# PROJECT E:
# TRUSTED CAMERA

with some Common Criteria touch

# Our system

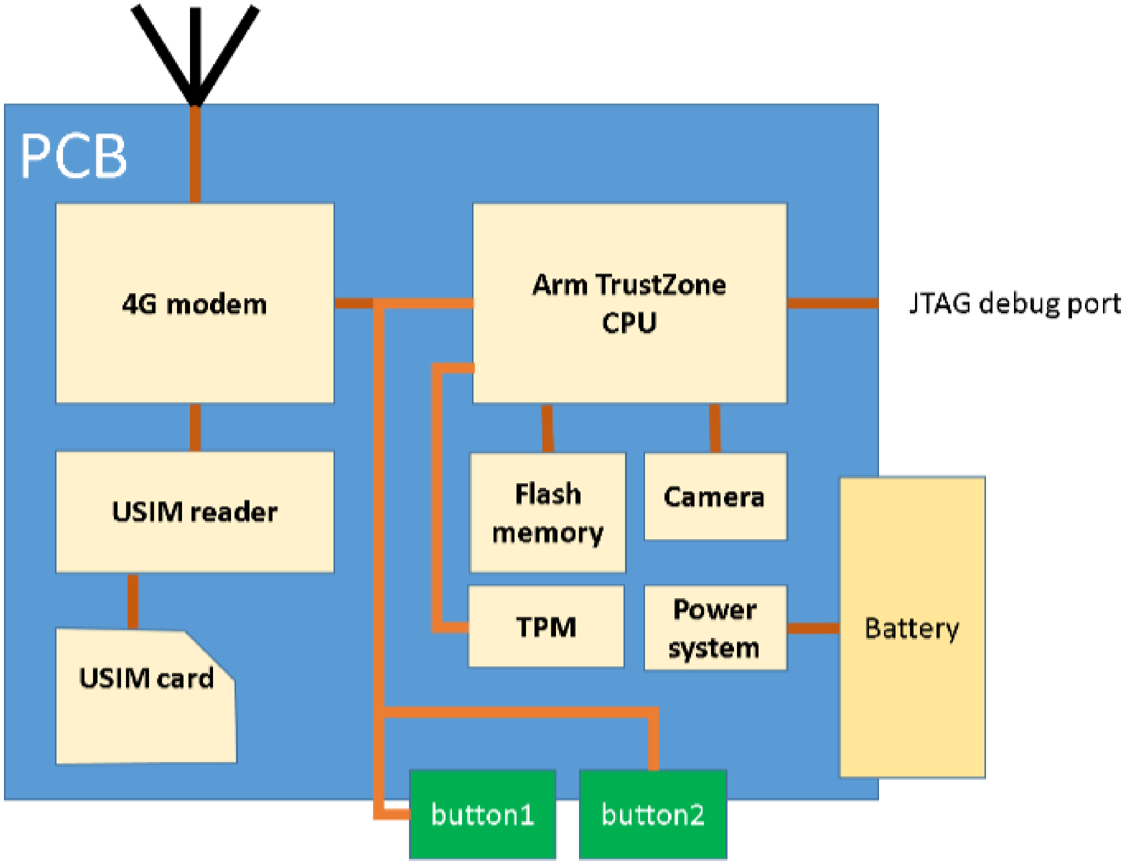


Figure 1: Trusted Camera components

# Our system under attack

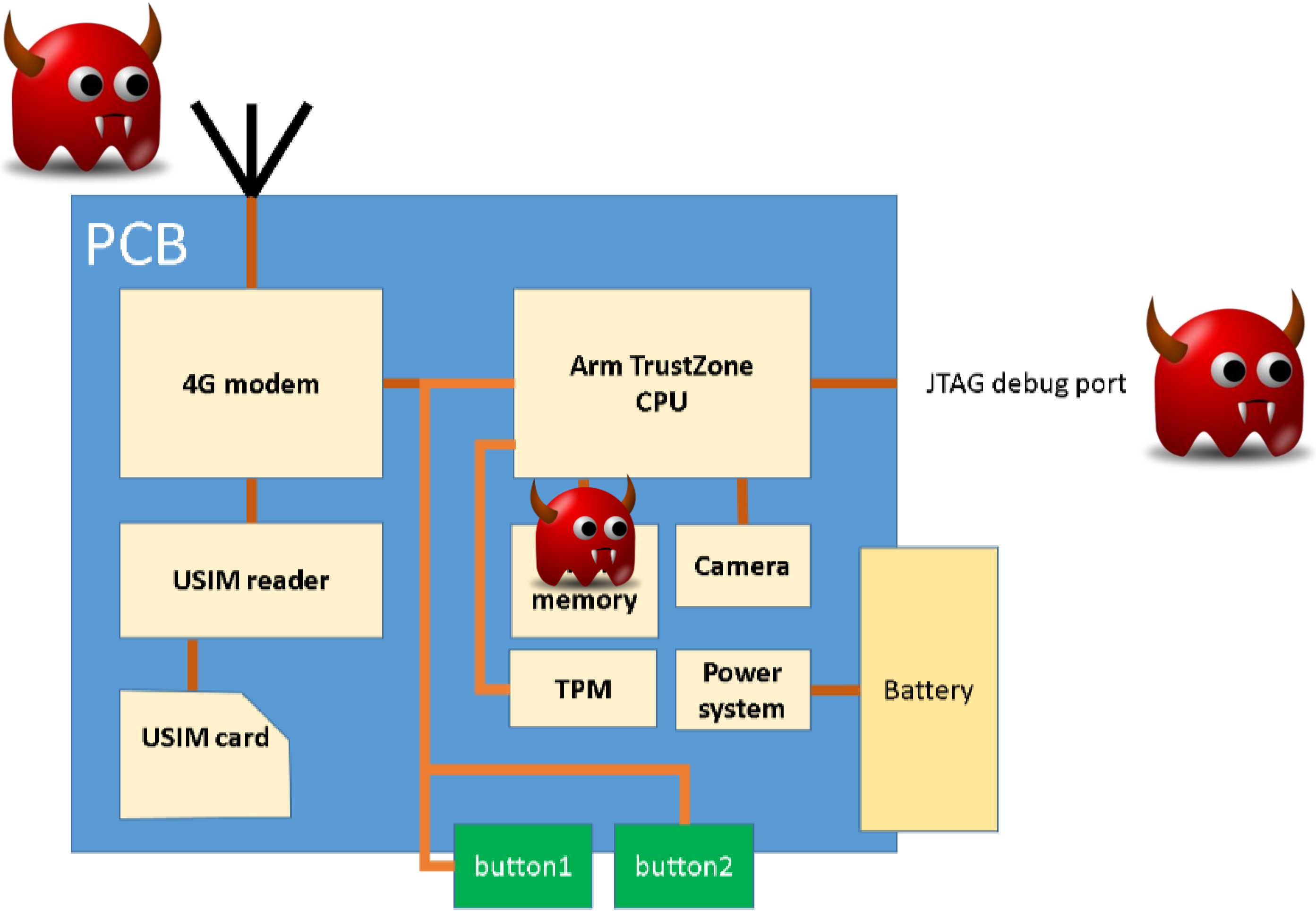


Figure 1: Trusted Camera components

# Task: design protection

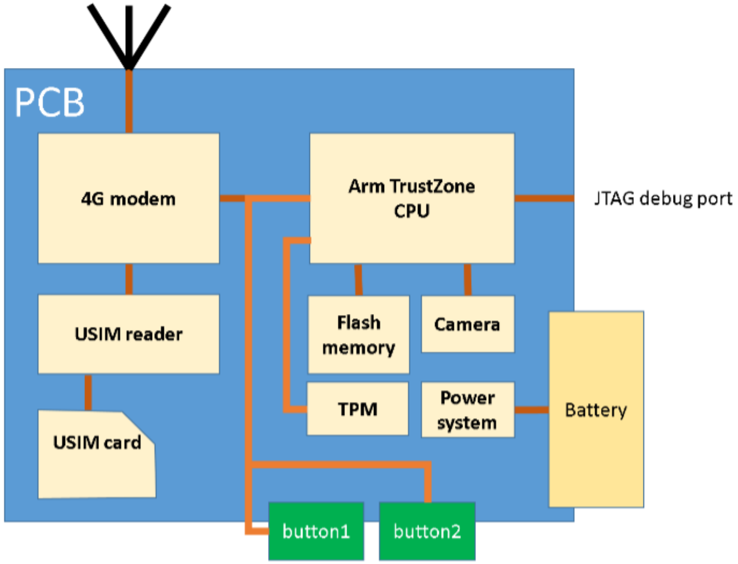


Figure 1: Trusted Camera components

## Protection against:

- Bugs in the (remote) management interface that allows one to insert executable foreign code.
- Loading of unauthorized firmware.
- Loading of SRTP keys of incorrect receiver.
- Opening camera device and replace flash memory contents with own code and configuration.
- Dishonest device repair personnel.
- Misuse of JTAG debug interface.
- Loss of key or compromised camera (fallen into the hands of a stranger).

# Analysis concepts: ST and TOE

Common Criteria uses the following useful concepts

