Common Criteria

Common Criteria
Evaluations Made ~~Easy~~
Less Difficult

Ms. Jean Schaffer
NIAP Director
(410) 854-4458

Mr. Olin Sibert
Senior Validator
(781) 863 5549

Goals

- Recap of benefits of a CC evaluation
  - And policies that require evaluations
- Explain what is needed to complete an evaluation
  - Successfully
  - Promptly
  - At reasonable cost
- Describe
  - Concepts
  - Process
  - Criteria
  - Documentation Requirements

Audience Assumptions

- You have a product (or plan)
  - It has existing, well-defined security features
  - You are responsible for development and delivery
- You understand security principles
- But… you are not intimately familiar with Common Criteria and evaluations

Benefits

- Improved Product Security
  - ~ 35-40% of products evaluated resulted in new release or patch to fix flaws
  - Number and severity of flaws mirror Evaluation Assurance Level
  - Conformance to U.S. Government Protection Profiles drove ~90% of security additions and enhancements
- Validation of Product Security Claims

NSTISSP No. 11 - Jan 2000
Revised July 2003

- Effective 1 July 2002, all ***COTS*** IA and IA-Enabled products must be evaluated by:
  - International Common Criteria Mutual Recognition Arrangement
  - NIAP Evaluation and Validation Program (CCEVS)
  - NIST FIPS validation program
  - All ***GOTS*** IA or IA enabled products must be evaluated by NSA or an NSA approved process.

Revised NSTISSP No. 11

- **Added** Annex, Deferred Compliance Authorization (DCA) Guidelines
  - No DCA's for encryption products.
  - DCA is for a specific COTS product for a specific application within the IT enterprise – **not** a blanket approval
  - Heads of federal departments or agencies (or their sub-delegated CIO) are the review and DCA approval authority for their respective organizations.
  - Must report DCAs to NSA/V1 for consolidated reporting to CNSS Chair.

DoD Directive 8500.1
24 Oct 2002

- All IA or IA-enabled products incorporated into DoD information systems must comply with NSTISSP 11
- Products must be satisfactorily evaluated and validated either
  - prior to purchase or
  - as a condition of purchase, the vendor's products will be satisfactorily evaluated and validated.
- Purchase contracts shall specify that product validation will be maintained for subsequent releases.

DoD Instruction 8500.2
12 Feb 2003

- Defines generic “robustness” levels of basic, medium, and high and assigns “baseline levels” of IA services dependent on value of information and environment
- If Government Protection Profile (PP) exist for a specific technology area
  - products must get evaluated against PP.
- If no Government PP exist for a specific technology area
  - as a condition of purchase, products must be submitted for evaluation at the appropriate EAL level as determined by ISSE and DAA.

NIST Special Pub 800-23

- Applies to U.S. Civil Government
- Recommends CC evaluations/validations

Agenda

- General Concepts
- Understanding the Evaluation Process
- Using the Evaluation Criteria
- Providing the Evaluation Evidence

Agenda

- General Concepts
- Understanding the Evaluation Process
- Using the Evaluation Criteria
- Providing the Evaluation Evidence

Concepts

- What is needed for an evaluation?

Concepts

- What is needed for an evaluation?
  - Sponsor

Concepts

- What is needed for an evaluation?
  - Sponsor
  - Product

Concepts

- What is needed for an evaluation?
  - Sponsor
  - Product
  - Requirements

Concepts

- What is needed for an evaluation?
  - Sponsor
  - Product
  - Requirements
  - Scheme

Concepts

- What is needed for an evaluation?
  - Sponsor
  - Product
  - Requirements
  - Scheme
  - Evaluation Laboratory

Concepts

- What is needed for an evaluation?
  - Sponsor
  - Product
  - Requirements
  - Scheme
  - Evaluation Laboratory
  - *Unnatural taste for acronyms*

Concept – Sponsor

- Formal concept from CC
  - *Sponsor* is responsible for TOE and its evaluation
  - Usually Sponsor == Product Developer / Manufacturer
    - Can be complicated for multi-component products
  - Developer may involve *consultant(s)* in supporting roles
    - Evidence preparation
    - Evaluation management
  - Consultant(s) vary widely in their expertise. Contact references prior to signing the contract.

What Makes a Product?

- Not just what comes in the box!
- In the “CC world”, a product—that is, a *product to be evaluated*—has a variety of other required aspects.

What Makes a Product? (1)

TOE (Target of Evaluation)

The product being evaluated

Defined by *Security Target (ST)* document

Described by *TOE Summary Specification* (TSS) in ST

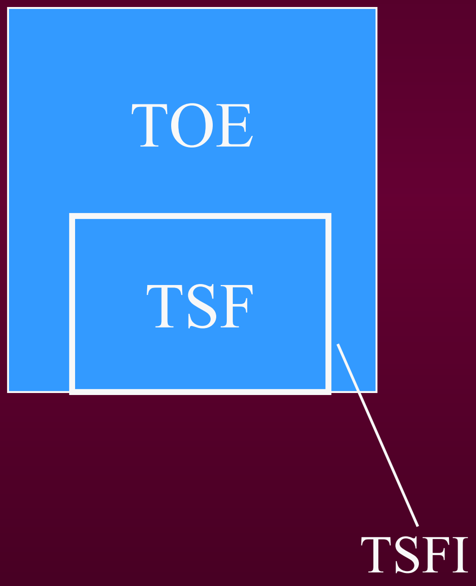
TOE

What Makes a Product? (2)

TOE (Target of Evaluation)
The product being evaluated

TSF (TOE Security Functions)
The security-enforcing part, and the part that is specified, described, and tested for evaluation.

TSFI (TSF Interface)
The TSF's interaction with the outside
Described by ADV_FSP documents



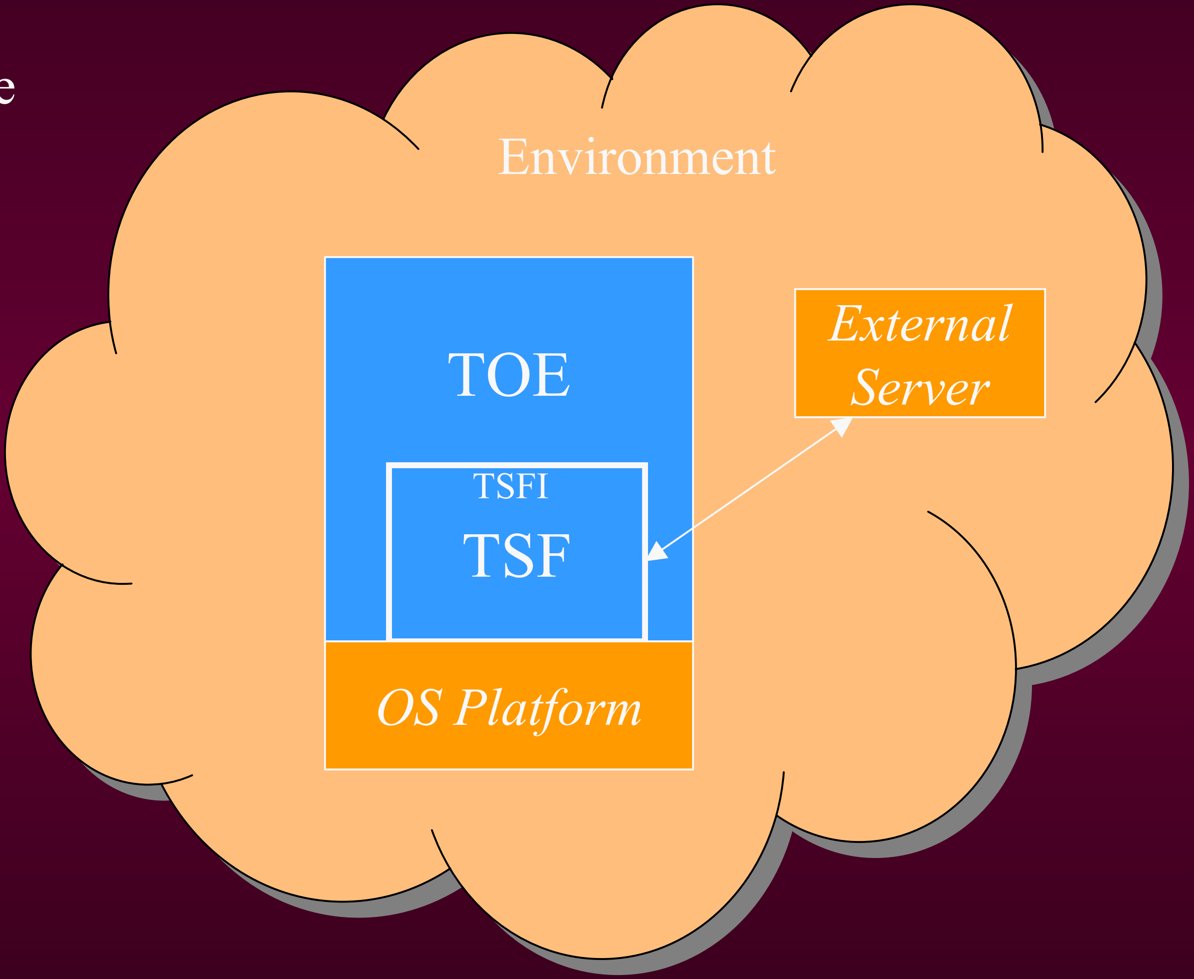
What Makes a Product? (3)

