Building the Bridges – A Proposal for Merging different Paradigms in Mobile NFC Ecosystem.

Raja Naeem Akram
Institute for Informatics & Digital Innovation
Edinburgh Napier University.
Edinburgh, United Kingdom
Email: R.Akram@napier.ac.uk

Konstantinos Markantonakis and Keith Mayes
Information Security Group, Smart Card Centre
Royal Holloway, University of London.
Egham, United Kingdom
Email: {K.Markantonakis, Keith.Mayes}@rhul.ac.uk

***Abstract*—In late 1990s. the multi-application initiative was put forward to have multiple applications on a single smart card. This would have enabled a cardholder to accumulate all of her smart card based applications (e.g. banking, telecom, and transport etc.) on a single device. However, despite the initial fervour for the multi-application smart card initiative; there were no wide spread adoption of this model. Nevertheless, the Near Field Communication (NFC) has reinvigorated the multi-application initiative again. In this paper, we will analyse why the multi-application smart card initiative failed to materialise a decade ago and whether this time around it will succeed as a viable model or not. The NFC trials being conducted basically rely on the existing ownership architectures, which can create market segregation and thus reducing the potential revenue generation capability. We propose a possible approach that avoids market segregation, increase revenue generation, and provide flexibility, robustness and scalability to existing ownership architecture.**

I. Introduction

From early 1980s to late 2000, the smart card technology evolved from a monolithic to a multi-application operating system that can support post-issuance application download [1]. The multi-application smart card initiative enabled diverse application to co-exist and share resources in a secure and reliable manner [2]. It was envisioned that diverse organisations (e.g. banks, telecom operators and transport, etc.) would approach each other to provide services on a single device. This assumption was based on experience of the collaborative attitude of different stack-holders in the smart card industry [3]. However, the reality was different.

The multi-application smart card initiative lost its appeal and it can be attributed to the issues related to the card ownership, marketing potential of card surface, customer loyalty, and potential revenue stream — that hindered any possible collaboration. In addition to these issues there were other voices that were concerned with the security implication of the multi-application smart card initiative [4, 5]. Nevertheless, the enthusiasm died quickly until a new technology termed as Near Field Communication (NFC) came on the scene. The NFC among other capabilities, enables a mobile phone to emulate as a contact-less smart card [6]. For last few years, the NFC based mobile services with applications like banking, telecom and transport are trailed in around 38 countries [7]. In these trials the smart card management architecture is based on the traditional framework that has been deployed in the smart card industry since its inception, namely Issuer Centric Smart Card Ownership Model (ICOM) [8]. In the ICOM, smart cards are issued and controlled by a centralised authority known as card issuer. Any application provider that would like to install their application on to these smart cards need prior-authorisation from the card issuer. The extension of the ICOM deployed in the NFC based trials is termed as Trusted Service Manager (TSM) architecture [9]–[11]. The TSM is an entity that manages the smart card platform and all application providers need its prior-authorisation for application installation. The TSM can be a card issuer or a third party that just manages the platform.

A contrasting approach to the smart card ownership model is based on the citizen ownership architecture. In this model, the smart cards are owned by cardholder (user) and they have the choice to install or delete any application as they require. The term ownership implies that the cardholders only have the right to choose an application either to be installed or deleted. They do not have the control of the smart card platform such as we have in the ICOM architecture. The security and reliability of the platform is assured by the platform itself so the application providers do not have rely on the trustworthiness of the cardholder [12]. Such an architecture is termed as User Centric Smart Card Ownership Model (UCOM) [8]. The UCOM provides a dynamic, ubiquitous, scalable and open environment. Where TSM can be argued to provide better acceptance in the smart card industry and a feasible business case.

The theme of this paper is to theoretically illustrate that a "coopetitive" attitude towards the multi-application smart card architecture would be beneficial to all stack-holders. The term coopetitive is borrowed from the discipline of game theory [13]; where it stands for the concept in which competitors collaborate with each other to share the common cost and compete where they see that they might have a competitive advantage. The coopetitive architecture is a merger of two ideas: TSM and UCOM. This paper Illustrates that such a model can increase scalability, and increase revenue generating opportunities then individually these both models can achieve.

In section two, we discuss what was the underlying causes that hindered the wide-spread deployment of the multi-application smart card in the first instance and recently why

there is a renewed interest in this idea. Section three introduces the TSM architecture and how it can hinder a scalable and ubiquitous framework. The UCOM architecture is discussed in section four along with why giving choice to user is a good idea both with regards to security and business. Section five provides the rational for having the coopetitive architecture, which is then detailed in section six. Finally, in section seven we discuss the future research directions and list the concluding remarks.

