Collaborative and Ubiquitous Consumer Oriented Trusted Service Manager

Raja Naeem Akram,
Department of Computer Science
University of Waikato.
Waikato, New Zealand
Email: R.Akram@rhul.ac.uk

Konstantinos Markantonakis
ISG Smart Card Centre,
Royal Holloway, University of London.
Egham, United Kingdom
Email: K.Markantonakis@rhul.ac.uk

Damien Sauveron
XLIM (UMR CNRS 7252 / Université de Limoges)
Département Mathématiques Informatique.
Limoges, France
Email: damien.sauveron@unilim.fr

***Abstract*—Near Field Communication (NFC) enables a mobile phone to emulate a contactless smart card. This has reinvigorated the multiapplication smart card initiative. Trusted Service Manager (TSM) is an entity that is trusted by all stakeholders in the proposed and trialled NFC-based smart card ecosystem. However, TSM-based models have the potential to create market segregation that might lead to limited or slow adoption. In addition, all major stakeholders (e.g. Telecom and banks) are pushing for their own TSM models and this might hinder deployment. In this paper we present a Collaborative and Ubiquitous Consumer Oriented Trusted Service Manager (CO-TSM)-based model that combines different TSM models while providing scalability to the overall architecture. In addition, our proposal also provides flexibility to both consumers and application providers. To support our proposal, we present a core architecture based on two contrasting approaches: the Issuer Centric Smart Card Ownership Model (ICOM) and the User Centric Smart Card Ownership Model (UCOM). Based on the core architecture, we then describe our proposal for an application download framework and a secure channel protocol. Finally, the implementation experience and performance measurements for the secure channel protocol are discussed.**

***Index Terms*—Smart Cards, Near Field Communication, Trusted Service Manager, GlobalPlatform, Java Card, Multos, User Centric Smart Cards.**

I. Introduction

Near Field Communication (NFC) technology has brought new life to multiapplication smart card technology. Despite there being a substantial number of smart cards in existence that can support multiple applications, there are not many deployments that can claim to have applications from multiple organisations on the same smart card [1]. Initially, there were some reservations regarding multiapplication smart card technology [2]–[4]. The smart card industry had numerous cooperative successes [5, 6] and in the early days of the multiapplication smart card initiative it was thought that diverse organisations would come together to offer their services via a single smart card. Unfortunately this momentum was short lived. The Issuer Centric Smart Card Ownership (ICOM) became, and still is, the most prevalent model for smart card-based services [7].

NFC is a technology that enables a mobile phone to emulate a smart card. It is not a deployment model that resolves potential issues with multiapplication smart card initiatives. The Trusted Service Manager (TSM) architecture was proposed to fill the need for a deployment model. NFC-based trials have been carried out in around 70 countries [8] and the most prominent model evaluated is based on the TSM. At a very simplistic level, a TSM is a trusted authority that brokers the relationship between a smart card and application providers. Almost every stakeholder in the smart card industry can take the role of a TSM. Traditional stakeholders in the smart card industry are card manufacturers and card issuers (banks, Telecom, and transport agencies). This is both an encouraging and a potentially discouraging development, as it has similarities to ICOM and as such might decelerate the deployment of any such schemes.

A number of variants for TSM-based models have been proposed and in each of these proposals the crucial role of a TSM is argued to be suitable for a particular industry (e.g. banks, or telecoms). To potentially avoid market fragmentation and create consumer-oriented framework, a model that is convergent and inclusive of all stakeholders including (especially) consumers[1] is required. In this proposal, we offer a model called the Consumer Oriented Trusted Service Manager (CO-TSM). It allows any TSM to interact with any other TSM or Service Provider[2] (SP), thus creating a collaborative, ubiquitous and scalable deployment model. In addition, we briefly explore few of the existing proposals and smart card architectures, putting them forward as evidence that our proposed model can be supported by existing technologies with minimal modifications. We discuss two variants of the CO-TSM, one based on the ICOM and other based on the User Centric Smart Card Ownership Model (UCOM) [7].

The UCOM can be considered as a contrasting approach to the ICOM. In the UCOM, individual users are given the "freedom of choice" that basically entitles them to install or delete any application they require after authorisation from the respective SPs. An SP has complete control of its application (but not the smart card on which its application is installed) and it has to explicitly sanction the application-download to

[1]In this paper, card users are termed users, consumers, or cardholders. All of these terms are used interchangeably.

[2]Service Provider (SP): An entity that has developed a smart card application to offer services to its customers. The role of an SP is similar to that of an application provider in the ICOM.

each user [9]. However, the control of the smart card, as defined by "freedom of choice," resides with its user.

A. Contribution

In this paper, our main focus is on TSM-based deployment models and smart card architectures (i.e. Java Card [10], GlobalPlatform [11] and Multos [12]). The salient contributions of this paper are as follows:

1) A discussion of TSM-based models and specially the GSMA's proposals
2) The proposed deployment architecture for CO-TSM
3) A detailed description of how a CO-TSM can be deployed in the ICOM based architecture
4) Proposals for how a CO-TSM can be extended to be a collaborative and ubiquitous CO-TSM based on the UCOM architecture

The objective of the paper is to provide a foundation for CO-TSM and show that alternative models for NFC-based smart card services are possible, especially the ones that consider users as crucial stakeholders in any potential future deployments.

B. Structure of the Paper

Section II discusses the TSM proposal. In section III, we briefly discuss the GSMA's TSM deployment models and also discuss potential issues associated with existing TSM-based models. In section IV we discuss two potential approaches for CO-TSM deployment based on ICOM and UCOM proposals. These proposals also indicate that the smart cards' core architecture has matured sufficiently to support new and innovative proposals like the CO-TSM. In section V, we discuss how the proposed model can be implemented with minimal changes to existing proposals. Analysis and future research directions are detailed in section VI and section VII concludes the paper.

