6-2014

Mobile contactless payments adoption challenge in the complex network actor ecosystem

Mario Silic
University of St Gallen, Switzerland, mario.silic@student.unisg.ch

Andrea Back
University of St Gallen, Switzerland, andrea.back@unisg.ch

Christian Ruf
University of St Gallen, Switzerland, christian.ruf@unisg.ch

27th Bled eConference

eEcosystems

June 1 - 5, 2014; Bled, Slovenia

Mobile contactless payments adoption challenge in the complex network actor ecosystem

Mario Silic
University of St Gallen, Switzerland
mario.silic@student.unisg.ch
Zagreb School of Economics and Management, Croatia

Andrea Back
University of St Gallen, Switzerland
andrea.back@unisg.ch

Christian Ruf
University of St Gallen, Switzerland
christian.ruf@unisg.ch

Abstract

Mobile contactless payments (MCP) technology brings an important dual use dilemma where consumer adoption can be halted if consumer is not fully persuaded that the security risk behind the technology use is very low. Currently, although many projects on the implementation of MCP solutions have commenced, MCP is still not picking up. Why? To fill this research gap and better understand how security is affecting MCP implementation, we employ triangulation approach to understand if security is the main obstacle to further adoption and extension of MCP solution. The results reveal that consumer security is the crucial factor in a successful MCP implementation. Our result offers important and new insights for practitioners as it provides a security dimension to consider in the entire contactless payment ecosystem.

Keywords: NFC, contactless paymen, information security, mobile, MCP

Prelude

Yves is one of 4 million people that have smart phone equipped with NFC technology and can use contactless mobile services in France through Cityzi France project. Yves is also a frequent user of public transport in Nice where he can pay his ticket using contactless mobile service. But he is never using it. Why? Is he afraid of doing so or is it simply because he does not know how to do it?

On the other side of the planet, in San Francisco, two researchers, Corey Benninger and Max Sobell, from the Intrepidus Group have developed an app called UltraReset which takes advantage of NFC vulnerabilities in the systems used by many public transit systems, including the New Jersey Path and San Francisco Muni trains where it was tested effectively. Using any Android phone with NFC capabilities the UltraReset app can take a train card with zero rides, and refill it repeatedly, for free.
...Maybe Yves is aware of the above...maybe not...nevertheless, question remains: is security responsible for the NFC mobile payments failure?

1 Introduction

Smartphones and other mobile devices become more and more powerful and achieved a substantial market penetration coupled with a decreasing price for such devices. A comparable development is also evident for wireless network technology; transfer rates and network coverage are increasing and prices for wireless data transfer contracts and other services decrease constantly. This has led to a situation in which a large majority of the population owns high-end mobile devices with the capabilities to access the Internet independently of their location. Other technologies, which extend the functionality of mobile devices, such as Near Field Communication (NFC), have also reached a substantial maturity level (Ming 2011; Ondrus and Pigneur 2007). Through combining these technologies, smartphones and NFC, novel mobile services, such as mobile contactless payment (MCP), can be realized. Several studies (Au and Zafar 2008; Dahlberg, Mallat, et al. 2008a; Hu 2008; Ondrus and Pigneur 2006, 2008; Pousttchi 2003) conclude that the benefits of MCP are far-reaching. On the one hand, MCP allows a faster and more convenient payment process at the point-of-sale, and on the other hand, it is capable of supporting additional customer services, such as digital membership cards. However, while the technology has made great advances and is capable of a nation-wide MCP service (Ondrus and Pigneur 2007), the industry is still caught in a series of more or less successful trials.

This inefficient series of trials in the implementation of MCP services has motivated information systems researchers (ISR) to identify the specific obstacles to MCP. Several studies conclude that the success of MCP implementation does not depend primarily on technological aspects, but on the complexity of the necessary collaboration between different organizations (Dahlberg, Huurros, et al. 2008a; Ondrus et al. 2009; Sammer et al. 2012). A study by (Ondrus et al., 2009) summarized the current state of the art and analyzed three failed MCP projects in Switzerland, concluding that the first necessary step for a successful MCP implementation is to develop interorganizational relationships (IOR). The important role of IORs is also confirmed by another study (Sammer et al. 2012), which reports evidence that some market actors, which are necessary for the implementation of mobile contactless payment services, are even actively hindering the development of MCP services. Research further suggests that the

organizational culture of the concerned organizations is an important factor (Cadden et al. 2010; Steensma et al. 2000).