II. Multi-application Smart Cards

In this section we open the discussion with illustrating the issues that decelerated the multi-application smart card initiate. Extending this discussion to show why there is a renewed interest in this idea after a decade.

A. What Went Wrong?

As traditionally smart cards role is of security nature, the concept of having multiple applications; where all of them might not be trusted prompted a debate of what kind of control should be in place to manage this initiative. As pointed out by Pierre Girard [14], there can be three possible architectures.

First architecture was based on the traditional centralised control which was successfully deployed before multi-application initiative; termed as Issuer Centric Smart Card Ownership Model (ICOM). In this model, an organisation (hereafter referred as card issuer in the ICOM) acquire smart cards from a card manufacturer and then issues them to individual customers. The application providers that would like to install their applications to the issued smart card negotiate terms and conditions with the card issuer. Unless, card issuer do not authorise an application provider they can not install their application on to the smart cards. In this model, the user has no say which application they would like to have it on their smart cards.

In second approach, customers would take the role of card issuer and acquire (blank) smart cards from a card manufacturer. A customer would then acquires an application from an organisation (e.g. bank, telecom and transport, etc.) and install onto her smart card. This approach was not considered a serious contender as organisations may not trust the customer and might not have behaviour guarantees of the smart card platform. Finally, the third approach was to have a certification authority that manages the multi-application scheme. This approach can be considered an extension to the ICOM model. We have a centralised authority that issues the smart cards but application providers do not have to reach an agreement with the card issuer. Instead they agree in principle with the certification authority and download application to smart cards that are under its management.

As noted by M'Chirgui [3], the smart card industry's rapid proliferation was due to the adoption of the coopetition attitude towards the product and market; as noted for other high-tech industries. The concept of coopetition can be described as two individuals (companies) who cooperate with each other to cook a pie (establish market) and then they compete with each other to take the biggest share of it. The examples of coopetition can be EMV [15], GlobalPlatform [16], and Java Card [17] specification. However, similar attitude was not apparent for deployment of the multi-application smart card initiative for a diverse set of reasons. Following are few of the major issues that contributed to the deceleration of the convergence of diverse services on a single device - discussed in detail in [8].

1) Smart Card Control (Ownership).
2) Marketing Potential
3) Customer Loyalty
4) Customer Relationship Management
5) Potential Revenue Source

The above mentioned reasons can be considered to overly simplifying the dynamics that led to the deceleration of the multi-application smart card initiative. Nevertheless they played their role, and recently these issues are coming back as the concept of having multi-application applications on a single device is gaining momentum.

B. Renewed Interest!

Similar to the issues that decelerated the multi-application smart cards; we cannot pin point one single factor that has reinvigorated the multi-application initiative again. However, in this section we discuss few of the contributing factors that has generated a substantial interest in the smart card service sector.

The most important of all is the Near Field Communication (NFC) that enables a mobile phone to emulate a contact-less smart card [18]. This facilitate the NFC enabled mobile phones to perform contact-less card transaction on existing smart card infrastructure (i.e, contact-less smart card terminals [19]). Therefore, it does not require any modification on the infrastructure side of the smart card service ecosystem. The only change is that a user's mobile phone acts as a contact-less smart card and from terminal's point of reference it communicates on a contact-less interface with a device that can be a traditional smart card or a mobile phone. The NFC trails are being carried out in 38 countries around the world [7]. Nevertheless, a practical deployments is still in the pipeline. However, it can be argued that NFC based service of some sort is going to be role out whether it would be part of the traditional smart card services or other possibilities.

In addition to the development taking place in terms of NFC and its implication on the traditional smart card industry. In a totally unrelated sector the dynamics of business was substantially reshaped. Here we refer to the concept referred as the "iPhone effect". Installing of an application on to a mobile was possible even before the iPhone came to market. However, iPhone made it consumer friendly; an average customer can easily navigate, search, and install third party software [20]. In addition, the application developers do not have to negotiate with the mobile operators to download their applications onto iPhone. Furthermore, Apple has managed to remain in the sales loop by charging a percentage on application sales directly to the application developers. Finally, mobile operator

got the opportunity to sell data plans and generate revenue from the data usage.

With ever growing younger consumer base that use a mobile phone for multitude of purposes [21]; it is obvious that smart card service sector could also harness the platform to reduce their investment (i.e. purchasing of new smart cards), decrease roll-out time for new services and remain competitive. Example of the competitive challenge faced by the traditional smart card industry can be mobile payment systems; there are a number of smart phone Apps (i.e. Starbucks Apps for Blackberry and iPhone, and Paypal App, etc.) that a user can download onto their mobile phones and then can use them to pay for different services.

