

M.Sc. assignment: Secure Access Control using Mobile Phone NFC



Company: Nedap N.V. - Security Management
Website: www.nedap-securitymanagement.com
Product: AEOS – Access control system
Location: Groenlo
Start: to be defined / a.s.a.p.
Duration: 6-9 months
Compensation: ca. € 325,- /month

Contact:

dr. ir. Georgios Karagiannis (g.karagiannis@utwente.nl)

ir. drs. Tim Garthoff (tim.garthoff@nedap.com)

Keywords

Near field communication (NFC) , access control, security, protocol, wireless communication, encryption, mobile application, JavaCard, Secure Element (SE), over-the-air (OTA), RF, TMS, Webservice, Cloud

Assignment description

Design a secure solution to use NFC in mobile (phone) devices for physical access control.

NFC is a technology that provides the possibility to communicate between two devices in close range of each other. Nowadays more and more mobile devices are equipped with an NFC chipset. Nedap Security management is interested in possible solutions to use NFC in mobile (phone) devices in the field of physical access control. Instead of using an RF-badge an NFC equipped device will be used to open a door when it is presented to a wireless card reader. The existing solutions are mostly vendor-dependent. In order to obtain a secured key/credential to open a door, Trusted Service Managers (TSMs) and/or Mobile Network Operators (MNOs) are required to provide certain services. This restricts the usability of the system and increases the system cost.

The goal of this master assignment is to design and develop a secure solution for physical access control by using NFC-equipped mobile (phone) devices in a vendor-independent manor. Such a physical access control system should be secure, easy to control and manage. The following research questions need to be answered:

- Which NFC protocol need to be used between mobile device and card reader?
- What is the best model/relation between credential, person and device?
- Where (e.g. NFC device, cloud, ...) and how to manage credentials and mobile application(s)?
- How to communicate credentials in a secure way?
- Who is making the authorization decisions (e.g. door, NFC device, cloud, ...)?
- Is it needed to use an on-device secure element?
- Which mobile applications are needed (e.g. user space app, JavaCard/secure element app)?

Company description

Nedap – founded in 1929 and based in the Netherlands employs approximately 660 people world wide. Our shares are listed on the Euronext stock exchange in Amsterdam. Nedap is a solution oriented, knowledge based organization with an extensive range of products, systems and services.

As an organization, Nedap is innovative and entrepreneurial. For seven decades our success has been built on highly successful co-operation with our customers and our expertise in RFID and electronics. Our RFID systems are used in various markets to offer the end user the ultimate solution in secure and reliable identification.

The unique capability to integrate these technologies offers a high level of flexibility, user convenience and makes Nedap a truly unique solution.

Nedap is well presented internationally, with a network of business partners and local sales offices throughout the world, where staff that speaks your language can advise and support you locally.

Nedap 's security management system AEOS enters its ninth year as one of the most comprehensive amongst the leading high-end security solutions on the market today. Being the first to introduce IP-based and web-enabled integrated security management solutions, AEOS raises the bar even further by incorporating functionality for future trends and requirements. Years of experience and an impressive track record of high-end applications have by now turned new and innovative developments into proven technology.