Environment

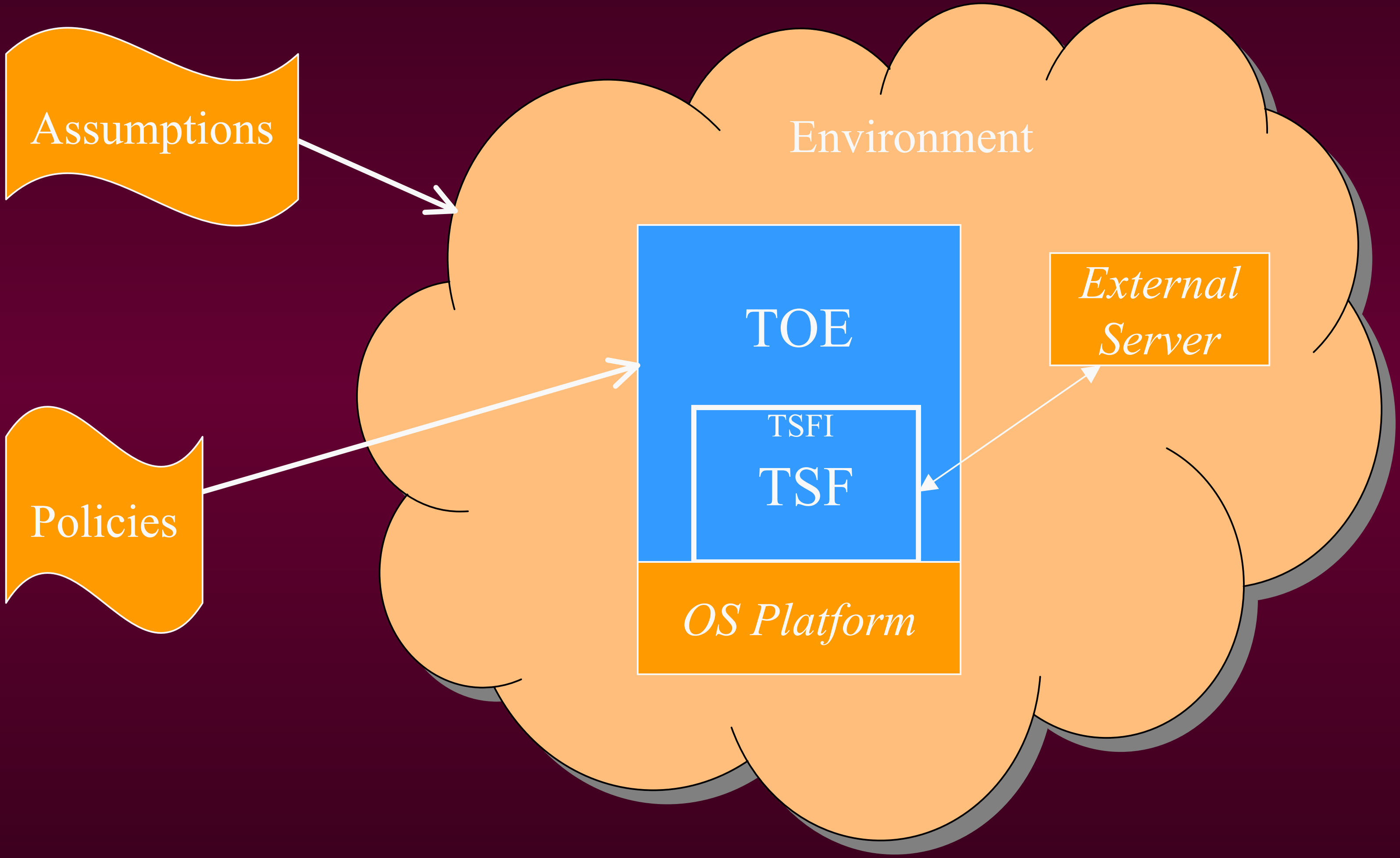
- Everything outside the TOE, and on which the TOE depends

Examples:

- *External server for authentication*
- *OS platform for software-only TOE*



What Makes a Product? (4)



Concept – Product

- Operational Product
  - TOE (Target of Evaluation)
  - TSF (TOE Security Functions)
  - TSFI (TSF Interface)
- Security and Assurance Claims
  - ST (Security Target)
- Supporting *Evidence*
  - Documents supporting assurance claims

Concept – Security Target

- Security Objectives
- SFRs (Security Functional Requirements)
  - Derived from CC's base functional requirements
  - Augmented with product-specific claims
  - Together, they constitute TSP – TOE Security Policy
- TSS (TOE Summary Specification)
- Environment
  - Threats, Assumptions, Policies
- Mappings

Concepts – Functions and Assurance

- Security Functions
  - What the product *does*
  - Easy to measure—does it fulfill its specifications?
  - Tailored to the product—CC allows great flexibility
- Security Assurance
  - How *well* the product performs its functions
  - Hard to measure—“well” has many meanings
  - Assurance is “packaged” as Evaluation Assurance Levels (EALs)

Concept – Criteria

- CC (Common Criteria)
  - Defines functional and assurance requirements
  - V2.2 is ISO 14508
  - V3.0 coming this summer
- CEM (Common Evaluation Methodology)
  - Defines how an evaluation is conducted
  - V2.2 will be published as ISO 18405
- PPs (Protection Profiles)
  - Application-specific “bundles” of requirements

Concept – Scheme

- National authority for overseeing evaluations
  - Oversees (*validates*) evaluations by Labs
  - Issues *certificates*
- Schemes are bound by Common Criteria
  - Evaluations are mutually recognized (at EAL 4 and below)

Common Criteria Recognition Arrangement (CCRA)

US Canada UK Germany France

Certificate Producers

Japan Australia/New Zealand

Netherlands Finland Greece Italy Norway Spain Israel

Sweden Austria Turkey Hungary Czech Republic

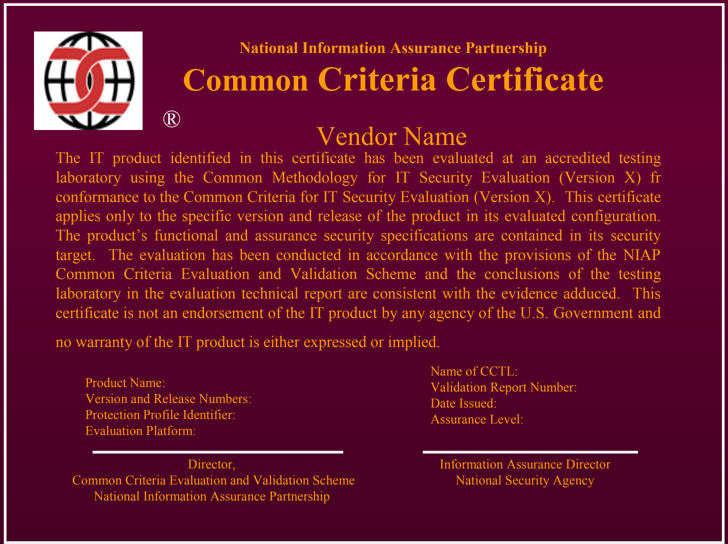
Certificate Consumers

NIAP

- NIAP (National Information Assurance Partnership)
  - U.S. Government initiative
  - Collaboration between
    - National Security Agency (NSA)
    - National Institute of Standards and Technology (NIST)
  - Functions
    - Security Requirements Definition and Specification
    - Product and System Security Testing, Evaluation, and Assessment
      - Oversight for the U.S. Scheme (CCEVS – Common Criteria Evaluation and Validation Scheme)

Common Criteria Evaluation and Validation Scheme (CCEVS)

- Oversees and validates evaluations
- Issues Certificates to vendors for successful completion of evaluations.
  - Not an NSA or NIST endorsement
  - Not a statement about goodness of product



National Information Assurance Partnership

Common Criteria Certificate

®

Vendor Name

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version X) fr conformance to the Common Criteria for IT Security Evaluation (Version X). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

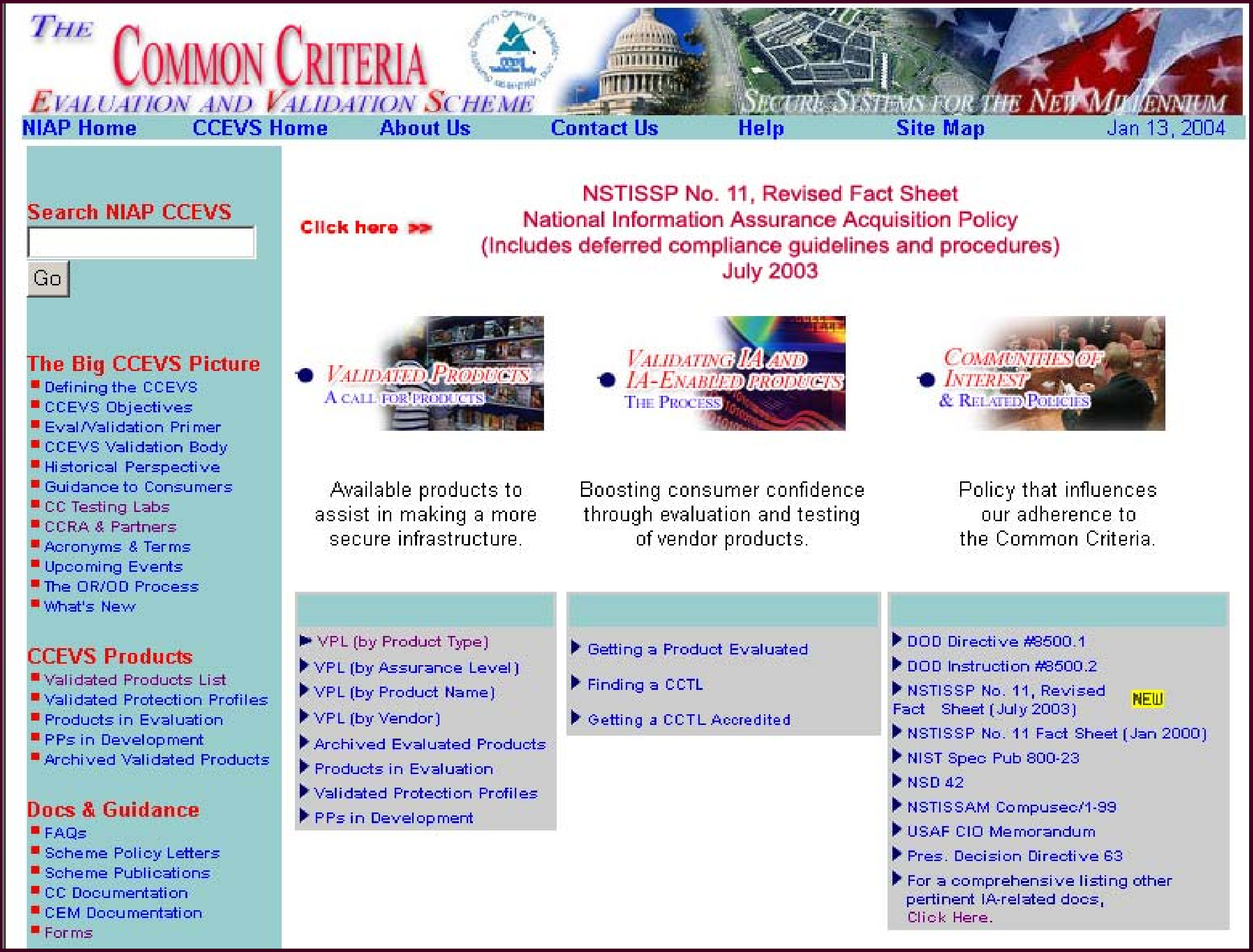
Product Name:
Version and Release Numbers:
Protection Profile Identifier:
Evaluation Platform:

Name of CCTL:
Validation Report Number:
Date Issued:
Assurance Level:

Director,
Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Information Assurance Director
National Security Agency

CCEVS Information http://niap.nist.gov//cc-scheme



THE COMMON CRITERIA EVALUATION AND VALIDATION SCHEME

SECURE SYSTEMS FOR THE NEW MILLENNIUM

NIAP Home | CCEVS Home | About Us | Contact Us | Help | Site Map | Jan 13, 2004

Search NIAP CCEVS

Go

The Big CCEVS Picture

- Defining the CCEVS
- CCEVS Objectives
- Eval/Validation Primer
- CCEVS Validation Body
- Historical Perspective
- Guidance to Consumers
- CC Testing Labs
- CCRA & Partners
- Acronyms & Terms
- Upcoming Events
- The OR/OD Process
- What's New

CCEVS Products

- Validated Products List
- Validated Protection Profiles
- Products in Evaluation
- PPs in Development
- Archived Validated Products

Docs & Guidance

- FAQs
- Scheme Policy Letters
- Scheme Publications
- CC Documentation
- CEM Documentation
- Forms

Click here >>

NSTISSP No. 11, Revised Fact Sheet
National Information Assurance Acquisition Policy
(Includes deferred compliance guidelines and procedures)
July 2003

VALIDATED PRODUCTS
A CALL FOR PRODUCTS

Available products to assist in making a more secure infrastructure.

