



Joint Interpretation Library

---

Requirements to perform  
Integrated Circuit Evaluations

Version 1.1

July 2003



Table of Contents

**1 Introduction ..... 4**

**2 Required Knowledge and Skill ..... 4**

2.1 Overview..... 4

2.2 IC Design and Production Process ..... 4

2.3 Smartcard Integrated Circuit Technology ..... 6

2.4 Smartcard specific Attacks ..... 7

2.5 The IT-Security Evaluation Facility (ITSEF)..... 8

2.6 Subcontracting with a specialised IT-Security Evaluation Facility..... 9

**3 Summary ..... 9**

**4 Literature ..... 10**

## **1 Introduction**

In order to ensure credible results from the evaluation of smartcard integrated circuits (ICs) according to the Common Criteria, an IT-Security Evaluation Facility (ITSEF) must have a minimum set of capabilities. These capabilities differ from those required for software systems in both the equipment required and the skills and knowledge needed by the evaluator.

Requirements for the accreditation are described in ISO/IEC 17025 [1] and supplemented by the certification bodies. Within ISO/IEC 17025, chapter 5, there are requirements for the technical skills and equipment to be available.

This document is intended to provide guidelines for the technical accreditation of ITSEFs for performing integrated circuit evaluations.

## **2 Required Knowledge and Skill**

### **2.1 Overview**

The required knowledge and skill of the evaluator can be grouped as follows:

- understanding of the smartcard design and production process in general and of the IC design and manufacturing process (refer to section 2.2),
- understanding of smartcard IC technology, its underlying principles and the development equipment used by IC manufacturers (refer to section 2.3),
- knowledge of smartcard fraud and attack scenarios,
- knowledge and experience in IC failure analysis, an understanding of the underlying physical principles and an ability to use the related equipment (refer to section 2.4),
- knowledge and experience in cryptographic attack techniques and the ability to perform the analysis (including data-capture and signal processing procedures) (refer to section 2.4).

In addition, the ITSEF will need equipment pertinent for IC failure analysis, diverse other smartcard attacks and cryptographic attack techniques (refer to section 2.4). The required tools can be categorised in standard (basic), specialised and bespoke (refer to section 2.5).

### **2.2 IC Design and Production Process**

IC hardware and software is in general developed by different companies. These components are then integrated and additional security relevant data is injected into the card.

The security objectives for an IC are twofold:

- Ensure a level of security for the card in the field.
- Maintain the level of security throughout the development and production process.

Although many specialists concentrate on security in the field (since the smartcard is delivered into a hostile, unregulated environment and may be subject to tampering), security during the development, production and personalization process is also important. The security objectives, that a smartcard component are assessed against, will depend very much on the application context which can be dependent upon the production and personalization process. In particular, personalization affects the security functionality to be provided by the smartcard.

The Common Criteria depict an ideal development process starting with a definition of the requirements followed by the design process, implementation, test, acceptance, delivery and usage. When looking at the components of a composite product this process must be interpreted and rearranged.

For instance, the chip manufacturer develops the design of the chip hardware and the software for testing. He receives the software from the software developer to create the ROM image. Then the mask files are sent to the mask manufacturer. The masks or reticles are returned to the chip manufacturer. After wafer production the chips are tested and initialisation data (transport keys, traceability data) are injected into the E<sup>2</sup>PROM (or other non-volatile memory). The initialisation data are defined by the card manufacturer. Operational dies are delivered or directly embedded into modules. The protection of die delivery can be complex: The authentication mechanism is realised by the software manufacturer but used by the card manufacturer (or personalisation centre). The keys are generated by the card manufacturer but injected into the card by the chip manufacturer using a procedure (for diversification etc.) defined by the card manufacturer.

These examples show that a real development process can be more complex than the assumed one by the Common Criteria. Inputs and outputs are not always as simple as expected by the Common Criteria. As a result, the corresponding assurance components of the Common Criteria (for instance delivery) must be interpreted, refined, and rearranged if needed. In addition, it must be ensured that the processes of different components (and their description in terms of Common Criteria assurance components) fit together.

The evaluators must understand the smartcard supply chain and its integration into the application context in order to be able to interpret the Common Criteria assurance requirements in an appropriate way. In particular, these assurance requirements are:

- User Guidance (AGD\_USR),
- Administrator Guidance (AGD\_ADM),
- Delivery (ADO\_DEL),
- Installation, Generation and Start-Up (ADO\_IGS),
- Tools and Techniques (ALC\_TAT),
- Life-Cycle Definition (ALV\_LCD), and
- Development Security (ALC\_DVS).

