RED ALERT LABS
IoT Security


# TrustBoost Training Day 4:

# Common Criteria Training

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.

12/11/2024

# AGENDA

**INTRODUCTION TO CC**

CC DEFINITION & HISTORY

CC SCHEMES

EUCC CANDIDATE SCHEME

**PART 1: INTRODUCTION TO CC (ISO/IEC 15408)**

CC FACTS

CC KEY DEFINITIONS

DOCUMENTATION

**PART 2: CERTIFICATION PROCESS**

PHASE 1: PREPARATION

PHASE 2: CONDUCT

PHASE 3: RECOVER & FINALIZE


01

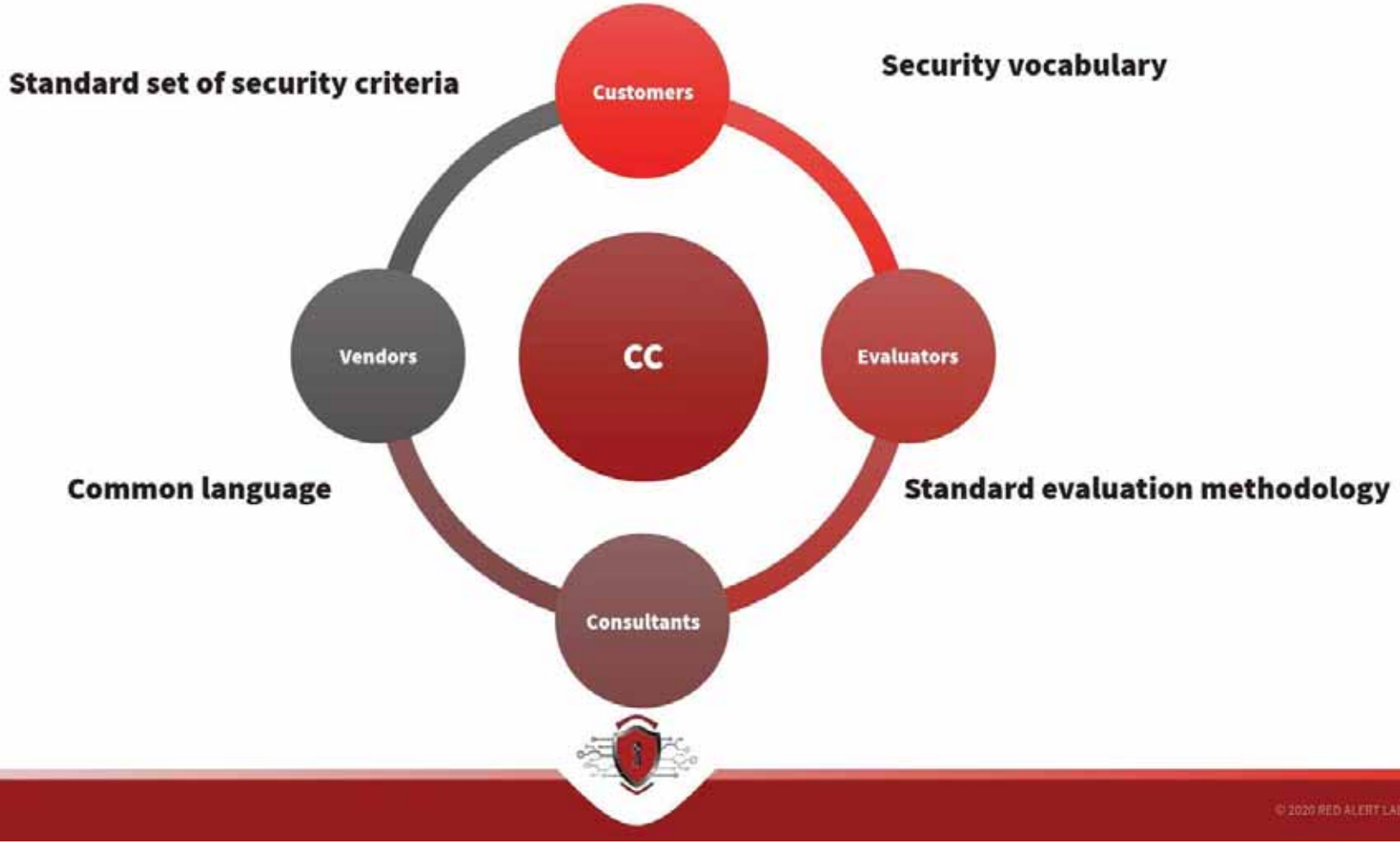
# INTRODUCTION TO CC

# WHAT IS CC ? DEFINITION

**To Product Managers:** CC is nothing but a “checkbox” tool procurement requirement. A crucial step to penetrate some markets.

**To Security Experts:** CC is an internationally recognized framework to describe and evaluate security attributes of an IT product/system. It is a way for customers to gain confidence in the product’s ability to resist cyber attacks

# WHAT IS CC ? DEFINITION



# What is CC ? Brief History

TCSEC – U.S.
(Orange Book)
1985

U.K. Confidence
Levels
1989

German Criteria

French Criteria

Canadian Criteria
1993

Federal Criteria
Draft 1993

ITSEC
1991

SOGIS

CYBERSECURITY
CERTIFICATION

Common Criteria

- v1 in 1996
- v2 in 1998
  → ISO 15408 in 1999
- v2.3 in 2005
- v3.0 in 2005 (obsolete)
- v3.1 in 2006
- v3.1R3 in 2009
- v3.1R4 in 2012
- v3.1R5 in 2017
- CC 2022 in 2022

# WHAT IS CC ? INTERNATIONAL ORGANIZATION

**Common Criteria Mutual Recognition Agreement (CCRA)**

States the conditions for participation including the requirements that each member country recognize certificates issued from other member countries.

Every member country has a CC governing body or Scheme responsible for managing the implementation and use of the CC in their country.

## ADVANTAGES:

- Avoids multiple certifications
- Easier product comparison
- Simplifies the expression of national or industry requirements

# WHAT IS CC ? SCHEMES

- Schemes often add their own policies and rules
- Some schemes have a direct influence on procurement (e.g. US)
- Others are more scientific in nature and make recommendations (Germany & France)
- US scheme has dominated the CC direction the last 6 years

- Each country's program for implementing and validating CC evaluations
- Each Schemes acts independently, with mutual criteria
- Schemes assign validators or certifiers (often not employees of govt)
- Schemes authorize labs to evaluate on their behalf

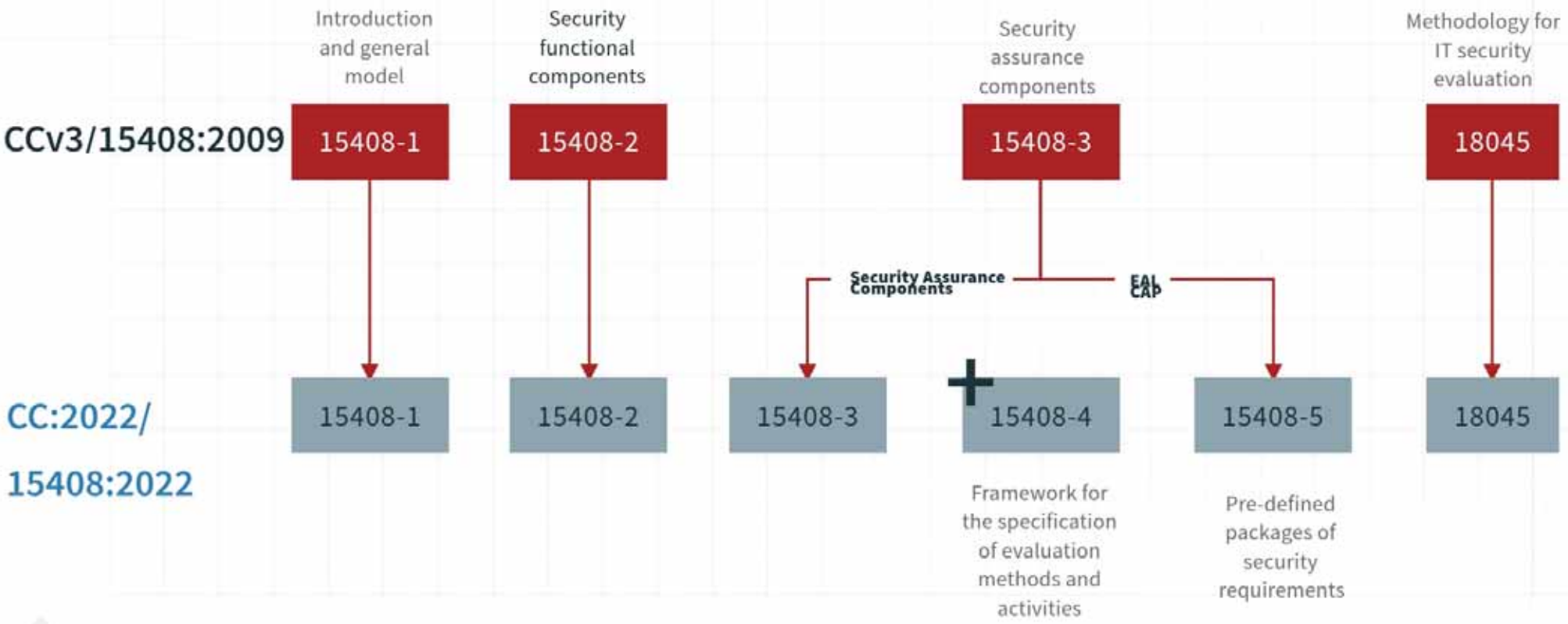
 


02

# PART 1: INTRODUCTION TO CC (ISO/IEC 15408)

## CC Facts

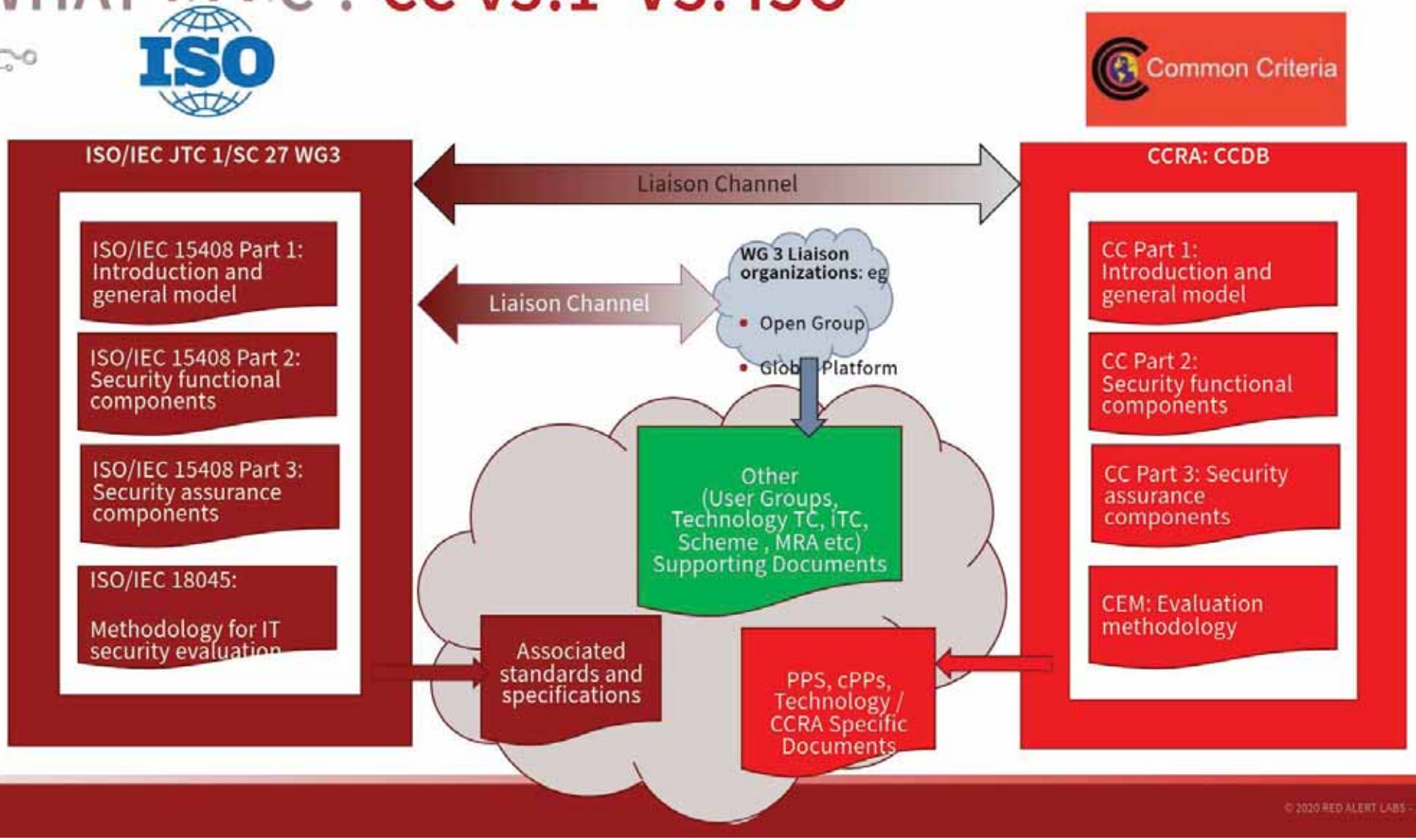
# WHAT IS CC ? CC FRAMEWORK



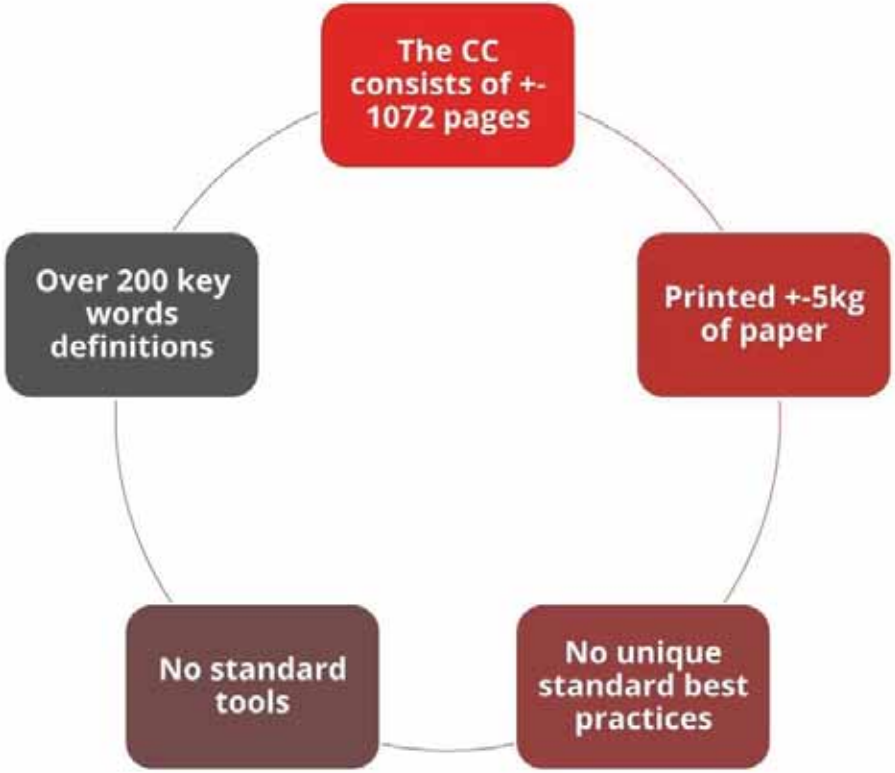



RED ALERT LABS
IoT Security

# WHAT IS CC ? CC v3.1 VS. ISO



# CC FACTS COMPLEXITY OF THE CC



# CC FACTS
# NEW CCRA/ MUTUAL RECOGNITION TERMS

# CC FACTS ICCC & ITC

## ICCC:

- The International Common Criteria Conference (ICCC) is the annual conference hosted by one of the Common Criteria Mutual Recognition Agreement (CCRA) member nations.
- Its purpose is to share information about Common Criteria-related activities including new development, applications of CC, and new opportunities

## iTC:

- Open technical community that defines appropriate Standards (GP plus CCRA Nations and anyone else)
- Produces Terms of Reference & workplan
- Push CCRA nations for position statements
- Develop cPP & supporting docs developed by iTC
- Liaises with CCDB to inform progress & endorsement

# CC FACTS
# COLLABORATIVE PROTECTION PROFILES (CPPS)

**A Protection Profile collaboratively developed by an international Technical Community endorsed by the CCMC.**

**A cPP and related Supporting Documents defines the minimum set of common security functional requirements and the achievable common level of security assurance.**

**It addresses vulnerability analysis requirements to ensure certified products reach an Achievable Common Level of Security Assurance.**

- Collaboration with industry
- Raise security level of COTS
- Reduce costs and time
- Objective, testable and repeatable tests
- use "Tailored Assurance" that is assurance activities are designed for the technology vs using generic EAL's

# Question time

- ✔ Question #1
  What does CC part 3 cover?
- ✔ Question #2
  What is a cPP?
- ✔ Question #3
  What is the difference between Certificate Authorizing Schemes and Certificate Issuing Schemes ?