II. Trusted Service Manager (TSM)

In this section, we discuss the generic architecture for a Trusted Services Manager (TSM) in the smart card industry.

In NFC trials around the world [8], the principal framework deployed is an extension of the ICOM model and is referred as the TSM [13]. It has gained support from the banking and Telecom sectors [14, 15].

The given TSM architecture is illustrated in Figure 1, which shows two TSM networks: namely TSM-1 and TSM-2. Each network has a Mobile Network Operator (MNO), a Card Issuing Bank (CIB), a Transport Service Operator (TSO) and a Leisure Centre (LC) as the scheme partners. The TSM acts as a trusted broker for the corresponding applications on the issued smart cards. A customer C_A receives a smart card (SC_A) from TSM-1. Customer C_A would only be able to have applications on SC_A from MNO_1, CIB_1, TSO_1, and LC_1. Similarly, C_C can only obtain applications from the respective scheme partners of TSM-2.

From an operational point of view, the TSM proposal is an extension of the existing ICOM. In ICOM, smart cards are issued by a card issuer and this entity manages the security

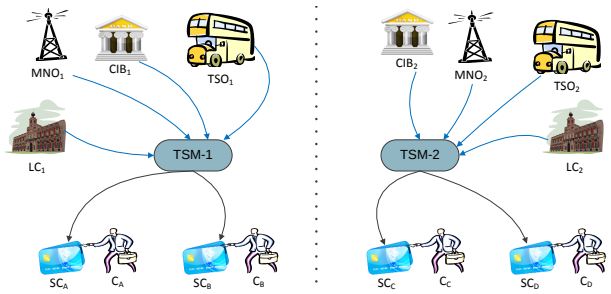

Figure 1. Generic TSM Deployment Architecture

and operational aspects of their cards. A user has to be a customer of the card issuer to gain a smart card. They can have applications from other application providers, but these applications have to be vetted by the card issuer. Each application provider has to abide by the terms and conditions (T&Cs) of the relevant card issuer. All activities related to card management (i.e. application installation, blocking, unblocking, deletion and enforcing security policies) are handled by the card issuer. In many respects, the TSM proposal in its simplest version is similar to the ICOM. TSM-based deployments can use different card management frameworks like Multos and GlobalPlatform: there are no restrictions imposed by the TSM on the choice of actual Smart Card Operating System (SCOS) or card management framework. We did not list the Java Card specification along with Multos and GlobalPlatform management frameworks, because most of the deployed Java Cards in the field use GlobalPlatform's management framework; therefore, discussion on GlobalPlatform's management framework implicitly also includes Java Cards.

The rationale behind including an entity that takes the role of a TSM is to resolve the issues that have plagued ICOMs in relation to the collaborative deployment of smart cards that have applications from diverse organisations. Therefore, the role of the TSM is to create a single (potentially neutral) entity that provides certain features to facilitate smart card management operations. Taking a generalised view of the role of a TSM, it should provide features briefly discussed in the following sections.

1) Relationship Management: Smart cards have proliferated in many aspects of modern life. Therefore, there are a number of SPs that serve their customers via smart cards. Any proposal for a multiapplication smart card has to include a mechanism to establish and manage relationships with SPs. Relationship management enables SPs to deliver their applications on TSM-managed smart cards that are issued by respective card issuers. A TSM can also manage more than one card issuer, thus enabling an SP to establish a relationship (contractual agreement) with a single TSM, providing the ability to install its application on smart cards issued by different card issuers. In addition, the TSM can also facilitate an SP in application management tasks: installation, deletion, update, and blocking/unblocking the relevant application.

2) Trust Management: One of the major concerns with multiapplication smart cards that have applications from dif-

ferent SPs is assuring each SP that the platform and its applications are secure. Each SP might have a different set of security requirements: TSMs will ensure that an SP's application will only be installed on smart cards that meet its security requirements. Similarly, the TSM also assures card issuers that the installed application will not violate their security policies. Therefore, TSMs act as trusted entities that manage the security expectations of both SPs and card issuers.

3) Business Management: One of the main motivations for card issuers to open their smart cards to other applications is to generate some sort of revenue. The TSM may manage these business aspects on behalf of the relevant card issuers. For an SP to get its application on a smart card, it may have to pay a small fee to the TSM. The fees collected from different SPs by the TSM might then be transferred to the respective card issuers after taking a certain commission for managing the services.

III. Models for TSM based Deployment

In this section, we present who will be the TSM into the GSMA's proposals for TSM-based deployment models. Due to space constraints, we the Multos Card Management Architecture [12] and GlobalPlatform's [17] proposals are not detailed but they are discussed in subsequent discussions. However, they will be mentioned in the subsequent discussions.

A. GSMA's Proposals

The GSMA represents the interests of mobile operators worldwide. Therefore, to safeguard the MNOs' stake in any future TSM-based deployments, the GSMA has published a couple of white papers [14, 16]. In this paper, we will only discuss the most recent publication: [16] as it includes the main discussion points of the [14] along with most recent assestment of the GSMA about the NFC based services market. The GSMA proposal puts special emphasis on the role of the MNO and it also proposes three potential modes listed in subsequent sections. Dotted lines shown in Figures 2 to 4 represent the business consideration (i.e. monetary and administrative consideration) in the proposal and we do not discuss them in this paper. These considerations are important but beyond of scope of this paper, which deals with the technical architecture to support NFC-based smart card services.