We consider that multi-application smart card initiative has mature to a level that it can be considered as a secure, reliable and viable business model. The divergence of different services on to a single device might be considered a natural next step in the smart card evolution. However, how successful this might be is still open for debate. In next section we discuss the proposed (and trailed) business model for the NFC based services roll-out.

III. Trusted Service Manager

The Trusted Service Manager (TSM) can be considered an extension to the ICOM. In this section, we discuss different ownership and card management architectures in the TSM environment, also elaborating on who is driving which initiative.

A. Possible Ownerships Architectures

A Trusted Service Manager (TSM) is an entity that manages the collaborative architecture in which different application providers share a platform[1]. The TSM can be a card issuer or a third party whom the card management tasks [10] are being delegated by the scheme participants (e.g. card issuer and application providers). In current proposals a TSM can be: a) Mobile Network Operation (MNO) [11, 22], b) Card Issuing Bank (CIS) [23] or c) A neutral third party.

No matter who takes the role of the TSM in a particular role out, an ownership architecture has to be decided among the scheme participants. Some of the possible architectures listed in the literature [6, 10].

IV. User Centric Smart Card Ownership Model

In this section we will briefly introduce the UCOM and then describe why a discussion on such a model is necessary in the context of future multi-application smart card initiative(s).

A. Brief Introduction

The architecture of the User Centric Smart Card Ownership Model (UCOM) supports the smart card ownership to be with its user. The term ownership does not imply that the cardholder owns the platform as a card issuer in the ICOM or TSM architecture. It implies that the user has the "*freedom of choice*"

[1]Platform: The term platform in context of the TSM refers to the secure elements present in a mobile phone. Secure elements can be Universal Integrated Circuit(UICC), embedded secure element, and Secure Memory Card [10].

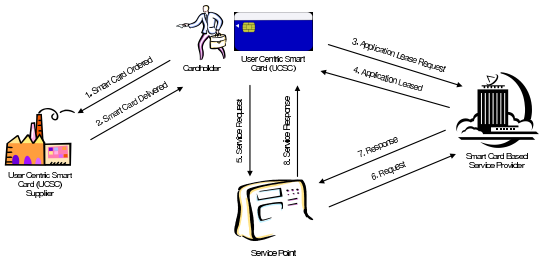

Figure 1. Generic Overview of User Centric Smart Card Model (UCOM)

[8] to install or delete any application they would require from their smart cards. The card issuers or application providers in the ICOM or TSM architecture are termed as Service Providers in the UCOM. A Service Provider (SP) is an organisation that will only develop a smart card based application and then issue its customers with unique credentials to download its application(s) directly to the respective smart cards [24].

As shown in figure 3, a card issuer acquires a UCOM supported smart cards referred as User Centric Smart Card (UCSC) from a card manufacturer. At this stage, the card might be a blank card under default ownership. The default ownership means that its under the ownership of the respective card manufacturer. The cardholder initiates the ownership transfer to him or herself and then can present this card to a SP to request their application. The SP would decide the lease of the application depending upon their Application Lease Policy (ALP) [24] which basically states the minimum security and operation requirements a smart card has to meet to get the lease. Only after the smart card satisfies the lease requirement of the respective SP [12, 25], the application can be downloaded onto it. The cardholder is not involved in this process except for initiating the request for the application lease.

B. Why User Centric Smart Card Ownership?

The UCOM architecture is different then the Open Card initiative [5], multi-functional smart card [26] or virtual smart cards (applications) [27]. The UCOM is in fact an ownership model rather then a complete platform or smart card operating system. To support UCOM requirements and services [8], the existing well-defined and studied architectures (e.g. Java Card [17], Multos [28], and GlobalPlatform [16]) are being modified [29] so they can efficiently support the user's ownership. Therefore, the main ingredients to support a user's ownership is a secure, reliable, flexible and ubiquitous way is already there. The only thing UCOM has done is to bring them together to support the concept of user's owned security devices (namely smart cards or secure element). The argument that an SP has to trust a cardholder before issuing its application is not valid [12] as the application lease is under sole discretion of the respective SP. In addition, only after gaining the assurance and validation that the smart card in questions supports its requirements that it will lease the application [25]. Therefore, the SP has to establish trust in the user's smart card and not the user. The assumption in the UCOM is that a user can have

malicious intend and under these circumstances how the whole framework can be secure and reliable.

A valid argument can be made that the UCOM architecture could only bring more complexity or complicate the security sensitive smart card industry. It is true that the modification required by UCOM do require some modification to the existing smart card platform but not to the service architecture (i.e. ATMs in banking ,or turnstile terminal for transport services) than the TSM architecture. In addition, as we will see in next section that underestimating the desire of the customers to have a choice might result in market segregation, decrease revenue generation, low customer satisfaction, and possibly another failure of multi-application smart card initiative.

