SECURE DEVICES, 2022

Mirosław Kutyłowski

COMMON CRITERIA FRAMEWORK

http://www.commoncriteriaportal.org

Book: Using the Common Criteria for IT Security Evaluation, Debra S. Herrmann

Problem: somebody has to deploy a secure IT system, how to purchase it?

- problematic requirements according to BSI guide:

  i. **incomplete** – forgetting some threats is common

  ii. **not embedded:** not corresponding really to the environment where the product has to be deployed

  iii. **implicit:** customer has in mind but the developer might be unaware of them

  iv. **not testable**: ambiguous, source of legal disputes, ...

  v. **too detailed:** unnecessary details make it harder to adjust the design

  vi. **unspecified meaning:** e.g. "*protect privacy*"

vii. **inconsistent:** e.g. ignoring trade-offs

- *specification-based purchasing process* versus *selection-based purchasing process*
- the user is not capable of determining the properties of the product himself: too complicated, too specialized knowledge required, a single error makes the product useless
- specifications of concrete products might be useless for the customers – hard to understand and compare the products
- informal specifications and descriptions, no access to crucial data

Idea of Common Criteria Framework:

- standardize the process of
  - designing requirements (Protection Profile –PP) (done from customer's point of view, but concerns a concrete product)
  - designing products (Security Target – ST), (done from developer's point of view, specific decisions how to meet PP)
  - evaluation of products (licensed labs checking conformance of implementation with the documentation) (certification body)

- international agreement of bodies from some countries (USA, France, UK, Germany, India, Turkey, Sweden, Spain, Australia, Canada, Malaysia, Netherlands, Korea, New Zeland, Italy, Turkey) many countries “consuming’
- idea: ease the process, reuse work, build from standard components
- typically ST as a response for PP:
  - more detailed
  - maybe chooses some concrete options
  - maybe fulfills more requirements (fulfills many PPs)
  - a relation to PP should be testable

Value:

- **CC certification does not mean a product is secure**
- it only says that is has been developed according to PP
- assurance level concerns only the stated requirements, e.g. trivial requirements ⇒ high EAL level (common mistake: EAL level ... without specifying PP)
- but it is cleaning up the chaos of different assumptions, descriptions, ...

Example:

the Estonian personal ID card,

Infineon chip with CC certificates issued by BSI,

faulty implementation of RSA key generation (on the chip), cryptoanalytic attack by people from Brno Masaryk University – a secret key could be derived from the public key

CC certificates has not been challenged – they are still valid while all RSA keys had to be revoked

Example for PP: BAC (Basic Access Control)

- used to secure wireless communication between a reader and an e-Passport (of an old generation)
- encryption primitive

$$\mathrm{EM}(K, S) = \mathrm{Enc}(\mathrm{KB}_{\mathrm{Enc}}, S) \| \mathrm{MAC}(\mathrm{KB}_{\mathrm{Mac}}, \mathrm{Enc}(\mathrm{KB}_{\mathrm{Enc}}, S), S)$$

where the key K is $(\mathrm{KB}_{\mathrm{Enc}}, \mathrm{KB}_{\mathrm{Mac}})$

- steps:
  1. The MRTD chip sends a nonce $r_{\mathrm{PI}\mathbb{C}C}$ to the terminal
  2. The terminal sends the encrypted challenge
     $$e_{\mathrm{PCD}} = \mathrm{EM}(K, r_{\mathrm{PCD}}, r_{\mathrm{PI}\mathbb{C}C}, K_{\mathrm{PCD}})$$
     to the MRTD chip, where $r_{\mathrm{PI}\mathbb{C}C}$ is the MRTD chip's nonce, r_{PCD} is the terminal's randomly chosen nonce, and K_{PCD} is keying material for the generation of the session keys.
  3. The MRTD chip decrypts and verifies $r_{\mathrm{PI}\mathbb{C}C}$, responds with
     $$e_{\mathrm{PICC}} = \mathrm{EM}(K, r_{\mathrm{PICC}}, r_{\mathrm{PCD}}, K_{\mathrm{PICC}})$$
  4. The terminal decrypts and verifies r_{PCD}
  5. both sides derive $K_{\mathrm{Enc}}, K_{\mathrm{Mac}}$ from the master key
     $$K_{\mathrm{PICC}}\,\mathrm{XOR}\,K_{\mathrm{PCD}}$$
     and a sequence number derived from the random nonces (key derivation function)
- ***K*** **derived from information available on the machine readable zone (optical reader applied, not available via wireless connection)**
- implementation: biometric passports.
- a simple system. Really?

Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Basic Access Control BSI-CC-PP-0055

1. Introduction

`this section aimed for customers looking for proper products, overview`

1.1 PP reference

`basic data, registration data`

Title: Protection Profile - Machine Readable Travel Document with ICAO Application and Basic Access Control (MRTD-PP)

Sponsor: Bundesamt für Sicherheit in der Informationstechnik CC Version: 3.1 (Revision 2)

Assurance Level: The minimum assurance level for this PP is EAL4 augmented.

General Status: Final

Version Number: 1.10

Registration: BSI-CC-PP-0055

Keywords: ICAO, machine readable travel document, basic access control

1.2 TOE Overview

"is aimed at potential consumers who are looking through lists of evaluated TOEs/Products to find TOEs that may meet their security needs, and are supported by their hardware, software and firmware"

preamble (a kind of abstract):

The protection profile defines the security objectives and requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organization (ICAO). It addresses the advanced security methods Basic Access Control in the 'ICAO Doc 9303' [6].

This part is challenging: how to describe a complicated product in a few words and avoid misunderstandings?

TOE definition (Target of Evaluation, the scope of PP)

which parts, which general purpose, which functionalities are present and which are missing,

e.g. ATM card with no contactless payments, a disk encryption software,

The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readabletravel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to 'ICAO Doc 9303' [6].

The TOE comprises at least

- *the circuitry of the MRTD's chip (the integrated circuit, IC)*
- *the IC Dedicated Software with the parts IC Dedicated Test Software and IC DedicatedSupport Software,*
- *the IC Embedded Software (operating system),*
- *the MRTD application and*
- *the associated guidance documentation.*

Usage and security features

crucial properties of the system (high level) and security features from the point of view of the security effect and not how it is achieved

> *A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this protection profile contains (i) visual (eye readable) biographical data and portrait of the holder, (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and (iii) data elements on the MRTD's chip according to LDS for contactless machine reading. The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and (ii) optional biometrics using the reference data stored in the MRTD. The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.*

- A State or Organization issues MRTDs to be used by the holder for international travel.

