A HCE-Based Authentication Approach for Multi-platform Mobile Devices

Luigi Manco(✉), Luca Mainetti, Luigi Patrono, Roberto Vergallo, and Alessandro Fiore

Department of Innovation Engineering, University of Salento, Lecce, Italy
{luigi.manco,luca.mainetti,luigi.patrono,roberto.vergallo,
alessandro.fiore}@unisalento.it

Abstract. Mobile devices are able to gather more and more functionalities useful to control people's daily life facilities. They offer computational power and different kinds of sensors and communication interfaces, enabling users to monitor and interact with the environment by a single integrated tool. Near Field Communication (NFC) represents a suitable technology in the interaction between digital world and real world. Most NFC-enabled mobile devices exploit the smart card features as a whole: e.g., they can be used as contactless payment and authentication systems. Nevertheless at present heterogeneity in mobile and IoT technologies does not permit to fully express potentialities of mobile devices as authentication systems, since most of the proposed solutions are strictly related to specific technological platforms. Basing on smart payment card approach, Europay, MasterCard e VISA (EMV) protocols and Host Card Emulation (HCE) technology, the current work proposes a distributed architecture for using NFC-enabled mobile devices as possession factor in Multifactor Authentication (MFA) systems. The innovative idea of the proposal relies on its independence with respect to the specific software and hardware technologies. The architecture is able to distribute tokens to registered mobile devices for univocally identifying user identity, tracing its actions in the meanwhile. As proof of concept, a real case has been implemented: an Android/iOS mobile application to control a car central locking system by NFC.

Keywords: Smart cities · Smart building · NFC · Mobile · HCE · Cloud

1 Introduction

In smart cities, advanced systems as sensing technologies and smart IoT devices, are addressed to improve and automate processes within a city [1], trying to enhance and ease citizens daily life: several real cases show that IoT technologies support added-value services for the administration of the city and for the citizens [2]. On the other hand, smart cities call for newer technical solutions and best-practice guidelines. In this regard, the presented paper analyses an innovative solution by which smartphones can be used as authentication system instead of common physical key: the smartphones can replace smart card, badges, tokens, and other long-standing, but often uncomfortable, methods of identification and security, providing to users a single mean of

A. Longo et al. (Eds.): IISSC 2017/CN4IoT 2017, LNICST 189, pp. 84–92, 2018.
https://doi.org/10.1007/978-3-319-67636-4_10

authentication, their own smartphones. Such solution has several applications in smart cities: one need only think to the buildings with access control systems based on badge. Another example is related to car sharing: the proposed solution offers a simple way to implement the car locking system that can recognise the user by means of only his smartphone, tracking also his movements during the use of the car.

Nowadays, the smartphone is clearly the collector of people's virtual social network. Nevertheless, research and industry offer exciting possibilities with respect to interaction between smartphones and the real world, mainly related to home automation and the Internet of Things (IoT) scenarios, thanks to the embedded sensors and the communication interfaces. In this sense, the smartphone is taking on the features of several daily life objects, acting as proxy for the interactions between people and environment.

Modern security systems adopt the so-called Multifactor Authentication (MFA) paradigm: authentication and security are guaranteed combining more than one method of authentication from independent categories of credentials to verify the user's identity in its mission-critical transactions. An authentication factor is a category of credential used for identity verification. The three most common categories are often described as something the user knows (the knowledge factor), something the user has (the possession factor), and something the user is (the inherence factor). Typical instances of the aforementioned factors are, namely, the password, the security token, and the biometric verification.

During the last years, several work in scientific and technical literature have focused on using mobile devices as tools for providing authentication factor facilities in MFA systems, namely [3–6].

In a mobile MFA system, NFC is the way forward: NFC Card emulation mode is well suited for mobile identification-based scenarios as possession factor [7–9]. Furthermore, NFC Card emulation mode is compatible with pre-existing smartcard-based authentication systems, at present widely distributed.

However, the widespread use of proprietary technologies in the mobile sector makes it difficult to use smartphones as universal tool for interacting with physical world. Specifically, NFC interface is not freely exploitable: iOS applications cannot leverage software tools, such as SDK APIs, to control NFC interface, and there is no way to use NFC in Apple devices, except by means of Apple Pay wallet. Moreover, NCF suffers for well-known security issues, but both industrial and research studies identified solutions for facing them [10–13]. So, there is the dire need of a solution that enables users to take advantage of such IoT technology independently from the specific smartphone platform, in order to enable the implementation of the virtual world typical scenarios in real life. As an example, Table 1 compares four recognised industrial solutions for second factor authentication system by means of mobile devices. It is worth noting that only one of them uses NFC technology and it is compatible only with Android devices. Moreover, none of them is compatible with pre-existing authentication systems.