V. Building the Bridges

The mobile phone platform has come a long way from just a medium of voice communication. It has developed into a social construct that has affiliations and emotional attachment with individual users [30]. It has become an entertainment hub, and a medium to connect with the rest of the word through social media sites. With ever increasing trend of convergence of different technologies onto a smart phone, the most desirable avenue for the revival of the multi-application smart cards was no-doubt on a mobile phone. The NFC technology has provided that opportunity to harness potentials of collaborative schemes that will see the deployment of multi-applications from diverse service providers on to a single mobile phone.

For any new bold step, there has to be forces that moves the competition in an industry. The pivotal forces in any market can be categories as: a) threat of new entrants, b) threat of substitute products/devices and c) consumers power (culture) [31]. Possible new entrants to the business hierarchy can either be based on revolutionary product, core competence, or establish and trusted brand. The smart card industry has not decided on the who should be taking the role of the TSM. Possible contenders can be smart card manufacturers, MNOs, CIBs, mobile phone manufacturers or independent/trusted third party (i.e. post office). Therefore, there is a possibility that new entrants may gain ground whose core competence is based on the multi-application smart cards and in this scenario card and phone manufacturers can be have an advantage. However, in term of trust in a technology smart card manufacturer are worse effected as for the entire period of smart card deployment their brand is never part of the final product. Therefore, even the core competence of MNOs or CIBs is not designing and managing the smart card but they have strong brand existing customer base.

In addition to this, with recent "App Culture" as prompted by the iPhone in which a user can download any application as they desire with easy from the Apple App Store [20]. New ideas are being circulated and test, for example Starbucks' customers can pay for coffee using their Starbucks Card Mobile App on their iPhones. This payment scheme does not use NFC technology, infact rely on the barcode scheme. This clearly gives an indication that their can be substitute technologies that can enter the traditional smart card industry.

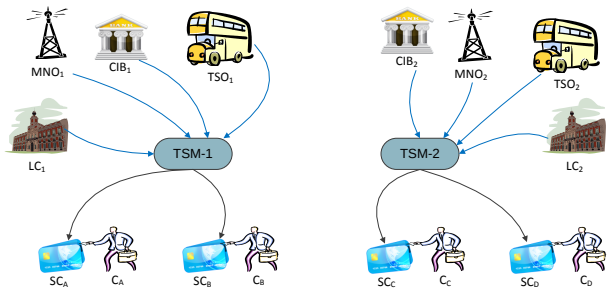

Figure 2. Trusted Service Manager Architecture

May be not as MNOs or CIBs but for other services like royalty card, travel, and mobile payments.

Furthermore, from a general user's perspective how they will measure the multi-application smart card role out. Theoretically, consumers compare new technology to the ones they already use or know off [32]–[34]. As the analysis performed on mobile phone users showed that they tend to compare services provided on the mobile phone with one available on their computers [35]. Although this result does not directly links to over point of focus, but its shows that any multi-application smart card architecture might be compared with the "App Culture". Authors at the time of writing the paper are not aware of any study conducted that shows that user would like or not prefer the same level of freedom of application choice for a NFC based services roll-out.

Therefore, as noted above the time is right for the stack-holders in the smart card industry to forge new alliances and develop innovative ideas for multi-application smart card roll-out. Now looking at the TSM architecture in its most simplistic form as illustrated in figure 2. Diverse set of companies would join together to roll-out the TSM based multi-application smart card scheme. In such an environment, a customer of MNO_1 (e.g. C_A) that has a relationship with TSM-1 would only be able to have applications from CIB_1, TSO_1 and leisure centre that are associated with the TSM-1. However, if the respective customer do banking with a CIB_2 that is associated with the TSM-2 then either she has to acquire a smart card from one of associates of TSM-2 or change the bank. Such a scheme has a potential of creating segmentation in the market. Where to fully benefit from the multi-application smart card functionality you have to be customer for a set of companies that are associated with the same TSM.

There are few possibilities to reduce this segmentations. First possible option is that each participant or application providers (i.e. CIBs, MNOs and TSOs etc.) maintain relationship with all or most of the TSMs. For example in figure 2 a CIB of TSM-1 should also have a relationship with the TSM-2, so that customer based managed by the TSM-2 could also take advantage of services provided by the CIB of TSM-1. In second possible scenario, all TSMs should have a inter-relationship mean that they create a syndicated TSM architecture. So any application provider affiliated with one TSM would be able to issue its application to a customer of

any other TSM. This in-fact boils down to creating another syndicated scheme which can be termed as TSM of TSMs in which several TSM participates to provides services to other TSMs. Both of these scenarios can be argued to be workable, but they have suffer from limited scalability, true flexibility and ubiquitousness of the framework.