- VPL (by Product Type)
- VPL (by Assurance Level)
- VPL (by Product Name)
- VPL (by Vendor)
- Archived Evaluated Products
- Products in Evaluation
- Validated Protection Profiles
- PPs in Development

VALIDATING IA AND IA-ENABLED PRODUCTS
THE PROCESS

Boosting consumer confidence through evaluation and testing of vendor products.

- Getting a Product Evaluated
- Finding a CCTL
- Getting a CCTL Accredited

COMMUNITIES OF INTEREST & RELATED POLICIES

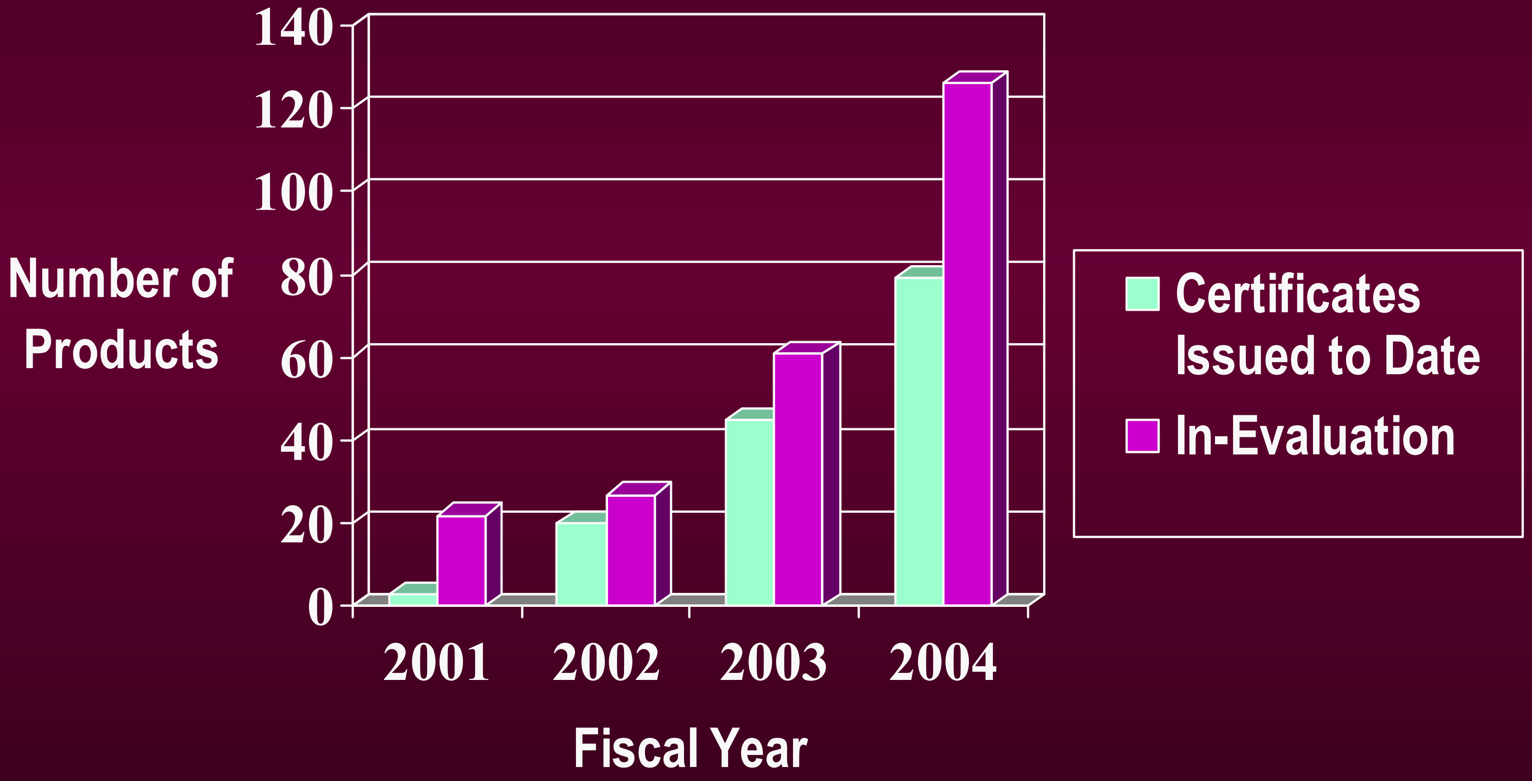
Policy that influences our adherence to the Common Criteria.

- DOD Directive #8500.1
- DOD Instruction #8500.2
- NSTISSP No. 11, Revised Fact Sheet (July 2003) NEW
- NSTISSP No. 11 Fact Sheet (Jan 2000)
- NIST Spec Pub 800-23
- NSD 42
- NSTISSAM Compusec/1-99
- USAF CIO Memorandum
- Pres. Decision Directive 63
- For a comprehensive listing other pertinent IA-related docs, Click Here.

NIAP CCEVS Project Status

- As of January 2005
  - 132 products “in progress”
  - 86 certificates issued to date
  - 35 cancelled/withdrew

NIAP CCEVS Project Status



Concept – Evaluation Laboratory

- Commercial organization that performs evaluations
  - Follows CEM rules
  - Uses own processes, reporting, analysis techniques
- Labs are *accredited* by NVLAP (National Voluntary Laboratory Accreditation Program) and accepted by NIAP to be part of the Scheme
- Lab organizations also develop evidence
  - Consulting personnel *strictly separate* from evaluation personnel

U.S. Approved Common Criteria Testing Laboratories

Booz, Allen & Hamilton	Linthicum, Maryland
Arca (was Cable & Wireless)	Sterling, Virginia
COACT, Inc.	Columbia, Maryland
Computer Sciences Corp.	Annapolis Junction, MD
Criterian Independent Lab	Fairmont, West Virginia
CygnaCom Solutions, Inc.	McLean, Virginia
InfoGard Laboratories, Inc	San Luis Obispo, CA
Lockheed-Martin IS&S SSO	Hanover, MD
Science Applications Int’l Corp.	Columbia, MD

Candidate Common Criteria Testing Laboratories

Ashton Security Labs	Herndon, VA
Atsec Information Security Corporation	Austin, Texas
BKP Security Labs	Santa Clara, CA
BT CC Testing Lab	Reston, VA
Corsec CCTL	Fairfax,VA
DSD Information Assurance Lab (DIAL)	Fairmont, WV

CCTL Evaluation Facts

- Prices and Evaluation Time for *typical* evaluations:
  - EAL 2 (e.g. IDS,Firewall,Router,Switch) ~$100K - $170K, 4-6 months
  - EAL 3 (e.g. Firewall, IDS – PP Compliant) ~$130K - $225K, 6-9 months
  - Simple EAL 4 (e.g. IDS, Firewall, Router, Switch) ~$175K - $300K, 7-12 months
  - Complex EAL 4 (e.g. Operating System – PP Compliant) ~$300K - $750K, 12-24 months
- Fixed Price Contracts generally are higher cost

CC Evaluation Facts

- Greatest influence for Time and Costs is driven not by the process but by the commercial market
  - CCTL selected factors
  - Time needed by vendor to prepare evidence
  - Suitability and quality of externally-prepared evidence
  - Vendor’s prior paradigm (design documentation and testing)

Concept – Evaluation Process

- Pre-evaluation / Qualification
- Evidence preparation
- Evaluation activities
- Validation
- Completion (Certificate)

Concept – Requirements

- Security Functional Requirements (SFRs)
- Assurance Requirements
  - Evaluation Assurance Level (EAL1-7) Packages
- Requirements are
  - Defined in CC, PPs, ST
    - Elaborated and refined as appropriate
  - Evaluated according to CEM rules

Concept – Evidence

- Evaluation documents
  - Security Target (ST)
- Specification / Design documents
- User documents
- Process documents
  - Configuration management, delivery, flaw remediation

Acronyms (so far)

NIST

NSA

NIAP

CCEVS FIPS

NSTISSP

CCRA

NVLAP CCTL

TOE

TSFI

TSF

ST TSS

CC

TSP SFR

CEM

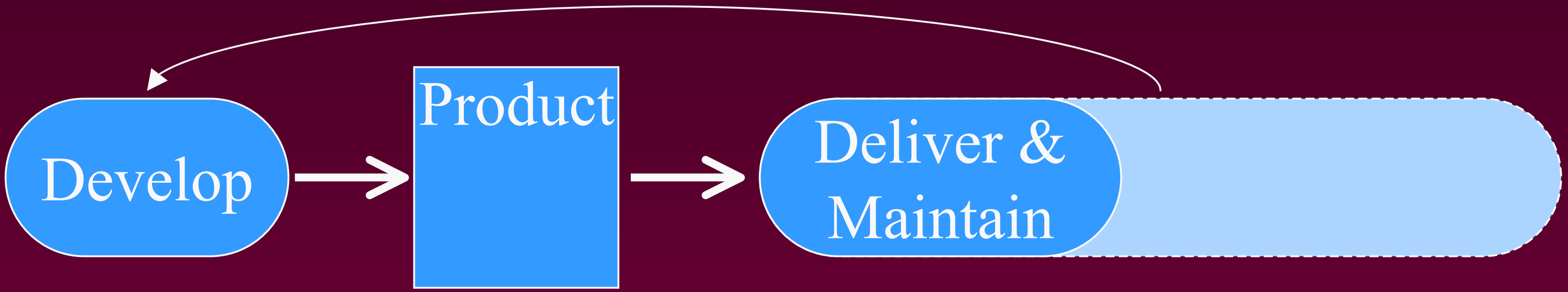
EAL

PP

Agenda

- General Concepts
- Understanding the Evaluation Process
- Using the Evaluation Criteria
- Providing the Evaluation Evidence

