
UK IT SECURITY EVALUATION & CERTIFICATION SCHEME

UK CC Interpretation - UK/3.1/008

12 March 2007

Status: Endorsed for use in UK Scheme

Subject: Treatment of commercial hardware that is part of a TOE

REFERENCES CC/CEM, Version 3.1, Revision 1, September 2006

Issue

1. The issue is what level of information must be supplied to the evaluators, and what activities must they undertake, when some of the security functionality of a TOE defined by a software vendor are implemented in part by the firmware/hardware platform?
2. This arises particularly in cases where
 - a. a software vendor's description of the security architecture (as provided for ADV_ARC.1) identifies that commercial hardware is included within the TOE has some responsibility for the protection mechanisms that support non-bypassability and/or self-protection.
 - b. A software vendor (e.g. for an operating system or firewall) is seeking compliance with a PP that includes requirements such as FPT_AMT¹ or FPT_STM, which are typically reliant on firmware/hardware.

Scope of Interpretation

3. The term "hardware" requires some expansion, as it is used to mean different things. It is quite uncommon to find vulnerabilities in commercial hardware (i.e. physical components). However, it is often the case for what is commonly termed "hardware" to include elements of firmware and software. For example, a NIC may include on-board firmware and a software device driver. A standard PC will include a firmware BIOS. On occasions, this paper uses the term "hardware" as a general term to distinguish it from the TOE software, and on other occasions, it is used very specifically to mean physical hardware. The context should make this clear.
4. This interpretation does *not* address the following issues that are dealt with elsewhere:
 - a. The treatment of third party software included as part of a software TOE;
 - b. Smartcard/IC security, which is covered by separate interpretations;
 - c. The treatment of hardware platforms that are outside the scope of the TOE.

¹ Where the abstract machine is part of the TOE.

Premises

5. This issue is based upon the following premises:
 - a. In cases where third party firmware/hardware is included as part of the TOE, a developer will typically not have access to proprietary information from the firmware/hardware vendor. However the consumer will expect the software vendor to have given due consideration to published information on the hardware/firmware. Also where the software vendor takes delivery of firmware/hardware from the firmware/hardware vendor and supplies it, together with the software vendor's product, as an appliance, then the consumer will expect the software vendor to have exercised due care whilst handling the firmware/hardware.²
 - b. The interpretation is based on the assertion that a primary role of evaluation is to build confidence in products/systems from the sponsor of an evaluation. For example, a consumer purchasing the Acme Firewall wants to obtain a firewall and platform in which he can place confidence. The consumer has an expectation that the EAL4 product he buys will operate in a secure manner. If a security flaw is subsequently discovered in the underlying hardware processor or network interface card (NIC), he will not realistically have expected that to be discovered by the Acme evaluation. The consumer will however, expect the hardware to offer the claimed functionality, and to resist known classes of vulnerability at the relevant level of attack potential.
 - c. It is desirable that the evaluation should focus its resources on those aspects of the TOE most likely to yield security vulnerabilities, and current experience suggests that these are more frequently found in software than in hardware.
 - d. Where not all aspects of a TOE have been evaluated to the same level of rigour, then the residual risks should be made clear to consumers.

Interpretation

6. Where SFRs are met in part by hardware/firmware included in the scope of the TOE, CEM requirements for each activity are modified as follows.

ADV Development

7. It is recognised that any SFR implemented in the software portion of a TOE ultimately relies on provision of supporting mechanisms in hardware (as reflected in the work unit ADV_ARC.1-4). However, for SFRs where the primary³ implementation is in software

² This contrasts with the scenario where the consumer has to procure the hardware/firmware directly from the hardware/firmware vendor.

³ The key notion in the meaning of "Primary" is that of "direction"; i.e. software may be regarded as primary in that it typically harnesses the functionality and directs the operation of hardware. The notion of the TOE supplier's scope of control is also relevant. (e.g. If the TOE is "W2K on specific Dell hardware" prime responsibility for most things will fall to W2K, and only if the TOE supplier claims, for example, FPT_PHP, will there be SFRs where there is no involvement from W2K, and the hardware vendor will need to be involved). However the latter notion extends to the typical scope of control for the TOE supplier's product type (e.g. if an operating system vendor also develops the hardware on which the operating system runs, then the

(as may be the case for some implementations of FPT_STM and FDP_RIP, which are ultimately reliant on hardware), this is not viewed to impose a requirement for the provision of hardware design information to the same level as would be the case for an SFR which is entirely mapped to the hardware portion of a TOE. The description of the hardware to be provided for satisfaction of ADV_ARC.1-4 is to identify the *role* the hardware plays in supporting the SFR (e.g. in the case of FPT_STM.1 this might be the identification that the hardware provides clock signals from the chipset and motherboard that are used to derive a system clock time). This description does not have to be at the level of detail required for the ADV_TDS component.

