MAKING SENSE OF SMART CARD SECURITY CERTIFICATIONS

Jason Reid, Mark Looi
Information Security Research Centre - Queensland University of Technology
reid@isrc.qut.edu.au, mlooi@isrc.qut.edu.au

Abstract Manufacturers and producers of smart card systems are all beginning to climb on the certification bandwagon. In this paper, we analyse the current state of smart card certifications and present arguments as to why smart card certifications may not be all they seem. We discuss certifications issued under the ITSEC and Common Criteria and analyse shortcomings and inconsistencies that appear to exist in the certifications. Specific examples are presented to justify our arguments.

Keywords: smart card, security, certification, ITSEC, Common Criteria.

1. INTRODUCTION

A number of smart card products have received security certification through the ITSEC and Common Criteria schemes in recent years. Successful evaluation, particularly to high assurance levels can be of great benefit in marketing these products since security concerns figure prominently in the realm of smart cards and the certification process is all about establishing confidence in security. The goal of this paper is to examine the applicability and value of smart card certifications from the perspective of card issuers. The paper presents a survey and analysis of certifications issued for smart cards in the finance and banking industry. This sector has an increasing need for confidence in smart card security because they are developing applications that leverage the card's facilities of tamper resistance, secure storage and onboard cryptographic processing to the full.

The paper is structured as follows. Section two presents an overview of the certification process under ITSEC and the Common Criteria. It highlights some of the challenges in applying the criteria to smart cards, challenges that flow from the nature of the device, the fact that they are issued in large numbers to untrusted users for their long term re-

tention, and the orientation of the evaluation criteria toward software and components for networked computer systems. Section three presents a thorough survey of smart card certifications issued for banking applications since December 1997. Although the focus of the survey is on a particular sector, this does not limit the more general relevance of the analysis. The issues raised are equally applicable to any card issuer who distributes smart cards to untrusted users. The survey analysis highlights the relationship between the scope of the evaluation and the level of security accreditation achieved. The discussion proceeds on the basis that certifications will be of the greatest benefit to issuers when they are sufficiently comprehensive to allow an assessment of whether a candidate card is secure enough for an intended application, the risks associated with its use being known and acceptable.

Under the ITSEC and Common Criteria schemes, the approach and requirements for the evaluation of individual information technology products is different to that of complete systems. Because this paper deals with smart cards which are evaluated as products, the following discussion deals only with the schemes as they apply to products.

2. HOW CERTIFICATION WORKS

2.1. ITSEC

The ITSEC scheme [3] evaluates the product or Target of Evaluation (TOE) against a security target. The security target is a document prepared by the evaluation sponsor. In general terms, the security target describes what the product does, the environment it is intended to operate in, the threats it is likely to encounter and how it protects against those threats. The security target makes claims about the security functionality of the TOE and the evaluation process determines whether these claims are substantiated. In this sense, the security target forms the basis of the evaluation and a certification must be interpreted within the scope of the security target's claims.

ITSEC uses an E scale with seven levels from E0 to E6. These evaluation levels represent increasing levels of confidence that the TOE meets its security target, where E0 denotes failure to establish any confidence and E6 denotes the highest level of confidence. The E scale is a measure of assurance that a target has been met, not a measure of security strength. Because the security target effectively defines the scope of the evaluation, it is potentially dangerous to automatically equate a high assurance rating with high levels security functionality in a particular operational environment. As the later analysis of actual smart card certifications will illustrate, security targets can tightly define and confine

the scope of what is actually evaluated. As examples, [1] and [2] exclude the integrated circuit, [14] and [15] limit the scope of the evaluation to the phases of design, manufacture and testing. As a consequence, it can be difficult to draw definite conclusions about the ability of a card to counter threats when they have been issued and are in the hands of untrusted card holders, particularly where the evaluation did not thoroughly examine threats in this phase of the card lifecycle. This can limit the utility that a potential issuer of a smart card can draw from a certification because issuers are primarily interested in how the card will fare in actual use.