1) Mode 1: MNO as TSM: Similar to the simple mode discussed in the previous section, this section gives complete control of a TSM to the MNO as depicted in Figure 2.

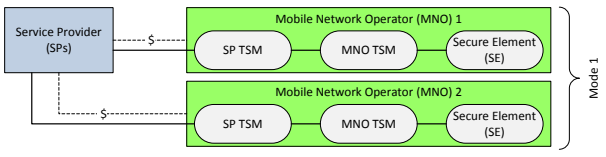

Figure 2. GSM Proposal for TSM: Mode 1

2) Mode 2: SP TSM as a Technical Aggregator: In this mode, the SP TSM acts as a technical aggregator and applications are installed on the secure element after obtaining the explicit permission of the MNO (Figure 3). The role of the SP TSM is to maintain the SP's relationships with different MNO-based TSMs. The SP TSM is logically a different entity that safeguards and manages its relationships with MNO TSMs. This proposal is put forward to potentially avoid market segmentation and provide a scalable TSM-based deployment model. We will return to these issues later in section III-B.

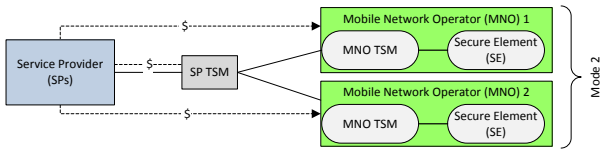

Figure 3. GSM Proposal for TSM: Mode 2

3) Mode 3: SP TSM as a Technical and Business Aggregator: In this mode, the SP TSM, along with being a technical aggregator, will also become a business aggregator as shown in Figure 4. The business aggregator role gives the SP TSM the right to market and sell the MNO TSM's services to third parties. The difference between mode 2 and 3 is the capacity of an SP TSM to resell the MNO TSM's business services.

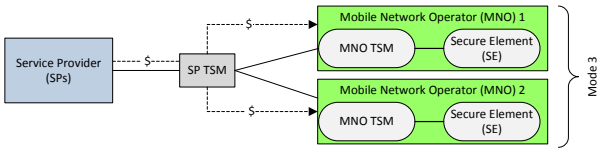

Figure 4. GSM Proposal for TSM: Mode 3

The mode descriptions in this section show that the TSM is not only important from the point of view of the technical management of cards, but also from the business perspective. Another important point to note is that all three modes discussed in this section do not include any relationships between MNO TSMs (i.e. MNO 1 and MNO 2).

We have discussed proposals from two different organisations. While these models are not an exhaustive list, the variants discussed provide a basic understanding of what these different organisations are recommending as the best possible deployment model. Keeping in mind the variants discussed here, in the next section we examine the shortcomings of potentially all proposed variants of TSM-based deployment models.

B. Issues with Proposed TSM and its Deployment Models

Based on the discussion in previous sections, it can be seen that the TSM for any NFC-based multiapplication smart card has some important responsibilities. These are the main reasons why TSM-based models were proposed for multiapplication smart cards. In the early days of multiapplication smart card technology, ICOM was considered adequate and it assisted in the proliferation of smart card technology. However,

ICOM was also one of the crucial reasons for the deceleration of the multiapplication smart card initiative [7]. Although TSM is an extension of ICOM, it is nevertheless a fresh endeavour to find an amicable solution for all stakeholders in the smart card industry.

However, most of the proposed variants of TSM-based deployment models (e.g. GSMA [16], GlobalPlatform [17], Multos Card Management Architecture [12]) suffer from major issues that might become an "Achilles heel" and smart card technology has been in this position before, in the latter part of the 1990s. In subsequent sections, we will discuss potential concerns with the existing proposals. This discussion also provides the rationale for our proposal.

1) Market Segmentation: The TSM architecture is illustrated in Figure 1 in which we have two TSM networks: TSM-1 and TSM-2. Each has a partnership with an MNO, a CIB, a TSO and an LC. Customer C_A who receives a smart card (SC_A) from TSM-1 would only be able to have applications on SC_A from MNO_1, CIB_1, TSO_1, and LC_1. However, if C_A does banking with CIB_2 that is associated with TSM-2, she has to either acquire a new smart card from TSM-2 or change banks, effectively creating market segmentation. Alternatively, CIB_2 has to establish relationships with all possible TSMs, which might not be practically feasible.

2) Scalability: The limited scalability arises because not all application providers can establish or manage a relationship with every possible TSM. Modes 2 and 3 depicted in Figures 3 and 4 attempt to resolve this issue by creating another (logical) entity termed an SP TSM. The SP TSM's role is to manage all relationships between an SP and potentially all TSMs the SP wants to be associated with. This in our opinion does not resolve the issue. Whether the SP manages these relationships itself or the SP TSM (logical entity of SP) manages it for the SP, in reality, it does not make any difference.

3) Flexibility: To be part of a collaborative scheme offered by a TSM, SPs might be required to pay a subscription fee. Therefore, small- or medium-scale organisations like local libraries, universities, and health centres may not be able to afford to be associated with a TSM. We consider that such a barrier would reduce a scheme's flexibility.

4) Ubiquitousness: Such systems lack true ubiquitousness, as different countries might opt for having their own independent TSMs. Therefore, tourists or business travellers would face difficulties in acquiring applications (e.g. applications from a TSO) in a foreign country where they do not have any presence. It is difficult to assume that a single company might have global presence in each and every country. In addition, even if a mobile operator has established relationships with a multitude of MNOs in other countries (e.g. as done for roaming services) it might be difficult for a user to download/install applications from the SPs in a foreign country using roaming style TSMs. Such a potential solution is not part of the current TSM based proposals; however, our proposed framework in this paper does facilitate such a scenario. Other issues related to the existing systems include ownership privileges, customer loyalty, customer relationship management, card surface marketing, and potential revenue generation opportunities as discussed in [2, 4, 7, 18].

