Hochschule Konstanz
Fakultät Informatik

Introduction to IT Security

WIN+AIN

Hanno Langweg

02b Security Management – Common Criteria

Security Management Topics

- IT security standards and processes
  - ISO 2700x
  - BSI base protection
  - Personnel security
  - Physical security
- Vulnerability management
- Product evaluations using Common Criteria

Common Criteria Evaluations

Examples of certified products

- Network connectors for e-health
- Smart metering gateways
- Digital tachographs
- E-passports
- Smart cards
- Card readers

Common Criteria (CC)

- CC de-facto standard for product evaluations
  - CC v2.3 is ISO 15408:2005
  - Current version is v3.1
    http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
- Abstract way to describe security functionality
- Separation of
  - Functional requirements
    http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf
    (300+ pages)
  - Assurance requirements
    http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf
    (200+ pages)

IT security requirements

- SFRs: Security functional requirements (what/how)
  e.g. identification&authentication, audit, crypto
- SARs: Assurance requirements (how to evaluate)
  - ASE: Evaluation of ST
  - ADV: Development specifications, architecture, access to development artifacts
  - AGD: Guidance documents
  - ALC: Life-cycle, configuration management, tools, flaw remediation process
  - ATE: Testing (coverage, depth, independence)
  - AVA: Vulnerability analysis

Common Criteria key concepts

- Framework where security requirements can be specified, claimed, and evaluated
- **Target of evaluation (TOE):** The product or system that is the subject of the evaluation, e.g. „MinuteGap Firewall“
- **Protection profile (PP):** Document that identifies security requirements relevant to a user community for a particular purpose, e.g. „Firewall Protection Profile“
- **Security target (ST):** Product specification explaining how security functionality is delivered by the product, e.g. „MinuteGap Firewall ST“ Can be standalone, can conform to one or more PPs
- **Evaluation assurance level (EAL):** a numerical rating (1-7) reflecting assurance requirements fulfilled during evaluation

EAL Evaluation assurance levels

- Cumulative assurance requirements
  Higher levels include lower level requirements
  Higher levels = higher confidence in evaluation result
  - Often used: EAL2, EAL4;
    for smartcards also >EAL4 often used
  - Popular augmentations:
    - AVA_VAN.5 **–** vulnerability analysis with **high attack potential**
    - ALC_FLR **– flaw remediation process** for security issues detected after certification

EAL Evaluation assurance levels

- EAL1 – functionally tested („low assurance“)
  - Review of functional and interface specifications
  - Some independent testing
- **EAL2** – structurally tested („minimal serious level“)
  - Analysis of security functions including high-level design
  - **Independent testing**, review of developer testing
  - Penetration testing with „basic“ attack potential
- EAL3 – methodically tested and checked
  - More testing, some development environment controls
  - **Site visit** of development/manufacturing sites
- **EAL4** – methodically designed, tested, and reviewed
  - **Source code** inspections
  - Pentesting „Extended-basic“ attack potential

EAL Evaluation assurance levels

- EAL5 – semiformally designed and tested
  - Formal model, modular design
  - Systematic vulnerability search, covert channel analysis
- EAL6 – semiformally verified design and tested
  - Structured development process
  - Pentesting with **„high“ attack potential**
- EAL7 – formally verified design and tested
  - Formal presentation of functional specification
  - Product or system design must be simple
  - Independent confirmation of developer tests

How to read Security Targets (and PPs)

- TOE **overview** and TOE description
- TOE **summary specification** (only for STs)
- **Security problem definition**
- Objectives for operational **environment**
- **Conformance** claims ST ➔ PPs

- Additional reading: BSI (2010). The PP/ST Guide. (AIS 41) Chapter 3: "Reading protection profiles and security targets"

Example: Card reader G87-1505 (eHealth)

– TOE **overview**

The TOE described in this Security Target is the smart card keyboard *"G87-1505"* with integrated smart card readers. The TOE fulfills the requirements to be used with the German electronic Health Card (eHC) and the German Profession Card (HPC) based on the regulations of the German healthcare system. For further information about card compatibility, please see [14].
The TOE can be used as a secure PIN entry device for applications according to [22], which specifically means that a PIN, which has been entered by a user at the TOE, never leaves the TOE in clear text, except to smart cards in local card slots.
The TOE signals whether the secure PIN entry mode is active or not by the display and by a red flashing LED beside the corresponding smartcard slots in case of a verification against an inserted smart card.
The TOE bases on the specification "Secure Interoperable ChipCard Terminal - SICCT" [15] extended and limited by the gematik- specification for the eHealth Terminal itself [14].