To establish assurance that a TOE meets its security target, the ITSEC scheme separates the concepts of confidence in the correctness of implemented security functionality, and confidence in the effectiveness of that functionality. This approach recognises that a set of correctly implemented security mechanisms will not be effective unless they are actually suitable for the task. They must bind together so that there is a synergy in their individual contributions to security that leaves no exploitable vulnerabilities. To enable evaluation on the basis of effectiveness and correctness, a security target should express claims about a TOE's security properties at three different levels of abstraction - essentially why, what and how. Security objectives are the highest level, the why. They explain why particular functionality is necessary. Security objectives reflect the threats that have been identified in the security target. Security enforcing functions are the what. They detail what security functionality is actually provided. Security mechanisms are how that security functionality is provided.

In addition to specifying a target assurance level, (E1 to E6) the security target must also claim a minimum strength of mechanisms (SoM) rating. ITSEC [3] defines strength of mechanisms as:

> "6.66 Strength of Mechanisms: an aspect of the assessment of the effectiveness of a Target of Evaluation, namely the ability of its security mechanisms to withstand direct attack against deficiencies in their underlying algorithms, principles and properties."

There are three possible strength of mechanism ratings, namely basic, medium and high. As the ITSEC definition suggests, the evaluator must determine whether individual, critical security mechanisms can resist a direct attack at the claimed minimum SoM level. This aspect of SoM, (examining the strength of individual mechanisms against direct attack) is very similar to the concept of strength of function[1] under the Com-

[1]Strength of function analysis or AVA_SOF is an assurance family in the Vulnerability Assessment class

mon Criteria [17]. But there is another critical aspect to the strength of mechanisms rating that is concerned with overall effectiveness of the security functions. This second facet of SoM is largely equivalent to the concept of attack potential [2] in the vulnerability assessment class under the Common Criteria. The evaluator must investigate whether critical mechanisms can be bypassed or avoided via an indirect attack. The existence of indirect attack methods results in an exploitable vulnerability. This second aspect of the minimum SoM claim and its relationship to effectiveness analysis is explained in the ITSEC Joint Interpretation Library [4]:

> "6.4.2 The minimum strength of mechanisms claim also provides a scale which shall be used to determine whether or not vulnerabilities in the TOE generally are exploitable in practice. This means, as a minimum, the examination of known and potential vulnerabilities is to be performed according to the level of expertise, opportunity and resources corresponding to the claimed minimum strength of mechanisms. Determination of whether or not a vulnerability is exploitable in the TOE's environment involve consideration of the levels of expertise, opportunity and resources required for its exploitation."

In this sense, the claimed minimum SoM is a measure of the attack potential that the TOE can resist. A TOE with a high SoM should resist attackers possessing a high level of expertise, opportunity and resources, within the scope of the claims made by the security target. The issue of scope is important because the security target can be very specific but the concept of exploitable vulnerabilities is, of its nature, quite general. Vulnerabilities that are exploitable in practice can be excluded from consideration through restrictions on the scope of the security target. The wording of security target claims becomes very important.

ITSEC is intended to provide evaluation criteria capable of producing results that are objective and reproducible. But determining what a high SoM means in the context of tamper resistant hardware is difficult to do in a purely objective manner. These difficulties are foreshadowed by ITSEC [3] where it states:

> "1.3 These criteria are not intended to cover physical aspects of hardware security such as the provision of tamper resistant enclosures or the control of electromagnetic emanations."

This is problematic for smart cards because their degree of tamper resistance is a critical aspect of their utility. The Smart Card Security User

[2] The three levels of attack potential map to the various components of the Vulnerability Analysis, (AVA_VLA) assurance family. AVA_VLA.4 requires resistance to attackers possessing a high attack potential. AVA_VLA.3 requires resistance to attackers possessing a moderate attack potential. AVA_VLA.2 requires resistance to attackers possessing a low attack potential. AVA_VLA.1 merely requires resistance to obvious attacks.

Group Smart Card Protection Profile [16] reinforces the importance of assessing tamper resistance saying "Physical attacks utilizing techniques derived from semiconductor engineering must be evaluated or the evaluation effort is inadequate."[3]

There are also difficulties in interpreting the factors of expertise, opportunity and resources in the context of smart cards. (These factors must be considered by the evaluator in the context of deciding whether a vulnerability is exploitable in practice and therefore whether the minimum SoM claim is justified). The concept of resources includes equipment and time, where "time is the time taken by an attacker to perform the attack, not including study time" [7]. Smart cards for financial and banking applications are issued in significant quantities to untrusted users for their long term retention. It should therefore be expected that an attacker could obtain multiple copies of a card without great difficulty. This allows them to experiment without time constraints, not caring if a number of cards are destroyed in the process.

