A Dynamic and Ubiquitous Smart Card Security Assurance and Validation Mechanism

Raja Naeem Akram, Konstantinos Markantonakis, Keith Mayes

A Dynamic and Ubiquitous Smart Card Security Assurance and Validation Mechanism

Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes

Information Security Group Smart card Centre, Royal Holloway, University of London
Egham, Surrey, United Kingdom
{R.N.Akram, K.Markantonakis, Keith.Mayes}@rhul.ac.uk

Abstract. Smart cards have been deployed as trusted components in a wide range of industries. The basis of the trust on a smart card platform and applications is static and evaluated before the card issuance to cardholders. A dynamic and post-issuance security assurance and validation mechanism can be useful, but it is not considered necessary in the Issuer Centric Smart Card Ownership Model. However, in an open and dynamic smart card environment like the User Centric Smart Card Ownership Model, it is essential to have a mechanism that on request could provide assurance and validation of the implemented and evaluated security mechanisms. Such a framework is the focus of this paper.

1 Introduction

Multi-application smart cards enable a secure and flexible execution environment for a diverse range of applications with their individual requirements [1]. Since the inception of the smart card technology, the main driving force in its adoption has been the Issuer Centric Smart Card Ownership Model (ICOM) [2], in which smart cards are in control of the issuing authority and cardholders (end-user) can only use sanctioned privileges. In this model, issuers either evaluate themselves or accept the third party evaluation of the security mechanisms.

The most prominent evaluation scheme in the smart card industry has been the Common Criteria (CC) [3]. Card issuers or card manufacturers initiate the evaluations process and the result of the evaluation is communicated to initiators, stakeholders, standardisation or government organisations. Smart cards do not carry any evaluation certificate or validation mechanism, so end-users cannot verify the their security conformance. It would be useful to have such a mechanism but it is not necessarily implemented in the ICOM. However, for the User Centric Smart Card Ownership Model (UCOM), such a mechanism is essential.

The UCOM enables a cardholder to choose an application they require on his or her card [4], that is managed by an open and dynamic mechanism of application installation, and deletion [5]. To ensure that the UCOM is a reliable, secure and efficient model, it is necessary that smart cards and their applications should provide assurance along with validation of the implemented security mechanisms to the requesting entities. Similar mechanisms are mentioned in literature [6–8], but their focus is on the ICOM. Although, the primary focus of

this paper is on a framework that satisfies the UCOM requirements, we consider that the framework could be equally valid in the ICOM environment.

In section two, we begin with a short discussion on the rationale behind the paper and requirements for the proposed framework. Section three discusses essential components of the CC scheme and why it is a suitable choice. Details of the framework are described in section four and the structure of the proposed CC certificate is briefly discussed in section five. Section six discusses the future research directions and finally section seven provides the concluding remarks.

2 Security Assurance and Validation Mechanism

In this section, a brief description of the rationale and requirements for the proposed model is provided.

2.1 Motivation for Security Assurance and Validation Mechanism

In the ICOM, smart cards are under control of their respective card issuers, and they define the security requirements [4]. Depending upon the card issuer, if it is a large scale organisation then they may require the card manufacturer to meet their requirements. If it is a medium or a small-scale organisation, they can choose a product that suits their requirements [4]. In these cases, the security assurance may be evaluated under a globally acceptable standard, most notably CC [3] (ISO/IEC 15408 [9]). The card manufacturer will provide a certification report issued by the CC Certification Body (CB) [3] to card issuers. The CC might also provide assurance against the possible negligence, malicious intention and distribution problem (in theory) [8] by defining the delivery procedures and audit of production sites. Therefore, card issuers do not require dynamic and ubiquitous security assurance mechanism. In addition, if card issuers decide to install an application (from an application provider) onto their smart cards, they can verify the compatibility, and security assurance of the application before installing it. Furthermore, prior agreements and trust relationship between card issuers and application providers, and tight application installation controls prevent any malicious application to be downloaded onto smart cards.

