A Privacy Preserving Application Acquisition Protocol

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

***Abstract*—In the smart card industry, the application acquisition process involves the card issuers and application providers. During this process, the respective card issuer reveals the identity of the smart card user to the individual application providers. In certain application scenarios it might be necessary (e.g. banking and identity applications). However, with introduction of the Trusted Service Manager (TSM) architecture there might be valid cases where revealing the card user's identity is not necessary. At the moment, the secure channel protocols for traditional smart card architecture including the TSM does not preserve the privacy of the card users. In this paper, we propose a secure and trusted channel protocol that provide such feature along with satisfying the requirements of an open and dynamic environment referred as User Centric Smart Card Ownership Model (UCOM). A comparison is provided between the proposed protocol and selected smart card protocols. In addition, we provide an informal analysis along with mechanical formal analysis using CasperFDR. Finally, we provide the test implementation and performance results.**

***Index Terms*—User Centric Smart Card Ownership Model, Application Installation Protocol, Privacy Preservation, Smart Cards, CasperFDR.**

I. Introduction

The introduction of the Near Field Communication (NFC) [1] technology and commercial realities have reinvigorated the multi-application smart card initiative [2]. In most of the trials [3], either the traditional ownership model termed as Issuer Centric Smart Card Ownership Model (ICOM) [4], or an extension of it referred to as Trusted Service Manager (TSM) [5] is deployed. In both of these architectures, the smart card is stringently controlled by a centralised authority (e.g. card issuer).

On contrary, the User Centric Smart Card Ownership Model (UCOM) [6] delegates the smart card's ownership to their respective users (cardholders). The term ownership means "*freedom of choice*" that the users only have the privilege to request installation or deletion of an application from a Service Provider (SP). Each SP has an Application Lease Policy (ALP) [6], which if satisfied by a smart card the SP would lease the respective application to it.

For leasing an application, the respective SP will establish a secure channel protocol with a smart card along with ascertaining its security and operation assurance. For this purpose, we propose a Privacy Preserving Secure and Trusted Channel Protocol (P-STCP) in this paper that satisfies the listed UCOM requirements and provide privacy preservation service to the card user. The P-STCP not only establishes a secure communication channel but also provides assurance that the participating smart card is secure and trustworthy; one feature that most of the smart card protocols do not entertain.

We start the discussion with a brief description of the related work and provide the rationale why we considered that most of the existing smart card protocols fall short. The discussion is then extended in section three to the smart card architecture in the UCOM environment that provides dynamic and ubiquitous security and reliability assurance. In section four, we propose the P-STCP. Section five provides an informal and mechanical formal (CasperFDR) analysis of the P-STCP and section six details performance measurement. Finally, in section seven future research directions and conclusion of the paper are provided.

II. Secure Channel Protocol

In this section, we explore the rationale behind the P-STCP along with the related work that we use as a point of reference for later discussions.

A. Motivation

A Secure Communication Protocol (SCP) by definition provides either or both: entity authentication and key exchange between communicating parties (end points). The SCP preserves the confidentiality and integrity of the messages on the channel but does not assure the same at the end points. Nevertheless, there can be implicit assurance in the integrity and security of the end points as articulated by ETSI TS 102 412 [7]. This states that the smart card is a secure end point under the assumption that it is a tamper-resistant device (which is under the control of a trustworthy entity: card issuer).

The implicit assumption is valid for the traditional smart card environment (e.g. ICOM and TSM) because it is issued by a "trusted" card issuer. This became the fundamental assumption in most of the smart card based SCPs. For the ICOM, this makes sense as the strict control of a smart card will effectively restrict the SCP to only execute with an entity that: (a) has prior authorisation from the card issuer, or (b) is initiated by an authorised entity. As the card issuer has the knowledge of the card user's identity and all application acquisition process is either initiated or sanctioned by it; there is no privacy protection for the respective card users.

On contrary, in the UCOM, there is no such authority (i.e. card issuer or centralised authority: TSM); hence, the assumption of the implicit assurance is no longer valid as illustrated

by the simulator problem described in [6]. A simulated smart card on a computer can initiate a communication channel with an SP in the UCOM; downloading its application, and then trying to reverse engineer it.

A trusted channel is a secure channel that is cryptographically bounded to the current state of the communicating parties [8]. This state can be a hardware and/or software configuration, and ideally it will require a trustworthy component to validate it to be same as claimed. Such a component in most of the instances is a Trusted Platform Manager (TPM) [9] as demonstrated by [10] and [11].

An SP does not have any prior trust relationship with a smart card in the UCOM. Therefore, the traditional smart card SCPs will fail to provide: (a) assurance that an SP is communicating with a genuine smart card platform and not a simulator, (b) the smart card security and operational environment is certified by a reputed third party evaluation, (c) the security and operational environment state is still valid as it was at the time of evaluation, and (d) the smart card is owned by the user who is requesting the application download. These issues in the context of the UCOM are further discussed in section II-C.

We define the P-STCP in the context of the UCOM as a protocol providing a secure and reliable communication channel coupled with an assurance of security and integrity concerning the communicating smart card platform along with provisioning the privacy protection to the card user. The P-STCP is used during: (a) application installation/deletion process, and/or (b) communication between an installed application and its respective SP.

A valid question arise is why we need the privacy protection for the smart card user. In answer to this, we consider that in certain instances respective SPs are only concerned with the security assurance and validation of the smart card platform and do not require user registration (i.e. anybody can download and use their application).

Examples of applications that can be downloaded in this scenario include pre-paid telecom applications, transport, hotel room access applications, and rental car keys, etc. In such a scenario, the SP is concerned with the (secure) application download on to a smart card that supports its ALP. From a customer's point of view, they do not give their personal details, and so they can preserve their privacy. Respective SPs are concerned with the usage of their applications than who use them. However, in certain countries even the pre-paid mobile SIMs or transport applications are tied to individual users.

In a TSM based architecture, the respective TSM might have relationship to companies that provide such services as listed above. That in reality does not require an active user registration before the lease of application. Therefore, existing protocols (e.g. SCP81 [12]) does not provide privacy protection. Furthermore, in the above discussed application acquisition process the user is not required to be pre-registered user of the respective SP. This gives the flexibility, increase dynamism and avoid pre-registration (authorisation) of the user that might involve offline process, which may take appreciable time.