Kuhn [8] states that a common attack methodology involves relatively expensive and time consuming reverse engineering aimed at analysing the security structure and design of the card, (including access control mechanisms, hardware security mechanisms, data protection systems and memory partitioning). Once this is understood, a simpler non-invasive attack, (typically involving manipulation of the power or clock signal) can often be designed. Such an attack can often be executed on cards of the same type in seconds [8]. At issue is whether the first stage of the process should be regarded as study time. If it is, a card compromised in this way would be rated basic. If it isn't, the reverse engineering effort may justify a claim of a high minimum SoM.

This problem of interpretation can be traced to the realisation that ITSEC was primarily envisaged as a scheme to evaluate networked computer systems or components of those systems.[4] The TOEs would typically be expensive parts of a connected, managed, interactive system so an attacker would not have inexpensive access to multiple copies with which to experiment. The aspect of time is more important in these systems because longer attack times increase the likelihood of detection. The likelihood of detection is also a factor in assessing opportunity since attacks taking a longer period of time require greater levels of opportunity

[3] Annex B, Section B.1.8, page B-3 of [16]. The Smart Card Security User Group members include American Express, Europay, JCB Co Ltd, Mastercard, Mondex, Visa, NIST and NSA. The Protection Profile has been prepared under the Common Criteria scheme. The document describes the security requirements for smart cards issued for sensitive applications, particularly in the areas of banking and payment systems.

[4] This is also true of the Common Criteria.

to avoid discovery. Collusion with insiders may be necessary to execute lengthy attacks. But with smart cards, detection risk does not necessarily increase with time because an attacker can work in private. So high levels of opportunity are not needed for attacks that require a lengthy execution. Time merely adds to the cost and even substantial costs may be justified by the potential rewards of compromising an electronic purse or debit card scheme.

Under ITSEC, the required standards of effectiveness to justify a high SoM are exacting, " ... successful attack being judged to be beyond normal practicality" [3]. Many of the cards in the survey (including [1],[2],[10],[14] and [15]) have been certified with a high SoM but concluding that an attack on these cards in their operational environment is beyond normal practicality may be dangerous. It should be assumed that, "given sufficient time and expertise, any smart card can be compromised".[5] So with financial smart card applications, attack practicality is influenced by matters of economics, measuring attack cost against potential reward. This requires a thorough risk analysis of the complete system. ITSEC can be used to evaluate complete systems but the scope of inquiry can be contained to a greater degree when the TOE is evaluated as a product thereby enabling certification to a higher level of assurance and SoM. These higher level certifications are useful to quote in marketing material and press releases where the constraints or limited scope of the security target are not given emphasis. Readers of this material should take great care that they are not inadvertently misled.

2.2. THE COMMON CRITERIA

The Common Criteria resulted from a cooperative effort to harmonise the disparate frameworks for information technology security evaluation that existed, particularly in Europe and North America. The general concepts and approach have much in common with ITSEC including evaluation against a security target to a defined level of assurance, considering aspects of correctness and effectiveness. The Common Criteria envisages the definition of Protection Profiles (PP), standardised and well understood sets of security requirements developed by a user group to specify their security functionality needs for a particular product. [16] is an example. This allows a manufacturer or product developer to build a product according to the requirements of a PP. They can then have it evaluated and claim conformance to the PP. The product is still eval-

[5] Section 2.6, page 7 of Smart Card Security User Group – Smart Card Protection Profile [16].

uated against a security target but the contents of the security target mirror the requirements laid down in the protection profile.

