



Joint Interpretation Library

---

Integrated Circuit Hardware Evaluation Methodology

Vulnerability Assessment

Version 1.3

April 1999

This document is paginated from i to iv and from 1 to 53

## Table of contents

<b>0</b>	<b>Introduction.....</b>	<b>1</b>
<b>1</b>	<b>Smartcard as a TOE.....</b>	<b>3</b>
1.1	TOE overview .....	3
1.1.1	Standards .....	4
1.1.2	Smartcard IC functional description .....	5
1.2	TOE evaluation boundaries .....	7
1.2.1	Smartcard lifecycle .....	7
1.2.2	Phase 1: Smartcard embedded software development .....	9
1.2.3	Phase 2: IC development .....	9
1.2.4	Phase 3: IC manufacturing .....	9
1.2.5	Phases 4,5: ICC production .....	10
1.2.6	Phase 6: ICC personalisation .....	10
1.2.7	Phase 7: End-user .....	10
<b>2</b>	<b>Scope of evaluation.....</b>	<b>11</b>
<b>3</b>	<b>Threat model.....</b>	<b>13</b>
3.1	Categorisation of threats .....	13
3.2	Phase 1: Smartcard embedded software delivery .....	14
3.2.1	Assets .....	14
3.2.2	Environmental threats .....	14
3.3	Phase 2: IC development .....	14
3.3.1	Assets .....	14
3.3.2	Environmental threats .....	14
3.4	Phase 3: IC manufacturing .....	15
3.4.1	Assets .....	15
3.4.2	Environmental threats .....	15
3.4.3	TOE threats .....	15
3.5	Phases 4,5: ICC production .....	15
3.5.1	Assets .....	15
3.5.2	Environmental threats .....	15
3.5.3	TOE threats .....	16
3.6	Phase 6: ICC personalisation .....	16
3.6.1	Assets .....	16
3.6.2	Environmental threats .....	16
3.6.3	TOE threats .....	17
3.7	Phase 7: End-user .....	17
3.7.1	Assets .....	17
3.7.2	TOE Threats .....	17

<b>4</b>	<b>Security objectives</b> .....	<b>19</b>
4.1	Phase 1: Smartcard embedded software delivery .....	19
4.2	Phase 2: IC development .....	19
4.3	Phase 3: IC manufacturing .....	20
4.4	Phases 4,5: ICC production .....	21
4.5	Phase 6: ICC personalisation .....	21
4.6	Phase 7: End-user .....	22
<b>5</b>	<b>Vulnerability model</b> .....	<b>23</b>
5.1	Import of subversive material .....	23
5.2	Imperfect Processing .....	24
5.3	Unauthorised Access .....	24
5.4	Vulnerability characterisation .....	25
5.4.1	Import of subversive material .....	25
5.4.2	Imperfect Processing .....	26
5.4.3	Unauthorized Access .....	27
<b>6</b>	<b>Test model</b> .....	<b>29</b>
6.1	Security Mechanism Testing Model .....	30
6.2	Classification of Security Mechanism .....	31
6.3	Physical Security Mechanism .....	31
6.3.1	Properties .....	32
6.3.2	Test Model .....	33
6.4	Data Storage Cell Security Mechanism .....	33
6.4.1	Properties .....	34
6.4.2	Test Model .....	34
6.5	Environmental Exchange Security Mechanism .....	35
6.5.1	Properties .....	35
6.5.2	Test Model .....	36
6.6	Leakage Security Mechanism .....	36
6.6.1	Properties .....	36
6.6.2	Test Model .....	37
<b>7</b>	<b>Calculating attack potential</b> .....	<b>39</b>
7.1	Introduction .....	39
7.2	Calculating attack potential to effect an attack .....	39
7.2.1	Expertise .....	40
7.2.2	Equipment .....	40
7.2.3	Collusion (Available knowledge) .....	41
7.2.4	Time .....	41
7.2.5	Calculating attack potential .....	42

<b>Annex A</b>	<b>Typical IC Manufacturing Process Description .....</b>	<b>45</b>
A.1	Background .....	45
A.2	Production of Wafers .....	45
A.3	Inside the Wafer Fabrication Facility .....	46
A.3.1	Schematic of a Cross section through a generic CMOS technology .....	46
A.3.2	Oxidation or Oxide Deposition .....	46
A.3.3	Masking .....	47
A.3.4	Etching .....	47
A.3.5	Implantation (or diffusion) .....	47
A.3.6	Repeating the steps .....	48
A.3.7	Dielectric deposition and metallisation .....	48
A.3.8	Passivation .....	48
A.3.9	Backgrinding .....	49
A.4	Electrical test .....	49
A.5	Packaging .....	49
<b>Annex B</b>	<b>Glossary of Terms.....</b>	<b>51</b>



## 0 Introduction

- 1 This document provides a basic model for evaluation of smartcards, and in particular for hardware evaluation, including dedicated software. The intention is that this model provide a basis for evaluation which supports the ITSEC/CC scheme objectives of repeatability, reproducibility, impartiality and objectivity. It also gives a basis for guidelines suitable for smartcard developers, helping to resolve the uncertainties in hardware evaluation.
- 2 This document should be read in conjunction with “Application of the ITSEC to IC” and with “Application of the CC to IC”.



## 1 Smartcard as a TOE

3 The purpose of this section is to provide a brief description of the scope of the TOE in order to understand its security requirements with respect to its physical characteristics and its envisaged usage.

### 1.1 TOE overview

4 A smartcard or Integrated Circuit Card (ICC) is a shaped piece of plastic with a small computer chip embedded into it. Two examples are the common ID-01 format, shaped in the familiar credit card size, and the ID-00 format frequently used in mobile telephones.

5 Smartcards fall into a number of categories:

- Contact Cards:
  - Memory only (sometimes with protection features),
  - Microprocessor with memory,
  - Microprocessor with memory and additional coprocessor,
- Contactless Cards:
  - As above but with power supplied either from an internal battery, or power derived from energy obtained through a contactless interface.
- a combination of both.

6 A chip is a semiconductor (silicon) Integrated Circuit (IC) fabricated in a complex microelectronic process. This involves taking a silicon substrate then repeatedly masking & doping the surface to form transistors, followed by patterning metal connections and a protective overcoat. This process eventually yields a design comprising typically several hundred thousand transistors, arranged in an area currently comprised less than 25 mm<sup>2</sup>. The design consists of central processing unit, optionally a coprocessor, input and output lines and volatile and non-volatile memory. See Annex A for a generic description of an IC manufacturing process.

7 The chip will be designed to be secure. In order to be secure, it should make appropriate use of both specific security enforcing design features, e.g. environmental sensors, and technological properties of the materials and processes used.

8 A part of the manufacturing process is the inclusion of operating system (OS) developer specific code, written in the microprocessor's native or machine code. This is usually contained in one of the numerous masks used during manufacture. In this document this is referred to as the ROM mask.

9 The IC itself is packaged. The current predominant method is die bonding in a module. A module consists of a carrier board on which the IC is seated. Wire bonds

are connected from the IC's Input / Output (I/O) pads to the carrier, which has contacts on its reverse side. The chip is then encapsulated in a protective material (usually some kind of epoxy) and the module is adhesively embedded into a pre-milled hole in the plastic card.

10 The plastic card was originally made from PVC [polyvinyl chloride], although more recently ABS [acrylonitrile-butadiene-styrol], PET [polyethylene terephthalate] or PC [Polycarbonate] have been used.

11 Smartcards have a wide variety of potential applications. The principal reason for their use is their ability to act as an intelligent remote processor, combined with the ability to maintain, with a relatively high degree of integrity and confidentiality, certain data contained within. It is this ability that, combined with appropriate software, enables applications to use cryptography (e.g. for digital signatures) and hence function as a controlled access mechanism for all kinds of applications. Currently popular applications comprise:

- GSM,
- Electronic commerce,
- Payment schemes,
- Authentication schemes.

12 A smartcard is usually part of an overall system, which may therefore apply additional measures to prevent or detect compromise of the system due to individual smartcard failures.

### 1.1.1 Standards

13 There are several standards that apply to smartcards at the application level, such as the EMV standards and the GSM standards.

14 However, at the IC physical level, the basic standards are:

- The ISO Standards ISO 7816 Identification Cards – integrated circuit cards with contacts:
  - Part 1 Physical Characteristics,
  - Part 2 Dimensions and Locations of Contacts.

15 There are additional requirements and tests in:

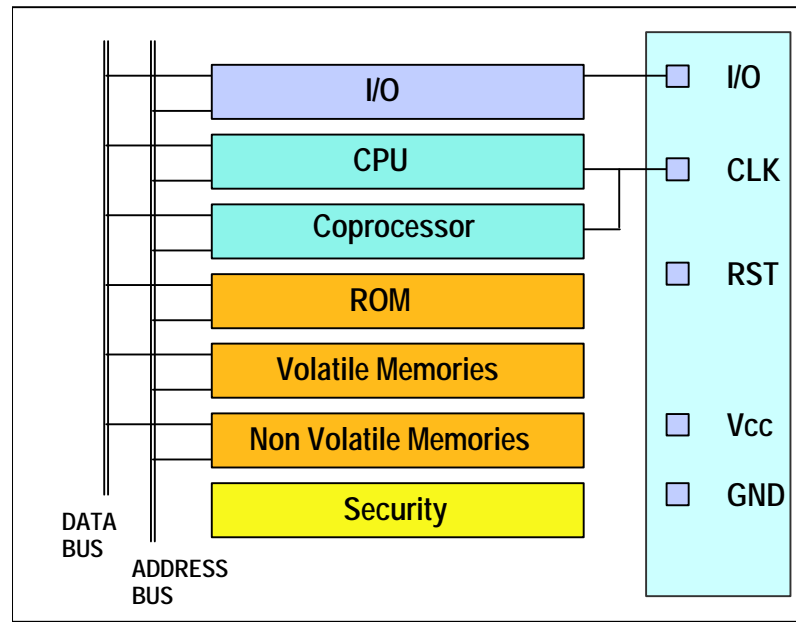
- ISO 7810 Identification Cards – Physical Characteristics,
- ISO/IEC 10373, 1993 Identification cards – Test Methods.

16 ISO 7816 Identification cards – integrated circuit cards with contacts Part 3 to 10 inclusive deal with electronic signals transmission protocols and inter-industry commands and registration, number systems and data elements.