In the UCOM, an SP may not necessarily have a prior trust relationship or agreement, with the card manufacturer or other SPs. In such a situation, how the SP will establish trust in the platform on which their application is going to be installed. Similarly, how a platform will trust the SP's application that it will not harm the platform [4]. During the installation process, both the SP and the platform would verify each other's security assurance certificates and provide their validations. Therefore, the UCOM requires a mechanism that supports a dynamic and ubiquitous security assurance and validation process.

The proposed process would be optional, and it would depend upon the security policy of the requesting entities. It could be the case that the application being installed does not have high security requirements. For example, an application that only has the unique student ID that a student presents to an access

control device along with the Personal Identification Number (PIN). The security of the application is based on the PIN not on the student ID as it might easily be discovered from the student records (e.g. email directory, class enrollment).

2.2 Requirements for Security Assurance and Validation Mechanism

Requirements for a security assurance and validation mechanism are listed below.

1. It should be automated and require minimum user (cardholder) interaction.
2. Base on well established globally acceptable security evaluation criteria.
3. No extensive modification to the existing infrastructure(s).
4. Provide effective protection against entity masquerading.
5. Protect the privacy of each of the entities involved in the process. For example, the card manufacturer should not be able to find out the individual card (it might be able to identify the card batch but not the individual cardholder or card itself). Similarly, an SP should not be able to find out about other applications installed on the smart card [10].

3 Common Criteria

In this section, a short description of the CC scheme is provided with its essential components.

3.1 Brief Introduction

In the security arena, the most sought-after concept is "trust" in ones capability and protection mechanisms. In a small, localised and restricted group, establishing trust is relatively easy as it can be accomplished individually. However, when you have no offline trust relationship with another organisation, it becomes difficult to trust their products. Third party evaluations were proposed to deal with such issues. Initially, under the guideline of Trusted Computing Security Evaluation Criteria (TCSEC) also known as Orange Book whose focus was on USA government sector's security requirements, where across the pacific, UK proposed the UK Confidence Levels [11]. In early 1990s, UK scheme was combined with Germany and French criteria to give way for Information Technology Security Evaluation Criteria (ITSEC) [8]. In 1996, CC was released, which was later adopted as ISO/IEC standard (ISO/IEC 15408 [9]), that is internationally accepted under the Common Criteria Recognition Agreement (CCRA) [3].

The CC scheme defines the methodology for expressing the security requirements, conformance claims, evaluations process and finally certification of the product. The security requirements for a product at an abstract level are stipulated by the Protection Profile (PP). The Security Target (ST) details these security requirements and makes the conformance claim for a product or its subcomponent, generally referred as Target of Evaluation (TOE). The evaluation

methodology defines the procedure that an evaluator should follow when processing the conformance claims regarding at a TOE and are published in the Common Methodology for Information Technology Security Evaluation (CEM) [12].

Protection Profile. An implementation independent document that states the security requirements at an abstract level. In practice, it generally deals with the customer's requirement and product designers try to get their product evaluated to a customer's PP. A PP can be inherited from another PP, forming a hierarchical structure of PPs where each sub-branch augmenting its parent PPs.

Security Target. An implementation independent document that describes the assets of a TOE and possible threats posed to its security. It also details the counter measures to protect against the posed threats along with the demonstration that they are fit for purpose. An ST may be in conformance of one or more PPs. Organisations evaluating smart card products to integrate them with their services will look into its ST to verify whether it satisfies their PP(s). If they satisfy then the given product can be considered secure for their application.

Evaluation Assurance Level (EAL). These are predefined assurance packages, with set of security requirements that ranges from 1 to 7, where the level seven being the strictest assurance package. These packages are described in the CEM [12]. A package can be used to construct more packages, PPs and STs.

3.2 Why Common Criteria?

Some reservations are expressed in the literature regarding the validity and the process efficiency of the CC [7, 12, 13]. However, the CC has taken a strong hold in the smart card industry, especially in high security smart cards like banking and IDS/passports etc, as a security evaluation-standard of choice.

It has a well established security requirement specification [3] and evaluation methodology [12], along with application providers (or SPs) and smart card manufacturers have extensive experience of the CC evaluation scheme. It is preferable to include the CC scheme in the proposed framework, with slight modification to the evaluation certificates that are discussed in section 5.

