Introduction to Common Criteria

April 11, 2006

Many Standards

- NIST (FIPS)
- OMB (Circular A 130 – security of federal systems)
- DoD (DITSCAP)
- Common Criteria (combines TCSEC, ITSEC)
- ISO-17799
- (etc.)

Many Parties

- Developers
- Accreditors
- Approvers
- Product vendors
- Certifiers
- Evaluators
- Consumers

Mutual Recognition Arrangement

National Information Assurance partnership (NIAP), in conjunction with the U.S. State Department,
negotiated a Recognition Arrangement that:

- Provides recognition of Common Criteria certificates by 19 nations:

  Canada, United Kingdom, France, Germany, Australia, New Zealand, Greece, Norway, Finland, Italy, Israel, Spain, The Netherlands, Japan, Hungary, Austria, Sweden, Turkey, US
- Eliminates need for costly security evaluations in more than one country
- Offers excellent global market opportunities for U.S. IT industry

Industry Use of the CC

Industry can use the CC paradigm in several important ways:

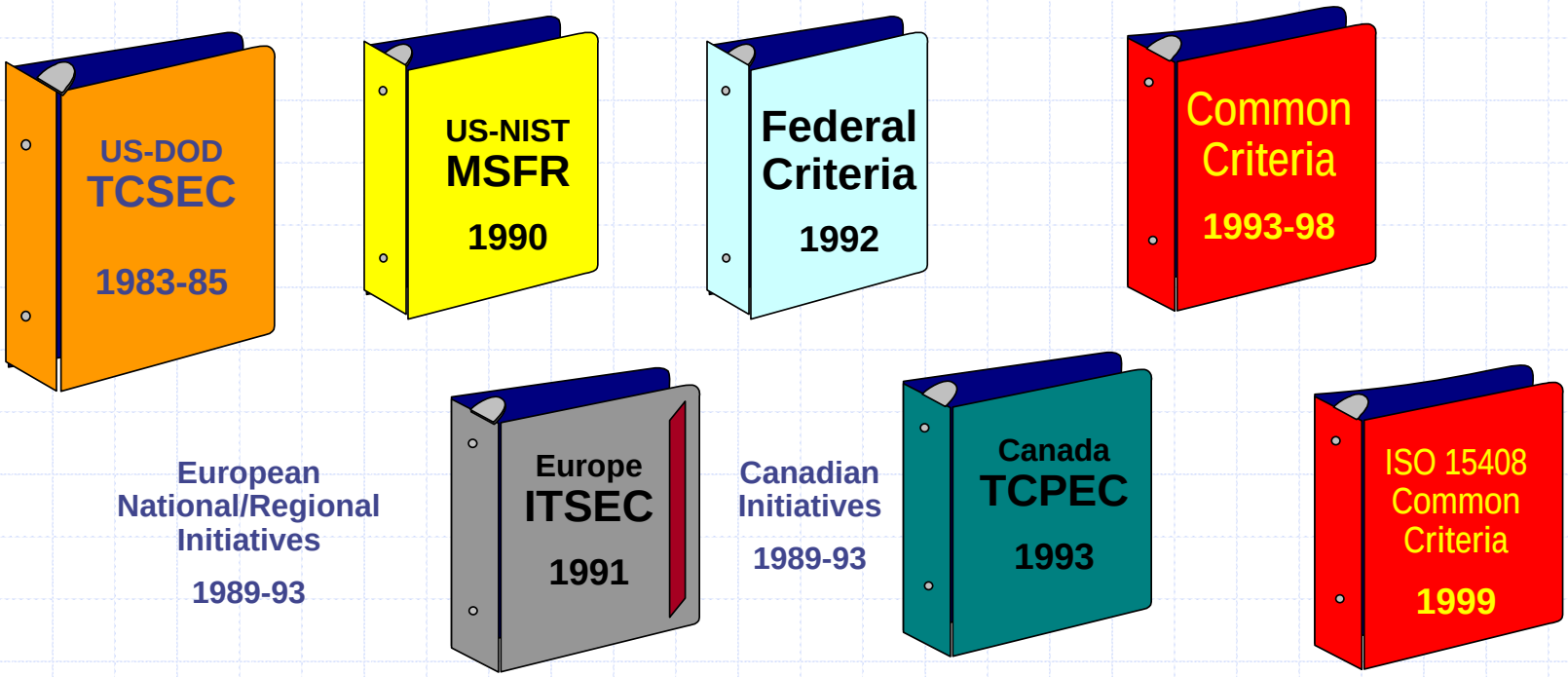
- For IT security requirements definition (by technology area and sector)
  - PPs
  - STs
- By encouraging vendors/developers to undergo IT security evaluations and assessments
- By giving acquisition preference/consideration to evaluated products (all things being equal)
  - Meets requirements
  - Meets cost-benefit (& other) requirements

First pass

- **What is CC?**
- CC Process?

An Evolutionary Process

Two decades of research and development...



TCSEC

- Known as Orange Book, DoD 5200.28-STD
- Four trust rating divisions (classes)
  - D: Minimal protection
  - C (C1,C2): Discretionary protection
  - B (B1, B2, B3): Mandatory protection
  - A (A1): Highly-secure

The Common Criteria

(International Standard-ISO/IEC 15408)

What the standard is –

- Common structure and language for expressing product/system IT security requirements (Part 1)
- Catalog of standardized IT security requirement components and packages (Parts 2 and 3)

How the standard is used: The CC Paradigm–

- Develop protection profiles and security targets -- specific IT security requirements and specifications for products and systems
- Evaluate products and systems against known and understood IT security requirements

IT Security Requirements

The Common Criteria defines two types of IT security requirements--

Functional Requirements

- for defining security behavior of the IT product or system:

• implemented requirements become security functions

Examples:

- ***Identification & Authentication***
- ***Audit***
- ***User Data Protection***
- ***Cryptographic Support***

Assurance Requirements

- for establishing confidence in security functions:

• correctness of implementation

• effectiveness in satisfying security objectives

Examples:

- ***Development***
- ***Configuration Management***
- ***Life Cycle Support***
- ***Testing***
- ***Vulnerability Analysis***

Evaluation Assurance Levels

Common Criteria defines seven hierarchical assurance levels--

	EAL Designation
EAL1	**Functionally Tested**
EAL2	**Structurally Tested**
EAL3	**Methodically Tested & Checked**
EAL4	**Methodically Designed, Tested & Reviewed**
EAL5	**Semiformally Designed & Tested**
EAL6	**Semiformally Verified Design & Tested**
EAL7	**Formally Verified Design & Tested**

Protection Profiles (generic) & Security Targets (specific)

Protection Profile contents

- **Introduction**
- **TOE Description**
- **Security Environment**
  - **Assumptions**
  - **Threats**
  - **Organizational security policies**
- **Security Objectives**
- **Security Requirements**
  - **Functional requirements**
  - **Assurance requirements**
- **Rationale**

Security Target contents

- **Introduction**
- **TOE Description**
- **Security Environment**
  - **Assumptions**
  - **Threats**
  - **Organizational security policies**
- **Security Objectives**
- **Security Requirements**
  - **Functional requirements**
  - **Assurance requirements**
  - ***TOE Summary Specification***
- ***PP Claims***
- **Rationale**

Examples

- ***Protection Profiles (Product Independent)***
  - **Operating Systems (C2, CS2, RBAC)**
  - **Firewalls (Packet Filter and Application)**
  - **Smart cards (Stored value and other)**
- ***Security Targets (Product Specific)***
  - **Oracle Database Management System**
  - **Lucent, Cisco, Checkpoint Firewalls**

Beneficiaries of the Standard

Consumer Consortia (Users Groups) –

- Use ISO/IEC 15408 to build protection profiles expressing their needs
- Work with developers to build matching IT products and systems

Individual IT Consumers –

- Look for protection profiles matching their security requirements -- use in procurement specifications
- In acquisitions, give preference to products that have been evaluated

Product and System Developers –

- Build products to meet targeted/selected protection profiles
- Use ISO/IEC 15408 to specify IT product and system security capabilities via security targets

Product Evaluators and Certifiers –

- Use ISO-compliant protection profiles and security targets to measure IT product and system compliance

First pass

- What is CC?
- **CC Process?**

Defining Requirements

ISO/IEC Standard 15408

A flexible, robust catalogue of standardized IT security requirements (features and assurances)

Protection Profiles

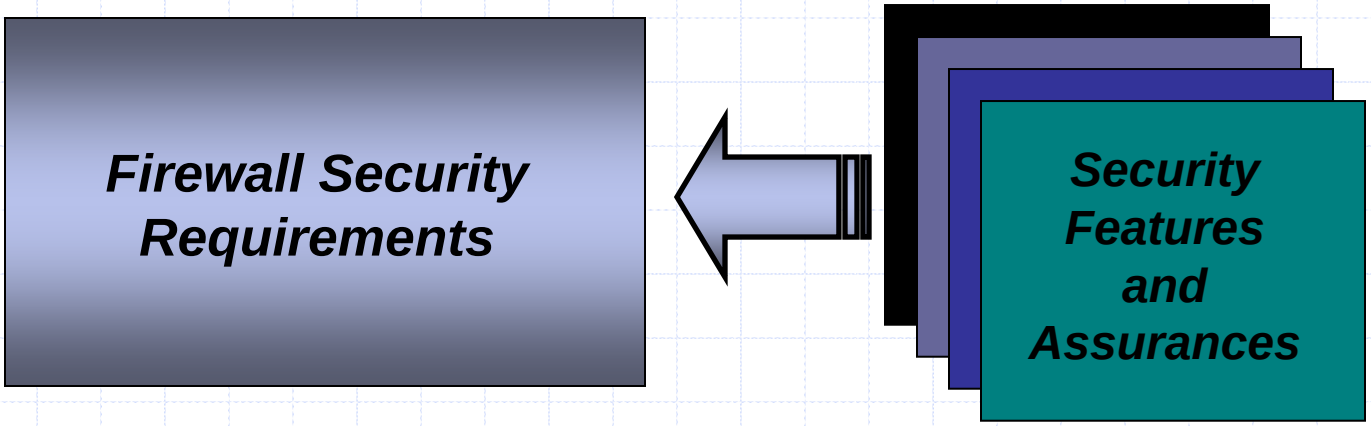
- ✓ Operating Systems
- ✓ Database Systems
- ✓ Firewalls
- ✓ Smart Cards
- ✓ Applications
- ✓ Biometrics
- ✓ Routers
- ✓ VPNs