The limited scalability roots from the fact: a) not all applications providers can establish or manage relationship with every possible TSM and b) there is a possibility that even with syndicated TSM architecture certain group of TSM end up having separate scheme where other group of TSM have their separate syndicated TSM architecture. In addition, a customer can only have an application from the a application provider which is associated with one of the TSMs. Now, to be part of a scheme offered by a TSM might require subscription fee for the application provider. Therefore, in such a situations small or medium scale organisations like local libraries, universities and health centres may not be able to afford to be part of such scheme.

We consider that such a barrier to enter the multi-application scheme reduces its flexibility to provide diverse services to general public. Furthermore, different countries might opt for having their own independent TSMs thus for a person travelling from one country to another face the difficulty to acquiring the applications which she may need to use during her stay (i.e. application from TSO of the visiting country). These issues are just on top of the ones that are discussed in [4, 8, 14, 36]: including ownership privileges, customer loyalty, customer relationship management, smart card marketing and revenue generation potential; so instead of reducing the issues the TSM architecture can be argued to increased it.

An argument can be made that none of the issues that are listed before have real significance. As even if there are multiple independent and isolated TSMs market competition will reduce the number by the process of elimination and only the best/strongest alliance will survive [37]. Thus market will self regulate itself and reduce the segmentation. Have competition among a large set of stack-holders (i.e. MNOs, CIBs, TSOs, card and phone manufacturers, and neutral third party etc.) will only reduce the profitability of the scheme as illustrated by the advantages that the smart card industry have achieve in past through coopetitive strategies [3]. In addition, modern high-tech industry's business strategy is inclined towards cooperation to create a market for emerging technologies and then compete to harness maximum profit out of this new found market; which is in other words the coopetitive strategy [13, 38, 39]. Furthermore, consumers tend to weight different schemes as whether they would be temporary or something long term; along with factors including coolness (enjoyment of use) and usefulness in daily life [40]–[43]. Therefore, their is a possibility that due to intense competition among different stack-holders in the smart card industry the adoption/acceptance of NFC based services on a mobile phone would be rapid and widespread.

In case of the UCOM architecture, most of the issues discussed until now are not present [8]. Nevertheless, the main issue is that the potential for the revenue generation is limited. As the UCOM smart cards are sold to the cardholders and after this the card manufacturer or any third party cannot be part of the value chain. We consider that UCOM architecture itself would be a suitable solution but it is difficult to assume that such a model can have a widespread acceptance in the business community. Therefore, a compromise between flexible, open, dynamic, and business viable solution combine the TSM and UCOM architectures: coopetitive architecture for multi-application smart cards. The coopetitive architecture focuses on the core competences of individual companies and leave other areas to organisations that might have expertise in that particular area. For example, a MNO in the coopetitive architecture can be a TSM and even have the ability to form alliance with other companies to provide their services on to the respective smart cards. But in addition, it also enables the users to directly request download of any application they like from any of the application provider of their choice. The main stack the MNO has is to generate maximum revenue out of their investment in the secure element and its security. So there is a way in which an application can be securely download onto a smart card that does not have any prior relationship with the particular TSM (i.e. in our example the MNO) and the MNO charges the customer for acquiring the application. Then in such a model there is a probability that customers would actually enable the TSM in the coopetitive architecture to generate higher revenue then in the traditional architecture. We discuss the details of the coopetitive architecture in next section.

VI. Coopetitive Smart Card Architecture

The coopetitive smart card architecture basically joins the business attractions of TSM architecture with the openness, scalability and flexibility of the UCOM architecture. In this architecture, users get their choice of selecting which application they want on their smart cards, and card issuers have a permanent presence on the cards along with being part of the revenue loop. In this section, first we will discuss the coopetitive architecture and then describe the multi-application smart card architecture to support it.

A. Coopetitive Architecture for Smart Cards

The ecosystem of a coopetitive architecture is illustrated in the figure 3, and at its centre there are three main entities; smart card issuer, cardholder and smart card. The card issuer (or TSM) would issue the smart cards to their respective customers. As a card issuer they would have their application pre-installed on to the smart card. The cardholder would have the choice to install or delete any application they would require; except for the card issuer's application(s). The management of the smart card application installation, deletion, and application/card lifecyle management is handled by the Platform Manager (PM). It facilitates both the card issuer and the cardholder to perform their sanctioned tasks.