4 Security Assurance and Validation Mechanism

In this section, the proposed framework for the security assurance and validation mechanism is provided.

4.1 Overview of the Framework

In the security assurance mechanism, an SP creates a PP, gets it certified from a CB and makes it public. A card manufacturers could develop a UCOM compatible smart card that satisfies the certified PP and get it evaluated. After

which the manufacturer gets the evaluation certificate that could be presented to requesting entities. In the validation mechanism, an entity would challenge the certificate bearer to provide the proof that the state at which the certificate was issued is still valid. A similar line of reasoning is also applicable in the SP to smart card security assurance and validation mechanism. An overview of the mechanism is provided in the figure 1, and discussed as below.

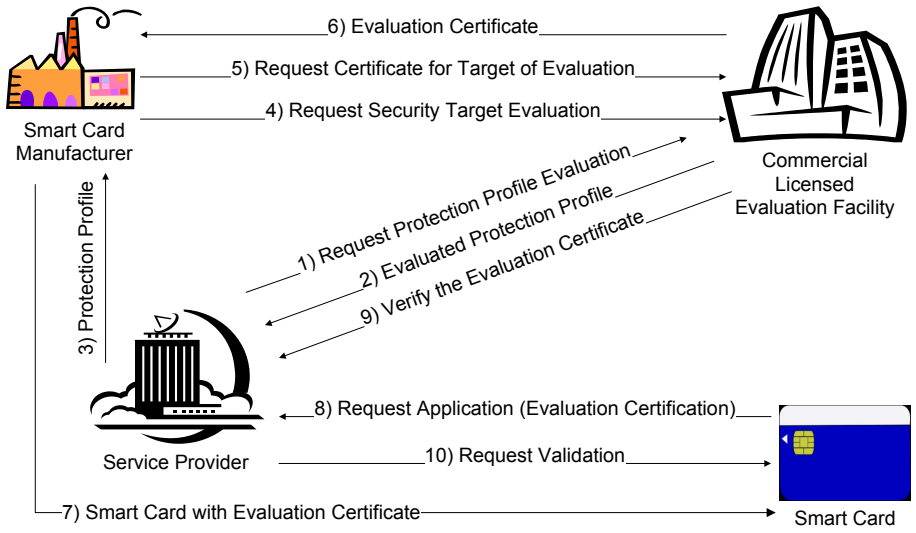

Fig. 1. Illustration of Security Assurance and Validation Mechanism

An SP would create (or reuse) a PP and requests the CC Commercial Licensed Evaluation Facility (CLEF) to evaluate the PP and after evaluation the CB will certify it. A smart card manufacturer creates an ST that conforms to the SP's PP and gets it evaluated by the CLEF. Then smart card (TOE) being evaluated and certified to the respective ST. After evaluation, the national CB would make the TOE (and related ST) public along with issuing an evaluation certificate that the card manufacturer would place on their respective smart cards. A cardholder could request and receives a UCOM compatible smart card from the manufacturer that he or she could use to request the SP's application and in this request the card provides the evaluation certificate to the SP that verifies whether the certification conforms to its PP or not. If successful, the SP would request the validation of the current state of the platform. The smart card provides the validation proof, if acceptable to the SP then it can lease its application. Similarly, the smart card could also evaluate and validate the SP's application. The framework can be divided into two phases; evaluation and assurance phase that are described in the subsequent sections.

4.2 Evaluation Phase

This section describes the pre-issuance security evaluation that is divided into two subsections; smart cards evaluation and application evaluation process.

Smart Card Evaluation Phase. In this phase, the card manufacturer would get their smart cards being evaluated to the defined ST or PPs. If the evaluation of the smart card is successful, the CB would issue a cryptographic certificate [13], referred as Common Criteria Platform Assurance Certificate (CC-PAC). The structure of the certificate is discussed in detail in section 5. However, the main component of the certificate includes an unique reference to the product (TOE), ST, PP, hardware test results and hash (using SHA family algorithms) [13] of the immutable part of the Smart Card Operating System (SCOS). The hardware test results can only ascertain the assurance against the invasive attacks, where in case of side channel attacks; it is difficult to determine their effectiveness remotely. A SCOS can be divided into mutable and immutable components. The mutable components can change (e.g. data variables) while the immutable components are less likely to be changed (e.g. program code). Therefore, the CC-PAC would only generate the hash of the program code.