Process Overview - Development

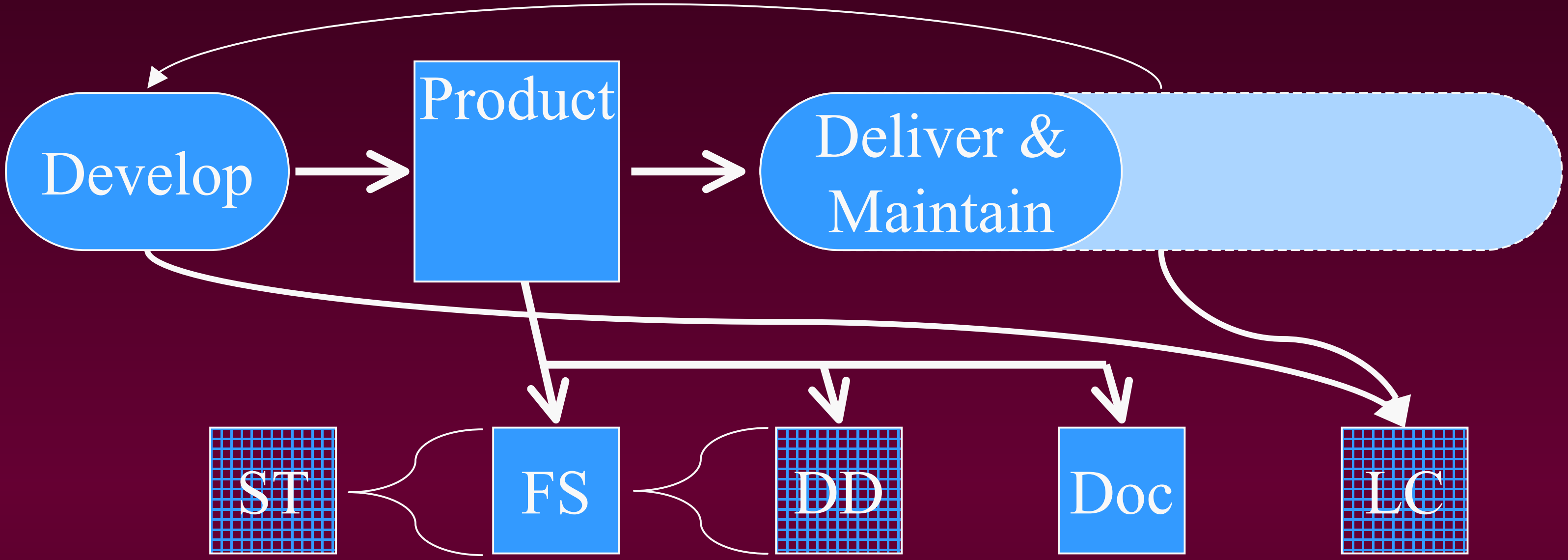


Develop

Product

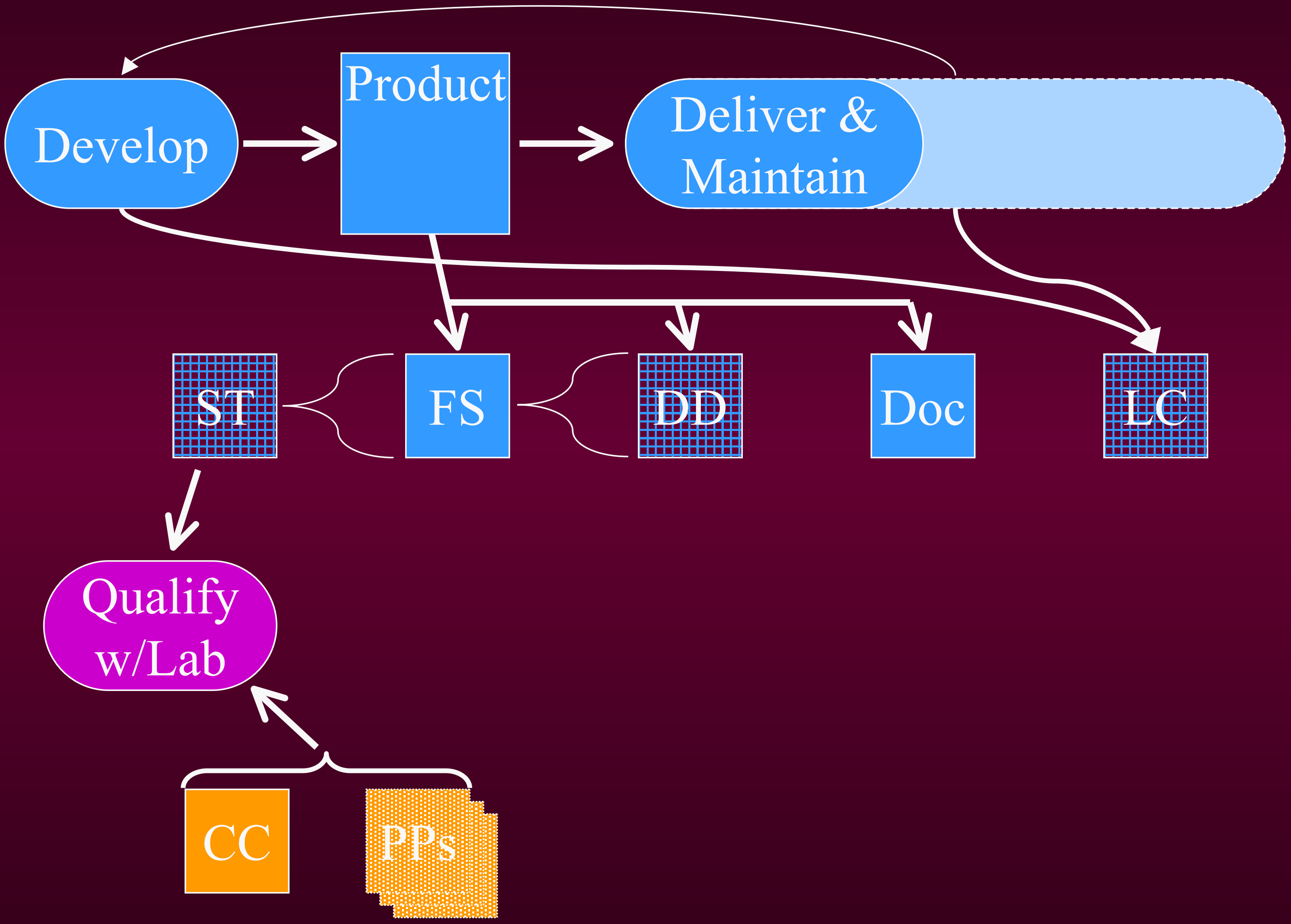
Deliver & Maintain

Process Overview - Evidence

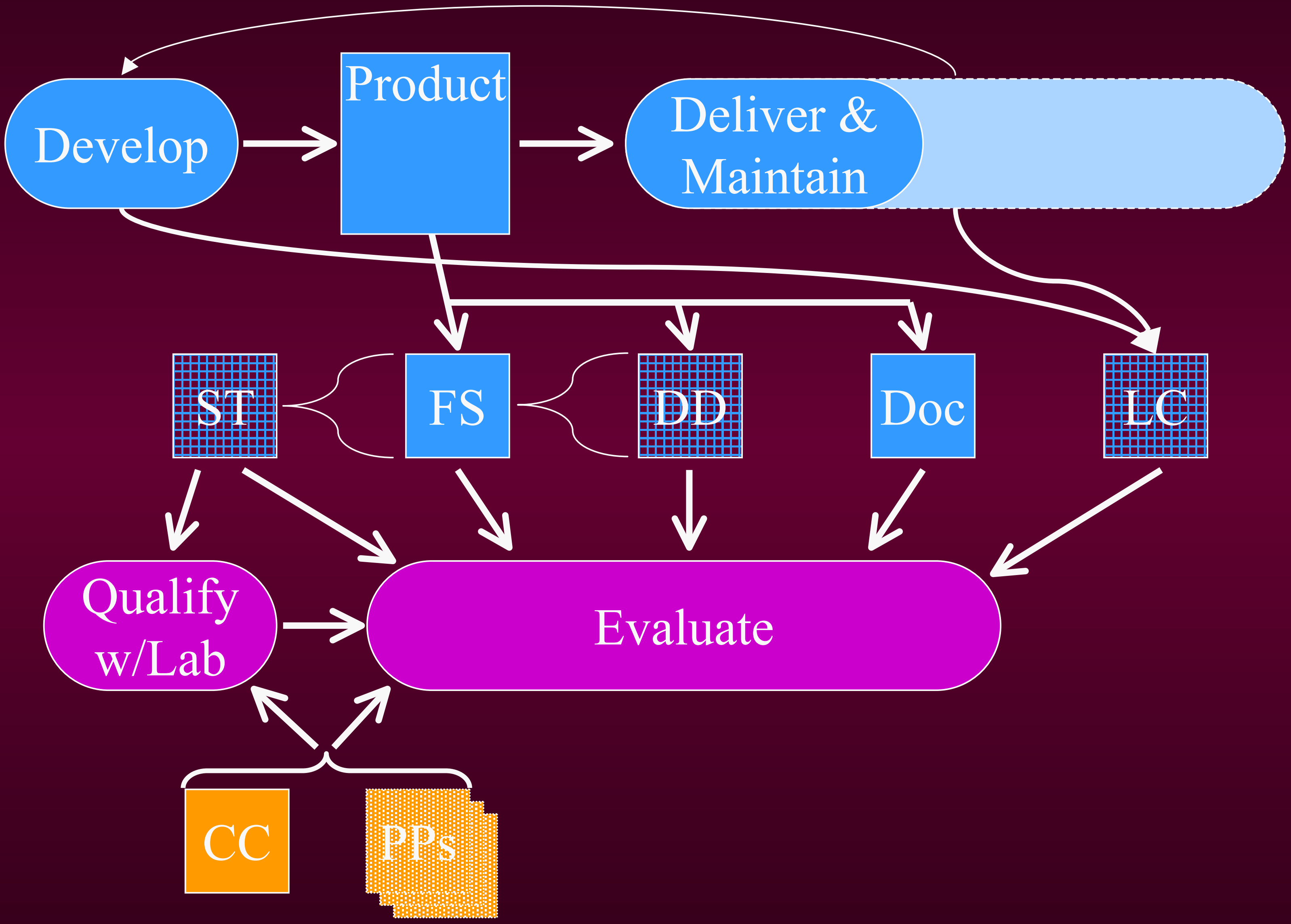


ST	Security Target	ASE
FS	Functional Specification	ADV_FSP
DD	Design Documentation	ADV_HLD, _LLD (_TDS)
Doc	Guidance Documentation	AGD
LC	Config Mgt, Delivery	ALC, ACM, ADO