Consumer-driven security requirements in specific information technology areas

Industry Responds

Protection Profile

Security Targets



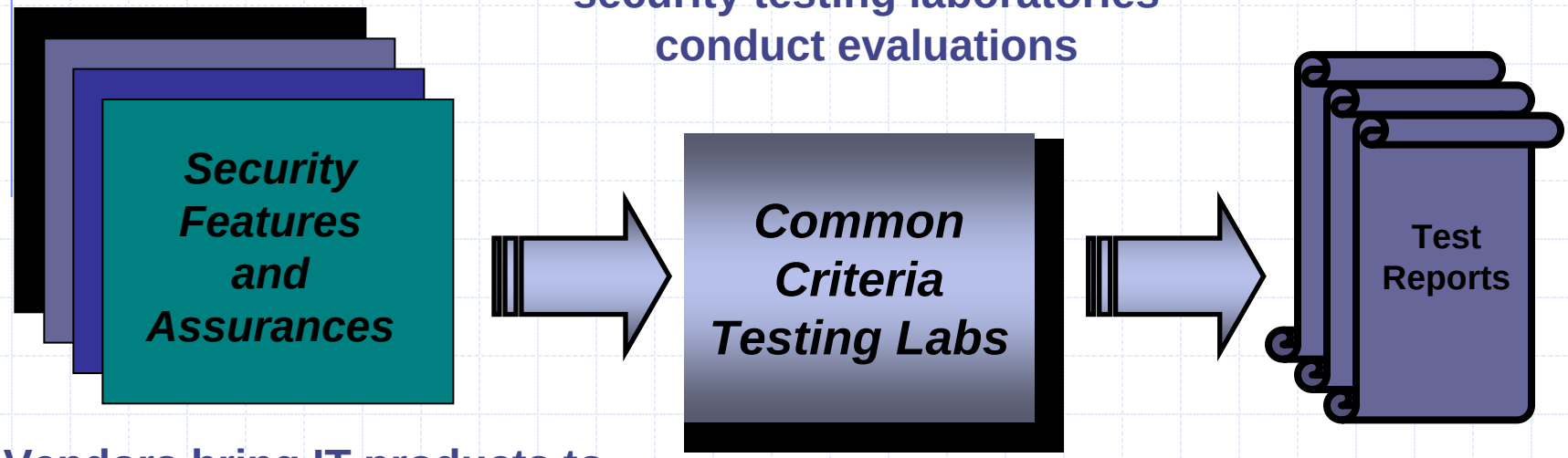
- ✓ CISCO Firewall
- ✓ Lucent Firewall
- ✓ Checkpoint Firewall
- ✓ Network Assoc. FW

Consumer statement of IT security requirements to industry in a specific information technology area

Vendor statements of security claims for their IT products

Demonstrating Conformance

Private sector, accredited security testing laboratories conduct evaluations

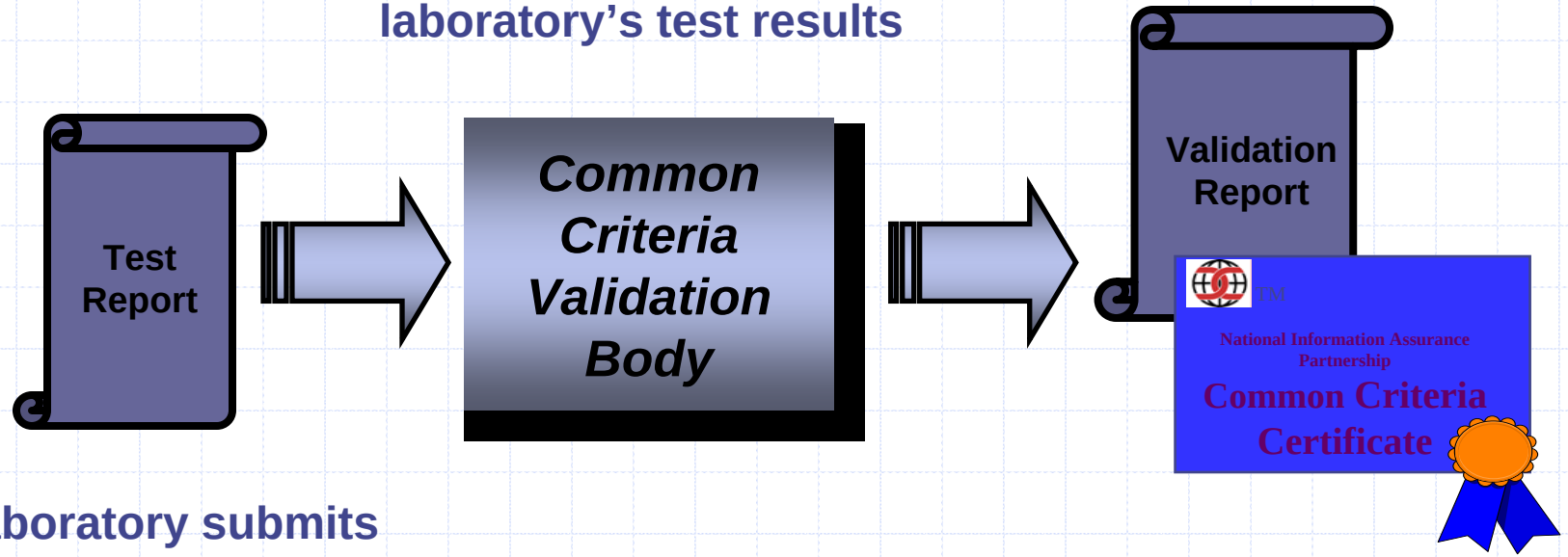


Vendors bring IT products to independent, impartial testing facilities for security evaluation

Test results submitted to the National Information Assurance Partnership (NIAP) for post-evaluation validation

Validating Test Results

Validation Body validates laboratory's test results



Laboratory submits test report to Validation Body

NIAP issues Validation Report and Common Criteria Certificate

Forums for Requirements Development

- Smart Card Security
- Healthcare Security
- Process Control Security
- Telecommunications Security

- Technology Areas
  - **Operating Systems**
  - **Database Systems**
  - **Firewalls**
  - **Biometrics**
- Industry Sectors
  - **Insurance**
  - **Audit and Controls**
  - **Banking and Finance**
  - **Manufacturing**

Examples of CC Certified Products

- Oracle 8 Release 8.1.7: EAL4, Oracle Corporation Certified in 2001/07
- Symantec Enterprise Firewall v7.0: EAL4, Symantec, Certified in 2002/05
- Gemplus 64k Java Card™: EAL5, Gemplus, Certified in 2002/02
- (etc.)