The presented study tries to overcome the problem of using smartphones as authentication means and credential category in a mobile MFA system independently from their specific operative system and software/hardware restrictions, maintaining all the necessary security requirements. The core idea is to use the recent Host Card Emulation (HCE) technology, through which the cloud generates and distributes virtual smart card

Table 1. Industrial solutions for mobile possession factor

Product	HW	Modality	Compatibility		
			iOS	Android	Pre-existing infrastructures
SPG	BLE	Nearby	Y	N	N
Lockitron	BLE+WiFi	Nearby	Y	Y	N
Key2Share	NFC	Proximity	N	Y	N
Unikey	BLE	Nearby	Y	Y	N

to mobile devices, enabling the smartphone to use NFC card emulation mode to communicate with smart devices and identify itself emulating the virtual card received by the HCE cloud. Such approach also permits to authenticate the user throughout the NFC transactions by means of a software solution, while leveraging cryptographic processes traditionally used by hardware-based secure elements without the need for a physical secure element.

The goal of the study is to create a system that permits to a mobile application to communicate with a smart device via NFC interface, transmitting to it user data useful for its authentication by the system. As specified in the paper introduction, the main obstacle is related with iOS platforms, since for such system NFC interface control is exclusively delegated to Apple Pay wallet. On the other hand, Android OS makes available specific APIs able to totally control smartphone NFC transceiver. So, the challenge is to implement in the smart device a software component able to read and accurately interpret the instructions received from the smartphone, regardless of which is the smartphone OS between the two considered. Shortly, the original contribution of the paper relies on the fact that the created system is platform-agnostic: the designed architecture enables both Android and Apple devices to be used as authentication factor, bypassing the limit imposed by Apple devices.

Finally, the proposed architecture has been validated by means of a proof-of-concept: a prototype able to control the car locking system by means of the user smartphone as second authentication factor.

The rest of the paper is organized as follows. Section 2 describes the design of the system architecture. Here the authors analyse the software and hardware architecture model and the information flowing through it. Section 3 presents the proof-of-concept validating the architecture.

2 System Architecture

2.1 Architecture Model

The proposed system architecture consists of three main components, as clearly shown by the UML deployment diagram reported in Fig. 1: (i) a mobile application for iOS/Android able to communicate via the smartphones NFC interface, (ii) a smart device equipped with NFC transceiver, and (iii) a cloud architecture based on Host Card Emulation (HCE) approach for sharing and synchronizing of virtual smart cards among subscribed smartphones.

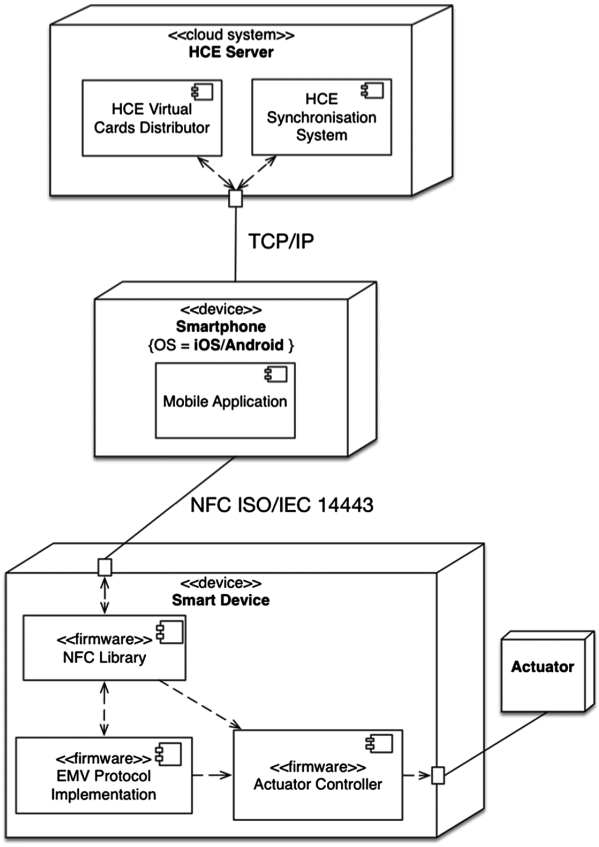

Fig. 1. Architecture deployment diagram: the mobile device authenticate itself to the Smart Device using the token provided by the HCE server and passing it through a communication channel compliant with NFC standard. The Smart Device hosts a custom implementation of EMV standard.

