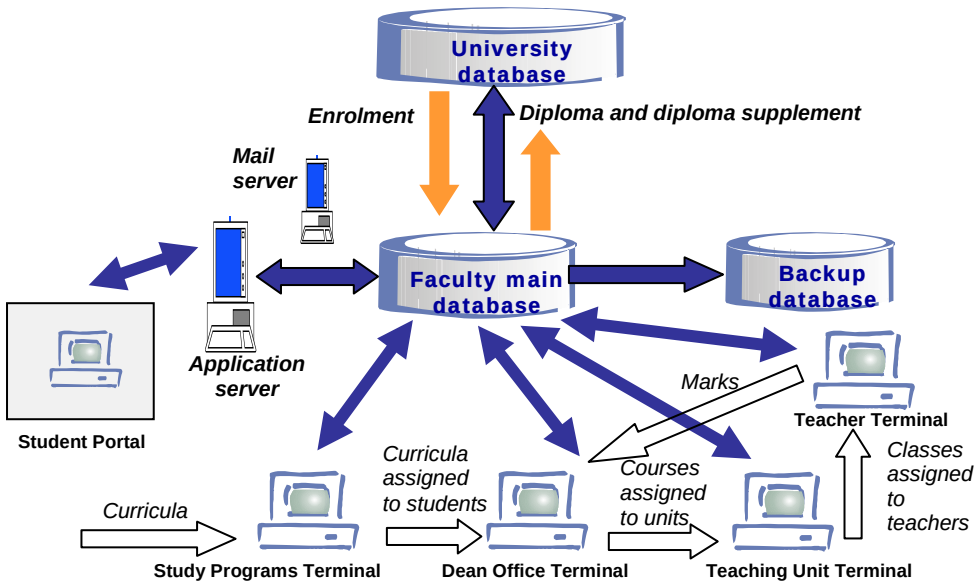


Figure 1: SEC system architecture with an example of teaching-related flow of information.

The data undergoing occasional modifications (e.g. student and teacher personal data, curricula, contact details, etc) are buffered in a Postgres database and synchronised twice a day to the main Oracle system. Students can browse their personal data (marks, enrolment in consecutive semesters, fees due and paid, etc) after logging in to a password-protected portal. An important function of the student portal is in teaching quality assurance by collecting students' answers to questionnaires on courses, teachers and organisation of studies. Thanks to the portal integrated with the information management system, more than 80% of the students give feedback to the Faculty on important aspects of the study. In the future, once electronic student ID cards are issued also to students, the functionality of the student portal will be extended to e.g. electronic submission of study-related documents to the dean's office.

DATA SECURITY

The means of data protection built into the SEC information management system include: limited access to data (user authorisation required, many user types defined with access right restrictions); protection of the data content from unauthorised reading (encryption); and measures of checking data integrity and authenticity (digital signature). The

basic tool of information protection is the microprocessor card. Hybrid microprocessor cards Gemplus MPCOS-EMV R5 8,000 (8kB) with Mifare contactless module (1kB) are currently used in the system [6][7]. They are used to store a) user identification data, b) cryptographic keys, c) electronic purse files, and d) access control information. Access to the smart card is protected by a secret personal identification number (PIN). Data written in to the database are encrypted and signed digitally [1][2].

The use of electronic cards introduces a very high data security level, which practically makes data eavesdropping or modification by unauthorised users impossible. No security-related incidents have been observed since the deployment of the system. On top of the above-described numerous security means, standard firewall technique of terminal communication with the database is used, the security mechanisms available with the Oracle DBMS are utilised and terminal communication with cards is kept secret.

A system terminal is a standard PC computer run under the MS Windows operating system, equipped with a card reader and dedicated software. An example of a card reader connected to a notebook computer through a serial USB port is shown in Figure 2. Software for the terminals was written in Object Pascal and C++ languages using Borland Delphi and Borland C++ Builder development environments respectively.

