EPiC Series in Computing

Volume 105, 2025, Pages 156–161

Proceedings of EUNIS 2024 annual congress in Athens


# A common European Student eCard

Tamas Molnar[1]

[1] Humboldt-Universität zu Berlin, Germany

tamas.molnar@cms.hu-berlin.de

**Abstract**

The Berlin Campuscard Alliance was involved in the EDSSI L2 project, where a technology demonstrator for an NFC-based student eCard was presented. As many HEIs in Europe start to think about transitioning to an ecard system, but facing high hurdles in the technology required, we decided to channel our very innovative Berlin Campuscard App development into a new project with the goal of offering European HEIs a solution for this problem. Our app contains several firsts and is one of the only apps currently in Europe, which can completely emulate the NFC technology used in smartcards by HEIs. This was accomplished by creating a ground-breaking solution, which to our knowledge has not been tried anywhere else, the cloud-based secure element.

This enables a host-card emulation with integrated security, without using the local secure-element of the device, which, because of the lack of standardization, would make testing of the app very problematic. Our solution solves this by moving this component to the server side, thereby standardizing it and making testing of the devices more manageable.

This technology in conjunction with the results of the EDSSI L2 project is the basis for the creation of a common solution for a European student eCard, which will offer students the seamless user experience when travelling from one HEI to another.

## 1 The road to a common European student eID

The Berlin Campuscard Alliance which was founded by six universities in Berlin in 2015 and was one of the pivotal partners in the development of the European Student Card initiative in the last decade. The origin of this was the development of a common ID system for universities in Berlin a very high level of automation. The development of this was finished by 2018 and with the joining of four additional institutions, it became the largest unified student ID system in Europe. Since then, we have improved this service progressively and in 2019 started to think about the next generation of student IDs, a Campuscard App.

R. Vogl, L. Desnos, J.-F. Desnos, S. Bolis, L. Merakos, G. Ferrell, E. Tsili and M. Roumeliotis (eds.), EUNIS 2024 (EPiC Series in Computing, vol. 105), pp. 156–161

One of the cornerstones of the development was the reuse of the existing infrastructure as much as possible, making the transition from physical cards to eCards in a cost-efficient fashion. In the case of Berlin, and as we later see, also for a large number of other HEIs, this means that the NFC infrastructure has to be taken into account. Currently, a large number of HEIs in Europe build their student service infrastructure around NFC, mainly on the Mifare Desfire platform, which makes transitioning to an app a challenging task.

The new Campuscard App was built around the following principles:

- The app in the fully developed phase has to be able to replace the physical plastic card completely
- The app has to be usable on Android and iOS devices
- The infrastructure is not to be modified; the app has to be created in way that the Elatec TWN4 card readers used in Berlin are able to communicate with it
- Data privacy should be the highest priority, therefore the if technologically possible, the data of the students should not be transferred to a third party.

Through these factors it became clear relatively quickly that the existing technology on the market will not be sufficient to tick all boxes, and we will have to do several "firsts" during the project.

Our approach to address these issues was twofold. Our goal in Berlin is to create an app for our Berlin Campuscard Alliance, which can replace the current physical cards one-on-one, and we aspire to develop a system, that can be reused throughout Europe.
We have therefore channeled our app development also into the EDSSI L2 project, where one of the main goals was the creation of a tech demo on TRL* Level 6 (European Commission, 2014), which has shown the feasibility of the approach for multiple HEIs throughout Europe.

# 2 The Campuscard App

The integration of the NFC components was the larger issue. The development of this feature required some very creative steps, as the current offering on the market did not satisfy our requirements.
System components, like NXP Mifare2Go (NXP, 2023) did not offer the flexibility and data privacy we set out to achieve, and also could lead to problems with financing the system on the long run, as these solutions require licensing based on the number of users per year. Such costs can get very fast out of hand when dealing with such a large system as ours in Berlin with over 100 000 users.
This meant that after inventing an automated card issuing in 2014 for the physical cards, we required a custom-made solution yet again, culminating in the development of "cloud-based-secure-element" (CBSE), which solved multiple problems, including the data privacy, but also the security.
To emulate a smartcard securely, a dedicated hardware on the device called "Secure Element"(SE) is used. This can be either a microchip hardwired to the device in "Embedded SE" or a removable piece of hardware (such as a SIM card) with similar capabilities to a smartcard. (Pourghomi & Ghinea, 2012)
2Since not every Android phone is equipped with embedded SE and a separate card is impractical, an alternative is used called "Host Card Emulation" (HCE). HCE allows routing the NFC protocol to the operating system and processing incoming NFC messages on the phone's CPU rather than in the SE. HCE is supported on all Android Phones with NFC capabilities since Android 4.4. (Google, 2023)