B. Related Work

In this section, we restrict to the discussion of the protocols that are specifically proposed for the smart card environment or being used as point of comparison in later discussions.

Since the possibility that two computing devices can communicate with each other, the work on the SCP is in research. An early discussion on various proposed protocols and their architecture can be found in [13]. A detailed comparison of authentication protocols for mobile network environment is presented in [14].

Early smart card protocols were based on the symmetric key crypto-system like (deprecated) SCP01 of the GlobalPlatform specification [15]. Other protocols specified by the GlobalPlatform specification are SCP02 (based on Triple-DES), SCP10 (based on asymmetric key crypto-system) [15], SCP81 (based on SSL/TLS) [12], SCP03 (based on AES) [16], and SCP80 for mobile telecom industry [17]. One thing to note is that most of the listed protocols either implicitly or explicitly provide the user's identity during the protocol execution [15], [18].

The concept of trusted channel protocols was put forward by Gasmi et al. [8] along with the adaptation of TLS protocol [19]. Later Armknecht et al. [11] proposed another adaptation of OpenSSL to accommodate the concept of the trusted channel, and also by Zhou and Zhang [10].

In section V-C, we will compare the proposed P-STCP with the existing protocols. These protocols include the Station-to-Station (STS) protocol proposed by Diffie et al. [20], the Aziz-Diffie (AD) protocol [21], the ASPeCT protocol [22], Just-Fast-Keying (JFK) [23], trusted TLS (T2LS) [8], GlobalPlatform SCP81 [12], Markantonakis-Mayes (MM) protocol [24], and Sirett-Mayes (SM) protocol [25].

The selection of the protocols is intentionally kept broad to include well-established protocols like STS, Aziz-Diffie (AD) and JFK protocols. Also including the ASPeCT protocol, which is designed specifically for the mobile network's value-added services. The T2LS is based on the concept of trusted channels where SCP81, SM, and MM protocols are specific to smart cards.

C. Requirements and Goals of the P-STCP

Proposed protocol that supports the UCOM architecture should meet the following requirements and goals;

1) *Mutual Entity Authentication*: Both a smart card and an SP authenticates to each other to avoid masquerading by a malicious entity.
2) Exchange of certified public keys between the entities to facilitate in the key generation and entity authentication process.
3) Mutual Key Agreement: Communicating parties will agree on the generation of a key during the protocol run.
4) Joint *Key Control*: Communicating parties will mutually control the generation of new keys to avoid one party choosing weak keys or predetermining any portion of the session key.
5) *Key Freshness*: The generated key will be fresh to the protocol session to protect replay attacks.

6) Mutual *Key Confirmation*: Communicating parties will provide implicit/explicit confirmation that they have generated the same keys during a protocol run.
7) Known-Key Security: If a malicious user is able to obtain a session key of a particular protocol run, it should not able him or her to retrieve the long-term secrets (*private keys,*) or *session keys* (future and past).
8) Unknown *Key* Share Resilience: In the unknown key share attack, an entity $\mathcal{X}$ believes that it has shared a key with an $\mathcal{Y}$, where the entity $\mathcal{Y}$ mistakenly believes that it has shared the key with entity $\mathcal{Z} \neq \mathcal{X}$
9) *Key* Compromise Impersonation (KCI) Resilience: If a malicious user retrieves the long-term key of an entity, it will enable him or her to impersonate the entity. Nevertheless, it should not facilitate him or her to impersonate other entities to it [26].
10) *Perfect Forward Secrecy*: In case, if the long-term keys of communicating entities are compromised. It does not enable a malicious user to compromise previously generated session keys.
11) Mutual *Non-Repudiation*: Communicating entities will not be able to deny that they have executed the protocol run with each other.
12) Partial Chosen Key (PCK) Attack: Protocols that claim to provide joint key control are susceptible to this attack [27]. In this attack, if two entities provide separate values to the key generation function then one entity has to communicate its contribution value to the other. The second entity can then compute the value of its contribution in such a way that it can dictate its strength (able to generate a partially weak key). However, this attack depends upon the computational capabilities of the second entity.
13) Trust Assurance (Trustworthiness): The communicating parties not only provide security and operation assurance but also validation proofs that are dynamically generated during the protocol execution [6].
14) Memory-DoS and Computation-DoS Prevention: The protocol should not require the server (in our case SP's servers) to allocate the resources before authenticating and validating the state of the requesting entity (a smart card) or verifying the credentials of the authorised user.
15) Privacy: A third party should not be able to know the identities of the user or her smart card, either over the Internet or Over-the-Air (OTA). In addition, during the trust validation and assurance process; the requesting SP should not be able to gain any additional information about the platform (e.g. applications installed on a smart card).
16) Simulator Attack: This attack discussed in [6] allows a malicious user to masquerade a smart card platform on a computer (as a simulation). Such a possibility will enable the malicious user to download an application onto a simulated platform and then perform reverse engineering on the downloaded application: revealing proprietary and sensitive data of the application. Therefore, any proposed protocol for the UCOM architecture should integrate the platform attestation in its specification that verifies the current state of the platform to be trustworthy.

For formal definition of the terms (italicised) used in the above list, readers are advised to refer to [13]. The stated goals in this section are later used as point of reference to compare (see table IV) the proposed P-STCP with listed protocols (see section II-B).

III. Smart Card Assurance and Validation Mechanism

In this section, we describe the UCOM smart card architecture with emphasis on trust assurance mechanism.

A. Smart Card Architecture

In the ICOM, both the card issuer and the application provider have an offline relationship. That may translate into having business and legally-binding contracts that define the terms and conditions for both parties to co-exist, and abide by each other's security requirements/policies on a smart card. However, such an assumption is impossible to make in the UCOM where smart cards are not under any centralised authority. This absence of the prior and offline trust in the UCOM is the major cause why most of the existing protocols fail the UCOM requirements (section II-C).

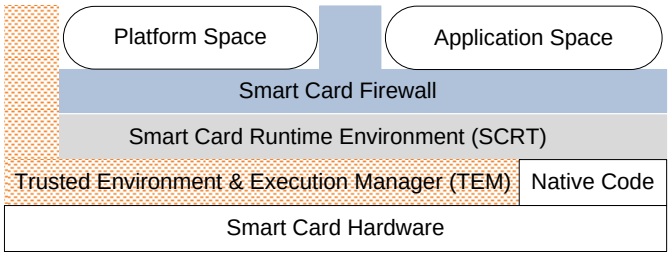

Figure 1. Overview of the simplified (UCOM) smart card architecture.