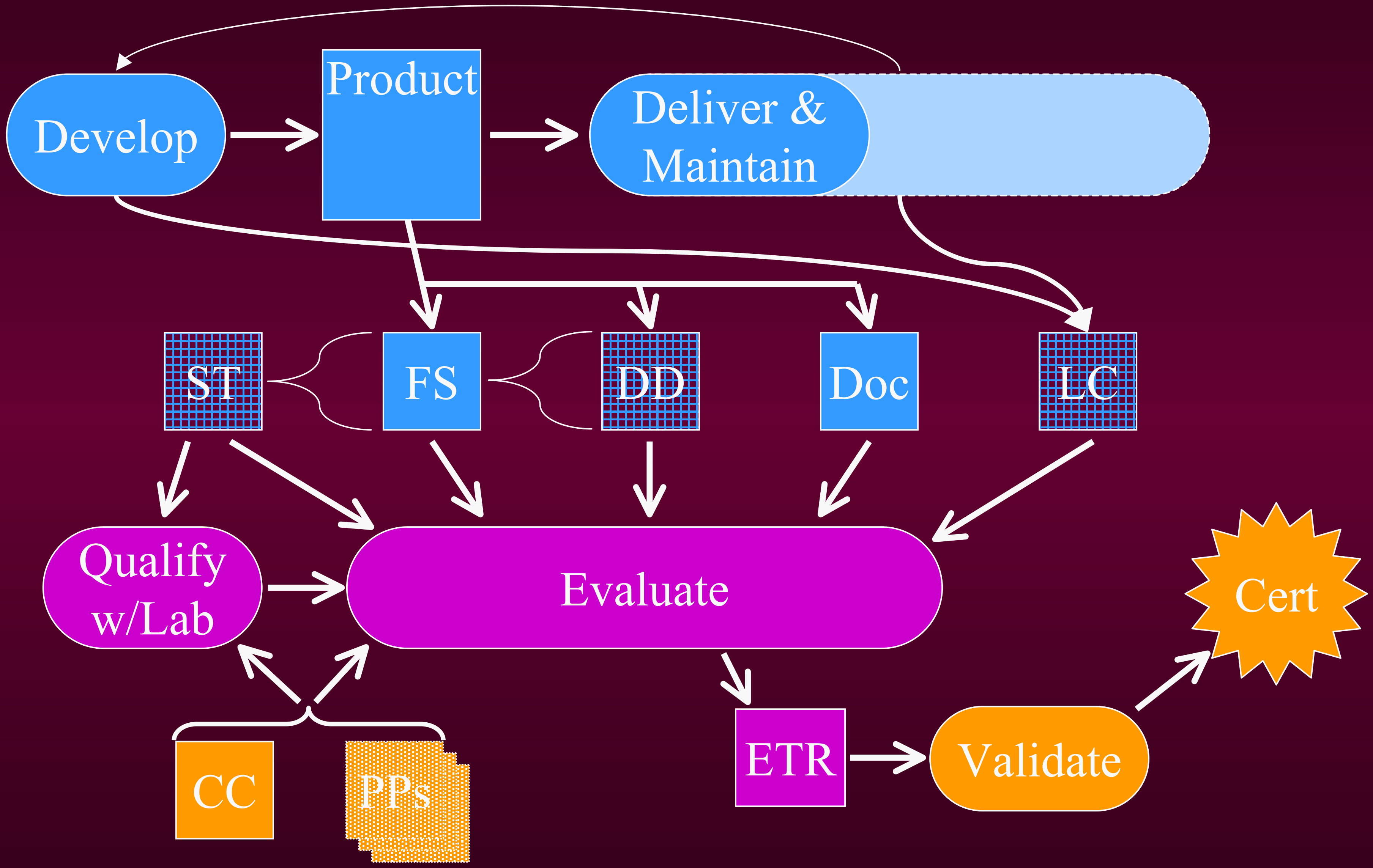
Process Overview - Qualification



Process Overview - Evaluation



Process Overview - Finish



Evaluation Process Documents

- ETR (Evaluation Test Report)
  - Produced by Lab to document process of evaluation
  - Composed of *verdicts* for each CEM work-unit
- EOR/EOD (Evaluation Observation Report / Decision)
  - Formal report by Lab to Sponsor about technical issue
- Test Plan
  - Evaluator's plan for independent product testing
- MSR (Monthly Status Report)
  - Lab's status and plans, reported to Sponsor and Scheme

Validator Role

- Validators – Scheme oversight
  - Employed or contracted by NSA (Aerospace, IDA, Mitre, Mitretek, Orion)
  - Work in *Validation Teams* (3-8 validators)
    - Each team is assigned to one Lab, works on a set of evaluations performed by that Lab
    - Each evaluation has one *Lead Validator*
      - Validates several evaluations
    - Team is led by *Senior Validator*
      - Ensures consistency among team's evaluations *and* among teams

Validator Communication

- Formally
  - Evaluators evaluate *Sponsor* work-product
  - Validators supervise *Evaluation Lab* activities
  - Sponsor communicates concerns to Lab; Evaluators raise issues to Validators; Validators represent the Scheme
- In practice
  - Sponsor, Lab, and Lead Validator should interact regularly as a group (e.g., weekly teleconference)
  - Sponsor should raise issues *concurrently* with Lab and Validator, not with Validator alone.

Validation Process

- Evaluation Kickoff
- Observation Report/Decision (OR/OD) Management
- Evaluation status tracking
  - Based on Lab’s MSRs
- Test supervision
- Evaluation assessment
  - Validation Report generated, maintained throughout
- Certificate issuance

Validation Process Documents

- VP (Validation Plan)
  - Produced at outset by Validator
  - Largely boilerplate around schedules and product details
- VR (Validation Report)
  - Produced, updated concurrently with evaluation
  - Assesses ETR for completeness, soundness
  - Also includes validator's comments on product
  - Focused on providing useful information to consumer
- Certificate
  - Issued by Scheme after validation completed

Issue Resolution

- EOR/EOD
  - Issues within a single evaluation
- OR/OD
  - Larger issues, raised to validation community
    - Decided by CCEVS on short schedule
  - Precedent Database (PD)
    - ODs sanitized, rationalized, published on periodic basis
- National Interpretations (NI)
- International Interpretations

Acronyms (Organizations and Process)

NSA NIST

NIAP

CCEVS FIPS

CCRA NSTISSP

NVLAP CCTL

TOE

TSF TSFI

ST TSS

TSP SFR

CC

EAL

PP

CEM

HLD ADV

ASE ACM

LLD

ACM

FSP

ADO

AGD

ETR MSR

EOR

EOD

OD OR PD NI

VP

VR

Agenda

- General Concepts
- Understanding the Evaluation Process
- Using the Evaluation Criteria
- Providing the Evaluation Evidence

CC Overview

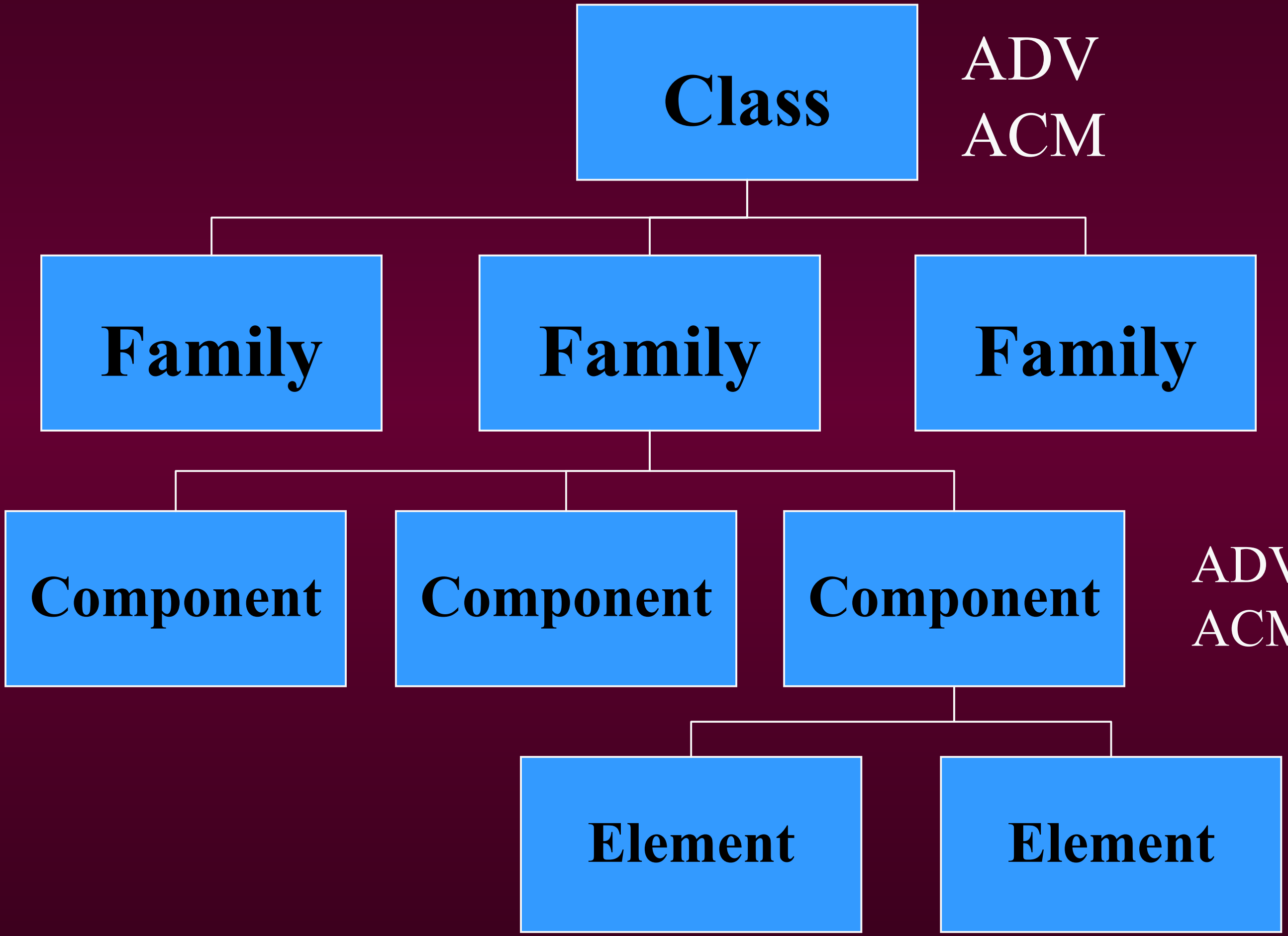
CC Structure

- Part 1 – Introduction
- Part 2 – SFR Components
  - Chinese menu—unbundled, some dependencies
- Part 3 – Assurance Components
  - Mostly bundled as Evaluation Assurance Levels (EAL1-7)
  - Some assurances not packaged with specific EALs
  - Lots of inter-requirement dependencies

CEM Structure

- Common Evaluation Methodology
  - Separate document for V2.x
  - Integrated in V3.0
- Mutually recognized at lower assurance (to EAL4)
- Evaluations defined by Work Units
  - One or more Work Unit per Evaluator Action
  - Developers should anticipate evaluator work