The student portal (PS) is encoded as PHP language scripts running on an Apache server. The electronic signature procedures are implemented by means of C++ and Object Pascal routines developed at the Faculty. The routines encode SHA-1 [8] and DSA [9] algorithms with the use of modular arithmetic [10]. Data encryption software modules use the TDEA (triple DES) algorithm [11].

Figure 2: Sample card reader (bottom right) connected to a PC terminal (dean's office terminal window).

Four layers of access protection to the card data files, implemented in the TUL EECCE information management system, are illustrated in Figure 3.

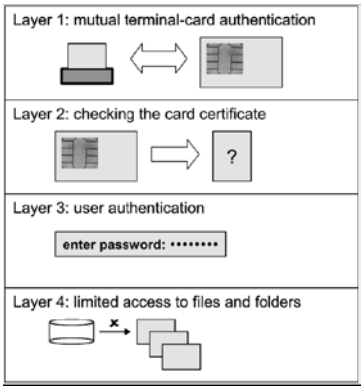
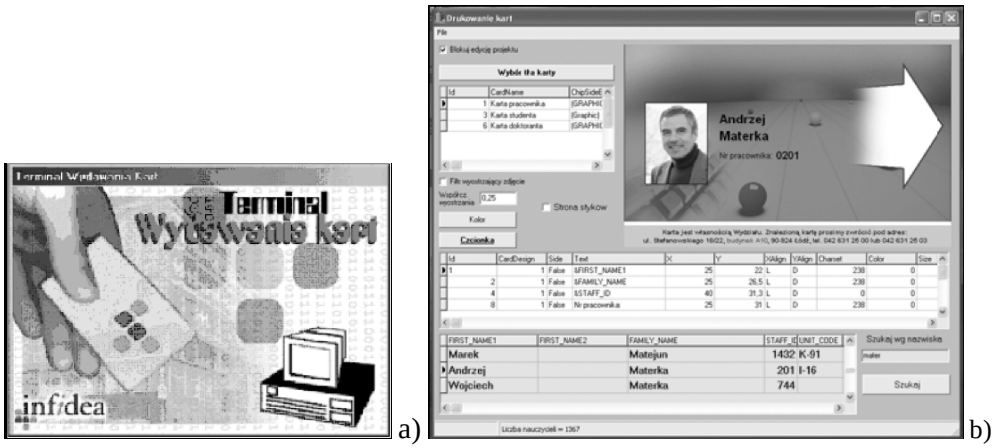


Figure 3: Layers of access protection to data stored in the card memory.

There are six user categories; each attributed different rights to access the card data files and database records – teachers, dean's office administrative staff, dean and dean deputies, teaching unit terminal operators, system administrators, and students.

A special printer is used to print the faculty- and user-related information on both sides of the white plastic cards as they come from the vendor. A card issuing terminal (TWK) is used for card personalisation. It comprises electronic encoding of data structure in the card memory, system information, user personal data and digital certificate of the card, prior to graphic personalisation (Figure 4).



a) b)

Figure 4: Logo (a) and example (b) window of smart card graphic personalisation terminal (in Polish: terminal wydawania kart – TWK).

TEACHING MANAGEMENT SUPPORT

The single-internet-database architecture (Figure 1) with terminals located in the Faculty teaching units (institutes and departments) allows for on-line assignment of teaching load and continuous verification of the assignment consistency (e.g. versus study programs) throughout the whole Faculty. For example, information about the actual number of students who have taken any subject class are easily available to a dean once teachers make proper choices from a list of student names generated by the system. After the pilot studies and initial tests, the system was put into operation in 2002, to include year 1 students, studying under the European credit transfer system (ECTS) [11]. Year by year, newly enrolled students' records were added to the database. Since 2006, the data of all the Faculty students have been stored and processed by the system. The benefits of using the system, in terms of speed of information collection and data consistency, as well as in availability of information which would otherwise not be possible to extract, are very clearly seen now. Positive evaluation made the Faculty decide to expand the system functionality to cover other strategic areas of its activity, beyond course assignment and marking.