The degree of assurance that a security target has been met is measured by the EAL scale, with possible ratings from EAL1 to EAL7. As with ITSEC, the scope, depth and rigour of the evaluation increases with EAL level. Each EAL has a predefined package of assurance components drawn from the various assurance classes. Some examples of assurance classes include vulnerability assessment (AVA), development (ADV), tests (ATE), and delivery and operation (ADO). To illustrate the relationship between EALs and assurance components, EAL1 does not include any components from the vulnerability assessment class whereas EAL3 includes AVA_VLA.1 - Vulnerability Assessment, AVA_SOF.1 - Strength of Function Analysis and AVA_MSU.1 - Misuse Analysis. A number of the certifications in the survey augment the assurance components of the selected EAL. This involves selecting a component that would normally only be required in a higher EAL. Table entries 3 and 5 are augmented by the selection of AVA_VLA.2, (independent vulnerability assessment, resists low attack potential) which is normally required by EAL4.

The Common Criteria assurance classes represent a refinement to the ITSEC methodology in terms of explicitness and modularity. The Common Criteria includes a catalogue of well defined and understood security functionality requirements [18]. These are known as functionality classes and security targets or protection profiles specify their required security functionality by drawing from this detailed catalogue. The advantage of this approach is that the security functionality will be expressed in an explicit, unambiguous way. The wording is well understood and [18] includes detailed guidance for interpretation and application. This explicitness means that the precise scope of a security target, (and therefore, a certification) can be established. The framework of functionality classes, families and components also enforces an internal consistency on the functionality claims and a relationship to the identified threats. Because security targets and protection profiles are constructed from a set of standardised components, comparison of certifications by users and mutual recognition by certification bodies is more practical.

The Common Criteria provides guidance on calculating attack potential that specifically factors in attack identification time, which is similar to study time under the ITSEC. So under the Common Criteria, attack identification time must be included. The detailed guidance on calculating attack potential aims at removing some of the subjectivity from this difficult assessment task and it may offer more clarity that the ITSEC.

3. A SURVEY OF SMART CARD CERTIFICATIONS

This section presents a survey of certifications issued for smart cards intended for use in banking and electronic purse applications. The scope of the security target and the definition of the TOE varies widely among the surveyed products. We present observations regarding the relationship between security target scope, TOE definition and the level of security accreditation achieved.

	Product Name	Sponsor	Developers	Scheme	Country	Reference / Certification Date	Assurance Level	Resists Attack Potential	Limited Scope?
1	MULTOS Version 3 on Hitachi H8/3112 [2]	National Westminster Bank Plc	Mondex International	ITSEC	UK	P130 Sept 1999	E6	High	Yes
2	Mondex Purse release 2.0 on MULTOS Version 3 on Hitachi H8/3112 [1]	National Westminster Bank Plc	Mondex International	ITSEC	UK	P129 Sept 1999	E6	High	Yes
3	Mondex Purse Version 2.03 on MULTOS V4.1N & SLE66CX160S [9]	Credit Mutuel	Mondex International, Keycorp, Infineon	CC	FRA	99/09 Nov 1999	EAL1 Augmented AVA_VLA.2	Low	No
4	SLE66CX160S Chipcard Security Controller [10]	Infineon Technologies	Infineon Technologies	ITSEC	GER	TUVIT-DSZ-ITSEC-9102-1999 Mar 1999	E4	High	Yes
5	Javacard/VOP GemXpresso 211 on Philips P8WE5032/MPH02 with applets Oberthur B0 v0.32 & Visa VSDC v1.08 [11]	Groupement Carte Blue	Philips Semiconductors, Gemplus, Oberthur, Visa International	CC	FRA	99/07 Dec 1999	EAL1 Augmented AVA_VLA.2	Low	No
6	Philips Smart card Controller P8WE5032V0B [12]	Philips Semiconductors	Philips Semiconductors	CC	GER	BSI-DSZ-CC-0153-1999 Nov 1999	EAL3	-	Yes
7	Banking Application B4/B0' Combined Smart Card MONEO/CB on ST19SF16B RCL [13]	Société Européenne de Monnaie Électronique	IBM Germany, ST Microelectronics	CC	FRA	99/04 Sept 1999	EAL1	-	No
8	ST16SF44 A Masked for application SCOT400 version 1 (reference ST16SF44ARHQ) [14]	ST Microelectronics, Bull CP8	ST Microelectronics, Bull CP8	ITSEC	FRA	98/01 Apr 1998	E3	High	Yes
9	Component ST16601 H/SKG masked for banking application B4/B0' V2 [15]	Groupement des Cartes Bancaires "CB"	ST Microelectronics, Bull CP8, GIE CB	ITSEC	FRA	97/04 Dec 1997	E3	High	Yes

Table 1 Survey of Smart Card Certifications.