Hierarchy of Requirements



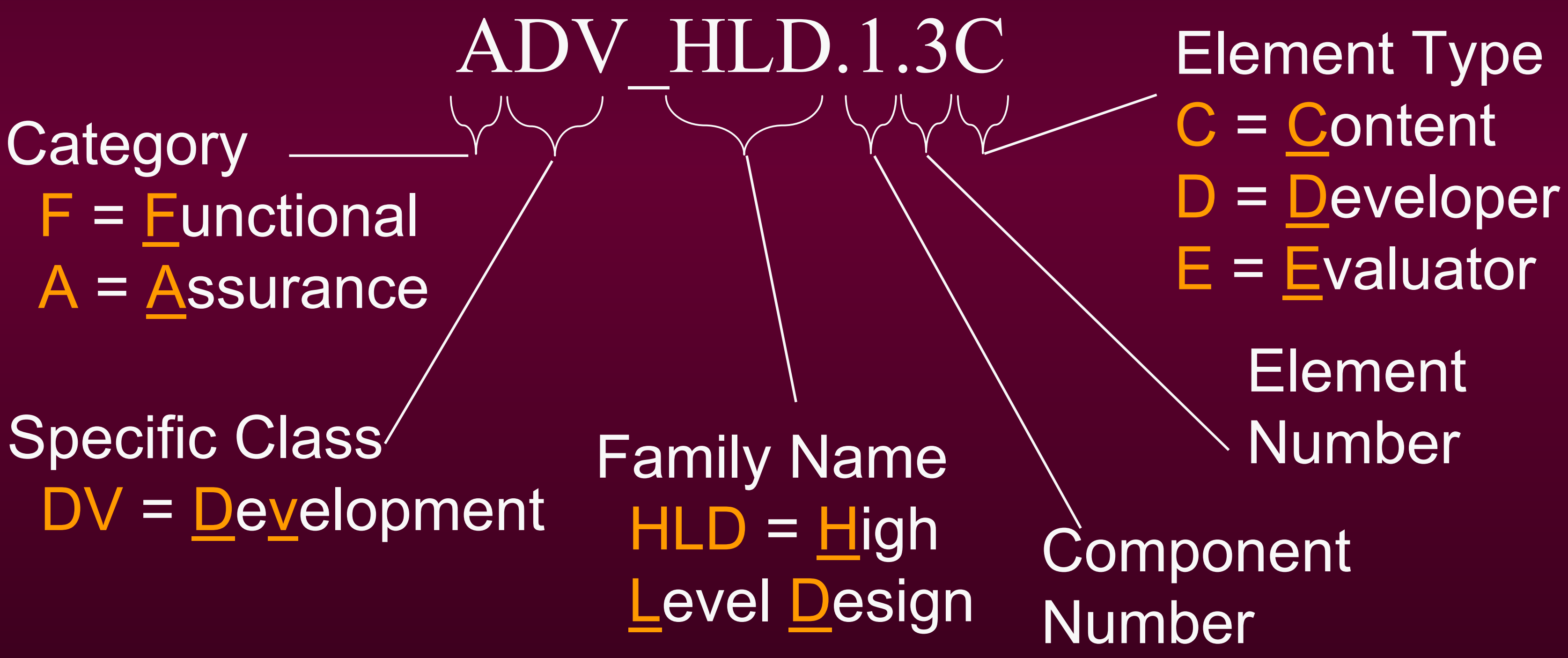
ADV
ACM

ADV_HLD
ACM_CAP

ADV_HLD.3
ACM_CAP.1

ADV_HLD.3.2D
ACM_CAP.1.2C

Interpreting Requirement Names



ADV_HLD.1.3C

Category
F = Functional
A = Assurance

Specific Class
DV = Development

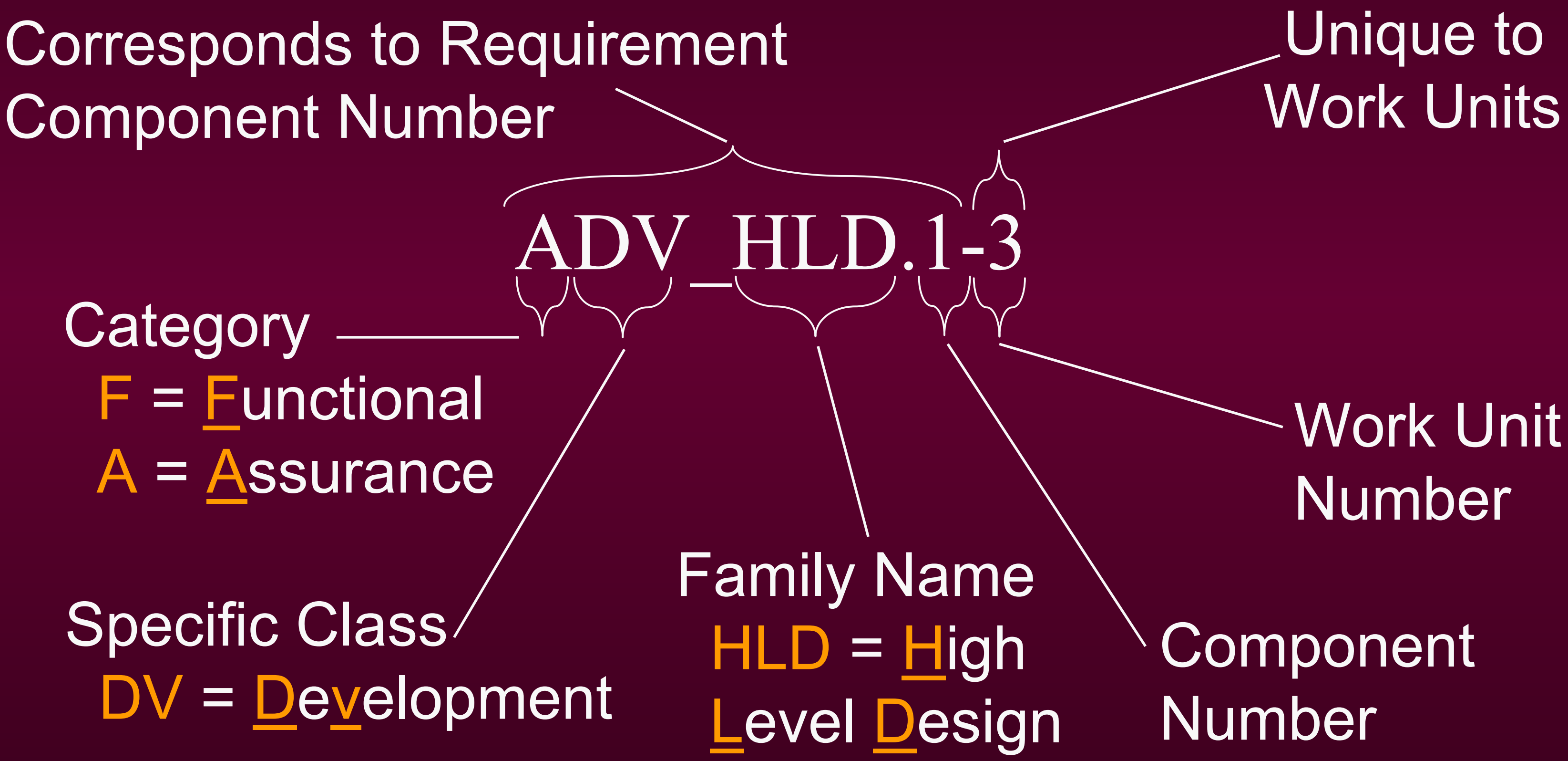
Family Name
HLD = High Level Design

Component Number

Element Number

Element Type
C = Content
D = Developer
E = Evaluator

Interpreting Work Unit Names



ADV_HLD.1-3

Corresponds to Requirement Component Number

Unique to Work Units

Category
F = Functional
A = Assurance

Work Unit Number

Specific Class
DV = Development

Family Name
HLD = High Level Design

Component Number

Definitions

- Class – organizational: members share common intent but differ in coverage of security objectives.
- Family – organizational: 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
- Element Type- assigns responsibility for satisfying assurance req't to developer, evaluator, or document

CC Functional Requirements

Security Functional Classes (CC 2.x)

- ✓ Security Audit (FAU)
- ✓ Communications (FCO)
- ✓ Cryptographic Support (FCS)
- ✓ User Data Protection (FDP)
- ✓ Identification & Authentication (FIA)
- ✓ Security Management (FMT)

Security Functional Classes (CC 2.x)

- ✓ Privacy (FPR)
- ✓ Protection of the Trusted Security Functions (FPT)
- ✓ Resource Utilization (FRU)
- ✓ TOE Access (FTA)
- ✓ Trusted Path (FTP)

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

Assurance Overview and EALs

Security Assurance Classes

- ✓ Evaluation Criteria (APE, ASE)
- ✓ Development (ADV)
- ✓ Configuration Management (ACM)
- ✓ Delivery and operation (ADO)
- ✓ Guidance documents (AGD)
- ✓ Life Cycle Support (ALC)
- ✓ Tests (ATE)
- ✓ Vulnerability assessment (AVA)
- ✓ *Also:* Functional TSF Protection (FPT_SEP, FPT_RVM)

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 complete
  - High is still being defined

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

EAL Summary

- EAL1: Black-box security from COTS products
- *EAL2-4: Security features in COTS products Evaluated based on internal knowledge of TOE "Good" / "Better" / "Best" Commercial Practice*
- EAL5-7: Developed specifically to satisfy (increasingly stringent) security requirements

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

EAL3: Methodically Tested 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 EAL
- 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: typically written as A*xx*_EXP_*xxx*
- 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 (cont.)

- 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, operating system, and application software are required).

Medium Robustness (cont)

- 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. Completion date is TBD.

Assurance Classes and Families

Assurances by EAL

Class	*EAL2 Families*	*EAL3 Families*	*EAL4 Families*
ACM	CAP.2	**CAP3**, SCP.1	**CAP4, SCP.2**, AUT.1
ADO	DEL.1, IGS.1	DEL.1, IGS.1	DEL.1, IGS.1
ADV	FSP.1, RCR.1, HLD.1	FSP.1, RCR.1, **HLD.2**	**FSP.2**, RCR.1. HLD.2, **LLD.1**, IMP.1, SPM.1
AGD	ADM.1, USR.1	ADM.1, USR.1	ADM.1, USR.1
ALC		DVS.1	DVS.1, LCD.1, TAT.1
ATE	FUN.1, COV.1, IND.2	FUN.1, **COV.2**, IND.2, DPT.1	FUN.1, COV.2, IND.2, DPT.1
AVA	SOF.1, VLA.1	SOF.1, VLA.1, MSU.1	SOF.1, **VLA.2, MSU.2**

“Hard” Assurances

Class	*EAL2 Families*	*EAL3 Families*	*EAL4 Families*
ACM	CAP.2	**CAP3**, SCP.1	**CAP4, SCP.2**, AUT.1
ADO	DEL.1, IGS.1	DEL.1, IGS.1	DEL.1, IGS.1
ADV	FSP.1, RCR.1, HLD.1	FSP.1, RCR.1, **HLD.2**	**FSP.2**, RCR.1. HLD.2, **LLD.1**, IMP.1, SPM.1
AGD	ADM.1, USR.1	ADM.1, USR.1	ADM.1, USR.1
ALC		DVS.1	DVS.1, LCD.1, TAT.1
ATE	FUN.1, COV.1, IND.2	FUN.1, **COV.2**, IND.2, DPT.1	FUN.1, COV.2, IND.2, DPT.1
AVA	SOF.1, VLA.1	SOF.1, VLA.1, MSU.1	SOF.1, **VLA.2**, **MSU.2**

Class APE
Protection Profile Evaluation

- Common Intent: The six families in this class are concerned with ...
  - complete, consistent, and technically sound (APE_DES, APE_ENV, APE_INT, APE_OBJ, APE_REQ, APE_SRE)

... protection profiles.

Typically not relevant to product evaluations

Class ASE
Security Target Evaluation

- Common Intent: The eight families in this class are concerned with ...
  - complete, consistent, and technically sound (ASE_DES, ASE_ENV, ASE_INT, ASE_OBJ, ASE_PPC, ASE_REQ, ASE_SRE, ASE_TSS)

... security targets that are suitable for TOE specification.

Class ACM
Configuration Management

- Common Intent: The three families in this class are concerned with ...
  - protecting the integrity (ACM_SCP)
    - SCP: CM scope (TOE Components; Problem Tracking)
  - tracking/restricting the modification (ACM_CAP, ACM_AUT)
    - CAP: CM capabilities (Version #; CI List; Auth. Controls; Acceptance)
    - AUT: CM automation (TOE Generation)

... of configuration items.