## 1.1.2 Smartcard IC functional description

### 1.1.2.1 Block diagram

17



*Fig. 1.1 - Generic IC block diagram*

18 The basic smartcard IC can be represented by the components shown above.

19 Most ICs in security-critical roles will make use of a coprocessor for cryptographic operations. The coprocessor is a specially developed unit of the IC that implements highly optimised arithmetic functions, such as modular multiplication and modular exponentiation, in support of public key cryptography. The coprocessor will typically have its own registers (large enough to make processing the target key lengths efficient), which will be mapped to areas of the IC volatile memories. It will also tend to use much higher internal clock speeds than the CPU. The coprocessor operates separately from the CPU, being passed data (or pointers), set into operation, and then returning its result.

20 Security is a pervasive issue for smartcards, and security properties are found at many levels in both hardware and software. However, there will typically be some specific security functionality implemented in the hardware. Such functionality may include:

- sensors of various sorts,
- memory area separation,
- security data support,
- noise generation,
- security interrupts (to enable integrity checks during operation).

1.1.2.1 Memories

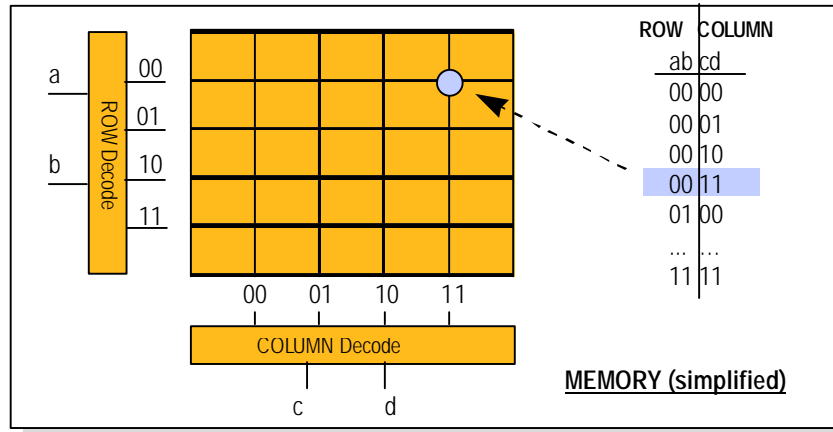


Fig. 1.2 - Generic Memory Schematic

**ROM**

21 ROM has the following features:

- Programmed by mask at factory,
- Read only in use,
- Smallest cell size of the various memory types (usually 1 transistor per cell),
- Typically the OS is stored here and sometimes application code.

**Volatile Memories**

22 Volatile Memories has the following features:

- Volatile, data is lost when power is removed,
- Read / write in use,
- Largest cell size of the various memory types (usually 6 transistors per cell),
- High speed memory for storing temporary data e.g. during calculations.

**Non Volatile Memories**

23 Non-Volatile Memories has the following features:

- Non-volatile, data is not lost when power is removed,
- Read / write in use,
- Medium cell size (usually 2 transistors per cell),
- Degrades with use (typically 100,000 to 1Million write/erase cycles),
- Finite lifetime (typically contains OS dynamic data, application code and application dynamic data).

## CPU

### **CPU operation (simplified):**

- *decode instruction, address*
- *fetch data*
- *perform calculation*
- *store result*
- *step to next instruction*

*Fig. 1.3 - CPU basic instruction set*

24 The CPU executes the instructions contained in the OS, and may have characteristics as follows:

- CISC / RISC,
- 8 bit / 16 bit / 32 bit data / address / instruction bus,
- Instruction set (including coprocessor),
- Clock speed,
- Memory management (e.g. restricted access).

## 1.2 TOE evaluation boundaries

### 1.2.1 Smartcard lifecycle

25 The Figure 1.4 shows a typical lifecycle for a smartcard.

26 By clearly defining the different phases of the lifecycle, an IC manufacturer can identify the assets at risk, and the threats to those assets, that are associated with each phase.

27 The phases of the lifecycle that are within the scope of the evaluation need to be clearly specified as this delineates the opening boundary of the evaluation. Evaluation will need to encompass:

- Manufacture and pre-issue processes for the TOE,
- TOE environment,
- TOE authorized use within each environment,
- TOE available operational modes within each environment,
- TOE authorized users within each environment.

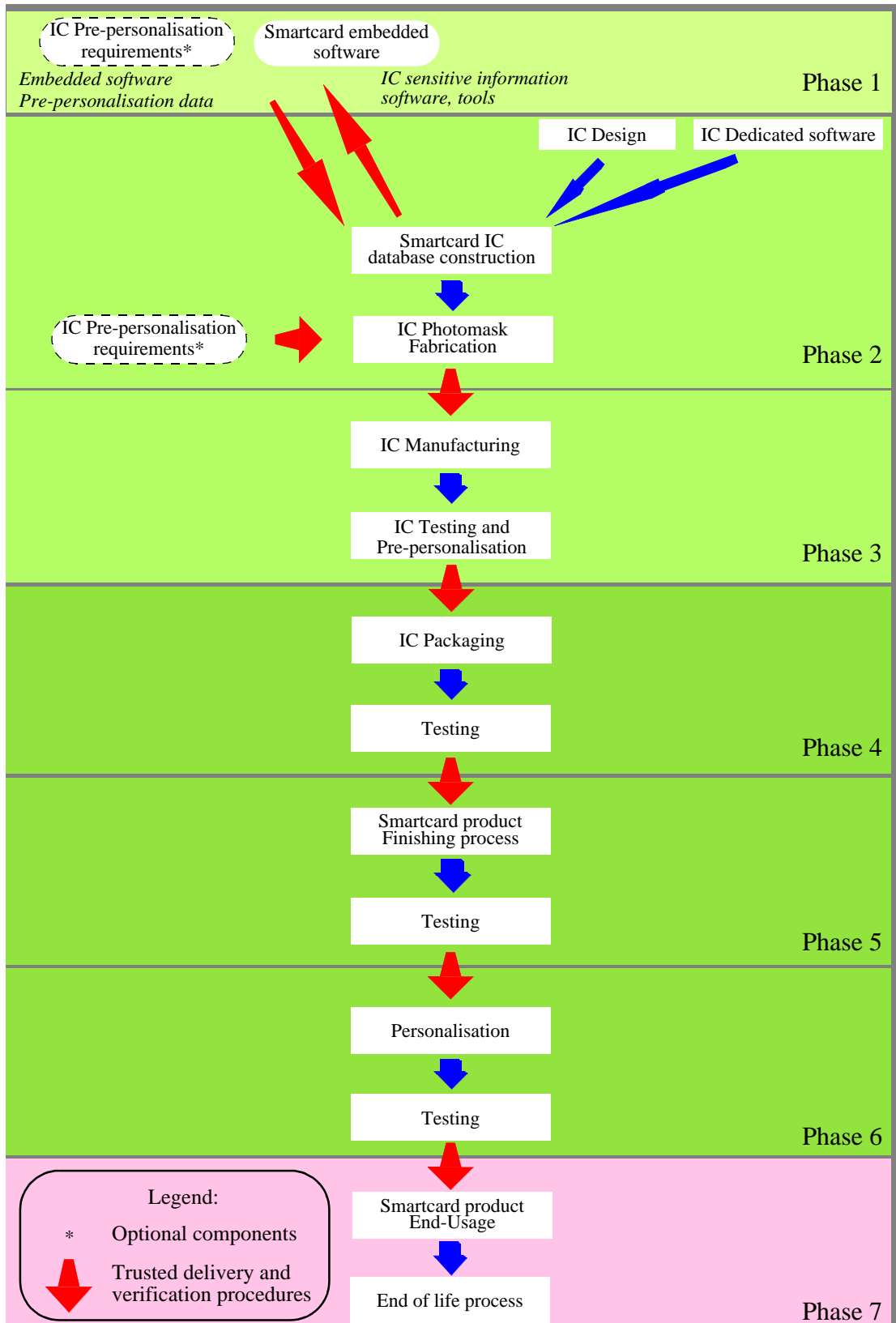


Fig. 1.4 - Typical smartcard product life-cycle

### 1.2.2 Phase 1: Smartcard embedded software development

28 The smartcard embedded software (OS and application code where this is written in the microprocessor's native language) will be typically developed using tools supplied by the IC designer. The development of the smartcard embedded software is beyond the scope of this document.

29 The transfer of the smartcard embedded software (to be embedded into the IC) to the IC designer is performed through a trusted delivery. The format of information to be transferred, and the manner of its transfer, will need to be specified by the IC designer (See "The Application of CC to Integrated Circuits").

### 1.2.3 Phase 2: IC development

30 The IC designer will design the IC using tools which may include the following:

- Schematic / Logic design tools,
- Simulation tools,
- Layout / Post layout simulation tools,
- Design verification tools,
- Test tools.

31 The IC designer also develops IC dedicated software, provides information, software or tools to the smartcard embedded software developer.

32 The IC designer receives the smartcard embedded software from the developer, through a trusted delivery. From the IC design, IC dedicated software and smartcard embedded software, the designer constructs the smartcard IC database, necessary for the IC photomask fabrication.

33 Photomasks are then generated from the verified IC database at the photomask manufacturer site and return to the IC manufacturer through a trusted delivery procedure.

### 1.2.4 Phase 3: IC manufacturing

34 The IC manufacture will take place in a semiconductor wafer fabrication plant and test facility.

35 Inputs to this process are the base silicon wafers, chemicals, materials used in production, and the set of photomasks.

36 Manufacturing includes:

- Fabrication of the ICs, including the smartcard embedded software,
- Testing of the IC (at wafer level),
- (Typically) the injection of certain pre-personalisation data.

37 Outputs from the manufacturing phase are the ICs themselves, and any rejects or scrap material.

38 Data, photomasks and pre-personalisation data used during manufacture will have secure storage and usage implications.

### 1.2.5 Phases 4,5: ICC production

39 The ICC is produced at a card manufacturing facility. From the beginning of this stage, the integrity and any confidentiality required of the IC should be demonstrable. This stage may include the following:

- Incorporation of wafer die into a module (IC packaging),
- Bonding the die to its contact plate,
- Embedding the module in an epoxy resin coat,
- Testing of the module,
- Incorporation of module into the plastic card body.

### 1.2.6 Phase 6: ICC personalisation

40 The final step necessary to prepare the ICC for issue to users consists of personalisation of ICC (though there may be other steps required to deliver applications and customisation data to end users, and indeed these steps may be allowed many times during the end-user phase of the ICC).