However, none of the above factors do really explain why MCP solutions are not picking up. There is currently a knowledge gap in understanding the very slow advance of the technology. On the one side number of technology vendors such as Nokia, Blackberry, Samsung, Microsoft and Google have been supporting the technology in their operating systems. On the other side the biggest players in the credit card business such as Mastercard, VISA or American Express and some of the largest banks (Bank of America, Citibank, Wells Fargo) have also rolled out some version of technology across their infrastructure. Also, mobile network operators followed the wave where AT&T, Verizon and T-mobile have all started to offer the service. Still, question remains: why MCP solutions are not progressing? Recent report from Gartner confirms that MCP solutions are not following the growth trend: "Near Field Communications' (NFC's) transaction value has been reduced by more 40 percent throughout the forecast period due to disappointing adoption of NFC technology in all markets in 2012 and the fact that some high-profile services, such as Google Wallet and Isis, are struggling to gain traction" Gartner (2013). We believe that initial issues identified by researchers which showed the importance of interorganizational relationships are today, well tackled by market players and as such do not represent important challenge anymore. Instead, we argue that the problem behind MCP struggle relates to the security aspects. Thus, our research question is:

What is the importance of the IT security risk in the MCP consumer adoption?

As there is currently an ongoing debate on the future of MCP solutions, we believe this study contribution brings important insights on the current MCP implementation challenges. In the next sections, we explore past literature and explain the research methodology.

2 Literature review

2.1 Mobile contactless payments

MCP displays several characteristics that relate it to interorganizational (IOR) theory. First, the implementation requires the combination of different services (payment, transactions, identification, etc.), which are usually provided by different organizations or even industries (Dahlberg, Mallat, et al. 2008a; Ondrus et al. 2009; Sammer et al. 2012). Second, most MCP services require the adaption of existing, or the implementation of a new IT infrastructure (for example, NFC-enabled terminals at the point-of-sale (Ondrus and Pigneur 2008)). Third, MCP requires acceptance by end-customers and merchants in terms of usability and trust (Dahlberg, Mallat, et al. 2008a). Fourth, MCP is a substitute for existing payment methods (common credit card payment), which, therefore, challenges existing networks (for example, the four-party system of the credit card payment process (Sammer et al. 2012)).

Based on these characteristics of common MCP solutions, the involved organizations have many IORs among them. Therefore, they resemble networks in which organizations share resources to provide the MCP service. Based on the categorization

of IORs by Parmigiani and Rivera-Santos (2011), we thus categorize MCP as a network.

Concerning the broader scope of IORs, several papers have presented research on specific types of IORs to explain the nature of these relationships. One type of IOR is the vertical relationship (i.e. buyer-supplier) and the supply chain, respectively.

2.2 Dual-Use Technology and Information Security

The term dual-use has its origins in military history. It is now primarily used to describe technology which can be used for two different and opposing aims. One example is the Global Positioning System (GPS) which originally was used for military use. It is now widely utilized in different end user applications for civilian purposes. Information governance reflects the dual-use dangers when combined with the mobile technology (Silic and Back, 2013a).

Another example of this duality dilemma relates to open source security software where on the one side, open source security software such as nmap can be very beneficial, but at the same it time it can be used by hackers to do negative actions against organizational system (Silic & Back, 2013b).

NFC technology has also important dual use side. Consumers may use it to transact, perform payments – thus, positive aims. But it can also be used by malicious users to exploit its vulnerabilities and conduct illegal actions against these same users.

Regarding security aspects of MCP technology, user privacy (Stephen et al. 2004) and main-in-the-middle attacks (Hancke, 2005) are major concerns. User privacy concerns are about collecting potentially sensitive consumer data without its prior consent. In man-in-the-middle attacks two parties are tricked into thinking their communication is secured when they talk to each other, while the attacker is actually in between them, communicating with both (Van Damme et al. 2009). Research regarding security aspects of the NFC payment ecosystem was mostly dealing with very technical aspects proposing methods or tools how to break the security measures but not really offering any insights on the security success or failure factor in the MCP implementation.

3 Method

For this study we use triangulation approach which includes three different sources. Using three different methods will help to strengthen and improve accuracy of our results. Firstly, we analyse practitioner surveys which will help to get more consumer view on the current challenges. Secondly, case study was conducted in French NFC project (Cityzi). Thirdly, we explored secondary sources where mainly online data was collected to better understand the current status of the contactless payments landscape.

