Winter 12-12-2015

Stakeholder Preferences for Mobile Payment Security Platforms: Understanding Trade-offs Between SIM, Embedded and Cloud-based Secure Elements

Mark de Reuver
Delft University of Technology, g.a.dereuver@tudelft.nl

Sebastiaan Blok
Delft University of Technology, jsebastiaanblok@gmail.com

Harry Bowman
Delft University of Technology, w.a.g.a.bouwman@tudelft.nl

STAKEHOLDER PREFERENCES FOR MOBILE PAYMENT SECURITY PLATFORMS: UNDERSTANDING TRADE-OFFS BETWEEN SIM, EMBEDDED AND CLOUD-BASED SECURE ELEMENTS

Mark de Reuver, Sebastiaan Blok, Harry Bouwman

Delft University of Technology, Faculty Technology Policy & Management

g.a.dereuver@tudelft.nl

Abstract

Authentication and identification for mobile payment transactions is typically provided by the secure element. While the SIM-card has long been the only option for locating the secure element, recently alternatives emerged like embedding the secure element into the device or offering it through the cloud. This paper elicits factors that influence stakeholder preferences for these three technical options. Exploratory interviews suggest a wide range of decision-making factors. Our results show that besides the basic security and performance traits of the technical options, other factors can only be understood when framing based on concepts of multisided platforms. The case of secure elements for mobile payments represents a highly complex illustration of platform competition that takes place on three different levels of the technical architecture.

Keywords: Mobile payment, multi-sided platforms, secure element, SIM-card

1 Introduction

In order to provide adequate security and prevent fraud, mobile payment solutions require a means to authenticate and identify the user. One way of doing so is storing user credentials into what is typically called a secure element. Most pilots on mobile payment use the SIM card as a secure element. The SIM, in the form of a Universal Integrated Circuit Card (UICC) can take over functions of plastic smartcards since it is able to hold a number of applications (Park, Kim, & Kim, 2008). Hence, the SIM card can be used for services such as ID cards, bank cards, bus tickets or even a security element that confirms a person's identity online without the need to introduce new hardware elements in the mobile handset (Mantoro & Milišić, 2010; Reveilhac & Pasquet, 2009). There are, however, technical alternatives. The embedded SE is a hardware module that is soldered onto the mobile handset and offers the same level of security as the SIM (Reveilhac & Pasquet, 2009). In a cloud-based solution the credentials are stored in the cloud environment of the service provider rather than on a hardware module (Pannifer, Clark, & Birch, 2014). Both solutions are capable of providing mobile authentication and identification services. As such, stakeholders currently face three different options for where to locate the secure element.

The decision where to locate the secure element goes beyond the mere technological and security traits of the three aforementioned options. Acceptance by consumers is an important issue as mobile payment solutions will not reach mass market without a critical mass of consumers (Dahlberg, Bouwman, Cerpa, & Guo, 2015; Dahlberg, Mallat, Ondrus, & Zmijewska, 2008) Similarly, standardization and reach are important conditions to reach a critical mass. In addition, collaboration issues between telecom operators and banks have been recognized as an important hurdle for mobile payment solutions (de Reuver, Verschuur, Nikayin, Cerpa, & Bouwman, 2014), hence the impact on interdependencies between actors also needs to be taken into account. Combined with the dynamics of rapidly emerging disruptive technologies, such as cloud-based or hybrid authentication mechanisms, stakeholders face a highly complex decision-making problem.

This paper attempts to understand the multifaceted nature of platform competition over the secure element for mobile payment. Specifically, we explore stakeholder preferences on whether to use the SIM card or alternative technologies for hosting the secure element. Given the complex multifaceted nature of the case, we take an exploratory approach and interview banks, telecom operators and experts.

Our paper contributes to the practical problem of where to locate the secure element for mobile payment (see also Ondrus et al 2015). Theoretically, we explore how notions of platform competition and network effects become manifest when platforms compete on different levels of the technical architecture. In addition, we compare the explanatory power of platform concepts as compared to the security and performance traits of the technologies.