5) Consumers: Almost all TSM variants focus exclusively on industrial stakeholders. We were unable to find any TSM variants that include consumers as genuine stakeholders in any potential deployment model. The cause is the core principles of the ICOM, which also do not focus significantly on consumers. We consider that consumers should be included in any potential TSM-based deployment model and our proposed solution gives them a stronger role.

In this entire process of developing an amicable solution based on TSM proposal, one set of stakeholders that is crucial to the survival of all other entities in the TSM ecosystem is missing: the users (consumers) of the system, which we consider to be a gross oversight. An amicable solution that includes all stakeholders (including users) would be beneficial for the success of multiapplication smart card initiatives.

IV. Proposed Consumer Oriented Trusted Service Manager based Model

In this section we discuss the proposed model for a CO-TSM-based model, along with the challenges and opportunities offered by the proposal.

A. Proposed Architecture

As pointed out by Porter [19], the crucial elements that stimulate competition and innovation in an industry are: a) the threat of new entrants, b) the threat of substitute products or devices, and c) consumer power (culture). For the smart card industry, these elements are present in a multitude of forms. The provision of applications on a mobile phone has enabled new entrants to venture into traditionally monopolised industries like the payment sector. Companies like PayPal, Google or any other third party can offer a mobile payment service. In addition smart phones, with the inclusion of NFC functionality, can provide a substitute for traditional smart card applications like transport ticketing and access control [20]. Technology savvy consumers require more features on a device, a need [21] which is successfully fulfilled by high-end smart phones (e.g. Android handsets). Smart cards are lagging behind in providing such possibilities. NFC technology provides an opportunity for the convergence of different services on a single smart card but concerns regarding the exact role of the TSM and who will be the TSM may have reduced the momentum. The proposed architecture based on a "Consumer Oriented Trusted Service Manager (CO-TSM)" enables a highly scalable and flexible alternative. The proposed architecture is depicted in Figure 5 and explained below.

The CO-TSM-based model enables a user to access/install an application even if the respective SP is not a member of the relevant CO-TSMs. In this model, a user (C_A) can request installation of an application from an application provider (e.g. MNO, CIB, TSO and LC) that is a member of any CO-TSM. The application installation is still authorised/overseen by the scheme manager — for example, CO-TSM-1 in Figure 5 is the scheme manager for SC_A as it has issued the smart card

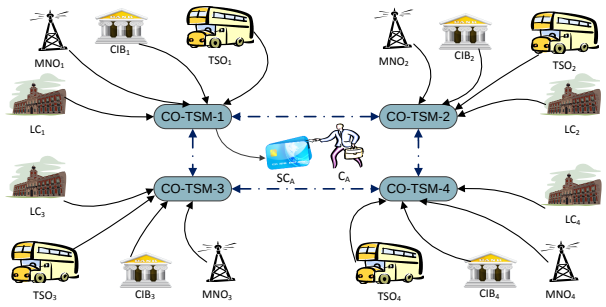

Figure 5. Generic Overview of the Model for Consumer Oriented Trusted Service Manager

to customer C_A or manages the card on behalf of the card issuer. A point to note for an SP to lease an application to a smart card, the CO-TSMs that are managing both the application and the smart cards may or may not have an offline relationship. It can be argued that the CO-TSM also faces with the scalability issues, as SPs that are associated with any of the CO-TSM cannot lease their application to the respective smart card (e.g. SC_A). However, it is still comparatively better than the traditional proposals mentioned in section III (i.e. GSMA [16], GlobalPlatform [17], and Multos Card Management Architecture [12]). Individual CO-TSMs in a grouping can be deployed based on an alternative discussed in section III-A. The dotted lines in Figure 5 indicate that applications from different CO-TSMs can be installed to any smart card that is under the management of any of these CO-TSMs, and it does not necessarily signify any offline relationships.

The role of the CO-TSM is very similar to that of the TSM, as discussed in section II except for one crucial feature. The proposed model enables an application to be installed even when it is not from a partner, as long as it satisfies the security/business requirements of the smart card. Similarly, it provides an assurance to the relevant SP that the smart card meets its security requirements. In addition, to make the proposed model flexible it will even allow application installations from SPs that do not pay the TSM directly for the service: in such situations it might charge a fee to the card user. This model also gives users the ability to request an application installation or deletion and the CO-TSM, in most instances, will comply with the user's request. Such a privilege was not even considered in the proposed TSM framework or any of the deployment models (e.g. GSMA [16], GlobalPlatform [17], Multos Card Management Architecture [12]). Salient features of the CO-TSM will include:

1) A CO-TSM will manage the relationships between card issuers, SPs and users. The concept of a CO-TSM is to provide an unbiased broker service that safeguards the interests of each of the stakeholders. Traditional card issuers want to keep control of their smart cards, while SPs issue their applications to as large a population as possible. Similarly, users want to download and use any application they require.
2) The CO-TSM becomes a security attestation and validation broker that is based on a security validation mechanism. The security validation mechanism [7] is based on the Common Criteria (CC) evaluation and certification [22], which is a widely accepted security evaluation scheme in the smart card industry. Security and operation evaluation by the CC will act as proof that the relevant smart card meets the SP's security requirement. However, the SP can also request online security attestation and validation proof signed by the respective CO-TSM. This is to provide a strong assurance of the security features of the smart card to the respective SP.
3) Each card issuer requires that any installed application will not damage its issued smart cards. In addition, the card issuer may also like to charge a fee for application installation. The assurance of applications' behaviour can either be provided by CC evaluation or by the scheme manager (i.e. the CO-TSM) associated with the SP. The charging mechanism can involve charging either the SP or the user and will be decided during the application installation protocol (section V-C). Instead of the CO-TSM ensuring the application's behaviour, protection mechanisms against malicious applications should be implemented at the smart card level.