An essential architectural change is required to the smart card architecture that can facilitate the establishment of the trustworthiness of both the smart card platform and (installed) application(s) that is referred as Trusted Environment & Execution Manager (TEM) and illustrated in overly simplified figure 1.

1) Trusted Environment & Execution Manager: The TEM is used to provide a remote, dynamic, and ubiquitous security assurance and validation that the platform's state is as it was at the time of a third party evaluation. For security assurance, the third party evaluator issues an Product Evaluation Certificate (PEC), which is a cryptographically signed certificate that details the security and operational functionality of the evaluated product. The evaluation certificate will also certify a unique signature key pair of the card manufacturer. During the manufacturing process, individual smart cards will generate a unique signature key pair [13] that will be certified by the respective card manufacturer. The certificate hierarchy in the UCOM architecture is shown in figure 2. One thing to note is that at present Common Criteria (CC) [28] or any other evaluation scheme for that matter does not provide the PEC but proposals presented in [6] and [29] can be utilised.

For security validation, the TEM implements a validation mechanism that is divided into two parts: tamper-evidence and

Table I
COMPARISON OF DIFFERENT PROPOSALS FOR VALIDATION MECHANISM.

Features	Active-Shield	KAT	Keyed-HMAC	PRNG	PUF
Robustness	Yes	Yes	Yes	Yes	Yes
Independence	No	No	No	Yes	Yes
Pseudo-randomness	No	No	Yes	Yes	Yes
Tamper-evidence	Yes	No	–	-	Yes
Unforgeable	No	No	Yes	Yes*	Yes
Assurance	Yes	No	No	No	Yes*

Note: "Yes" means that the mechanism supports the feature. Similarly, "No" indicates that the mechanism does not support the required feature. The entry "Yes*" means that it can support this feature if adequately considered during the design.

reliability assurance. Smart cards are required to be a tamper-resistant device [30] and for this purpose card manufacturers implement hardware based tamper protections. The tamper-evidence process verifies whether the implemented tamper-resistant mechanisms are still in place and effective. The reliability assurance process on the other hand verify the software part of the smart card platform that is crucial for its security and reliability is not been tampered.

A TEM tamper-evidence process should provide properties that are listed as below:

1) Robustness: On input of a certain data, it always produces the associated output.
2) Independence: When the same data is input to two self-test mechanism on different devices, it outputs different values.
3) Pseudo-randomness: The generated output should be computationally difficult to distinguish from a pseudo-random function.
4) Tamper-evidence: An invasive attack to access the function should have irreversible changes, which render the device dead.
5) Unforgeable: It should be computationally difficult to simulate the validation mechanism to mimic the actual deployed function on a device.
6) Assurance: The function can provide assurance (either implicitly or explicitly) to independent (non-related) verifiers. It should not require an active connection with the device manufacturer to provide the assurance.

For the TEM tamper-evidence process there can be several candidates including using active (intelligent) shield/mesh [30], Known Answer Test (KAT) [31], hard-wired HMAC key, attestation based on Pseudorandom Number Generator (PRNG) [32] and Physically Unclonable Function (PUF) [33], etc. Based on the above listed features and table I, we can safely assume that PUFs are better candidate for the validation mechanism. Appendix B, details the TEM validation process based on both the PRNG and PUF based mechanisms.

Nevertheless, for this paper we assume that such a mechanism is in place that can provide tamper-evidence to a requesting entity as part of the P-STCP. The software state of a platform can be validated by measuring its hash value and if it matches with the one that is listed in the evaluation certificate then we can consider with reasonable assurance that the state of the platform is as it was at the time of evaluation.

After a cardholder acquires a smart card; the respective TEM will generate and certify a signature key pair for the user (figure 2). The certificate includes user's information (e.g. cardholder's name, and date of birth, etc.) that will provide the proof of ownership; assuring an SP that the smart card is registered to a particular user.

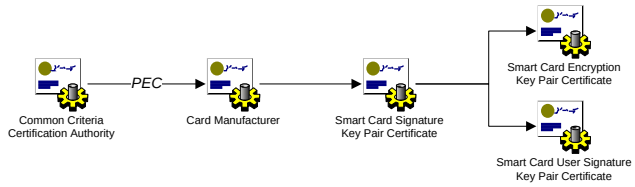

Figure 2. Certificate hierarchy in the UCOM architecture.

IV. PRIVACY PRESERVING SECURE AND TRUSTED CHANNEL PROTOCOL

In this section, we start the discussion with the notation used followed by the description of the proposed P-STCP.

A. Protocol Notation

The notation used in the protocol description is listed in table II;

Table II
NOTATION USED IN PROTOCOL DESCRIPTION.

SP	:	Denotes a Service Provider.
SC	:	Denotes a smart card.
X_i	:	Represents the identity of an entity X.
g^{rx}	:	Diffie-Hellman exponential generated by an entity X.
$Cert_X$	:	Signature key certificate of an entity X.
X_{Sup}	:	List of Diffie-Hellman groups and protocol parameters (e.g. cryptographic algorithms) supported by an entity X.
X_{Sel}	:	List of Diffie-Hellman groups and protocol parameters selected by an entity X.
N_x	:	Random number generated by an entity x.
$A \rightarrow B$	:	Message sent by an entity A to an entity B.
$X \vert\vert Y$	:	Concatenation of the data items X, Y.
$[M]_{K_a}^{K_e}$	:	Message M encrypted by the session encryption key K_e and then MAC is computed using the session MAC key K_a.
$Sig_x(Z)$	:	Signature generated on data Z by the entity x using a signature algorithm [34].
$H(Z)$	:	Is the result of generating a hash of data Z.
$H_k(Z)$	:	Result of generating a keyed hash of data Z using key k.

B. The P-STCP Protocol

Protocol messages are listed in table III and described as below;

Table III
PRIVACY PRESERVING SECURE AND TRUSTED CHANNEL PROTOCOL (P-STCP).

