brightsight®

your
partner
in security
approval

The Advantages of Using TOE Type Specific Assurance Methodology

Different Assurance levels in one TOE

Dirk-Jan Out, Leo Kool, Rob van Marrewijk
11 September 2013; commoncriteria@brightsight.com

What is the motivation?

- Use
  - well-established
  - well-accepted

  security evaluation requirements from a specific domain

Example in presentation:
payment terminals

Common Approval Scheme
A EUROPEAN INITIATIVE FOR CARD PAYMENTS IN EUROPE
PCI Security Standards Council

- Use
  - well-established
  - well-accepted

  security evaluation framework to incorporate security evaluation requirements

Common Criteria

Common Criteria

SEPA Single Euro Payments Area

Background:
harmonize security evaluation of payment terminals in Europe

Goal of the presentation

- Common Criteria and the difference with CAS/PCI

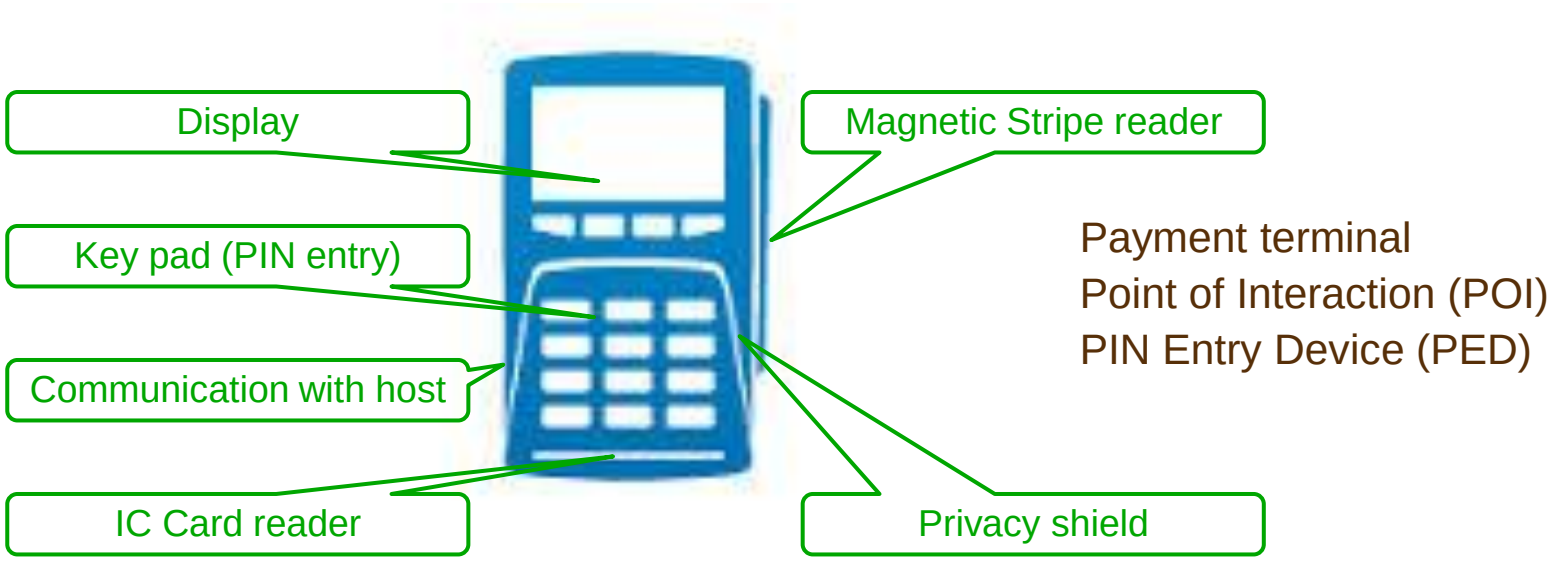
CAS: Common Approval Scheme Initiative: Security group of European banks

PCI-SSC: Collaboration of credit card organization for security of payment terminals

- Experiences gained with the EU pilot performed with this ‘multiple-assurance within one TOE type’ methodology

Payment terminal and security

- Protect the primary asset: PIN (and sometimes account date)
- Protect the secondary assets: keys