Class ADO
Delivery and Operation

- Common Intent: The two families in this class are concerned with ...
  - delivery (ADO_DEL)
    - DEL (Defined Procedures; Modification Detection)
  - installation, generation, start-up (ADO_IGS)
    - IGS (Procedures)

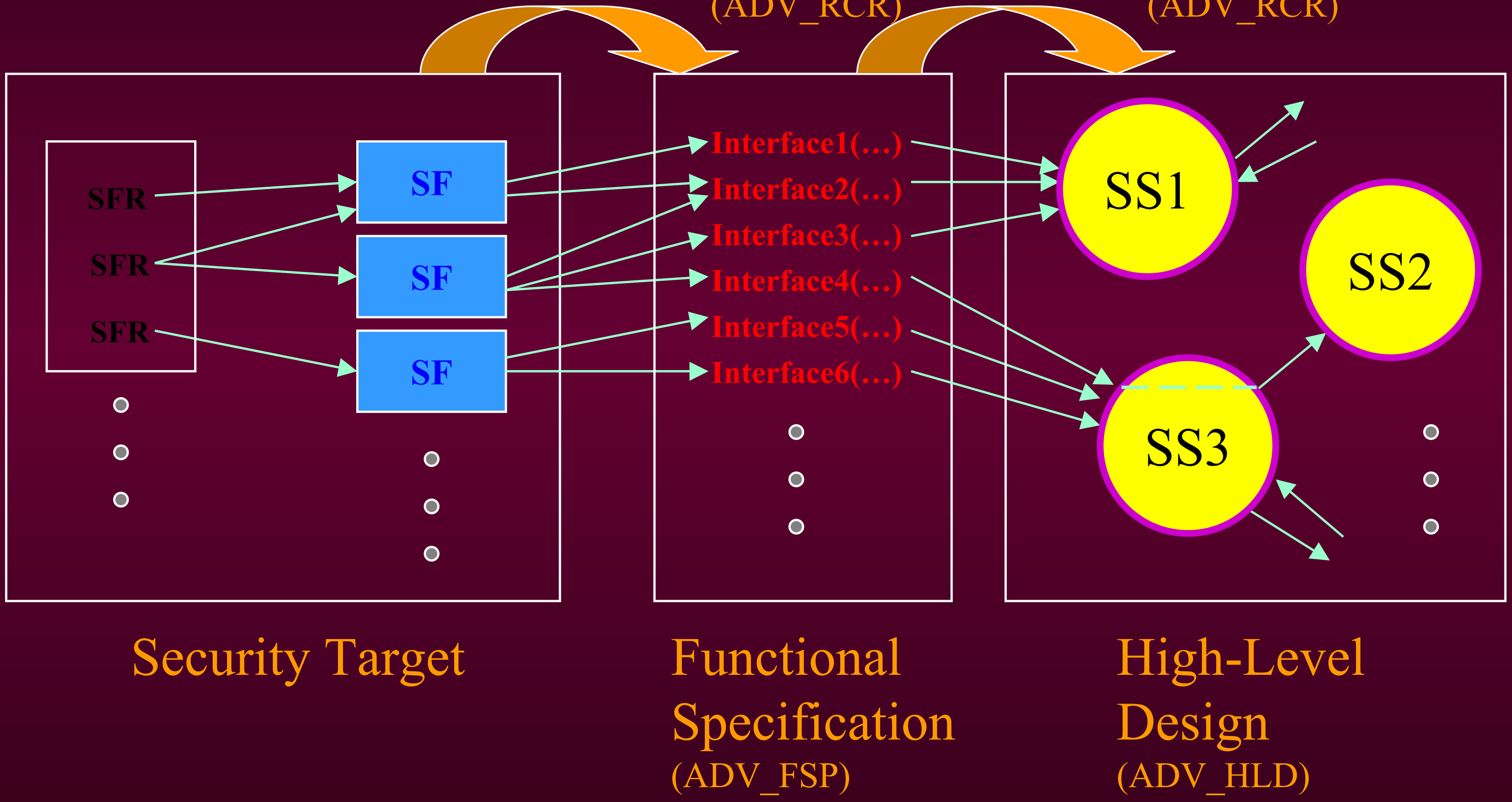
... of the TOE.

Class ADV
Development

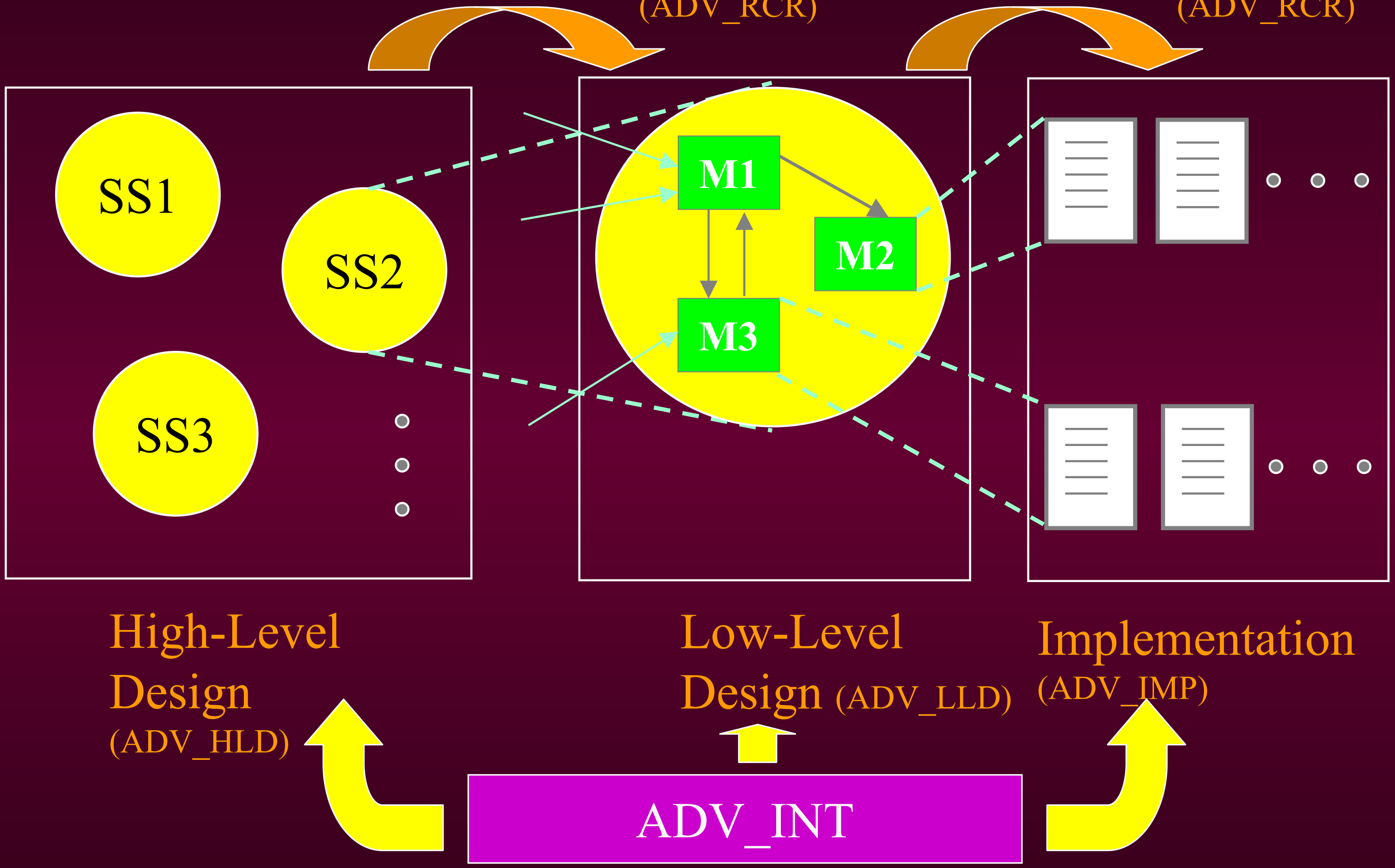
- Common Intent: The seven families in this class are concerned with ...
  - levels of abstraction (ADV_FSP, ADV_HLD, ADV_IMP, ADV_LLD)
  - correspondence mapping of representations (ADV_RCR)
  - internal structure (ADV_INT)
  - policy model (ADV_SPM)

... of the TSF.

ADV Overview



ADV Overview



High-Level Design (ADV_HLD)

Low-Level Design (ADV_LLD)

Implementation (ADV_IMP)

ADV_INT

Class AGD
Guidance Documents

- Common Intent: The two families in this class are concerned with ...
  - user (AGD_USR)
    - USR (Documentation for Users)
  - administrator (AGD_ADM)
    - ADM (Documentation for Administrators)

... guidance documentation.

Class ALC
Life Cycle Support

- Common Intent: The four families in this class are concerned with refinement of the TOE during ...
  - development (ALC_DVS, ALC_FLR)
    - DVS: Development Security (Measures Identified)
    - FLR: Flaw Remediation (Basic Procedures)
  - maintenance (ALC_LCD, ALC_TAT)
    - LCD: Life Cycle Definition (Defined Model)
    - TAT: Tools and Techniques (Well-defined Tools)

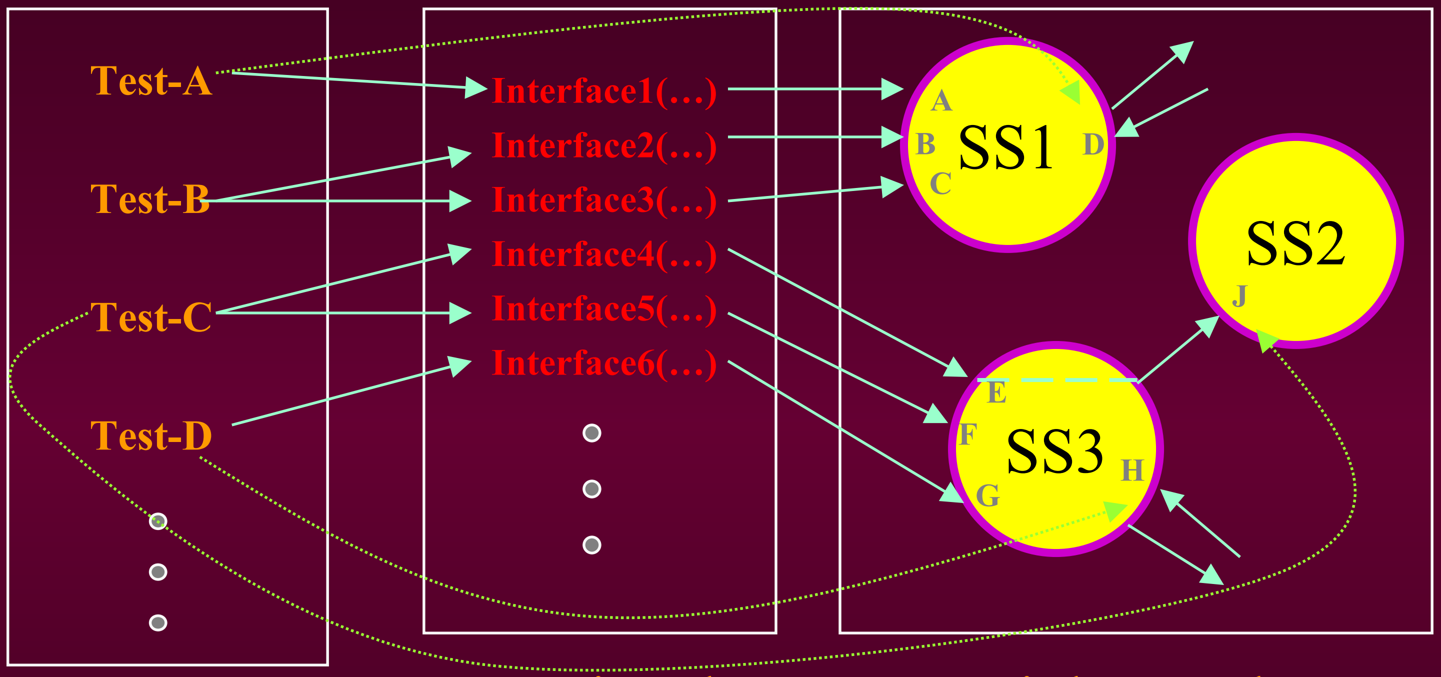
... phases.