Second Pass

- Resources

Common Criteria Resources

Part 1: Introduction, PP and ST Contents and Formats

Part 2: Security Functional Requirements

Part 3: Security Assurance Requirements

Other Documents

Common Evaluation Methodology (CEM)

- **PP Evaluation Standard**
- **ST Evaluation Standard**
- **TOE Evaluation Standard**

Guide to Writing PP and ST

Terminology (1 of 2)

- **Evaluation (TOE):** ***An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.***
- **Protection Profile (PP):** ***An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.***
- **Security Target (ST):** ***A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.***
- **TOE Security Functions (TSF):** ***A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct***

Terminology (2 of 2)

- **Threats:** ***Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and /or denial of service.***
- **Organizational Security Policy:** ***A set of rules, procedures, practices, and guidelines imposed by an organization upon its operations and to which the TOE may have to comply.***
- **Secure Usage Assumption:** ***Describes the security aspects of the environment in which the TOE will be used or is intended to be used.***
- **Security Objective:** ***Reflects the intent to counter identified threats and/or address any identified organizational security policies and/or***

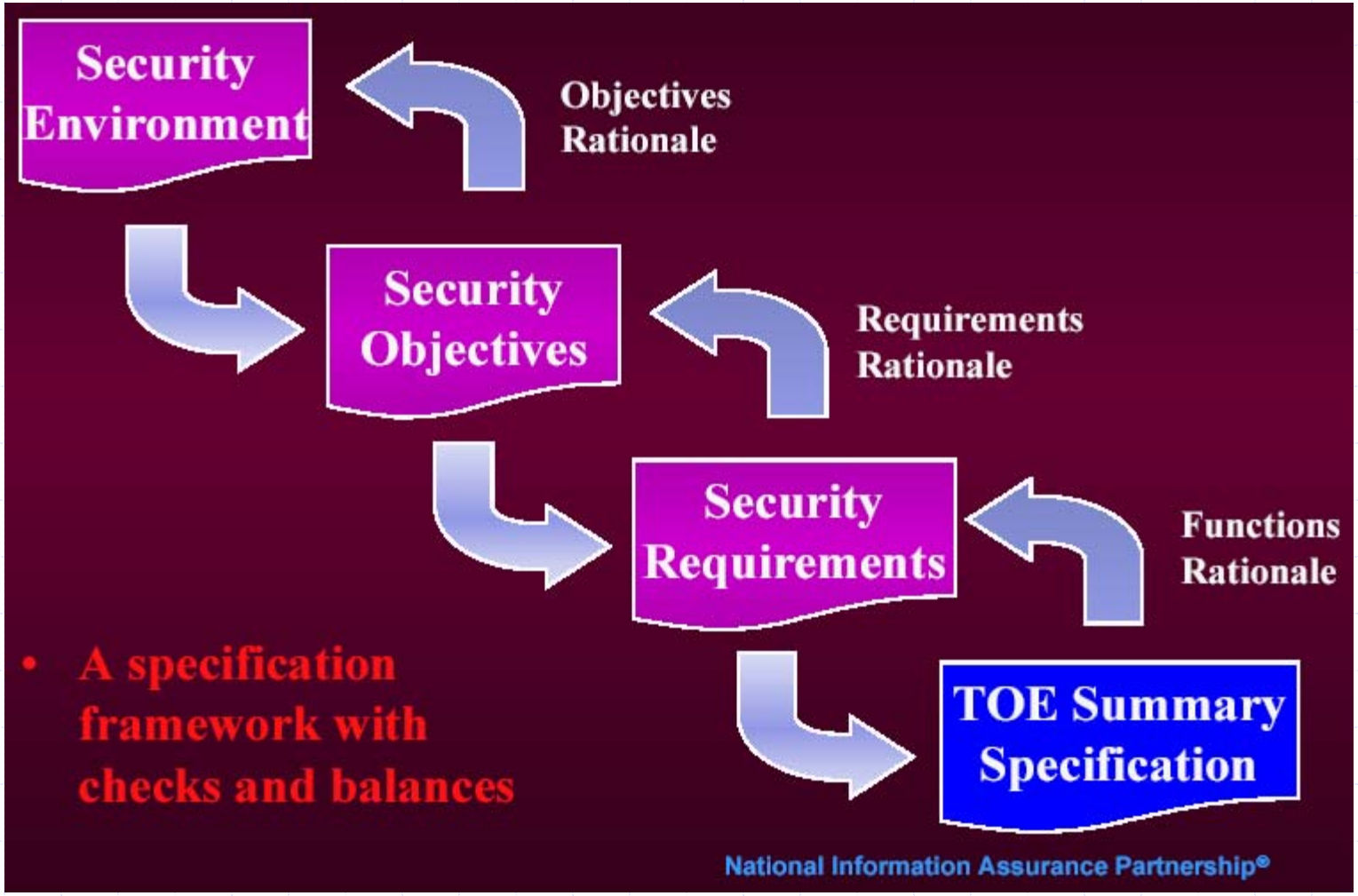
Protection Profiles

- Answers the question:
  - What do I need in a security solution?
- Implementation independent
- Multiple implementations may satisfy PP requirements
- Authors can be both consumers and producers of IT products and systems
- Makes a statement of implementation independent security needs
- Example
  - generic operating system with discretionary access controls, audit, and identification and

Security Targets

- Answers the question:
  - What do you provide in a security solution?
  - Implementation specific
  - Authors can be product vendors,product developers, or product integrators
  - defines the implementation dependent capabilities of a specific product
  - Examples:
    - Microsoft NT 4.0.0.2 (TOE)
    - Sun OS 4.7.4 (TOE)

PP/ ST specification framework



TOE Security Environment

- Secure Usage Assumptions
  - The non-IT security aspects of the environment in which the TOE will be used or is intended to be used.
- Threats
  - The ability to exploit a vulnerability by a threat agent.
- Organizational Security Policies
  - A set of rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Secure Usage

- Describes the security aspects of the environment in which the TOE will be used or is intended to be used
- Information about intended usage and the environment:
  - intended application, potential asset value, and usage limitations
  - physical issues, connectivity issues, and personnel issues
  - must not impose requirements on the TOE or on its IT environment
  - generate objectives for the (non-IT) environment

Threat

- The ability of a threat agent to mount an attack on an asset, and the result of that attack
- Threats provide a basis for statement of countermeasures
- A well-written threat statement addresses
  - Threat Agent and/or Attacker
  - The Attack
  - Assets
  - Results

Security Policies

- Organizational Security Policy:
  - A set of rules, procedures, practices, and guidelines imposed by an organization upon its operations and to which the TOE may have to comply.
  - Organizationally-Imposed Requirements
    - Passwords Shall Be 8 Characters
    - Cryptography Shall Be Used for Intra-Node Communication

Environment Examples

- A.Physical_Protection
  - The TOE is installed in a restricted and controlled access area sufficient to prevent unauthorized physical access to the TOE.
- T.Intercept
  - An non-administrative user obtains unauthorized access to controlled information by intercepting information transmitted to/from the TOE.
- P.Accountability
  - The authorized users of the TOE shall be held accountable for their actions within the TOE.