G87-1505 | Common-Criteria 3.1-Document | Version 2.17, Final

1.2 TOE Overview

The TOE described in this Security Target is the smart card keyboard "G87-1505" with integrated smart card readers. The TOE fulfills the requirements to be used with the German electronic Health Card (eHC) and the German Profession Card (HPC) based on the regulations of the German healthcare system. For further information about card compatibility, please see [14].
The TOE can be used as a secure PIN entry device for applications according to [22], which specifically means that a PIN, which has been entered by a user at the TOE, never leaves the TOE in clear text, except to smart cards in local card slots.
The TOE signals whether the secure PIN entry mode is active or not by the display and by a red flashing LED beside the corresponding smartcard slots in case of a verification against an inserted smart card.
The TOE bases on the specification "Secure Interoperable ChipCard Terminal - SICCT" [15] extended and limited by the gematik- specification for the eHealth Terminal itself [14].

In its core functionality, the TOE is not different from any other smart card terminal which provides an interface to one or more smart cards including a mean to securely enter a PIN.
Additionally, the TOE provides an interface which allows routing the communication of a smart card to a remote IT product outside the TOE.
The G87-1505 does not provide a LAN- Interface for the communication with remote ITE. Separate software (Translating Proxy), which is not part of the TOE, secures the compatibility to communicate with other ITE over the LAN. The G87-1505 uses the LAN- Interface of the Host-PC for the communication. The Cherry Translating Proxy must be installed on the Host-PC for the communication with the so-called connector.
The TOE provides a PIN- Pad for secure PIN entry and a monochrome display (128x64 pixels) with backlight. Also, two ID-1 and two ID-000 contact units available for corresponding cards.
Both ID-1 card slots are equipped with two LED's for the visualizing of the Secure PIN entry- Mode and the activation of a card. Both LED's, a red one for Secure PIN entry and a green one to indicate card activity, of one ID-1 card slot directed to the surface of the TOE via one light conductor.

Figure 1: G87-1505

The TOE provides the following main functions:
- The access to one or more slots for smart cards
- Secure Network connectivity
- Secure PIN entry functionality
- Enforcement of the encryption of communication
- User authentification
- Management functionality including update and downgrade of Firmware, and
- Passive physical protection

The TOE use a SM-KT in form of a ID-000 card for cryptographic operation e.g. for authentication, integrity assurance and to ensure the confidentiality of data transmitted over the network interface. As physical characteristics of the SM-KT the TOE supports gSMC-KT cards.
IPv6 will be supported in addition to IPv4 by a firmware update.
The TOE uses the USB- Interface of the HOST-PC for power supply.

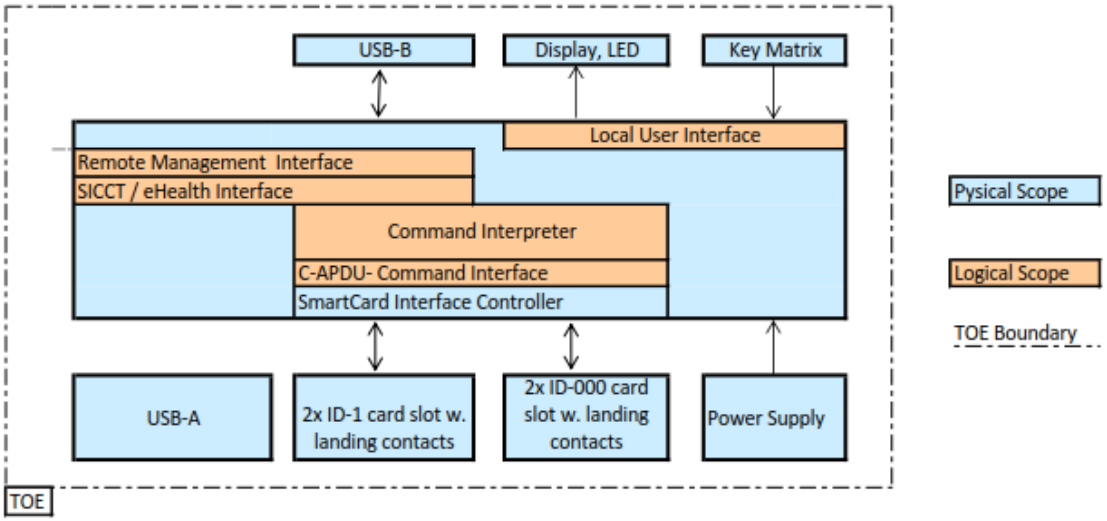
3 pages TOE overview: usage and major security features, TOE type, required hardware/software/firmware

Example: Card reader G87-1505 (eHealth)

– TOE description

The TOE consists of hardware and software with the major security feature to enter a PIN in a secure way and transfer this PIN securely to a card in one of the slots of the TOE.
In addition, the TOE provides the following security features to fulfill the requirements of the German health card system.