- The traveler presents a MRTD to the inspection system to prove his or her identity.

- The MRTD in context of this protection profile contains (i) visual (eye readable) biographical data and portrait of the holder,

- (ii) a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and

- (iii) data elements on the MRTD's chip according to LDS for contactless machine reading.

- The authentication of the traveler is based on (i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and

- (ii) optional biometrics using the reference data stored in the MRTD.

- The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

Usage and security features (continued)

For this protection profile the MRTD is viewed as unit of

(a) the physical MRTD as travel document in form of paper, plastic and chip. It presents visual readable data including (but not limited to) personal data of the MRTD holder

(1)the biographical data on the biographical data page of the passport book,

(2)the printed data in the Machine-Readable Zone (MRZ) and

(3)the printed portrait.

(b) the logical MRTD as data of the MRTD holder stored according to the Logical DataStructure [6] as specified by ICAO on the contactless integrated circuit. It presents contactless readable data including (but not limited to) personal data of the MRTDholder

(1) the digital Machine Readable Zone Data (digital MRZ data, EF.DG1),

(2) the digitized portraits (EF.DG2),

(3) the optional biometric reference data of finger(s) (EF.DG3) or iris image(s)(EF.DG4 or both

(4) the other data according to LDS (EF.DG5 to EF.DG16) and

(5) the Document security object

The issuing State or Organization implements security features of the MRTD to maintain the authenticity and integrity of the MRTD and their data. The MRTD as the passport book and the MRTD's chip is uniquely identified by the Document Number.

The physical MRTD is protected by physical security measures (e.g. watermark on paper,security printing), logical (e.g. authentication keys of the MRTD's chip) and organizational security measures (e.g. control of materials, personalization procedures) [6]. These security measures include the binding of the MRTD's chip to the passport book.

The logical MRTD is protected in authenticity and integrity by a digital signature created by the document signer acting for the issuing State or Organization and the security features of the MRTD's chip.

The ICAO defines the baseline security methods Passive Authentication and the optionaladvanced security methods Basic Access Control to the logical MRTD, Active Authentication ofthe MRTD's chip, Extended Access Control to and the Data Encryption of additional sensitivebiometrics as optional security measure in the 'ICAO Doc 9303' [6]. The Passive Authentication Mechanism and the Data Encryption are performed completely and independently on the TOE by the TOE environment.

This protection profile addresses the protection of the logical MRTD (i) in integrity by write-only-once access control and by physical means, and (ii) in confidentiality by the Basic Access Control Mechanism. This protection profile does not address the Active Authentication and the Extended Access Control as optional security mechanisms.

Life cycle

the whole process from the very beginning (design) until a TOE death:

Phase 1 “Development”

Phase 2 “Manufacturing”

Phase 3 “Personalization of the MRTD”

Phase 4 “Operational Use”

Required non-TOE hardware/software/firmware:

other components that can be crucial for evaluation

e.g: one could require a special kind of hardware for reading the TOE.

this happens for instance in case of digital signatures where one can demand certified readers

2. Conformance Claim

- CC Conformance Claim: version of CC
- PP claim: other PP taken into account in a plug-and-play way
- Package claim: which EAL package level

EAL packages:

- The CC formalizes assurance into 6 categories (the so-called "assurance classes" which are further subdivided into 27 sub-categories (the so-called "assurance families"). In each assurance family, the CC allows grading of an evaluation with respect to that assurance family.
- 7 predefined ratings, called evaluation assurance levels or EALs. called EAL1 to EAL7, with EAL1 the lowest and EAL7 the highest
- Each EAL can be seen as an array of 27 numbers, one for each assurance family.
- EAL1 assigns a rating of 1 to 13 of the assurance families, and 0 to the other 14 assurance families,
- EAL2 assigns the rating 2 to 7 assurance families, the rating 1 to 11 assurance families, and 0 to the other 9 assurance families
- ...
- monotonic: EALn+1 gives at least the same assurance level as EALn in each assurance families

Levels

- EAL1: Functionally Tested:
  - correct operation, no serious threats
  - minimal effort from the manufacturer
- EAL2: Structurally Tested
  - delivery of design information and test results,
  - effort on the part of the developer than is consistent with good commercial practice.
- EAL3: Methodically Tested and Checked
  - maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.
  - developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.

- EAL4: Methodically Designed, Tested and Reviewed
  - maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources.
  - the highest level at which it is likely to be economically feasible to retrofit to an existing product line.
- EAL5: Semiformally Designed and Tested
- EAL6: Semiformally Verified Design and Tested
- EAL7: Formally Verified Design and Tested

assurance classes examples

→ development:

- ADV_ARC - 1 1 1 1 1 1 architecture requirements
- ADV_FSP 1 2 3 4 5 5 6 functional specifications
- ADV_IMP - - - 1 1 2 2 implementation representation
- ADV_INT - - - - 2 3 3 “is designed and structured such that the likelihood of flaws is reduced and that maintenance can be more readily performed without the introduction of flaws”
- ADV_SPM - - - - - 1 1 security policy modeling
- ADV_TDS - 1 2 3 4 5 6 TOE design

→ guidance documents

- AGD_OPE 1 1 1 1 1 1 1 Operational user guidance
- AGD_PRE 1 1 1 1 1 1 1 Preparative procedures

- life-cycle support
  - ALC_CMC 1 2 3 4 4 5 5 Configuration Management capabilities
  - ALC_CMS 1 2 3 4 5 5 5 Configuration Management scope
  - ALC_DEL - 1 1 1 1 1 1 Delivery
  - ALC_DVS - - 1 1 1 2 2 Development security
  - ALC_FLR - - - - - - - Flaw remediation (nothing defined for EAL, you are free to design properties and name them)
  - ALC_LCD - - 1 1 1 1 2 Life-cycle definition
  - ALC_TAT - - - 1 2 3 3 Tools and techniques

- security target evaluation
  - ASE_CCL 1 1 1 1 1 1 1 Conformance claims
  - ASE_ECD 1 1 1 1 1 1 1 Extended components definition
  - ASE_INT 1 1 1 1 1 1 1 ST introduction
  - ASE_OBJ 1 2 2 2 2 2 2 Security objectives
  - ASE_REQ 1 2 2 2 2 2 2 Security requirements
  - ASE_SPD - 1 1 1 1 1 1 Security problem definition
  - ASE_TSS - 1 1 1 1 1 1 TOE summary specification
- tests
  - ATE_COV - 1 2 2 2 3 3 Coverage
  - ATE_DPT - - 1 1 3 3 4 Depth
  - ATE_FUN - 1 1 1 1 2 2 Functional tests
  - ATE_IND 1 2 2 2 2 2 3 Independent testing
- vulnerability assesment
  - AVA_VAN 1 2 2 3 4 5 5 Vulnerability analysis

for example, a product could score in the assurance family developer test coverage (ATE_COV):