### 1.2.7 Phase 7: End-user

41 The end-user phase is defined as the phase where the ICC, and therefore the IC, will be issued to end-users for operational deployment.

42 The end-user phase contains also the end of life process of the ICC, which is a critical aspect in the life-cycle of a smartcard.

## 2 Scope of evaluation

43 An ITSEC/CC evaluation is performed against a document known as the Security Target (ST). The ST defines precisely what is to be evaluated - referred to as the Target of Evaluation (TOE). The ST will also define the scope of the evaluation, both in terms of the physical description and the environment of use during its life-cycle, including the processes by which the product is developed, manufactured and used. The limits of the evaluation in terms of life-cycle (Phases 1 to 7) shall be explicitly addressed in the ST.

44 The hardware evaluation methodology documented here can be applied to the following aspects which may be within the scope of the hardware evaluation:

- Secure use and distribution of smartcard embedded software development tools,
- Delivery of the smartcard embedded software to the IC designer,
- Delivery and processing of pre-personalisation data,
- Design of the IC, including the development of IC dedicated software,
- Generation of the IC database (including smartcard embedded software),
- Fabrication of IC photomasks,
- IC Manufacturing,
- ICC Production,
- ICC Personalisation,
- ICC during its end use.

45 Whilst in principle it is possible to evaluate the IC on its own, in practice this is unlikely. Any usable IC will also have software involved at one or more levels (e.g. Kernel, Operating System, Application). As a minimum, enough software will be required to test the IC against its ST. It may also be the case that some threats (e.g. data leakage via power traces) relevant to the IC can only be countered by a combination of hardware and software. The following evaluation scenarios are thus more likely:

- The TOE is limited to the IC plus a minimal software kernel,
- The IC is evaluated in the context of the evaluation of a composite TOE which takes into account the security of the various components that comprise it (e.g. application, OS and hardware).

- 46 Where the IC is treated as a distinct entity, the evaluation provides separable and reusable results that can be used within the context of subsequent composite TOE evaluations. It is expected that the IC designer will inform the smartcard embedded software developer of all assumptions or dependencies which need to be upheld in order to design and build a secure product, e.g. by means of a security interface document (guidance documents).
- 47 The evaluators of subsequent composite TOE evaluations will need to have access to detailed results of the IC evaluation in order to validate the effectiveness of the security requirements which are implemented by a combination of hardware and software. Moreover, where the IC is being evaluated in the context of a composite TOE evaluation, it is necessary for the ST for the composite TOE to clearly define the separation between the various components, and the dependencies between them. It needs to be clear which functionality required of the composite TOE are implemented by the software components, and which (if any) are implemented by the IC.

## 3 Threat model

48 At each phase in the life-cycle, consideration must be given to the threats to which the IC will be subjected.

49 Threats have been related to the phases of the smartcard life-cycle (and delivery between phases) as described above:

- Smartcard embedded software phase (Delivery to IC designer),
- IC development phase including photomasks fabrication,
- IC manufacturing phase,
- ICC production phase,
- ICC personalisation phase,
- End-user phase.

50 Threats must be characterised by identifying:

- Assets at risk (e.g. keys and other secret data, code, design materials, physical form of the TOE),
- Threat agents,
- Attack methods used.

51 The assets generally have both confidentiality and integrity concerns (including in some cases data authenticity).

### 3.1 Categorisation of threats

52 All threats described below must be addressed by the TOE or its environment (or some combination thereof). The following should be noted:

- An ITSEC ST must clearly distinguish between those threats that are countered by the TOE (possibly with support from its environment), and those that are addressed wholly by countermeasures within the environment;
- CC does not require such a distinction to be made in the ST (although this may be helpful); however, it should be clear from the definition of security objectives the extent to which the TOE counters the threats.

53 Threats that are to be countered wholly by measures taken within the environment are termed **Environmental** threats in this document.

54 Threats that are to be countered wholly or in part by the TOE are categorised as **TOE** threats.

## 3.2 Phase 1: Smartcard embedded software delivery

### 3.2.1 Assets

55 The main asset to be protected in this phase is the smartcard embedded software, the confidentiality and integrity of which needs to be ensured.

### 3.2.2 Environmental threats

56 Software to be embedded within the IC could be tampered with. Subversive software could be inserted with the aim of either creating denial-of-service or destroying smartcard confidentiality or integrity features.

57 As smartcard embedded software development is out of the scope of this document, the embedded software is only considered as being vulnerable when it is delivered from the embedded software developer to the IC designer.

58 Smartcard embedded software developer will usually be given design tools (e.g. simulator and/or emulator) with which to facilitate software design. In the wrong hands, software or hardware development tools could be subsequently used to mount an attack on the operational smartcard or be used in some way to produce clones.

59 Accountability of development tools within the development or manufacturing environments is therefore required, for example where such tools could be used within the manufacturing environment to examine unfinished chips without that examination being detected.

## 3.3 Phase 2: IC development

### 3.3.1 Assets

60 The main assets to be protected in this phase are the IC design, test materials, and processing masks, the confidentiality and integrity of which need to be ensured.

### 3.3.2 Environmental threats

61 IC design material may be stolen from the various development environments. Alternatively, tampering with the design may arise. Sensitive material will relate to:

- Logic development (schematics, logic plans, design simulation),
- Layout development (layout plans, mask data),
- Test development (test tools, test vectors, including those used in production test).

62 The processing masks are vulnerable at the following stages in their development:

- Design and maintenance (i.e. by the mask developer. [The IC manufacturer may subcontract this work]).

- Creation and storage of the image and /or data.
- Delivery to IC manufacturer.

### **3.4 Phase 3: IC manufacturing**

#### **3.4.1 Assets**

63 The main assets to be protected in this phase are the IC design, test materials, processing masks, security critical data (including pre-personalisation data and cryptographic keys), and the ICs themselves (which may be in a vulnerable state), the confidentiality and integrity of which need to be ensured.

#### **3.4.2 Environmental threats**

64 Data or information about the IC's design, processing masks, or the ICs themselves (or failure parts), may be stolen from the manufacturing environment.

65 Tests analysis data, tests results and security critical data (e.g. pre-personalisation data, cryptographic keys) may be stolen, or interfered with.

66 ICs may be vulnerable to attack during delivery to the ICC Production Environment, e.g. substitution of cloned or Trojan Horse ICs into the delivery channel.

#### **3.4.3 TOE threats**

67 There may be unauthorised use or modification of ICs within the manufacturing and testing environment, e.g. to inject ICs with weak keys, or to gain access to cryptographic keys in the pre-personalisation data.

68 ICs may be cloned in order to develop further attacks.

### **3.5 Phases 4,5: ICC production**

#### **3.5.1 Assets**

69 The main assets to be protected in this phase are IC design details (e.g. through reverse engineering), security critical data (including pre-personalisation data and cryptographic keys), and the ICs themselves (which may be in a vulnerable state), the confidentiality and integrity of which need to be ensured.

#### **3.5.2 Environmental threats**

70 In the ICC production phase, ICs will typically be in an early personalised state. In this case the ability to download subversive software should be reduced. However if devices can be stolen, then they may be more readily subjected to tampering attacks as in the end-user phase.

71 ICs may be stolen from the various production environments. Alternatively, tampering with the design may arise. Sensitive material will relate to:

- Test methods (test tools, test vectors).
- Pre-personalisation data.
- Other security critical data such as cryptographic keys.

72 ICs may be cloned in order to develop further attacks, typically through reuse of rejected chips or cards.

73 The ICC may also be vulnerable whilst being delivered to the personalisation environment.

### 3.5.3 TOE threats

74 There may be unauthorised use or modification of ICs within the production environment, e.g. by injecting ICs with weak keys, or gaining access to cryptographic keys in the pre-personalisation data.

## 3.6 Phase 6: ICC personalisation

### 3.6.1 Assets

75 The main assets to be protected in this phase are IC design details (e.g. through reverse engineering), security critical data (including personalisation data and cryptographic keys), and the ICs themselves (which may be in a vulnerable state), the confidentiality and integrity of which need to be ensured.

### 3.6.2 Environmental threats

76 In the ICC personalisation phase, personalisation data will be loaded in ICs.

77 ICs may be stolen from the personalisation environment. Alternatively, tampering with the design may arise. Sensitive material will relate to:

- Test methods (test tools, test vectors),
- Personalisation data,
- Other security critical data such as cryptographic keys.

78 ICs may be cloned in order to develop further attacks, typically through reuse of rejected chips or cards.

79 ICs may also be vulnerable whilst being delivered from the ICC personalisation environment to the end-user environment.

### 3.6.3 TOE threats

80 There may be unauthorised use or modification of ICs within the personalisation environment, e.g. by loading ICs with erroneous personalisation data, or by gaining access to cryptographic keys.

## 3.7 Phase 7: End-user

### 3.7.1 Assets

81 The main assets to be protected in this phase are the details of the IC design (e.g. through reverse engineering), and security critical data (including personalisation data and cryptographic keys), the confidentiality and integrity of which needs to be ensured.

### 3.7.2 TOE Threats

82 During its operational life, the ICC and therefore the IC is less strictly controlled than in the manufacturing environment and hence more susceptible to physical threats. The following potential physical attacks should be considered during IC design:

- Inducement of failures,
- Inferring secret information from timing, voltage or processing activity.

83 Physical threats may be mounted against the card during its operational life. These threats are often described as tampering resistance. They may comprise one or other of the following, or suitable combinations thereof, they could even be combined with DPA or DFA threats:

- Forcing operation outside of defined specification envelopes (e.g. temperature, voltage, frequency),
- Subjecting devices to external energy fields or focused beams,
- Ageing inducement,
- Re-enablement of test functionality,
- Reverse engineering, e.g. to extract memory contents, or to identify structures on the chip (thereby facilitating subsequent attacks such as cloning, probing, reversion to test mode or defeating sensors).

84 Note that the above lists of threats are not intended to be exhaustive. Potential threat methods will depend on techniques developed over time and the specific properties of the IC being evaluated.



## 4 Security objectives

85 Security objectives for smartcards cover the need to protect data critical to the security of the smartcard, whether stored on-card or off-card, thereby ensuring that the identified threats to the assets are adequately countered.

86 Security plans (i.e. security policy and security measures needed to uphold the policy) must be developed to cover design, manufacture, production and personalisation stages and consideration given to the likely threats which may be mounted during the ICC's operational life.