Each CO-TSM can support any deployment model mentioned in section III (e.g GSMA). The proposed model does not concern with who is taking the role of the CO-TSM or under which deployment model (section III) it is rolled out. The only crucial point is that it supports the above listed (modified) features.

For a CO-TSM proposal to become a fully collaborative and ubiquitous model, it should support the additional requirements listed below:

4) A user has the "freedom of choice" to install any application she requires, even if the respective SP of the application is not member of any of the CO-TSMs.
5) A user can acquire (purchase) her own smart card and this smart card might not have any card issuer. She could then join a CO-TSM and can delegate the management of the smart card to it.

The collaborative and ubiquitous CO-TSM does not suffer from the scalability and flexibility issues discussed previously. It gives the consumer the true choice to install any application whether the respective SP is a member of any CO-TSM or not.

B. Deployment Challenges and Opportunities

The proposed CO-TSM-based model based on the first three points (section IV-A) in a limited sense enables users' choice, giving them the privilege to install any application they might require — as long as the respective SP has partnered with a CO-TSM. To do so, the proposed model has to face many challenges. The CO-TSM takes on responsibility for smart card security and has to provide assurances to SPs with which it might have no direct contractual agreement. Therefore, the smart card architecture has to be adequately modified to provide such assurances and also safeguard the interests (i.e. applications and SCOS) of both SPs and card issuers.

The next challenge is associated with the application download processes that initiates communication between the CO-TSM and the respective SP. The application download process should provide a secure and trusted protocol, remote security attestation and validation and charging mechanisms (fee payment if applicable). Once the application is downloaded, it requires a secure and reliable platform that is part of the smart card architecture. The application can be managed by the SP including application deletion and blocking/unblocking operations. In addition, the model should enable the user to request application installation and deletion as required. The CO-TSM will follow the requests of the card user and perform these tasks on her behalf.

The proposed CO-TSM (based on the first three points in section IV-A) seems like an extension of the existing ICOM-based proposals. However, the inclusion of the users' rights and removal of any previous (offline) partnership between the respective CO-TSMs and SPs increases the scalability, and flexibility of the traditional TSM proposal. In addition, if a CO-TSM supports points four and five (section IV-A) then the proposal moves closer to a UCOM rather than ICOM. With regards to supporting such a CO-TSM model, we use our experience from the development of the UCOM architecture and adjust it to support the CO-TSM. If the CO-TSM supports all five points discussed in section IV-A, it will intrinsically support the ICOM and UCOM together. In subsequent sections, we explore the pros and cons of deployment of CO-TSM proposal based on ICOM or UCOM architecture.

C. CO-TSM based on Issuer Centric Smart Card Ownership Model (ICOM)

The ICOM is deeply founded on the notion of centralised control (i.e. card issuer) and least privileges to users in terms of application download or deletion. Building a CO-TSM based on such a model is possible if we consider that CO-TSMs will form syndicates and let users choose the applications they require on their smart cards. Such a model requires three elements: 1) all CO-TSMs establish an offline trust relationship, 2) SPs have to establish relationships with at least one of the CO-TSMs that are part of the syndicate and 3) introduces the role of the consumer in the deployment model in a limited sense. These three requirements create the same issues discussed in section III-B.

Beside the traditional ICOM proposal, GlobalPlatform has proposed the GlobalPlatform Consumer-Centric Model (GP-CCM) [23] that proposes delegation of some privileges to the individual consumers. This proposal has the potential to be incorporated as part of the CO-TSM and gives potentially more freedom to individual consumers. Although complete specifications for the Consumer-Centric Model are not yet published (only a white paper has been published on GP-CCM); however, in this section we discuss the potential CO-TSM based on this model.

The proposals of hierarchy for the Security Domains and Supplementary Security Domain Manager [23] can provide a strong smart card architecture to support different features of the CO-TSM. These proposals also help increase the rights of individual users to request installation and deletion of an application (as sanctioned by the card management authority: Card Issuer or CO-TSM). The GP-CCM as CO-TSM is a comparatively better option than the traditional ICOM architecture. However, the GP-CCM in its current state does not support all necessary services and architectural requirements to allow a collaborative and ubiquitous CO-TSM.

In the Multos deployment model [12], another ICOM based solution, it is very difficult to add consumer interactions. However, collaborative and ubiquitous, consumer-oriented TSMs are possible but they would require extensive modifications.

D. CO-TSM based on User Centric Smart Card Ownership Model (UCOM)

The User Centric Smart Card Ownership Model (UCOM) [7] gives a user complete "freedom of choice" that enables her to download and delete any application she requires. As the premise of the UCOM is that there is no centralised security authority, it creates unique challenges compared to the ICOM. The solution to most of these challenges requires a robust smart card architecture that satisfies many of the requirements and features of the CO-TSM.

The necessary modification to the UCOM is to accommodate the card issuer and CO-TSM, which can be achieved by modifying the Coopetitive Architecture [24]. The Coopetitive Architecture is based on the UCOM. It takes all the smart card architectural improvements carried out as part of the UCOM and includes the traditional TSM and card issuers. In the next section, we compare the UCOM- and ICOM (including GP-CCM)-based CO-TSM along with the base model that we have selected for the CO-TSM smart card architecture in this paper.