Smart cards could be subjected to extensive evaluation either by the manufacturer, evaluation labs or academic community even after their issuance; therefore, if such evaluations discover vulnerabilities in a particular batch, SPs can immediately disable their application leases to them. The CC may degrade their CC-PAC assurance level or include it to the certification revocation list, prohibiting smart cards from downloading applications in the future.

Application Evaluation Phase. An SP would create an ST according to its security requirements and get it evaluated by the CLEF. If successful, the CB would issue a cryptographically signed Common Criteria Application Assurance Certificate (CC-AAC) that would contain the unique reference to the ST and the hash of immutable application code.

4.3 Assurance Phase

This phase deals with the process that requests, verifies and validates the CC-PAC and CC-ACC. In the UCOM, it would be the part of the application installation mechanism [5].

There are subtle differences between the assurance mechanisms between card platforms to SPs and vice versa, so we discuss them separately in the subsequent sections. Furthermore, each of these sub-sections discusses two possible way of establishing the assurance depending upon the requesting entity's security policy. These mechanisms are static and dynamic assurance. In the static assurance only the CC certificate is verified, while in the dynamic assurance the requesting entity requests for the validation of the claim that the current state of the entity

in question is in conformance with the CC certificate. It is correct that effective tamper-resistant mechanisms can avoid any possible modification/changes to certified component of the device, thus removing any requirement for the dynamic assurance. However, the mechanism is included to provide assurance against the replay attack on the validation message and possible future vulnerabilities that effectively overcome the hardware protection mechanisms.

The proposed mechanism only provides protection against the modification or alteration of the component that has been evaluated by the certification authority (CLEF).

Smart Card to Service Provider. In this process an SP requests a smart card to provide the security assurance and validation of its current state. Figure 2 illustrates the process that is described as below:

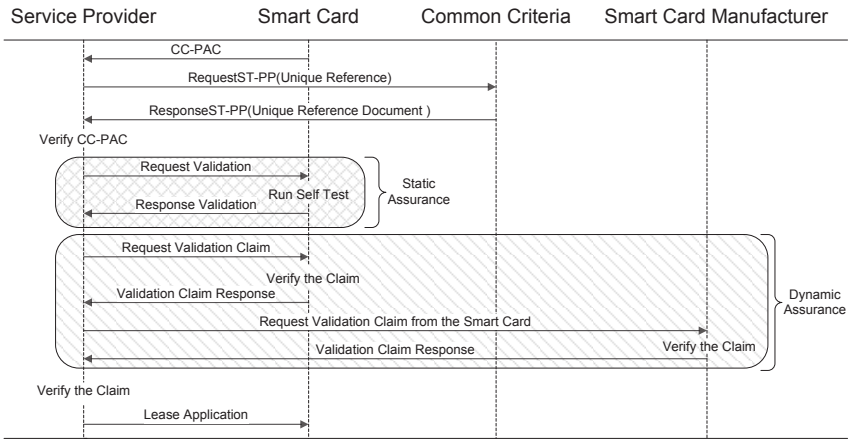

Fig. 2. Illustration of Smart Card to Service Provider Process

A card requests for the application lease from an SP. This message has the CC-PAC that contains the unique reference to the PP/ST, for which the smart card is being evaluated. The SP would request the unique PP/ST from the CC authority and compares it with their security requirements (PP). If successful, the SP would have the assurance that the card is in conformance with their requirements. Subsequently, the SP could either opt for the static or the dynamic assurance, depending upon their security policy.

In case of the static assurance, the card would initiate the self-test mechanism that would perform the hardware and SCOS tests. The test results are communicated to the SP that can compare them with the CC-PAC. If both match then the current state of the smart card can be assumed to be similar to the time of the evaluation. In the dynamic assurance, the SP would generate a

random number [13] and send it to both the smart card and its manufacturer. That would set the random number as their basis for the generation of the hash value for the SCOS (Hash(Random Number | SCOS)). The results would then be sent to the SP that compares them. If it is successful then the card would have proven the present state to be the one that was evaluated by the CLEF.