- 0: It is not known whether the developer has performed tests on the product;
- 1: The developer has performed some tests on some interfaces of the product;
- 2: The developer has performed some tests on all interfaces of the product;
- 3: The developer has performed a very large amount of tests on all interfaces of the product

example more formal: ALC_FLR

ALC_FLR.1:

- *The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.*
- *The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.*
- *The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.*
- *The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.*

- ALC_FLR.2:
  - ALC_FLR.1 as before
  - *The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.*
  - *The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.*
  - *The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.*
  - *The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.*

- ALC_FLR.3:
  - first 5 as before
  - *The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.*
  - next 3 as before
  - *The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.*
  - *The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.*

CEM -Common Evaluation Methodology

- given CC documentation, EAL classification etc, perform a check
- idea: evaluation by non-experts, semi-automated, mainly paper work (frequently companies hire people with average or no knowledge in security technologies)
- mapping:
  - assurance class ⇒ activity
  - assurance component ⇒ sub-activity
  - evaluator action element ⇒ action

3.1Evaluation of flaw remediation (ALC_FLR.1)

3.1.1 Objectives

The objective of this sub-activity is to determine whether the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users.

3.1.2 Input

The evaluation evidence for this sub-activity is:

a) the flaw remediation procedures documentation.

3.1.3Evaluator actions

This sub-activity comprises one CC Part 3 evaluator action element:

a)ALC_FLR.1.1E

3.1.3.1Action ALC_FLR.1.1E

ALC_FLR.1.1C - The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1-1 The evaluator shall examine the flaw remediation procedures documentation to determine that it describes the procedures used to track all reported security flaws in each release of the TOE.

The procedures describe the actions that are taken by the developer from the time each suspected security flaw is reported to the time that it is resolved. This includes the flaw's entire timeframe, from initial detection through ascertaining the flaw is a security flaw, to resolution of the security flaw.

If a flaw is discovered not to be security-relevant, there is no need (for the purposes of the ALC_FLR requirements) for the flaw remediation procedures to track it further; only that there be an explanation of why the flaw is not security-relevant.

...

- responsibilities:
  - **sponsor:** requesting and supporting an evaluation. different agreements for the evaluation (e.g. commissioning the evaluation), providing evaluation evidence.
  - **developer:** produces TOE, providing the evidence required for the evaluation on behalf of the sponsor.
  - **evaluator:** performs the evaluation tasks required in the context of an evaluation, performs the evaluation sub-activities and provides the results of the evaluation assessment to the evaluation authority.
  - **evaluation authority:** establishes and maintains the scheme, monitors the evaluation conducted by the evaluator, issues certification/validation reports as well as certificates based on the evaluation results
- verdicts: pass, fail, inconclusive
- parts:
  - evaluation input task (are all documents available to perform evaluation?)
  - evaluation sub-activities
  - evaluation output task (deliver the Observation Report (OR) and the Evaluation Technical Report (ETR)).
  - demonstration of the technical competence task

3 Security Problem Definition

- **Object Security Problem (OSP)**: "The security problem definition defines the security problem that is to be addressed.

  – `axiomatic:` deriving the security problem definition outside the CC scope

  – `crucial:` the usefulness of the results of an evaluation strongly depends on the security problem definition.

  – `requires work:` spend significant resources and use well-defined processes and analyses to derive a good security problem definition.

- good example:

  Secure signature-creation devices must, by appropriate technical and operational means, ensure at the least that:

  1) The signature-creation-data used for signature-creation can practically occur only once, and that their secrecy is reasonably assured;

  2) The signature-creation-data used for signature-creation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;

  3) The signature-creation-data used for signature-creation can be reliably protected by the legitimate signatory against the use of others

Assets

entities that someone places value upon. Examples of assets include: - contents of a file or a server; - the authenticity of votes cast in an election; - the availability of an electronic commerce process; - the ability to use an expensive printer; - access to a classified facility.

no threat no asset!

Logical MRTD Data

The logical MRTD data consists of the EF.COM, EF.DG1 to EF.DG16 (with different securityneeds) and the Document Security Object EF.SOD according to LDS [6]. These data are user data of the TOE. The EF.COM lists the existing elementary files (EF) with the user data. The EF.DG1to EF.DG13 and EF.DG 16 contain personal data of the MRTD holder. The Chip Authentication Public Key (EF.DG 14) is used by the inspection system for the Chip Authentication. The EF.SOD is used by the inspection system for Passive Authentication of the logical MRTD.

Authenticity of the MRTD's chip

The authenticity of the MRTD's chip personalized by the issuing State or Organization for theMRTD holder is used by the traveler to prove his possession of a genuine MRTD.

3. **Subjects**

actors that have influence of TOE.

Examples in our case:

Manufacturer

The generic term for the IC Manufacturer producing the integrated circuit and the MRTD Manufacturer completing the IC to the MRTD's chip. The Manufacturer is the default user of theTOE during the Phase 2 Manufacturing. The TOE does not distinguish between the users ICManufacturer and MRTD Manufacturer using this role Manufacturer.

Personalization Agent

The agent is acting on behalf of the issuing State or Organization to personalize the MRTD forthe holder by some or all of the following activities (i) establishing the identity the holder for thebiographic data in the MRTD, (ii) enrolling the biometric reference data of the MRTD holder i.e.the portrait, the encoded finger image(s) and/or the encoded iris image(s) (iii) writing these dataon the physical and logical MRTD for the holder as defined for global, international and national interoperability, (iv) writing the initial TSF data and (iv) signing the Document Security Object defined in [6].

***Terminal* ...**

***Inspection System* ...**

MRTD Holder

The rightful holder of the MRTD for whom the issuing State or Organization personalized the MRTD.

Traveler ...

Attacker ...

A threat agent trying (i) to identify and to trace the movement of the MRTD's chip remotely (i.e.without knowing or optically reading the printed MRZ data), (ii) to read or to manipulate the logical MRTD without authorization, or (iii) to forge a genuine MRTD.

Assumptions:

assumptions are acceptable, where certain properties of the TOE environment are already known or can be assumed

this is NOT the place for putting properties derived from specific properties of the TOE

Examples:

A.MRTD_ Delivery

MRTD delivery during steps 4 to 6 Procedures shall guarantee the control of the TOE delivery and storage process and conformanceto its objectives:

-Procedures shall ensure protection of TOE material/information under delivery and storage.

-Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.

-Procedures shall ensure that people dealing with the procedure for delivery have got the necessary skills.

3. **Threats**

threats to assets, events that that endenger assets

T.Chip_ID Identification of MRTD's chip

Adverse action: *An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface.*

Threat agent: *having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance*

Asset: *Anonymity of user*

T.Skimming Skimming the logical MRTD

Adverse action: *An attacker imitates an inspection system trying to establish a communicationto read the logical MRTD or parts of it via the contactless communication channel of the TOE.*

Threat agent: *having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance*

Asset: *confidentiality of logical MRTD*

4. Security objectives

- "*The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition. Their role:*

  - a high-level, natural language solution of the problem;

  - divide this solution into partwise solutions, each addressing a part of the problem;

  - demonstrate that these partwise solutions form a complete solution to the problem."
- bridge between the security problem and Security Functional Requirements (SFR)
- **mapping objectives to threats**: table, each threat shoud be covered, each objective has to respond to some threat

  answers to questions:

  - what is really needed?
  - have we forgot about something?
- **rationale:** verifiable explanation why the mapping is sound

Examples of security objectives

OT.AC_ Pers   Access Control for Personalization of logical MRTD

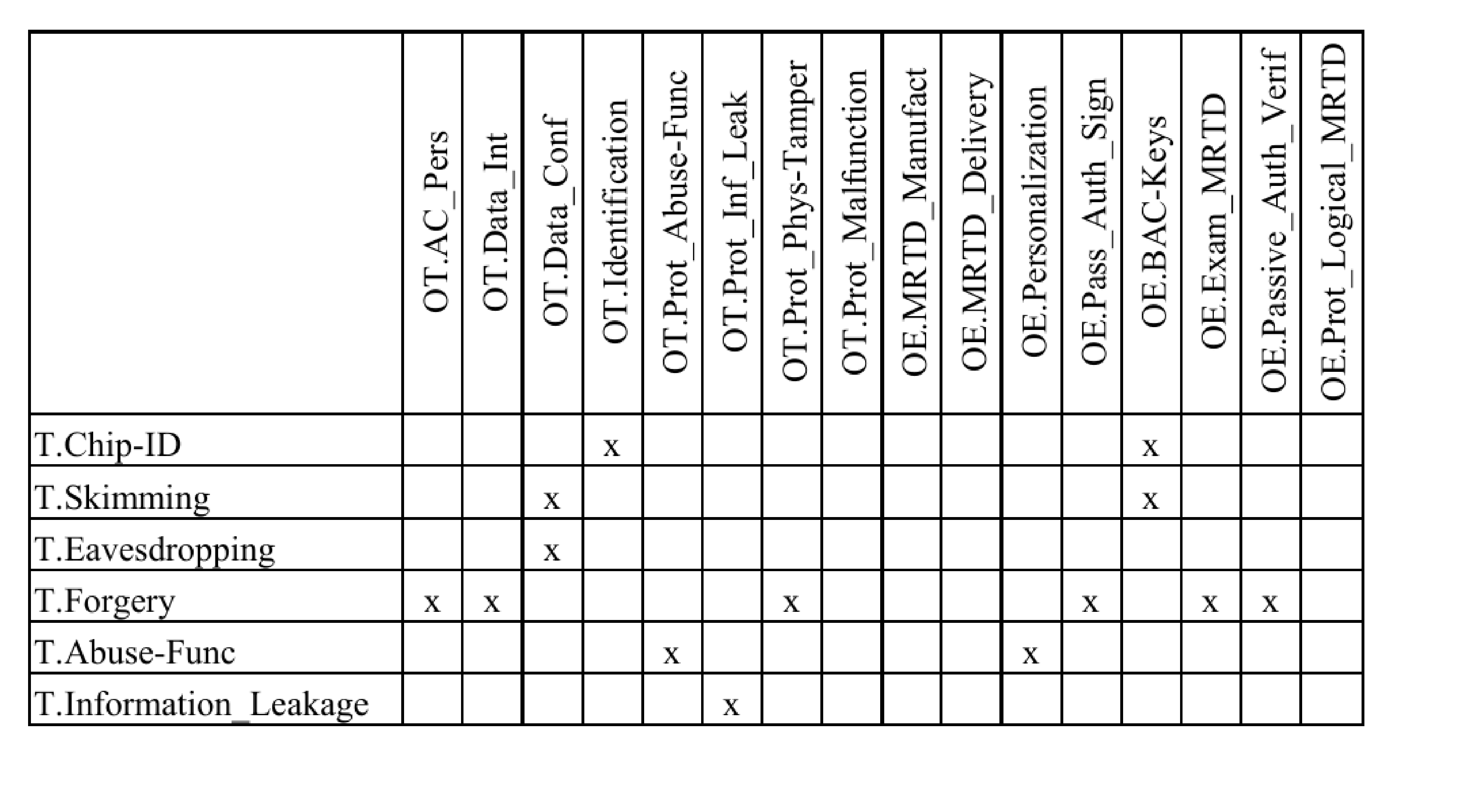
The TOE must ensure that the logical MRTD data in EF.DG1 to EF.DG16, the Document security object according to LDS [6] and the TSF data can be written by authorized Personalization Agents only. The logical MRTD data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after its personalization. The Document security object can be updated by authorized Personalization Agents if data in the data groupsEF.DG 3 to EF.DG16 are added.