This paper proceeds as follows. Section 2 provides a background on mobile payment, authentication and identification technologies as well as the three main options for locating the secure element. Section 3 details the method of the study, followed by the results in Section 4. Section 5 discusses the significance of the results along the concepts of platform competition. Section 6 concludes the paper.

2 Background

2.1 Mobile payment

Mobile payment can be defined as the use of a mobile device to conduct payment by connecting to a server, perform authentication and authorization, make a payment, initiate accounting and finally confirm the completed transaction (Antovski & Gusev, 2003; Dahlberg et al., 2008; Ding & Hampe,

2003). In this paper, we focus on proximity payments rather than remote payments. Mobile payments may be classified into those based on smart card schemes and those based on mobile smart devices (Ondrus & Pigneur, 2006). In practice this implies payments at point of sales as well as for instance transactions for public transport or access services, where face-to-face contact between buyer and seller is not necessary.

Various players are looking to dominate the advanced mobile payment market, including telecom operators, banks, credit card providers, payment providers and actors like Apple and Google (Ondrus & Lyytinen, 2011). Currently, market expectations are rising again thanks to increased penetration of Near Field Communication (NFC) on mobile phones (Juntunen, Tuunainen, & Luukkainen, 2012). NFC-enabled mobile payment uses the antenna, NFC controller and secure element located in the phone. The secure element can be integrated in the device (embedded), in the SIM card or in a micro-SD memory card. Consumers conduct payments by holding the phone in front of an NFC-enabled payment terminal. Several service models exist for mobile payment which involve different actors (Chaix /& Torre, 2012; Ondrus & Pigneur, 2006; Pousttchi, Schiessler, & Wiedemann, 2009). However, most models assume a trusted service manager (TSM) that mediates between banks, telecom operators, and the mobile payment service provider. The TSM provides the generic functionality for service deployment and authentication. The TSM can be a bank, telecom operator, payment service provider or independent organization. A TSM can be centralized or split e.g. a part is of the functionality is offered by the service provider and another part by the telecom operator. If a telecom operator is involved, the secure element of the TSM can be placed on the SIM card of the phone.

2.2 Authentication through secure element

Authentication mechanisms control whether one is granted access. In general, three ways for authentication exist (Stamp, 2011): Something a person knows (e.g. password); Something a person has (e.g. smart card); Something a person is (e.g. biometrics). Many authentication systems combine two methods, for instance payment cards require presenting the card (i.e., something a person has) and a PIN (i.e., something a person has).

A secure element (SE) combines these means partly by integrating hardware, software, interfaces and protocols in a mobile handset for secure storage (Reveilhac & Pasquet, 2009). SE should provide secure memory, cryptographic functions and a secure environment for execution (Madlmayr et al., 2007). When multiple applications are stored on the SE, they must be protected from each other and the applications should only be managed by authorized parties (Madlmayr et al., 2007).

2.3 Technology options for secure element

In this paper, we consider the three main technology options for providing a secure element.[1] A first option for locating the secure element is the SIM card, as being controlled by the mobile network operator. As SIM cards are already used to identify and authenticate mobile devices to the operator network, they could be used for hosting an SE for mobile payment as well. SIM cards can be used to identify and authenticate subscribers, store data and run and store applications. Reported advantages of the SIM card for hosting the SE include strong cryptographic calculation power and security (Chen, Mayes, Lien, & Chiu, 2011). SIM cards have been designed to be secure and tamper resistant, provide encryption capabilities for securely storing private keys and guarded by PIN and PUK codes with limited attempts (Abbott & Practical, 2002). The next generation SIM cards (referred to as Universal

[1] Although theoretically possible, in this paper we will not consider the micro-SD card option for storing the SE, as most handsets no longer have a slot for inserting a micro-SD card.