V. Implementation Framework for CO-TSM Model

In this section, we discuss the potential implementation of the CO-TSM-based model's core components. The implementation solution presented in this section supports both variants (three- and five-requirement supporting CO-TSM), which makes this solution the preferable option.

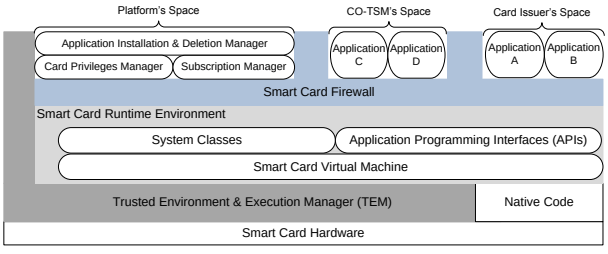

Figure 6. Smart Card Architecture

A. Smart Card Architecture

The proposed smart card architecture to support the CO-TSM-based model shown in Figure 6 is a modified version of the Coopetitive Smart Card (CSC) [25]. The CSC architecture is an extension of the GlobalPlatform specification for smart

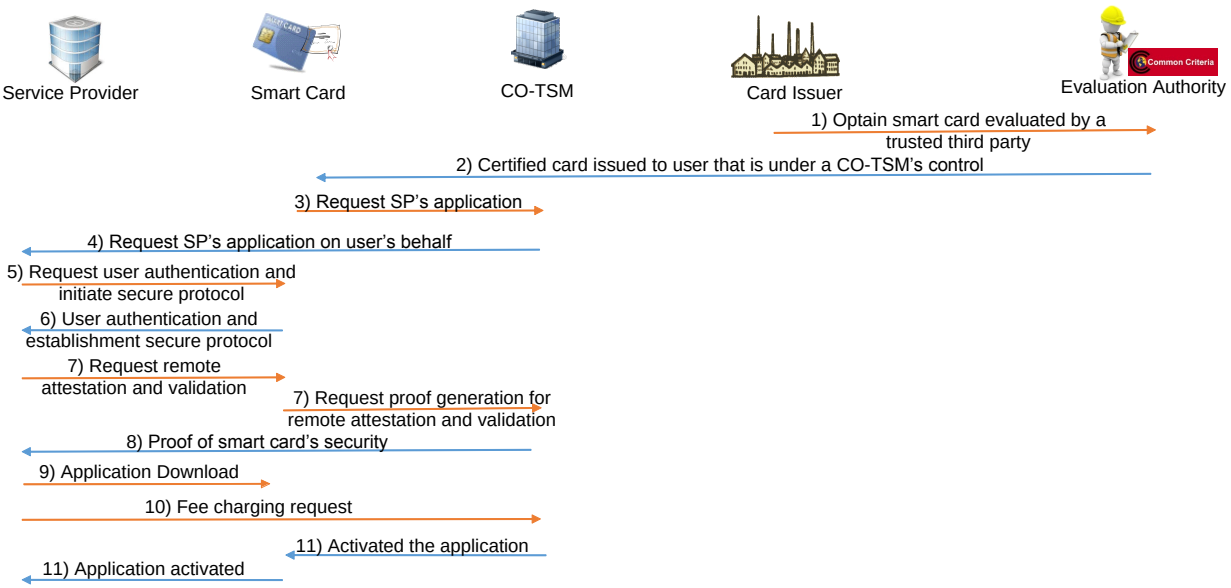

Figure 7. Application Installation Process

cards and UCOM architecture. The following discussion is restricted to those sections of the model that are modified to accommodate the proposed CO-TSM-based model.

Above the hardware layer, there is a new entity called the "Trusted Environment & Execution Manager (TEM)" [26] that basically provides a trusted computing platform for smart cards. The remote attestation and validation mechanism is based on the TEM and it is explained in detail in [27]–[29]. The platform space has platform-specific services including application installation, card privileges and subscription manager. The CO-TSM and card issuer's space are two (logically) separate application areas. These areas are under the respective control of the CO-TSM and the card issuer. All application management operations (i.e. card content management operations) including installation, deletion and blocking/unblocking of applications are controlled by the respective subscription managers of each of these application areas. The subscription manager provides a secure mechanism to the respective CO-TSM and card issuer to manage their applications areas. The card privileges manager enforces any policies defined by the card issuer in relation to the CO-TSM's space (e.g. whether CO-TSMs have to get explicit permission before any application installation or deletion operation). All application management operations related to the card issuer space are under the control of the card issuer — making this space emulate an ICOM-based architecture. In the card issuer space, the card issuer can install or delete any application as necessary. Neither the user nor the CO-TSM has any control in this space.

B. Application Installation Process

A card issuer will acquire smart cards from a card manufacturer, which has the smart cards certified by a trusted third party (e.g. Common Criteria evaluation laboratory) as represented by message 1 in Figure 7. On successful completion of the evaluation, the evaluation laboratory will issue a (cryptographic) certificate[3] to the smart card stipulating the security functionality (represented by message 2 in Figure 7). The card issuer will issue certified smart cards that are under the management of the CO-TSM to its customers. The application installation process initiates when the user requests application installation: the message sequence starting from the third message as depicted in Figure 7 and described below.

3) The smart card creates an application installation request based on the information provided by the user. The information includes the application and SP identifier along with the URL of the SP's application download server (from where a smart card downloads the SP's respective application).
4) The CO-TSM connects with the SP on behalf of the smart card and its user. This connection registers the request for application download onto the relevant smart card.
5) The SP then requests the user to authenticate, to validate whether the user is allowed to download the application or not. In addition, the SP also initiates the secure channel protocol.
6) A secure channel is established between the smart card and SP, after user authentication.
7) The SP requests the smart card to provide security attestation and validation proof, which is required to assure the SP that the smart card meets the security requirements of the SP and its current state is the same as it was at the time of third party evaluation certification. The smart card requests the CO-TSM to initiate the attestation process and on successful completion, it generates a security proof.
8) The proof is then communicated to the SP, which can independently verify it, and if it trusts the evaluation

[3]At present the certification bodies, based on the results of evaluation laboratories, only issue a paper-based certificate. However, proposals like those of Dusart and Sauveron [30], and Akram et al. [27] can be deployed to incorporate a digital (cryptographic) certificate.

certification authority it will accept the proof.