* Technology readiness level

The drawback of HCE is, however, that encryption secrets, that would normally be kept secure in the SE are now exposed to the operating system and can potentially be stolen.
A solution to this is a web-based SE, also called “cloud SE”. In a cloud SE all secrets are stored on a web server and are not directly accessible to the phone user or anyone else who doesn’t have server access. The Android app relays all messages from the card reader to the server, where they are decrypted, processed by the card emulation code, and the encrypted responses sent back to the app, which passes them on to the reader. During this process, no secret is ever exposed to the user or any attacker intercepting the communication.
An NFC transaction consists of several messages passed back and forth between reader and smartcard/phone in order to authenticate both sides, select an application and provide the requested data. To facilitate this exchange of messages as quickly as possible (ideally without the user noticing any delay), the CampusCard app uses a WebSocket endpoint instead of a regular HTTP REST interface, which establishes a connection between app and server only once and thus saves some communication overhead. The server interprets every incoming message as a Smartcard APDU (Application Protocol Data Unit) and processes it according to the Mifare DesFire specifications.
A more secure version of this concept relies on single use tokens instead of one universal secret:
Before every transaction, a secret is generated and shared between the web Server and the card reader. In the next transaction, this secret is used for communication by both the Card Reader and the App back-end, and is discarded afterward. (Ozdenizci, OK, & Coskun, 2016)
This way, even when the secret is compromised, it can only be used for one single transaction.
The disadvantage of this is that not only the app must be connected to the internet but also the reader’s back-end must be in constant communication with the App back-end. It is planned to implement this version when the App is used for monetary features, such as the cafeteria payment feature of the CampusCard.
The main advantage of this procedure is that the university has complete control over the data and there is no third-party system or company involved. This means that the student data and all information regarding to the use of the virtual card never leaves the service area of the card. This could have been also achieved by a traditional approach by using the local secure element of the device, as some projects like Optimos 2.0 did in the past. However, this approach would have one major problem: the secure element of android-based devices is not standardized, which requires dedicated testing for each device, which is not possible with the resources of a university.
One additional drawback remains however. Apple is prohibiting any direct access to the NFC chip in the iPhone, this solution will not work on iOS. There the only solution currently is the use of the Apple Wallet and even this service has several problems, which are currently not solved.
The most prominent problem is the inability of the standard Apple Wallet to handle multiple applications on a single virtual card. Normally a physical Mifare DESfire card can hold multiple applications, which are called by a unique application identifier (AID) for each application (service) on the card. However, as Apple currently does not support the use multiple AIDs on a virtual card, each service will require a unique virtual card in the Apple Wallet application. This is not only inconvenient when using the Wallet, but also limits the number of applications, which can be used, as the number of virtual cards in Apple Wallet is limited by the limit in the secure enclave. This limit is between 8 and 24 cards depending on the device and the iOS version. (Apple, 2024)
Apple offers products for corporate users to circumvent this limitation, especially for corporate employee badges, but this product is not available for higher education. We are as of early 2024 in talks with Apple and other companies to find a solution for this.

# 3 The European Solution

As a next step, we have started to assess the possibility to channel our highly advanced Berlin Campuscard App and the EDSSI L2 tech demo into a new project with the goal to create a European eCard App. The goal is to create a fully functional and production-ready system, which can be adapted to different requirements of different EU countries and also include the possibility to connect any local NFC-based service.

To achieve this, we are creating an initiative of large universities as the basis for further development of the system including the following tasks:

- Adaption of the system to the different legal requirements of different EU countries
- Adaption of the system to the different process requirements of different EU countries
- Creation of a standardized interface to connect the different existing card- or campusmanagement systems in different EU countries
- Translation of the platform into different languages
- Testing the system in conjunction with the different requirements

This enables European HEIs to gather the technology for the app at a fraction of the costs involved in the development of a fully-fledged app, as the groundwork with all the high costs and time-consuming development and pitfalls was done either by the EDSSI L2 project or by the development of the Berlin Campuscard App.

The app developed by the project consists of 3 layers:

- The common components, which is supplied by the Berlin Campuscard and is based on the Berlin Campuscard App and the EDSSI L2 components. These include not only the backend and the fronted of the system, but also the NFC solutions
- The national components include the technical components required for national services in a member state. This can be a payment system or any other nationwide service, which can be used by any HEI in the country. Examples are the Izzly payment system in France and the VDV eTicket in Germany
- The local components include the technical components required for local services of a HEI, which are only usable at that HEI or in that city by multiple HEIs. Example is the payment system based on the Studentenwerk system in Germany.