The main idea is based on the use of HCE technology, through which the cloud generates and distributes virtual smart card, also known as token, to mobile devices. The NFC card emulation mode allows the smartphone to emulate contactless card by means of such tokens. Another common secure system commonly used for card-emulation mode in NFC contactless transactions is the Secure Element, a chip embedded directly into the device's hardware, or in a SIM/UICC card provided by network operators, in which can be found the secure tokens and execution environment. Differently from this last, HCE moves the secure components to the cloud and avoids any hardware restriction.

As shown in Fig. 1, in the presented architecture a mobile application receives and manages the virtual card from a HCE server. More specifically, within iOS platforms such application is exclusively represented by Apple Pay wallet, while for Android platforms it can be a dedicated application also. Through the NFC card emulation mode,

such mobile application can communicate with the Smart Device using the HCE-generated virtual smart card.

In order to perform the communication with the smartphone, the Smart Device grounds on three main software modules. The first one is the interface for the communications with the smartphone. It is physically implemented on the device though a dedicated driver library aimed to interface the smart device with its own NCF antenna and to reorganise the data received from the smartphone. On the other side, there is the interface for controlling the actuator, the second module implemented within the smart device.

The third module is completely dedicated to overcome the iOS restrictions relating to the use of NFC. It is a custom implementation of EMV standard, an open-standard set of specifications for smart card payments, also known as chip cards, and payment terminals for reading them. The EMV specifics are based on various standards, such as ISO/IEC 7816 for contact cards payment and ISO/IEC 14443 for contactless cards ones. Relating to the present study, the Smart Device in the architecture embeds the implementation of the ISO/IEC 14443 standard, since it is the protocol involved in the Apple Pay wallet contactless payment processes. Therefore, in such architecture the Smart Device acts as a sort of Electronic Funds Transfer at Point of Sale (EFTPOS), which receives a payment request from the wallet and performs some resulting actions. By means of such module, the Smart Device uses payment information received from smartphone to authenticate the Apple Pay wallet users. Differently with respect to a standard EFTPOS, in this case the module does not initialize a payment process for an authenticated user, but it invokes the Actuator Controller module.

2.2 Architecture Information Flow

The Fig. 2 depicts a high-level abstraction schema that shows the information flow through the presented architecture.

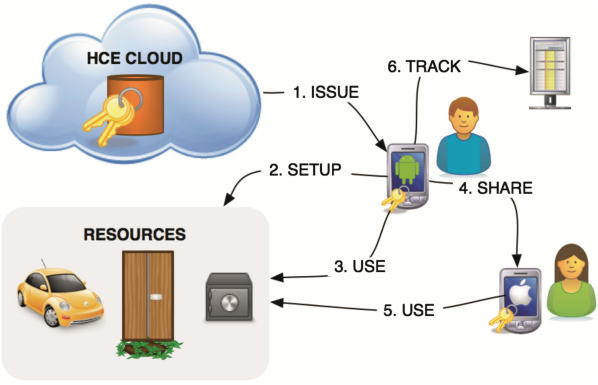

Fig. 2. Information flow describing the steps in using mobile devices as authentication factor.

The user loads his own personal information in the smartphone by means of the ad-hoc Android mobile application or the Apple Pay wallet, depending on the considered operative system. In the latter case, such information have to be strictly related to a physical smart card, since the mobile application are dealing with a mobile wallet. What matters is that, ones loaded into the smartphone, such information are transmitted to the HCE platform and they do not rely anymore on the smartphone, coherently with the required security standards.

The HCE cloud platform stores the personal information for the registered users and it generates a linked virtual smart cards, so that mapping the user/smartphone pair to the virtual smart cards exploitable for NFC communication. Next, the HCE platform provides the smartphone with the generated virtual smart card.

Once obtained the virtual smart card, the smartphone can establish a communication channel with the smart device by the NFC card emulation mode. During a first phase, the smartphone sets up the smart device to get it trusting the virtual smart card information. Subsequent smartphone/smart device communication streams are aimed to activate the bound actuator.