RED ALERT LABS
IoT Security

# Answer

- ✔ What does CC part 3 cover?

  States a set of Security Assurance Requirements related to the product's development

- ✔ What is a cPP?

  COLLABORATIVE PROTECTION PROFILES

- ✔ What is the difference between Certificate Authorizing Schemes and Certificate Issuing Schemes ?

  Certificate Authorizing Schemes: These are organizations or national bodies authorized (like ANSSI, NCSC, ...) by the mutual recognition agreements (such as CCRA, and SOGIS-MRA) to endorse the validity of certifications for recognition across member countries.

  Certificate Issuing Schemes: These refer to the national certification bodies that actually issue the certificates following the evaluation process conducted by accredited labs.



RED ALERT LABS
IoT Security

# CC FACTS COSTS (INVESTMENTS)

- EVALUATION LAB
- CC CONSULTANCY
- IN-HOUSE EVIDENCE DEVELOPMENT
- SITE VISIT EXPENSES
- TRAVEL EXPENSES
- EQUIPMENT COSTS
- LOST OPPORTUNITY
- CERTIFICATION SCHEME (ANSSI -> FREE, BSI -> 2,5K€ TO 12K€)

**TOTAL COSTS**

→ EVALUATION LAB FEES:

- EAL 2: 80K€ → 150 K€
- EAL 3: 120K€ → 200 K€
- EAL 4: 150K€ → 300 K€

# CC FACTS TIME ESTIMATES

| EAL Level | Evaluation Times |
|---|---|
| EAL 2 | 4 – 6 months |
| EAL 3 | 6 – 9 months |
| EAL 4 | 7 – 12 months |
| >EAL 4 | 12 – 24 months |

- Most of the time is spent on:

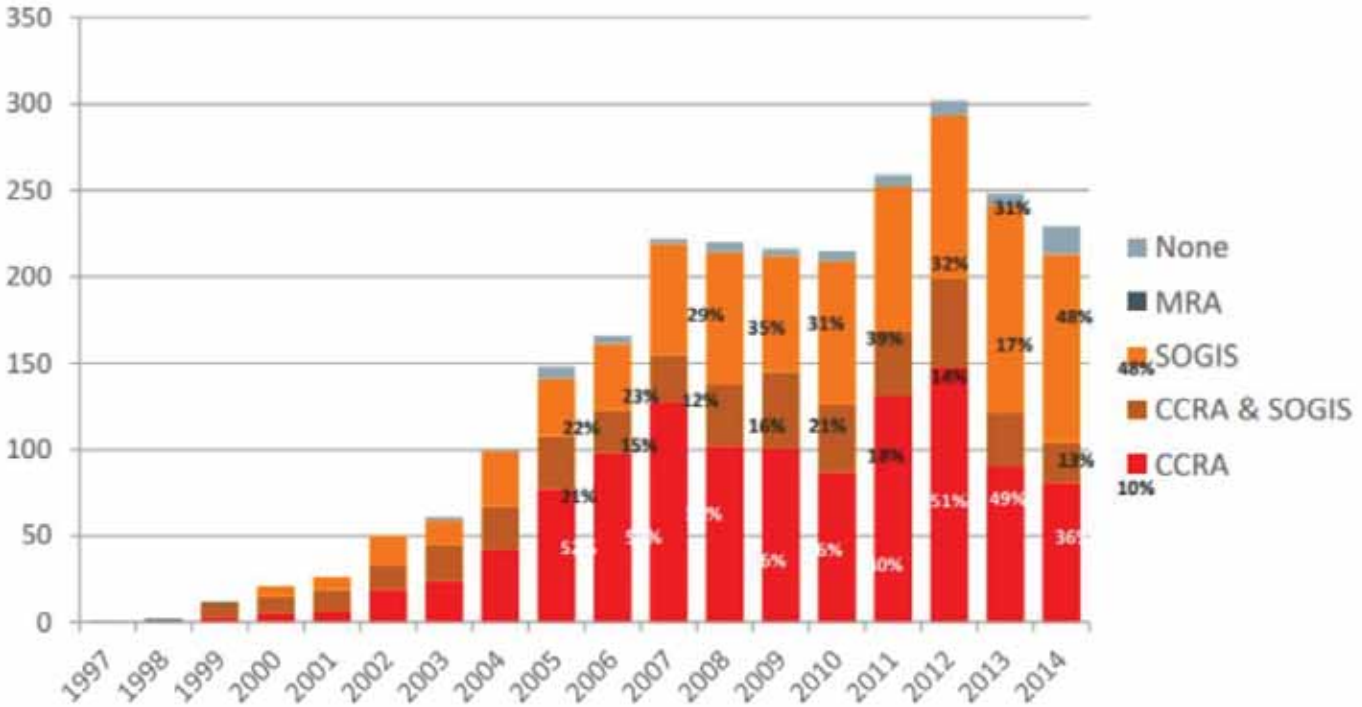
  ASSEMBLING THE RAW TECHNICAL INFORMATION

  FORMATTING DOCUMENTATION FOR THE CC EVALUATORS (IF NO CC CONSULTANT)

  DEVELOPING SPECIAL TEST CASES

  RESPONDING TO CC EVALUATOR'S QUESTIONS

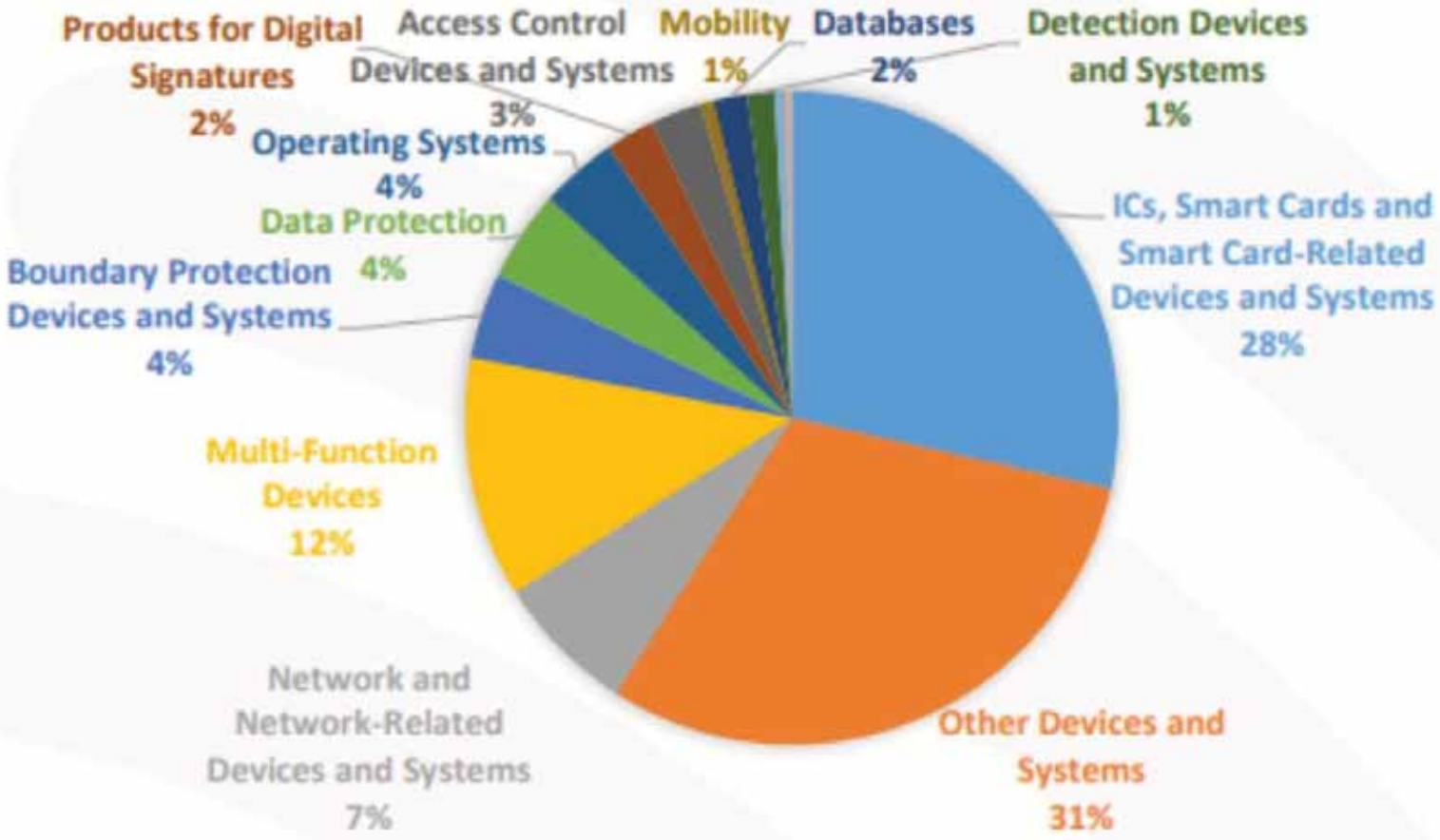
# CC FACTS MUTUAL RECOGNITIONS




46% for CCRA, 34% total for SOGIS.
More SOGIS than CCRA in 2013 and 2014.

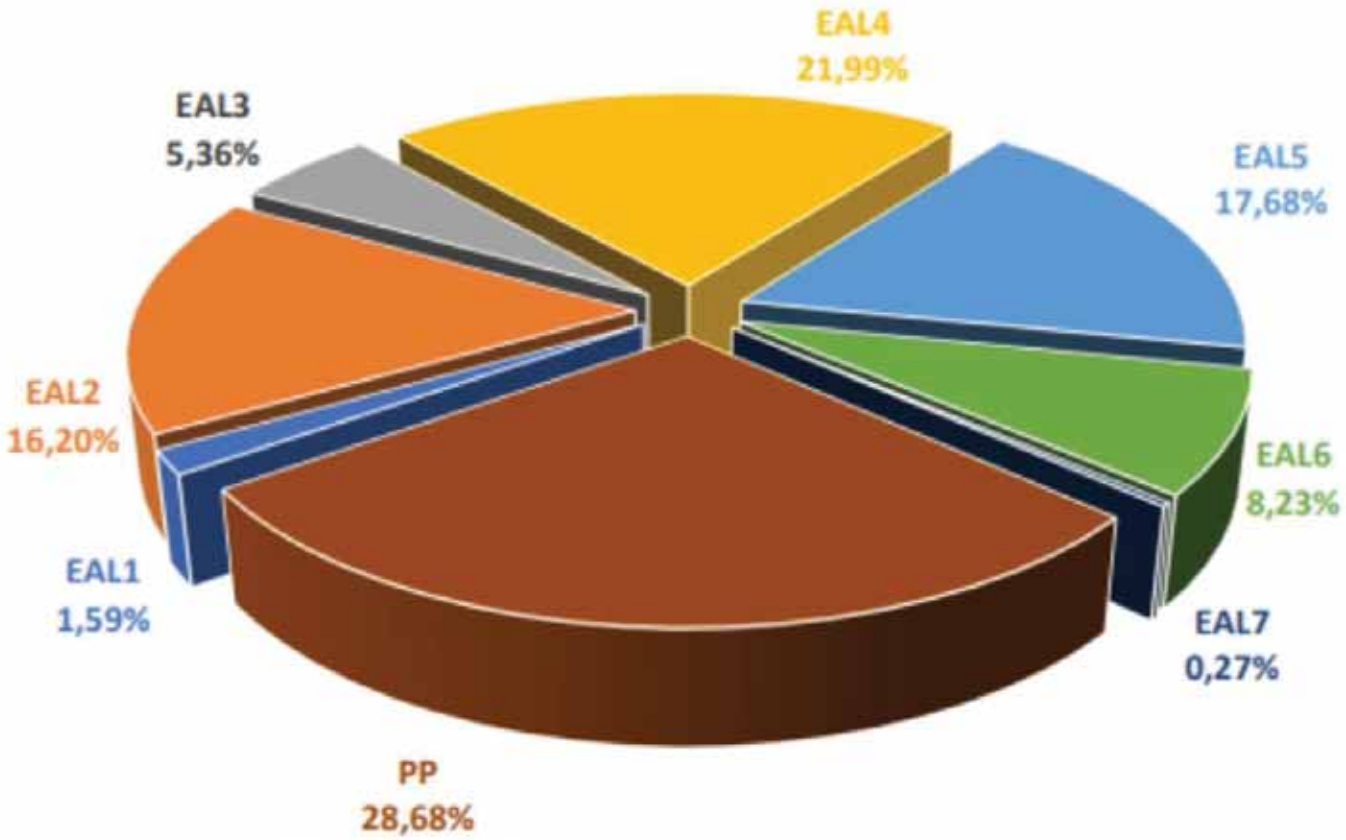
Source: ICCC 15 Presentation – Oracle : 18 Years of Common Criteria Certification Evaluation Trends from a Global Perspective.