3.1 Practitioner Survey Review

We analysed practitioner surveys in an attempt to understand how practitioners see the security topic relationship to MCP. All of the selected interviews addressed directly our research question. In order to address a possible bias from surveys due to different interests of the sponsoring organizations (generally all surveys are financed by 3rd party companies to promote their interests), we highlight the sponsoring organizations.

Finally, we believe practitioner surveys may be very interesting source of information when combined with other more scientific methods as they offer useful insights from consumer perspective. The relevant surveys were identified using Google search, EBSCO and ISI Web of Knowledge databases, and are outlined in Table 1.

Survey name	Country	Sample size	Sponsor
2013: Mobile Payment Index study	Global	2,006	eDigitalResearch
2013: The year of the Mobile Wallet?	UK	2,000	ICM Group
2012: MCP – are you ready?	France	2,582	Les Numériques.fr
2013: MCP quarterly survey	Global	2,085	YouGov (Firstsource Solutions)
2013: NFC survey	UK	2,000	Zapp

Table 1: Practitioner surveys

3.2 Interviews

After reviewing secondary data about different MCP services and conducting expert interviews, we decided to assess the MCP service provided in France: Cityzi – case study.

Cityzi is a NFC-based multi-service that includes three end-customer applications, including payment, on which we focused our research:

- Payment, including services for public transport (purchase of tickets for the public transport) and retailers (payment, mobile loyalty and coupon programs).
- Cityzi tags, including the e-campus project with the aim of accessing various pieces of information using Cityzi tags.
- Third party applications, including tourist information.

Today, Cityzi is available in five cities (Nice, Strasbourg, Caen, Marseille, and Paris) and further expansion is planned. Technically, Cityzi is based on a state-of-the-art NFC-based solution integrated in to the subscriber identity module (SIM) cards, which is compatible with most modern smartphones. Due to the market penetration (more than 1.5 million terminals, support for over 30 different smartphones, more than 4 million registered users) of the solution, it can be considered as one of the most mature and successful solutions in Europe.

Cityzi is organized by the Association Française du Sans Contact Mobile (AFSCM). A summary of seven different interviewees we conducted, including information about their position and organization, is given in Table 2. Important to note is that seven interviewees represented well all different organizations members of AFSCM.

Organization	**Org. Size**	**Department**	**Position of Interview Partner**
AFSCM	Small (<50)	Top Management	CEO
Technology vendor 1 (TV1)	Small (<50)	Top Management	CEO
Technology vendor 2 (TV2)	Large (>250)	NFC Business Development	Director NFC products
Technology vendor 3 (TV3)	Large (>250)	Sub-division eDocuments	Senior Manager (Director NFC products)
Mobile network operator 1 (MNO1)	Medium (50-250)	NFC Business Development	Director NFC products
Mobile network operator 2 (MNO2)	Large (>250)	NFC Business Development	Senior Manager (Business Development)
Service Provider 1 (SP1)	Small (<50)	Top Management	CEO

Table 2. Interviewees and Information about their Position and Organization.

The data collection approach included primary data derived from interviews and questionnaires, as well as secondary data derived from press releases, and organizational websites. All interviews were conducted as semi-structured telephone interviews, which were audio recorded and transcribed. The interviews lasted an average of 60 minutes. The qualitative interview followed a guideline, which included the following sections: Information about the organization and interviewee, description of the activities within Cityzi, description of the interorganizational relationships concerning Cityzi, and an outlook. All interviews were conducted between October 2012 and November 2013 and included only executives from the stated organizations. To assess the MCP services in a case study, we define a case study protocol to ensure the comparability of the data collected from each company. The case study protocol represents a generic structure of a MCP ecosystem and is applicable for western markets. The case study protocol is displayed and described in Table 3.

Concept	**Description**
Company	Companies that are involved in the MCP service. Companies are associated and aggregated to actors of the network.