OT.Data_ Int   Integrity of personal data

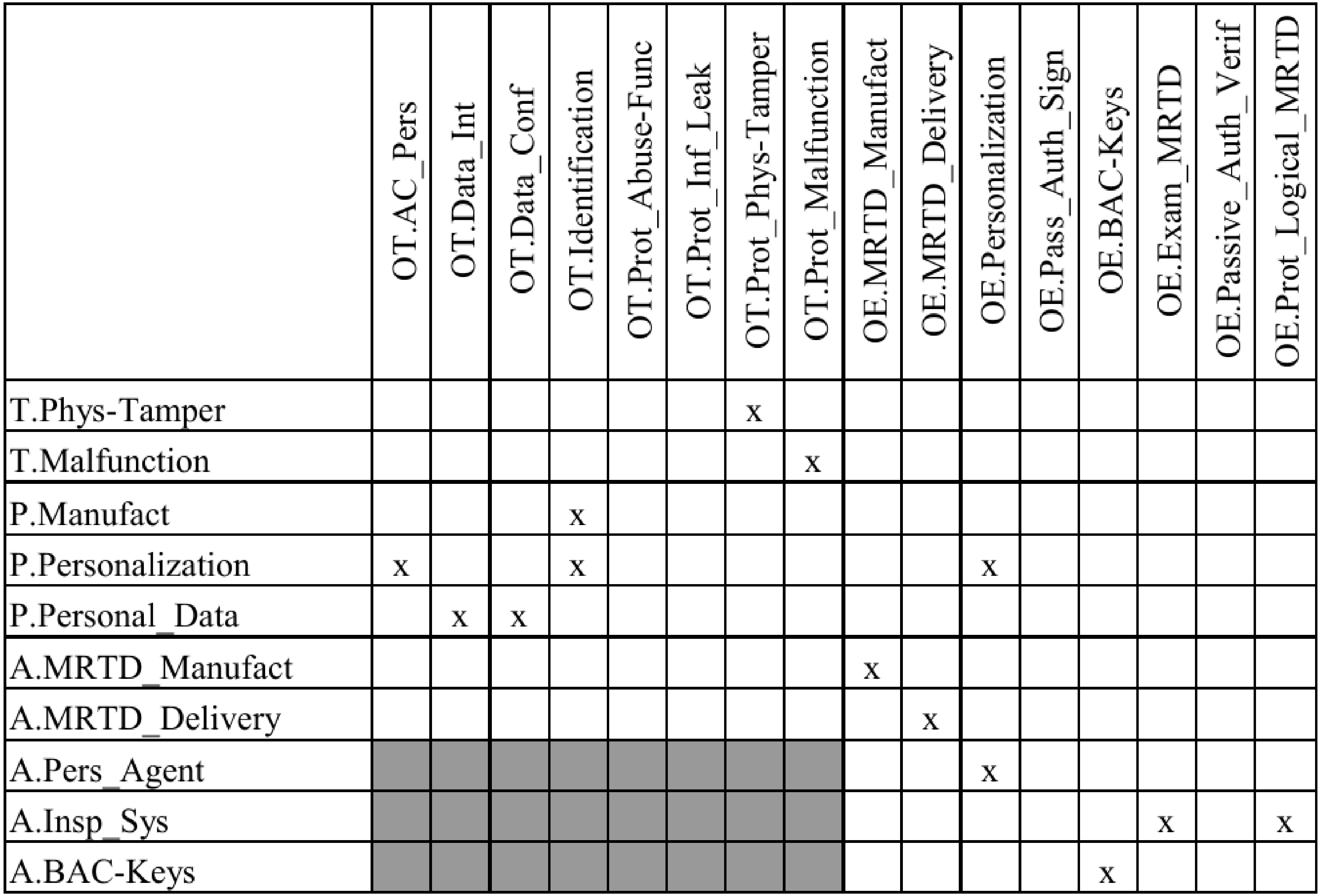
The TOE must ensure the integrity of the logical MRTD stored on the MRTD's chip against physical manipulation and unauthorized writing. The TOE must ensure that the inspection systemis able to detect any modification of the transmitted logical MRTD data.

Conditions:

- in each column and row at least one x
- if this property holds after removing a column then maybe the corresponding security objective can be removed
- this is an instance of solving the set cover problem (hard problem but the instance size is small)



	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Chip-ID				x									x			
T.Skimming			x										x			
T.Eavesdropping			x													
T.Forgery	x	x					x					x		x	x	
T.Abuse-Func					x						x					
T.Information_Leakage						x										



	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OE.MRTD_Manufact	OE.MRTD_Delivery	OE.Personalization	OE.Pass_Auth_Sign	OE.BAC-Keys	OE.Exam_MRTD	OE.Passive_Auth_Verif	OE.Prot_Logical_MRTD
T.Phys-Tamper							x									
T.Malfunction								x								
P.Manufact				x												
P.Personalization	x			x							x					
P.Personal_Data		x	x													
A.MRTD_Manufact									x							
A.MRTD_Delivery										x						
A.Pers_Agent	▨	▨	▨	▨	▨	▨	▨	▨			x					
A.Insp_Sys	▨	▨	▨	▨	▨	▨	▨	▨						x		x
A.BAC-Keys	▨	▨	▨	▨	▨	▨	▨	▨					x			

Table 1: Security Objective Rationale

The threats T.Information_Leakage “Information Leakage from MRTD’s chip”, *T.Phys-Tamper “Physical Tampering” and T.Malfunction “Malfunction due to Environmental Stress” are typical for integrated circuits like smart cards under direct attack with high attack potential. The protection of the TOE against these threats is addressed by the directly related security objectives OT.Prot_Inf_Leak “Protection against Information Leakage”, OT.Prot_Phys-Tamper “Protection against Physical Tampering” and OT.Prot_Malfunction “Protection against Malfunctions”.*

→ each x in the table requires justification that is simple and verifiable

5. Extended Component Definition

- In many cases in the next section we use standard components in CC Part 2 or CC Part 3.
- in some cases, there may be requirements in an ST that are not based on components in CC Part 2 or CC Part 3.
- in this case new components (extended components) need to be defined

6.1 SFR (Security Functional requirements)

- *The SFRs are a translation of the security objectives for the TOE.*
- *They are usually at a more detailed level of abstraction, but they have to be a complete translation (the security objectives must be completely addressed) and be independent of any specific technical solution (implementation).*
- *The CC requires this translation into a standardised language for several reasons:*
  - *to provide an exact description of what is to be evaluated. As security objectives for the TOE are usually formulated in natural language, translation into a standardised language enforces a more exact description of the functionality of the TOE.*
  - *to allow comparison between two STs. As different ST authors may use different terminology in describing their security objectives, the standardised language enforces using the same terminology and concepts. This allows easy comparison*

Predefined classes used to define SFR:

- Logging and audit class FAU

- Identification and authentication class FIA

- Cryptographic operation class FCS

- Access control families FDP_ACC, FDP_ACF

- Information flow control families FDP_IFC, FDP_IFF

- Management functions class FMT

- (Technical) protection of user data families FDP_RIP, FDP_ITT, FDP_ROL

- (Technical) protection of TSF data class FPT

- Protection of (user) data during communication with external entities families FDP_ETC, FDP_ITC, FDP_UCT, FDP_UIT, FDP_DAU, classes FCO and FTP

Customizing SFRs:

- `refinement` (more requirements),
- `selection` (options),
- `assignment` (values),
- `iterations` (the same component may appear at different places with different roles)