Security Objectives

- Establish the basis for the selection of security requirements (functional & assurance)
- Based completely upon the statement of the security environment
- Objectives describe
  - Support for assumptions
  - Mitigation of threats (eliminate, minimize, monitor)
  - Enforcement organizational security policy

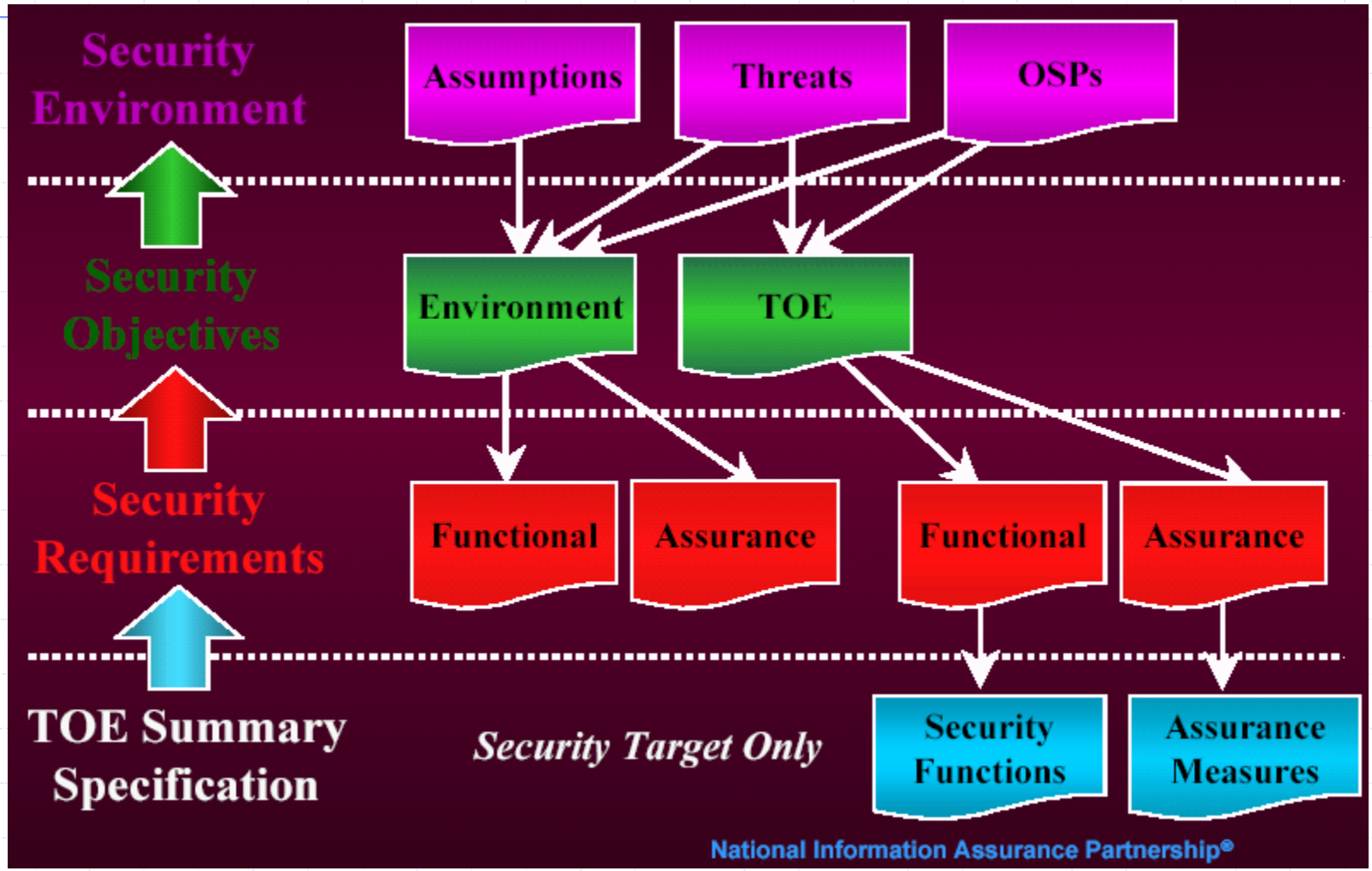
Types of Security Objectives

- Security objectives for the TOE
  - Implemented by security requirements allocated to the TOE
  - Security objectives for the environment
    - Implemented by security requirements allocated to the IT systems that interact with the TOE
    - Implemented by personnel and procedural means
    - Outside the scope of the CC

Creating PPs/ STs

- **top down** approach
  - usually PPs
  - start with environment
  - derive objectives
  - select requirements
- **technology** specific
  - usually PPs
  - survey product in technology (requirement)
  - identify function in environment
  - complete specification
- **product** approach
  - usually STs
  - define what product does (functional requirements)
  - define existing documentation/ assurance (assurance requriement)
  - "back in" environment