3.1. EXPLANATION OF TABLE HEADINGS

The column, "Resists Attack Potential" in Table 1 requires some explanation. For ITSEC certifications it refers to the claimed minimum strength of mechanisms (SoM). As was discussed in section 2.1, the SoM claim implies that the TOE can resist attackers possessing the stated level of expertise, opportunity and resources. So a TOE claiming a basic SoM could be compromised by an attacker with a medium level of expertise, opportunity and resources but a TOE with a high SoM could resist an attacker with a high level of expertise, opportunity and resources, successful attack being beyond practicality. For the Common Criteria certifications, the value in this column is determined by the vulnerability component selected from the AVA_VLA assurance family.[6] Without augmentation AVA_VLA.1 applies to EALs 1-3. AVA_VLA.1 does not require the evaluator to conduct an independent search for vulnerabilities. It merely requires that there are no obvious exploitable weaknesses. Therefore a TOE certified with vulnerability component AVA_VLA.1 might be compromised by an attacker with a low attack potential. Table entries 6 and 7 don't have an entry in this column because they are EAL3 and EAL1 certifications. They have not been certified to resist attackers with a low attack potential. Entries 3 and 5 are EAL1 certifications but they have been augmented by the inclusion of vulnerability component, AVA_VLA.2. This vulnerability component requires an independent search for vulnerabilities that could be exploited by an attacker with low attack potential. The TOE must resist such attackers.

The column labelled "Limited Scope?" is concerned with whether there are significant limitations on the scope of the evaluation.[7] Some interesting patterns emerge. All of the surveyed ITSEC certifications claim a high minimum SoM, implying that successful attacks are not practical, even for attackers with a high attack potential. All of these evaluations also have their scope limited in critical ways. Table entries 1 and 2 exclude the integrated circuit from the TOE while entries 8 and 9 limit the evaluation to phases of the card lifecycle up to and including integrated circuit testing. Bonding, personalisation and actual use are excluded. Entry 4 evaluates very specific security functionality namely, bus and memory encryption with true random number generation, monitoring of opera-

[6]The three levels of attack potential map to the four components of the vulnerability analysis, (AVA_VLA) assurance family. AVA_VLA.4 requires resistance to attackers possessing a high attack potential. AVA_VLA.3 requires resistance to attackers possessing a moderate attack potential. AVA_VLA.2 requires resistance to attackers possessing a low attack potential. AVA_VLA.1 requires resistance to obvious attacks.

[7]While a yes/no dimension admittedly requires a degree of generalisation and subjectivity, the column remains informative nonetheless.

tional modes, phase management and espionage protection. This scope limitation raises some interesting issues which are discussed in greater detail in the sections that follow.

3.2. MONDEX - E6 HIGH OR EAL1 LOW?

Table entry 2 lists the UK ITSEC certification of the Mondex Purse on MULTOS Version 3 on the Hitachi H8/3112 chip . This product was successfully evaluated at E6, SoM High in September 1999. Table entry 3 lists the French Common Criteria evaluation of the Mondex Purse on MULTOS Version 4.1 on the Infineon SLE66CX160S chip. This product was certified[8] at EAL1 augmented with AVA_VLA.2. The difference in the certification level achieved by the two Mondex products under the ITSEC and Common Criteria certification schemes is significant to say the least. The UK ITSEC E6 certification represents the highest level of assurance and the Highest SoM rating. The French Common Criteria EAL1 evaluation represents the lowest level of assurance, but more importantly, the vulnerability assessment at AVA_VLA.2 means that the product is only certified to resist attackers possessing a low attack potential. The certifications imply that attacks on the Hitachi H8/3112 based purse are beyond practicality but attacks on the SLE66CX160S based purse could be achieved by attackers possessing a moderate attack potential.