87 Procedures must exist to control sales, distribution, storage and usage of software and hardware development tools and confidential documents that might have a bearing on the IC's confidentiality or integrity.

88 The ICC shall be designed, built and evaluated to withstand the threat posed by attackers with expertise, resources and opportunities commensurate with the minimum strength of mechanism claim for ITSEC and vulnerability assessment for CC, using the tables described in chapter 7.

89 For ITSEC, the trusted delivery channels shall be commensurate with the defined level of assurance, as stated in [ITSEC-JIL] chapter 10.

### 4.1 Phase 1: Smartcard embedded software delivery

90 The principal security objective for this phase is to protect the integrity, (including authenticity) and (where appropriate) confidentiality of the embedded software.

91 The IC developer's security plan should cover the interface with the smartcard embedded software development system. This plan shall describe personnel, physical and procedural security measures for ensuring the trusted delivery of the embedded software to the IC design environment, i.e. without loss of integrity (including authenticity) and (where appropriate) confidentiality. Procedures must be adhered to and personnel must understand their significance and implementation requirements.

### 4.2 Phase 2: IC development

92 The principal security objective for this phase is to protect the confidentiality and integrity of the IC design.

93 The IC developer's Security Plan shall describe personnel, physical and procedural security measures for ensuring that the development environment be secure. Procedures must be adhered to and personnel must understand their significance and implementation requirements.

- 94 Access to the site shall be restricted to authorised personnel. The status of personnel should always be identifiable whilst on site (e.g. by the wearing of passes), and visitors and maintenance people should be escorted. Site security shall always be enforced, possibly via a combination of alarms, security personnel and surveillance cameras.
- 95 Access shall be controlled to computer systems, development tools and databases where the confidentiality or integrity of the IC design might otherwise be put at risk. Access control should be based on a positive process that limits access to a definite and recognisable group (e.g. a list of names, or by membership of an identifiable organisational group).
- 96 Sensitive documents, database backups, diskettes and IC layout information shall be stored in secure physical containers.
- 97 Satisfactory disposal procedures shall be in place. These shall ensure (as a minimum) that there is accountability of disposed materials (to a level sufficient to show that individual dies are accounted for), and that confidential material is destroyed in such a way that confidentiality is not breached.
- 98 Any additional sites delegated work (e.g. sites used to generate photomasks) shall be subject to an equivalent level of physical security and the work items afforded appropriate accountability and secure transportation between sites.
- 99 Development modifications shall not occur in an unauthorised manner.
- 100 Sensitive data (e.g. IC dedicated software) must not be subject to disclosure or unauthorised change.
- 101 Trusted delivery to the IC Manufacturing Environment shall be used.

### 4.3 Phase 3: IC manufacturing

- 102 The principal security objectives for this phase are to:
- protect the integrity and (where appropriate) confidentiality of design and test materials,
  - protect the integrity and (where appropriate) confidentiality software,
  - protect the confidentiality and integrity of pre-personalisation data, and other sensitive data (e.g. cryptographic keys),
  - prevent unauthorised access to ICs,
  - prevent unauthorised access to test software design, test facilities and test scripts.
- 103 Similar environmental controls shall therefore exist to those expressed for the previous two phases.
- 104 Accountability for each wafer shall be enforced by production control systems, and appropriate procedures.

105 The site of any testing and programming done off-site shall be afforded a level of physical security equivalent to that of the main manufacturing environment. Transportation delivery between sites shall be assured.

106 Trusted delivery to the ICC production environment shall be used.

#### 4.4 Phases 4,5: ICC production

107 The principal security objectives for this phase are to:

- protect the integrity and (where appropriate) confidentiality of design and test materials and software,
- protect the confidentiality and integrity of pre-personalisation data, and other sensitive data (e.g. cryptographic keys),
- prevent unauthorised access to ICs.

108 Similar environmental controls to the previous phases shall therefore be used.

109 Accountability for all ICs and cards shall be enforced by production control systems, and appropriate procedures. Those ICs and cards which are rejected shall be destroyed to a level of rigour which ensures that no reusable parts remain.

110 Trusted delivery to the personalisation environment shall be used.

#### 4.5 Phase 6: ICC personalisation

111 The principal security objectives for this phase are to:

- protect the integrity and (where appropriate) confidentiality of design and test materials and software,
- protect the confidentiality and integrity of personalisation data, and other sensitive data (e.g. cryptographic keys),
- prevent unauthorised access to ICs.

112 Similar environmental controls to the previous phases shall therefore be used.

113 Accountability for all cards shall be enforced by production control systems, and appropriate procedures. Those cards which are rejected shall be destroyed to a level of rigour which ensures that no reusable parts remain.

114 Trusted delivery to the end-user environment shall be used (unless the TOE can by this stage authenticate itself to the end-user).

## 4.6 Phase 7: End-user

115 The principal security objectives for this phase are to:

- protect the integrity and authenticity of the IC,
- protect the integrity and (where appropriate) confidentiality of software,
- protect the confidentiality and integrity of sensitive data, e.g. cryptographic keys.

116 The ICC shall be able to demonstrate its authenticity.

117 Modifications while in operational deployment shall not occur in an unauthorised manner.

## 5 Vulnerability model

118 It is important to be realistic about the analysis of smartcard devices; it is likely be impossible to design a smartcard that could withstand a highly skilled attacker with infinite resource, time and motivation.

119 Threats to the ICC arise from three fundamental areas:

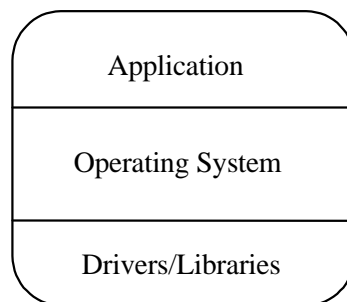
- *import of subversive material* - execution of subversive or invalid application code, or use of subversive data;
- *imperfect processing* - the IC may be induced, by invasive or non-invasive means, to perform outside of its specification;
- *Unauthorized access* - reading or altering the content of stored data in unauthorized ways.

120 These are described in more detail in the subsections that follow.

121 When considering requirements for physical security, it is important to look not only at the protection of the raw IC product itself, but also to provide mechanisms that can be used by programmers to provide integrated protection of an application (“application” in this sense includes both operating systems and user applications).

### 5.1 Import of subversive material

122 The basic IC package will generally require an operating system to make it useable. Therefore consider the following three layers of software:



123 In principle, any of these three layers might have components which are loaded into Non Volatile Memories (NVM) and which are therefore vulnerable to:

- substitution of subversive code (or data),
- deliberate/accidental corruption in a manner which also represents a security threat.

- 124 Applications, especially for multi-application cards, can be expected to reside mostly in NVM. The operating system is likely to be largely resident in ROM, but may have NVM components. Even the basic library might have loadable components to allow a more flexible offering on a basic silicon design.
- 125 Loading components which have been altered could have various effects that compromise security, such as
- directly revealing the contents of memory areas (e.g. by providing an unconstrained memory dump instruction),
  - providing indirect signaling (e.g. by accentuating use of critical features such as an NVM write), or producing corruptions in critical locations (e.g. the balance of an electronic purse).
- 126 Subversive code could be used to deliberately alter code, leading to additional knowledge of certain applications. This way, more sophisticated attacks could be mounted. For example, virus-like code which identifies the presence of an electronic purse application, locates its balance or other critical data, and alters it, using knowledge of the application's own protection mechanisms to make this undetectable.
- 127 This is addressed by a combination of developers' security, delivery and configuration assessment, and functionality (e.g. for load functionality). Such aspects may need to be supported by hardware features (e.g. to protect keys). Also this area is likely to be closely related to application and operating system properties - hence there is a requirement to demonstrate hardware support for application or operating system TOEs.

## 5.2 Imperfect Processing

- 128 When any hardware operates in an environment which is outside of its specification, it may execute imperfectly. This may have unexpected effects on security in simple or complex ways. The environment may be influenced by accident, or deliberately and the effects may be predictable or non-deterministic.
- 129 This area is mainly linked with hardware features (e.g. the physical, environmental envelope, or environmental exchange). Ultimately, the effects of imperfect processing are to cause or assist unauthorised access or else to assist in breaking a TOE (e.g. an application's PIN mechanism).

## 5.3 Unauthorised Access

- 130 Unauthorised access covers the possibility of an attacker either reading or manipulating code or data on an IC and in doing so revealing its content, processes and architecture.

131 The resources, ingenuity and competency of the attacker should not be underestimated. Even “strong” designs may be compromised eventually. And in an organized attack, the hacker can be assumed to have:

- adequate supply of functional IC cards,
- appropriate test equipment,
- an attack methodology,
- skills and knowledge to apply attack methodology.

## 5.4 Vulnerability characterisation

132 The sections below take the original threats above and discuss them further in terms of vulnerabilities. Often similar effects can result from more than one of the different threat/vulnerability groupings (e.g. unauthorised access to memory contents might be gained by: loading subversive code; exploiting imperfect processing by inducing corruption in the program counter; imaging of memory cells; by reconstituting a fuse giving access to test mode). No attempt is made to avoid this overlap - it is instead considered as a useful element of redundancy in the analysis.

### 5.4.1 Import of subversive material

133 Subversive data may be placed in any known storage sites (e.g. memory or registers). In the case of Volatile and Non-Volatile Memories, there is assumed to be a loading process carried out by the IC using functionality provided by the mask.

#### 5.4.1.1 Smartcard embedded software mask

134 The smartcard embedded software mask is vulnerable at various stages in its development:

- design (i.e. by the mask developer),
- creation and storage of the image (i.e. database) by the developer,
- transfer of image between developer and manufacturer,
- storage of image by the manufacturer,
- creation of masks from image.

135 At any of these points, an attacker might attempt to change the content of the mask, or corruption might be introduced.

#### 5.4.1.2 Externally loaded data

136 There may be various types and stages of loading (e.g. loading of operating system components or initialisation data or personalisation and enablement), and loading

of applications and application customisation or configuration data. Concerns arising here are:

- data loaded from a malicious or unreliable source,
- data claiming to be from an approved source but actually supplied by an unreliable source,
- loading of data that has been tampered with or corrupted.

137 However, there may also be security-critical data such as secret keys included in the loaded data, and this gives rise to a further vulnerability:

- confidential parts of loaded data revealed to an attacker.

