EPiC Series in Computing

Volume 95, 2023, Pages 216–221

Proceedings of European University Information Systems Congress 2023

The Campuscard App – A secure solution to the NFC problem

Tamas Molnar[1] and Dominik Dreiner[2]

[1] Humboldt-Universität zu Berlin, Germany

[2] Humboldt-Universität zu Berlin, Germany

tamas.molnar@cms.hu-berlin.de, dominik.dreiner@cms.hu-berlin.de

Abstract

The Campuscard Berlin is the largest unified student ID system in Europe with 140 000 student IDs at ten universities. The system has been developed in house by the Service Center Campuscard at Humboldt-Universität zu Berlin with major innovations to the student ID process. As a continuation, we started to develop a Campuscard App as a next-generation solution, which should completely emulate the physical cards, so that the users only need to use their smartphones.

With the NFC-based infrastructure in Berlin in place and no way of modification, we needed to find a way to create an app, which can emulate NFC and securely communicate with the card-readers of the service providers. In addition, we had the requirement of data privacy, so that we were very much discouraged to use Google Wallet or NXP Mifare2Go if any other solution was possible.

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.

The development of our app was started in 2019, and we plan with full feature roll-out by mid-2023.

1 The Berlin Campuscard

The Campuscard Alliance in Berlin was founded by six universities in 2015 to create a standardized student ID system to supersede the obsolete paper-based IDs used by the institutions. In this project we created a self-service-based approach, where the large number of students could be handled based on a streamlined issuing process.
As there were no solutions readily available on the market for the requirements issued by the universities, we developed all the components in-house, including the complete software stack, and even the composition and design of the hardware used in the card issuing and validation terminals.

This enabled a 24/7 usable self-service approach, where the over 140 000 student IDs could be issued with only a fraction of personnel required compared to competing traditional systems. As the transportation ticket on the ID makes it a necessary to revalidate the cards each semester, we included thermo-rewrite printer-based kiosk. These machines enable the 140 000 users to print their ticket onto the card each semester and allows the universities to have an automated process, which requires very little personnel.

The development of the system was finished in 2018 and with the joining of four addition institutions it became the largest unified student ID system in Europe. Since then, we improved this service progressively and in 2019 started to think about the next generation of student IDs, a Campuscard App.

2 The Campuscard App

The development was augmented by the changing requirements because of the pandemic and by 2021 we developed the app-based student ID full steam with a roll-out for the first version planned by end of 2022.

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. In Berlin the students use their cards for 3 main NFC based services:

- Transportation ticket (eTicket)
- Payment at the canteens
- Access and identification at the library

Apart from the system behind the transportation ticket, where a smartphone solution was being developed by an umbrella organization of transportation providers in Germany (VDV, 2023), we had to create a completely new solution.
This meant that we create a project where we built an app in multiple phases, where we could address the problems sequentially. First the groundwork of the app was constructed, which included all basic features required by the app. These are the image of the card, the European Campuscard integration, and all support features.
This level was accomplished by early 2023, with the app ready for deployment. The security of the app was tested by an external audit by the company Appvisory.
This is followed by the inclusion of the eTicket functionality and the inclusion of the other two services.

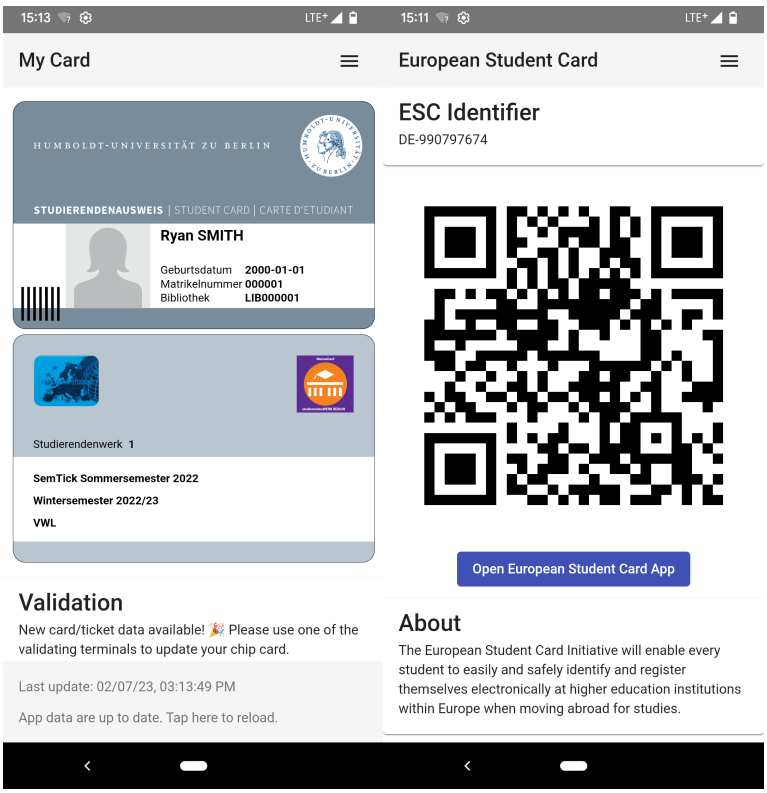

Figure 1 – Screenshots of the phase 1 of the Campuscard App

As it can be seen in figure 1, our current version of the Campuscard app (as of early 2023) has most features already integrated, apart from the NFC component, which proved to the challenge. This was

taken care of in the phase 2 of the app. The phase 2, as of early 2023 is still in beta, but it is feature complete.

3 Technical challenges and solutions

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 using Goggle Wallet or 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 both 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)

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.

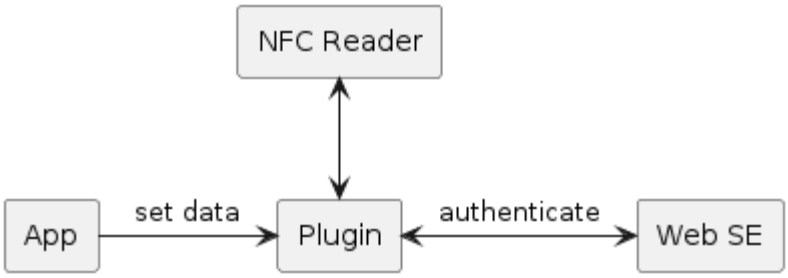

Figure 1 – Data model of the Cloud Based Secure Element

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 one is as of early 2023 that there is no launch yet for the Apple Wallet for Higher Education product by Apple in the EMEA market. This product exists since 2019 on the US market, and is used by a large number of universities, but is not available in Europe. This would however be essential to be able to integrate the NFC solutions of universities into an iOS version of the app, as any other way is restricted by Apple.
In addition, the use of a cloud-based secure element means that the device has to be online for the transaction. Normally this should not be a major issue, as most smartphone users are online at any given time, in addition university buildings have a very coverage of eduroam.

As of early 2023, we plan to roll-out the fully featured app with the complete NFC functionality by summer 2023, this will be followed by the iOS version at a later date.

Bibliography

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

Dominik Dreiner

Dominik Dreiner studied Computer Science at Freie Universität Berlin. Since 2019 he has been a developer at the Berlin Campuscard project, most recently working on the mobile app version of the Campuscard.

dominik.dreiner@cms.hu-berlin.de