As an example, consider a scenario in which a user enrols into the multi-application smart card service architecture

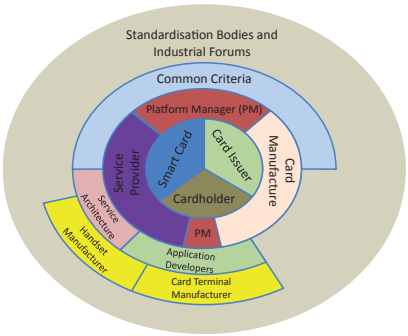

Figure 3. Coopetitive Architecture's Smart Card Ecosystem

through a MNO. As the customer of the MNO, the user can receive a NFC enabled mobile phone (under a fixed period contract) and secure element(s) that support multi-application architecture. As par current architecture, MNOs subsidies the mobile phone in return for a fixed period contract with their customers. The phone is under MNO lock and it can only be used on the issuing MNO's network. At the end of the contract, the customer can request the respective MNO to unlock the mobile phone. The acquired secure element(s) would have MNO's application installed by default. In addition, if the user is customer of any other organisations that are associated partner with the MNO in the TSM scheme. Then she may get their applications pre-installed on the secure element. The issuer secure element would enable the user to request installation or deletion of any application she requires, except for the MNO's application. At the end of the contract the MNO would not only unlock the mobile phone but also the TSM. From this point forward, the user can either use the secure element under UCOM architecture or register their secure element with any other TSM (or continue with the original MNO).

Similarly, other entities like CIBs, TSOs, smart card and mobile phone manufacturers, or independent third parties can participate by offering competitive products that adhere to the coopetitive architecture. The security and reliability of the coopetitive smart cards would be a key issue which is dealt with separately in the ICOM and UCOM scenarios. However, we consider that further work would only strength the contribution that an open and dynamic system can bring to the multi-application smart card architecture.

Before we discuss the smart card architecture that would support the coopetitive lifecycle; we list the fundamental attributes of the coopetitive architecture for multi-application smart cards.

1) The scheme manager (TSM) would enable the provision for the cardholders to request installation or deletion of any application as they require.
2) To provide privacy to the cardholders, the applications that they request to install or delete would not be revealed to the respective TSM. Unless the application in question is from an associate of the TSM. In that case the TSM would be notified of installation and deletion. For any independent entity (not related to the respective TSM), the identity of the application would be revealed to the TSM.
3) The security and reliability of the platform has to be decentralised. In scenarios where a cardholder does not want to reveal who is the active TSM of the card. The respective smart card would still be able to provide security assurance and validations in a unlink-able way. The unlink-ability relates to the mechanism that does not rely on the TSM, but on the independent third party's evaluation (i.e. Common Criteria Evaluations [12, 25, 44]). The property of the unlink-ability would be that application providers that does not belong to the respective TSM will not know whether the requesting user with with a particular TSM or not. Similarly, the respective TSM should not know whose application is being requested to be installed or deleted from the secure element.
4) The cardholder should be given the choice to change the TSM if they require after meeting terms and conditions of the original TSM. This would enable the cardholders to move the TSMs that they consider provide them best service. Obviously, the original TSM has made investment in the platform that is issued to the cardholder. Therefore, cardholder would have to honour any terms and conditions that she agreed at the time of acquiring the secure element.
5) If a cardholder does not want to be with any of the TSM, then the framework should move back to default UCOM architectures. Similarly, the TSMs would also have the choice to remove the privileges of a cardholder to install or delete applications; if it does not conforms with the TSM's terms and conditions.

VII. Conclusion and Future Research Directions

In this paper, we started the discussion on the reasons behind why the multi-application smart card initiative failed in 1990s. Most of the reasons behind this lack of adoption was due to business issues that were closely related to the smart card ownership model. However, Near Field Communication (NFC) technology has reinvigorated the multi-application smart card initiative — the smart car ownership model is still adheres of the ICOM. We consider that the TSM model has potential but there are scalability and market segmentation issues that may hinder its adoption. The UCOM on other hand breaks away from all traditional notion of smart card ownership model but it might not gain wide spread acceptance in the smart card industry. Joining the TSM and UCOM into the coopetitive architecture delivers the benefits of the both models, along with satisfying their unique requirements.

This paper provides the ground work for the coopetitive architecture, and as part of our future research directions we would like to explore the effect of coopetitive architecture on the individual operations, security, privacy and reliability of the smart cards. This includes looking the runtime environment, spaces and domain management, inter-application communi-

cation, security attestation based on PUF and common criteria, application management that includes application installation, and deletion — to name a few.

REFERENCES

[1] D. Deville, A. Galland, G. Grimaud, and S. Jean, "Smart Card Operating Systems: Past, Present and Future," in *In Proceedings of the 5 th NORDU/USENIX Conference*, 2003.