## Security Target (ST)

A security target contains the IT security objectives and requirements of a specific identified TOE and defines the functional and assurance measures offered by that TOE to meet stated requirements.

For a brief intro to CC see link below.

http://www.fmv.se/Global/Dokument/Verksamhet/CSEC/ccintroduction.pdf

## Target of Evaluation (TOE)

**TOE Description** provides context for the evaluation.  The description may be a set of assumptions, and may describe the application context for compliant TOEs. Example smart card TOE in document below.

http://www.commoncriteriaportal.org/files/ppfiles/scsugpp.pdf

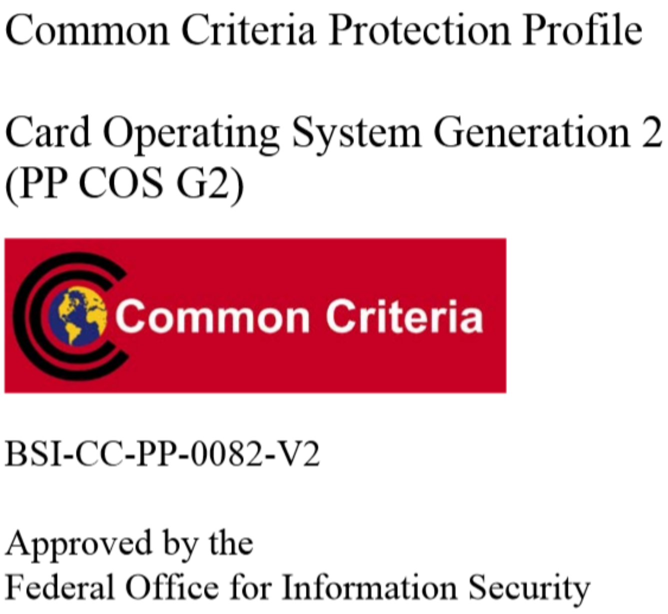
# Protection Profile

A protection profile defines an implementation-independent set of security requirements and objectives for a category of products or systems which meet similar consumer needs for IT security.

A PP is intended to be reusable and to define requirements which are known to be useful and effective in meeting the identified objectives.

The PP concept has been developed to support the definition of functional standards, and as an aid to formulating procurement specifications.

An ST may claim conformance to one or more PPs.



Common Criteria Protection Profile

Card Operating System Generation 2
(PP COS G2)

BSI-CC-PP-0082-V2

Approved by the
Federal Office for Information Security

# Security Objectives

These reflect the stated intent to counter identified threats and/or  comply with any organizational security policies.  Security objectives

for both the TOE and for the

environment are included, and **traced back to threats, policies or assumptions**.

| Threats | Assumption | Counter Measure 1 | Counter Measure 2 |
|---|---|---|---|
| 1 | x | | |
| 2 | | x | |
| 3 | | x | x |
| 4 | | x | x |