Integrated Circuit Card or UICC) can store multiple applications from both the operator and third parties. The operating system on the card prevents the applications from accessing or sharing data between them (Alimi & Pasquet, 2009). The UICC can thus be safely used for other applications such as mobile payment, loyalty cards or point-of sales transactions.

A second option is to use an embedded SE, which refers to a tamper resistant module that is soldered onto the mobile handset and offers the same level of security as the SIM (Reveilhac & Pasquet, 2009). Similar as for the SIM-based scenario, the entire application is stored on the element. The chip is embedded within the device during the manufacturing phase and must be personalized after the device is delivered to the user. As the SE is soldered onto the handset in cannot be used in a different handset. This means that the user must personalize his handset every time he purchases a new one. An example of a mobile handset with an embedded SE is Apple's iPhone.

A third option is to virtualize the SE into a cloud system. Google recently introduced Host Card Emulation (HCE) for the Android OS in which a cloud based solution can be used rather than a physical SE in the mobile handset. In this case the application is held within the operating system of the mobile phone which is called the "host" (Pannifer et al., 2014). With a cloud solution the credentials to exchange with the contact point can be stored in the cloud owned by the SP. The handset must connect to the cloud by making use of the internet after which handset will receive keys that allow using the application at a contact point. These keys are provided via an internet connection and are often provided in a limited amount with a limited validity period.

3 Method

We explore preferences for SIM, embedded and cloud-based SE through interviews with stakeholders in the Dutch mobile payment industry. The main goal of the interviews is to elicit which factors influence their preferences for one of the three options. Interviewees must be affiliated with a stakeholder in the mobile payment industry, i.e. bank, telecom operator, service provider or consultancy firm. Interviewees must at least have a working experience of a couple years within the industry. In addition, we strived for respondents with technical as well as business expertise. Interview candidates were sourced through the personal network of the authors as well as the client network of a prominent mobile payment security firm, followed by a snowballing approach. An overview of interviewees is provided in Table 1.

The interviews are based on a semi-structured approach (Table 2). As the research focuses on an industry that is subjected to change new insights might arise that have not been addressed during desk research. Interviews lasted between 30 and 60 minutes. Respondents received a brief introduction of the study prior to the interview. Interviews were recorded, transcribed and coded. We analyzed transcripts by first selecting relevant quotations on preferences for SIM versus embedded or cloud-based secure elements. Coding was initial based on open and selective coding (Glaser & Strauss, 2009), making use of clustering techniques (Miles & Huberman, 1994). Through open coding, we assigned different labels to those quotations. Next, we clustered the codes into themes through an inductive approach.

Actor role	Code	Job description
Telecom operators	MNO1	Program manager mobile commerce and payment
	MNO2	Business development manager mobile commerce
Banks	BA1	Senior product manager
	BA2	Cards and online payments manager
	BA3	Senior product manager electronic commerce
	BA4	Former program director mobile payment platform
Experts	IE1	Managing consultant identity management
	IE2	Consultant
	IE3	Managing partner
	IE4	Card scheme manager
	IE5	Business developer
	IE6	Associate professor specialized in mobile payment

Table 1. Interviewees

Topic	Question
SIM in general	What is your opinion on the function of the SIM in regard to mobile authentication and identification services?
Application markets	What do you find interesting markets to target with mobile authentication and identification services and why? Is mobile payment interesting for your company to offer mobile authentication and identification services in regard to market size, potential revenue and needed security? What do you see as requirements when offering mobile authentication and identification services to mobile payment?
Technical alternatives for locating the SE	What added-value can the SIM provide to your company in regard to mobile authentication and identification services? What technical alternatives would you consider when offering authentication services and why? What technical solution would have you preference and why? Why not another solution? What are limitations of the SIM when offering authentication and identification services on a business and organizational level? Do you see the SIM as a long-term solution for mobile authentication and identification services? What are external (technical, organizational, business, social acceptance) factors that may influence the SIM for authentication?