1.	$SC \rightarrow SP$	:	$H_{N_{SC}}(g^{r_{SC}})\|\|SC_{Sup}$
2.	$SP \rightarrow SC$	:	$VR\|\|g^{r_{SP}}\|\|N_{SP}\|\|H_{SP_k}(g^{r_{SP}}\|\|N_{SP}\|\|H_{N_{SC}}(g^{r_{SC}})\|\|SC_{IP})$
3.	$SC \rightarrow SP$	:	$N_{SC}\|\|g^{r_{SC}}\|\|[Sig_{SC}(H(SC_{Platform})\|\|SC_i\|\|g^{r_{SP}}\|\|g^{r_{SC}}\|\|N_{SP}\|\|N_{SC})\|\|Cert_{SC}]_{K_a}^{K_e}\|\|S_{Cookie}$
4.	$SP \rightarrow SC$	:	$[Sig_{SP}(SP_i\|\|SC_i\|\|g^{r_{SP}}\|\|g^{r_{SC}}\|\|N_{SP}\|\|N_{SC}\|\|ALP)\|\|Cert_{SP}]_{K_a}^{K_e}\|\|S_{Cookie}$

a) Message 1: A smart card generates a random number (N_{SC}) and Diffie-Hellman exponential ($g^{r_{SC}}$). Then it generates the MAC of the $g^{r_{SC}}$ using the N_{SC} as the MAC key. The reason for generating the MAC and sending it instead of the random number and Diffie-Hellman exponential is to avoid partial chosen key attack. As an SP is computational superior to a smart card instead of sending the values, which can enable a malicious user to adjust the generation of Diffie-Hellman exponential to generate a week key. Therefore, the smart card sends a commitment (i.e. generated MAC).

On receipt of the first message, the SP will verify the features listed in the SC_{Sup}. If they satisfy the SP's ALP requirements then it will proceed with the protocol.

b) Message 2: The SP can either generate or opt for a pre-computed buffer with values of random numbers and Diffie-Hellman exponentials. A third possibility can be that an SP might generate a $g^{r_{SP}}$ and use it for limited time (i.e. 30 seconds). On each request, the SP will only generate a new random number or select a random number from a pre-computed buffer. All three of these scenarios are possible in both versions of the protocol and they can be opted to reduce computation load on the SP's server and possibly assist in prevention of resource exhaustion DoS attacks. Finally, it will calculate the $S_{Cookie} = H_{SP_k}(g^{r_{SP}}||N_{SP}||H_{N_{SC}}(g^{r_{SC}})||SC_{IP})$. The entire message is then appended with the platform validation request message.

The smart card will initiate the generation of the session keys K_e and K_a on the receipt of the second message. It can be calculated as "$k_{DH} = (g^{r_{SP}})^{r_{SC}} \ mod \ n$" which will be the shared secret from which the rest of keys will be generated. The encryption key is generated as $K_e = H_{k_{DH}}(N_{SP}||N_{SC}||\text{'1'})$ and MAC key as $K_a = H_{k_{DH}}(N_{SP}||N_{SC}||\text{'2'})$. We can further generate (session) keys in the similar manner for application download protocol or for the application that requested it.

c) Message 3: The smart card will generate the platform assurance and validation proof, append it with the random numbers of the SP and smart card. The message is then signed by the smart card and appended by the smart card certificate. Finally, the whole message is encrypted by K_e and MACed by K_a. The encrypted and MACed message is then appended with the session cookie generated by the SP.

On receipt, the SP will first verify the commitment sent by the smart card in the first message. The SP then verify the session cookie and after successful conclusion, it will calculate the session keys K_e and K_a. Once the keys are generated, the SP will verify the MAC and decrypt the received message. It will then verify the signed data and check whether the state reported by the TEM is same as listed in the evaluation certificate.

d) Message 4: The SP will then signs the SP's and SC's random number; append them with the ALP. The signed message is appended with the SP's and SC's identities. Then the whole message is encrypted and MACed.

On receipt of this message, the smart card verifies the ALP. If the smart card can accommodate the requirements then it will proceed to next step by providing the key material to the application download process or the application that requested P-STCP.

C. Post-Protocol Process

On its successful completion, not only the P-STCP will provide an SP the assurance that the requesting smart card is suitable for its application but also generates the key material for the application download process. For completeness, an SP and a smart card can use a symmetric key application download protocol from the GlobalPlatform specification [15].

V. PROTOCOL ANALYSIS

In this section, we analytically discuss the proposed P-STCP in terms of informal, and formal mechanical analysis along with performance results.

A. Brief Informal Analysis of the Protocol

In this section, we discuss the listed requirements for the P-STCP from section II-C.

1) Requirements One to Twelve: In this section, we constantly refer to the protocol requirements and goals in section II-C with their respective numbers (Gn, where n can be 1 to 16) as listed in the same section. Therefore, here onward in this section any reference to a goal or requirement number refers to the listed item in section II-C.

During the P-STCP protocol, in message three and four the communicating entities authenticate to each other satisfying the G1. Similarly, for G2, all communicating entities exchange cryptographic certificates to facilitate in authentication and ownership proof (in case of user signature key certificate).

The proposed P-STCP satisfies the requirement G3, G4, G5 and G12 by first requiring the SP to reveal the generated Diffie-Hellman exponentials as it is computationally (more) powerful than the smart card. If the smart card reveals the generated exponential in the first message then the SP can choose a weak key. Whereas, as smart cards are computationally restricted device they cannot perform such a task.

In the P-STCP, session keys generated in one session has no link with the session keys generated in other session, even when the session is established between the same entities. This enables the protocol to provide resilience against the known-key security (G7). This unlinkability of session key is based

on the fact that each entity not only generate a new Diffie-Hellman exponential but also a random number which are used during the P-STCP. Therefore, even if an adversary "$\mathcal{A}$" finds out about the exponential and random numbers of a particular session; it would not enable him to generate past or future session keys.

Furthermore, to provide unknown key share resilience (G8) that P-STCP includes the Diffie-Hellman exponentials along with generated random numbers and each communicating entity then signs them. Therefore, the receiving entity can then ascertain the identity of the entity with whom it has shared the key.

The P-STCP can be considered to be a KCI resilient (G9) protocol, as protection against the KCI is based on the digital signatures. In addition, the cryptographic certificates of each signature key also include its association with a particular SP or a smart card. Therefore, if $\mathcal{A}$ has the knowledge of the signature key of a smart card (or an SP) then it can only masquerade the smart card to other entities but not other entities to the smart card.