#### 5.4.2 Imperfect Processing

138 Vulnerabilities associated with imperfect processing may arise from any deviation from specification. Most commonly, the effects might be arbitrary corruption of the contents of memory, registers or buses. A more general view of the threat is the possibility of causing insecure transitions in the IC state. This may include execution of code outside of program structures (e.g. executing data, or executing in instruction space but without respect to intended instruction boundaries).

139 In general, it is impossible to guarantee that deviations from specification will not occur, either accidentally or by an attacker deliberately taking an IC outside its intended operating envelope. In particular, vulnerabilities may arise from varying:

- temperature,
- voltage and current,

140 or applying:

- various types of electromagnetic radiation, ranging from radio waves to x-rays,
- magnetic fields of various orientations and frequencies,

141 or simply from:

- removing power at critical points in processing.

142 The questions raised for a particular IC will relate not only to the effects that these conditions may have on the general execution of programs, but also to effects on critical structures (e.g. in more general terms the existence of “security bits” that could be reset).

### 5.4.3 Unauthorized Access

143 Unauthorized access to the contents of the IC includes a wide range of possible vulnerabilities, with a number of possible categorisations. The fundamental danger is that:

- confidential data might be read, inferred or deduced,
- critical data might be modified.

144 Both of these vulnerabilities may arise from the previous vulnerability types, but also in a number of other ways:

- inspection of memory structures,
- indirect modification of bus, register or memory cell contents (by invasive or non-invasive effects),
- inference from surface scanning (e.g. optical inspection),
- inference from interface scanning,
- direct reading,
- direct writing,
- access to test mode functionality.

145 There is an additional vulnerability category that may be used to assist exploitation of other vulnerabilities, namely the alteration of structures on the IC itself (e.g. reconstituting fuses or adding connections).

146 A physical attack can be direct or indirect, destructive or non-destructive.

147 Direct attacks result in some physical alteration to the chip whereas indirect attacks do not. Though an indirect attack does not physically alter the IC, it can be used to discover the structure of the IC or to read memory contents. Either method may be used to manipulate memory or data.

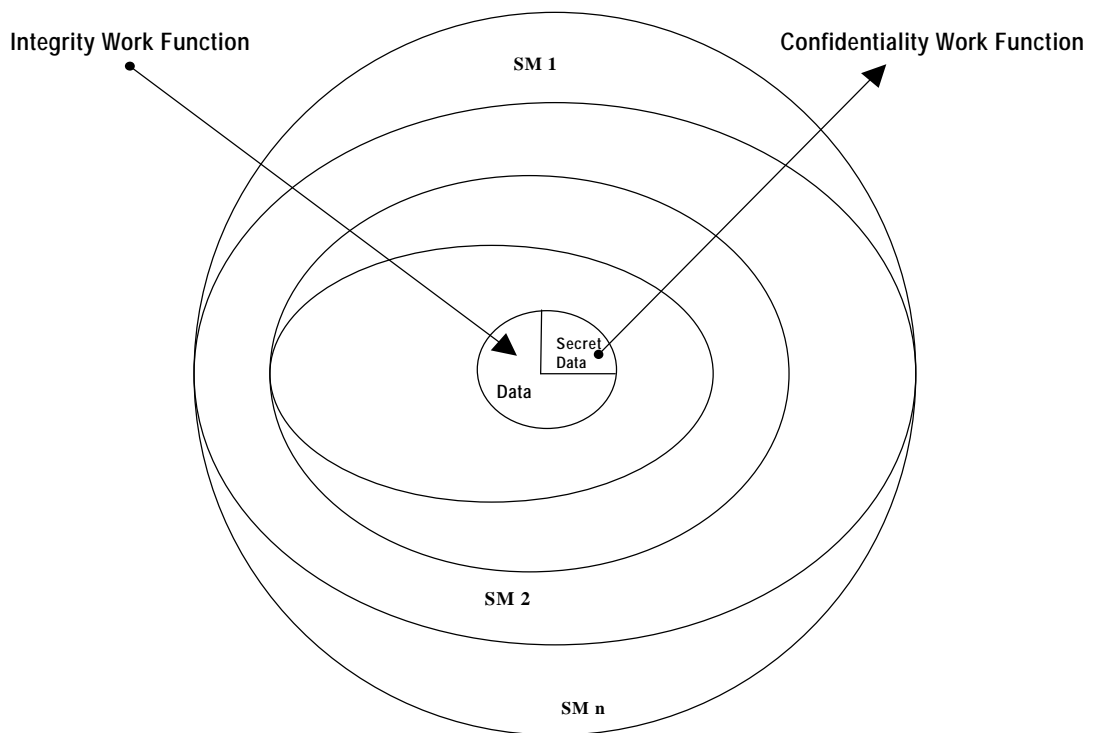


## 6 Test model

148 One of the basic precepts in using a smartcard is that the chip offers adequate tamper resistance. The construction of tamper resistant modules is a well-known concept in the design of security systems and has been modelled by the use of barriers offering passive and dynamic resistance to attack.

149 The smartcard IC is used in an environment where the stability and accuracy of external signals are questionable. The IC is exposed directly to all external events with no intermediation by way of filters, power-on reset circuitry or clock shaping which are familiar to designers of traditional embedded microprocessor systems. Moreover, it is very difficult to avoid or monitor any abuse to the smartcard IC.

150 Faced with such a harsh environment, careful consideration needs to be paid when designing all external interfaces to the chip. In particular, the IC should be viewed as presenting a set of security mechanisms that offer protection of the security relevant elements of the TOE.



*Fig. 6.1 - Evaluation approach.*

151 Figure 6.1 depicts a set of security mechanisms protecting some data.

152 At this level the security mechanism is still an abstract concept; for example, a security mechanism may be physical or logical. However, a security mechanism

should be viewed as a means of classifying a TOE claim to ensure that the approach to testing the security mechanism is consistent, irrespective of the ITSEF used.

153 Using this approach, the integrity of (or probability of compromising) the security mechanism is itself a security requirement.

154 The objective of this chapter is to describe, a generalised model that provides an extendable strategy to testing a hardware TOE based upon available knowledge and identified security mechanism. For example, a hardware security mechanism might be protective coating, or a cunningly devised layout. A coating is a type of physical security mechanism. At present there are a number of ways such a security mechanism might be attacked and these define the tests to be applied. As new attacks emerge, these can be translated into additional tests.

## 6.1 Security Mechanism Testing Model

155 An abstract model is introduced here to provide a framework for testing a smartcard security mechanism claim. In this section the abstract model is expressed in more concrete terms, based upon the current perceived status of smartcard technology. As such technology advances, the model can readily be updated to reflect the changes in knowledge, skills and resources that will inevitably result.

156 Each security mechanism (SM) defines a set of properties. If one or more of these properties are not in evidence, this will manifest itself in the corresponding test result and, inevitably, in the final security function.

157 Denote by  $\{SM_i: i=1,2,..m\}$  the total set of identified security mechanism classifications. It is unlikely that  $m$  will ever be large as there are a limited set of physical properties which an ICC can manifest.

158 Each  $SM_i$  defines a test model based on an analysis of the security mechanism into less abstract characteristics based on attack methods. As new classes of attack emerge - due to advancing technology and knowledge - these hierarchies may be extended. However, it is unlikely that the depth of such a model will exceed 4 levels before a suitable testing level emerges.

159 The lowest level is defined to be where attacks can be realised. It is at this level that any testing is to be applied.

160 The resulting model is a tree-structure with hierarchical and branching relationships. The tests are defined at the end - nodes.  $SM_i$  denotes the security mechanism type and the  $A_{i...s}$  denote attack classes.

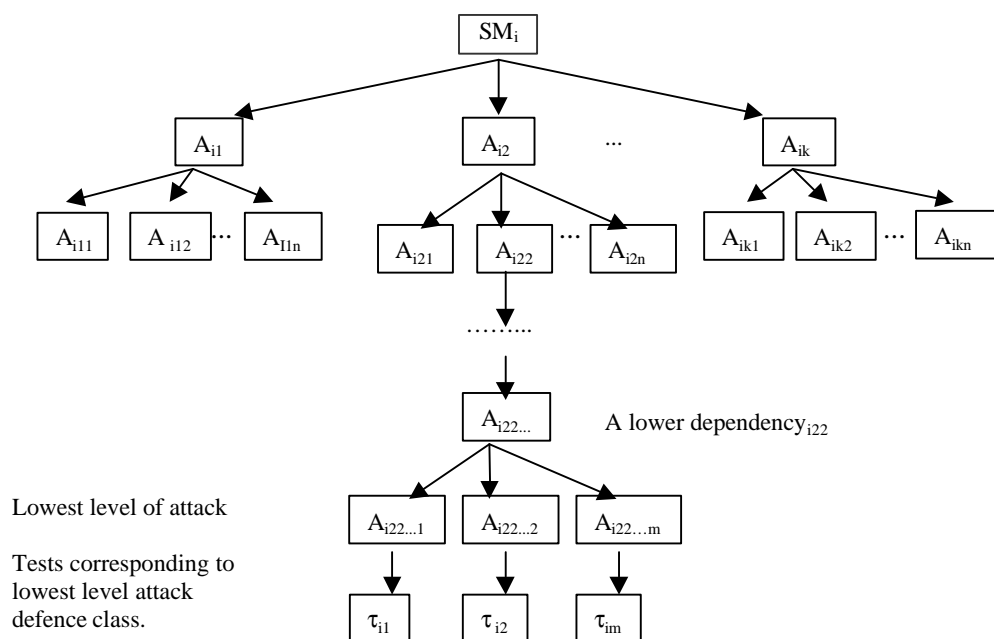


Fig. 6.2 - Test Model corresponding to  $SM_i$ .

161 Note that  $\tau_{ij}$  may define a number of tests to address a particular class of attack at this lowest level. Tests are not described in the following sections.

## 6.2 Classification of Security Mechanism

162 Currently, there are four main security mechanism types:

- Physical
- Data Storage Cell
- Environmental Exchange
- Leakage

163 Specific properties of such security mechanism are described in more detail in the subsections that follow. These are not intended to be exhaustive lists. A TOE security mechanism claim may have properties which are not listed in any of the classifications below but which still afford some protection. For this reason, the test models described below are completely generic.

## 6.3 Physical Security Mechanism

164 A Physical Security Mechanism prevents an attacker from accessing the processing, connection buses and memory storage elements of the IC. Fundamentally, the

breach of such a mechanism enables assessment of the physical layout of the IC, to facilitate probing and microscopy. Once some structure has been established it is possible to monitor processing on-chip or access memory content, destructive or otherwise.