# TOE Security Environment

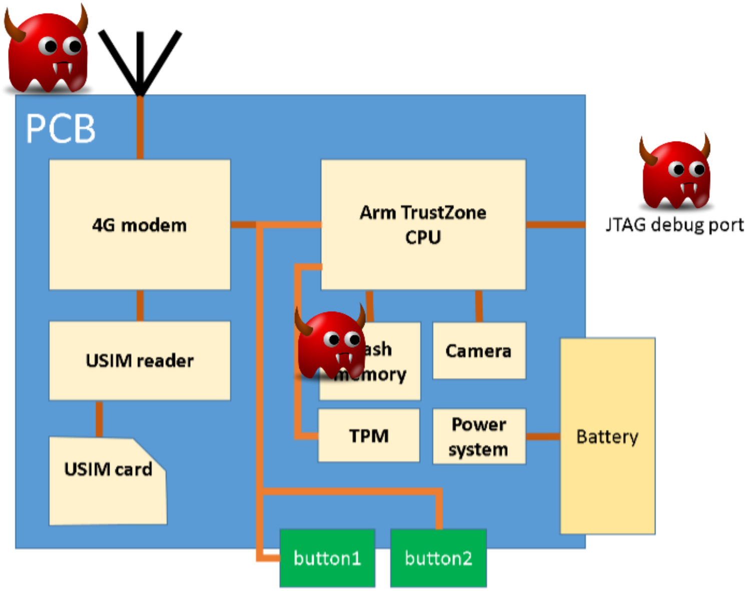


Figure 1: Trusted Camera components

This is a narrative statement of the security problem to be solved by the TOE. It describes the security aspects of the environment in which the TOE is intended to be used. It will address:

**assumptions:**

describe the security aspects of the environment in which the TOE is intended to be used, including physical, personnel and connectivity aspects of the environment

**threats:**

the anticipated threats to the IT assets, even those not countered by the TOE. The threat is described in terms of the agent, the attack and the subject of the attack

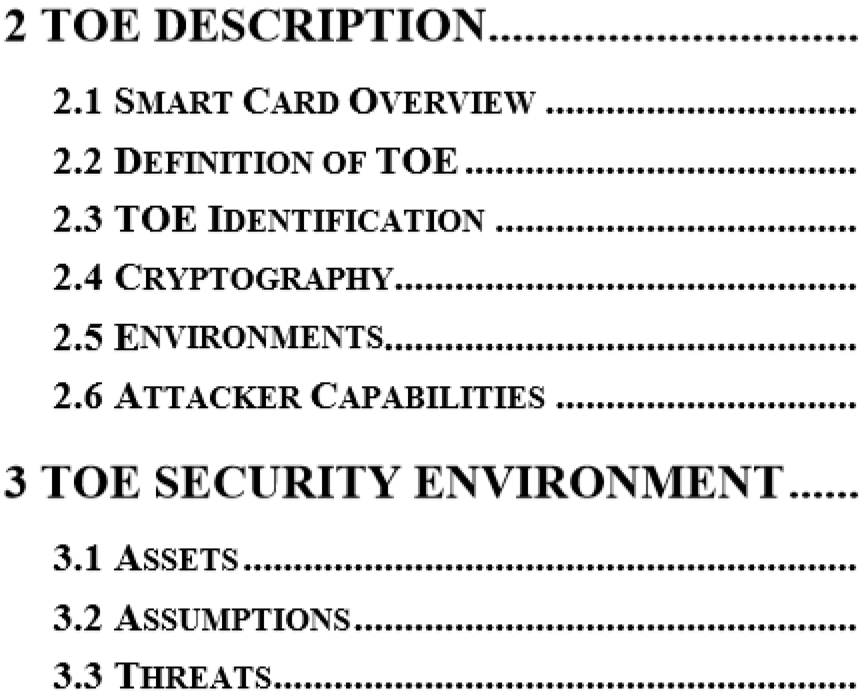
**organizational security policies:**

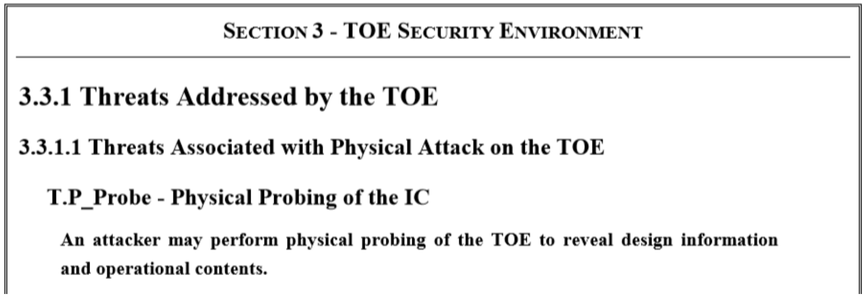
identify any rules with which the TOE must comply.