PP/ST Framework



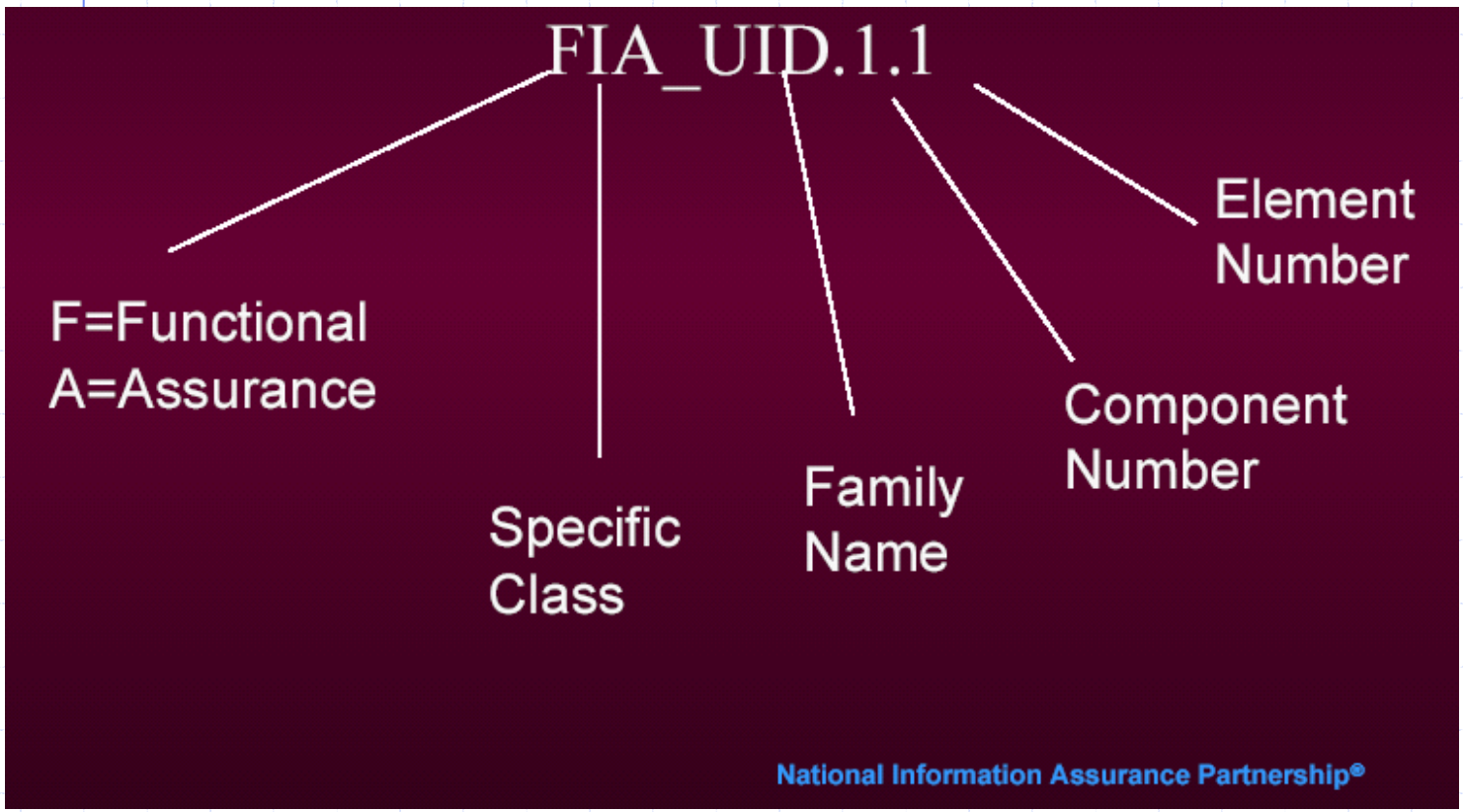
Definitions

- Class - for organizational purposes; all members share a common intent but differ in coverage of security objectives.
- Family- for organizational purposes; all members share security objectives but differ in rigor or emphasis
- Component - describes an actual set of security requirements; smallest selectable set
- Element - members of a component; cannot be selected individually; explicit shall statements

Security Functionality Classes

- Audit (FAU)
- Cryptography Support (FCS)
- Communications (FCO)
- User Data Protection (FDP)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Privacy (FPR)
- Protection of the TOE Security Functions (FPT)
- Resource Utilisation (FRU)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

Interpreting Functional Requirement Names



Class

↓

Family

↓

Component

↓

Element

Requirements Rationale

- Threats/OSPs (through security objectives) drive functional requirement selection
- Rationale must demonstrate that the functional requirements are suitable to meet and traceable to the security objectives
- The rationale must demonstrate:
  - why the choice of security requirements meets an objective
  - functional & assurance requirements are not contradictory and are complete
  - strength of function (SOF) claims are consistent with the security objectives

Operations on Requirements (Functional)

- Types of operations
  - assignment
  - selection
  - refinement
  - iteration
- Functional requirements have placeholders indicating where assignment and selection operations are allowed
- Refinement and iteration may be performed on any functional requirement

Assignment Operations

- Specification of a parameter filled in when component is used
- “Fill in the Blank” operation
- Allows PP/ST writer to provide information relating to application of the requirement
- The PP writer may defer completing assignments,
  but the ST writer must complete all assignments

Selection Operations

- Specification of elements selected from a list given in the component
  - "Multiple Choice" operation
  - Allows PP/ST writer to select from a provided list of choices
  - The PP writer may defer completing selections,
    but the ST writer must complete all selections

Refinement Operations

- A mechanism to tailor a requirement by specifying additional detail in order to meet a security objective
- Can be performed on any functional component
- Rules for refinement:
  - the refinement shall only restrict the set of possible acceptable
  - functions used to implement the requirement
  - the refinement may not levy completely new requirements
  - the refinement may not increase the list of dependencies of the requirement being refined
  - the refinement may provide an elaboration or interpretation
  - the refinement may not eliminate the requirement

Iteration Operations

- Repetitive use of the same component to address different aspects of the requirement being stated (e.g., identification of more than one type of user).
- Can be performed on any functional component

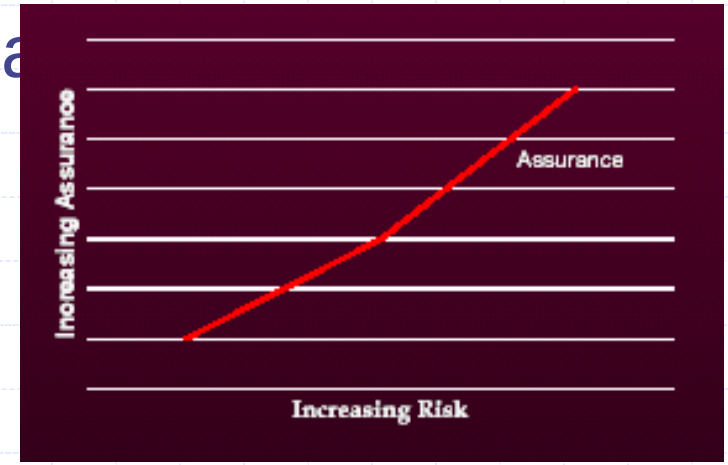
Dependencies
(Functional Components)

- Some requirement components are not self sufficient
- Some functional requirement components have functional and assurance dependencies
- Some dependencies may be eliminated with sufficient rationale

What is Assurance?