# CC FACTS CERTIFIED TYPES OF PRODUCTS




Source: jtsec report - 2023 CC Statistics Report.pdf

# CC FACTS Most used assurance levels in the last 5 years

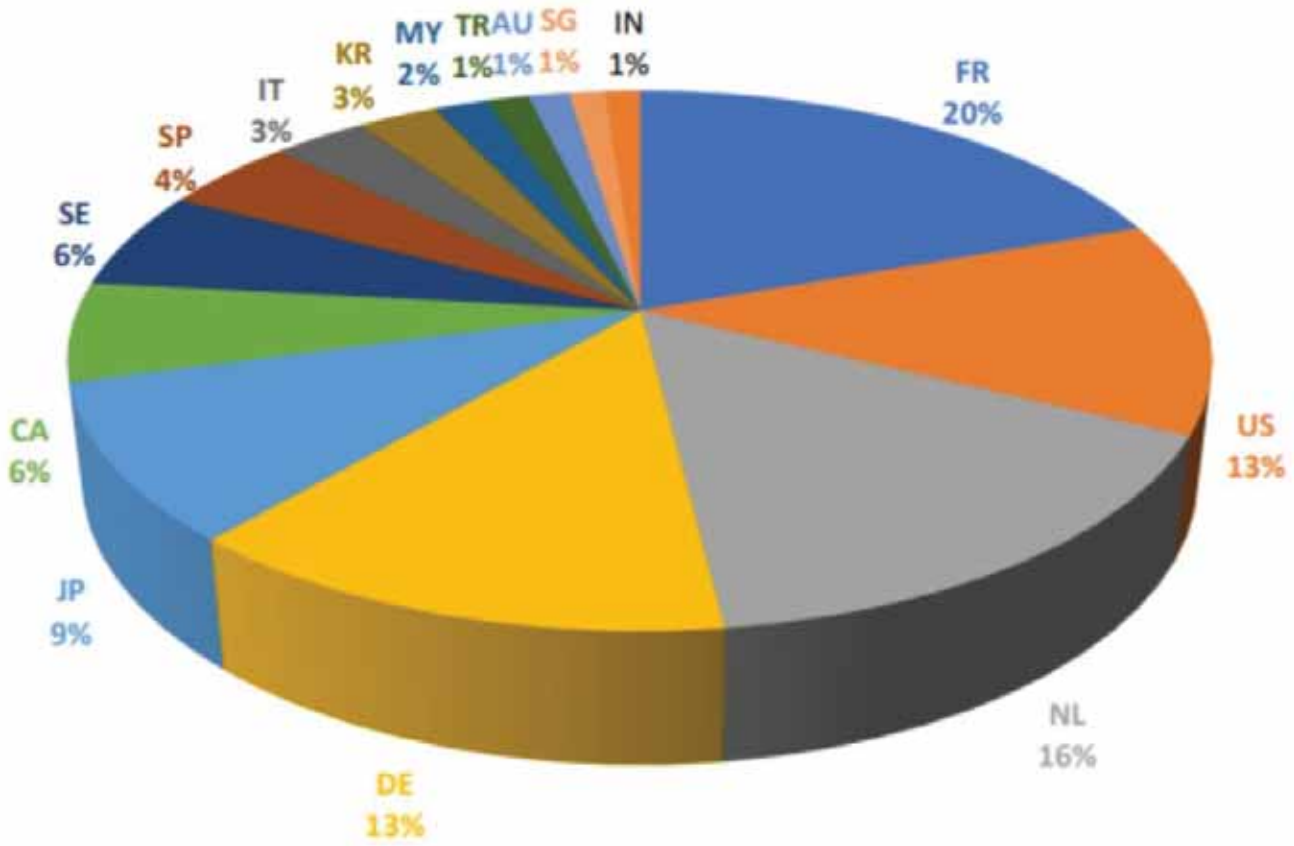



Source: jtsec report – 2023 CC Statistics Report.pdf

# CC FACTS Total number of certified products by year

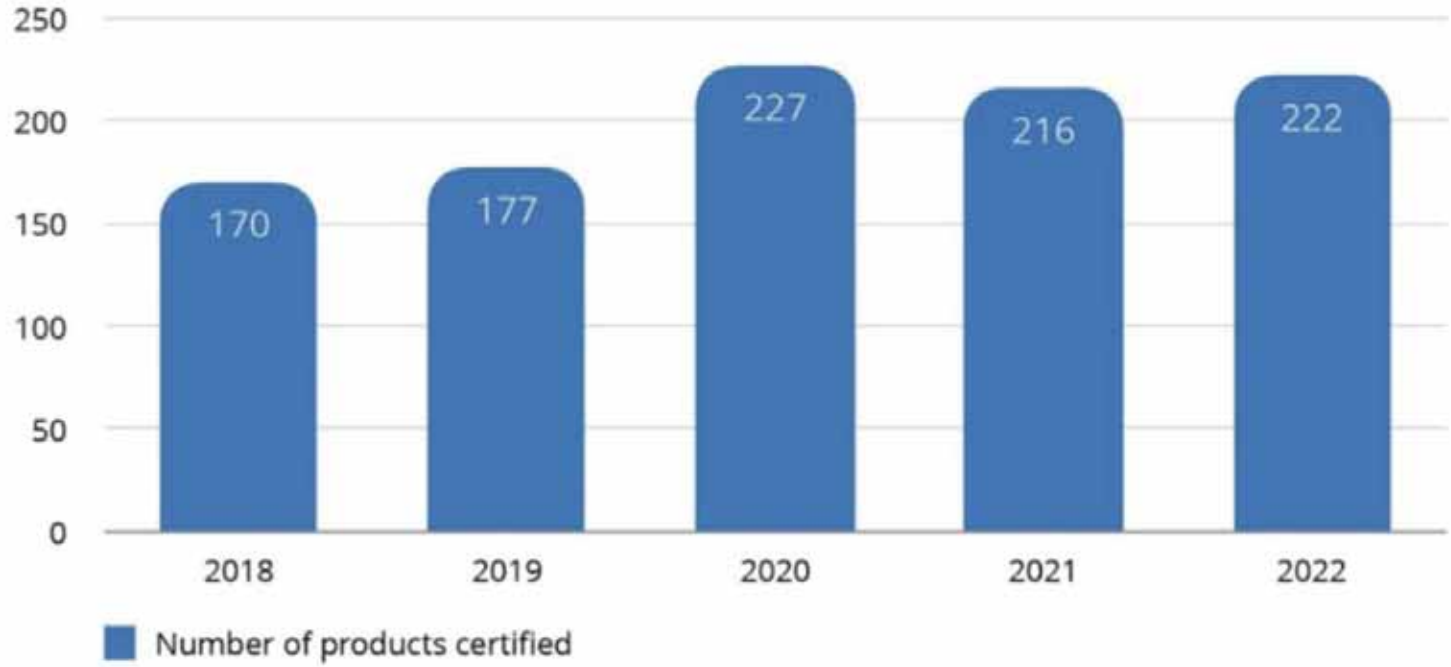

Source: jtsec report – 2023 CC Statistics Report.pdf

# CC FACTS Top certifying schemes in the last 5 years




Source: jtsec report – 2023 CC Statistics Report.pdf

# CC FACTS Certified products in the European Union up to 2022



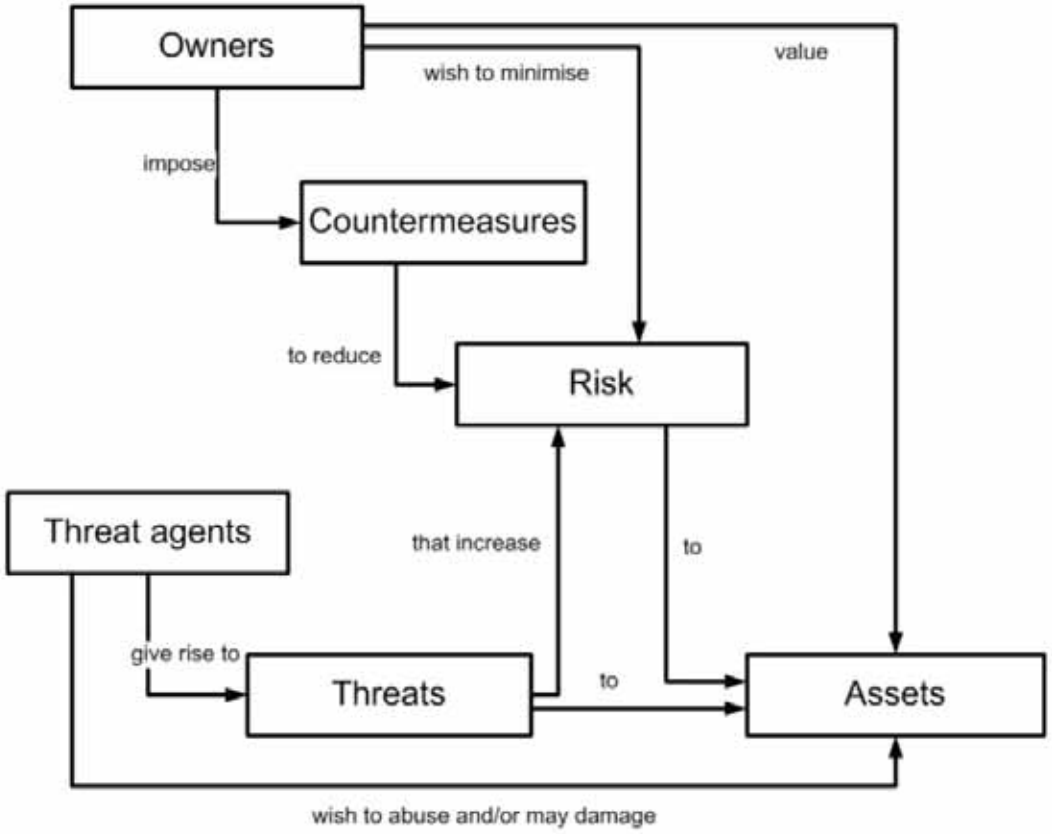

Source: ENISA: Market of Cybersecurity Assessments - Jan 31, 2024




# PART 1: INTRODUCTION TO CC (ISO/IEC 15408)

## CC Key Definitions

# CC KEY DEFINITIONS CC SECURITY CONCEPT



# CC KEY DEFINITIONS EVALUATION VS. CERTIFICATION

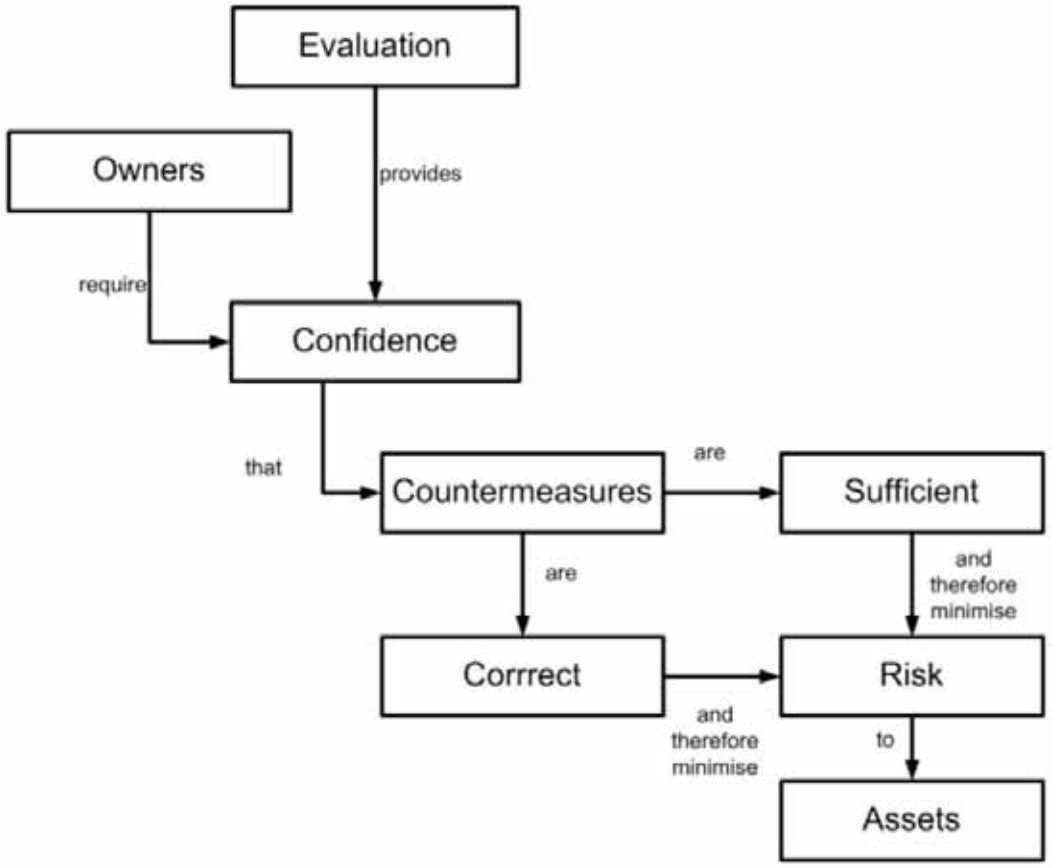
## EVALUATION

Examination of evidence by independent, accredited third-party testing laboratories.

## CERTIFICATION

(or VALIDATION) – marks the final, official completion of a successful Common Criteria EVALUATION.

# CC KEY DEFINITIONS EVALUATION PROCESS



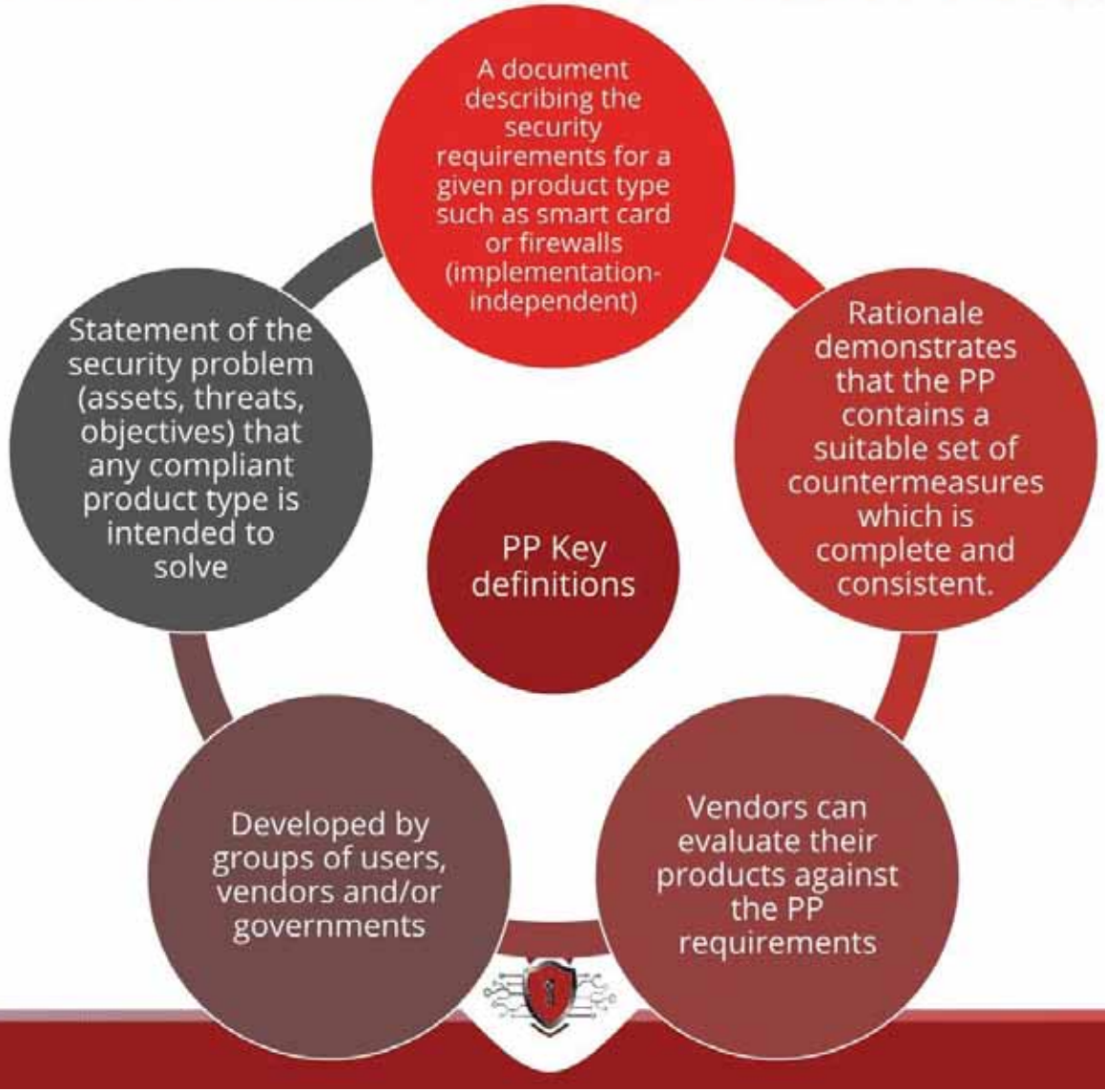

"A detailed exam of the security aspects of an IT system or product performing in parallel the necessary tests to assure that it works correctly, it is effective and it doesn't show any logical vulnerability".

# CC KEY DEFINITIONS TARGET OF EVALUATION (TOE)

- The TOE is the focus of the evaluation.
- It is generally a subset of a product containing all of the security-relevant functionality.
- TOE boundary sets the physical and logical limits of the evaluation.