The database in a faculty system is a rich source of information, essential to various aspects of the faculty activity. Often, there is a need to extract this information in a non-standard form, e.g. for statistical purposes. A reporting module was designed and written for this purpose (Figure 5). Various information selection criteria can be chosen from a list corresponding to the information fields stored in the database. The module dynamically generates an SQL query which is sent to the base. The result (a report generated in response) is displayed on the computer screen and can be saved as an HTML or Excel file. This unique flexibility in report generation is a very useful feature, e.g. to satisfy the needs of statistical report preparation requested by the Ministry for Science and Higher Education.

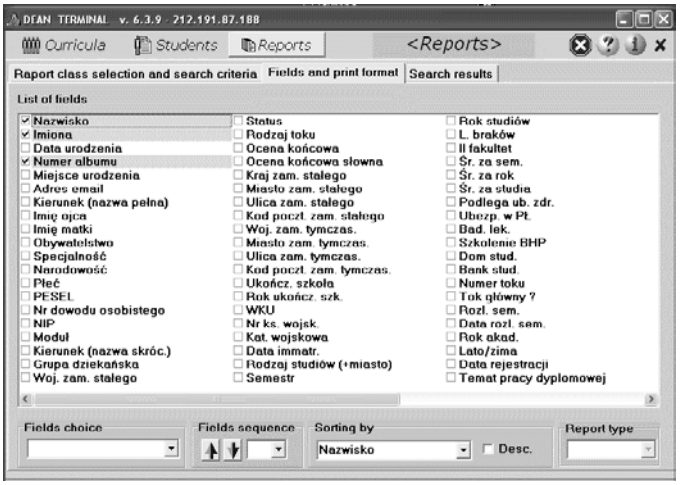


Figure 5: Example window of flexible reporting module.

One of the essential factors of faculty management is identification of various sources of costs of running the teaching process. The cost components (staff salaries, cost of overtime hours) should be evaluated and compared with the faculty income (yearly funds granted by the Ministry, student fees, etc). One can then compute average costs of running specific courses or form of studies, e.g. evening courses, part-time studies, for cost efficiency. Such data are the basis for strategic analyses, e.g. in the area of employment structure that matches the teaching quality criteria and gives maximum cost efficiency at the same time. To allow cost analysis in the SEC system, the system has been augmented

with two terminals: staff terminal (TK with *Kadry* program) and finance terminal (TF with *Krezus* program), and the functionality of the teaching unit terminal (TJD, using the *Ekstazjusz* program) has been significantly enhanced. The terminals are used to collect and process information for the cost analysis task, as illustrated in Figure 6.

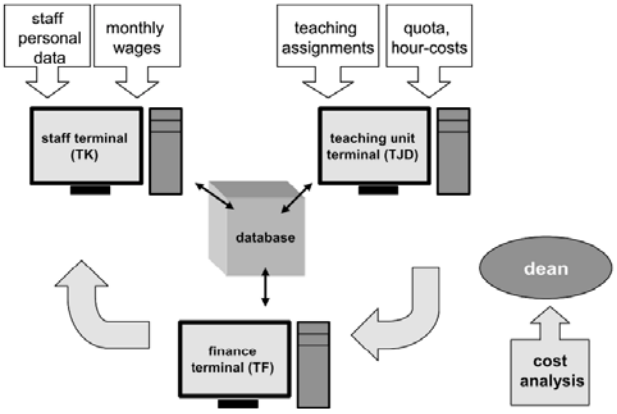


Figure 6: Diagram of information flow for cost analysis.

RESEARCH ACTIVITY TERMINAL

The architecture of Figure 1 was also adopted for a system collecting and processing information related to the Faculty research activity. A new research terminal (TBN – Terminal Badań Naukowych in Polish) was designed and implemented for the purpose, running the *Skryba* program. Depending on the user privileges (read-out from the user card), the terminal changes its interface to allow writing in the information to the database (for officers representing the faculty units, see Figure 7) or reading out the information only (for dean's office workers). The TBN terminal allows collection of detailed information about research projects/grants carried out in the institutes and departments, as well as on publications (bibliography data).