- *Assurance is a property of the TOE which gives confidence that the claimed security measures of the TOE are effective and implemented correctly.*

- Why do we need a



Common Criteria Part 2: Annexes

- Annex A:
  - *Security Functional Requirements Application Notes*
    - Dependency Table
- Annexes B - M:
  - *Similar to Part 2 but more informative*
    - user notes
    - evaluator notes
    - documentation notes

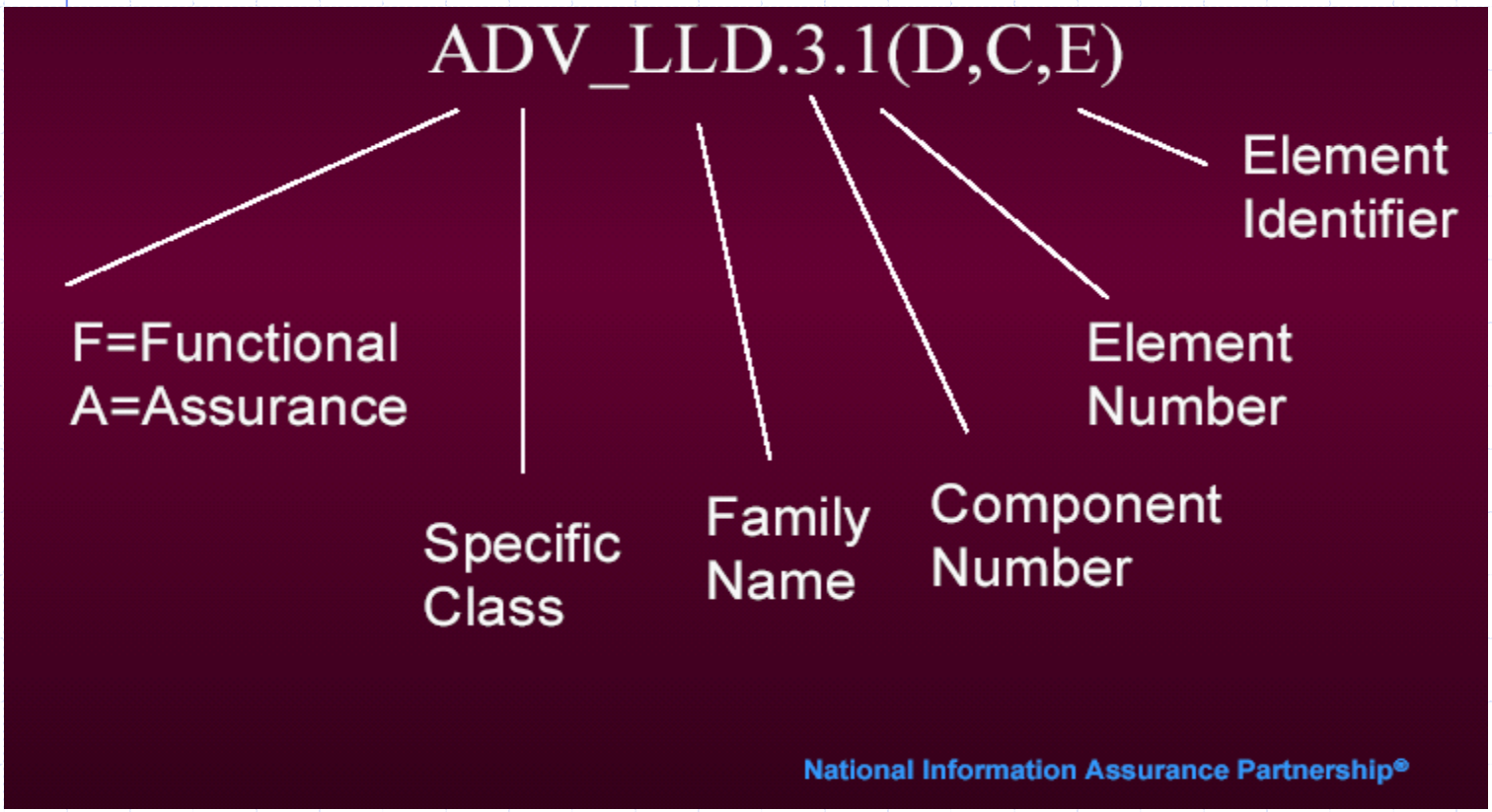
How to gain Assurance?