Table 2. Interview question list

It is important to be aware of the role and interests of respondents. A mobile operator will, for instance, have preference for a SIM-based solution, as it controls and owns this resource. So, when comparing the different alternatives, it is key that the background of the respondent is taken into account, as it could lead to a biased view. This is an important reason for interviewing experts that have a different, often more neutral background. Based on the interviews, a comparison between the alternatives has been made to generate an overview of the unique characteristics of SE solutions.

4 Results

First, interviewees suggest a number of technology-related factors that influence their preferences on where to locate the secure elements. Regarding security issues, several interviewees argue that hardware components, like the SIM, are generally more secure than software components, like cloud-based SE [BA2, BA3, IE4]. Hardware components are generally more difficult to alter or to infect

with malware. In addition, the process of issuing SIM cards reduces risk of fraud since consumers have to identify themselves face-to-face. While security is an important issue, some bank representatives questioned whether micropayments of fewer than ten euros actually require strong security in the first place.

Regarding performance issues, SIM cards are superior to embedded and cloud-based solutions as they work even without Internet connectivity or battery. Interviewees also expect SIM-based solutions to perform better since they would be more mature than cloud-based solutions. A downside is that SIM cards have insufficient memory for storing applications, requiring a so-called SIM swap, i.e. replacement with UICCs. Interviewees also argued that upgrading hardware is generally more difficult than software.

For any mobile payment solution, broad acceptance from consumers as well as merchants is required. On the one hand, consumer acceptance of SIM-based SE might be higher since consumers will also be able to switch to another device manufacturer without having to change their mobile payment subscription. On the other hand, cloud-based solutions might lead to more control for the consumer and customer lock-in will be limited. With cloud-based solutions a consumer can change more easily from handset or phone subscription without the need to go through a difficult provisioning process. Next, to that a cloud-based solution will offer the possibility to facilitate a payment application over multiple machines [IE2], which could be relevant if for instance tablets, smart watches or smart car solutions would be used for payments. One of the experts said that there is a mismatch between the life cycle of the handset and authentication means [IE5]. Authentication means are used over a longer period than a handset or a phone subscription. For example, the expert [IE5] commented that a credit card has a validity of a number of years while most phone subscriptions are only valid for one or two years.

SIM-based solutions provide high reach and installed base since they work in any mobile phone regardless device brand or operating system. In contrast, relying on embedded SE implies fragmentation of the market due to the variety of handsets [MNO1, MNO2, BA2, BA3, IE1, IE4, IE3]. A representative of a bank mention, that *"the embedded SE differs per supplier and per handset. The embedded SE can even differ per version, for instance not all Samsung Galaxy S6 have similar embedded elements. This means that adjustments to the payment application have to be made per device. As the SIM is standardized, we see it as an easier solution for mobile payments"* [BA3]. As such, the SIM card is a more standardized solution with a high reach and installed base.

Dependency was another recurrent theme in the interviews. While cloud-based solutions can be hosted by the service provider or bank in-house, SIM-based solutions imply dependency on operators. One of the respondents stress that "*banks want to stay in control and want limited dependence of other parties, especially if they come from a different sector [like telecommunications]"* [BA2]. Dealing with multiple operators is required to gain sufficient reach in a country, which creates coordination issues and complexity. Interviewees did not agree on whether they would rather depend on operators or on device makers. Embedded SE solutions imply dependency on device makers, and interviewees did not agree whether they would prefer to be dependent on operators or on device manufacturers.

Costs are another important issue as margins in the payment industry are low [BA1, BA2 BA3, IE3]. Several respondents argued that SIM based solutions are too expensive or at least have been overpriced in the past. According to different respondents, the MNOs have overestimated the value of the SIM, as they wanted their own mobile wallet and a fee per payment transaction [BA1, BA3, BA4]. Other interviewees, especially those from telecom operators, argued that their pricing models have been reduced dramatically in order to remain competitive with alternative solutions. "*We started a new trend as we have lowered the price of the SIM. We don't want that our customers base their decision on costs and therefore we want to offer the SIM for the same price as the costs for a HCE solution. Next, to that banks will be allowed to issue their own mobile wallet. Banks should really look at what they find the best technology and we are confident that the SIM scores well on this"* [MNO1]. Another issue that could lead to high costs is that a SIM swap is needed to facilitate authentication services

[MNO1, MNO2, IE6]. Most of the SIMs that are currently deployed in the market cannot meet the requirements needed to facilitate mobile payments. A SIM swap is an extensive and expensive process.