8. Paragraph 204 of CC Part 3 states that “all portions of the TSF are security relevant, meaning that they must preserve the security of the TOE as expressed by the SFRs and requirements for domain separation and non-bypassability”. Therefore, the security functionality of the TOE includes all properties of the TSF and specific mechanisms that are relied upon to provide domain separation and non-bypassability properties of the TSF.
9. Where the ADV_TDS, and ADV_IMP families are selected for use in the TOE assurance requirements, the following table shall be used to determine evaluation deliverable requirements. The detail provided in the security architecture description for software/firmware/hardware remains unchanged.

TOE should be evaluated in an equivalent manner to W2K).

		Primary³ responsibility for implementation of security functionality allocated to:		
		Software	Firmware	Hardware
Design information required for:	Software	Full TDS and IMP requirements	ARC will describe any software reliance on firmware in terms of the functionality provided by the firmware. The firmware description need only go to the subsystem level of detail ⁴ .	ARC will describe any software reliance on hardware in terms of the functionality provided by the hardware. The hardware description need only go to the subsystem level of detail ⁴ .
	Firmware	Full description of security functionality. The description shall identify which firmware subsystems ⁴ support the implementation of each SFR.	Full TDS and IMP requirements.	ARC will describe any software reliance on hardware in terms of the functionality provided by the hardware. The hardware description need only go to the subsystem level of detail ⁴
	Hardware	Full description of security functionality. Physical description of hardware (sufficient detail to allow procurement of unique hardware, down to a level where changes in detailed specification have no security impact (e.g. no need for make of power supply or hard disk)). The description shall identify which physical components support the implementation of each SFR.		Full TDS and IMP requirements.

10. For example, where FPT_STM Reliable Time Stamps is used in the TOE functional requirements, and the TOE includes the firmware/hardware platform, the following deliverables shall typically be required:

- a. Software – the role of software shall be fully defined in TDS for the TOE; the subsystems and modules used to translate the CMOS clock at boot-up and the relative

⁴ It may not be practical, due to limited public domain information, to identify more than one firmware subsystem (e.g. device driver or BIOS).

time as determined by hardware clock cycles into a date/time into human readable form, which can then be used to display system time or stamp audit records with date/time. The implementation representation shall be supplied as required.

- b. Firmware – the subsystem description for TDS shall identify those features of firmware that support the issue of date/timestamps, and which components of firmware implement those features.
- c. Hardware – the hardware component that supplies a time signal shall be identified (e.g. Intel Pentium 4) together with security relevant characteristics of the design, (the processor speed may play a part in the accurate translation of hardware clock cycles to relative time).

For hardware and firmware in this case, the level of information required will typically reside in the public domain.

- 11. In the case of FDP_RIP, where enforcement of the requirement commonly relies upon third party firmware (e.g. in NIC or processor), some information may be found in the public domain, but confirmation of the measures taken to clear buffers may be difficult to obtain. In such cases, a vulnerability search supported by penetration testing may be considered an acceptable alternative.
- 12. Note that in many cases it will not be necessary to distinguish hardware and firmware where these are supplied as a single entity.
- 13. Where the hardware is included in the scope of the TOE, and hardware functions are needed to support the security functionality that is primarily provided in software (e.g. FDP_RIP.1 where clearing contents of memory is controlled by kernel memory manager), the functional description of the hardware relied upon should be provided so as to ensure it is capable of providing the required functions, and for input into the vulnerability analysis. At ADV_TDS.3 (and above), this functional description should be sufficient to understand the interaction between the hardware components of the specification.

ATE Testing

- 14. Where a TOE includes hardware that implements security features, the requirements from class ATE shall be applied to testing of this hardware. Such testing will typically be at the TSFI, but shall also consider any assurance requirements taken from the ATE_DPT family.

AVA Vulnerability analysis

- 15. Where a TOE includes hardware (e.g. NIC or PC platform) that implements, or supports the implementation of security features, the developer ARC security architectural description and evaluator vulnerability analysis shall also include hardware vulnerability information from the public domain, and from the same design sources as are required for the ADV class by this interpretation.
- 16. For example, if the hardware specification contains a NIC, the security architectural description will consider the role the NIC plays in protecting the TOE from bypass/tampering and the evaluator vulnerability analysis will consider known (in the public domain) hardware/firmware vulnerabilities associated with that item. Both will

consider processing of packets from an untrusted user interface, and the potential that packets leaving the TOE contain residual information as a result of buffer mis-management within the NIC. Penetration testing can then be performed.