165 Various coatings may be applied at different stages in the fabrication process to thwart an attack (e.g. by preventing scanning). Coatings may be added as part of a normal process, (e.g. metal or oxide layers), or specifically to prevent invasive ingress.

166 Coatings are applied to hinder access to data buses and/or memory cells to:

- read data,
- write data,
- manipulate the IC communication lines to invoke different operating modes.

167 Such coatings may be designed to make removal difficult without damaging the functionality of the device.

168 Such layers may be passive in as much as they are difficult to remove, or active in that they create some form of change to the underlying surfaces or enable a sensor to be invoked when any attempt at removal is made. Such sensors may detect optical or electrical changes of state in the barrier.

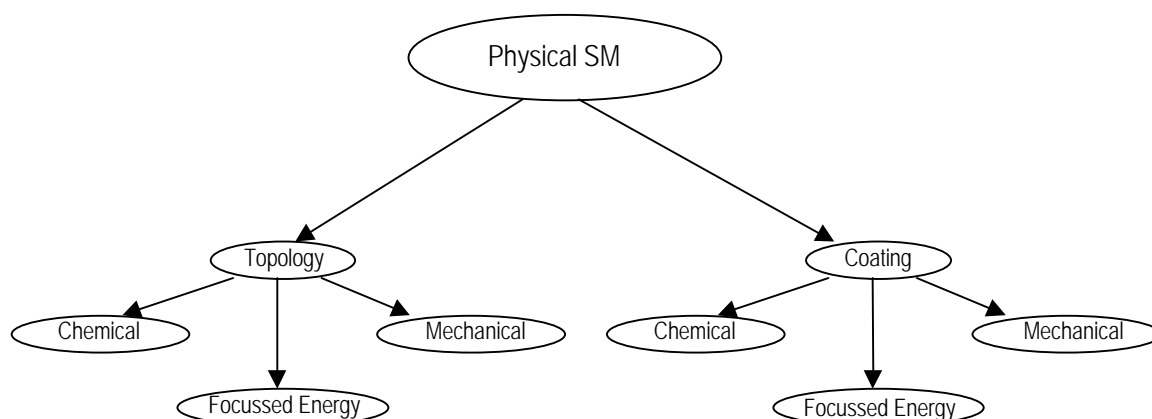
### 6.3.1 Properties

169 The security mechanism may comprise a number of properties relating to the coating material and the IC construction.

- It should be difficult for any attack to discover the architectural layout of the chip so that it is difficult to exploit the various probing and microsurgery techniques.
- Materials used in attaching the IC to the contact foil and for covering the bonded IC should be resistant to removal by chemical or applied energy methods. Ideally, any attempt at removal should cause sufficient damage to the die that it becomes inoperative or unrecognisable.
- The IC should be designed with tightly integrated components and smaller structures, to hinder material removal. Ideally, any such removal should destroy the underlying structural layout.
- The IC layout should not permit easy access to protected areas via more open areas.
- Interconnections between functional blocks, such as the processor and memory, should be protected.

- An advanced process technology is recommended to maximise the protection to programs and data that is offered by a tightly integrated structure.
- The IC should prevent access to any critical access control logic to stop any potential regression to a test mode state. Ideally, any manipulation of a critical access control logic should destroy the underlying critical structure.

### 6.3.2 Test Model



#### Topology/Coating

170 If a physical security mechanism forms an active part of the circuitry it is classified as a *topological* defence. Naturally, this also includes the layout of the interconnection circuitry between functional blocks. A design may also deliberately mask the circuitry by use of, say, random logic. Various forms of coating may be applied that are resistant to chemical, mechanical and focussed energy attacks.

#### Resistance

171 The resistance of any topology/coating of the TOE is subject to three attack types:

*Chemical* - application of chemical solvents (e.g. fuming nitric acid).

*Focused Energy* - application of heat, electromagnetic radiation, sound.

*Mechanical* - grinding, cutting, lapping, drilling or similar.

## 6.4 Data Storage Cell Security Mechanism

172 The data storage cell security mechanism refers to the resistance that the ICC presents to active and passive probing when the chip is in a static state (not operating) and a dynamic state (operating in its normal environmental envelope). It is assumed that attacks against the data storage cell security mechanism relate only

to the difficulty of measuring such charge and not to the difficulty of gaining access to the circuitry, which is a property of the physical security mechanism.

173

Attacks against the data storage cell security mechanism are either galvanic (direct electrical ohmic contact using probes) or are effected by imaging the storage state directly or indirectly (with an electro-magnetic radiation (EMR) beam of any wavelength). It is also possible to excite the various chip elements with EMR and then probe to deduce the relevant charge state.

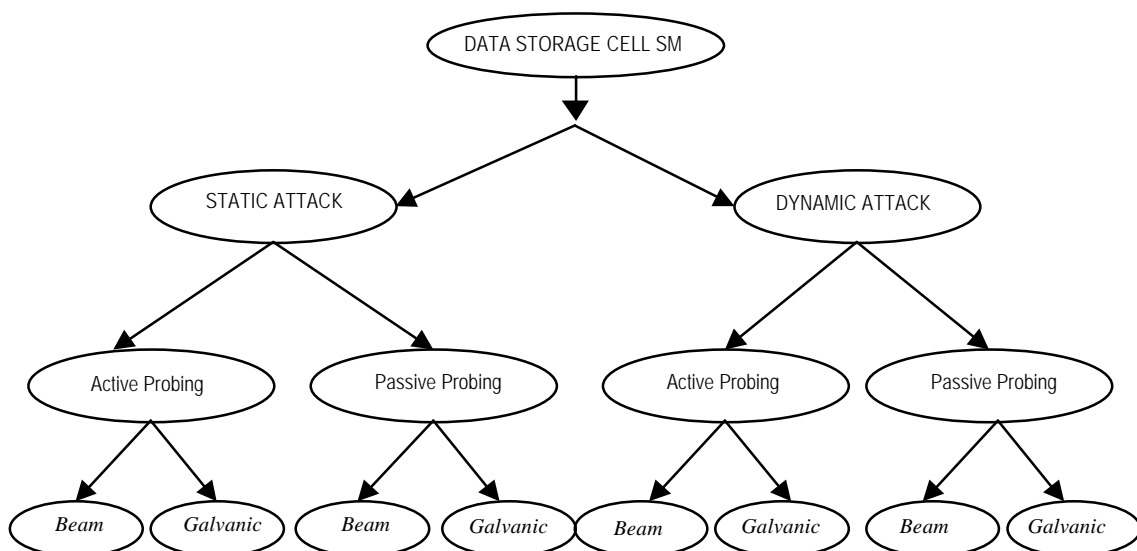
### 6.4.1 Properties

174

Based on the security policy, the following properties can be stated:

- It must not be feasible to determine the layout of the memory in terms of the physical addresses.
- It must not be feasible to read or modify any sensitive working data from the volatile memory at any stage of the IC's life during general usage or by manipulation of power or environmental factors.
- It must not be feasible to read or modify any sensitive data from the ROM area at any stage of the IC's life during general usage or by manipulation of power or environmental factors.
- It must not be feasible to read or modify any sensitive working data from the non-volatile memory at any stage of the IC's life during general usage or by manipulation of power or environmental factors.

### 6.4.2 Test Model



### Static/Dynamic Attacks

*Static attack* - TOE is not operating.

*Dynamic attack* - TOE is operating.

### Probing

*Active probing* - deliberate alteration of TOE state.

*Passive probing* - TOE state not altered (or probes have minimal impact upon data being investigated).

### Probe type

*Galvanic* - use of direct electrical ohmic contact to derive measurements.

*Beam* - any form of visualisation direct or indirect due to the emission of EMR at any measurable wavelength.

## 6.5 Environmental Exchange Security Mechanism

175 The ICC's environmental exchange security mechanism is designed to protect the chip against changes in the environment that will take the ICC out of its normal operating mode. If this security mechanism can be broken, then the chip will malfunction, resulting in the unusual processing of data or the corruption of stored data.

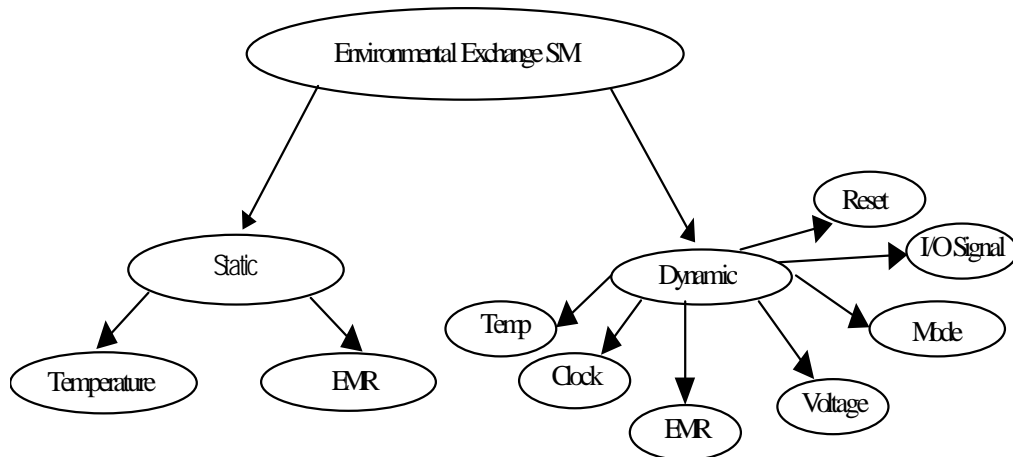
176 This security mechanism is defined to be active in that it must detect an unusual mode of operation and either:

- Correct the malfunction, or
- Shut down in a 'fail safe' mode.

### 6.5.1 Properties

- IC should operate normally under the entire range of "normal" temperatures (see ISO 7816), electrical current, and voltages, providing a set of sensors that can detect the appropriate abnormal state. Out-of-specification inputs should not pose a security threat.
- Logic design should cater for poor signals and supplies.
- IC may protect against single bit manipulations which can be used to reveal secret information.
- IC may protect against single bit errors.
- IC may be protected from being into an unauthorised mode of operation.

### 6.5.2 Test Model



## 6.6 Leakage Security Mechanism

177 The TOE is presented as a “black box” in this model. The object is to characterise the emanations from the TOE under a varying set of environmental conditions and determine how these may be exploited, (e.g. synchronisation of signals for repeated measurements), characteristic power traces resulting from different ICC operations, timings for processing, (e.g. coprocessor, if present).