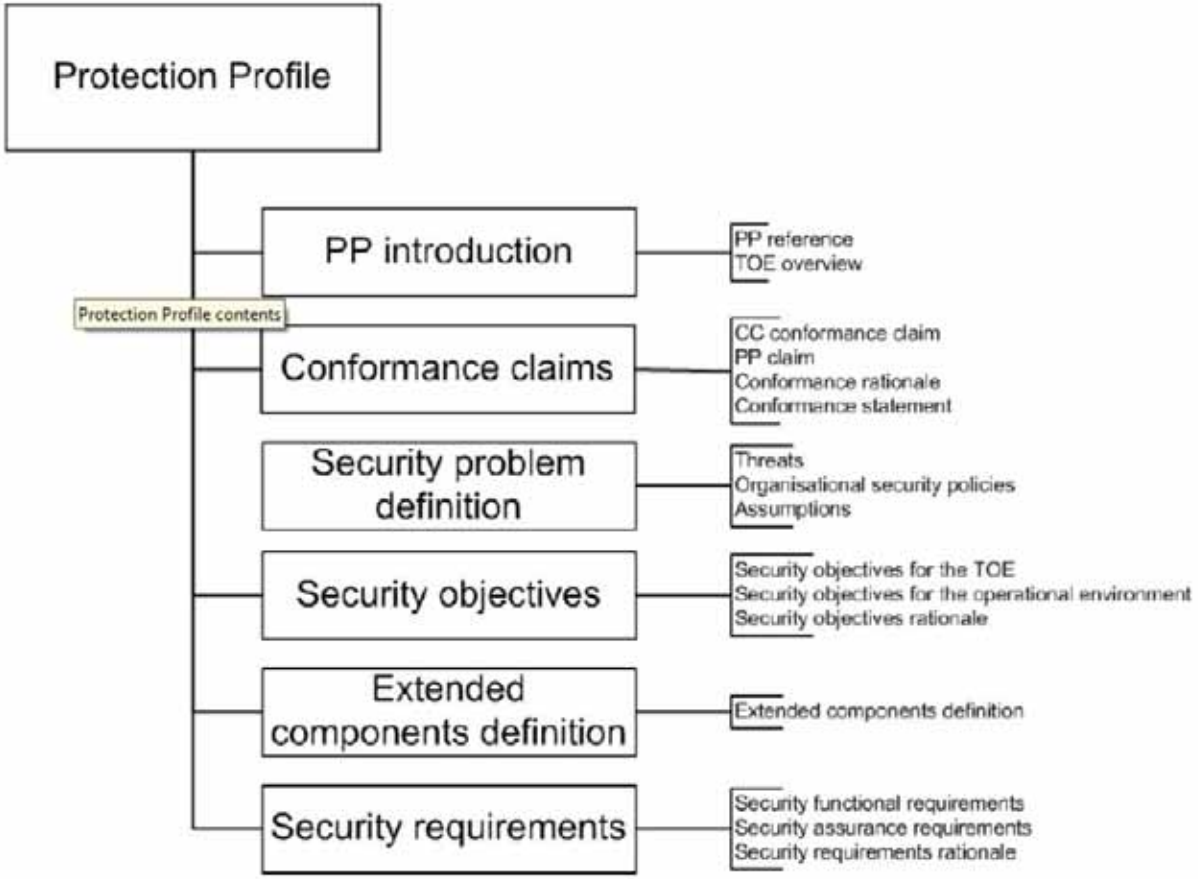
 

# CC KEY DEFINITIONS PROTECTION PROFILE (PP)



# CC KEY DEFINITIONS PROTECTION PROFILE

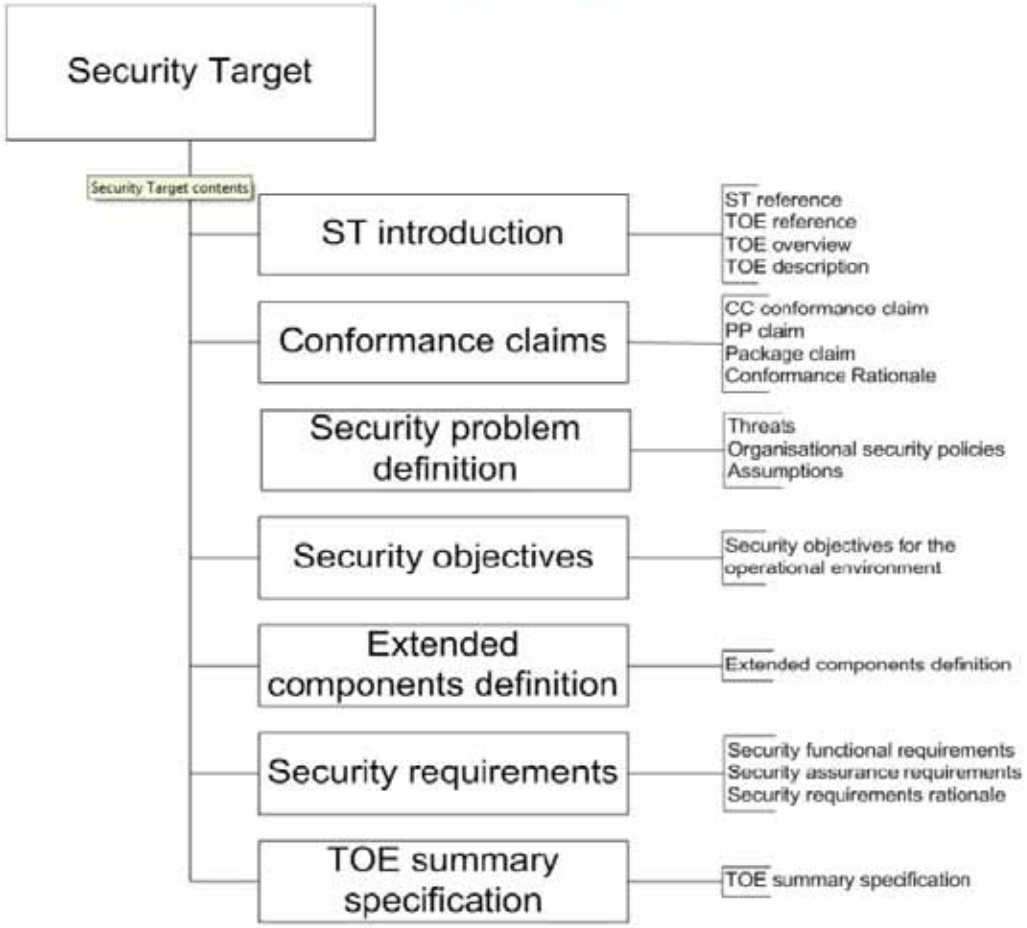


# CC KEY DEFINITIONS SECURITY TARGET (ST)

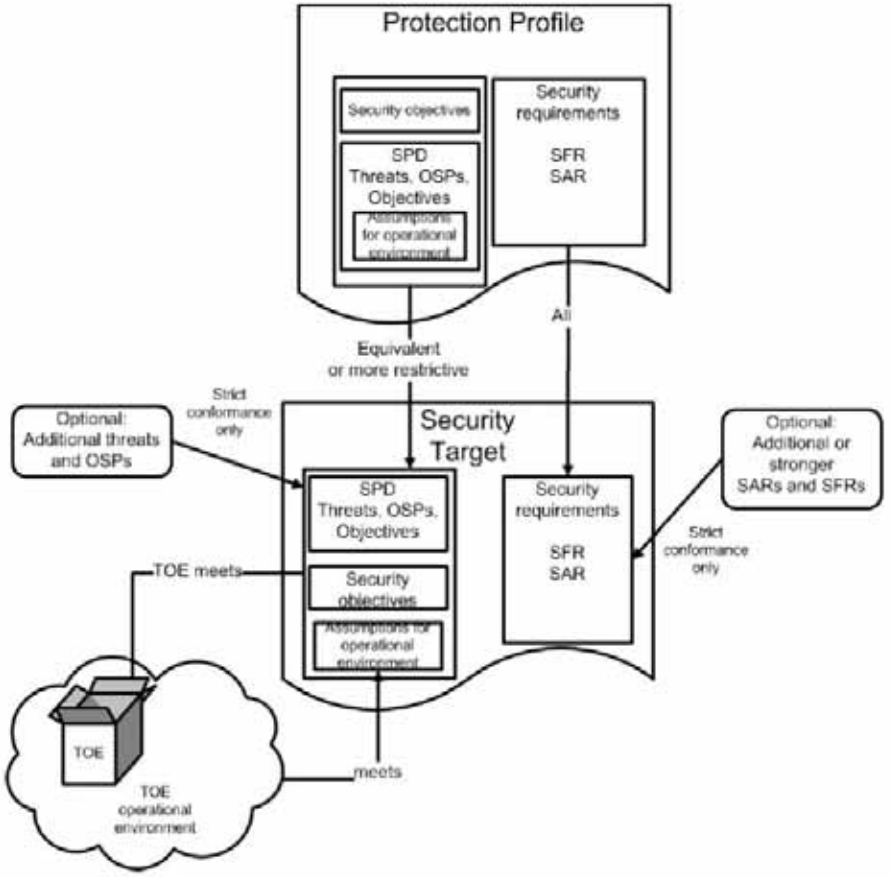
# CC KEY DEFINITIONS SECURITY TARGET



# CC KEY DEFINITIONS ST VS. PP

- A **Security Target** may claim conformance to one or more identified **Protection Profiles.**
- A ST which claims compliance to a PP:
  - must describe the tailoring operations
  - may add security objectives, requirements, etc.



# Question time

- **Question #1**

  Evaluation = third party Examination of evidence while

  certification = official completion of a successful Common Criteria EVALUATION

- **Question #2**

  What is the difference between a PP and ST?

- **Question #3**

  What is a TOE ?



RED ALERT LABS
IoT Security

# Answer

- ✔ What is the difference between evaluation & certification?

  Evaluation = third party examination of evidence while

  certification = official completion of a successful Common Criteria evaluation

- ✔ What is the difference between a PP and ST?

  A Security Target may claim conformance to one or more identified Protection Profiles

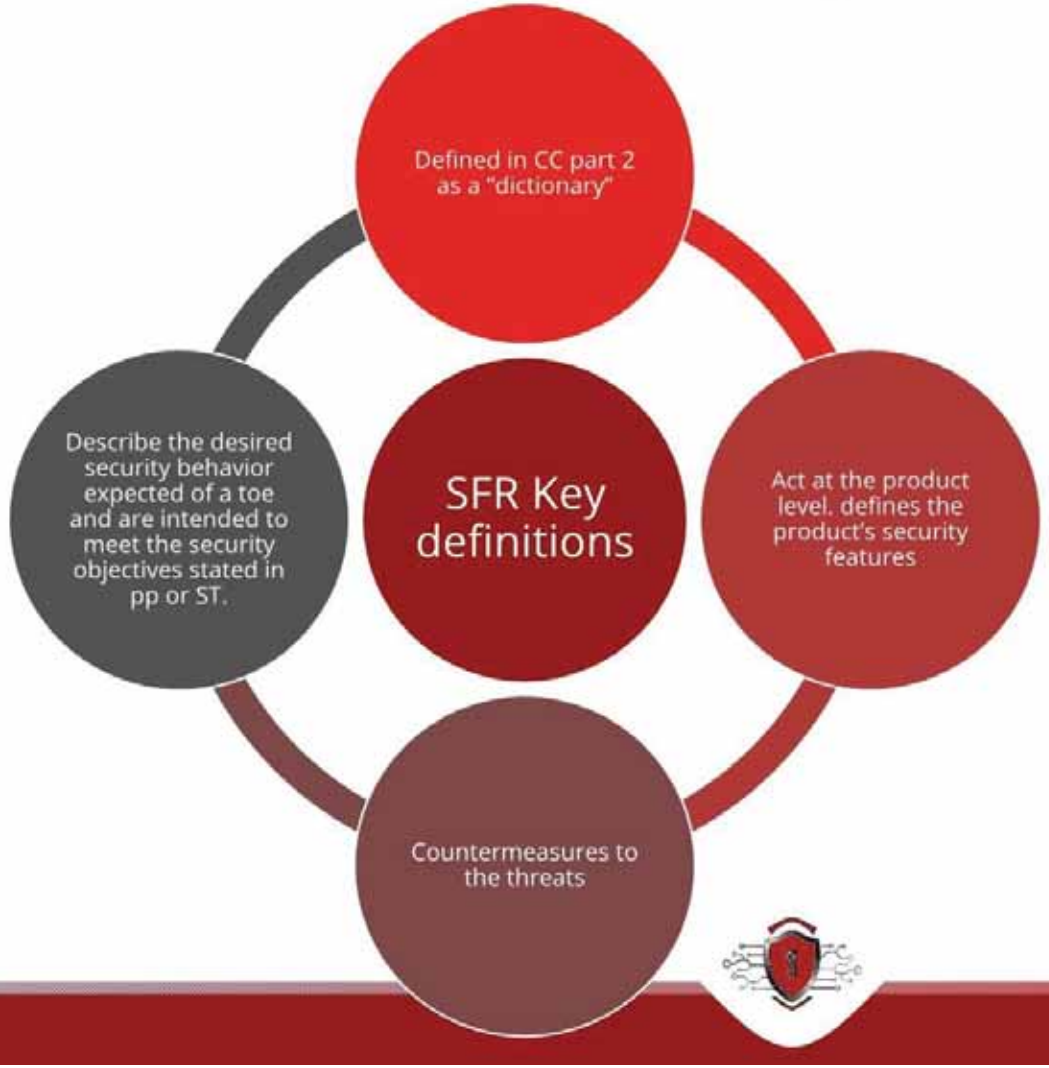
- ✔ What is a TOE ?

  Target Of Evaluation is the focus of the evaluation



RED ALERT LABS
IoT Security

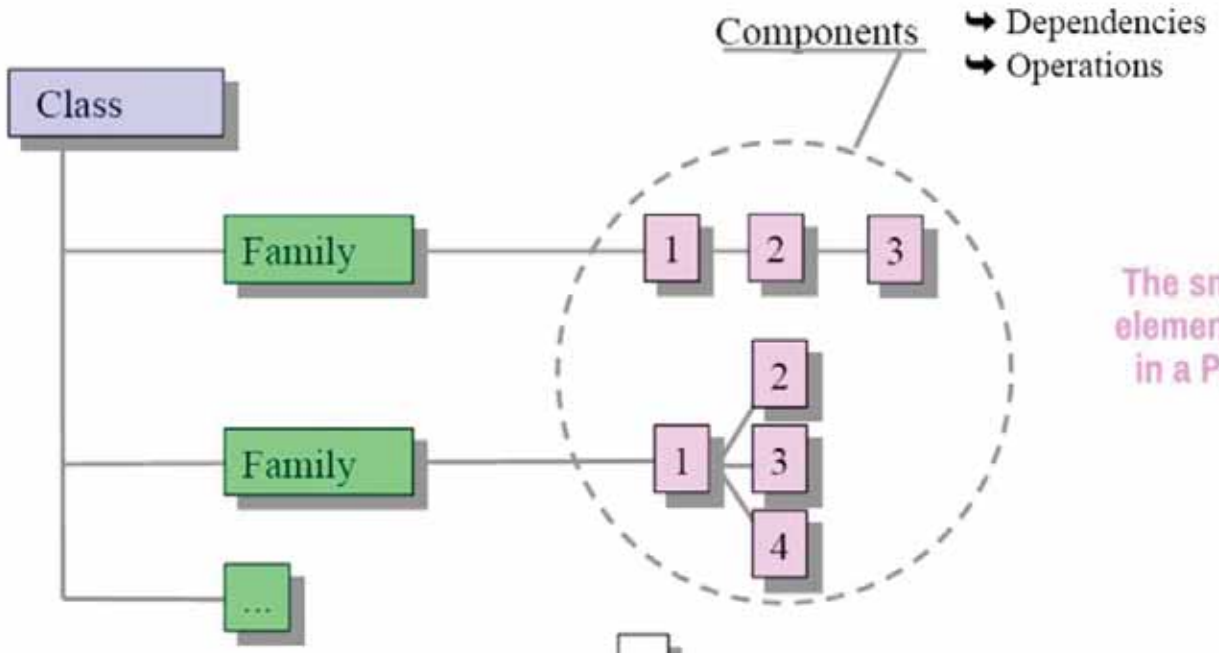
# CC KEY DEFINITIONS
# SECURITY FUNCTIONAL REQUIREMENTS (SFR)




- e.g. how to protect the user data by using access controls ?

# CC KEY DEFINITIONS SFRS: HIERARCHICAL STRUCTURE

A grouping of families that share a common focus




The smallest selectable set of elements that may be included in a PP, an ST, or a package.

A grouping of components that share security objectives but may differ in emphasis or rigour.

Applies to functional and assurance requirements

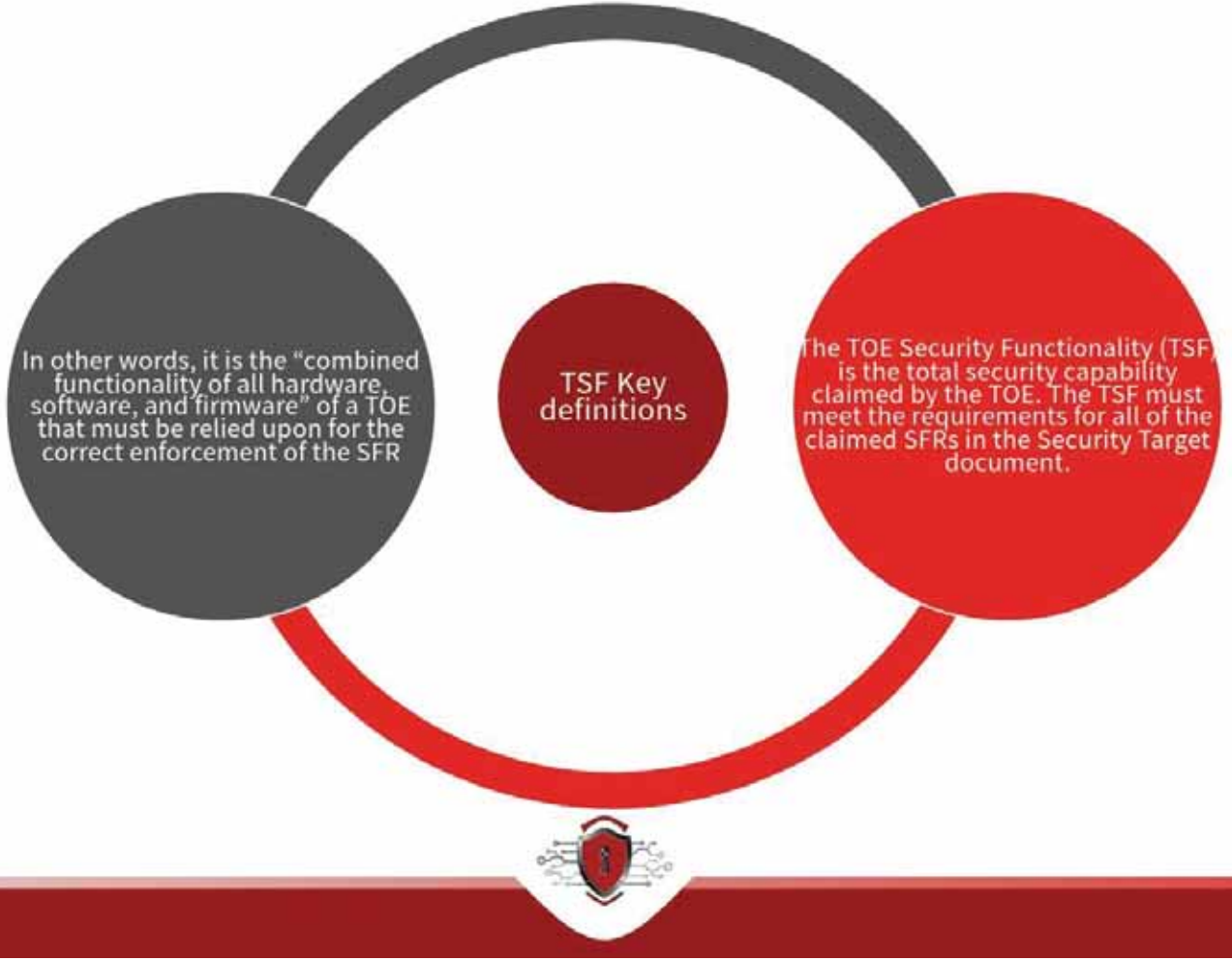
# CC KEY DEFINITIONS SFRS: 11 CLASSES

- FAU: Audit
- FCS: Cryptographic support
- FCO: Communications
- FDP: User data protection
- FIA: Identification and Authentication
- FMT: Security Management
- FPR: Privacy
- FPT: Protection of the TOE security functions
- FRU: Resource Utilization
- FTA: TOE access
- FTP: Trusted Paths/Channels