A hurdle for using SIM-based SE that may be specific to the context of the research is the lack of trust in operators. Several bank interviewees argued they no longer trust telecom operators in their offerings. Telecom operators were generally referred to as difficult to collaborate with and too focused on short-term profits. Especially since recent collaboration initiatives with telecom operators has largely failed (e.g. the Travik initiative), banks and service providers had little confidence in renewed collaboration with operators. Banks focus more on customer retention while MNOs are more sales driven organizations [BA1]. One expert [IE6] says, "*there are many examples of failed attempts of MNOs to extend their business. MNOs believe in control to create value and this mind-set is a barrier when entering a new market."* Another argues that "*MNOs have overplayed their hand in the past, as they wanted maximum profit at the expense of the bank's business model"* [BA1, IE2, IE3].

A final observation is that several respondents indicated it is too difficult to make a trade-off between the SIM card and the two alternatives. They observed that stakeholders are experimenting with all three options at the moment. One independent expert commented that there are simply not enough example cases to base a decision upon. Respondents also clearly indicated that they simply expect that new alternatives will come up and that cloud-based solutions will evolve. As such, most interviewees from other actors than the operators indicated they are not yet willing to make a choice between the technologies. Furthermore, the world of mobile payments is changing so fast as new technologies are introduced to the market that a solution that is implemented now must be seen as short-term as new technologies are constantly introduced to the market [BA1, BA3].

Findings are summarized in Table 3.

Issue	Advantage of SIM	Disadvantage of SIM
Security	Hardware is generally more secure than software[2] Lower chance of fraud due to linkage with person	SIM can get lost or removed from handset Micropayments might not require such strong security
Performance	SIM does not need Internet connectivity or battery SIM more mature solution than cloud-based solutions	SIM has insufficient memory to store applications, unless replaced by UICC Hardware more difficult to replace and upgrade than software[2]
Consumer acceptance	Easier to switch device brands[1] SIM is a very personal technology	Less easy to switch operator Mismatch between lifecycle of handset / subscription and lifecycle of payment mechanism Cloud-based SE works even when switching operator or device[2]
Reach	SIM works on any device brand, thus offering higher reach and installed base[1] Operators are better organized than hardware providers SIM works with any operating system, thus offering higher reach and installed base[2]	SIM solutions only work within one specific country
Issue	Advantage of SIM	Disadvantage of SIM

Dependency	Operators are more accessible than foreign device makers	SIM implies dependency on operators Dealing with multiple operators is too complex International operators are difficult to influence
Costs	SIM becoming less expensive due to threats of new technologies	SIM too expensive Business conditions from operators are too diverse
Trust		Banks no longer trust telecom operators Telecom operators have image of being difficult to collaborate with Past collaborations with telecom operators failed because too expensive and want to own the wallet brand
Uncertainties		Cloud-based solutions may become more secure in the future[2] New alternatives will come up in the future Too many technologies to make a choice Banks work on different solutions Too few actual implementation cases to judge

Table 3. Reported pros and cons of SIM based secure element
[1] = Only applies to SIM versus embedded SE; [2] = Only applies to SIM versus cloud-based SE

5 Discussion

As mobile payment technologies are only valuable once adopted by a critical mass of consumers and of merchants, by their very nature mobile payment technologies exhibit characteristics of multi-sided platforms (Gawer, 2011). As such, understanding the dynamics and evolution of such multisided digital platform is already complex in its own right (Tiwana, 2013). We find several factors in our analysis that can be framed from a multi-sided platform perspective. Consumer acceptance is generally considered important, including lock-in, switching costs, and flexibility to change handset and operator brands. Even more important in the interviews anticipated reach, which is required to create network effects, was speculated about. Respondents clearly indicated they would only accept solutions that can be used by a majority of users, thus requiring a broad reach of handset brands and operators.