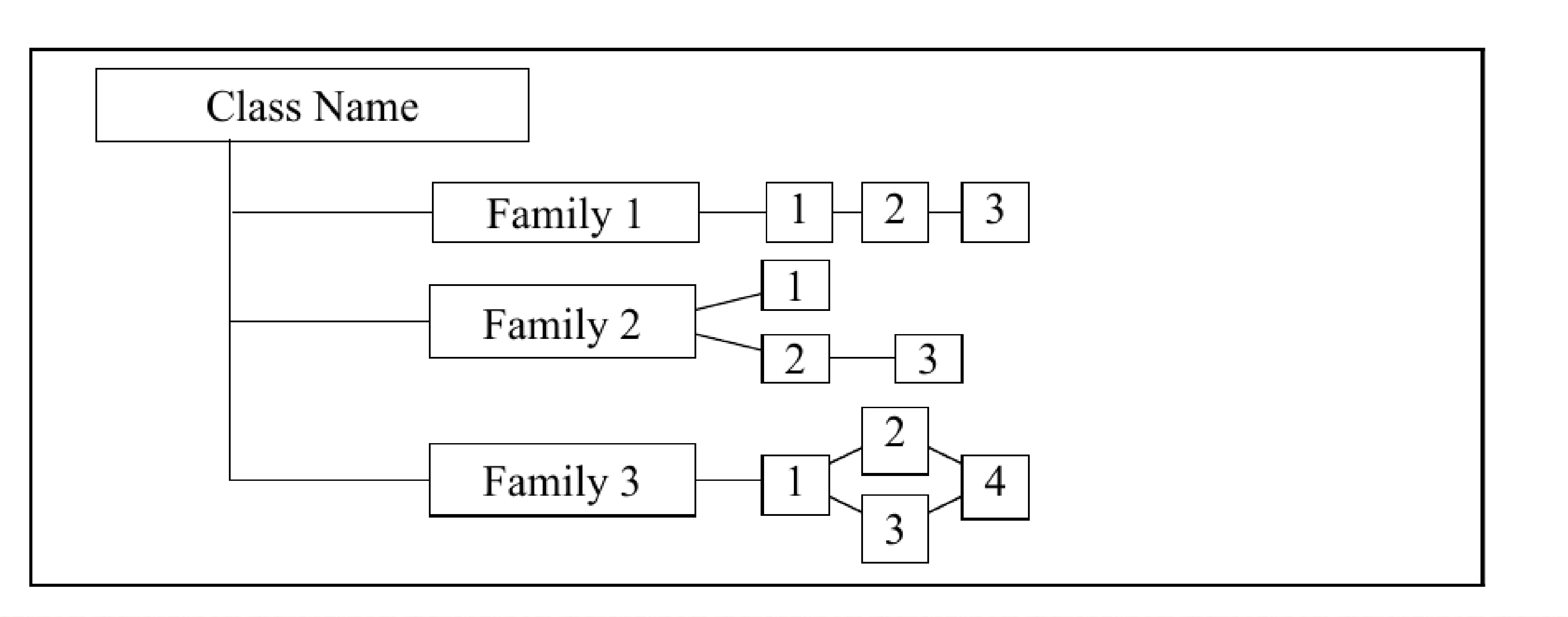
these options appear in the text of a component, nothing else can be changed in the definition of a class

Dependencies

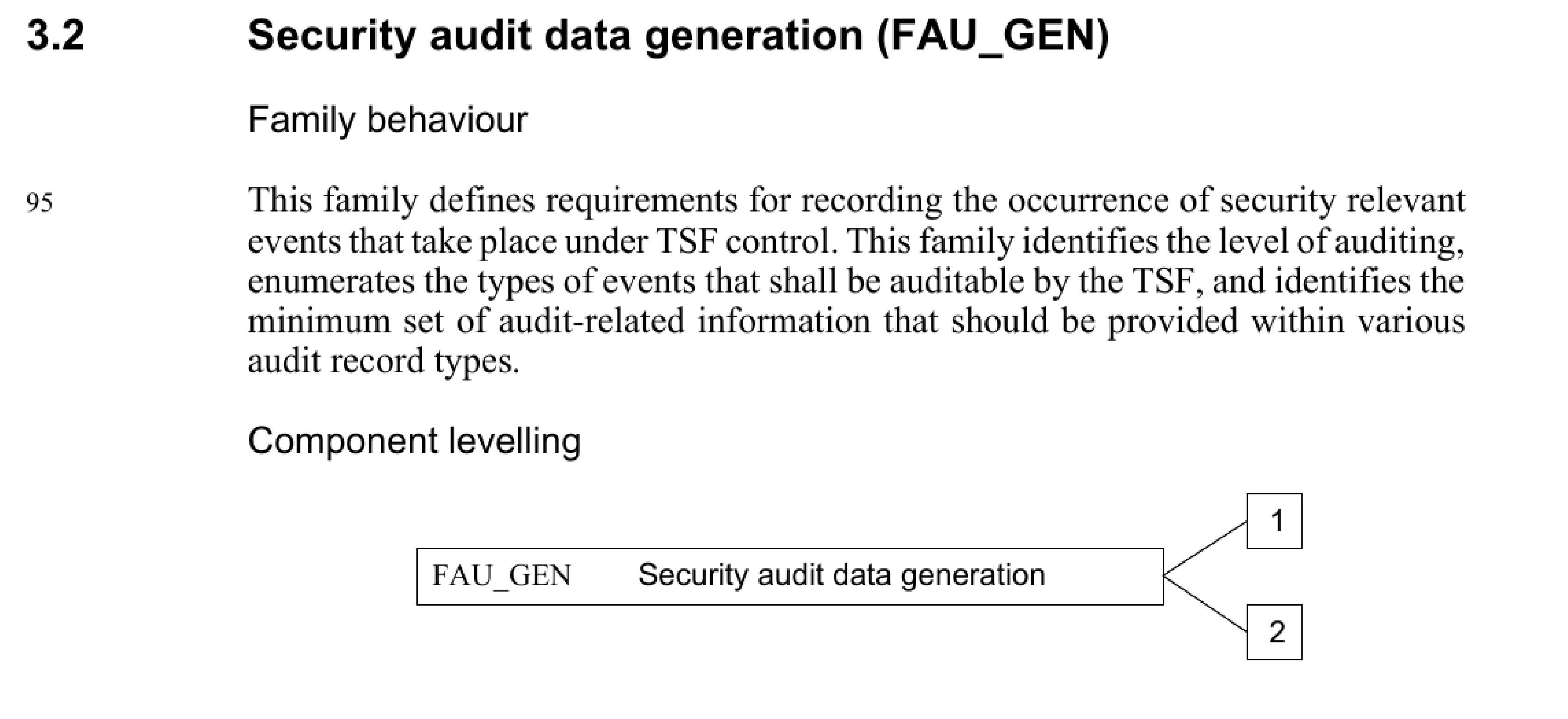
- while SFRs are concentrated on single atomic issues there are dependencies between SFRs
- some dependencies are already mentioned in CC
- PP: for each SFR there is a list of declared dependencies – an information to ST editors
- having in mind all subtle issues and alternatives to achieve goals