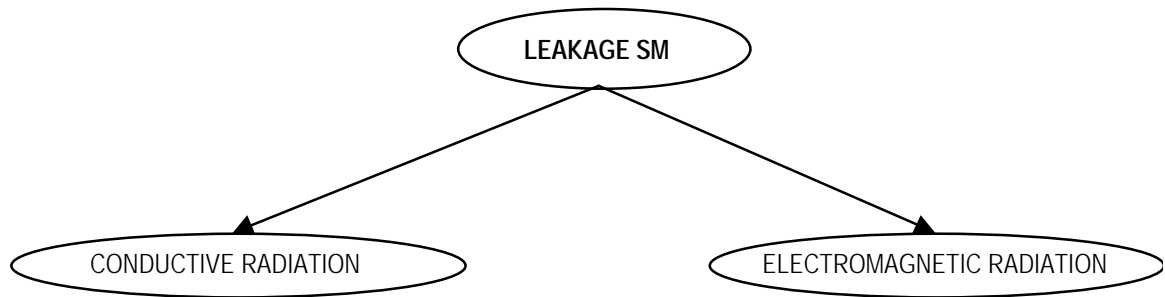
178 The ICC must protect against “emitted radiation” and “timing” attacks or deter utilisation of “clock” and “power” signals for monitoring or process manipulation. For example, constant or uncorrelatable power and timing references over the external contacts would be desirable.

### 6.6.1 Properties

179 The IC should ensure that it is difficult to characterise the operation of the chip or to determine sensitive data from any combination of:

- measurable timing information
- measurable current consumption
- measurable emitted electro-magnetic radiation.

6.6.2 Test Model





## 7 Calculating attack potential

### 7.1 Introduction

180 This chapter provides guidance metrics to calculate attack potential required by an attacker to effect an attack. The underlying objective is to aid in expressing the total effort required to mount a successful attack. This should be applied to operational behaviour of a smartcard and not to applications specific only to hardware or software.

181 For ITSEC “Strength of Mechanisms” analysis as well as for CC “Vulnerability Assessment” analysis, the evaluator determines the minimum attack potential required by an attacker to effect an attack and to arrive at some conclusion about the TOE’s resistance to attacks.

182 In order to simplify the calculating of attack potential, levels 1, 2 and 3 are introduced. The levels are used to refer to the concepts of “Strength of Mechanisms” (SoM), “Vulnerability Assessment” (VLA) and “Strength of Functions” (SoF). When CC evaluation is chosen, it is proposed that the levels described should be used as an interpretation of the VLA and SoF components, so that levels 1, 2 and 3 should provide protection against attacker with low, moderate and high attack potential and basic, medium and high SoF respectively. When ITSEC evaluation is chosen, the levels 1, 2 and 3 should be used as an interpretation of basic, medium and high SoM. Table 1 summarises these correspondences.

<b>Table 1: SoF, Attack potential and SoM</b>			
	<b>Common Criteria</b>		<b>ITSEC</b>
<b>Levels</b>	<b>Attack potential</b>	<b>SoF rating</b>	<b>SoM rating</b>
<b>Level 1</b>	<b>Low (VLA.2)</b>	<b>SoF-basic</b>	<b>SoM-basic</b>
<b>Level 2</b>	<b>Moderate (VLA.3)</b>	<b>SoF-medium</b>	<b>SoM-medium</b>
<b>Level 3</b>	<b>High (VLA.4)</b>	<b>SoF-high</b>	<b>SoM-high</b>

### 7.2 Calculating attack potential to effect an attack

183 The evaluator may determine the attack potential required to successfully effect an attack using the tables defined hereafter.

184 This calculation is based on the definition of different factors which are expertise, equipment, collusion and time. These factors are described in the following sections.

### 7.2.1 Expertise

185 Three levels of expertise are defined:

- layman,
- proficient,
- expert.

186 “Layman” is interpreted as someone without any particular technical skills with which to mount an attack on the TOE. For instance, the end-user of the Smartcard (card holder).

187 “Proficient” is interpreted as someone who knows electronics and is able to use general-purpose electronics equipment such as oscilloscopes, pattern generators or measure test benches.

188 “Expert” is interpreted as someone who has the capability to understand internal structures of the integrated circuit and also to use high-level sophisticated equipment such as Focused Ion Beam and Scanning Electronical Microscopes.

### 7.2.2 Equipment

189 Three levels of equipment are defined:

- without any equipment,
- with domestic equipment,
- with specialist equipment.

190 In the context of Smartcard Integrated Circuits, the definition of “without any equipment” makes no sense, since it is necessary in order to use the smartcard to have at least minimal equipment, such as a card reader or personal computer.

191 When considering equipment at the disposal of attackers, the availability of equipment is very important: some equipment is freely available in the public domain; other equipment can be cheaply rented. The “ease of use” of equipment should also be considered, since it is necessary to have appropriate expertise in the equipment in order to use it to good affect.

192 In this context, three types of equipment are defined:

- type 1 - Domestic Equipment: personal computers, card readers, pattern generators, optical microscopes...
- type 2 - Dedicated Equipment: dedicated electronic cards, specialised test bench (e.g. non-public domain equipment).

- type 3 - Sophisticated Equipment: Focused Ion Beam, Scanning Electronical Microscope.

193 With the advent of public-domain knowledge, it may be necessary to downgrade equipment over time.

### 7.2.3 Collusion (Available knowledge)

194 In the context of smartcard integrated circuits, available knowledge has to be considered. This could either be in the public-domain or confidential in nature; it could directly concern the TOE (e.g. internal structures of the Integrated Circuit) or relate to specific avenues of attack.

195 This knowledge may be obtained directly by collusion, or may be recovered by reverse engineering starting from a zero knowledge base. The relevant reverse engineering should require effort comparable to that required to complete the attack.

196 Consequently, three levels of collusion which provide opportunities to attackers, must be considered:

- Public-Domain Information: all the information, whether it be on design and manufacturing of the TOE or attacks opportunities, is freely available.
- Developer Information: detailed information, not publicly available, on the internal structures of the TOE, equivalent to the level information owned by the developer; this could be via collusion with the developer or with a person who has the same level of information.
- Developer and Administrator Information: information from both developer and administrator sources. This is information added by one of the parties involved in the smartcard application security management, such as embedders, personaliser, system integrator, system manager etc.

### 7.2.4 Time

197 Time spent by an attacker to realize an attack includes:

- study time, if the information for the attack is not in the public domain, as recognized to be applicable by JIL Chapter 6, 6.4.1.,
- time for attack.

198 The amount of time to be considered is the sum of the two time parameters above; it is expressed in minutes, hours, days, months and years.

7.2.5 Calculating attack potential

199

Add together the two numbers found by looking up Time and Collusion factors in Table 3 and by looking up Expertise and Equipment factors in Table 4. The final result is given in Table 5.

<b>Table 3: Time/Collusion COLLUSION</b>			
<b>TIME</b>	<b>public</b>	<b>with developer</b>	<b>with developer and administrator</b>
<b>in minutes</b>	<b>0</b>	<b>3</b>	<b>6</b>
<b>in hours</b>	<b>1</b>	<b>6</b>	<b>8</b>
<b>in days</b>	<b>2</b>	<b>8</b>	<b>10</b>
<b>in months</b>	<b>6</b>	<b>10</b>	<b>16</b>
<b>in years</b>	<b>10</b>	<b>16</b>	<b>20</b>

<b>Table 4: Expertise/Equipment EQUIPMENT</b>			
<b>EXPERTISE</b>	<b>Domestic</b>	<b>Dedicated</b>	<b>Sophisticated</b>
<b>Layman</b>	<b>1</b>	<b>Not applicable</b>	<b>Not applicable</b>
<b>Proficient</b>	<b>3</b>	<b>3</b>	<b>Not applicable</b>
<b>Expert</b>	<b>4</b>	<b>6</b>	<b>10</b>

200

To implement an effective attack, it may be necessary to subvert a succession of different mechanisms (on an “attack path”). The intention is to estimate the minimum effort required for a successful attack. Therefore the sums of the individual effort estimates along the weakest attack path should be used in table 5.

201

<b>Table 5: Calculated attack potential</b>	
<b>Result</b>	<b>Level</b>
<b>1 -&gt; 5</b>	<b>Fail</b>
<b>6 -&gt; 11</b>	<b>Level 1</b>
<b>12 -&gt; 24</b>	<b>Level 2</b>
<b>25 -&gt;</b>	<b>Level 3</b>

202

The above tables should be used as guidance only.



## Annex A Typical IC Manufacturing Process Description

### A.1 Background

203 The process of manufacturing semiconductors, or integrated circuits (commonly called ICs, or chips) typically consists of up to a hundred processing stages, during which several hundred identical copies of an integrated circuit are formed on a single wafer.

204 Generally, the process involves the creation of around 25 patterned layers on and into the substrate (or surface of the wafer), ultimately forming the complete integrated circuit. This layering process creates electrically active regions in and on the semiconductor wafer surface.

205 These electrically active regions form transistors - the building blocks used to form memory cells and also logic gates which in turn can be combined to form circuit functions like Arithmetic & Logic Units (ALU's). These are the basis for the CPU of a Microcontroller as used in the Smartcard.

206 Making semiconductors is not easy and is not cheap. Current facilities operating with 200mm wafer diameter and 0.35-0.25 $\mu\text{m}$  linewidths cost between \$1bn & \$2bn. It is estimated that to build and fully equip the next generation wafer fab utilising 300mm wafers will cost close to \$3bn. And completion of building and commissioning can take upwards of 20 months.

207 The focus for this next generation wafer fab is always decreasing geometry size. However, experts claim the gains to be had from larger wafer sizes and better yields are decreasing and the focus is now on making equipment with higher throughput, better reliability and shorter set-up times, combined with better factory management software packages to co-ordinate workflow.

208 Current geometries of 0.25 $\mu\text{m}$  minimum feature size and chip sizes of up to 400mm<sup>2</sup> are state of the art. Smart Card devices are somewhat more conservative using trusted, well-tested processes at 0.5 $\mu\text{m}$ , and for mechanical reasons chip sizes below 25mm<sup>2</sup>.

### A.2 Production of Wafers

209 The first step in semiconductor manufacturing begins with production of a wafer-a thin, round slice of a semiconductor material, usually silicon.