9) After verifying the evaluation certificate and attestation proof, the SP will proceed with the application download process to the respective smart card.
10) Once the application download is completed, the SP will request activation of the application. This may require payment of a CO-TSM fee for application installation. Either the SP or the user can take the charge.
11) Finally, the CO-TSM instructs the card to activate the application and once activated, it can communicate with the SP to confirm its status.

C. Application Installation Protocol

To achieve a practical implementation of the above process, we have modified a variant of Secure and Trusted Channel Protocol (STCP) that is detailed in [24]. For the remote attestation and validation mechanism, we have included the proposal in [28] in the modified protocol. The variant that we have modified is termed an "Application and Contractual Agreement Protocol (ACAP) [24]". This protocol not only establishes a secure and trusted channel but also generates a contractual agreement between the communicating parties along with managing any financial transactions among them.

The Authentication and Key Exchange (AKE) phase of the ACAP authenticates the user to the SP and also establishes a secure and trusted channel. The contract phase of the ACAP establishes a contractual agreement between the SP and CO-TSM (on behalf of the smart card). This agreement includes the Application Lease Policy (ALP) and smart card security policy. The ALP details the security and operational requirements that a smart card has to meet to install the application. The security policy stipulates the security and operational policy of the smart card that every application has to abide by. Finally, the charge phase negotiates who is going to be charged and how they are going to pay the fee. Performance measurements of all of these three phases are provided in Table I.

The architecture of the ACAP test-bed is based upon three entities: a smart card, an SP and two CO-TSMs. The entities SP and CO-TSM are implemented on a laptop with a 1.83 GHz processor, and 2 GB of RAM, running on Windows XP. The smart card entity is implemented on a 16-bit Java Card. The performance measures are taken from two different 16-bit Java Cards. For comparison, we have selected the SSL performance measured by Pascal Urien [31], TLS from Urien and Elrharbi [32], and (public key based) Kerberos by Harbitter and Menascé [33].

The rationale behind the choice of SSL and TLS for comparison lies in the GlobalPlatform specification [34], which specifies the adoption of TLS for NFC-based mobile service architecture. By comparison, the public key-based Kerberos is suitable for the Multos application management architecture [35]. Table I shows that the proposed protocol performs better than other listed protocols when we take in to consideration that these measurements include the time taken by the online attestation mechanism. All other protocols discussed provide neither an attestation feature nor any contractual and charge phase. Furthermore, the ACAP protocol was evaluated using CasperFDR [36] and no feasible attack(s) were identified.

VI. Analysis and Future Research Direction

The basic concerns with TSM-based models are market segmentation, limited scalability and flexibility, ubiquitousness and lack of consumer involvement (as discussed in section III-B). The design of the CO-TSM based model was to rectify all these concerns while keeping the basic architecture of the TSM intact. The proposal does not completely disassociate itself from ICOM or TSM: it includes the consumers in these architectures.

The proposed model, to a very large extent, enables a user to have a much broader choice of applications compared to other proposals including both the UCOM and the GP-CCM. Including users and bringing in the concept of security evaluation closely coupled with remote attestation assisted by trusted computing platforms has enabled the proposal to be scalable, flexible and ubiquitous. In addition, this model does not give preference to any stakeholder for the role of card issuer or CO-TSM. As long as the CO-TSM complies with the listed features discussed in section IV-A, the overall model does not create any segmentation in the market.

A preliminary application installation process was described in this paper, but we consider that the proposed smart card architecture requires additional focus. This focus includes the management of spaces that encompass user domains (GlobalPlatform application domains). However, the concept of how the management of spaces and applications can be carried out independently, with spaces managed by CO-TSM/card-issuer and application domains by respective SPs, is not explored in detail. Further refinement and evaluation is also required for the trusted computing platform for smart cards and how it can assist our proposed model.

VII. Conclusion

In this paper, we presented the existing TSM proposal and described the rationale behind it. We then extended our discussion to include proposals by GSMA for TSM-based deployment models that compete with proposals put forward or based upon GlobalPlatform and Multos Card Management Architecture, and the concerns associated with these divergent TSM approaches. The objective of discussing the concerns related to TSMs was to highlight issues that can decelerate commercial adoption and to provide a rationale for our proposal. In subsequent sections we described our proposed entity, referred to as CO-TSM, and its associated deployment model. We listed salient features of the CO-TSM and two potential scenarios of its deployment: CO-TSM based on ICOM and CO-TSM based on UCOM architecture. The main differentiator between these two scenarios is the degree of consumer inclusiveness to avoid market segmentation and saleability issues. We selected the UCOM based architecture as the preferable deployment model for the CO-TSM as it intrinsically supports both scenarios and it makes the proposal

Table I
PROTOCOL PERFORMANCE MEASURES (MILLISECONDS)

Protocols / Phases	SSL [31]	TLS [32]	Kerberos [33]	ACAP	
				Card One	Card Two
	32-bit	32-bit	32-bit	16-bit	16-bit
AKE Phase	4200	4300	4240	4347	4296
Contract Phase	-	-	-	1325	1924
Charge Phase	-	-	-	1587	1540
Total	-	-	-	7259	7760

a fully collaborative and ubiquitous solution. Furthermore, to support the proposed model, we provided implementation details of technical components that included smart card architecture, security evaluation, certification, attestation and the application installation process. Performance measurements for a modified ACAP protocol to support the proposed model were then presented.