[2] K. Markantonakis, "The Case for a Secure Multi-Application Smart Card Operating System," in *ISW '97: Proceedings of the First International Workshop on Information Security*. London, UK: Springer-Verlag, 1998, pp. 188–197.

[3] Z. M'Chirgui, "The Economics of the Smart Card Industry: Towards Coopetitive Strategies," *Economics of Innovation and New Technology*, vol. 14, no. 6, pp. 455–477, 2005.

[4] "Framework for Smart card Use in Government," Foundation for Information Policy Research, Consultation Response, 1999.

[5] S. Chaumette and D. Sauveron, "New Security Problems Raised by Open Multiapplication Smart Cards." *LaBRI, Université Bordeaux 1.*, pp. 1332–04, 2004.

[6] "Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications," White Paper, November 2006.

[7] NFC Trials, Pilots, Tests and Live Services around the World. Online. NFC World.

[8] R. N. Akram, K. Markantonakis, and K. Mayes, "A Paradigm Shift in Smart Card Ownership Model," in *Proceedings of the 2010 International Conference on Computational Science and Its Applications (ICCSA 2010)*, B. O. Apduhan, O. Gervasi, A. Iglesias, D. Taniar, and M. Gavrilova, Eds. Fukuoka, Japan: IEEE Computer Society, March 2010, pp. 191–200.

[9] "Pay-Buy-Mobile: Business Opportunity Analysis," GSM Association, White Paper 1.0, November 2007.

[10] "The GlobalPlatform Proposition for NFC Mobile: Secure Element Management and Messaging," GlobalPlatform, White Paper, April 2009.

[11] J. Guaus, L. Kanniainen, P. Koistinen, P. Laaksonen, K. Murphy, J. Remes, N. Taylor, and O. Welin, "Best Practice for Mobile Financial Services: Enrolment Business Model Analysis," Mobey Forum Mobile Financial Services Ltd., Helsinki, Finland, Online, June 2008.

[12] R. N. Akram, K. Markantonakis, and K. Mayes, "A Dynamic and Ubiquitous Smart Card Security Assurance and Validation Mechanism," in *25th IFIP International Information Security Conference (SEC 2010)*, ser. IFIP AICT Series, K. Rannenberg and V. Varadharajan, Eds. Brisbane, Australia: Springer, September 2010, pp. 161–172.

[13] A. M. Brandenburger and B. J. Nalebuff, *Co-Opetition : A Revolution Mindset That Combines Competition and Cooperation : The Game Theory Strategy That's Changing the Game of Business*, 1st ed. Doubleday Business, Dec. 1997.

[14] P. Girard, "Which Security Policy for Multiplication Smart Cards?" in *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology*. Berkeley, CA, USA: USENIX Association, 1999, pp. 3–3.

[15] *EMV 4.2 : Book 1 - Application Independent ICC to Terminal Interface Requirements, Book 2 - Security and Key Management, Book 3 - Application Specification, Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements*, EMVCo Std. 4.2, May 2008.

[16] *GlobalPlatform: GlobalPlatform Card Specification, Version 2.2,*, GlobalPlatform Std., March 2006.

[17] *Java Card Platform Specification: Classic Edition; Application Programming Interface, Runtime Environment Specification, Virtual Machine Specification, Connected Edition; Runtime Environment Specification, Java Servlet Specification, Application Programming Interface, Virtual Machine Specification, Sample Structure of Application Modules*, Sun Microsystem Inc Std. Version 3.0.1, May 2009.

[18] *ISO/IEC 18092: Near Field Communication - Interface and Protocol (NFCIP-1)*, International Organization for Standardization (ISO) Std., April 2004.

[19] K. Mayes and K. Markantonakis, Eds., *Smart Cards, Tokens, Security and Applications*. Springer, 2008.

[20] J. Laugesen and Y. Yuan, "What Factors Contributed to the Success of Apple's iPhone?" in *Proceedings of the 2010 Ninth International Conference on Mobile Business / 2010 Ninth Global Mobility Roundtable*, ser. ICMB-GMR '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 91–99.

[21] (2008, March) The Apple iPhone: Success and Challenges for the Mobile Industry. Online. Rubicon Consulting Inc. California, USA.

[22] "Mobile NFC Services," GSM Association, White Paper Version 1.0, 2007.

[23] (2007, October) The Role and Scope of EMVCo in Standardising the Mobile Payments Infrastructure. Online. EMVCo. California, USA.

[24] R. N. Akram, K. Markantonakis, and K. Mayes, "Application Management Framework in User Centric Smart Card Ownership Model," in *The 10th International Workshop on Information Security Applications (WISA09)*, H. Y. YOUM and M. Yung, Eds., vol. 5932/2009. Busan, Korea: Springer, August 2009, pp. 20–35.