ALC_DEL Delivery

17. Where the software vendor takes responsibility for the supply of the associated hardware to consumers, the evaluators will have to examine the software vendor's delivery of both software and hardware through application of an ALC_DEL component (if required by the assurance package). The evaluators will also have to examine the software vendor's process for checking the hardware delivered to him or otherwise establishing confidence in its authenticity. Where the software vendor does not take responsibility for delivery of the associated hardware to the consumer, the software vendor shall provide information in the guidance documentation to identify this potential source of vulnerability, and shall suggest appropriate means of procurement or other measures to ensure a secure platform.⁵

ALC Configuration Management

18. Where the software vendor takes responsibility for the supply of the associated hardware, the evaluators will have to examine the Software vendor's configuration management, for both development of software and control of hardware, through application of requirements from the ALC_CMC family (if required by the assurance package). Where the developer does not take this responsibility, the developer shall ensure that the hardware is identified to a level of detail that makes it apparent to potential customers what product must be purchased, and what configuration options must be used, in order for the TOE to run securely.⁵ This would include the BIOS version for any PC hardware platform.

AGD Preparative and operational guidance

19. The evaluators shall ensure that the appropriate guidance for hardware configuration is provided. This may include, for example, the need to disable certain features of the hardware.

Platform claims

20. Inclusion of specific hardware within the TOE will often reduce both the utility and useful life of the evaluation results. This is because software products tend to be supported on a range of hardware platforms, in many cases without change to the software. Where certification occurs on a specific, named platform, that platform may be unsuitable for the consumer's needs, or may quickly become obsolete. For this reason it is desirable for a range of platforms to be included in the certification.
21. For certification of a TOE that includes hardware, a statement shall be included in the TOE Description in the ST concerning the validity of the results on different platforms.⁶

⁵ The point here is that we do not want to penalise developers who do take responsibility for providing the hardware together with the software. Where developers do not take responsibility, then consumers who buy things from them need to be aware of the different assurance involved.

⁶ For a TOE that does not include hardware, the requirement is only for a statement of which hardware was used for testing, since no assurance is claimed for the hardware.

22. Where a TOE includes hardware, the results of the evaluation shall by default be valid for only the specific platform(s) tested by the evaluator. These platforms shall be identified in the CR. Where wider applicability of results is sought (e.g. for all Intel platforms) a rationale shall be provided to the evaluators as part of the evidence to meet ATE_FUN and other families where relevant (e.g. ADV_IMP, AGD_PRE or ALC_CMC).
23. The rationale should clearly state the specific platforms that were tested, the range of platforms that the evaluation results are valid for, and the basis on which that range has been chosen. The guidelines of the parallel interpretation applying to TOEs that do not include hardware platforms, shall form the basis of the approach. These will be supplemented by additional information that addresses paragraphs 7-19 above, where affected by the different platforms. For example, if the information provided for design was generic in nature, then no additional information may be required. However, if tests specific to one platform were carried out, then these may need to be repeated for all platforms.
24. The rationale shall be summarised in the CR.

Additional Advice

25. The approach of paragraphs 20-24 above addresses the range of hardware platforms formally included within the scope of the TOE. However it may be useful to the consumer for a CR to supplement the formal certification result with advice on the possible risks of using other hardware platforms. This may apply where the software vendor maintains a list of hardware which he claims supports secure operation of his product and subsequently adds to the list included within the formal certification result.
26. When formulating advice on such risks, the evaluators should consider factors such as:
 - a. The actions taken by the developer when adding items to the list;
 - b. The potential impact of using hardware from another vendor;
 - c. The potential impact of using items with higher specification or increased functionality (e.g. 1Gb NIC in place of 10/100 NIC, or a dual port NIC in place of a single port NIC, NIC with capability for remote wakeup, rmon);
 - d. The potential impact of using items with lower specification (e.g. problems caused by insufficient memory) although this is usually addressed by an assumption regarding minimum hardware configuration.
27. A summary of the evaluators' recommendations should be included in the CR, and shall be accompanied by a note that these are additional to the formal certification result. A consumer can then make a judgement for use, taking into account the status of the recommendations and the identified risks.

A note on drivers

28. Device drivers may be seen to exist on the boundary of ownership between the operating system and the hardware peripheral device. The driver will often be written by the peripheral supplier, but will be packaged with the operating system. It is difficult to provide a standard approach for evaluations, and this may require case-by-case interpretation. Two examples are offered for guidance in situations where the hardware provides a supporting role in implementing security functionality:

- a. The hardware peripheral vendor always provides the driver. In this case, the driver version would be identified, and the evaluator would search for vulnerabilities in the public domain and consider carrying out some specific tests.
- b. Software developer provides a standard set of drivers and no others can be loaded. In this case the drivers would be treated as part of the o/s, and be subject to the same activities as the rest of the o/s.

The rationale here is the same one that pervades this interpretation. In case a) the driver is seen to originate from a third party, and in case b) it is seen to be the TOE developer's responsibility.