Hierarchy

- fulfilling Family 1.3 automatically fulfills Family1.2 and Family1.2
- fulfilling Family3.2 automatically fulfills Family3.1 but not Family3.3 and not Family3.4
- terminology: Family1.3 **is hierarchical to** Family1.2 (the links on the graph towards class name)



Example



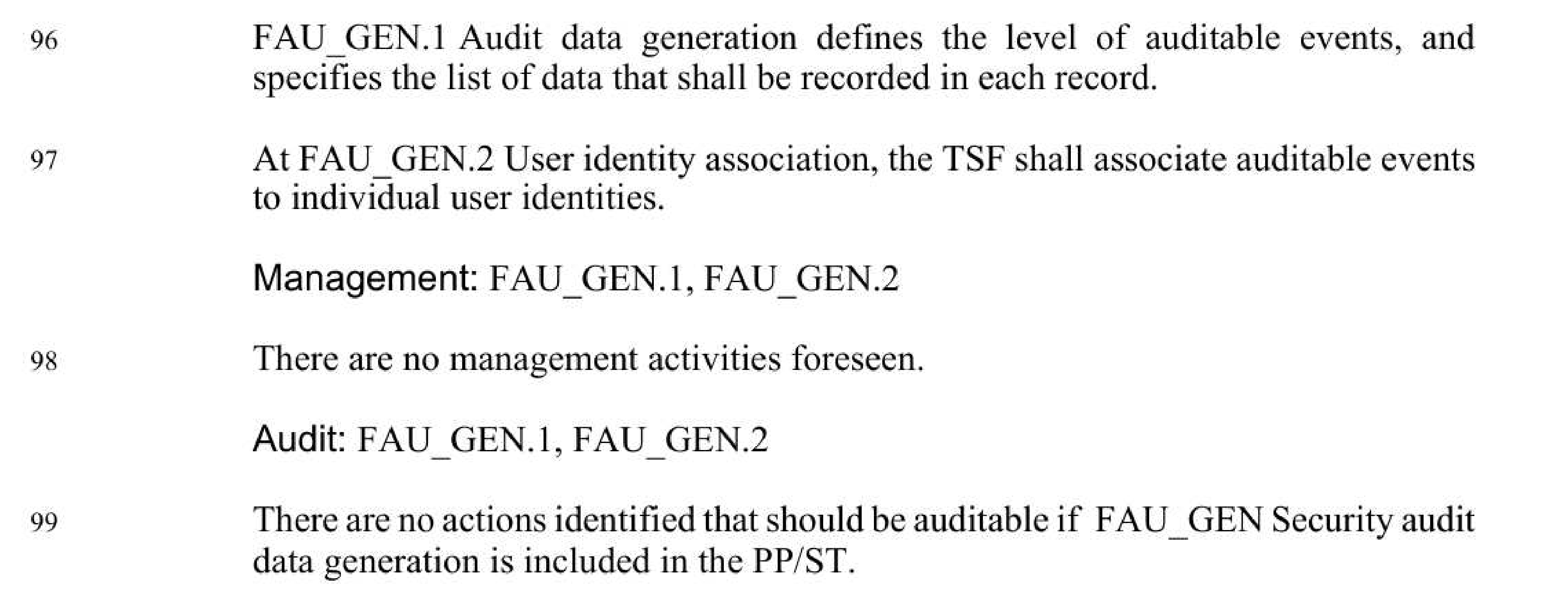
3.2 Security audit data generation (FAU_GEN)