**They aim at formalizing the security objectives**

**of the TOE in a common way**

# CC KEY DEFINITIONS TOE SECURITY FUNCTIONALITY (TSF)



# CC KEY DEFINITIONS SFRS: OPERATIONS

Class Family Component

**FMT_MOF.1 Management of security functions behaviour**

Dependencies: (FMT_SMF.1) and (FMT_SMR.1)

Component Element

**FMT_MOF.1.1** The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

# CC KEY DEFINITIONS SFRS: ITERATIONS & REFINEMENTS

Iteration

**FMT_MOF.1/Iteration Management of security functions behaviour**

Dependencies: (FMT_SMF.1) and (FMT_SMR.1)

**FMT_MOF.1.1**

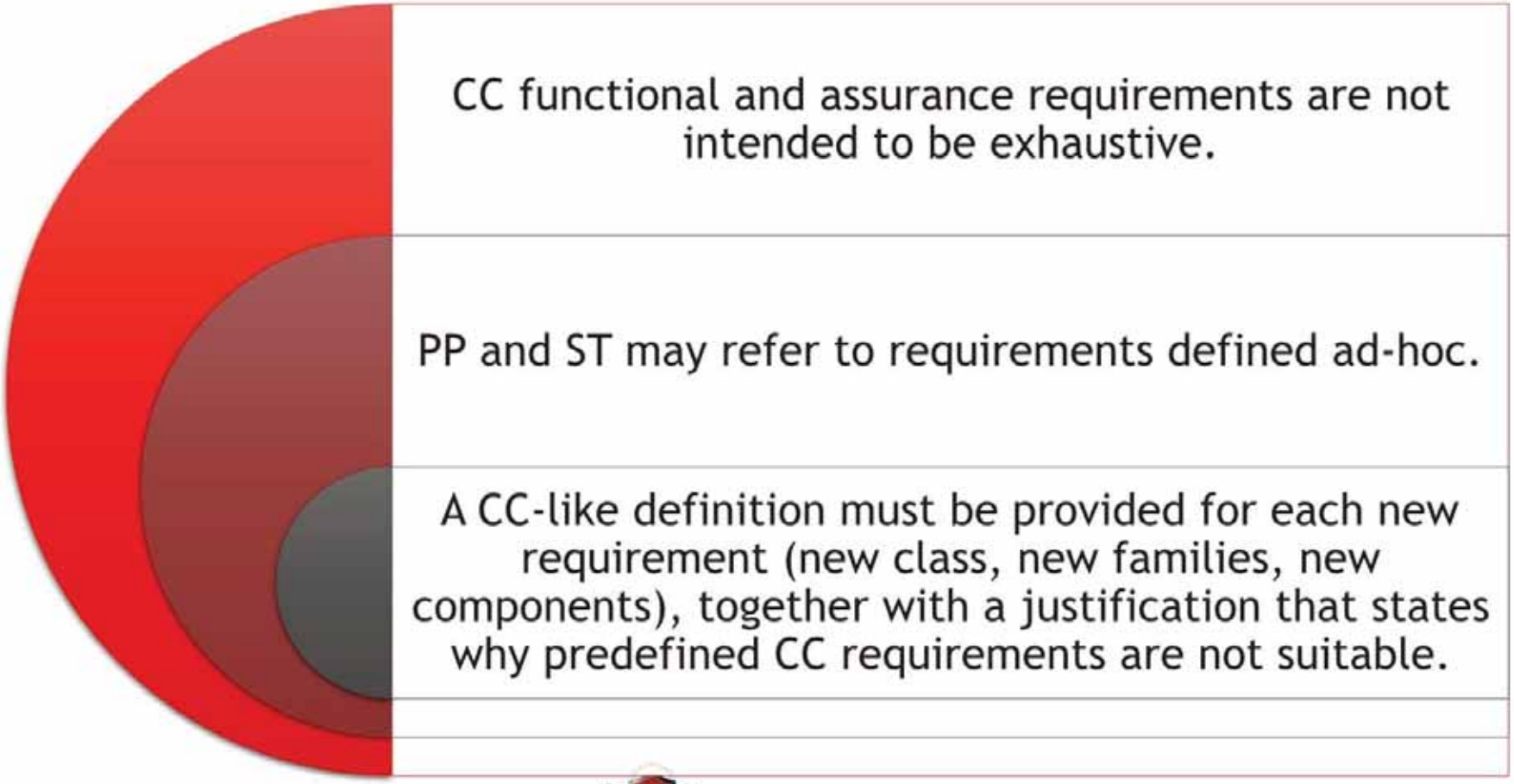
The TSF shall restrict the ability to [selection: determine the behavior of, disable, enable, modify the behavior of] the functions [assignment: list of functions] to [assignment: the authorized identified roles].

Refinement:

**FMT_MOF.1.1/Iteration**

The TSF shall restrict the ability to [selection: disable, enable] the functions [assignment: list of functions] to the Administrator.

# CC KEY DEFINITIONS SFRS: EXTENDED



# Question time

- Question #1
  What is an SFR?
- Question #2
  How many classes are in the CC SFR ?



RED ALERT LABS
IoT Security

# Answer

- What is an SFR?

  SFR Describes the desired security behavior expected of a toe

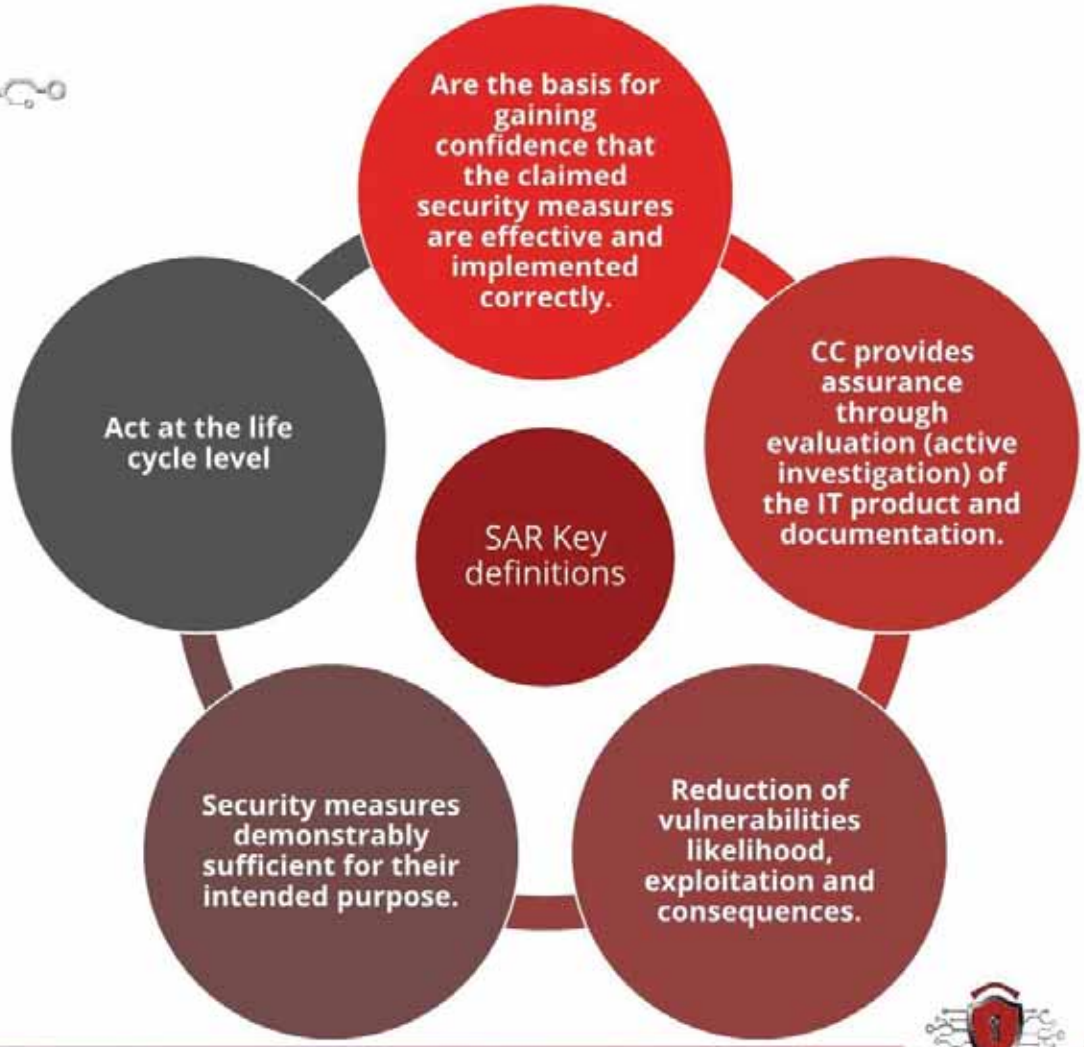
- How many classes are in the CC SFR ?

  There are 11 SFR classes



RED ALERT LABS
IoT Security

# CC KEY DEFINITIONS SECURITY ASSURANCE REQUIREMENTS (SAR)




Increasing level of effort:

- SCOPE: THE PORTION OF THE PRODUCT INVOLVED.
- DEPTH: THE LEVEL OF DETAIL REQUIRED (DESIGN, IMPLEMENTATION).
- RIGOR: THE STRUCTURE OR THE FORMALIZATION DEGREE REQUIRED.

# CC KEY DEFINITIONS SARS: ELEMENTS

- Each assurance component is composed of a set of assurance elements that constitute the security requirements.

- Each assurance element belongs to one of the three sets of elements:

**DEVELOPER ACTION (D):** THE ACTIVITIES THAT SHALL BE PERFORMED BY THE DEVELOPER.

**CONTENT AND PRESENTATION OF EVIDENCE (C):** THE EVIDENCE REQUIRED (FOR INSTANCE, SPECIFIC DOCUMENTATION), WHAT THE EVIDENCE SHALL DEMONSTRATE, WHAT INFORMATION THE EVIDENCE SHALL CONVEY.

**EVALUATOR ACTION (E):** THE ACTIVITIES THAT SHALL BE PERFORMED BY THE EVALUATOR (DETAILED IN CEM).

# CC KEY DEFINITIONS SARS: LIST OF CLASSES

| Assurance Class |
| --- |
| ADV: Development |
| AGD: Guidance documents |
| ALC: Life-cycle support |
| ASE: Security Target evaluation |
| ATE: Tests |
| AVA: Vulnerability assessment |
| ACO: Composition |
| APE: Protection Profile evaluation |

# CC KEY DEFINITIONS EVALUATION ASSURANCE LEVEL (EAL)

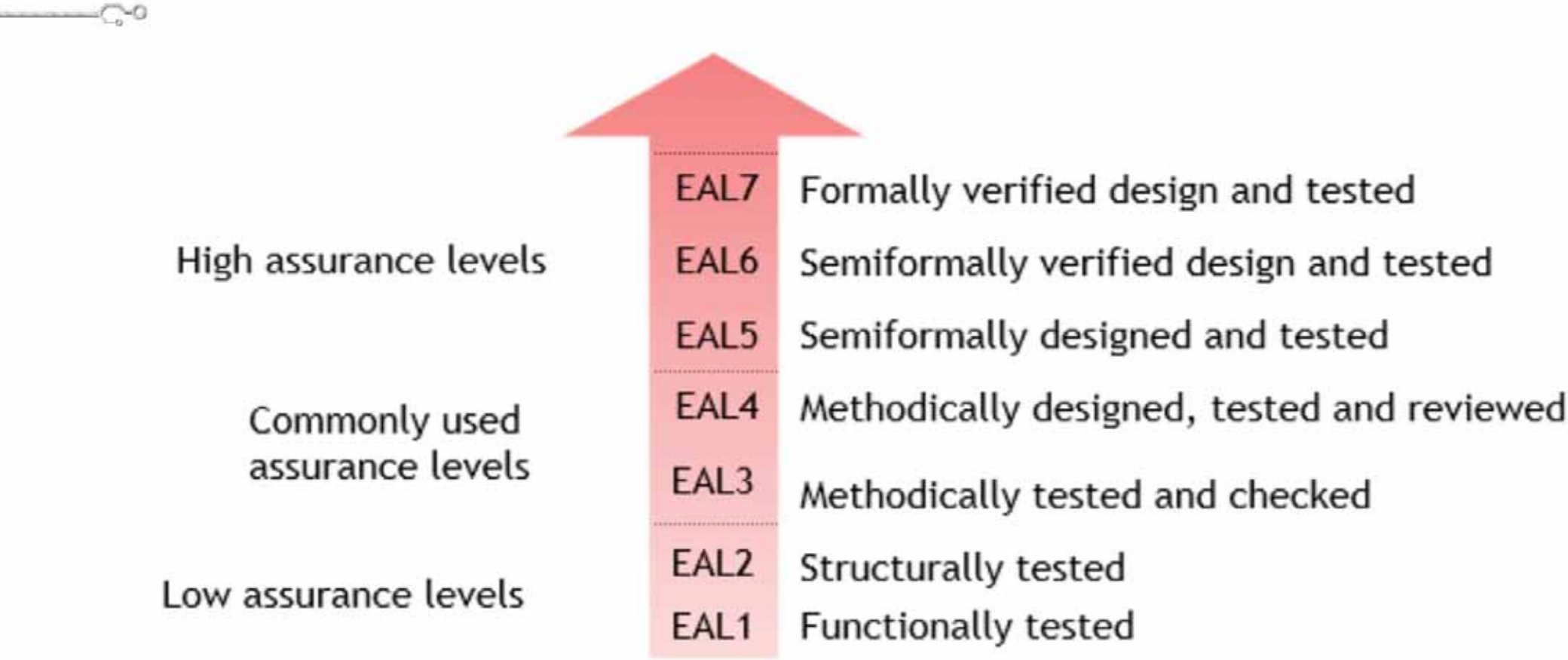
Increasing scale, constructed from assurance components

Balance the level of assurance with the cost and feasibility of acquiring it

The depth and rigor of SAR evaluation is determined by the EAL and subsequent attack potential of that EAL

EAL 1-7 is a scale of increasing assurance gained that TSF compromise and bypass cannot occur at increasing levels of attack potential (expertise, resources, motivation)

# CC KEY DEFINITIONS EVALUATION ASSURANCE LEVEL



# CC KEY DEFINITIONS EAL 1

# CC KEY DEFINITIONS EVALUATION ASSURANCE LEVEL

## EAL2- Airport security in the 90s

- Show up at last minute
- Keep your shoes and belt on
- Bring your own drinks

## EAL3- Airport security after Y2K

- Show up 2 hours before the flight
- Strip
- No liquids

## EAL4-EAL5 plus

- You get pulled aside for the personal examination
- You look suspicious so they also bring you in another room for interviews
- If you are lucky all you do is miss your flight

# CC KEY DEFINITIONS EVALUATION ASSURANCE LEVEL

| Assurance class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL |
| Development | ADV_ARC | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 |
| | ADV_IMP | | | | 1 | 1 | 2 | 2 |
| | ADV_INT | | | | | 2 | 3 | 3 |
| | ADV_SPM | | | | | | 1 | 1 |
| | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 |
| Guidance documents | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_PRE | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Life-cycle support | ALC_CMC | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 |
| | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 |
| Security Target evaluation | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 |
| | ATE_DPT | | | 1 | 1 | 3 | 3 | 4 |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| Vulnerability assessment | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 |

# Question time

- **Question #1**
  What is an SAR?
- **Question #2**
  Describe one of the SAR classes?
- **Question #3**
  Describe what is an EAL scale?



RED ALERT LABS
IoT Security

# Answer

- ✔ What is an SAR?

  Security Assurance Requirement

- ✔ Describe one of the SAR classes?

  ADV: Development

  AGD: Guidance documents

  ASE: Security Target

- ✔ Describe what is an EAL scale?

  EAL 1-7 is a scale of increasing assurance gained that TSF compromise and bypass cannot occur at increasing levels of attack potential (expertise, resources, motivation)



RED ALERT LABS
IoT Security


04

# PART 1: INTRODUCTION TO CC (ISO/IEC 15408)

## Documentation

# CC DOCUMENTATION OVERVIEW
# SECURITY TARGET (ASE)

First document the developer produces and is evaluated.

Depending on the product's complexity, how much internal documentation exists, cost/effort will be more or less higher

Requires interviews with the technical team, read and examine internal documents.

CC knowledge ➔ HIGH

CC consultant charges around 15-30 K€ for ST development.

