ECCA NEWS

www.ecca.eu • DECEMBER 2008

2009 ECCA ANNUAL CONFERENCE

Venue: Lausanne, Switzerland

We hope you can join us for our 7th Annual Conference in Lausanne, Switzerland, from May 24th to 26th.

A word from the President

All of us in the university business do almost the same things – teaching and research. Nevertheless, we surprisingly do these in many different ways. Campus card systems are one example where we all have our own system.

This may not necessarily be bad, in the beginning of all developments everyone must explore new ways and eventually the majority finds the "main road".

ECCA's role has always been to help our members to find this "main road" with as little effort as possible. In this issue we present a few steps in that direction. We have, at last, a new website up and running which we hope will improve the service to you. Any comments are most appreciated! We also have information about the EECS project which we think is a major step in that direction. I hope you can join us at our annual conference in June 2009 where we can once again discuss and talk about the latest developments in card technology.

Tor Fridell, President, ECCA

ECCA Board Members

Contact Details

Name	Role	University	Email
Tor Fridell	Chairperson	Linkoping University, Sweden	tor.fridell@tfk.liu.se
Wolfgang Franke	Vice Chairperson	Johannes Kepler University, Linz, Austria	wolfgang.franke@jku.at
Sinead Nealon	Secretary	Waterford Institute of Technology, Ireland	snealon@wit.ie
Eugene McKenna	Treasurer	Waterford Institute of Technology, Ireland	emckenna@wit.ie
Michal Strzelecki	Board Member	Technical University of Lodz, Poland	mstrzel@p.lodz.pl
Anki Gustafsson	Board Member	Göthenburg University, Sweden,	anki.gustafsson@ped.gu.se

Log on to ECCA's New Website www.ecca.eu

We have just recently launched our new website. We hope you find it easy to navigate and if you want further information added to it please let us know. The site will be updated on a regular basis with the latest news and also information relating to our 2009 conference.

As a member of ECCA you have full access to all sections of the website. Non-members have restricted access. For some sections you will therefore be asked for a username and password. Please check the email where this information is provided. We request that members keep this information confidential and do not share such information with non-members of ECCA.

If you have any problems accessing the site please let us know.

You can contact us by email: **info@ecca.eu** or by phone: **+ 353 51 306231**

An Update on the European Education Connectivity Solution (EECS) Project

Background:

The origin of the European Education Connectivity Solution Project (EECS) has come about through the establishment of the European Campus Card Association (ECCA) in 2002. The key aim of ECCA was to introduce standards and interoperability into campus cards. After much research by the associations standards committee a decision was taken to seek funding from the EU to assist with the development of a prototype project.

In April 2008, ECCA and the EECS consortium involved submitted a funding proposal application for the first phase of the EECS project to the EU under the Framework 7 SME Programme. The initial funding application evaluation by the EU has now been accepted. The EECS project budget is based on a total cost of €1.5million with contributions from the SME consortium partners and the FP7 funding.

Purpose:

The EECS project will offer a solution to enable academic mobility within Europe by researching and developing a secure, standardised campus card system. The creation of a standardised campus card system will facilitate academic mobility by allowing Higher Education institutions to share information using a common campus card that will act as a student's "electronic key" and will enable access to a student's records on secure databases. A standardised campus card will enable more efficient electronic exchange of data amongst H.E. Institutions with the technology of the new millennium. In Europe many Higher Education institutions operate campus card systems in order to facilitate access to services for students, academics and visitors: point of sale, library access, access to classrooms/residences, printing/photocopying, etc. However, these systems operate in isolation on a stand-alone basis, providing no interoperability with other H.E. Institutions card systems due to the lack of system standards.

The core technological ambitions of the project are to:

- Facilitate the interoperability of campus systems and basic functionalities, including the transfer of student information and access to a range of fundamental campus services for students.
- Develop an information transmission interface that will translate information stored on one campus card into a common format based on European standards.
- Facilitate the secure authentication of information transfer between educational institutions.