- Analysis of the correspondence between TOE design representations
- Analysis of the TOE design representations against the requirements
- Analysis of functional tests coverage, and results
- Independent functional testing
- Penetration testing
- Verification of mathematical proofs
- Analysis of guidance documents
- Analysis of processes and procedures
- Checking that processes and procedures are being applied

Definitions

- Class - for organizational purposes; all members share a common intent but differ in coverage of security objectives.
- Family- for organizational purposes; all members share security objectives but differ in rigor or emphasis
- Component - describes an actual set of security requirements; smallest selectable set
- Element - members of a component; cannot be selected individually; explicit shall statements

Interpreting Assurance requirement Names



Class

↓

Family

↓

Component

↓

Element

Security Assurance Classes

- Configuration Management (ACM)
- Delivery and operation (ADO)
- Development (ADV)
- Guidance documents (AGD)
- Life Cycle Support (ALC)
- Tests (ATE)
- Vulnerability assessment (AVA)
- Evaluation Criteria (APE, ASE)
- Assurance Maintenance (AMA)

Dependencies
(Assurance Components)

- Dependencies have same meaning as for functional requirements
- Table A.1 (Part 2: Annexes page 4) identifies all dependencies
  - direct (as stated in the requirement)
  - indirect (as a result of “chasing down” the dependencies)

Operations on Requirements (Assurance)

- Iteration
- Refinement

Requirements Packages

- Reusable set of functional or assurance components combined together to satisfy a set of
  identified security objectives
- In CC Part 3 there are 7 assurance packages called Evaluation Assurance Levels (increasing
  rigor and formalism from EAL1 to EAL7)
- Packages being specified for levels of robustness
  – Basic and Medium are in draft

Evaluation Assurance Levels (EALs)

- Provide an increasing scale
- This scale balances:
  - level of assurance obtained
  - cost/feasibility of acquiring it

Considerations for EAL Selection

- Value of the assets
- Risk of the assets being compromised
- Current state of practice in definition and construction of the TOE
- Security Environment
- Development, evaluation, & maintenance costs
- Resources of adversaries
- Functional requirement dependencies

EAL1 - Functionally Tested

- Confidence in current operation is required
- No assistance from TOE developer
- Applicable where threat to security is not serious
- Incomplete independent testing against specification and guidance documentation

EAL2: Structurally Tested

- Requires some cooperation of the developer
- Low to moderate of independently assured security
- Adds requirements for configuration list, delivery,
  high-level design documentation, developer functional testing, vulnerability analysis, more extensive (but still not complete) independent testing

and Checked

- Requires positive security engineering at the design stage without substantial changes in existing practices
- Moderate assurance through investigation of product and development environment controls, and high-level design documentation
- Places additional requirements on testing (now complete), development environment controls and TOE configuration management

EAL4: Methodically Designed, Tested, and Reviewed

- Requires security engineering based on good commercial development practices
- Highest level likely for retrofit of an existing product
- Additional requirements on design, implementation, vulnerability analysis, low level design documentation, development and system automated configuration management, and an informal security policy model

EAL5: Semiformally Designed and Tested

- Higher assurance, risk situations
- Requires rigorous commercial development practices and moderate use of specialist engineering techniques
- Introduces structured implementation of TSF
- Additional requirements on semi-formal functional specification, high-level design, and their correspondence, increased vulnerability testing, full implementation representation, and covert channel analysis

EAL6: Semiformally Verified Design and Tested

- Applicable to a rigorous development environment
- High assurance for high value assets/risk situations
- Additional requirements on analysis, layered TOE design, semi-formal low-level design documentation, complete CM system automation and a structured development environment, and increased vulnerability testing/covert
  channel analysis

EAL7: Formally Verified Design and Tested

- Maximum assurance for extremely high risk situations
- Generally for experimental application
- Assurance is gained through application of formal methods in the documentation of the functional specification and high-level design
- Additional requirements for complete developer test analysis, complete independent confirmation of the test results, and complete documentation of the structure of the TSF

EAL Augmentation

- The tailoring of an existing Evaluation Assurance Level (EAL)
  - Specify assurance component(s) in addition to those in an existing
- Allowed augmentation operations
  - Specify a higher component in the same family
  - Specify a higher component from another family
  - Specify new components that are not contained in an EAL
- Disallowed augmentation operation
  - Removal of components from an EAL definition

U.S. Government Packages

- Based on DoDI 8500.2 and NIST guidance,
  U.S. Government Protection Profiles are developed according to the following defined packages:
  – U.S. Government Basic Robustness
  – U.S. Government Medium Robustness
  – U.S. Government High Robustness

Basic Robustness

- Basic Robustness provides assurance by an analysis of the TOE security functions using
  - guidance documentation,
  - functional specification,
  - high level design, and
  - interface specification.
- EAL 2 augmented portions require
  - accuracy of system documentation,
  - the tracking and correction of system flaws.

Basic Robustness (

- Assurance requirements include all components of
  EAL 2 augmented with
  - Flaw Reporting Procedures (ALC_FLR.2)
  - Examination of Guidance (AVA_MSU.1)
- Allow “Partial” TOEs
  - Software only
  - Portion of system (e.g., database only)

Medium Robustness

- Medium robustness provides assurance by an analysis of the TOE security functions using
  – architectural design documents,
  – low-level design of the TOE,
  – implementation representation of the entire TSF,
  – complete interface specifications,
  – systematic cryptographic module covert channel,
  – informal TOE security policy model, and
  – modular TOE design.
- Allow only “complete” TOEs (i.e. hardware

Medium Robustness

- Medium robustness includes components of EAL 4 augmented with
  - Implementation of the TSF (ADV_IMP.2)
  - Testing: Low-level Design (ATE_DPT.2)
  - Flaw Reporting Procedures (ALC_FLR.2)
  - Moderately Resistant (AVA_VLA.3)
  - Functional Specification (ADV_FSP_(EXP).1
  - Security-enforcing High-level design (ADV_HLD_(EXP).1)
  - Security-enforcing Low-level design (ADV_LLD_(EXP).1
  - Architectural Design with Justification (ADV_ARC_(EXP).1
  - Modular Decomposition (ADV_INT_(EXP).1)
  - Systematic Cryptographic Module Covert Channel Analysis (AVA_CCA_(EXP).1)

High Robustness

- High robustness will build upon Medium robustness requirements and are currently being targeted at the EAL 6 level.
- The exact assurance requirements are still being developed.

Lab Related Information

- Activities:
  - Generation of PP and ST
  - Verification of Functional requirements according to given ST
- Objective:
  - Familiarize with the CC methodology
    - Usage of existing class, family and components
    - Creation of new class and family (if necessary)
  - Validate products according to PP/ST
- Further readings recommended
  - Types and usage of functional and assurance class and family