PCI requirements (v2.1) – a wide variety of topics

Core Derived Test Requirements—Physical

DTR A1.1	Tamper-Detection Mechanisms
DTR A1.2	Independent Security Mechanisms
DTR A2	Response to Internal Access
DTR A3	Robustness Under Changing Environmental and Operational Conditions
DTR A4	Protection of Sensitive Functions or Information
DTR A5	Audible Tones During PIN Entry
DTR A6	Monitoring During PIN Entry
DTR A7	Determining Keys Analysis
DTR A8.1	Prompts Under Control of the Crypto
DTR A8.2	Altering User Interface Prompts Attac
DTR A8.3	Cryptographically Based Controls
DTR A9	Visual Observation Deterrents
DTR A10	Unique Enclosure
DTR A11	Magnetic-Stripe Reader

Online Derived Test Requirements

DTR C1	Key Substitution

Offline Derived Test Requirements

DTR D1	Penetration Protection
DTR D2.1	ICC Reader Slot Geometry
DTR D2.2	ICC Reader Slot Geometry
DTR D3	ICC Reader Construction (Wires)
DTR D4	PIN Protection During Transmission Between PED and ICC Reader

Core Derived Test Requirements—Logical

DTR B1	Self-Test
DTR B2	Logical Anomalies
DTR B3	Firmware Certification
DTR B4	Firmware Updates
DTR B5	Display During PIN Entry
DTR B6	Clearing of Internal Buffers
DTR B7	Protection of Sensitive Services
DTR B8	Sensitive Services Limits
DTR B9	Random Numbers
DTR B10	Exhaustive PIN Determination
DTR B11	Key Management
DTR B12	Encryption Algorithm Test
DTR B13	Encryption or Decryption of Arbitrary Data Within the Device
DTR B14	Clear-Text Key Security
DTR B15	Transaction Controls

PCI requirements (v2.1) – coverage

Core Derived Test Requirements—Physical

DTR A1.1 Tamper-Detection Mechanisms

TA1.1.3 The tester shall open the PED to activate the tamper-detection mechanisms and then perform tests to support evidence that the PED is no longer operational. The tester shall then perform tests to support evidence that keys and secret data have been erased or are otherwise nonrecoverable. Tests that may be performed could include attempting a transaction to determine if the transaction fails, using a special function of the PED that allows a user to determine the status of secret data, or using special software to determine if secret data has been erased.