The EECS project objectives are to:

- Research the current and potential European campus card market, current available card system technologies, current standards and existing third party IP in order to establish a set of campus card system standards that will lead to new technologies and products, facilitating interoperability and student mobility between European Higher Education Institutions as envisaged by the Bologna Declaration and the European Campus Card Association.
- Research and design modules for an EECS prototype, to include card management, client application interface, data exchange and information transmission systems, to provide interoperability between card systems and facilitate information transfer between European HE Institutions.
- Build and Test a full working EECS prototype, including the core modules of card management, client application interface, data exchange and information transmission systems. (See Fig 1. below)
- Develop a Marketing and Dissemination plan to inform potential customers of the new campus card system and to allow the SMEs to exploit the project results by increasing product awareness and generating sales leads for the partner SMEs.

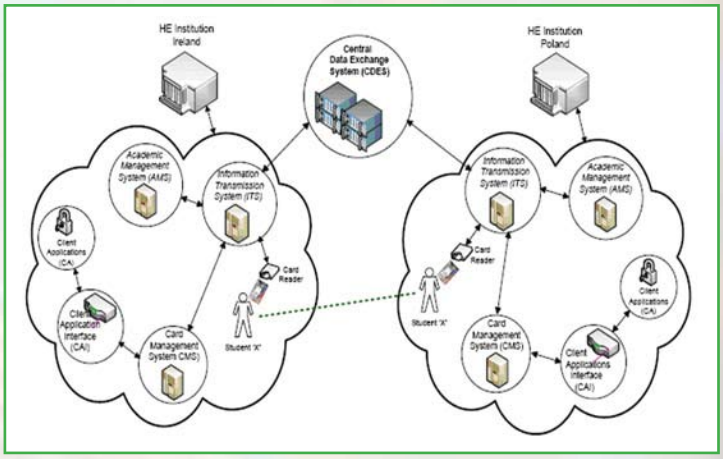

Fig 1. EECS Prototype

The above diagram describes in graphical form an outline of the EECS start to finish procedures. The example given can represent two campuses; Campus A located in Ireland and Campus B located in Poland. The following is a guide as to how the (push-pull) system will work:

(i) Student 'X' from Campus A in Ireland is required to study in Campus B in Poland.

(ii) Student 'X' requests Campus A in Ireland to transfer (push) all necessary academic and card application information required by Campus B in Poland into the Central Data Exchange System (CDES). To enable the activation of this process, Student 'X' must insert the campus ID card into the card reader of the Information Transmission System (ITS) in Ireland, where a unique security code is placed on the microchip of the card.

(iii) Student 'X' travels to Campus B in Poland, and authorises the HE institution to retrieve (pull) the relevant information from the CDES into the academic management system and the card management system as appropriate. To enable access to the information, Student 'X' must insert the campus ID card into the card reader of the ITS in Poland. The unique security code on the microchip grants the HE institution access to the required information and authenticates the transfer process.

(iv) Upon completion of study term in Poland, Student 'X' can, if required, request that all appropriate data be transferred back (push) to Campus A in Ireland. To enable this request, Student 'X' must insert the ID card into the card reader at the ITS in Poland. The appropriate data will be pushed back into the CDES. On return to Campus A in Ireland, Student 'X' can request the institution to pull the information from the CDES. Again, Student 'X' will be required to insert the ID card into the card reader at the ITS in Ireland to authenticate the process.

(v) Once the process of information transfer is complete, the unique security code on the card is removed. With the removal of the unique security code, no information can be accessed or transferred by any institution.

EECS Consortium:

The EECS Consortium consists of three European SMEs and three Academic Research Centres from four member states as follows:

SME's - OneCard Solutions, Ireland (Project Coordinators), OP Team, Poland, Mecenat, Sweden.

H.E. Institutions - University of Zagreb, Croatia, Technical University of Lodz, Poland, Waterford Institute of Technology, Ireland.

Current Status:

The EECS project is currently at the negotiation stage of the FP7-SME-2008-1 call. Negotiations are due to be completed by December 2008. Subject to approval, the project will commence on the 2nd of February 2009 for duration of two years.