➔ Check: CC Part 1 Annex A - Specification of Security Targets + CEM

# CC DOCUMENTATION OVERVIEW
# DEVELOPMENT EVIDENCE (ADV)

- Product Design Documents used by the evaluators **to verify the vendor security functional claims**
- Demonstrates how the TSFs meet the SFRs
- CC knowledge ➔ MODERATE to HIGH
- Functional Specifications

➔ **Check the CEM and CC Part 3**

# CC DOCUMENTATION OVERVIEW
# DEVELOPMENT EVIDENCE (ADV)

- TOE Design Description
- Implementation Description (e.g. source code)
- Security Architecture Description
- TSF Internal Description
- Security Policy Model

➔ **Check the CEM and CC Part 3**

# CC DOCUMENTATION OVERVIEW
# LIFE-CYCLE SUPPORT (ALC)

- The goal is to assess the vendor's security procedures during development and support of the TOE.
- Could be derived directly from the standard documentation for any commercial product vendor
- CC knowledge → LOW

| | | | |
|---|---|---|---|
| Configuration Management Capabilities (SW Source Code control) | CM Scope | Delivery | Development Security |
| Flaw remediation | Lifecycle definition | Tools & Techniques | |

→ **Check the CEM and CC Part 3**

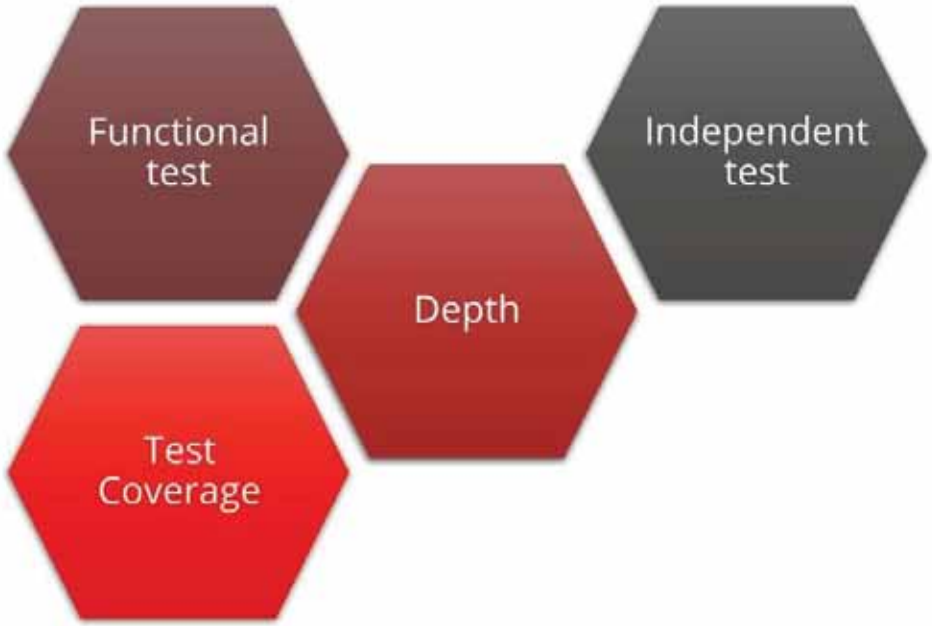
# CC DOCUMENTATION OVERVIEW TESTS (ATE)

- The goal is to confirm that the TOE security functions perform as designed.
- QA team members must be closely involved:

  **PROVIDE WHAT WAS TESTED AND HOW IT WAS TESTED ?**

  **MAY BE REQUIRED TO DEVELOP ADDITIONAL TESTS TO ADDRESS SECURITY FUNCTIONS AS DEFINED IN THE ST AND THE FS**

- CC knowledge ➔ LOW to MODERATE




➔ **Check the CEM and CC Part 3**

# CC DOCUMENTATION OVERVIEW GUIDANCE (AGD)

- These refer to the user documentation delivered with the product.
- The goal is to avoid insecurely configured products to be released by providing proper instructions to users on how to security set up, install and configure products in accordance with the evaluation conditions.
- CC knowledge ➔ LOW

It includes mainly:

- User Manuals,
- Administrator guides
- Installation and setup manuals.

Guidance evidence can be delivered as addendums to standard product documentation to the end-user or can be integrated into the standard user guidance.

➔ **Check the CEM and CC Part 3**

# Question time

- **Question #1**
  What is the first document that the developer should create?
- **Question #2**
  Mention 2 areas covered by lifecycle support documentation.
- **Question #3**
  The guidance evidence includes mainly…?



RED ALERT LABS
IoT Security

# Answer

- What is the first document that the developer should create?

  Security Target

- Mention 2 areas covered by lifecycle support documentation.

  Low User Manuals

  Administrator guides

- The guidance evidence includes mainly…?

  Installation and setup manuals



RED ALERT LABS
IoT Security

# CC DOCUMENTATION OVERVIEW
# EFFORT REQUIRED - ESTIMATION

# CC DOCUMENTATION OVERVIEW **GENERAL TIPS**

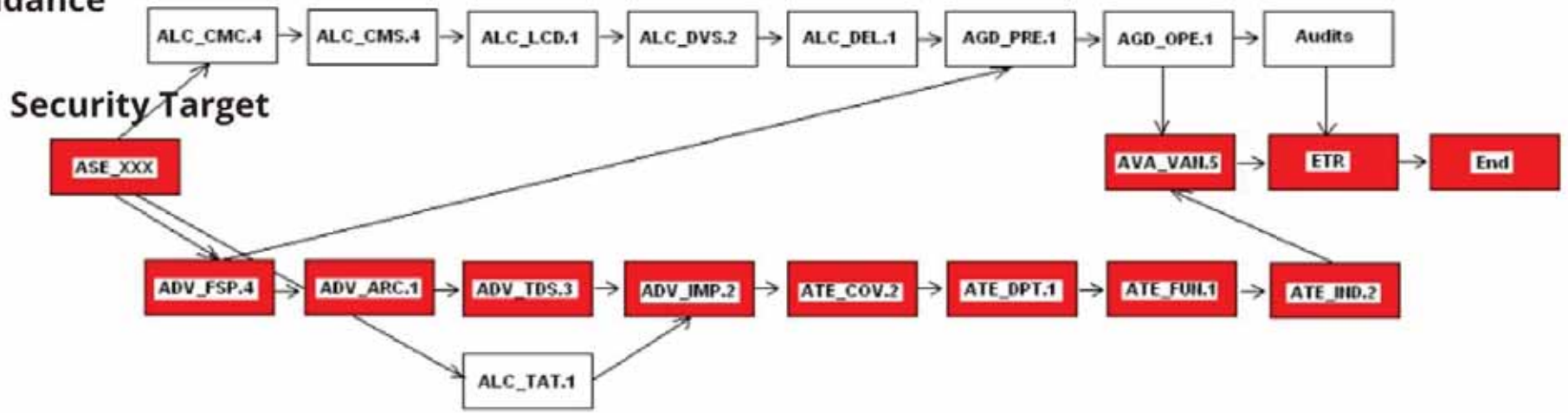
- Develop an internal simple questionnaire format document to smartly prepare and plan the CC documentation process.
  - **TYPICAL QUESTIONS:**
    - What documentation do you have on how your team uses configuration management ?
    - Do you have existing manuals describing the administrator's functions ?
    - What kind of user roles does the product support ?
    - Are most of your tests automated ?
    - How complex is your test requirements ?
    - Are there any reported security vulnerability on your product ? Or any used 3rd party product ?
    - ...

# CC DOCUMENTATION OVERVIEW GENERAL TIPS

The recommended order of deliverables is as follows:

**➔ Configuration Management ➔ Delivery, Installation and operation ➔ Life-cycle support ➔ User Guidance**




**➔ Development Evidence ➔ Tests**

# CC EVALUATION - GENERAL PROCESS

# CC DOCUMENTATION OVERVIEW
# STANDARD ENGINEERING & TECHNICAL WRITERS

# CC DOCUMENTATION OVERVIEW
# SECURITY & QUALITY ENGINEERING

# Question time

- Question #1

  Describe the general evaluation process as discussed in this section



RED ALERT LABS
IoT Security

# Answer

- ✔ Describe the general evaluation process as discussed in this section

  The lab performs detailed testing on the product to validate that the security functions operate as specified in the ST. This includes analyzing source code, reviewing documentation, and running tests on the product.

  The evaluator also verifies whether the product meets the defined assurance level, which could range from a basic functional test (EAL1) to a thorough formal verification and testing process (EAL7).



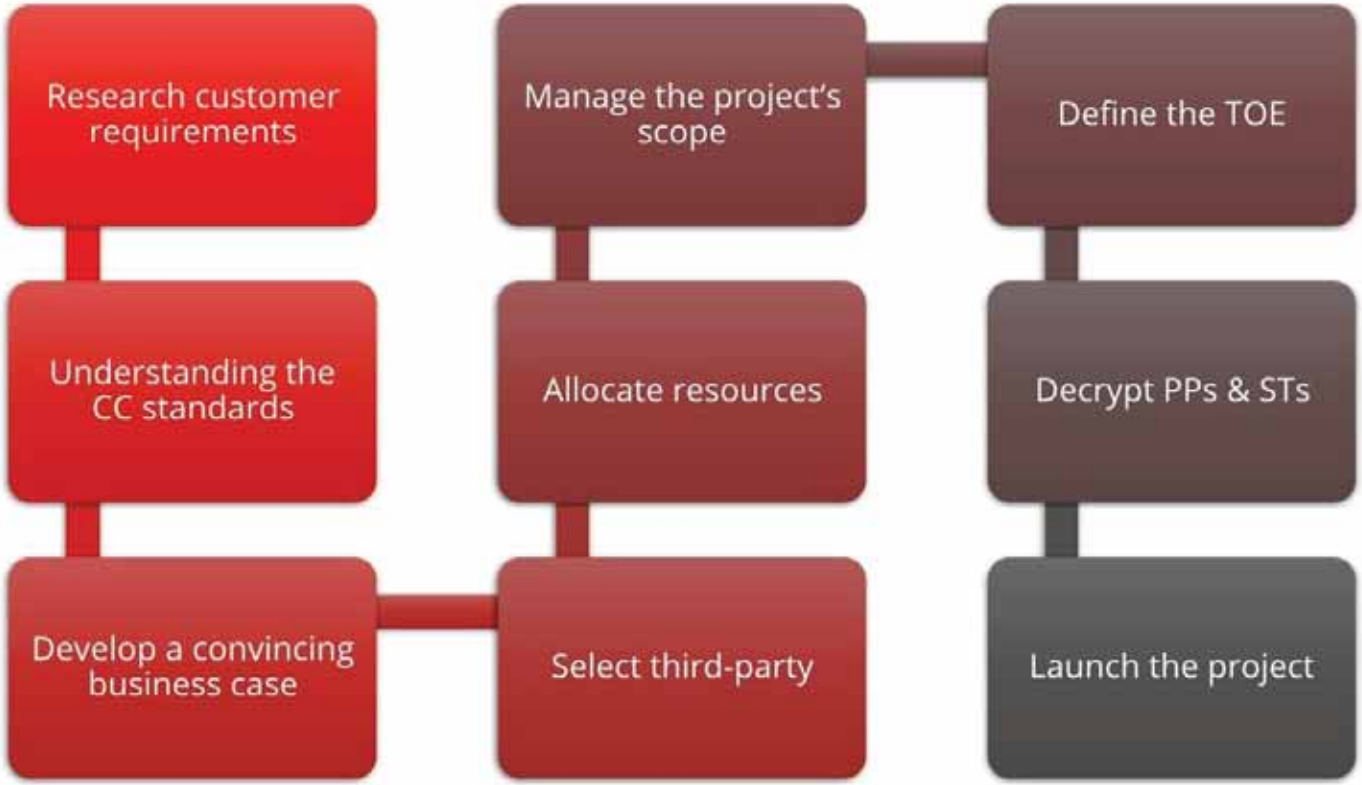
RED ALERT LABS
IoT Security




# PART 2: CERTIFICATION PROCESS

## Phase 1: Preparation

# PHASE 1: PREPARATION
# GET STARTED



# PHASE 1: PREPARATION
# RESEARCH CUSTOMER REQUIREMENTS

- Do they require that the evaluation be performed against a particular PP ?
- Do they require a specific EAL ?
- What SFRs they expect to be included ?
- What product version do they expect to be evaluated ?
- When do they need the evaluation and certification to be completed ?
- What other competitors products have already been evaluated ?

# PHASE 1: PREPARATION
# UNDERSTAND THE CC STANDARDS

## EYES WIDE OPEN 

CC Training

Know your product:

- Not only the product security features
- But also all the life cycle process of the product security features

Leverage existing internally developed documentation

# PHASE 1: PREPARATION
# BUSINESS CASE DEVELOPMENT

ROI

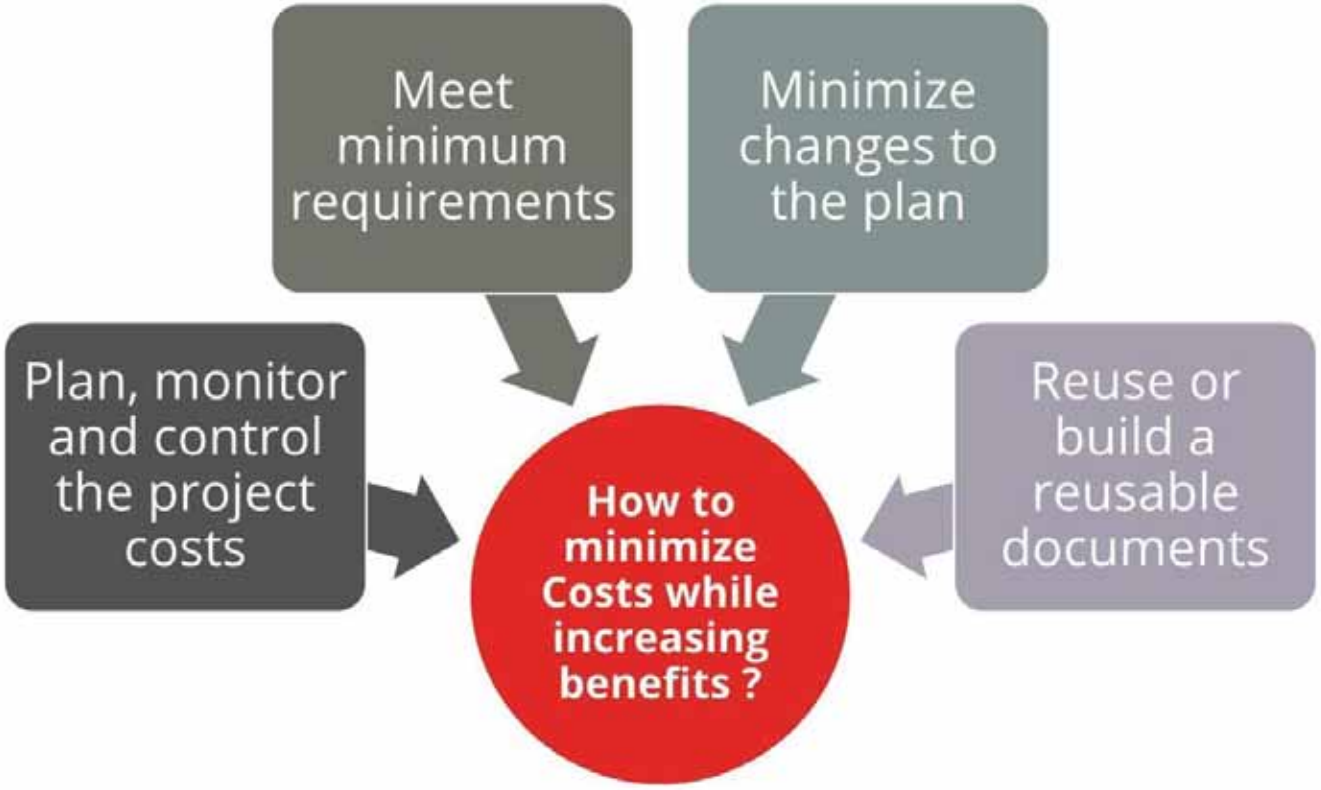
**Costs (investments)**

- Evaluation Lab
- CC consultancy
- Site visit expenses
- Equipment Costs
- Lost opportunity

**Benefits (returns)**

- what are your potential weaknesses if you don't pursue CC evaluations ?

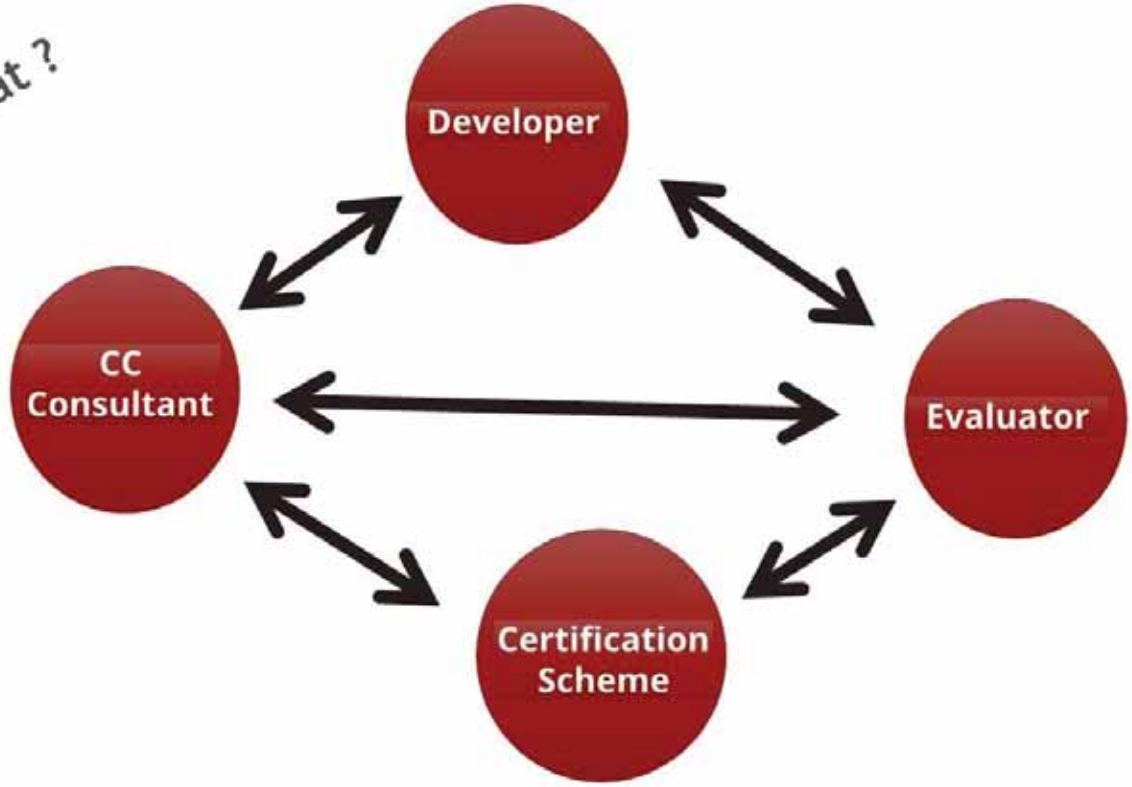
# PHASE 1: PREPARATION
# MANAGING THE PROJECT'S SCOPE



# PHASE 1: PREPARATION
# RESOURCE ALLOCATION

Who does what ?