Furthermore, the virtual smart card can be shared among users, so that sharing the access to the physical resources and the cloud architecture can keep trace of the whole actions performed by user, by means of a synchronizing service.

3 Proof of Concept

The presented study proposes a HCE-compliant cloud architecture that permits to convert the Android and iOS smartphones into a strong user authentication means. In order to validate the architecture, a mobile application system for controlling the electric door locking mechanisms in building and automotive areas by means of the smartphone has been realised.

According as the considered operative system, Android or iOS, the prototype is composed by two different mobile applications and two HCE cloud platforms. Accordingly, the smart device embeds the firmware able to treat differently the NFC requests coming from the two OSs.

In iOS devices, as stated in the previous sections, it was necessary to use Apple Pay wallet in order to establish NFC communications with the smart device. It uses a proprietary HCE cloud platform, compliant with the described architecture.

Instead, for Android devices, an ad-hoc HCE platform and a mobile application have been created. The application aimed to send to HCE platform the user credentials and to communicate with the smart device via NFC. The HCE platform was able to receive the user credentials sent by the smartphone and to reply sending to it an access token suitable for being used during the NFC card emulation mode communications.

The smart device has been composed by an Arduino Mega board equipped with a compatible NFC expansion shield. Also, it was connected to the actuator, namely the locking motor, by means of two relays, as shown in Fig. 3.

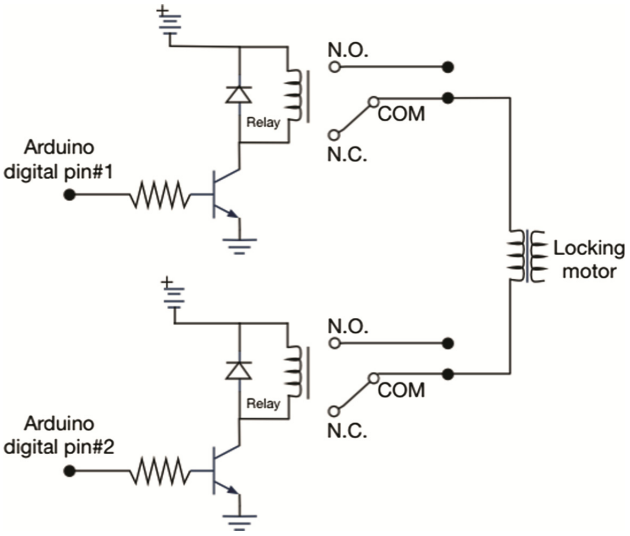

Fig. 3. Electric scheme of the connection block between the Arduino board and the locking motor

Coherently with the workflow depicted in the Fig. 2, the user authenticates itself to smart device, communicating with it by NFC card emulation mode. The smart device verifies the user identity basing on the data set during a preparation phase and, in case of success, it activates the two relays. They are disposed and connected to the circuit so

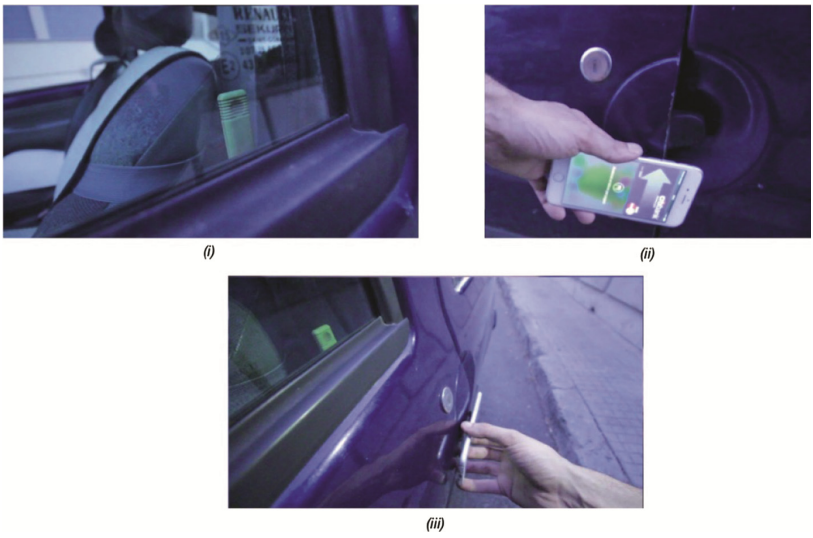

Fig. 4. Implementation of the prototype in a real case: the car locking system is not blocked (i). When the smartphone is moved closer the NFC antenna embedded in the car door (ii), the blocking system gets locked (iii)