Each form of research achievement is allocated a number of points, which are used to evaluate research activity in the Faculty units. The points scored by a Faculty unit (institute or department) in a year are the basis for research funds allocation in the following year. Reports are generated, to make e.g. a list of publications for each unit, and the whole Faculty for documentation required by the Ministry for Science and Higher Education and University Library, for staff assessment, planning and other needs. A staff portal (based on an idea similar to the described above student portal) is under development now to provide individual staff members with an Internet access to their research record data. Another direction of the system expansion is in the area of card-based access control, e.g. to student laboratories. Both contact and contactless cards are considered in an in-progress Faculty project. Once electronic student ID cards are introduced within the University, they will be integrated with the existing system.

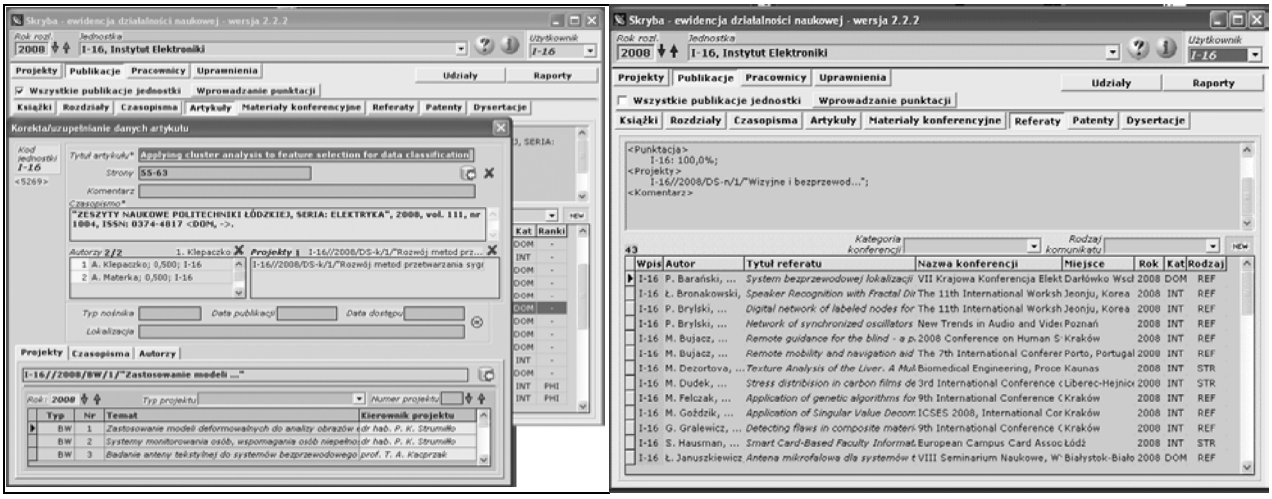


Figure 7: Sample windows for entering information on journal papers of TBN terminal (module *Skryba).*

DESIGN, DEVELOPMENT AND EXPANSION

The prototype system was designed and built between 1996 and 1998 by a seven-person team of experienced electronic engineers/computer programmers. Four of them had had previous 2-4 years' teaching and research work experience at foreign universities (USA, Australia, Japan, Great Britain), which helped to introduce the credit point study system at the Faculty. The functionality of the prototype information management system was discussed in detail with the Faculty