# PHASE 1: PREPARATION
# THIRD-PARTY SELECTION

# PHASE 1: PREPARATION
# DEFINE THE TARGET OF EVALUATION

## TOE Reference

- The product unique name
- version

## TOE Overview:

- Summarize the usage and major security features of the TOE.
- High-level description of these security features (e.g authentication, auditing, security management, etc.)
- Identify the TOE Type (e.g Access Control Devices and Systems, Biometric Systems and Devices, Data Protection, Databases, ICs/Smart Cards, Operating Systems, etc.)
- Identify any non-TOE HW, SW and firmware required by the TOE

## TOE Description –

- Describe the physical scope and the logical scope of the TOE (e.g an nice block diagram of the system architecture
- the surrounding (interfacing) IT environment
- the Operational Guidance.

# PHASE 1: PREPARATION
# DEFINING THE TARGET OF EVALUATION

The **TOE** definition needs to include specific reference to the **guidance** evaluated as part of the TOE.

The **guidance** reference in the **ST** needs to be unambiguous should be generally consistent with the information in the **ST**.

The **guidance** needs to clearly provide any details that serve to define the **TOE** not included in the **ST**.

The **guidance** set needs to be clear on its own to help direct users appropriately even when the **ST** is not available.

# Question time

- **Question #1**
  Define the TOE before Allocating resources. TRUE or FLASE
- **Question #2**
  How do you minimize evaluation costs?
- **Question #3**
  List the 3rd party selection criteria



RED ALERT LABS
IoT Security

# Answer

- You should define the TOE before Allocating resources. TRUE or FLASE

  False

- How do you minimize evaluation costs?

  Plan, monitor and control the project costs;

  Meet minimum requirements;

  Minimize changes to the plan;

  Reuse or build a reusable documents

- List the 3rd party selection criteria

  Technical expertise; Quality of relationship; Costs; Contract terms; cooperative relationships



RED ALERT LABS
IoT Security

# PHASE 1: PREPARATION DECRYPTING PPS & STS

# PHASE 1: PREPARATION DECRYPTING PPS & STS

## Introduction

PP/ST reference. TOE reference (only ST).

TOE overview: usage, TOE type, non-TOE HW/SW/firmware

TOE Description (only ST): physical and logical scope

## Conformance Claim

Conformance with the CC itself, PPs, Packages.

The PP conformance statement states how STs or other PPs must conform to that PP ("strict" or "demonstrable").

# PHASE 1: PREPARATION DECRYPTING PPS & STS

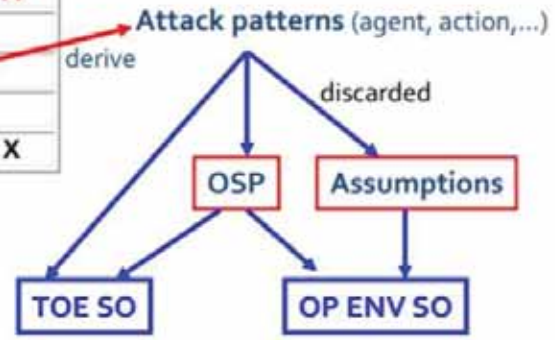
- Security Problem Definition

  ATTACK PATTERNS (AGENT, ACTION,…) DERIVE TOE SO & OP ENV SO

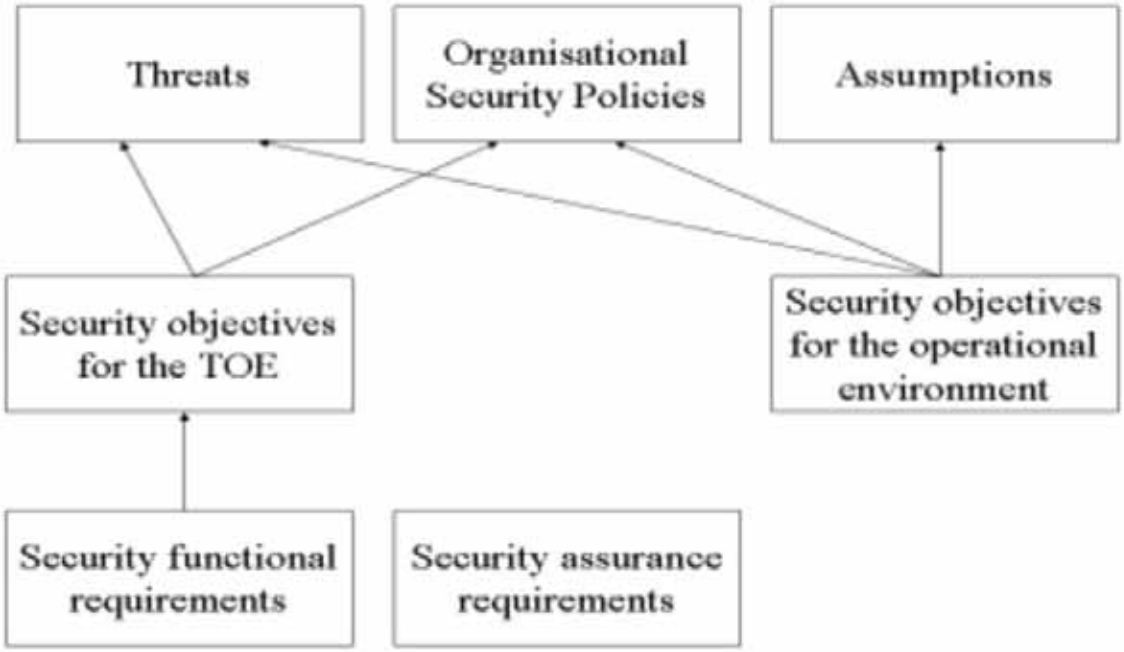
  DISCARDED ASSUMPTIONS OSP

  MANY APPROACHES: RISK/THREAT ANALYSIS, THREAT DB, …., A SIMPLE ONE

| ASSETS / IMPACT | C | I | A |
|---|---|---|---|
| A1 | X | | |
| A2 | X | X | |
| ..... | | | |
| An | | X | X |



# PHASE 1: PREPARATION DECRYPTING PPS & STS




**If** all SFRs and SARs are satisfied and all SOs for the operational environment are achieved, **then** the security problem is solved.

# PHASE 1: PREPARATION HOW TO USE A PP ?

- part of a specification for a specific consumer
- part of a regulation from a specific regulatory entity; as a baseline defined by a group of IT developers.

**How a PP should be used**

- a detailed specification;
- a complete specification
- a specification of a single product

**How a PP should NOT be used**

# PHASE 1: PREPARATION HOW TO USE AN ST ?

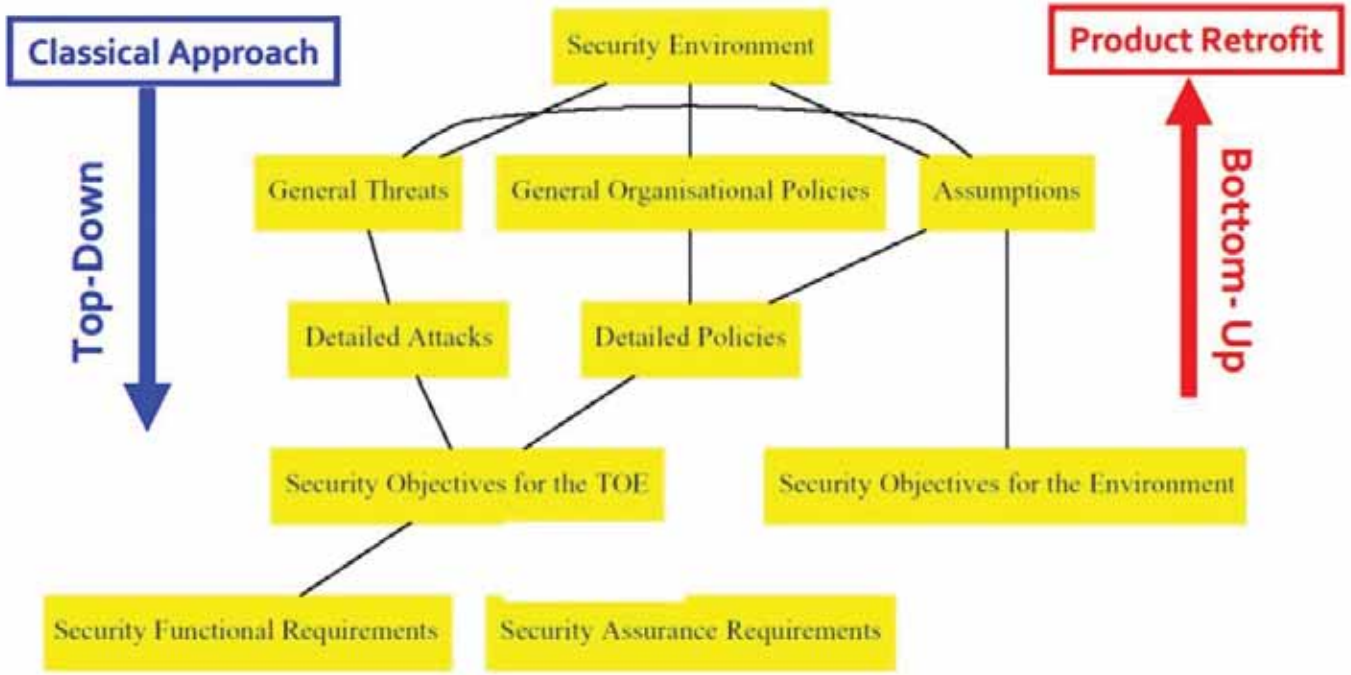
- Before and during the evaluation, the ST specifies “what is to be evaluated”
- After the evaluation, the ST specifies “what was evaluated”

How an ST should be used

- a detailed specification
- a complete specification

How an ST should NOT be used

# PHASE 1: PREPARATION
# 2 DIFFERENT APPROACHES OF IMPLEMENTATIONS



# PHASE 1: PREPARATION LUNCH THE PROJECT

- Preparation for the kick-off meeting with the scheme
- SECURITY TARGET PRESENTATION:
  - What is to be evaluated ?
  - What is the Evaluated Environment ?
  - What is the Evaluation Level against it you must evaluate ?

The Evaluation Work Plan

# Question time

- **Question #1**
  A PP should be used as a specification of a single product. TRUE or FALSE?
- **Question #2**
  What is the product retrofit approach to implementation?



RED ALERT LABS
IoT Security

# Answer

- A PP should be used as a specification of a single product. TRUE or FALSE?

  False

- What is the product retrofit approach to implementation?

  Bottom up



RED ALERT LABS
IoT Security




# PART 2: CERTIFICATION PROCESS

## Phase 2: Conduct

# PHASE 2: CONDUCT – SAR
# DEVELOPMENT (ADV)

Verify the vendor's security functional claims

## Understanding how the TSF meet the SFRs

| Functional Specifications (ADV_FSP) | Security Architecture (ADV_ARC) | TOE Design (ADV_TDS) | Implementation Representation (ADV_IMP) | TSF Internals (ADV_INT) | Security Policy Modeling (ADV_SPM) |
|---|---|---|---|---|---|

# PHASE 2: CONDUCT - SAR
# FUNCTIONAL SPECIFICATION (ADV_FSP)

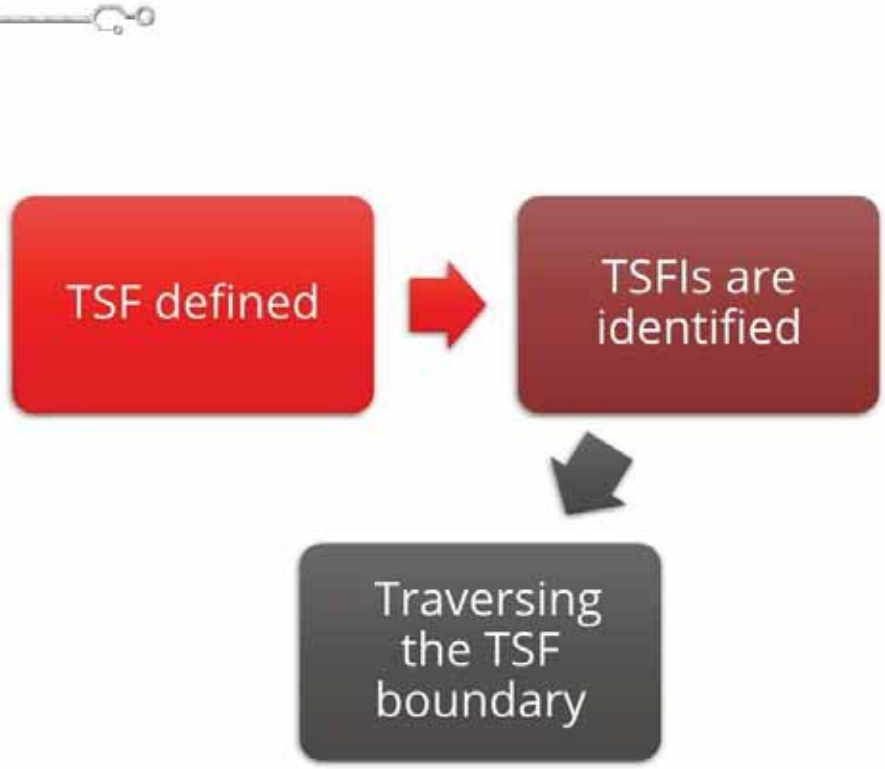
Describe the TSFI

- Purpose
- Method of use
- Parameters
- Actions
- Error messages

Mapping with the SFR

(EAL 5) The functional specification shall describe the TSFI using a semi-formal style.

# PHASE 2: CONDUCT - SAR
# FUNCTIONAL SPECIFICATION (ADV_FSP)




Question that should be asked when determining the TSFIs is:

"How can a potential attacker interact with the TSF in an attempt to subvert any of the the SFRs?"

# PHASE 2: CONDUCT - SAR
# TOE DESIGN (ADV_TDS)

- Describe the TSF boundary
- How the TSF implement the SFRs ?
- Definition of Subsystems and Modules + mapping with the TSFI
  - SFR-enforcing
  - SFR-supporting
  - SFR-non-interfering
- (EAL 5)The design shall provide a **semiformal** description of each subsystem of the TSF, supported by informal, explanatory text where appropriate.

# PHASE 2: CONDUCT - SAR
# IMPLEMENTATION REPRESENTATION (ADV_IMP)

Mapping between the implementation representation (source code) and the TOE design of the TSF.

Determine if the implementation is sufficient enough to satisfy the Security Requirements of the Security Target

Describe the TSF implementation

Understand implementation details for Vulnerability analysis

# PHASE 2: CONDUCT - SAR
# TSF INTERNALS (ADV_INT)

Provide a means for requiring the entire TSF to be well-structured. The intent is that the entire TSF has been designed and implemented using sound engineering principles.

- Coding rules
- Best practices
- Modular design

→ **Provide justification**

# Question time

- ✔ Question #1
  Describe ADV_IMP
- ✔ Question #2
  Explain what is covered in ADV_FSP



RED ALERT LABS
IoT Security

# Answer

- ✔ Describe ADV_IMP

  ADV_IMP: Implementation representation: Determine if the implementation is sufficient enough to satisfy the Security Requirements of the Security Target

- ✔ Explain what is covered in ADV_FSP

  ADV_FSP: Functional specifications: aims to protect subversion of the SFRs by an attacker, interacting through TSFIs



RED ALERT LABS
IoT Security

# PHASE 2: CONDUCT - SAR
# SECURITY ARCHITECTURE (ADV_ARC)

- Description of Security Domains
- Description of Initialization process
- Self protection
- Prevent bypassing of TSF
- Support the claims of the TSF.
- Consistency with the TOE design (ADV_TDS)

→ ALL THE MODULES MUST BE FOUND IN BOTH DOCUMENTS.