The P-STCP also meet the perfect forward secrecy (G10) by making the key generation process independent of any long term keys. The session keys are generated using fresh values of Diffie-Hellman exponentials and random numbers, regardless of the long term keys like smart card, user and SP's signature keys. Therefore, even if $\mathcal{A}$ finds out the signature key of any entity it will not enable him to find out past session keys. This independence of long term secrets from the session key generation process also enabled the P-STCP to satisfy the G7.

Communicating entities in the P-STCP share signed messages with each other that includes the session information; thus, providing mutual non-repudiation (G11).

2) Trust Assurance (Trustworthiness): In the proposed P-STCP, only smart cards provide the assurance of their current state to be secure and trustworthy to respective SPs; not the other way around. The reason behind this is the deployment environment of the P-STCP where smart cards are inherently not trustworthy and the UCOM not requiring the trustworthiness of an SP. The UCOM assumes that an SP can be malicious but it will translate into the lease of a malicious application(s). Therefore, security and reliability analysis (e.g. bytecode verification [35]) of the downloaded application and not the respective SP is required. Details of which are omitted in this paper as they fall beyond the scope of the P-STCP.

A trusted channel establishment between a smart card and an SP is based on the security and trustworthiness of the TEM. The argument for the trust goes as; the respective smart card manufacturer gets a particular batch of smart cards certified from a third party evaluator. As discussed in section III-A1, the evaluation facility will issue a certificate for the evaluated product to the respective manufacturer. That in return will mass-produce the smart cards that comply with the evaluation certificate. The TEM security validation mechanism is also evaluated, and during the P-STCP, the SP will validate the hardware and software (e.g Smart Card Operating System: SCOS).

If and only if the validation mechanism is successful that the TEM will generate the signature on the test results. On receipt of these results; an SP can also verify the test results and validate the certificate chain (i.e. to check the evaluation authority of the smart card). In case it trusts the evaluation authority and current state validates that the smart card complies with the evaluation, then it will continue the protocol, otherwise it is terminated.

Therefore, the trust in the established protocol session comes from assurance that the smart card is still in compliance with the evaluated state. That is certified to be secure and trustworthy by a third party evaluation. In which the respective SP has implicit or explicit trust.

3) Denial-of-Service Protection: The aim of the DoS protection is to provide a level of assurance that the proposed protocol might not be used to mount a DoS attack against the SP. This is achieved by (a) adding a session cookie to the protocol messages that serves as the session identifier (e.g. $H_{SP_k}(g^{r_{SP}}|N_{SP}|SC_{IP})$), which includes the smart card's IP address, and (b) by not requiring the SP to perform any public key operations unless it receives user or platform authentication.

The session cookie is generated by the respective SP and it is smart card's responsibility to include the cookie in every message that it sends to the SP. On receiving a message from a smart card, the SP verifies the session cookie and if it belongs to an active session, then it can ascertain that the message came from a genuine host and not from an entity that is trying to mount the DoS attack.

The second feature, which does not require the SP to perform any heavy computations until the smart card does not provide a signed message either by the user's or platform's signature key. This is necessary to avoid the SP to commit memory and computational resources; unless the communicating smart card is authenticated to the SP's.

4) Privacy: The privacy preservation goal of the P-STCP requires that the privacy of the user should be protected. This requirement does not include the privacy for the SP as part of their business model is to advertise their presence and identity (i.e. web servers). Therefore, the privacy requirement is restricted to the preservation of the user's and her smart cards identity. The smart card's identity is protected to avoid traceability. With traceability, we mean that if a user acquires an application from a malicious SP then it knows the smart card's identity. In the future, if the user tries to acquire an application from another SP using the same smart card, the malicious SP eavesdropping on the communication channel might trace it back to the user. In the proposed protocol, we do not send any information that can be uniquely attached to a particular user or a smart card in plaintext. All communications that include the identities and cryptographic certificates are encrypted.

However, if a user always gets online through a permanent connection (i.e. fixed Internet Protocol address) then a malicious user can trace the communication to a user. Only if the malicious user has previously recorded the association of the IP address with the respective user. In such a scenario, privacy preservation is difficult to maintain in a restricted framework of the secure channel protocols; therefore, the proposed P-STCP does not provide the protection against traceability

Table IV
PROTOCOL COMPARISON ON THE BASIS OF THE STATED GOALS (SEE SECTION II-C.)

Goals	Protocols								
	STS	AD	ASPeCT	JFK	T2LS	SCP81	MM	SM	P-STCP
1. Mutual Entity Authentication	$*$	$*$	$*$	$*$	$*$	$*$	$-*$	$-*$	$*$
2. Exchange Certificates	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$-*$	$*$
3. Mutual Key Agreement	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$-*$	$*$
4. Joint Key Control	$*$	$*$	$*$	$*$	$*$	$*$			$*$
5. Key Freshness	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$-*$	$*$
6. Mutual Key Confirmation	$*$		$*$	$*$			$*$	$-*$	$*$
7. Known-Key Security	$*$	$*$	$*$	$*$	$*$	$*$	$*$		$*$
8. Unknown Key Share Resilience	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$-*$	$*$
9. KCI Resilience	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
10. Perfect Forward Secrecy	$*$		$*$	$*$	$*$	$*$			$*$
11. Mutual Non-Repudiation	$*$	$(*)$	$+*$	$*$	$*$	$*$	$+*$	$+*$	$*$
12. PCK Attack Resilience	$(*)$	$(*)$		$(*)$	$(*)$	$(*)$			$*$
13. Trust Assurance					$*$	$-*$			$*$
14. DoS Prevention				$*$					$*$
15. Privacy	$(*)$		$*$	$*$					$*$
16. Simulator Attack Resilience					$-*$				$*$

Note: $*$ means that the protocol meets the stated goal, $(*)$ shows that the protocol can be modified to satisfy the requirement, $+*$ shows that protocol can meet the stated goal but requires an additional pass or extra signature generation, and $-*$ means that the protocol (implicitly) meets the requirement not because of the protocol messages but because of the prior relationship between the communicating entities.

under fixed uniquely associated IP addresses to users.

5) Simulator Protection: The proposed P-STCP provides protection in relation to the simulator attack: relying on the TEM's operations, trustworthiness, and effectiveness of the evaluation laboratory. The certification assures that the smart card is tamper-resistant, and it is highly unlikely that a malicious user can retrieve the signature key pair of the smart card. In addition, it also assures that the TEM validation mechanism is effective and reliable.