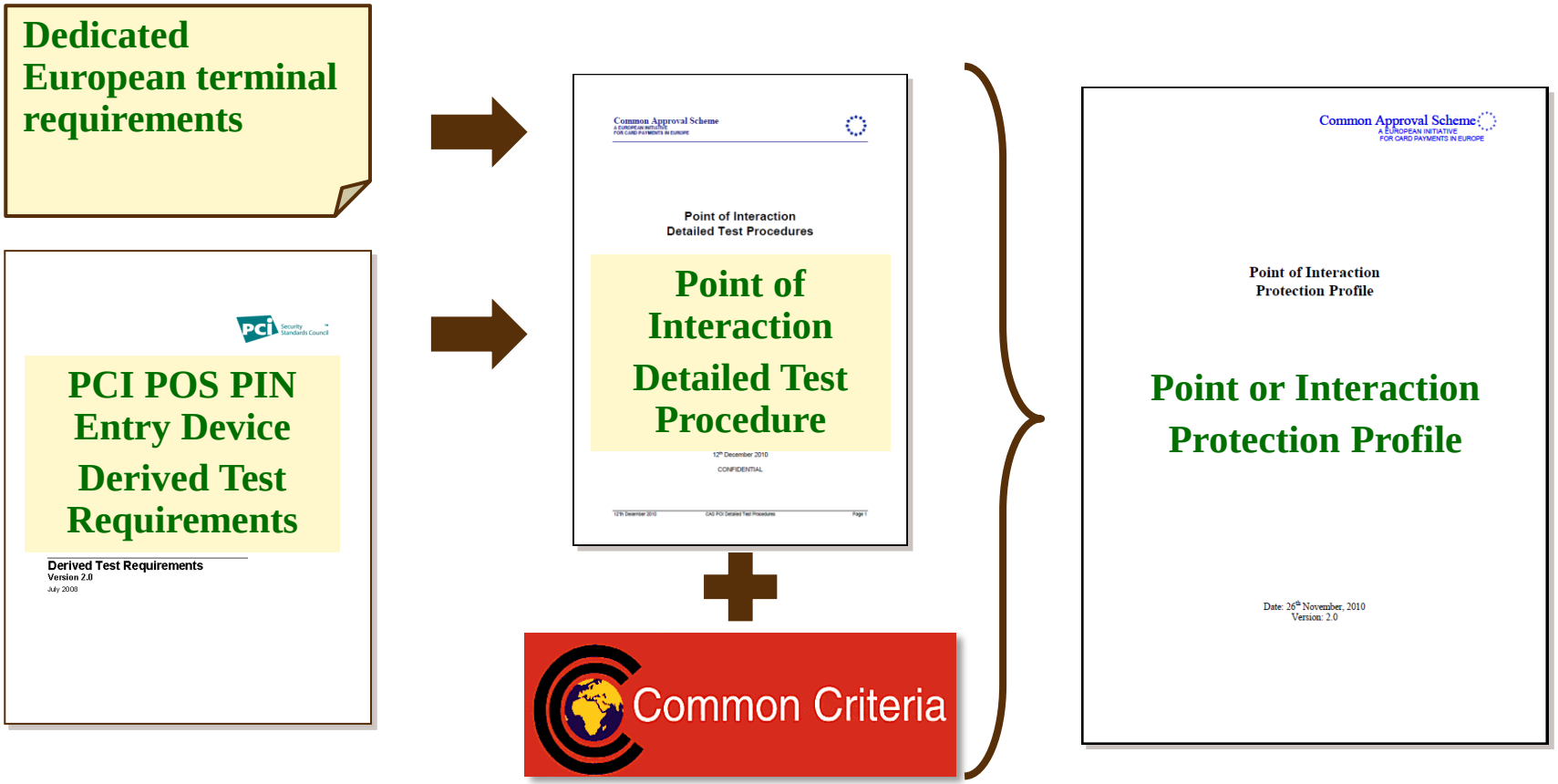
TA1.1.4 The tester shall examine the response to Section A1.1 of the *PCI POS PED Evaluation Vendor Questionnaire* relating to response of the PED to tamper detection, for consistency.

TA1.1.5 The tester shall examine vendor-supplied documentation to determine if the PED employs active or passive (i.e., removal of power) erasure. If the PED employs passive erasure, the tester shall verify that erasure occurs rapidly enough to prevent an attacker from opening the PED and stopping erasure before it is effective. The tester may create an attack scenario, which may be performed in its entirety or in part to verify the theory.