Finally, we have demonstrated that there are potential innovative alternatives to existing TSM deployment models that should be considered for future commercial roll-outs.

REFERENCES

[1] 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.

[2] 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.

[3] S. Chaumette and D. Sauveron, "Some Security Problems Raised by Open Multiapplication Smart Cards," *10th Nordic Workshop on Secure IT-systems: NordSec 2005*, pp. 20–21, October 2005.

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

[5] R. A. Lindly, "The Age of Smart Cards: An Exploratory Investigation of the Sociotechnical Factors Influencing Smart Card Innovation," Ph.D. dissertation, University of Wollongong, New South Wales, Australia, 1996.

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

[7] 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*, B. O. Apduhan, and M. Gavrilova, Eds. Fukuoka, Japan: IEEE CS, March 2010, pp. 191–200.

[8] (Visited January, 2014) NFC Trials, Pilots, Tests and Live Services around the World. Online. NFC World. [Online].

[9] 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)*, ser. LNCS, H. Y. YOUM and M. Yung, Eds., vol. 5932/2009. Busan, Korea: Springer, August 2009, pp. 20–35.

[10] *Java Card Platform Specification*, Oracle Std. V3.0.1, May 2009.

[11] "GlobalPlatform Card Security Requirement Specification 1.0," Online, Redwood City, USA, Specification, May 2003. [Online].

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

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

[14] "EPC-GSMA Mobile Contactless Payments Service Management Roles Requirements and Specifications," European Payments Council (EPC) and GSM Association, Tech. Rep. EPC 220-08, October 2010.

[15] "The Role and Scope of EMVCo in Standardising the Mobile Payments Infrastructure," EMVCo., USA, Tech. Rep., October 2007. [Online].

[16] (2013, December) The Role of the Trusted Service Manager in Mobile Commerce. GSMA Mobile Commerce. London, United Kingdom.

[17] "GlobalPlatform's Proposition for NFC Mobile: Secure Element Managment and Messaging," Online, GlobalPlatform, Spec., April 2009.

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

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

[20] N. Mallat, "Exploring Consumer Adoption of Mobile Payments - A Qualitative Study," *J. Strateg. Inf. Syst.*, vol. 16, pp. 413–432, December 2007.

[21] 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 CS, 2010, pp. 91–99.

[22] *ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation*, Std. Version 2.2, Rev. 256, 2004.

[23] "GlobalPlatform A New Model: The Consumer-Centric Model and How It Applies to the Mobile Ecosystem," GlobalPlatform, Whitepaper, March 2012.

[24] R. N. Akram, K. Markantonakis, and K. Mayes, "Coopetitive Architecture to Support a Dynamic and Scalable NFC based Mobile Services Architecture," in *The 2012 International Conference on Information and Communications Security (ICICS 2012)*, K. Chow and L. C. Hui, Eds. Hong Kong, China: Springer, October 2012.

[25] R. N. Akram, K. Markantonakis, and K. Mayes,, "Building the Bridges – A Proposal for Merging different Paradigms in Mobile NFC Ecosystem," in *8th International Conference on Computational Intelligence and Security*, S. Xie, Ed. China: IEEE CS, 2012.

[26] R. N. Akram, K. Markantonakis, and K. Mayes,, "Trusted Platform Module for Smart Cards," in *6th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, O. Alfandi, Ed. Dubai, UAE: IEEE CS, March 2014.

[27] 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, Kai Rannenberg and V. Varadharajan, Eds. Brisbane, Australia: Springer, September 2010, pp. 161–171.

[28] R. N. Akram, K. Markantonakis, and K. Mayes,, "Remote Attestation Mechanism for User Centric Smart Cards using Pseudorandom Number Generators," in *5th International Conference on Information and Communications Security*, S. Qing and J. Zhou, Eds. Beijing, China: Springer, November 2013.

[29] R. N. Akram, K. Markantonakis, and K. Mayes,, "Remote Attestation Mechanism based on Physical Unclonable Functions," in *The 2013 Workshop on RFID and IoT Security (RFIDsec'13 Asia)*, C. M. J. Zhou and J. Weng, Eds. Guangzhou, China: IOS Press., November 2013.

[30] P. Dusart and D. Sauveron, "Which Trust Can Be Expected of the Common Criteria Certification at End-User Level?" *Future Generation Communication and Networking*, pp. 423–428, 2007.

[31] P. Urien, "Collaboration of SSL Smart Cards within the WEB2 Landscape," *Collaborative Technologies and Systems, International Symposium on*, vol. 0, pp. 187–194, 2009.

[32] P. Urien and S. Elrharbi, "Tandem Smart Cards: Enforcing Trust for TLS-Based Network Services," *Applications and Services in Wireless Networks, International Workshop on*, pp. 96–104, 2008.

[33] A. Harbitter and D. A. Menascé, "The Performance of Public Key-Enabled Kerberos Authentication in Mobile Computing Applications," pp. 78–85, 2001.

[34] "GlobalPlatform Device: Secure Element Remote Application Management," Online, GlobalPlatform, Spec, February 2011.

[35] "Multos: Guide to Loading and Deleting Applications," MAOSCO, Tech. Rep. MAO-DOC-TEC-008 v2.21, 2006. [Online].

[36] G. Lowe, "Casper: A Compiler for the Analysis of Security Protocols," *J. Comput. Secur.*, vol. 6, pp. 53–84, January 1998.