This will in theory give the assurance to the respective SP that the smart card with whom it is communicating is not a simulator, and the current state of the smart card is as it was at the time of evaluation. It does not mean that it can still be secure or a malicious user is not able to simulate the environment with a genuine TEM signature key pair. It only gives the assurance that the smart card is secure against the attacks it was evaluated by the third party as stated in the issued certificate [6] and is state-of-the-art tamper-resistant device at the time of evaluation. Therefore, if the evaluation certificate does not meet SPs requirements or it out-dates the current attacker capability then the respective SP should decline the application lease. As stated earlier, granting an application lease is on the sole discretion of the respective SP, so if they are not satisfied with the requesting smart card, they should not lease the application.

B. Protocol Verification by CasperFDR

The CasperFDR approach was adopted to test the soundness of the proposed protocol under the defined security properties. In this approach, the Casper compiler [36] takes a high-level description of the protocol, together with its security requirements. It then translates the description into the process algebra of Communicating Sequential Processes (CSP) [37]. The CSP description of the protocol can be machine-verified using the Failures-Divergence Refinement (FDR) model checker [38]. The intruder's capability modelled in the Casper script (appendix A) for the proposed protocol is:

1) an intruder can masquerade any entity in the network.
2) intruder can read the messages transmitted in the network.
3) an intruder cannot influence the internal process of an entity in the network.

The security specification for which the CasperFDR evaluates the network is as shown below. The listed specifications are defined in the #Specification section of appendix A:

1) the protocol run is fresh and both applications were alive.
2) the key generated by the server application is known only to the client application.
3) entities mutually authenticate each other and have mutual key assurance at the conclusion of the protocol.
4) long terms keys of communicating entities are not compromised.
5) intruder is unable to deduce the identities of the user or the smart card from observing the protocol messages.

The protocol description defined in the Casper script (appendix A) is a simplified representation of the proposed protocol. The CasperFDR tool evaluated the protocol and did not find any feasible attack(s).

C. Revisiting the Requirements and Goals

Table IV provides the comparison between the listed protocols in section II-B with the proposed protocol in terms of the required goals (see section II-C).

As shown in the table IV, the STS protocol meets the first eleven goals. The main issue with the STS protocol is that it does not provide adequate protection against partial chosen key attack (G12). The remaining goals are not met by the STS because of the design architecture and deployment environment, which did not require these goals. Similarly, the AD protocol does not meet G6, and G10-G16. In the AD protocol, the user reveals her identity by sending the user certificate in clear along with non-existence of key confirmation.

The most promising results were from the ASPeCT and JFK protocols that meet a large set of goals. Both of these protocols can be easily modified to provide the trust assurance (requiring

Table V
PROTOCOL PERFORMANCE MEASURES (MILLISECONDS).

Measures	SSL	TLS	Kerberos	P-STCP	
				Card One	Card Two
Card Specification	32bit	32bit	32bit	16bit	16bit
Average	4200	4300	4240	2998.71	3091.38
Best Run	NA	NA	NA	2906	3031
Worse Run	NA	NA	NA	3922	4344
Standard Deviation	NA	NA	NA	117.71	96.32

Note: Above mentioned measurement values for SSL are taken from [39], TLS from [40], [41] and Kerberos from [42].

additional signature). Furthermore, both of these protocols are vulnerable to the partial chosen key attacks. However, in the table IV we opt for the possibility that the JFK can be modified to meet this goal. The reason behind this is based on the entity that takes the initiators role and if in the JFK we opt for the assumption that an SP will always take the initiators role then this goal is met by the JKF.

The T2LS protocol meets the trust assurance goal by default but because it is based on the TLS protocol, which does not meet most of the requirements of the P-STCP, so the T2LS also does not meet them. A note in favour of the SCP10, SCP81, MM, and SM protocol is that they were designed with the assumption that an application provider has a prior trusted relationship with the card issuer; thus, implicitly trusting the respective smart card. Most of these protocols to some extent have the similar architecture in which a server generates the key and then communicates that key to the client (i.e. read smart card). There is no non-repudiation as they do not use signatures in the protocol run.

As apparent from the table IV, the proposed P-STCP satisfies all goals that were described in section II-C. The protocols that are proposed specifically for the smart card environment only meet half of the stated goals. However, the security requirements for the UCOM are more stringent than the ICOM. Nevertheless, we still consider that the proposed P-STCP should be deployed even in the ICOM and especially with any future ownership model that will support multi-applications on a smart card under the Trusted Service Manager (TSM) architecture.

VI. PRACTICAL IMPLEMENTATION

The proposed protocol in section IV do not specify actual details of the cryptographic algorithms, which are left to the respective SPs and smart cards. However, in our implementation we use AES (128-bit key) in Cipher Block Chaining (CBC) mode without padding [43] for both encryption and generating MACs. The signature algorithm was chosen to be RSA with 512-bit key. For generating hash values, we use SHA-256 [44]. For Diffie-Hellman key generation, we chose the 2058-bit MODP group specified in the RFC-5114 [45].

Our implementation model has two entities; a smart card, and an SP, implemented on a Java Card and 1.83GHz with 2GB RAM laptop, respectively. We have implemented two applets on 16bit Java Cards; one takes the role of the TEM and second as the protocol handler. At the time of writing the paper, we did not have access to the smart card platform that will enable us to implement the TEM close to the hardware level (see figure 1). We suffice our implementation at the application level and consider that similar or better performance can be attained if TEM is implemented as part of the platform (which we plan to do in future). At the application level, implementation of the TEM cannot have memory access to measure the hash value of the SCOS. Therefore, we generated the hash values on a fixed set of values stored in an array of size 256 bytes to represent an SCOS.

The performance of the raw implementation without any pre-computation, measured on two different Java Cards is listed in the table V. The implementation of the protocol on Java Cards takes 9799 bytes. The values in the table V were taken from the data set that was collected by executing each protocol on individual cards for 1000 times and recording the time it takes to complete each iteration. We choose performance measures of the SSL, TLS, and public key based Kerberos [42] to provide a comparison with our proposal. The rationale for this choice is based on the GlobalPlatform's SCP81 for the TSM architecture (based on the SSL/TLS) and Multos [46] application installation architecture [18] that can adopt the public key based Kerberos.