How can this considerable disparity be explained? One possibility is that the SLE66CX160S chip is less secure than the Hitachi H8/3112. But this seems to be a less than satisfactory explanation given that the SLE66CX160S chip was certified at E4 SoM High in March 1999,[9] and the Hitachi H8/3112 has not been certified at all. A more plausible explanation can be found in the certification report for Mondex on the Hitachi chip which includes the following assumption about the TOE's environment:[10]

> "The ICC used for the purse is tamper-resistant and withstands tampering attacks with a strength that is consistent with a High SoM."

An identical assumption appears in the UK ITSEC MULTOS certification [2]. It is quite clear from other sections of the certification reports that the chip is excluded from the TOE and has not been evaluated under ITSEC. If disparity in the security of the underlying chips can-

[8] Only one month later, in November 1999.
[9] Refer to table entry 4.
[10] Annex A: Summary of the Security Target - Environmental Assumptions in [2]. Note that the TOE in table entry 2 is the Mondex application and the TOE in table entry 1 is the MULTOS operating system.

not explain the differences in certification level[11], it raises the following question. Would the Mondex purse on the Hitachi chip have reached E6 SoM High if the chip had been included in the TOE? We are unable to answer this question but the exclusion of the chip seems somewhat artificial and conspicuous. It is the only instance that we can locate where a certification of a smart card loaded with an application excluded the chip. Table entries 3, 5, 7, 8 and 9 are certifications of smart cards loaded with banking applications and the TOE includes the integrated circuit, operating system and application.

The separate evaluations of the MULTOS operating system [2] (where the chip is excluded) and the Mondex purse [1] (where the chip and operating system are excluded) creates similar uncertainty. The summary of the Mondex purse security target [1] states that "The TOE is also protected against specific hardware attacks by the MULTOS software interacting with the hardware alarm sensors". But the MULTOS ITSEC evaluators did not examine this aspect of the card's operation because hardware tamper resistance was assumed to justify a high minimum SoM. The evaluator did not perform independent penetration testing to verify it. Also, the security functionality claimed in the MULTOS security target is very specific and focuses on the secure loading and deletion of applications and insuring that one application cannot access another application's memory space. The Mondex E6 evaluation relies on the synergistic cooperation of hardware alarm sensors and MULTOS software to defeat certain hardware attacks[12] but confidence in this functionality has not been established within the same independent evaluation framework.

The Common Criteria certifications in table entries 3, 5, and 7 evaluate cards loaded with a financial application.[13] These TOEs include the three layers namely, integrated circuit, operating system and application as an integrated whole. Table entries 3 and 5 resist attackers with a low attack potential while entry 7 does not, (resisting only obvious attacks). This tends to encourage a speculation that attaining certifications with resistance to medium and high attack potentials under the Common Criteria is more difficult than under ITSEC. The lowest ITSEC SoM in the survey is High and the highest under the Common Criteria is Low. The Smart Card Security User Group Smart Card Protection Profile (SCSUG-PP)[14] emphasises that a vulnerability to certain types of threats

[11] Another possible explanation is that the TOE could have achieved a higher level of assurance but the sponsor only required evaluation at a lower level.

[12] Threats of this nature are included in the security target. "Creating value within a purse using electronic or physical means" and "forging a purse with value on it" are examples [1].

[13] Table entries 3 and 7 include stored value electronic purse applications.

[14] Annex D - Packages, Section D.5.1 - Allocation of Threats to Packages, page D-8 of [16].

can only be ascertained by examining the integrated circuit, operating system and application as an integrated whole because effective security relies on a synergistic contribution of these three layers. Resistance to differential power analysis and manipulations of the clock signal and power are examples of threats that must be examined in the context of the integrated platform.