Pictures from ECCA 2008 – Lodz, Poland

MIFARE Technology for Campus Cards

Establishing a suitable card technology for use in European campuses was one of the main priorities of ECCA since the Association was founded in 2002. After much consultation and research of the various options with key personnel involved in campus card services, it was agreed that MIFARE technology was the best overall solution for campus cards.

MIFARE is the industry standard for contactless and dual interface smart card and reader technology operating at 13.56 Mhz. Conforming fully to ISO 14443A – the international standard for contactless smart cards and readers – the platform consists of chip solutions for pure contactless and dual interface smart cards and reader devices. The diversity of the MIFARE product range covers low and high-end applications, which will provide campuses with a smart card technology suitable for use in a wide array of applications. These applications can range from secure ID, cashless payments, library services, time & attendance, transportation, network printing to high-end security applications, such as examination authentication, student information transfer or secure access control.

The Latest MIFARE Technology Development

The new MIFARE Plus card, which will be introduced in early 2009, can be operated in multiple security levels. The highest security level uses state-of-the-art AES (Advanced Encryption Standard) encryption based on a 128-bit key length. AES has been analysed extensively and is now the new world benchmark in encryption standards, as was the case with its predecessor, the Data Encryption Standard (DES).

The crypto architecture of MIFARE Plus will be reviewed by multiple independent parties and the chip itself is targeted to receive Common Criteria certification. In its highest security level, MIFARE Plus will not use any part of the recently hacked Crypto1 algorithm which is utilised in MIFARE Classic.

Migrating from MIFARE Classic

In order to speed up and ease the migration process for existing infrastructures based on MIFARE Classic, the MIFARE Plus chip on its lowest security level will be backwards compatible with MIFARE Classic. Cards using chips in this lowest security level can be switched to a higher security level after issuance. Once the command for this one-way switch has been given, the card will from then on only operate in that higher security level and cannot be switched back to a lower security level. The switch itself is protected by an AES key that shall be different for each card, so switching to a higher level cannot be done unless this AES-secured key is known.

When upgrading a MIFARE Classic-based infrastructure to MIFARE Plus, the issuance of MIFARE Plus cards can start from the moment that cards can be delivered and appropriate card personalization is established. After issuance, those cards will then start to work on the lowest security level (backwards compatible to MIFARE Classic). Once all readers have been upgraded to work with the higher security level of MIFARE Plus, the cards in the field can be switched as well to the higher security level without re-issuance. This can result in a much quicker transition of the infrastructure to start operation exclusively on the required higher security level.

Cost of the new MIFARE Plus Card

Although there are no real guidelines available on the cost of the new MIFARE Plus card, we should expect a price increase when compared with the MIFARE Classic card. However indications are that any increase in the cost of the new card will be small.

Is existing MIFARE Classic Campus Card Secure?

The MIFARE Standard Classic card is still and will remain a good option for campus cards. However it's important that campus card system integrators take into account whether they have implemented appropriate security measures for the use of the MIFARE Classic card. This is particularly important in applications that need security. In any scheme, it is the overall end-to-end system security that should be taken into account. The security of a system must not be restricted to the individual components. It is also essential to ensure that the individual components are used in the right way to prevent attacks on the system. Where funds are stored in a back office account as is the case with the vast majority of Campus card systems worldwide, it's relativity straight forward to provide adequate security. In the case where funds are stored on the MIFARE chip it's a more difficult task and therefore it's not a recommended system.

For the latest update on MIFARE Technology, visit www.mifare.net

ECCA Board Members

L-R: Eugene McKenna, Sinead Nealon, Tor Fridell, Anki Gustafsson, Michal Strzelecki, Wolfgang Franke.

If any of our members (Corporate or Educational) would like to include an article in our next newsletter please contact us for details.

Contact Us

If you require further information on our annual conference, the EECS project or any ECCA item please contact any board member or email us on info@ecca.eu

Tel: +353 51 302818 ✠ Email: info@ecca.eu ✠ Website: www.ecca.eu