VII. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

In this paper, we have proposed a protocol that provides a secure and trusted communication channel to the communicating parties. The proposed protocol was compared with nine other protocols against the stated goals and requirements, and it performed better then the selected protocols. We provide the mechanical formal analysis of the P-STCP that did not find any feasible attacks, and then finally we showed that it performs better then other protocols that are proposed for the TSM architecture. We consider that the proposed protocol is not only suitable for the UCOM architecture but we recommend it for the ICOM or TSM architectures.

As part of future research, the TEM architecture has to be formalised by defining how a PUF or another mechanism can provide assurance of hardware protection. Furthermore, we will look into how the UCOM architecture can be expanded into the other computing domains like mobile phones, tablets, and personal computers through a portable, cross-platform, fault-tolerant, and tamper-resistant generic device that is in a user's control.

VIII. ACKNOWLEDGEMENTS

We would like to extend our appreciation to the anonymous reviewers for their valuable time and feedback. Additionally, thanks to Min Chen, Babar Mahmood, and Hisham Abbasi for patience while proof reading drafts.

REFERENCES

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

[2] "Co-Branded Multi-Application Contactless Cards for Transit and Financial Payment," Smart Card Alliance, USA, White Paper TC-08001, March 2008.

[3] (2011) NFC Trials, Pilots, Tests and Live Services around the World. Online. NFC World.

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

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

[6] Anonymous.

[7] "Smart Cards; Smart Card Platform Requirements Stage 1(Release 9)," ETSI, France, Tech. Rep. ETSI TS 102 412 (V9.1.0), June 2009.

[8] Y. Gasmi, A.-R. Sadeghi, P. Stewin, M. Unger, and N. Asokan, "Beyond Secure Channels," in *STC '07: Proceedings of the 2007 ACM workshop on Scalable trusted computing*. New York, NY, USA: ACM, 2007, pp. 30–40.

[9] *Trusted Module Specification 1.2*, Trusted Computing Group Std., Rev. 103, July 2007.

[10] L. Zhou and Z. Zhang, "Trusted Channels with Password-Based Authentication and TPM-Based Attestation," *International Conference on Communications and Mobile Computing*, pp. 223–227, 2010.

[11] F. Armknecht, Y. Gasmi, A.-R. Sadeghi, P. Stewin, M. Unger, G. Ramunno, and D. Vernizzi, "An efficient implementation of trusted channels based on openssl," in *Proceedings of the 3rd ACM workshop on Scalable trusted computing*, ser. STC '08. New York, NY, USA: ACM, 2008, pp. 41–50.

[12] *Remote Application Management over HTTP*, Online, GlobalPlatform Specification, September 2006.

[13] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC, October 1996.

[14] G. Horn, K. M. Martin, and C. J. Mitchell, "Authentication Protocols for Mobile Network Environment Value-Added Services," in *IEEE Transactions on Vehicular Technology*, vol. 51. IEEE, March 2002, pp. 383–392.

[15] *GlobalPlatform: GlobalPlatform Card Specification,Version 2.2,*, Online, GlobalPlatform Specification, March 2006.

[16] *GlobalPlatform Card Technology: Secure Channel Protocol 03*, Online, GlobalPlatform Public Release, September 2009. [Online]. Available: http://www.globalplatform.org/specificationscard.asp

[17] "Smart Cards; Secured Packet Structure for UICC based Applications (Release 6)," ETSI, France, Tech. Rep. ETSI TS 102 225 (V6.8.0), April 2006.

[18] "Multos: Guide to Loading and Deleting Applications," MAOSCO, Tech. Rep. MAO-DOC-TEC-008 v2.21, 2006. [Online]. Available: http://www.multos.com/downloads/technical/glda.pdf

[19] T. Dierks and E. Rescorla, "RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2," Tech. Rep., August 2008.

[20] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "Authentication and Authenticated Key Exchanges," *Des. Codes Cryptography*, vol. 2, pp. 107–125, June 1992.

[21] A. Aziz and W. Diffie, "Privacy And Authentication For Wireless Local Area Networks," *IEEE Personal Communications*, vol. 1, pp. 25–31, First Quarter 1994.

[22] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," in *Computer Security - ESORICS 98*, ser. Lecture Notes in Computer Science, J.-J. Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann, Eds. Springer Berlin / Heidelberg, 1998, vol. 1485, pp. 277–293, 10.1007/BFb0055870.

[23] W. Aiello, S. M. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A. D. Keromytis, and O. Reingold, "Just fast keying: Key agreement in a hostile internet," *ACM Trans. Inf. Syst. Secur.*, vol. 7, pp. 242–273, May 2004.

[24] K. Markantonakis and K. Mayes, "A Secure Channel Protocol for Multi-application Smart Cards based on Public Key Cryptography," in *CMS 2004 - Eight IFIP TC-6-11 Conference on Communications and Multimedia Security*, D. Chadwick and B. Prennel, Eds. Springer, September 2004, pp. 79–96.

[25] W. G. Sirett, J. A. MacDonald, K. Mayes, and C. Markantonakis, "Design, Installation and Execution of a Security Agent for Mobile Stations," in *Smart Card Research and Advanced Applications, 7th IFIP WG 8.8/11.2 International Conference, CARDIS*, ser. LNCS, J. Domingo-Ferrer, J. Posegga, and D. Schreckling, Eds., vol. 3928. Tarragona, Spain: Springer, April 2006, pp. 1–15.

[26] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key Agreement Protocols and Their Security Analysis," in *Proceedings of the 6th IMA International Conference on Cryptography and Coding*. London, UK: Springer-Verlag, 1997, pp. 30–45.

[27] C. Mitchell, M. Ward, and P. Wilson, "Key control in key agreement protocols," *Electronics Letters*, vol. 34, no. 10, pp. 980 –981, May 1998.

[28] *Common Criteria for Information Technology Security Evaluation*, Online, Common Criteria Specification Version 3.1, August 2006.

[29] D. Sauveron and P. Dusart, "Which Trust Can Be Expected of the Common Criteria Certification at End-User Level?" *Future Generation Communication and Networking*, vol. 2, pp. 423–428, 2007.

[30] W. Rankl and W. Effing, *Smart Card Handbook*. New York, NY, USA: John Wiley & Sons, Inc., 2003.