SCSUG-PP [16] requires an assurance level of EAL4 augmented by the selection of AVA_VLA.3 which demands resistance to attackers possessing a medium attack potential. AVA_VLA.3 mandates that the evaluator perform and document a systematic search for vulnerabilities. The SCSUG-PP reinforces this requirement through a refinement to the vulnerability analysis component[15] requiring that the analysis take into account certain guidelines that direct the search for exploitable vulnerabilities:[16]

> "(Refinement) The analysis shall take into account the following generic vulnerabilities: a) The TOE may be subject to deconstruction to reveal internal circuits and structures.
> b) The TOE may be subject to tampering with the structure and content of internal memories, data transport mechanisms, security functions, and test methods.
> c) The TOE may be subject to analysis of information which is internal to the device, through monitoring of connections between elements of the circuits and structures.
> d) The TOE may be subject to use of logical commands to produce responses that lead to security vulnerabilities.
> e) The TOE may be subject to manipulations outside defined operational boundaries that lead to security vulnerabilities.
> f) The TOE may be subject to analysis of information that is available external to the device through monitoring emanations or any of the connections to the device including power, ground, clock, i/o, and reset.
> g) The TOE may be subject to vulnerabilities that have been identified in preceding generations of the same, or a similar, TOE."

This guidance is reflected in the specific identification of these issues as threats and the inclusion of security objectives that address them. They are also directly reflected in detailed functional and assurance requirements.

Contrast this approach with that of table entry 6, (a Philips Smart Card Controller used as the IC in the entry 5) whose security target specifically excludes threats relating to physical tampering. The security targets for table entries 8 and 9 naturally focus on threats that are relevant to the card lifecycle stages of design, manufacture and testing since the evaluation limits its scope to these phases. These threats in-

[15] Specifically AVA_VAL.3.1C - Content and presentation of evidence elements.
[16] Section 6.6.5, page 98 of [16].

clude theft, alteration or substitution of the mask, theft or disclosure of application software, personalisation of card(s) by an unauthorised entity, and unauthorised modification of configuration data.[17] It seems reasonable to question whether the High SoM would have been achieved had threats in the environment of actual use been fully considered in the security target. As a consequence, the certification does not provide the card issuer with an authoritative independent assessment of how the card will counter these threats when in the unsupervised custody of untrusted users.

This is not to say that card certifications examining the phases of design, manufacture and testing are not important. This is a critical part of the card lifecycle where vulnerabilities can be introduced. But it is also only part of the picture. Similarly with the UK ITSEC certifications of MULTOS and Mondex, whose focus is on protocol design and the quality of the software that comprises the operating system and application. This is also very important since software bugs can be exploited simply with a card reader and a PC. But the approach of the SCSUG-PP [16] suggests that still more is needed. Unless a sensible, realistic and complete set of threats are examined and addressed in the context of an integrated product in an operational environment, a certification runs the risk of misleading those who do not carefully study the scope of the security target.

4. CONCLUSIONS

We have presented an analysis of ITSEC and Common Criteria certifications as they apply to smart cards. This included a survey of actual smart card certifications relevant to the finance and banking industry. We highlighted the difficulty in interpreting and determining minimum strength of mechanism and performing vulnerability analysis in the context of smart cards, a problem that flows from the orientation of the two certification schemes toward software and components for networked computer systems. These are typically expensive, monitored and afforded external protection whereas smart cards are inexpensive and issued in large numbers to untrusted users for their long term and unsupervised retention. This together with the nature of a smart card as a small portable device without its own power or clock signal, creates a unique set of threats and considerable difficulty in applying SoM and vulnerability assessment guidance.

[17] SCSUG-PP [16] also requires effective protection against these threats.

We discussed the ITSEC certifications in the survey, noting that they all claimed a high SoM but the scope of each evaluation was also limited in some way, either to particular phases of the card lifecycle, by exclusion of the chip from the TOE or by specifically excluding relevant threats. We questioned whether a high SoM would be attained if all threats were considered in the context of the integrated product, as it is issued to the user in its actual mode of use. We contrasted the Common Criteria certifications which were evaluated to resist attack potentials rated at low, (or less). We questioned whether the security target scope restrictions contributed to this difference. The analysis served to highlight the importance of interpreting a certification in the context of the security target.

As a final note we wish to emphasise that evaluations that are limited in scope in some way are still useful, but they do require care in their interpretation. Card issuers will derive the greatest utility from certifications that are based on a realistic and complete set of threats. The SCSUG-PP [16] recognises this and presents a thorough and detailed evaluation baseline. While the design, development and manufacturing phases are important, and software quality is equally important, addressing threats in the context of an integrated product in its environment of use is the only way to arrive at a balanced assessment of a card's security from the issuer's perspective. After all, one of the key aims of certification is to provide a basis by which, potential purchasers of a product can decide whether it is appropriate for their needs.