Class ATE
Tests

- Common Intent: The four families in this class are concerned with ...
  - coverage (ATE_COV)
    - COV (Evidence of Testing vs. FSP; Coverage Analysis)
  - depth (ATE_DPT)
    - DPT (Testing HLD)
  - vendor functional and independent (ATE_FUN)
    - FUN (Developer Functional Testing)
  - evaluator independent (ATE_IND)
    - IND (Evaluator Subset Tests; More Tests)

... testing.

ATE_COV, ATE_DPT



Test Procedure Descriptions

Functional Specification

High-Level Design

Class AVA
Vulnerability Assessment

- Common Intent: The four families in this class are concerned with ...
  - exploitable covert channels (AVA_CCA)
  - misuse (AVA_MSU)
    - MSU (Examine AGD; Documented Analysis & Completeness)
  - strength and vulnerabilities (AVA_SOF, AVA_VLA)
    - SOF (Developer Analysis)
    - VLA (Analysis & Obvious Flaws; Evaluator Penetration Test)

... of the TOE.

Acronyms (Requirements)

NSA NIST

NIAP

CCEVS FIPS

CCRA

NSTISSP

NVLAP

CCTL

EOR ETR MSR

EOD

OD OR PD NI

VP VR

TOE

TSF TSFI

ST TSS

TSP SFR

CC

EAL

PP

CEM

ASE FSP HLD

APE **ADV** LLD

SPM

RCR

CAP SCP

ACM

AUT DEL

IGS **ADO**

USR **AGD**

ADM

DVS

LCD

FUN

ALC COV

TAT **ATE**

DPT

AVA FLR IND

VLA

SOF

MSU

FCO

FDP FAU

FIA FCS

FPR

FMT

FPT FRU

FTA

FTP

Agenda

- General Concepts
- Understanding the Evaluation Process
- Using the Evaluation Criteria
- Providing the Evaluation Evidence

Evaluation Evidence – In Theory

- Evidence Package
  - Prepared by Sponsor as product is developed
  - Fully compliant with CC requirements
- Evaluation Process
  - Review Evidence
    - Largely hands-off, little interaction with Sponsor
- Done!

Evaluation Evidence – In Practice

- Evidence Package
  - Prepared—iteratively—by Sponsor during evaluation
  - Poor match to CC requirements, CEM work units
- Evaluation Process
  - Assess acceptability of evidence
    - Work with Sponsor to get required materials
    - Work with Validator to find minimal acceptable quality
    - Evaluate, Review, Update, Re-evaluate
  - Highly interactive with Sponsor, Scheme

Making Evaluations Efficient

- Help the Evaluators
  - *Anticipate* CC requirements, CEM work units
  - *Explain* how evidence satisfies requirements
  - *Reuse* existing material and add rationale
  - Tell a *coherent story*
  - Make sure evaluators *understand* the product
  - Don’t make everything *evaluation-specific*

Evaluation Deliverables

Major Evaluation Deliverables

- Security Target (ASE)
  - TOE Summary Specification
- User/Administrator Documentation (AGD)
- Functional Specification (ADV_FSP)
- Internal Design Documentation (ADV_HLD, ADV_LLD, FPT_SEP, FPT_RVM)
- Life Cycle Processes (ACM, ADO, ALC, AVA, AMA)
- Test Plans and Procedures (ATE)
- *Everything else* (SFRs, ADV_SPM, ADV_RCR, ADV_IMP)

Deliverable: Security Target

- Much of ST is very CC-specific
  - Requires specialized knowledge, expertise to prepare
  - Consultants often helpful here
- *But…* TOE Summary Specification is *not* specialized
  - Tells overall story of TOE and relationship to product
    - Product "Technical Overview"
  - What the TOE does, facilities provided, types of interfaces, user/admin roles, platform requirements, etc.
  - What is/isn't in TOE (e.g., by administrative policy)
  - What security features satisfy which CC SFRs
  - Recommendation: Prepare the TSS *first*, then derive the rest of the ST (and other evidence)

Security Target – Specialized Parts

• Enumeration of	*Examples*
– Objectives	O.SELFPRO
– Assumptions	A.NOEVIL
– Operational Environment	OE.GENPUR
– Policy	P.CRYPTO
– Threats	T.NOAUTH
• Requirement Operations	*selection, etc.*
• Extended Requirements	Fxx_EXP_XXX

- Mappings
- ST is a *public document*
  - Learn from examples of others

Deliverable: AGD Documentation

- Standard user/administrator documentation
  - Must describe how to configure TOE in "evaluated configuration(s)"
  - Must clearly define administrative role(s) and capabilities
- Recommendation
  - Ensure standard documentation satisfies requirements
  - Usually pretty straightforward

Deliverable: Functional Specification

- Identify and describe *all* interfaces to TSF
  - System calls and other programmatic interfaces
  - Protocols (at all appropriate levels)
  - Hardware instructions
  - Administrative GUIs
- Recommended style
  - Describe interface classes (often a new CC-specific document)
  - Use existing interface documentation for details
- EAL4 adds requirements for *completeness*
  - Each interface described completely
  - Set of interfaces described is complete TSF interface

Deliverable: Internal Design Doc

- Usually the hardest part of evaluation
  - Rarely exists (even if so, often outdated)
- EAL2: Define and describe subsystems (HLD) and interfaces
- EAL3: Describe subsystem roles in security enforcement
- EAL4: Describe modules (LLD), interfaces, security roles
- Recommendation
  - Start from top-down story (driven by TSS)
  - Reuse existing material where possible—with new rationale
  - Should be prepared by *product* expert, *not* inexperienced outsiders (i.e. consultants)

Deliverable: Life Cycle Processes

- Lots of variety
  - Life cycle processes often occur in disparate components of Sponsor organization
- Recommendation
  - Identify responsible parties early on
  - Prepare high-level descriptions of processes
    - Often through interview by product or security expert
  - Ensure that descriptions satisfy CC requirements
    - And explain how in the documents

Deliverable: Test Plans and Procedures

- Functional testing required
  - Tests must be clearly related to SFRs
  - SFR coverage must be complete
    - Except for SFRs that are *arguably infeasible to test*
    - Example: FDP_RDP (Residual Data Protection)
- Recommendation
  - Ensure that existing procedures satisfy CC requirements
    - Can be a *lot* of work, depending on existing test approach

Deliverables: Everything Else

- TSF Protection (FPT_SEP, FPT_RVM)
  - Typically part of HLD/LLD
  - Clear explanation of how TSF is protected from external adversaries, including role(s) played by hardware, internal privilege mechanisms, access control to TSF data, etc.
- Implementation
  - EAL4 requires Evaluator access to source code
- Miscellaneous Assurances (ADV_RCR, ADV_SPM)
  - Integrate with other ADV documents
  - ADV_SPM usually a vacuous requirement

Changes in CC 3.0

Common Criteria Version 3.0

- Schedule
  - March 2005: Final technical draft, Review by Schemes
  - May 2005: Technical editors' draft
  - Summer 2005: Public Release, Trial evaluations (voluntary)
  - 2006: Adoption by CCRA and ISO, Begin evaluation changeover
- Goals
  - Reorganize and streamline functional requirements
  - Better accommodate real-world development assurances
  - Address product composition and hardware platform issues
  - Reduce evaluation costs

CC 3.0 - Functional Requirements

- Major reorganization
  - Mostly same basic mechanisms (I&A, Access Control, Audit, Administrative Roles, Residual Data Protection)
  - New TSF Physical Protection (e.g., smart cards)
  - Access Control subsumes Information Flow, Import, Export
  - Move most FPT concepts to ADV_ARC
- Major effects on STs
  - Completely new SFR mappings
- Minimal effects on products
  - Requirements intended to be more comprehensible

CC 3.0 - Development Assurances

- Rewrite
  - Old ADV codify strictest “waterfall” model—not real world
  - No useful distinctions made for security-relevance inside TSF
  - New structure
    - ADV_TDS – TSF design description
    - ADV_ARC – Security architecture description
    - Explicit distinctions based on relative security-criticality of interfaces *and* mechanisms
    - Levels of abstraction can be defined to match TSF
    - Strong attempt to focus evaluation effort on high-return areas
    - Strong attempt to match real-world development practices

CC 3.0 - Composition Assurance

- New class: ACP – Composition Assurance
  - Define requirements for describing a TOE that can be securely combined (“composed”) with another TOE
  - Describe dependencies of a first (e.g., “upper”) TOE on a second (e.g., “lower”) TOE
  - Describe expectations of upper TOE for lower TOE’s behaviour
  - Also ADV_CMP for lower TOE’s interface

CC 3.0 - Platform Assurance

- New class: APT – Platform Assurance
  - Requirements for specifying COTS hardware platforms on which a TOE depends
  - Allow evaluated products to define an ongoing class of hardware *by specification*, not by instance
  - Acknowledge inherent assurances provided by common hardware development processes
  - Avoid requiring unavailable, unevaluatable, or inappropriate software-focused "evidence" items

Acronyms (Deliverables & CC 3.0)

NSA NIST

NIAP

CCEVS FIPS

CCRA NSTISSP

NVLAP CCTL

ETR MSR

EOR EOD

OD NI

OR PD

VP

VR A.xxx

T.xxx

TOE

TSF TSFI

ST TSS

TSP SFR

CC

EAL

PP

CEM

O.xxx

OE.xxx

P.xxx SOF

ASE FSP HLD

APE **ADV** LLD

SPM

RCR

CAP SCP

ACM DEL

AUT

IGS **ADO**

USR **AGD**

ADM

DVS

LCD

FUN COV

ALC

TAT **ATE**

DPT

AVA FLR IND

VLA

MSU EXP TDS

ARC

FCO

FDP FAU

FIA FCS

FPR

FMT

FPT FRU

FTA

FTP

ACP

APT

Recap

- General Concepts
- Understanding the Evaluation Process
- Using the Evaluation Criteria
- Providing the Evaluation Evidence