Actor	Actors represent different companies categorized by a classification adapted from (Au and Zafar 2008) and (Sammer et al. 2012). The classification includes the following actors: (1) Regulation agencies: This categorization includes government agencies, which are concerned with financial or technological issues related to MCP. (2) Financial Service Provider: Companies that facilitate the process of clearing payments. (3) Merchants: Companies at the point-of-sale. For example retailers. (4) Technology vendors: Companies that provide or manufacture technologies such as cell phones, NFC-transactions modules or terminals at the point-of-sale. (5) Mobile network operators (MNO): Are wireless service providers and handle issues concerning the secure element (SIM). (6) MCP Associations: These are associations that coordinate the implementation of MCP services and represent a forum for the attending companies.
IOR	To identify IORs we define them as any relation that either is a transaction (transaction cost theory view) of real or virtual commodities (knowledge, money, information…) or the option for a company to obtain access to complementary resources (resources based view).

Table 3. Actors in the NFC ecosystem

All transcribed interviews were coded using a predefined categorization and the software NVivo 10. Two of the authors independently coded the interview data. Cohen's kappa, which measures interrater-reliability, was statistically significant within a range between 0.83 and 1 for each coded category. In a second round, discrepancies were discussed and resolved. By following the approach recommended by (Miles and Huberman, 1994).

3.3 Secondary data

We use Romano et al. (2003) research methodology to analyze web based qualitative data. This approach helped us to follow a structured approach in assessing and analyzing data. We collected different data from online (web based) sources including technical forums, online news and industry articles, interviews from information professionals and NFC dedicated websites. Further, we searched through technology and industry online magazines, search engines, forums by providing certain keywords: NFC challenges, NFC payments, MCP, mobile contactless payments, MCP security, and MCP future. We limited our search from September 2013 to December 2013. Secondary data sources were particularly useful as we could receive views from various channels such as online and industry magazines which provided an independent view on the NFC technology challenges, current status and future developments. Secondary data sources are summarized in Table 4.

Data source	Description
Interviews	In total ten online interviews were analyzed

Online articles	Fifteen online articles from nfctimes.com, nfcworld.com, techcrunch.com, mbweek.com, bankingtech.com, lesnumeriques.com
Press releases	Four press releases from orange.com, afscm.org, gemalto.com
Forums	Seven articles were analyzed from nfc-forum.org, nfcworld.com, forum.xda-developers.com/general/nfc

Table 4. Secondary data sources

4 Results

In the next sections we will present the results of three distinct methodological approaches. The results reveal that security dimension is an important obstacle in the MCP expansion. This also demonstrates the fragility of the MCP network structure where the absence of support from a single actor can lead to a decreased network performance.

4.1 Practitioner survey results

From the five surveys we analyzed security was highlighted as the most important factor in the current MCP projects. One survey found that security and fraud are the biggest barriers to mobile payment adoption which is an even quite worrying fact as 73% of respondents are aware of the technology (eDigitalResearch, 2013). In other words despite progress in the awareness, the usage does not follow. Similar was confirmed by another survey (ICM research, 2013) which found that 80% of consumers are aware, but only 8% do actually use the technology. Survey also stresses the importance of consumer security concerns which are not properly addressed. French survey done by Les Numériques (2012) showed that 44% of respondents are ready to adopt the new technology but only if strong security guarantees are provided. In UK, survey performed by YouGov (2013) revealed that consumers don't trust mobile payments. It strongly pointed out consumer fears over security which is very consistent with previous survey findings (Zap, 2013).

4.2 Cityzi - case study results

All interviewees confirmed that security is a very important aspect going together with inter-operability. For example, one interviewee highlighted the high level of the security risk when purchasing services and further explained that it represented high barrier for the service expansion: "*…as there is no sufficient guarantee to do mobile payment or buy tickets and having guarantee of a safe transaction related to Fraud, hacking,etc...*".. For another interviewee security is clearly stopping the service expansion as infrastructure is in place, all main actors formed a good alliance between them but confidence in the security measures is not yet there: "*...reason why we did not get any significant numbers is because banks were blocking the numbers as they were afraid to open the security flow. It is mainly because security aspect was a bit missing*". There was a clear consensus among all interviewees that the security aspect is the missing piece where one actor (banks) was not fully satisfied with the existing security

requirements of the current NFC version in use and in that context did not want to push for the solution too much not to create security holes which could bring important financial risks. This aspect was clearly pointed out by one interviewee who commented: "*it is needed to go step further to satisfy all constraints: for banks it is security aspect*". Despite the fact that all interviewees pointed out at security as the main road blocker in the current setup, most of them were seeing the next version of NFC as the right solution which will solve the current financial limits imposed by the financial players (banks, card issuers). For example for one interviewee: "*the security aspect will be enforced and Mastercard and VISA will not add any limits anymore*", which clearly shows that when one actor in the entire network chain is not fully supporting the solution, the challenge arises and entire network chain may break down. Finally, when we questioned interviewees about the type of security which is currently slowing down the implementation, they said that it is mainly the "consumer security" where consumers do not feel confident in transacting as they heard that it is insecure and some illegal activities can be easily performed on their behalf.