# Also in TOE

- **Description of the assets**
  - The things you want to protect

- **Description of attacker capabilities**
  - Often a rationale that limits the capabilities in the context of the use of the product





SECTION 3 - TOE SECURITY ENVIRONMENT

**3.3.1 Threats Addressed by the TOE**

**3.3.1.1 Threats Associated with Physical Attack on the TOE**

**T.P_Probe - Physical Probing of the IC**

An attacker may perform physical probing of the TOE to reveal design information and operational contents.

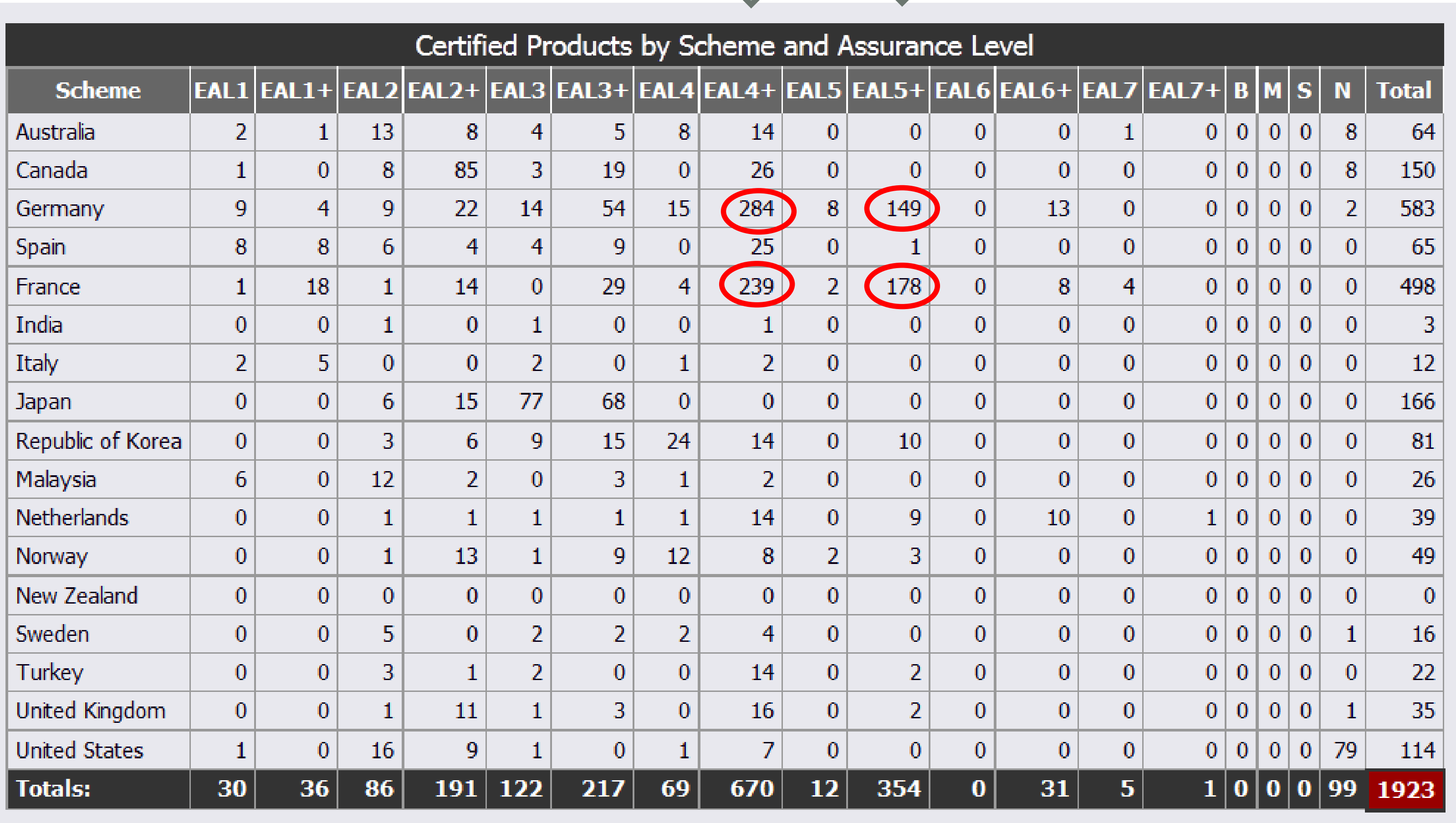
# Seven EAL levels

| Level | Description |
|---|---|
| EAL1 | functionally tested |
| EAL2 | structurally tested |
| EAL3 | methodically tested and checked |
| EAL4 | methodically designed, tested and reviewed |
| EAL5 | semiformally designed and tested |
| EAL6 | semiformally verified design and tested |
| EAL7 | formally verified design and tested |

e.g CitrixXenServer

smartcards

# Stats of products at EALx



Certified Products by Scheme and Assurance Level

| Scheme | EAL1 | EAL1+ | EAL2 | EAL2+ | EAL3 | EAL3+ | EAL4 | EAL4+ | EAL5 | EAL5+ | EAL6 | EAL6+ | EAL7 | EAL7+ | B | M | S | N | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Australia | 2 | 1 | 13 | 8 | 4 | 5 | 8 | 14 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 8 | 64 |
| Canada | 1 | 0 | 8 | 85 | 3 | 19 | 0 | 26 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 8 | 150 |
| Germany | 9 | 4 | 9 | 22 | 14 | 54 | 15 | 284 | 8 | 149 | 0 | 13 | 0 | 0 | 0 | 0 | 0 | 2 | 583 |
| Spain | 8 | 8 | 6 | 4 | 4 | 9 | 0 | 25 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 65 |
| France | 1 | 18 | 1 | 14 | 0 | 29 | 4 | 239 | 2 | 178 | 0 | 8 | 4 | 0 | 0 | 0 | 0 | 0 | 498 |
| India | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 |
| Italy | 2 | 5 | 0 | 0 | 2 | 0 | 1 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 12 |
| Japan | 0 | 0 | 6 | 15 | 77 | 68 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 166 |
| Republic of Korea | 0 | 0 | 3 | 6 | 9 | 15 | 24 | 14 | 0 | 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 81 |