Although these issues are common to platform theory, in this specific case, the three competing platform technologies are on different levels of the technical architecture: the device itself (i.e. embedded SE), the operator-controlled part of the device (i.e. SIM), and the cloud (i.e. cloud-based SE). Understanding the dynamics and preferences for the three competing platform technologies thus involves different dynamics and interdependencies. Whereas the attractiveness of embedded SE depends on such things like fragmentation of the device market, the attractiveness of cloud-based SE depends on the diversity of operating systems. As such, the case of where to locate the secure element of mobile payment exhibits a rather peculiar case of platform competition, where actors that normally compete (e.g. telecom operators) have to collaborate (e.g. to offer a standardized SIM-based solution) and actors that normally collaborate (e.g. telecom operator and device manufacturer) now have to compete (e.g. by offering competing solutions).

Two major themes emerging from the interview analysis are dependencies of banks and service providers on operators and the associated lack of trust between parties. From a resource dependence perspective (Pfeffer & Salancik, 1978), it is predicted that actors will always try to minimize their dependence on others in order to limit external control. As such, the preference for cloud-based SE can

be understood since they can, in principle, be hosted in-house by banks and service providers or outsourced to IT providers that they can control directly. Interestingly, interviewed banks especially indicated that they find operators do not understand their core values (i.e. brand identity) and business logic (i.e. low margins, focused on retaining customers in a defensive fashion). Combined with bad experiences in collaborative platform projects in the past, these observations explain why banks are reluctant to be dependent on operators and therefore opt for none SIM based solutions.

6 Conclusions

This paper shows the complexity of factors that influence decision making of stakeholders about where to locate the SE for mobile payment. From a technical perspective, SIM-based SE appears to be superior to embedded and cloud-based SE in terms of security as well as performance traits. While most respondents expect cloud-based SE to evolve and improve in the future, currently SIM-based authentication is considered more secure, more reliable and less prone to identity fraud. Despite these straightforward results, the interviews clearly indicate that stakeholders are in much doubt on which SE solution to choose. Banks and service providers are experimenting with all three technical alternatives for locating the SE, and several interviewees indicate their doubt on what to choose or recommend. As such, it must be that other factors than the pure technological traits are needed to explain preferences of stakeholders for SIM-based versus embedded and cloud-based SE.

In this paper, we attempt to elicit a wide range of factors rather than to make inferential claims on commonly shared opinions among stakeholders. Although we had only twelve interviewees, we did find similar patterns in the interviews, indicating a certain degree of saturation. A limitation of the paper is that we treated the cloud-based models as one single group, and did not differentiate between the approaches from Google versus Apple. Future research could take a more fine-grained perspective and differentiate how stakeholders perceive the different models.

A validity threat could be bias towards interviewee's business interests. We did find that, unsurprisingly, operators were generally more favorable about SIM-based solutions than other groups of respondents. At the same time, especially the discourse of the operators showed several fragments of what might be touted wishful thinking or at least insufficiently justified claims. By incorporating the perspectives of banks as well as external industry experts, we ensured a diversity of perspectives. In our future research, we will nevertheless address this validity issue by triangulating the findings in this paper with those in other studies where we used analytical hierarchy processing as well as correlational studies. Such more confirmatory approaches will also help to prioritize the broad set of factors that were elicited in the current exploratory study.

References

Abbott, J., & Practical, G. (2002). Smart cards: How secure are they. *GSEC Practical v1, 3*, 2-18.

Alimi, V., & Pasquet, M. (2009). *Post-distribution provisioning and personalization of a payment application on a UICC-based Secure Element.* Paper presented at the Availability, Reliability and Security, 2009. ARES'09. International Conference on.