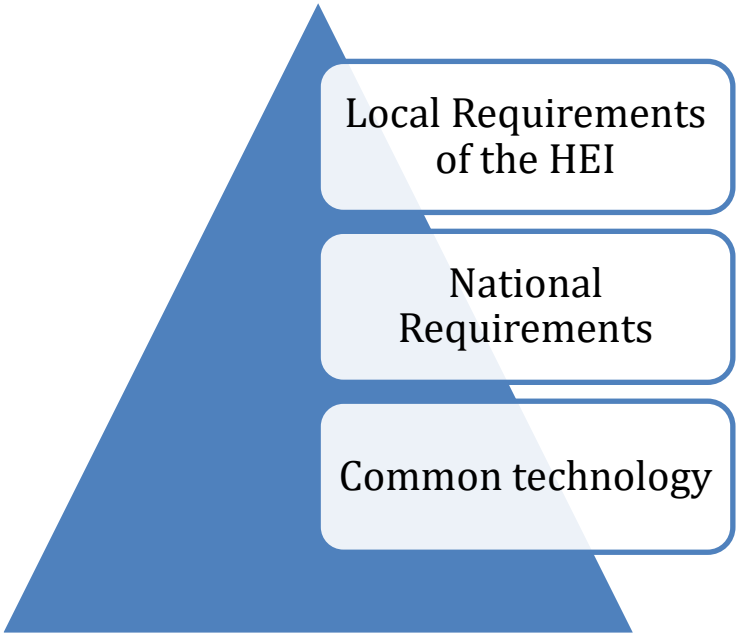


**Figure 1.** – Technology Layers of the Common European Campuscard App

The result will be a template for a European Campuscard App, which can be integrated into the local service infrastructure, creating a local "flavor" of the app, which in turn complies to all local requirements. This local version is built on the standard developed by this consortium and fulfils thereby automatically the technical requirements for the connection of foreign services, meaning that it is seamlessly compatible to the version of other institutions in the consortium.

The EU-wide combability also enables for the first time that the students can automatically use their home student ID at a foreign institution. This is theoretical currently possible with the ESC (European Student Card), however in reality this is often hampered by either a technology barrier (incomparably) or laws which only enable the use of national/local services for students with a local student ID. This is for example the case in Germany. With this solution both problems are solved. The technological barrier is overcome by the smartphone-based solution, which integrates the layer required for the services at the foreign HEI and by integration of the registration at the foreign HEI, the students have all rights with their home eCard as they would have with the plastic card of the foreign HEI.

Last but not least, the use of a smartphone-based solution has strong financial benefits for the HEIs. In comparison to a plastic card-based system, this can save the cost of the card and the printing. This makes up a large financial benefit even if the HEI has the possibility to acquire cards at a very discounted rate.

This approach will enable in the first step to roll out the new common European Campuscard System, which in turn will enable students a seamless use of their student IDs akin to the use of eduroam.

## References

Apple. (2024, 01 26). *Apple Platform Security*. Retrieved from iOS Documentation: https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web

European Commission. (2014). *Horizon 2020*. Retrieved from Horizon 2020 Annex G: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

Google. (2023). *Android Developer Documentation.* Retrieved from developer.android.com: https://developer.android.com/guide/topics/connectivity/nfc/hce

NXP. (2023). *NXP.com.* Retrieved from NXP: https://www.nxp.com/docs/en/brochure/MIFARE-2GO-LEAFLET.pdf

Ozdenizci, B., OK, K., & Coskun, V. (2016). Tokenization-Based Communication Architecture for HCE-Enabled NFC Services. *Mobile Information Systems*.

Pourghomi, P., & Ghinea, G. (2012). Managing NFC payments applications through cloud computing. *7th Internation Conference for Internet Technology and Secure Transaction* (pp. 772-777). IEEE.

VDV. (2023). *e-Ticket Deutschland*. Retrieved from https://www.eticket-deutschland.de/motics

# 4 Author´s Biography

Dr. Tamas Molnar

Dr. Tamas Molnar is the head of unit of the Service Centre Campuscard since 2015 and project manager for the Campus card system since 2011.
He has studied electrical engineering at the University of Technology in Budapest, business information systems with a focus on public IT at the Corvinus University Budapest and the University of Potsdam before doing a Ph.D. in software usability at Humboldt-Universität zu Berlin in 2014.
He worked in various IT projects parallel to his studies and was also a teaching assistant at Corvinus University Budapest. After receiving a degree in business information systems, he worked in the IT department of the Brandenburg State Forestry Institute as a software security specialist and project lead. From 2011 he works at Humboldt-Universität zu Berlin first as project manager for the student card project and later from 2015 onwards as head of unit for the Campuscard Berlin, which is responsible for the student IDs for 10 universities in Berlin.

tamas.molnar@cms.hu-berlin.de