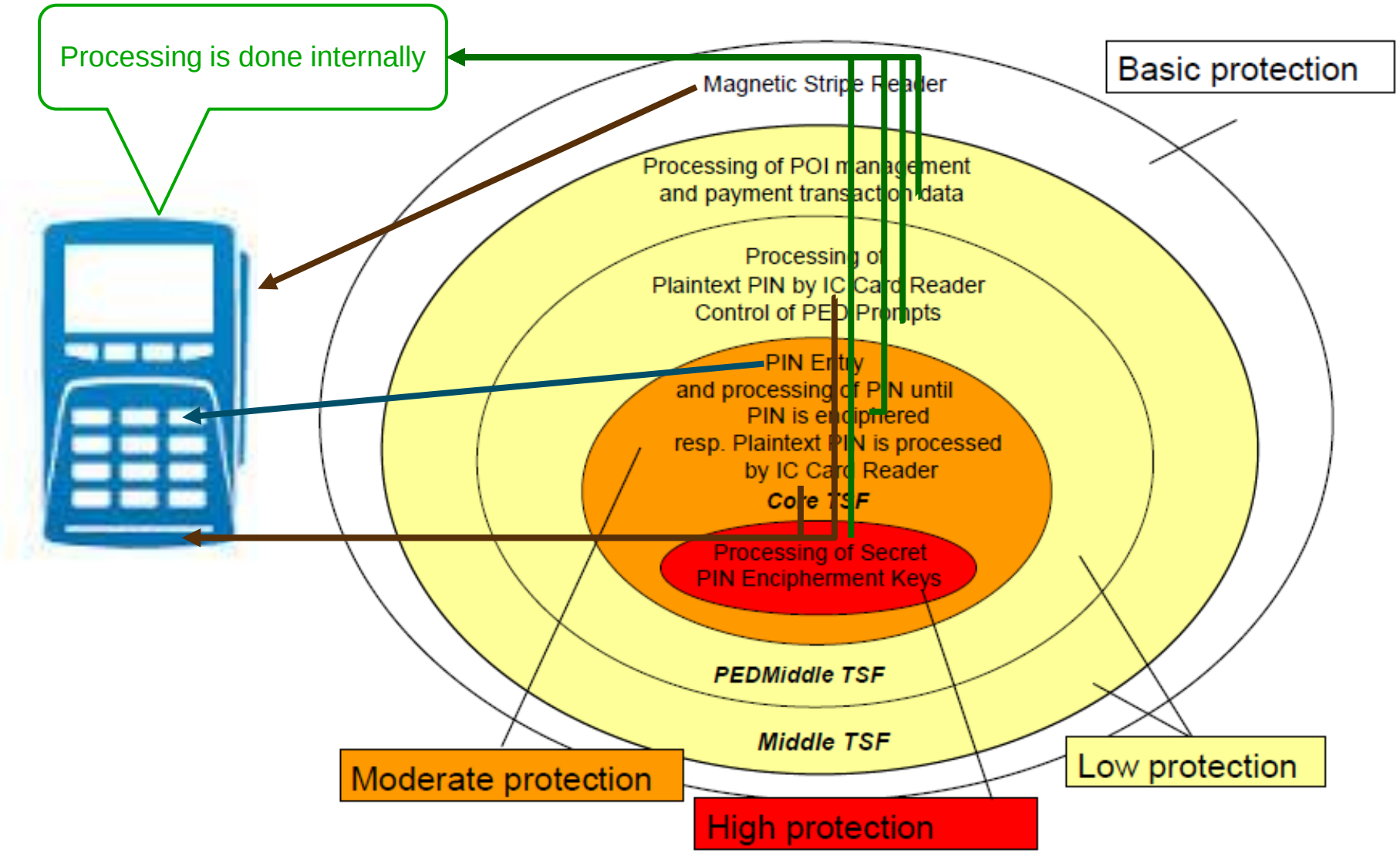
TA1.1.6 The tester shall develop attack scenario(s) to disable or defeat the tamper-detection mechanisms and insert a PIN-disclosing bug or gain access to secret information, which requires an attack potential of <25 per PED, exclusive of the ICC reader, for identification and initial exploitation. The attack potential value shall be based on the scheme depicted in Appendix B. The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.

- Activities
- Suggestions
- Evidence from developer
- Document assessment
- Special cases
- Vulnerability analysis
- Rating
- Penetration test

Creating Point of Interaction Protection Profile



POI PP – Build upon terminal architecture



POI PP – how it is build up (1)

- EAL POI
  - specific evaluation package,
  - built upon EAL2
  - Different assurance levels:
    - Higher protection -> higher assurance, including code review
    - Most important e.g. PIN encryption keys: EAL4 elements

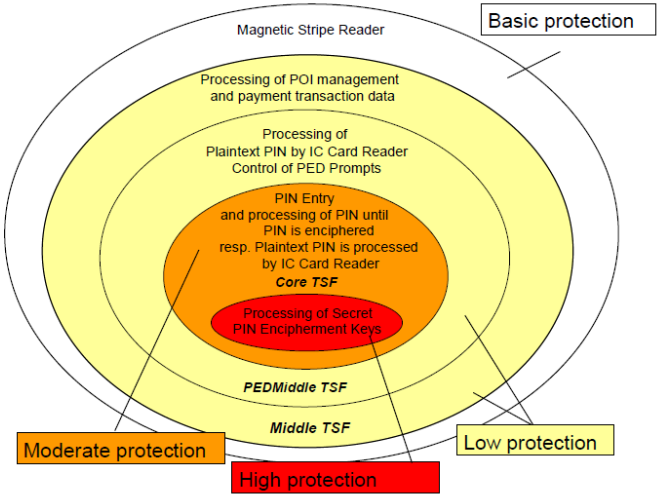
  Consequence

  Inside the TOE the boundaries between the different protection areas must be well defined, to clearly separate between these assurance levels

- ALC development environment made specific
  - ALC_DVS.2
  - including the site audit of Initial Key Loading facility