Family behaviour

95 This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

Component levelling

Example cnt



96 FAU_GEN.1 Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.

97 At FAU_GEN.2 User identity association, the TSF shall associate auditable events to individual user identities.

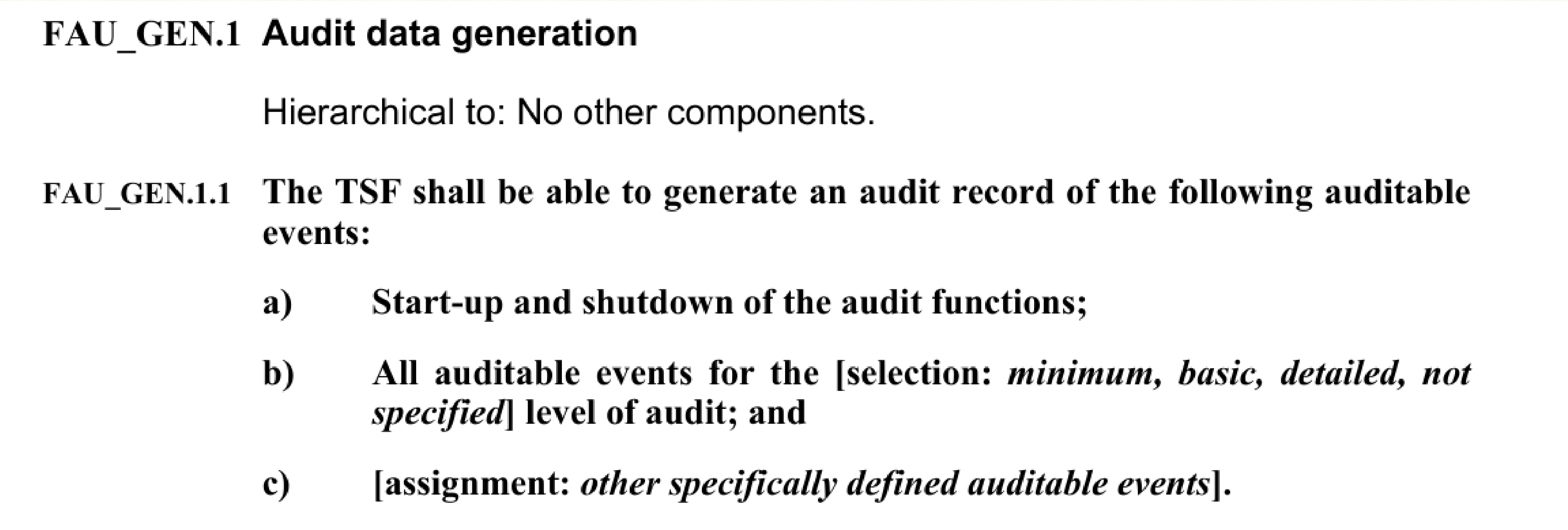
Management: FAU_GEN.1, FAU_GEN.2

98 There are no management activities foreseen.

Audit: FAU_GEN.1, FAU_GEN.2

99 There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

Example cnt



FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

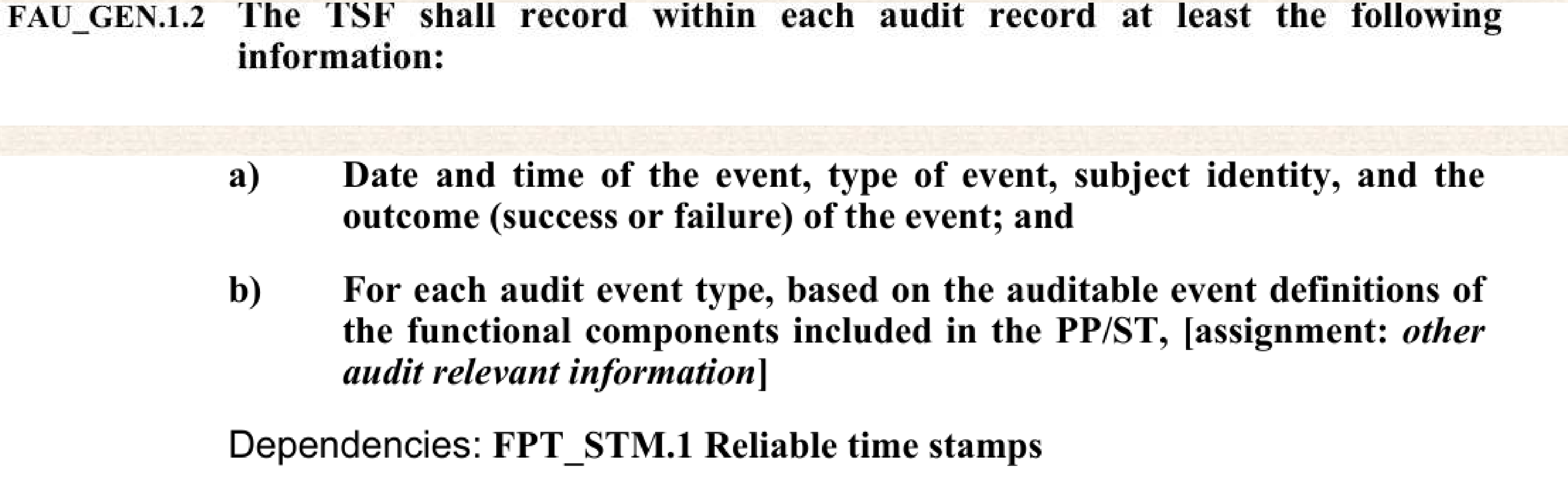
FAU_GEN.1.1 **The TSF shall be able to generate an audit record of the following auditable events:**

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection: *minimum, basic, detailed, not specified*] level of audit; and

c) [assignment: *other specifically defined auditable events*].

Example cnt



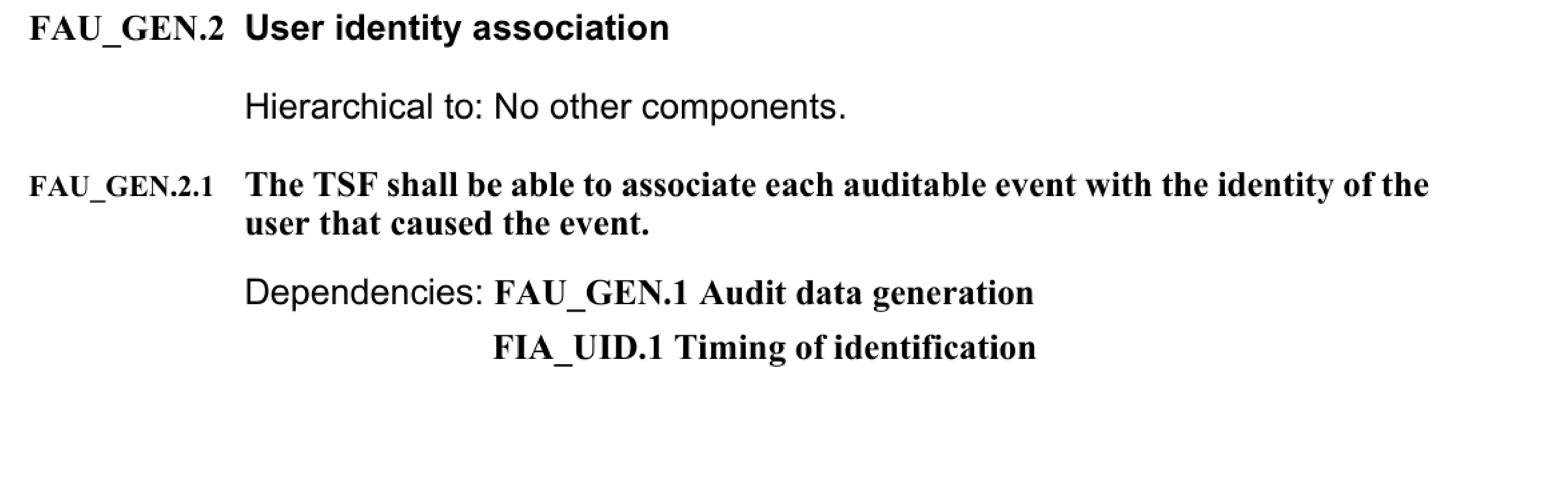
FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*]

Dependencies: **FPT_STM.1 Reliable time stamps**

Example cnt



FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 **The TSF shall be able to associate each auditable event with the identity of the user that caused the event.**

Dependencies: **FAU_GEN.1 Audit data generation**
FIA_UID.1 Timing of identification

Rationale

again, PP must provide:

- a table with all SFR and SO with “x” marks
- a concise justification that each security objective is covered by SFR’s

	OT.AC_Pers	OT.Data_Int	OT.Data_Conf	OT.Identification	OT.Prot_Inf_Leak	OT.Prot_Phys-Tamper	OT.Prot_Malfunction	OT.Prot_Abuse-Func
FAU_SAS.1				x				
FCS_CKM.1	x	x	x					
FCS_CKM.4	x		x					
FCS_COP.1/SHA	x	x	x					
FCS_COP.1/ENC	x	x	x					
FCS_COP.1/AUTH	x	x						
FCS_COP.1/MAC	x	x	x					
FCS_RND.1	x	x	x					
FIA_UID.1			x	x				
FIA_AFL.1			x	x				
FIA_UAU.1			x	x				
FIA_UAU.4	x	x	x					