4.3 Secondary data results

From the secondary data results we got a strong confirmation that MCP is not progressing mainly due to consumer security barriers. It seems that further expansion is strongly influenced by consumers' fear of conducting insecure transactions and in that context despite high awareness; they refuse to adopt the new technology. The analyzed data from different sources (e.g. mbweek.com) showed that mobile payments are held back by security and complexity. In one interview it was explained that the need is there but adoption is still far behind: "*People want to pay with mobiles, but they need to be convinced that payment is secure, and it has to work everywhere and be totally hassle free. History shows us that mass adoption always follows trust and convenience, which in turn is enabled by cooperation*". Another one also added: "*With banks routinely issuing contactless payment cards to customers, there is a need to raise awareness of the potential security threats*". Overall, all sources did mention consumer security to be one of the main factors in the current contactless payments adoption challenges. Few websites and forums, that are more vendor dependent and as such can have some financial benefits, did not clearly point security as being an issue but were rather speaking of sporadic incidents that are following any new technology introduction.

5 Triangulation, Discussion and Conclusion

We triangulate our findings by combining the results from three methodological sources. Practitioner survey results revealed that consumer security is top concern for further adoption of MCP technology. Furthermore, it seems that current security measures are not enough to convince consumers to use MCP despite very high existing consumer awareness and knowledge about the technology. All surveys were very consistent saying that over 75% of consumers are aware about the new mobile payment technology, but majority of consumers are not willing to adopt it for security reasons. Case study from the French NFC project, Cityzi, provided overview of the actor network where clearly, security was highlighted as a top barrier in further service expansion and adoption. Moreover, it was found that the current implementation is slowed down by network actors which are not confident in the current security

countermeasures. Secondary data source provided valuable insights as an independent source which revealed that security is a barrier to further MCP adoption.

Based on the triangulation of these three methodological approaches, we can see that security aspect was the major show stopper for a successful MCP project. Clearly, strong information security safeguards are mandatory to bring confidence and security in the entire transaction flow. While there are some other examples such as Osaifu keita (launched in Japan by NTT Docomo) which was very successful with over 30 million users, it is important to highlight that generally, MCP implementation was successful in all countries where there were no prior similar existing card payment systems (Andren and Lagstrom, 2011). This finding is in line with previous studies which confirmed that any complication associated to m-payments solutions will not be tolerated or waited by the customers (Stoughton et al., 2011).

Furthermore, to establish such a complex system as MCP, different organizations have to cooperate and form interorganizational relationships. Previous studies (i.e. Ondrus et al. 2009; Sammer et al. 2012) did confirm that interorganizational relationships are a success factor and as such do have an important role in the entire MCP ecosystem. Also, competition and rivalry between organizations were previously identified as a major obstacle to the implementation of MCP (e.g. Andren et al. 2011).

Finally, we believe that this dual use side of MCP technology needs further and deeper understanding and analysis. As positive aims behind the MCP solutions are rather evident; however, the negative context needs to be approached more from consumer standpoint with the objective to better understand consumer behaviours and the entire complex trust process.

Our study has some limitations. Our study focus was mainly on the MCP technology while the same conclusion may not be applicable to the entire NFC technology. In this context, our results could not be generalizable to the entire NFC ecosystem and further studies can eventually explore the role of security on other parts of the NFC ecosystem.

Finally, we believe this study offers important contribution for practitioners as it provides novel insights on the failure factor regarding MCP implementation. From a theoretical point of view, our results contribute to our understanding of the problems and solutions associated with the implementation of such complex technological systems. The results further contribute to the existing knowledge on MCP implementation and provide evidence of the security component as being the most critical element in the entire MCP chain.

Based on this conclusion, we propose that research concerning the implementation of MCP systems or other comparable systems explores the influence of security component on the entire solution ecosystem.

References

Andrén Meiton, E., & Lagström, M. (2011). Contactless Mobile Payments entering Europe: The contactless mobile payment ecosystem and potential on the European market (Doctoral dissertation, KTH).