# PHASE 2: CONDUCT - SAR
# SECURITY ARCHITECTURE (ADV_ARC)

| CC requirement | Description |
|---|---|
| **ADV_ARC.1.1D** | Design and implement the TOE so that the security features of the TSF cannot be bypassed. |
| **ADV_ARC.1.2D** | Design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities. |
| **ADV_ARC.1.3D** | Provide security architecture (ARC) description of the TSF |
| **ADV_ARC.1.1C** | ARC shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions in TDS |
| **ADV_ARC.1.2C** | ARC shall describe the security domains maintained by the TSF consistently with the SFRs |
| **ADV_ARC.1.3C** | ARC shall describe how initialization is secure |
| **ADV_ARC.1.4C** | ARC shall demonstrate that the TSF protects itself from tampering |
| **ADV_ARC.1.5C** | ARC demonstrate that the TSF prevents bypass of the SFR-enforcing functionality. |

# PHASE 2: CONDUCT - SAR
# TEST EVIDENCE (ATE)

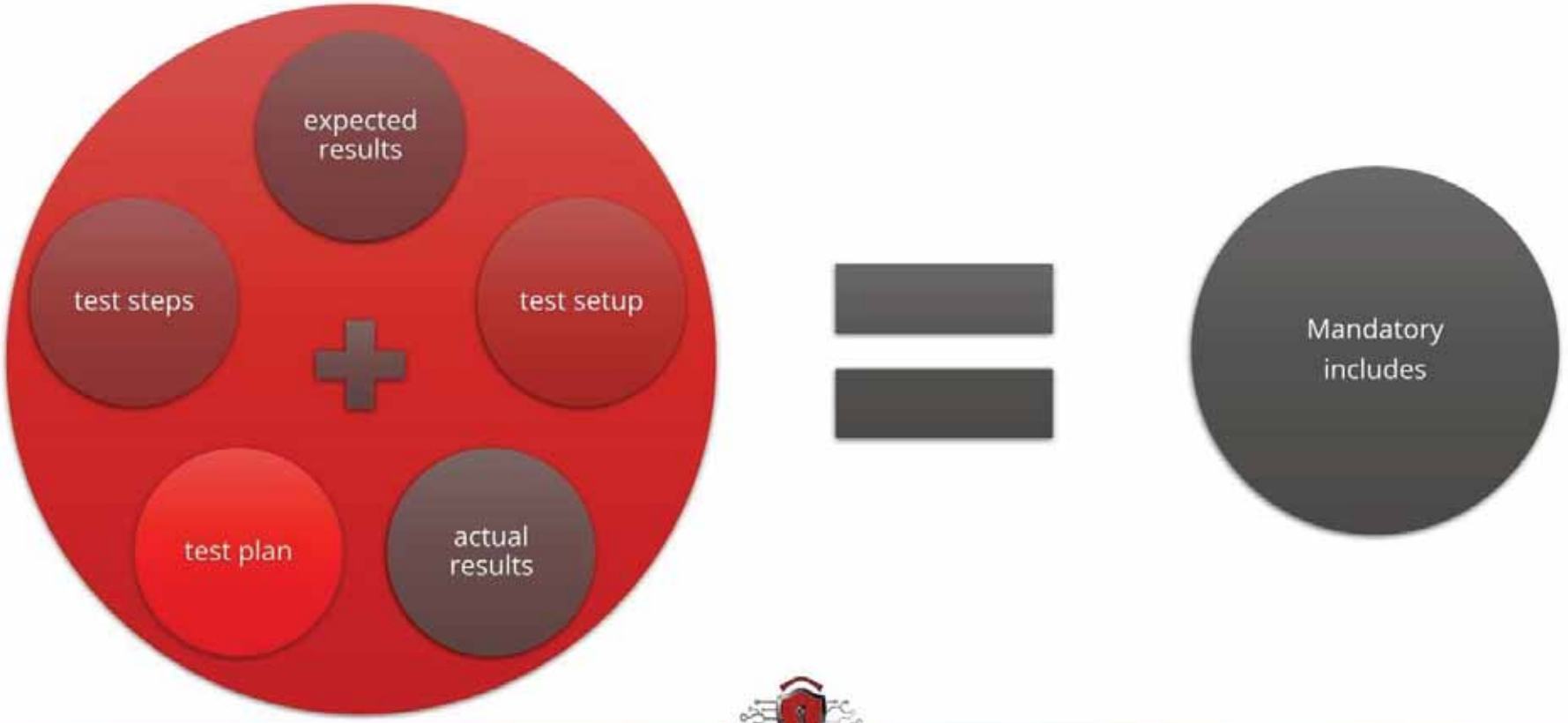
- **Confirm that the TOE security functionalities perform as designed.**

Correlate to the functional specification & the Security Target

Close involvement of the QA team members.

# PHASE 2: CONDUCT - SAR
# FUNCTIONAL TESTS (ATE_FUN)

- Describes the tests performed by the developer on security functionalities claimed in the ST.



# PHASE 2: CONDUCT - SAR
# TEST COVERAGE (ATE_COV) & TESTING DEPTH (ATE_DPT)

Describes the breadth of test coverage performed by developers across the TOE module interfaces.

**(ATE_COV)**

- demonstrate that all the TSFI has been tested
- mapping table between SFR, TSFI and tests details

Examine the depth of testing conducted by the developer.

**(ATE_DPT)**

- Correspondence between the tests and the TSF subsystems in the TOE design
- All subsystems and modules (EAL 5) must be tested

# PHASE 2: CONDUCT - SAR
## INDEPENDENT TESTS (ATE_IND) & GUIDANCE EVIDENCE (AGD)

Intended to provide greater assurance over developer testing.

**(ATE_IND)**

Developed by the evaluator.

Requires the developer to provide the TOE and an equivalent test environment so that the evaluator so the evaluator can run a subset of the developer's tests.

User documentation delivered with the product.

**(AGD)**

User manuals

Administrator guides

Setup & Installation manuals

- Operational Guidance (AGD_OPE)
- Preparative Guidance (AGD_PRE)

**COULD NEGOTIATE THIS TO HAPPEN DURING THE EVALUATOR'S ON-SITE VISIT**

# PHASE 2: CONDUCT - SAR
# PREPARATIVE GUIDANCE (AGD_PRE)

Provides information to the users on how to securely install and configure the TOE

include directions on securing the operational environment.

must be consistent with the ALC_DEL.

minimum system requirements

requirements of the operational environment

...

# PHASE 2: CONDUCT - SAR

## OPERATIONAL GUIDANCE (AGD_OPE) & LIFE-CYCLE DEFINITION (ALC_LCD)

Describes to the user the security functionality of the TOE

**(AGD_OPE)**

- role specific functions and privileges
- methods available to the user
- authorized parameters
- responses or error codes

Describes the product's lifecycle.

**(ALC_LCD)**

- Development phases
- Development procedures
- Tools
- Techniques
- Overall management structure with defined roles and responsibilities

# PHASE 2: CONDUCT - SAR
# LIFE-CYCLE SUPPORT EVIDENCE (ALC)

**Assess the vendor's security procedures during development and support of the TOE.**

- Configuration management (CM) capabilities (ALC_CMC)
- CM scope (ALC_CMS)
- Delivery (ALC_DEL)
- Development security (ALC_DVS)
- Flaw remediation (ALC_FLR)
- Lifecycle definition (ALC_LCD)
- Tools and Techniques (ALC_TAT)

# PHASE 2: CONDUCT - SAR
# TOOLS & TECHINQUES (ALC_TAT)

Describes the developer's use of tools.

- compilers
- testing tools
- ...

It includes requirements to prevent ill-defined, inconsistent or incorrect development tools from being used to develop the TOE.

(EAL 5) Compliance with the implementation standards.

# PHASE 2: CONDUCT - SAR
# CONFIGURATION MANAGEMENT SCOPE (ALC_CMS)

- What is managed by the configuration system ?
  - e.g the source code, documentation, tools, etc.
- Problem tracking (security flaw reports) shall be covered
- (EAL 5) Development tools shall be listed as well as other related information

# PHASE 2: CONDUCT - SAR
# CONFIGURATION MANAGEMENT CAPABILITIES (ALC_CMC)

- Ensure that the TOE is correct and complete before it is sent to the customer
- Ensure that no configuration items are missing during evaluation
- Prevent unauthorized modification, addition or deletion of TOE configuration items

Roles, responsibilities, procedures, bug tracking, access control, etc.

→ **on-site visit from the evaluator is required**

# Question time

- **Question #1**

  ATE Class confirms that the TOE security functionalities perform as designed. TRUE or FALSE

- **Question #2**

  What evidence describes the tests performed by the developer on security functionalities claimed in the ST?

- **Question #3**

  What evidence ensures that no configuration items are missing during evaluation?



RED ALERT LABS
IoT Security

# Answer

- ✔ ATE Class confirms that the TOE security functionalities perform as designed. TRUE or FALSE

  True

- ✔ What evidence describes the tests performed by the developer on security functionalities claimed in the ST?

  ATE_FUN Functional test

- ✔ What evidence ensures that no configuration items are missing during evaluation?

  ALC_CMC Configuration Management Capabilities



RED ALERT LABS
IoT Security




# PART 2: CERTIFICATION PROCESS

## Phase 3: RECOVER and/or FINALIZE

# PHASE 3: RECOVER & FINALIZE
# EVALUATOR'S OBSERVATION REPORTS

- If the evaluator find an inconsistency or some missing information or error in the evidence documentation

  ➔ produces an OR

Will not give much information on how to rectify the situation (depends on the lab)

Avoid evaluators who provide ambiguous feedback such as FSP are inconsistent with ST

# PHASE 3: RECOVER & FINALIZE
# EVALUATION TECHNICAL REPORT (ETR)

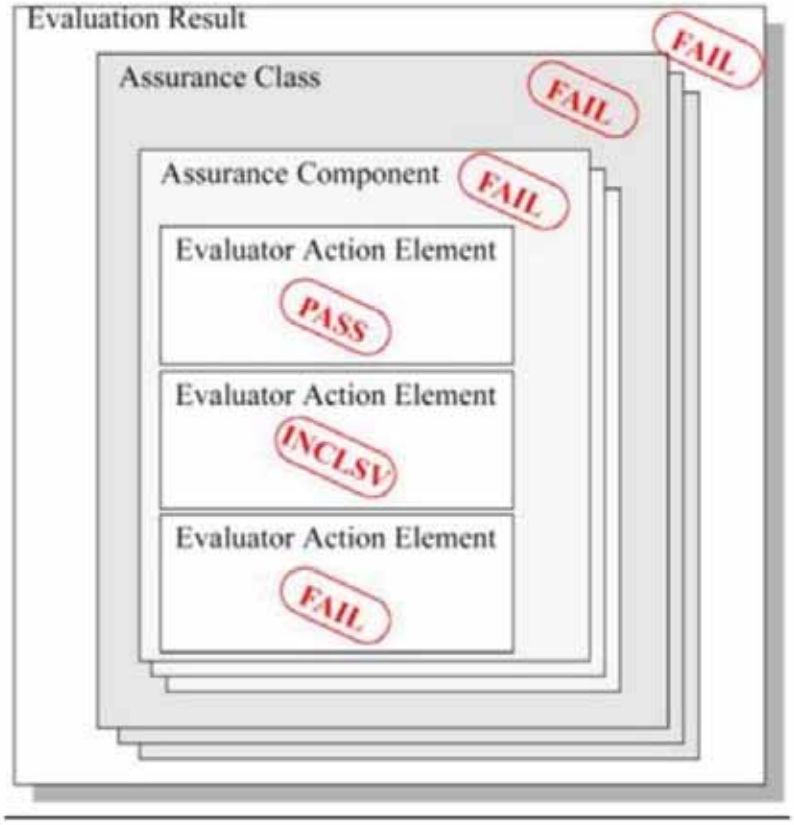
- CC evaluation labs are required to produce and send reports to the national scheme
- These reports are called ETRs

  → SUMMARIZE THE EVALUATION PROGRESS INCLUDING THE STATUS AND DISPOSITION OF ISSUES AND COMMENTS REPORTED TO THE VENDOR

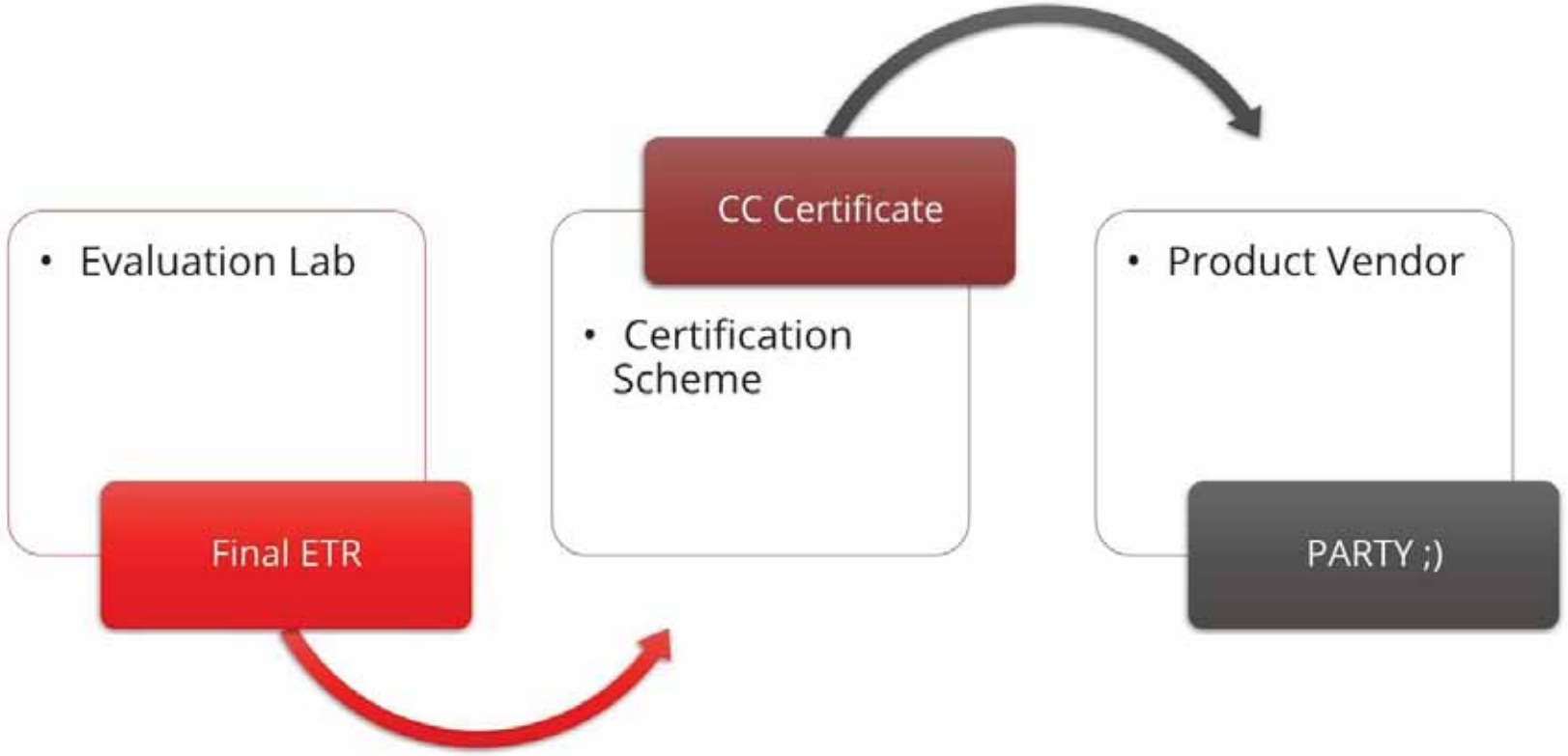
- A final ETR is summited to the Scheme when all the evaluation activity work units have been completed

# PHASE 3: RECOVER & FINALIZE
# CERTIFICATION RECEPTION

- When the Scheme receives the final ETR from the CC evaluation lab the validators will:
  - → REVIEW/VALIDATE THE RESULTS
  - → ASK QUESTIONS TO THE EVALUATION LAB
  - → DECIDE WHETHER THE EVALUATION SUCCESSFULLY MET ALL OF THE REQUIREMENTS OR NOT.



# PHASE 3: RECOVER & FINALIZE
# VALIDATION & CERTIFICATION



# Question time

- Question #1

  Describe the steps from start to when the product reaches the vendor



RED ALERT LABS
IoT Security

# Answer

- Describe the steps from start to when the product reaches the vendor

  START => SUBMIT EVIDENCE =>EVALUATE EVICENCE => OBSERVATION REPORT => ETR => CERTIFICATE => VENDOR



RED ALERT LABS
IoT Security

# PHASE 3: RECOVER & FINALIZE
# RE-CERTIFICATION/ASSURANCE CONTINUITY

## ASSUMPTION

CC certificates are only valid for a single version of a product.

## GOAL

Shorten the re-evaluation cycle for previously evaluated product

## HOW TO DO ?

Provide evidence that changes in the newer version of the product do not compromise the security claims and evidence presented in the prior version's evaluation.

An Impact Analysis Report (IAR) is submitted to the same evaluation lab that performed the original evaluation.

# THANK YOU