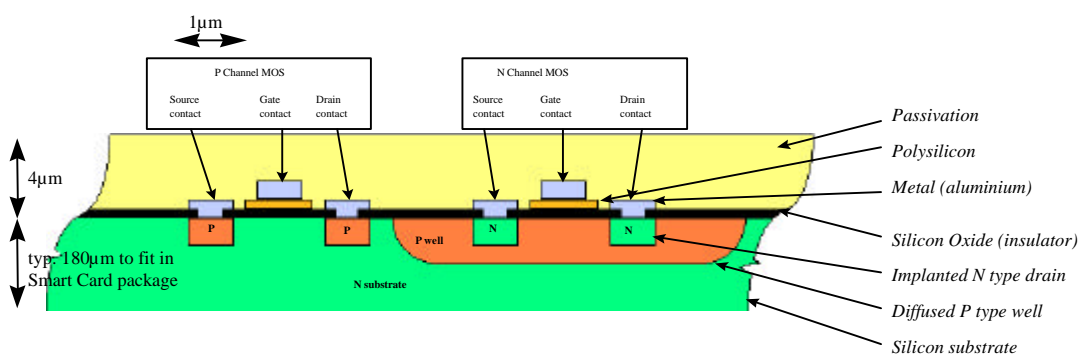
210 In this process, purified polycrystalline silicon, created from sand, is heated to a molten liquid. A small piece of solid silicon (seed) is placed into the top of the molten liquid, and as the seed is slowly pulled from the melt the liquid cools to form a single crystal ingot. The surface tension between the seed and molten silicon causes a small amount of the liquid to rise with the seed and cool.

- 211 The crystal ingot is then ground to a uniform diameter and a diamond saw blade cuts the ingot into thin wafers.
- 212 The wafer is processed through a series of machines, where it is ground smooth and chemically polished to a mirror-like finish.
- 213 The wafers are then ready to be sent to the wafer fabrication area where they are used as the starting material for manufacturing integrated circuits.
- 214 Current state of the art for wafer diameter is 170 to 200mm (6 to 8 inch), but research is ongoing to produce 300mm (12 inch) wafers.

**A.3 Inside the Wafer Fabrication Facility**

- 215 The heart of semiconductor manufacturing is the wafer fabrication facility where the integrated circuit is formed in and on the wafer. The fabrication process, which takes place in a clean room, involves a series of principal steps as described below.
- 216 Typically it takes from 30 to 40 days to complete the fabrication process, however with factory loading and scheduling (this is a batch process) typical commercial lead-times can be 12 to 16 weeks. Typically a wafer fab will have around 20,000 wafer starts per month.
- 217 Wafers typically travel around the fab in batches or lots of 25 to 50 wafers. The trend is for less and less human handling of the product. A batch of wafers can easily be worth \$1M in end user value.

**A.3.1 Schematic of a Cross section through a generic CMOS technology**



**A.3.2 Oxidation or Oxide Deposition**

- 218 Wafers are pre-cleaned using high purity, low particle chemicals (important for high-yield products). The silicon wafers are heated and exposed to ultra-pure oxygen in the diffusion furnaces under carefully controlled conditions forming a silicon dioxide film of uniform thickness on the surface of the wafer.

219 This process is carried out at high temperature, around 1000 deg.C. The oxide thickness is proportional to the time exposed.

### A.3.3 Masking

220 Masking is used to protect one area of the wafer while working on another. This process is referred to as photolithography or photo-masking.

221 A photoresist or light-sensitive film is applied to the wafer, giving it characteristics similar to a piece of photographic paper. This is usually applied in liquid form to the surface of the wafer whilst it is being spun at high speed, thus ensuring an even coating.

222 A photographic aligner then aligns the wafer to a mask and then projects an intense light through the mask and through a series of reducing lenses, exposing the photoresist with the mask pattern. This process is commonly carried out for a small block of IC's at a time, and not the whole wafer in one go. The aligner thus 'steps' across the wafer until all IC's are complete. These machines are referred to as steppers.

223 Precise alignment of the wafer to the mask prior to exposure is critical. Most alignment tools are fully automatic, and expensive.

224 Currently lithography usually uses UV light to project onto the wafer, but as smaller geometries are realised, the wavelength of the light starts to compromise the accuracy of the process. As such, lithography is the technique most under scrutiny to push increasing transistor count or density on a wafer. Current initiatives underway are looking at using Extreme Ultraviolet light to progress under 0.15  $\mu\text{m}$ , or X Ray. Whilst other techniques include the use of electron or particle beam write techniques. These suffer usually from the time it takes to write a pattern, a single device at a time.

### A.3.4 Etching

225 The wafer is then "developed" (i.e. the exposed photoresist is removed). It is then exposed to a chemical solution or plasma (ionised gas discharge). The exposed areas of resist soften upon exposure, and are therefore more etched away.

226 Decreasing feature size has here relied on advances in the etching process. Chemical etching of selective areas has evolved to plasma etching where a reactive gas is used.

227 The remaining photoresist is removed using additional chemicals or plasma and the wafer is inspected to ensure the image transfer from the mask to the top layer is correct.

### A.3.5 Implantation (or diffusion)

228 Atoms with one less electron than silicon (such as boron), or one more electron than silicon (such as phosphorous), are introduced into the area exposed by the etch

process to alter the electrical characteristics of the silicon. These areas are called P-type (boron) or N-type (phosphorous) to reflect their electrical properties.

229 This process is now commonly carried out using Ion Implantation. In some cases however, diffusion is used. A gas mixture containing the appropriate chemicals is allowed to flow over the exposed chip surface. The particles activated by high temperature diffuse into the silicon. Again as feature sizes reduce and more accuracy in definition is required, implantation is preferred. In this process, ions of boron or phosphorous are accelerated by a high voltage into a beam targeted at the chip surface. They become implanted in the surface resulting in the P or N type region required to produce a transistor.

### A.3.6 Repeating the steps

230 The oxidation, masking, etching and implantation steps are repeated several times until the last layer is formed. At this stage all the active elements are complete.

### A.3.7 Dielectric deposition and metallisation

231 Following completion of the above steps the individual transistors on each chip are interconnected using a series of metal depositions and dielectric (insulator) depositions. This process requires a further series of patterning steps to define the routing of metal tracks.

232 The deposition of metal, usually aluminium is carried out by a process called sputtering. Here positive charged ions of the inert gas Argon are accelerated at an Aluminium target, the displaced atoms of Aluminium are thus sputtered onto the wafer surface. The aluminium coated wafer is then masked and etched similar to earlier steps to define the tracking of interconnection lines between circuits.

233 The dielectric layer can be grown using a process called Chemical Vapour Deposition (CVD). Gases are selectively mixed and in a controlled chemical reaction induce a thin film to grow on the surface of the silicon. For example nitride layers  $\text{Si}_3\text{N}_4$  are grown by passing  $\text{SiH}_2\text{Cl}_2$  and  $\text{NH}_3$  gases over the surface. Dopants can also be introduced during these processes. This is a variant of the oxidation process, where the gas used is Oxygen.

234 Current smartcard semiconductor fabrication includes typically two or three metal layers separated by dielectric layers.

### A.3.8 Passivation

235 After the last metal layer is patterned, several final layers can be deposited to protect the circuit from damage and contamination. These are often oxides or nitrides. Some manufacturers choose a special coating like a polyimide. This is called the passivation layer.

236 Finally, openings are etched in this layer to allow access to the top layer of metal by electrical probes (for testing) and wire bonds (for packaging). These connection areas are called bond pads.

### A.3.9 Backgrinding

237 As a final process before being assembled into micromodules, the thickness of the wafer is reduced. The wafer is inverted and using a combination of chemical etching and mechanical lapping is ground down to a thickness of 180µm typically. This allows the wafer to attain some degree of flexibility whilst adding to the ease with which it can be mounted in the micromodule.

### A.4 Electrical test

238 An automatic, computer-driven electrical test system then checks the functionality of each chip on the wafer. Chips that do not pass the test are marked with ink for rejection.

239 Test timing is critical. It needs to be as short as possible whilst giving the maximum assurance that the device is fully functional.

### A.5 Packaging

240 A diamond saw typically slices the wafer into single chips. The inked chips are discarded and securely destroyed by crushing the silicon (which can then be recycled), and the remaining chips are visually inspected under a microscope before packaging.

241 The chip is then assembled into a module that provides the contact leads for the chip. A wire-bonding machine then attaches wires to the leads of the package.

242 Encapsulated with a plastic coating for protection, usually some compound of Epoxy Resin, the chip is tested again (though the testing is now considerably less rigorous).



## Annex B Glossary of Terms

ABS	Acrylonitrile-butadiene-styrol
CAD	Computer Aided Design.
Card	Generic ICC
CC	Common Criteria
CEM	Common Evaluation Methodology
Chip	Integrated Circuit (IC)
CISC	Complex Instruction Set Computer
CLK	Clock
CPU	Central Processing Unit
DFA	Differential Fault Analysis. The running of the IC in a hostile environment (e.g. strong electric field) to induce errors in cryptographic calculations.
DPA	Differential Power Analysis. The measurement of current drawn by the IC during cryptographic operation, which can then be used to infer computational paths taken by the algorithm, and hence secrets being operated on
E Beam	The Beam used in a Scanning Electron Microscope
EEPROM	Electrically Erasable Programmable Read Only Memory
EMV	Europay - Mastercard - Visa
ETR	Evaluation Technical Report
FIB	Focused Ion Beam
GSM	Global System for Mobile Telecommunications, a popular mobile phone standard (formerly Group Special Mobile)
HDL	Hardware Description Language
IC	Integrated Circuit
ICC	Integrated Circuit Card or Smartcard
ID 00	An ICC physical format used in GSM Cards

ID 01	An ICC physical format used in Bank Cards
ISO	International Organisation for Standardization
ITSEC	Information Technology Security Evaluation Criteria.
ITSEM	Information Technology Security Evaluation Manual
OS	Operating System
PC	Polycarbonate
PET	Polyethylene terephthalate
PVC	Polyvinyl chloride
RAM	Random Access Memory
RISC	Reduced Instruction Set Computer
RNG	Random Number Generator
ROM	Read Only Memory
SEF	Security Enforcing Function (ITSEC term)
SFR	Security Functional Requirement (CC term)
Smartcard	Integrated Circuit Card (ICC)
SM	Security Mechanisms
SOF	Strength of Function (CC term)
SOM	Strength of Mechanisms (ITSEC term)
ST	Security Target
TOE	Target of Evaluation
UV	Ultra Violet