The generation of hash with the initial value being the SP's random number would avoid any possible rogue entity from replaying the validation message. Furthermore, it protects against a rogue manufacturer that places the CC certificate of a genuine manufacturer on their non-certified smart cards, along with the associated correct response for the requesting entity.

4.4 Service Provider to Smart Card.

In this process, an SP's application(s) provides assurance of the conformance to a card's security policy, illustrated in the figure 4 and described as below:

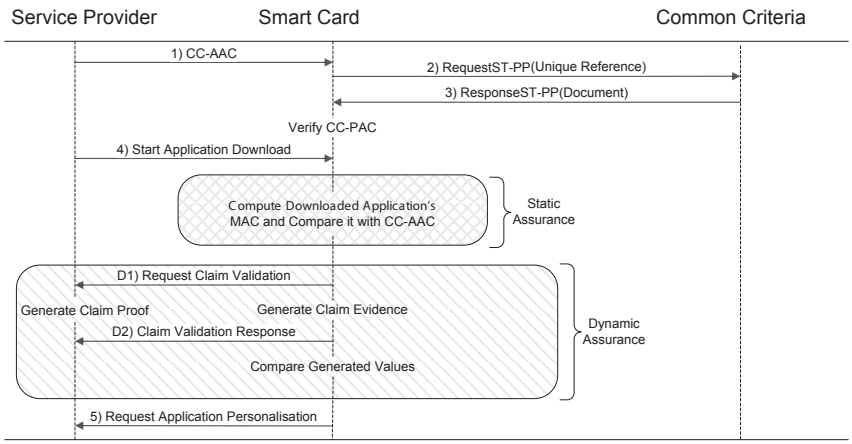

Fig. 3. Illustration of Service Provider to Smart Card Process

A smart card requests for the application lease from an SP, and in response the SP would send the CC-AAC that has a unique reference to the ST/PP to which the application is evaluated. The card then verifies whether it satisfies its security policy or not. If successful, the card could start the download of the application after which it can either opt for the static or the dynamic assurance.

In the static assurance process, the smart card would calculate the hash of the downloaded application and compare it with the CC-AAC. If successful, the smart card could assume that the state of the application is similar to the time it was evaluated. If the dynamic assurance process is selected, the smart card would generate a random number and sends it to the SP. Both, the smart card and SP

would generate the hash of the application by taking the random number as the starting point (Hash(Random Number | Application)). The SP sends the results back to the smart card that would compare it with its calculation. If successful, the application has proved its state to be similar to the time of evaluation.

5 Common Criteria Certificate

In this section, the structure of the CC certificates issued to smart cards and applications, and the process to verify/validating them, are discussed.

5.1 Common Criteria Platform Assurance Certificate (CC-PAC)

The main components of the CC-PAC are; Manufacturer's ID, Evaluator's (CLEF) ID, Reference to the evaluation target documents (PPs and ST), Digest of immutable SCOS program code, Hardware test results and acceptable ranges, Manufacturer's signature verification key [13], and Validity Period.

The manufacturer's ID uniquely identifies the smart card manufacturer, and similarly the CLEF ID identifies the evaluation body that has carried out the TOE evaluation. The next field has the unique reference to the PPs and ST, and they are already in use in the CC documentation [3]. The reference has to be unique, so the requesting entity could easily locate the related documents to verify the conformance with their security policy. Next the CLEF would generate a digest of the immutable section (code space) of the evaluated SCOS. As every SCOS has some data fields that can change with time, including them to the digest would make it difficult to verify it later in the assurance and validation process. The results with an acceptable range of deviation of the hardware's self-test mechanism would also be included in the certificate. The mechanism for the hardware's self-text mechanism and how we can be assured of its operations is beyond the scope of the paper. Finally, the certificate would contain the manufacturer's signature verification key that it would use to issue certificates to the individual smart cards of the batch. These certificates are valid for a limited time as listed in the validity period.