Au, Y. A., and Zafar, H. (2008). A Multi-Country Assessment of Mobile Payment Adoption. The University Of Texas At San Antonio, College Of Business Working Paper Series, # 0055IS-296-2008, 1-43.

Cadden, T., Humphreys, P., and McHugh, M. (2010). The influence of organisational culture on strategic supply chain relationship success. Journal of General Management 36 (2), 37–64.

Dahlberg, T., Huurros, M., and Ainamo, A. (2008a). Lost Opportunity Why Has Dominant Design Failed to Emerge for the Mobile Payment Services Market in Finland?. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences, Hawaii, 83–83.

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

eDigitalResearch (2013). http://ecustomeropinions.com/survey/survey.php?sid=305283920&data1=, Retrieved on November 15th, 2013

Gartner (2013). Gartner report. Retrieved from http://www.gartner.com/newsroom/id/2504915

Hancke G.(2005). A practical relay attack on ISO 14443 proximity cards. Technical report, University of Cambridge

Hu, X. (2008). Are Mobile Payment and Banking the Killer Apps for Mobile Commerce?. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences, Hawaii, 1530-1605.

ICM Research (2013). http://www.icmresearch.com/2013-the-year-of-the-mobile-wallet, Retrieved on November 10th, 2013

Le Numeriques (2012). http://www.lesnumeriques.com/paiement-sans-contact-etes-prets-n27337.html, Retrieved on November 10th, 2013

Miles, M. B., and Huberman, A. M. (1994). Qualitative Data Analysis: An Expanded Sourcebook. 2nd Edition, Sage Publications, Thousand Oaks.

Ming, L. T. (2011). Value Chain Flexibility with RFID: A Case Study of the Octopus Card. International Journal of Engineering Business Management 3 (1), 44.

Ondrus, J., Lyytinen, K., and Pigneur, Y. (2009). Why mobile payments fail? Towards a dynamic and multi-perspective explanation. In Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, Hawaii,1-10.

Ondrus, J., and 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., and Pigneur, Y. (2007). An Assessment of NFC for Future Mobile Payment Systems. In Proceedings of the International Conference on Mobile Business (ICMB 2007), Toronto, 43–43.

Ondrus, J., and Pigneur, Y. (2008). Near field communication: an assessment for future payment systems. Information Systems and e-Business Management 7 (3), 347–361.

Parmigiani, A., and Rivera-Santos, M. (2011). Clearing a Path Through the Forest: A Meta-Review of Interorganizational Relationships. Journal of Management 37 (4), 1108–1136.

Pousttchi, K. (2003). Conditions for acceptance and usage of mobile payment procedures. In Proceedings of the Second International Conference on Mobile Business, Vienna, 201-210.

Romano, N. C., Donovan, C., Chen, H., & Nunamaker, J. F. (2003). A methodology for analysing web-based qualitative data, Journal of Management Information Systems, (19:4), 213-246.

Sammer, T., Lazur, C., Walter, T., and Back, A. (2012). Barrieren am Weg zum Mobile Contactless Payment: Eine Marktanalyse und Bestandsaufnahme der Situation in der Schweiz. GI-Edition - Lecture Notes in Informatics (P-202), 42-55.

Silic, M., and Back, A. (2013a). Factors Impacting Information Governance in the Mobile Device Dual-use Context. Records Management Journal, 23(2), 2-2.

Silic, M., and Back, A. (2013b). Information Security and Open Source Dual Use Security Software: Trust Paradox. In Open Source Software: Quality Verification (pp. 194-206). Springer Berlin Heidelberg.

Steensma, H. K., Marino, L., Weaver, K. M., and Dickson, P. H. (2000). The Influence of National Culture on the Formation of Technology Alliances by Entrepreneurial Firms. The Academy of Management Journal 43 (5), 951–973.

Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels (2004). Security and privacy aspects of low-cost radio frequency identi cation systems. In Security in Pervasive Computing, volume 2802 of Lecture Notes in Computer Science

Stoughton, D., Hargreave, N., & Yohannan, R. (2011, May18).SingaporeInterviewVCitibank.

Van Damme, G., Wouters, K., & Preneel, B. (2009). Practical Experiences with NFC Security on mobile Phones. In Workshop on RFID Security–RFIDSec'09.

YouGov (2013). http://research.yougov.co.uk/, Retrieved on November 5th, 2013

Zapp (2013). http://zappit.co/, Retrieved on November 5th, 2013