dean officers – the prospective users. System design and deployment required solution of many complex engineering problems (functionality specification, database design, software development user interfaces, secure card reader communication, algorithms for data encryption and digital signature) and, even more difficult, many logistic problems related to organisation of the work of different groups of users (teachers, administration, students). One of the major problems at that time was extraction of tacit organisational knowledge of many individual staff members and its conversion into explicit formal procedures appropriate for a computer implementation. For 10 years of the system's operation, its functionality has been continuously evaluated (by a formal team of nominated users), updated and upgraded by a team of a few programmers. One of the recent projects in this area is the Electronic Education Connectivity Solution, aimed at providing support to Bologna processed/governed student mobility between European universities, funded in 2009-2011 from the resources of the EU Seventh Framework Programme (FP7) [13]. Since the very beginning of the system's development, and especially after introduction of the ECTS study system at TUL in 2002, it was evident there is a need for data exchange between the University central database and faculty local systems. Since both the SEC system and the central University system keep evolving, updates of the data exchange protocols are necessary, and result in additional burden and cost. This gives incentive to integrate both systems and (probably as the major benefit) gradually introduce mature solutions implemented in SEC to all the faculties of the Technical University of Łódź (20,000 students and 3,000 staff members). The integration process is underway but it will take several years because of the number of problems that must be solved *in-vivo*, such as data migration, introduction of common procedures, functionality merging and staff training.

SUMMARY AND CONCLUSION

The core elements of the SEC information management system at the TUL EECCE Faculty are an Internet database, a number of software terminals with various functionality and microprocessor cards for the storage of users' personal information and, private keys for data encryption and digital signatures. The system ensures there is a high security level necessary for storing personal information. The database – as a single source of information – allows fast access and reduces the very high costs of verification and processing of data collected in paper form. The introduction of the system contributed much to the quality of the Faculty work. Some vital decision-support analyses were not possible at all before, e.g. detailed cost evaluation of an average teaching hour, say, at evening courses in satellite TUL campuses.

Implementation of a campus card system is a complex task, not only from the technical point of view, but also from the mainly organisational view. We found it essential that users of the university systems were involved in the process of setting system specification, testing and evaluation of new hardware and software modules. It would be very difficult for an independent external software company, with little experience in the management of a teaching and research organisation, to develop a system tailored to the needs of the Faculty. The authors hope that this paper will help in the sharing of experience by universities implementing such systems at their campuses. Since design, development and implementation are very complex tasks, we believe such information exchange is necessary. There is strong Europe-wide commitment to this approach, with an emphasis on developing standards for information exchange, especially in view of the huge diversity in the tradition of European academic institutions and the rapidly growing number of students on international exchange [14].

ACKNOWLEDGEMENTS

The authors wish to thank Anna Janisz and Krzysztof Ślot for their kind support with the design of some illustrations.

REFERENCES

1. Hendry, M., *Smart Card Security and Applications.* Boston: Artech House (1997).
2. White, G., Fisch E. and Pooch U., *Computer System and Network Security.* Boca Raton: CRC Press (2000).
3. Allen, C. and Barr, W., *Smart Cards: Seizing Strategic Business Opportunities.* New York: McGraw-Hill (1997).
4. Materka, A., Strzelecki, M. and Dębiec, P., Student's electronic card: a secure Internet database system for university management support. *Advances in Soft Computing*, Springer Berlin/Heidelberg, 64 (2009).
5. Oracle (2009), 1 February 2010, http://www.oracle.com/database
6. Ślot, K., Karta elektroniczna systemu EKN (in Polish). *Proc. 1st National Seminar Electronic University Staff and Student Cards K@Elektron*, Cracow, Poland (2003).
7. SmartCart Readers (2009), 1 February 2010, http://www.gemalto.com/readers
8. FIPS PUB 186-3: *Digital signature standard* (2009), 1 February 2010, http://csrc.nist.gov/publications/fips/fips 186-3/fips186-3.pdf
9. FIPS PUB 180-3: *Secure hash standard* (2008), 1 February 2010, http://csrc.nist.gov/publications/fips/fips180-3/fips180-3 final.pdf
10. Cormen, T.H., Leiserson, C.E. and Rivest R.L., *Introduction to Algorithms.* Cambridge, MA: MIT Press (1990).
11. FIPS PUB 46-3: *Data encryption standard* (1999), 1 February 2010, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
12. EU: ECTS Users Guide. Brussels (2009).
13. European Education Connectivity Solution (EECS) Project (2009), 1 February 2010, http://www.eecscard.eu
14. European Campus Card Association (2009), 1 February 2010, http://www.ecca.ie