5.2 Common Criteria Application Assurance Certificate (CC-AAC)

The structure of the CC-AAC is similar to the CC-PAC, except for few changes. Those components that are common in both the CC-AAC and CC-PAC are not explained in this section. Details of data fields included in the CC-AAC are; SP's ID, Evaluator's (CLEF) ID, Reference to the evaluation target documents (PPs and ST), Digest of immutable (pre-personalisation) application program code, and Validity Period.

The CC-AAC would contain the SP's identity and digest of immutable application program code. Smart card applications have several life-cycle stages and one of them is personalisation stage. Prior to personalisation stage applications are not customised for individual users; therefore, all application instances on

different smart cards are identical. After personalisation of an application, it differs from the other instances. Therefore, for assurance and validation purposes it is logical to generate the digest of the application in pre-personalisation stage.

5.3 Framework for Verification of Common Criteria Certificate

The subtle details of the certificate verification mechanism would be different from the SPs and smart cards perspective. However, we can draw a generic representation of the steps each of these entities performs in the verification process, and it is illustrated in the flowchart shown in figure 5.

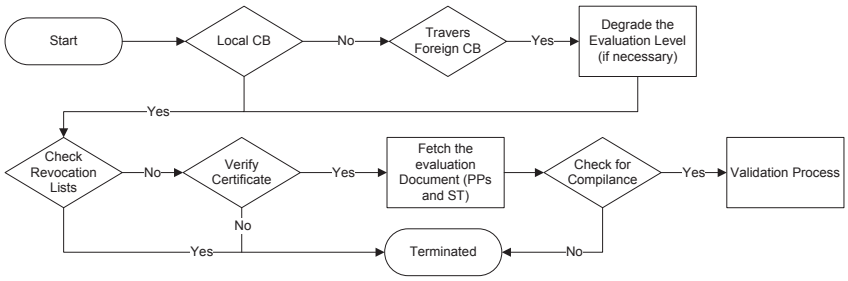

Fig. 4. Illustration of Certificate Verification Process

To verify whether the certificate is issued by the local CB or not. The local CB would be the certification authority that has also issued the assurance certificate to the verifying entity. For example, if CBA has issued CC certificates to an SP's application AppA and a smart card SCA then if AppA presents the CC-AAC to the smart card SCA, it would be considered to be issued by the local CB. So if the certificate was not from the local CB, then the verifying entity would check for the foreign CB and evaluate any possible degradation necessary for the evaluation certificate. The rationale behind the degradation is in the international recognition agreement (CCRA) regarding the CC that only accepts certificates of to a certain assurance level (e.g. EAL), that are mutually acceptable across different countries.

In the subsequent step, the verifying entity would check the revocation list(s) of the CC certificates. This is the list with details of the CC certificates that are no longer valid, may be because of the discovery of new vulnerabilities that can compromise the security of the related TOEs. After checking the revocation list, the verifying entity would check the certificate. Then it can use the unique reference to the evaluation documents in the certificate to locate the ST and PPs. The verifying entity would then check for the conformance of the ST and PPs with their security requirements. If successful, the requesting entity could then initiate the validation process.

The discovery and verification of the certificate are comparatively easy for the SPs as they have more computational power than a resource restricted smart card. To perform such tasks, a smart card would request the SP to provide the communication facility to communicate directly with the CC authority (even if required to discover foreign CBs and degrade the evaluation level).

Similarly, for a smart card it is comparatively difficult to validate the conformance of the CC-PAC evaluation documents with its security policy. Such a process is beyond the scope of this paper. However, a solution can be possible by designing the security policy of the smart card in the PP style along with a mechanism that registers all PPs into a tree like data structure. From this structure, the smart card can calculate the proximity of its PP with the PP(s) listed in the CC-PAC.

6 Future Work

In this section we discuss the future research directions to make this proposal a practical solution.