as to be activated in a complementary manner, accordingly with the Arduino board directives: the Arduino board can activate one by one the relays according to the state of the locking motor, imposing a clockwise or a counter clockwise rotatory motion to it. In this way, two consecutive proximity communication steps between the smartphone and the smart device force two complementary motor directions, hence closing and opening the door, and vice versa.

Finally, the prototype has been implemented in a real case: the smart device was assembled in a car door and connected to the locking motor. Figure 4 shows the prototype at work by means of an iOS smartphone: when the smartphone is moved closer to the NFC antenna embedded in the car door, the locking motor is activated and the car locking system blocks or unblocks the corresponding door.

4 Conclusions and Future Work

The presented work introduced a software and hardware solution able to implement a multifactor authentication system in which possession factor is represented by the user NFC-compliant smartphone. The security token useful for the second factor in the authentication system is handed out to user mobile device by a HCE-based cloud software component. Mobile device communicate such token for authenticating the user via NFC card emulation mode, so that emulating a real smartcard.

The described strategy is compatible with both Android and iOS mobile platforms, bypassing the iOS restrictions in using NFC features. It can be also seamless integrated in pre-existing smartcard-based authentication systems, thanks to the adoption of the card emulation mode.

The model validation has included the implementation of a prototype able to control the car locking system by means of the user smartphone as second authentication factor. The experimentation showed the proper functioning of the developed solution.

The future work concern the improvement of the features for the developed HCE system by adopting the newest techniques on the cloud topic.

References

1. Hancke, G.P., de Carvalho e Silva, B.: The role of advanced sensing in smart cities. Sensors **13**(1), 393–425 (2013). Multidisciplinary Digital Publishing Institute, Switzerland
2. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of Things for smart cities. IEEE Internet Things J. **1**(1), 22–32 (2014)
3. Aloul, F., Zahidi, S., El-Hajj, W.: Two factor authentication using mobile phones. In: 2009 IEEE/ACS International Conference on Computer Systems and Applications, pp. 641–644 (2009)
4. Smith, M., Tassone, J., Holmes, D.: Method and system for providing identity, authentication, and access services. US 9076273 B2, 07 July 2015
5. Mandalapu, A., Raj, L.D.: An NFC featured three level authentication system for tenable transaction and abridgment of ATM card blocking intricacies. In: 2015 International Conference and Workshop on Computing and Communication (IEMCON), pp. 1–6 (2015)

6. Chen, W., Hancke, G.P., Mayes, K.E., Lien, Y., Chiu, J.-H.: NFC mobile transactions and authentication based on GSM network. In: 2010 Second International Workshop on Near Field Communication, pp. 83–89 (2010)
7. Adukkathayar, A., Krishnan, G.S., Chinchole, R.: Secure multifactor authentication payment system using NFC. In: 2015 10th International Conference on Computer Science & Education (ICCSE), pp. 349–354 (2015)
8. Ivey, R.G.F., Braun, K.A., Blashill, J.: System and method for two factor user authentication using a smartphone and NFC token and for the automatic generation as well as storing and inputting of logins for websites and web applications. 14/600391, 20 January 2015
9. Subpratatsavee, P., Sriboon, W., Issavasopon, W.: Automated car parking authentication system using NFC and public key cryptography based on android phone. Appl. Mech. Mater. **752–753**, 1006–1009 (2015)
10. Armando, A., Merlo, A., Verderame, L.: Trusted host-based card emulation. In: 2015 International Conference on High Performance Computing & Simulation (HPCS), pp. 221–228 (2015)
11. Cavdar, D., Tomur, E.: A practical NFC relay attack on mobile devices using card emulation mode. In: 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1308–1312 (2015)
12. Oh, S., Doo, T., Ko, T., Kwak, J., Hong, M.: Countermeasure of NFC relay attack with jamming. In: 12th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT), pp. 1–4 (2015)
13. Urien, P.: New direction for open NFC trusted mobile applications: the MOBISIM project. In: IEEE Conference on Communications and Network Security (CNS), pp. 711–712 (2015)