[25] ——, "Simulator Problem in User Centric Smart Card Ownership Model," in *6th IEEE/IFIP International Symposium on Trusted Computing and Communications (TrustCom-10)*, H. Y. Tang and X. Fu, Eds. HongKong, China: IEEE Computer Society, December 2010.

[26] I. Bakdi, "Towards a Secure and Practical Multifunctional Smart Card," in *Smart Card Research and Advanced Applications*, ser. Lecture Notes in Computer Science, vol. 3928. Berlin: Springer, 2006, pp. 16–31.

[27] R. N. Akram, K. Markantonakis, and K. Mayes, "Location Based Application Availability," in *On the Move to Meaningful Internet Systems: OTM 2009 Workshops*, R. M. P. Herrero and T. Dillon, Eds., vol. 5872/2009. Vilamoura, Portugal: Springer, November 2009.

[28] *Multos: The Multos Specification,*, Online, Std.

[29] R. N. Akram, K. Markantonakis, and K. Mayes, "Firewall Mechanism in a User Centric Smart Card Ownership Model," in *Smart Card Research and Advanced Application, 9th IFIP WG 8.8/11.2 International Conference, CARDIS 2010*, D. Gollmann, J.-L. Lanet, and J. Iguchi-Cartigny, Eds., vol. 6035/2010. Passau, Germany: Springer, April 2010, pp. 118–132.

[30] J. Vincent, "Affiliations, Emotion and the Mobile Phone," in *Cross-Modal Analysis of Speech, Gestures, Gaze and Facial Expressions*, ser. Lecture Notes in Computer Science, A. Esposito and R. Vích, Eds. Springer, 2009, vol. 5641, pp. 28–41.

[31] M. E. Porter, "How Competitive Forces Shape Strategy," *Harvard Business Review*, vol. 57, no. 2, 1979.

[32] J. R. Bettman, M. F. Luce, and J. W. Payne, "Constructive Consumer Choice Processes," *Journal of Consumer Research: An Interdisciplinary Quarterly*, vol. 25, no. 3, pp. 187–217, December 1998.

[33] D. Kahneman, "Maps of Bounded Rationality: Psychology for Behavioral Economics," *American Economic Review*, vol. 93, no. 5, pp. 1449–1475, December 2003.

[34] L. Borghans, A. L. Duckworth, J. J. Heckman, and B. ter Weel, "The Economics and Psychology of Personality Traits," Geary Institute, University College Dublin, Working Papers 200827, Dec. 2008.

[35] M. Bodker, G. Gimpel, and J. Hedman, "Smart Phones and Their Substitutes: Task-Medium Fit and Business Models," *Mobile Business, International Conference on*, vol. 0, pp. 24–29, 2009.

[36] D. Sauveron, "Multiapplication Smart Card: Towards an Open Smart Card?" *Inf. Secur. Tech. Rep.*, vol. 14, no. 2, pp. 70–78, 2009.

[37] Z. M'chirgui, O. Chanel, and D. Calcei, "Why are some coalitions more successful than others in setting standards? Empirical evidence from the Blu-ray vs. HD-DVD standard war," HAL, Working Papers halshs-00543972, Dec. 2010.

[38] Y. Luo, "A coopetition perspective of global competition," *Journal of World Business*, vol. 42, no. 2, pp. 129 – 144, 2007.

[39] K. Walley, "Coopetition An Introduction to the Subject and an Agenda for Research," *International Studies of Management and Organization*, vol. 37, no. 2, pp. 11–37, August 2007.

[40] I. D. Constantiou, J. Damsgaard, and L. Knutsen, "Exploring perceptions and use of mobile services: user differences in an advancing market," *Int. J. Mob. Commun.*, vol. 4, pp. 231–247, February 2006.

[41] K. H. Shih, H. F. Hung, and B. Lin, "Assessing user experiences and usage intentions of m-banking service," *Int. J. Mob. Commun.*, vol. 8, pp. 257–277, May 2010.

[42] N. Mallat, "Exploring consumer adoption of mobile payments - A qualitative study," *J. Strateg. Inf. Syst.*, vol. 16, pp. 413–432, December 2007.

[43] H. H. Bauer, T. Reichardt, S. Exler, and E. Tranka, "Utility-based design of mobile ticketing applications a conjoint-analytical approach," *Int. J. Mob. Commun.*, vol. 5, pp. 457–473, March 2007.

[44] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Part 2: Security Functional Requirements, Part 3: Security Assurance Requirements,*, Common Criteria Std. Version 3.1, August 2006.