In addition, differences between the evaluation of smartcard ICs and the evaluation of software mean that the interpretation of Common Criteria assurance components of the classes ASE, ADV, ATE and AVA is also required.

Some guidance is already given in [2]. Especially the documents [3] - [8] provide detailed guidance on the evaluation of smartcard ICs.

Note that the evaluator also needs to understand the smartcard IC design and manufacturing process since it can not be expected that each IC manufacturer will describe their processes and security measures without assuming such an understanding.

### 2.3 Smartcard Integrated Circuit Technology

The evaluator must understand smartcard integrated circuit technology and the underlying principles to the extent necessary to comprehend the design decisions of the IC manufacturer. Basic knowledge about

- electron theory of semiconductors (physics) and the electrical behaviour of semiconductors and transistors,
- physical and electrical behaviour of all standard materials used in integrated circuit manufacturing (for instance silicon, poly-silicon, metal, and isolating and passivation material),
- physical layout (implementation on the semiconductor surface) of standard cells (simple gates), memory cells (E<sup>2</sup>PROM, RAM, ROM) and memory blocks,
- layout principles and methods of routing and layering,
- production steps and the resulting layer structure on the chip's surface.

The evaluator must have detailed knowledge of

- digital and analogue circuit engineering (digital gates of different complexity and standard analogue circuitry),
- static and dynamic behaviour of digital and analogue circuitry,
- microcontroller architecture and functionality,
- realisation of standard circuitry as used in micro-controllers.

The evaluator must be able to understand the schematics (block diagrams, schematics on gate and transistor level). The functional components can be described in the form of standard schematics or in VHDL-sources.

The evaluator must have knowledge of the VLSI design process and must basically understand the process from the schematics or VHDL-sources (logical representation of the chip) to the actual layout and dice/wafers (physical representation). The evaluator must

understand the processes of technology qualification, functional testing, characterisation, and reliability testing.

The evaluator must understand the development equipment used by the manufacturers for micro-controller software. This includes simulators, emulators, and special evaluation software masks. The evaluator must be able to read micro-controller source code and to develop software for penetration testing and other investigations. Therefore, the evaluator must understand the CPU instruction set, the memory map and use of other peripheral units of the micro-controller.

## 2.4 Smartcard Specific Attacks

The following provides an overview about smartcard specific attacks. This is not a complete list but provides some examples. Detailed information about smartcard specific attacks can be found in 'Annex A: Examples for Smartcard specific Attacks' of this paper.

The evaluator must know about standard smartcard fraud and attack scenarios and in principle be able to develop new ideas for such attacks. In addition, the evaluator must know about attack scenarios for ICs such as physical manipulation and probing, malfunction attacks, inherent and forced leakage attacks, abuse of test features, cryptographic or software attacks, which are not described here.

The evaluator must be able to adapt and combine these attack scenarios for the individual chip being subject to evaluation. During vulnerability analysis the evaluator must be able to find possible weaknesses (in schematics and their realisation on the chip and the combination thereof) and be able to use the standard techniques to assess them.

The evaluator must have knowledge and experience in IC failure analysis to be used for physical manipulation and probing. The evaluator must at least understand the physical principles, and the usage (as appropriate) of the equipment classed as 'standard' and 'specialised' (in section 2.5). Moreover, the evaluator must be able to use the 'bespoke' tools with the help of trained operators. The evaluator must know how these tools and techniques can be used during vulnerability analysis in order to assess the IC's security properties and functions. The method and purpose of using the equipment (especially Focused Ion Beam (FIB), Scanning Electron Microscope (SEM) or E-beam Tester) during the vulnerability assessment should not necessarily correspond to the expectations of the operating personnel. The evaluator should instruct the operating personnel.

The evaluator must have knowledge and experience of other smartcard attacks (such as Differential Power Analysis (DPA), Differential EM radiation Analysis (DEMA) and related attacks) and possess the equipment (physical and analysis tools) necessary to perform such attacks. The evaluator must be able to operate this equipment (including data-capture procedures) and to perform the analysis (mathematics). Knowledge and experience in cryptography and standard cryptographic attack techniques is required. The principles of timing and other attacks (such as Differential Fault Analysis (DFA)) must be understood. The evaluator must be able to find vulnerabilities related to such attacks.