- secure communication,
- secure update function,
- management function,
- user authentication
- active tamper protection



3 pages TOE description: physical+logical scope of TOE

Example: Card reader G87-1505 (eHealth)

– TOE **summary specification** (only for STs)

The TOE is designed for the use within the Telematikinfrastruktur (TI) of the German Healthcare-System.
The TOE will be used as a part of a signature application component for the creation of qualified signatures and for the processing and storage of personal data on healthcards.
The Protection of personal identification data (PIN), the secure transmission of data and the secure firmware update are the main features.
The following security functions are implemented to guarantee these features of the TOE:

6 pages, reasonaby accessible to a non-CC expert

Example: Card reader G87-1505 (eHealth)

– Security problem definition

This chapter describes:

- The **assets** which have to be protected by the TOE.
- The **subjects** which are interacting with the TOE.
- The **threats** which exist against the assets of the TOE
- The **organisational security policies** the TOE has to comply to.
- The **assumptions** which have to be made about the environment of the TOE.

Threat	Description
T.COM	An attacker may try to intercept the communication between the TOE and the connector in order to gain knowledge about communication data which is transmitted between the TOE and the connector or in order to manipulate this communication. As part of this threat an authorized user, who is communicating with the TOE (via a connector) could try to influence communications of other users with the TOE in order to manipulate this communication or to gain knowledge about the transmitted data.
T.PIN	An attacker may try to release the PIN which has been entered by a user from

5 pages definition of what the TOE is designed to protect

Example: Card reader G87-1505 (eHealth)

– Objectives for operational **environment**

Objective	Description
OE.ENV	It is assumed that the TOE is used in a controlled environment. Specifically it is assumed: • The card terminal prevents (not visible) physical manipulations for at least 10 minutes. The environment ensures beyond these 10 minutes that the card terminal is protected against unauthorized physical access or such is perceptible, • That the user handles his PIN with care; specifically that the user will keep their PIN secret, • That the user can enter the PIN in a way that nobody else can read it, • That the user only enters the card PIN when the TOE indicates a secure state, • That the medical supplier checks the sealing and the physical integrity of the TOE regularly before it is used, • The medical supplier sends the TOE back to the manufacturer in case he suspects an unauthorized reset to factory defaults has been performed by unauthorized personnel, and • That the network of the medical supplier is appropriately secured so authorized entities are trustworthy, so also [13].

2 pages of conditions that the TOE takes for granted

Example: Card reader G87-1505 (eHealth)

– Rationale: every threat+assumption mapped to objective for TOE or environment

	O.ACCESS_CONTROL	O.PIN_ENTRY	O.I&A	O.MANAGEMENT	O.SECURE_CHANNEL	O.STATE	O.PROTECTION	OE.ENV	OE.ADMIN	OE.CONNECTOR	OE.SM	OE.PUSH_SERVER	OE.ID000_CARDS
T.COM			X		X		X	X					
T.PIN	X	X					X	X					
T.DATA	X		X	X			X	X					
T.F-CONNECTOR								X	X	X			
OSP.PIN_ENTRY		X				X	X						
A.ENV								X					
A.ADMIN									X				
A.CONNECTOR										X			
A.SM											X		
A.PUSH_SERVER												X	
A.ID000_CARDS													X

Example: Card reader G87-1505 (eHealth)

– **Conformance** claims ST ➔ PPs

2.2 PP Claim

This Security Target claims strict conformance to the Common Criteria Protection Profile "Electronic Health Card Terminal (eHCT)", BSI-CC_PP_0032-V3-2016; Version 3.7, 21th September 2016.

2.3 Package Claim

The assurance level for the TOE is EAL 3 augmented by the components ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_TAT.1 and AVA.VAN.4.

independent testing, site visit; no source code

basic modular design

well-defined development tools

methodical vulnerability analysis, pentesting, moderate attack potential

complete functional specification

source code for security functionality

2.4 Conformance Claim with Technical Directives of the BSI

The Security Target based on the requirements of BSI TR-03120 [16] regarding sealing and physical protection of the TOE housing.

Common Criteria: Evaluation Process

- **National Authority** authorises evaluators
  - Germany: **BSI accredits** commercial organisations
  - Fee charged for evaluation
- Team of four to six **evaluators**
  - Develop work plan
  - Evaluate Security Target (ST) first
  - Confirm that TOE complies with ST
- Controlled by CEM Common Evaluation **Methodology**
  - https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf (400+ pages)
- **Expensive**; ca. >50 TEUR EAL2, can be >1 MEUR EAL6

What happens during an evaluation (i)

- (Hire consultants to prepare development facility and processes for evaluation)
- Application for certification, kick-off
- **Evaluation** by accredited facility
  - ASE, ADV, AGD, ALC **documentation-based**, ca. 50%-80% of total effort
  - **Flaw hypotheses** developed during document phase
  - ATE, AVA **independent testing**, code inspections, ca. 20%-50% of total effort
- **Certification** based on evaluation results
  - All reports with verdict PASS ➔ certificate issued
    Might include obligations for environment/use of TOE