5. ACKNOWLEDGMENTS

The authors would like to thank Bill Caelli for the help and advice he gave during the discussions that led to this paper. This work was carried out under the auspices of SPIRT, and the authors acknowledge the support of Telstra.

References

[1] UK IT Security Evaluation and Certification Scheme - Certification Body, UK ITSEC Scheme Certification report No. P129 Mondex Purse Release 2.0 on MULTOS Version3 and Hitachi H8/3112 integrated circuit card. , UK ITSEC, September 1999.

[2] UK IT Security Evaluation and Certification Scheme - Certification Body, UK ITSEC Scheme Certification report No. P130 MULTOS Version3 on Hitachi H8/3112 integrated circuit card., UK ITSEC, September 1999.

[3] ITSEC, Information Technology Security Evaluation Criteria Version 1.2, June 1991.

[4] ITSEC, ITSEC Joint Interpretation Library (ITSEC JIL) Version 2.0, November 1998.

[5] TCSEC, Trusted Computer Systems Evaluation Criteria DOD 5200.28-STD, Department of Defence, United States of America, December 1985.

[6] Common Criteria, Common Criteria for Information Technology Security Evaluation [CEM] Part 1 , Version 2.1, August 1999.

[7] ITSEM, Information Technology Security Evaluation Manual, Version 1.0 September 1993.

[8] Kuhn, M G, Kommerling, O, Design Principles for Tamper-Resistant Smartcard Processors, USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA, May 10-11, 1999.

[9] Organisme de Certification SCSSI, Schéma Français de la Sécurité des Technologies de l'Information d'Évaluation et de Certification Rapport de certification 99/09 Porte-monnaie électronique Mondex Purse 2 version 0203 (composant SLE66CX160S, système d'exploitation MULTOS V4.1N), SCSSI, November 1999.

[10] Die Zertifizierungsstelle der TUV Informationstechnik, Zertifizierungsbericht SLE66CX160S Der Infineon Technologies TUVIT-DSZ-ITSEC-9102-1999, TUV Informationstechnik, March 1999.

[11] Organisme de Certification SCSSI, Schéma Français de la Sécurité des Technologies de l'Information d'Évaluation et de Certification Rapport de certification 99/07 Plate-forme Javacard/VOP GemXpresso 211 (microcircuit Philips P8WE5032/MPH02) avec applets Oberthur B0' v0.32 et Visa VSDC v1.08, SCSSI, December 1999.

[12] Bundesamt für Sicherheit in der Informationstechnik, Certification Report BSI-DSZ-CC-0153-1999 for Philips Smart Card Controller P8WE5032V0B, BSI, Nov 1999.

[13] Organisme de Certification SCSSI, Schéma Français d'Évaluation et de Certification de la Sécurité des Technologies de l'Information. Evaluation et Certification Française CERTIFICAT 99/04 Application bancaire B4/B0' V2 de la carte mixte MONEO/CB (référence : ST19SF16B RCL version B303/B002), SCSSI, September 1999.

[14] Organisme de Certification SCSSI, Schéma Français de la Sécurité des Technologies de l'Information d'Évaluation et de Certification Rapport de certification 98/01 Composant ST16SF44A masqué pour l'application SCOT400 Version 1 (référence ST16SF44ARHQ), SCSSI, April 1998.

[15] Organisme de Certification SCSSI, Schéma Français de la Sécurité des Technologies de l'Information d'Évaluation et de Certification Rapport de certification 97/04 Composant ST16601 H/SKG masqué pour l'application bancaire B4/B0' V2, SCSSI, December 1997

[16] Smart Card Security User Group, Smart Card Protection Profile - Draft, Version 2.0, May 1 2000.

[17] Common Criteria, Common Criteria for Information Technology Security Evaluation [CEM] Part 3 - Security Assurance Requirements, Version 2.1, August 1999.

[18] Common Criteria, Common Criteria for Information Technology Security Evaluation [CEM] Part 2 - Security Functional Requirements, Version 2.1, August 1999