The evaluator must be able to develop software to communicate with the smartcard. Therefore, the evaluator must understand the I/O protocol being supported, the operating conditions and the external command interface if being used or attacked.

The evaluator must know how to handle chip card readers and be able to modify them in order to use the chips in different packages and to apply non-standard operating conditions. Therefore, the evaluator must be able to use standard equipment such as voltage supply, signal and function generators, oscilloscopes, and soldering irons.

### **2.5 The IT-Security Evaluation Facility (ITSEF)**

The IT-Security Evaluation Facility (ITSEF) must be well organised and provide instructions for the evaluator. These instructions must describe physical, procedural and organisational security measures or refer to other documents, which describe them. A Quality Management System must exist. The requirements of ISO/IEC17025 must be met. In order to accomplish the vulnerability and failure analysis, physical manipulations, and attack scenarios mentioned in section 2.4, the IT-Security Evaluation Facility must have unrestricted access to the following tools and shall be able to use them efficiently.

Standard equipment:

- Standard laser emitter
- UV-light emitter
- Climate chamber
- Voltage supply
- Oscilloscope analogue
- Chip card reader
- PC or work station
- Signal analysis software
- Signal generation software

Specialised equipment:

- Visible light microscope and camera
- UV light microscope and camera
- Microprobe work station
- Laser cutter

- Signal and function processor
- Oscilloscope digital
- Signal analyser
- Tools for chemical etching (wet)
- Tools for chemical etching (plasma)
- Tools for grinding

Bespoke equipment:

- Scanning electron microscope (SEM)
- E-beam tester
- Scanning Force Microscope (SFM)
- Focused Ion Beam (FIB)
- Special purpose laser system
- New technical design verification and failure analysis tools

The optical microscope and a camera must give sufficient magnification and resolution for the technology being assessed. The Microprobe Workstation must be equipped with appropriate needles. Supply equipment (voltage supply, signal and function generators) must be available.

For the equipment categorised as 'bespoke', the evaluator must have a good understanding of the underlying physical principles and of the capabilities of the tools. If the ITSEF uses other facilities, appropriate security measures must be applied to protect the chip vendor's information and samples, and the know-how of the ITSEF. If the ITSEF hires bespoke equipment, the evaluator must be present and must instruct the operating personnel.

## **2.6 Subcontracting with a specialised IT-Security Evaluation Facility**

When an ITSEF subcontracts work, this work shall be placed with a competent subcontractor. A competent subcontractor is one that, for example, complies with the International Standard for the work in question. ISO/IEC 17025 permits subcontracting of work subject to certain conditions.

## **3 Summary**

This document has described the knowledge, skills and facilities required by an ITSEF before it can be capable of preparing and carrying out an evaluation of smartcard integrated circuits. These capabilities are not limited to having access to sophisticated types of equipment and the knowledge of how to use them. Moreover, the ITSEF evaluator should completely comprehend the smartcard design and production process and have the ability to develop and

test for new attack scenarios. This knowledge cannot be gathered through short-term training but requires years of relevant experience.

If an ITSEF is known to meet the guidelines in this document, then a level of confidence will be provided to both the manufacturers (paying for the evaluation) and to the customers (accepting a certificate). Without these guidelines, that confidence can only be deduced by examining the detailed information from evaluation reports (although that still remains the ultimate measure of the ITSEF's performance).

## **4 Literature**

- [1] ISO/IEC 17025: General requirements for the competence of testing and calibration laboratories
- [2] Information Technology Security Evaluation Criteria: The Application of ITSEC to Integrated Circuits, January 1999
- [3] Joint Interpretation Library - Application of Attack Potential to Smartcards, Version 1.1, July 2002 (also Common Criteria supporting document)
- [4] Joint Interpretation Library - Application of CC to Integrated Circuits, Version 1.2, July 2002 (also Common Criteria supporting document)
- [5] Joint Interpretation Library - ETR-lite for Composition, Version 1.1, July 2002 (also Common Criteria supporting document)
- [6] Joint Interpretation Library - ETR-lite for Composition: Annex A: Composite smartcard evaluation : Recommended best practice, Version 1.2, March 2002 (also Common Criteria supporting document)
- [7] Joint Interpretation Library - Common Criteria supporting document: ST-lite, Version 1.1, July 2002 (also Common Criteria supporting document)
- [8] Joint Interpretation Library - Guidance for Smartcard Evaluation, Version 1.1, March 2002 (also Common Criteria supporting document)