[31] *FIPS 140-2: Security Requirements for Cryptographic Modules*, Online, National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication, Rev. Supercedes FIPS PUB 140-1, May 2005. [Online]. Available: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[32] R. Kennell and L. H. Jamieson, "Establishing the genuinity of remote computer systems," in *Proceedings of the 12th conference on USENIX Security Symposium - Volume 12*. Berkeley, CA, USA: USENIX Association, 2003, pp. 21–21. [Online]. Available: http://portal.acm.org/citation.cfm?id=1251353.1251374

[33] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM conference on Computer and communications security*, ser. CCS '02. New York, NY, USA: ACM, 2002, pp. 148–160.

[34] *FIPS 186-3 : Digital Signature Standard (DSS)*, Online, National Institute of Standards and Technology (NIST) Std., June 2009.

[35] D. A. Basin, S. Friedrich, J. Posegga, and H. Vogt, "Java Bytecode Verification by Model Checking," in *CAV '99: Proceedings of the 11th International Conference on Computer Aided Verification*. London, UK: Springer-Verlag, 1999, pp. 491–494.

[36] G. Lowe, "Casper: a compiler for the analysis of security protocols," *J. Comput. Secur.*, vol. 6, pp. 53–84, January 1998. [Online]. Available: http://dl.acm.org/citation.cfm?id=353677.353680

[37] C. A. R. Hoare, *Communicating sequential processes*. New York, NY, USA: ACM, 1978, vol. 21, no. 8.

[38] P. Ryan and S. Schneider, *The Modelling and Analysis of Security Protocols: the CSP Approach*. Addison-Wesley Professional, 2000.

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

[40] 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.

[41] P. Urien, E. Marie, and C. Kiennert, "An Innovative Solution for Cloud Computing Authentication: Grids of EAP-TLS Smart Cards," *Digital Telecommunications, International Conference on*, pp. 22–27, 2010.

[42] A. Harbitter and D. A. Menascé, "The performance of public key-enabled kerberos authentication in mobile computing applications," pp. 78–85, 2001.

[43] Joan Daemen and Vincent Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Berlin, Heidelberg, New York: Springer Verlag, 2002.

[44] *FIPS 180-2: Secure Hash Standard (SHS)*, National Institute of Standards and Technology (NIST) Std., 2002.

[45] M. Lepinski and S. Kent, "RFC 5114 - Additional Diffie-Hellman Groups for Use with IETF Standards," Tech. Rep., January 2008.

[46] "Multos: The Multos Specification,," Online.

APPENDIX A
CASPERFDR SCRIPT

```
#Free variables
datatype Field = Gen | Exp(Field, Num)
unwinding 2
halfkeySP,iMsg, rMsg, halfkeySC, EnMaKey :
Field
SC, SP: Agent
gSC, gSP: Num
nSC:SessionKey
nSP, SCOShash: Nonnce
```

```
VKey: Agent->PublicKey
SKey: Agent->SecretKey
InverseKeys = (VKey, SKey), (EnMaKey,
EnMaKey), (Gen, Gen), (Exp, Exp),(nSC, nSC)

#Protocol description
0.    -> SC : SP
[SC!=SP]
1. SC -> SP : {Exp(Gen,gSC)}{nSC}%saveMsg
[SC!=SP]
2. SP -> SC : Exp(Gen,gSP)%halfkeySP, nSP
[SC!=SP]
<EnMaKey := Exp(halfkeySP,gSC)>
3. SC -> SP : Exp(Gen, gSC)%halfkeySC, nSC
[decryptable(saveMsg, nSC) and
nth(decrypt(saveMsg, nSC), 1)==halfkeySC]
<EnMaKey := Exp(halfkeySC, gSP)>
4. SP->SC:nSC,nSP
5. SC -> SP : {{Exp(Gen, gSC)%iMsg, SCOShash,
SC, SP, nSC, nSP}{SKey(SC)}}{EnMaKey}
[iMsg==halfkeySC]
6. SP -> SC : {{Exp(Gen, gSP)%rMsg, SP,
SC,nSP,nSC}\
{SKey(SP)}}{EnMaKey}
[rMsg==halfkeySP]

#Actual variables
SCard, SProvider, MaliciousEntity: Agent
GSC, GSP, GMalicious: Num
NSC: SessionKey
NSP, SmartCardOShash, NMalicious: Nonce
InverseKeys=(NSC, NSC)

#Processes
INITIATOR(SP,SC, gSP, nSP)knows SKey(SP), VKey
RESPONDER(SC,SP,SCOShash, gSC, nSC) knows
SKey(SC), VKey

#System
INITIATOR(SProvider, SCard, GSP, NSP)
RESPONDER(SCard, SProvider, SmartCardOShash,
GSC, NSC)

#Functions
symbolic VKey, SKey

#Intruder Information
Intruder = MaliciousEntity
IntruderKnowledge = {SProvider, SCard,
MaliciousEntity, \
GMalicious, NMalicious, SKey(MaliciousEntity),
VKey}

#Specification
Aliveness(SP,SC)
Aliveness(SC, SP)
Agreement(SP, SC, [EnMaKey])
Secret(SP, EnMaKey, [SC])
Secret(SC, EnMaKey, [SP])

#Equivalences
forall x, y : Num . Exp(Exp(Gen, x), y) =
Exp(Exp(Gen, y), x)
```

APPENDIX B
TEM VALIDATION PROCESS

Algorithm 1: Algorithm for the TEM validation mechanism.

Input :
l: list of selected memory addresses.
hK: hard-wired key.

Output: S: signature key of the $\mathcal{SC}$.

Data:
$seed$: temporary input value for the PUF set to zero.
n: number of memory addresses in the list l.
i: counter set to zero.
a: memory address.
$prKey$; PRNG secret key unique to each smart card.
k: secret key used to encrypt the signature key.
S_e: encrypted signature key S.

```
AttestationHandler (l, hK) begin
    while i < n do
        a ⟵ Read (i, l)
        seed ⟵ GenHash (ReadMemoryContents
        (a), hK,seed)
        i ⟵ i+1
    if seed ≠ ∅ then
        if Attestation == PUF then
            k ⟵ PUF (seed)
        if Attestation == PRNG then
            k ⟵ PRNG (seed, prKey)
    else
        return testfailed
    S ⟵ DecryptionFunction (k, S_e)
    return S
```