- Geographical Issues: Whether the concept of the local CB should be related with the geographical location from where the verification is initiated or to the individual evaluation body. Consider a user that purchases a smart card from France (certified by the French CB), but the user requests an application while visiting UK. Should the French CB be considered as the local CB or the British CB? While investigating it we should consider possible pros and cons in each scheme and how they would affect the overall performance.
- Hardware self-test mechanism: In this paper, we did not divulge into the specificities of the mechanism that can be implemented to check any possible modification because of the invasive attacks on the smart card hardware. Further research is required to implement such mechanisms that can remotely validate the security of the hardware.

7 Conclusion

In this paper, we proposed a framework for provide security assurance and validation to a requesting entity based on the Common Criteria scheme. Although the focus of the paper is the UCOM but the proposal tends to be the ownership model neutral and can be adaptable for the ICOM environment if necessary.

The paper provides a short introduction to the UCOM and how it is different from the ICOM in terms of requirements for the security assurance and validation mechanism. The rationale in the UCOM to have such a mechanism was detailed along with the requirements for such a mechanism. A brief discussion of the Common Criteria scheme was provided and the proposal based on the Common Criteria was described. The structure of the Common Criteria certificates that applications and smart cards can have with them in a digital form was examined.

The proposal in the paper is by no means a complete solution and there are several issues that need to be resolved. However, in this paper we demonstrated that such a mechanism can be useful and in both the ICOM and the UCOM environments the stakeholders can benefit from it.

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. D. Sauveron, "Multiapplication Smart Card: Towards an Open Smart Card?" *Inf. Secur. Tech. Rep.*, vol. 14, no. 2, pp. 70–78, 2009.
3. *Common Criteria for Information Technology Security Evaluation; Part 1: Introduction and General Model, Part 2: Functional Security Components, Part 3: Assurance Security Components*, Std. Version 3.1, Rev. 3, July 2009. [Online]. Available: http://www.commoncriteriaportal.org/thecc.html
4. R. N. Akram, K. Markantonakis, and K. Mayes, "A Paradigm Shift in Smart Card Ownership Model," in *Proceedings of the 2010 International Conference on Computational Science and Its Applications (ICCSA 2010)*, B. O. Apduhan, O. Gervasi, A. Iglesias, D. Taniar, and M. Gavrilova, Eds. Fukuoka, Japan: IEEE Computer Society, March 2010, pp. 191–200.
5. ——, "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.
6. P. A. Karger, V. R. Austel, and D. C. Toll, "A New Mandatory Secruity Policy Combining Secrecy and Integrity," IBM Thomas J. Watson Research Center, Yorktown Heights, NY, Tech. Rep. RC 21717(97406), March 2000.
7. D. C. Toll, P. A. Karger, E. R. Palmer, S. K. McIntosh, and S. Weber, "The Caernarvon Secure Embedded Operating System," *SIGOPS Oper. Syst. Rev.*, vol. 42, no. 1, pp. 32–39, 2008.
8. D. Sauveron and P. Dusart, "Which Trust Can Be Expected of the Common Criteria Certification at End-User Level?" in *FGCN '07: Proceedings of the Future Generation Communication and Networking*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 423–428.
9. *ISO/IEC 15408 Standard. Common Criteria for Information Technology Security Evaluation*, Std. Version 2.2, Rev. 256, 2004.
10. R. N. Akram, K. Markantonakis, and K. Mayes, "Firewall Mechanism in a User Centric Smart Card Ownership Model," in *Smart Card Research and Advanced Application, 9th IFIP WG 8.8/11.2 International Conference, CARDIS 2010*, ser. LNCS, D. Gollmann, J.-L. Lanet, and J. Iguchi-Cartigny, Eds., vol. 6035/2010. Passau, Germany: Springer, April 2010, pp. 118–132.
11. K. Mayes and K. Markantonakis, Eds., *Smart Cards, Tokens, Security and Applications*. Springer, 2008.
12. "Common Methodology for Information Technology Security Evaluation; Evaluation Methodology," Tech. Rep. Version 3.1, July 2009. [Online]. Available: http://www.commoncriteriaportal.org/thecc.html
13. B. Schneier, *Applied cryptography (2nd ed.): protocols, algorithms, and source code in C*. New York, NY, USA: John Wiley & Sons, Inc., 1995.