Antovski, L., & Gusev, M. (2003). *M-payments.* Paper presented at the Information Technology Interfaces, 2003. ITI 2003. Proceedings of the 25th International Conference on.

Chaix, L., & Torre, D. (2012). Which economic model for mobile payments?

Chen, W.-D., Mayes, K. E., Lien, Y.-H., & Chiu, J.-H. (2011). *NFC mobile payment with citizen digital certificate.* Paper presented at the Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on.

Dahlberg, T., Bouwman, H., Cerpa, N., & Guo, J. (2015). *M-Payment-How Disruptive Technologies Could Change The Payment Ecosystem.* Paper presented at the European Conference on Information Systems, Munster, Germany.

Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications, 7*(2), 165-181.

de Reuver, M., Verschuur, E., Nikayin, F., Cerpa, N., & Bouwman, H. (2014). Collective action for mobile payment platforms: A case study on collaboration issues between banks and telecom operators. *Electronic Commerce Research and Applications*.

Ding, M., & Hampe, J. F. (2003). Reconsidering the challenges of mpayments: A roadmap to plotting the potential of the future mcommerce market. *BLED 2003 Proceedings*, 49.

Gawer, A. (2011). *Platforms, markets and innovation*: Edward Elgar Publishing.

Glaser, B. G., & Strauss, A. L. (2009). *The discovery of grounded theory: Strategies for qualitative research*: Transaction Publishers.

Juntunen, A., Tuunainen, V. K., & Luukkainen, S. (2012). Critical business model issues in deploying NFC technology for mobile services: case mobile ticketing. *International Journal of E-Services and Mobile Applications (IJESMA), 4*(3), 23-41.

Madlmayr, G., Dillinger, O., Langer, J., Schaffer, C., Kantner, C., & Scharinger, J. (2007). *The benefit of using SIM application toolkit in the context of near field communication applications.* Paper presented at the Management of Mobile Business, 2007. ICMB 2007. International Conference on the.

Mantoro, T., & Milišić, A. (2010). *Smart card authentication for Internet applications using NFC enabled phone.* Paper presented at the Information and Communication Technology for the Muslim World (ICT4M), 2010 International Conference on.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*: Sage.

Ondrus, J., & Lyytinen, K. (2011). *Mobile Payments Market: Towards Another Clash of the Titans?* Paper presented at the Mobile Business (ICMB), 2011 Tenth International Conference on.

Ondrus, J., & Pigneur, Y. (2006). Towards a holistic analysis of mobile payments: A multiple perspectives approach. *Electronic Commerce Research and Applications, 5*(3), 246-257.

Ondrus, J. (2015). Clashing over the NFC Secure Element for Platform Leadership in the Mobile Payment Ecosystem, Proceedings of the 17th International Conference on Electronic Commerce (ICEC), Seoul, South Korea, 3-5 August.

Pannifer, S., Clark, D., & Birch, D. (2014). HCE and SIM Secure Element: It's not black and white. Guildford: Consult Hyperion.

Park, J., Kim, K., & Kim, M. (2008). *The Aegis: UICC-Based Security Framework.* Paper presented at the Future Generation Communication and Networking, 2008. FGCN'08. Second International Conference on.

Pfeffer, J., & Salancik, G. R. (1978). *The external control of organizations: A resource dependence perspective*: Stanford University Press.

Pousttchi, K., Schiessler, M., & Wiedemann, D. G. (2009). Proposing a comprehensive framework for analysis and engineering of mobile payment business models. *Information Systems and E-Business Management, 7*(3), 363-393.

Reveilhac, M., & Pasquet, M. (2009). *Promising secure element alternatives for NFC technology.* Paper presented at the Near Field Communication, 2009. NFC'09. First International Workshop on.

Stamp, M. (2011). *Information security: principles and practice*: John Wiley & Sons.

Tiwana, A. (2013). *Platform ecosystems: aligning architecture, governance, and strategy*: Newnes.