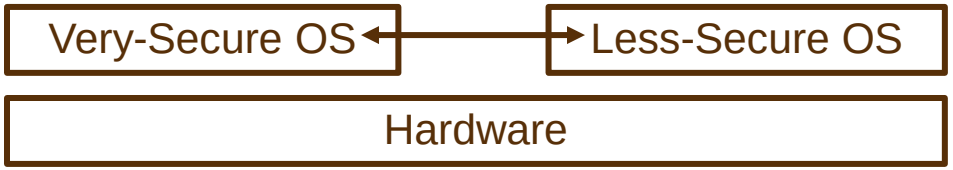
POI PP – how it is build up (2)

- Vulnerability analysis by AVA_POI (extended assurance requirement)
  - POI-High for Keys in Core TSF,
    - Processing of Secret PIN Encipherment Keys
  - POI-Moderate for Core TSF,
    - PIN Entry and processing of PIN until PIN is enciphered resp. Plaintext PIN is processed by IC Card Reader
  - POI-Low for PEDMiddle TSF, and Middle TSF
    - Processing of Plaintext PIN by IC Card Reader Control of PED, Prompts
  - POI-Basic for MSR
    - Processing Magnetic Stripe Reader data



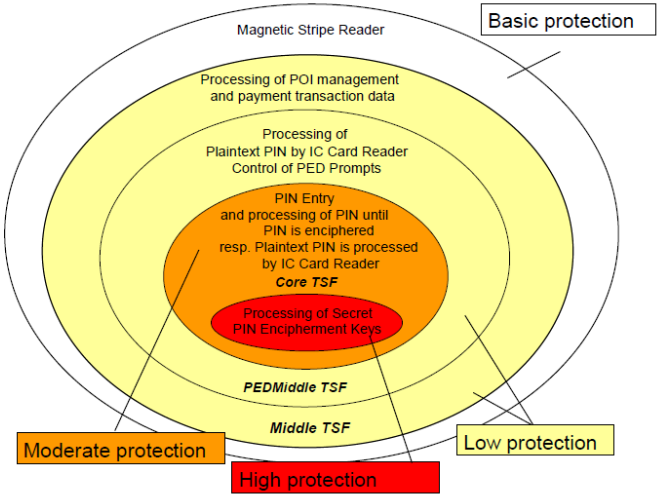
Difference Common Criteria – CAS/PCI

- Different EAL POI assurance levels are related attack potentials claimed in the CAS/PCI requirements.
- Common Criteria forces the developer to describe the design in terms of subsystems.
- The POI PP requires different attack potentials for the subsystems and therefore an attack potential of susbsystem interaction.



TOE Type Specific Assurance Methodology

- Most payment terminals are designed with PCI in mind
  - Thus have different attack potentials for different secure processes
  - Thus classical EAL packages would not fit
- The Common Criteria together with the POI PP enforces the developer to give a more clear picture of all interaction inside the TOE
- During the evaluation the interaction of the subsystems are tested more severely



Experience

- Domain specific legacy (PCI) comes into Common Criteria
- Different assurance levels
  - Be alerted as there is repetition of requirements
  - Fits well in the design philosophy of the developers
- Understanding the design
  - PCI is topic-based:

    "*handle a topic by finding an concluding argument*"

  - Common Criteria is model-based:

    "*before performing a vulnerability analysis a thorough understanding of the TOE is established*"

Questions?

Players

Smart Card people know a similar group: JHAS

- JTEMS: Joint Interpretation Library Terminal Evaluation Subgroup
  - European Banking Organizations representing banks EU countries
  - European Evaluation Labs
  - Dutch, UK, German and France CC Schemes
  - (occasionally) vendors

  Developed Point or Interaction Protection Profile (POI PP)

Joint Interpretation Library

- JIL: Collective EU Schemes; JTEMS reports to them

Common Approval Scheme
A EUROPEAN INITIATIVE FOR CARD PAYMENTS IN EUROPE

- CAS: Common Approval Scheme Initiative: Security group of European banks

OSeC

- OSeC: Steering group that organizes pilot for the POI PP

PCI Security Standards Council™

- PCI-SSC: Collaboration of credit card organization that defines
  - *What*: Payment terminal security requirements (since 2004)
  - *How*: Approval process for these requirements
  - *Who*: Which labs are allowed to perform evaluations