What happens during an evaluation (ii)

- AVA_VAN.5 – **vulnerability** analysis for high attack potential mandatory at >=EAL6
  - Guideline for calculation of attack potential in CEM
  - **High attack potential** e.g.
    - Multiple experts
    - Only public knowledge of TOE
    - Easy access to TOE (e.g. connected to internet)
    - Only standard equipment
    - Up to six months effort to identify and exploit
- **Lower EALs often augmented** with AVA_VAN.5

What happens during an evaluation (iii)

- **Vulnerability analysis** for developer‘s code
  - Flaw hypotheses, **interfaces** to security functionality, **circumvention** of mechanisms, **correctness** of data parsing and control flow, **cryptographic** mechanisms
  - Detailed notes/recommendations for some mechanisms
- Vulnerability analysis for **third-party libraries**
  - **CVE search**: Are there known vulnerabilities for the specific versions of integrated libraries?
  - Long term support and availability of **security patches**?

Certified Products

expand/collapse all categories

- Access Control Devices and Systems – 70 Certified Products
- Biometric Systems and Devices – 3 Certified Products
- Boundary Protection Devices and Systems – 108 Certified Pr
- Data Protection – 61 Certified Products
- Databases – 29 Certified Products
- Detection Devices and Systems – 20 Certified Products
- ICs, Smart Cards and Smart Card-Related Devices and Systems – 816 Certified Products
- Key Management Systems – 28 Certified Products
- Multi-Function Devices – 162 Certified Products
- Network and Network-Related Devices and Systems – 194 Certified Products
- Operating Systems – 98 Certified Products
- Other Devices and Systems – 219 Certified Products
- Products for Digital Signatures – 81 Certified Products
- Trusted Computing – 4 Certified Products

Nom et version du produit

Virtual Machine of Multos M3 G230M mask with AMD 113v4

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 7

How to read certification reports

- Recognition agreements
  - CCRA (<=EAL2), **SOGIS-MRA (<=EAL4)**
  - Part B Certification results
- Special attention on report chapters
  - B.2 **Identification of the TOE**
    ⇨ Product version, hashes for files
  - B.4 **Assumptions**
  - B.8 Evaluated **configuration**
  - B.10 **Obligations** and notes for the usage of the TOE
- Is the evaluated TOE suitable for my needs?

High EAL = high security?

- High EAL = high assurance (**confidence**)
  - How reliable are the evaluation results?
  - How thorough was the testing?
- But: **EAL has nothing to do with security functional requirements**
  - Need to look at SFR
  - Possible to have very few requirements (i.e. little functionality) evaluated at high EAL, i.e. very likely that (albeit few) requirements are correctly implemented
- Often adversaries excluded from PP/ST that are hard to protect against
  - Need to look for **assumptions, objectives for environment**

Apple Mac OS X 10.6: EAL3+

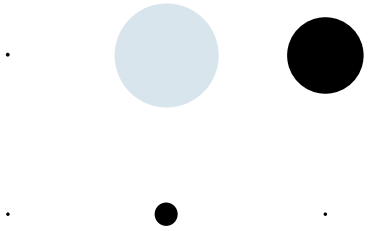
Assumptions About the Environment of the Configuration

Several assumptions are made about the physical environment of the Common Criteria configuration.

- The processing resources of the Common Criteria Evaluated Configuration will be located within controlled access facilities which will prevent unauthorized physical access. The hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- All systems with which the Common Criteria Evaluated Configuration communicates, and the communication paths themselves, are assumed to be under the same management as the Common Criteria configuration and abide by the same security policies.

OpenLimit SignCubes Basiskomponenten 2.1 Version 2.1.6.3: EAL4+

The user ensures that all components of the operating system are correct. The user ensures that no malicious or harmful program is installed on the system.



Other security evaluation schemes

Other evaluation and certification schemes

- BSZ Accelerated Security Certification („Beschleunigte Sicherheits-Zertifizierung“)
  - 30 person-days pentesting, workshop, PASS/FAIL
  - Faster+cheaper than CC; limited to low assurance
  - Launched in 2019, little national experience
- FIPS 140-2 „Security Requirements for Cryptographic Modules“
- PCI-DSS: Collection of best practices tailored to financial institutions
- VDE, TÜV, LGA etc.: evaluations against confidential criteria; customers need to trust evaluator‘s brand

Summary

- Common Criteria (CC) evaluation
  - Internationally recognised evaluation criteria for products
  - Scope defined by security target (and protection profile)
  - Thoroughness of evaluation defined by evaluation assurance level (EAL)
- Other evaluation schemes
  - More specific than CC
  - Scope: sector, product type?
  - Depth: evaluation methods, effort?
  - Validity: verifiable results, known methodology?