| Malaysia | 6 | 0 | 12 | 2 | 0 | 3 | 1 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 26 |
| Netherlands | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 14 | 0 | 9 | 0 | 10 | 0 | 1 | 0 | 0 | 0 | 0 | 39 |
| Norway | 0 | 0 | 1 | 13 | 1 | 9 | 12 | 8 | 2 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 49 |
| New Zealand | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Sweden | 0 | 0 | 5 | 0 | 2 | 2 | 2 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 16 |
| Turkey | 0 | 0 | 3 | 1 | 2 | 0 | 0 | 14 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 22 |
| United Kingdom | 0 | 0 | 1 | 11 | 1 | 3 | 0 | 16 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 35 |
| United States | 1 | 0 | 16 | 9 | 1 | 0 | 1 | 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 79 | 114 |
| **Totals:** | **30** | **36** | **86** | **191** | **122** | **217** | **69** | **670** | **12** | **354** | **0** | **31** | **5** | **1** | **0** | **0** | **0** | **99** | **1923** |

# Trusted Camera project

- Look at the system and its life-cycle

- Define the ST and TOE:
  - the threats you consider, assumptions, etc

- Make a design for the protection functions
  - Likely you need to decide if you have a professional camera or a consumer product. (i.e. acceptable cost level, repair, product warrantee (cost), etc)

- Check if your design is good
  - That is, it deals with all threats and not over-engineered

# Project execution

Your group will need to provide the following deliverables in:

1. **Latest 2017-10-19:** First submission in PDF form
2. **Latest 2017-10-25:** Submit your two review reports
3. **Latest 2017-10-28:** Mail final report bundle via urkund Ben.

NOTE: The deadlines are subject to late changes so check always the course home page.

# Peer reviewing by two groups

Use portal https://eitn50.eit.lth.se:3119

Only group leader can login.

Keep deadlines!!!

An update of the project description will follow on October 25 with more detailed instruction how to do grading.