ICCC^7

Product Vendors Guide to Planning for Government Required Validations

September 19, 2006

Matthew Keller – Corsec Security, Inc

Agenda

- “Do I Need a FIPS140-2 or CC Validation?”
- Evaluation Processes
- Planning a Successful Effort
- Critical PreEvaluation Steps
- Evaluation Concerns
- Business Advantages
- Intermediate Wins During the Process
- FAQs

Do I Need a Validation?

- Motivating Factors for Evaluation
  - U.S. Government - NSTISSP #11 / DoD 8500
  - Australian requirements – AISEP
  - 24 MRA Countries
  - Financial Industry
- Critical Factors
  - Your Customer’s Requirements
  - Current Market Recognition

Corsec®

Basic CC Concepts

- **Protection Profile (PP)**
  - An implementation-independent set of security requirements for a **category of TOEs** that meet specific consumer needs
- **Security Target (ST)**
  - A implementation-dependent set of security requirements and specifications used as the **basis for evaluation** of the identified TOE
- **Target of Evaluation (TOE)**
  - An **IT product or system** and its associated administrator and user guidance documentation that is the subject of an evaluation
- **Evaluation Assurance Level (EAL)** -
  - A *package* consisting of **assurance components** that represents a point on the CC predefined assurance scale.

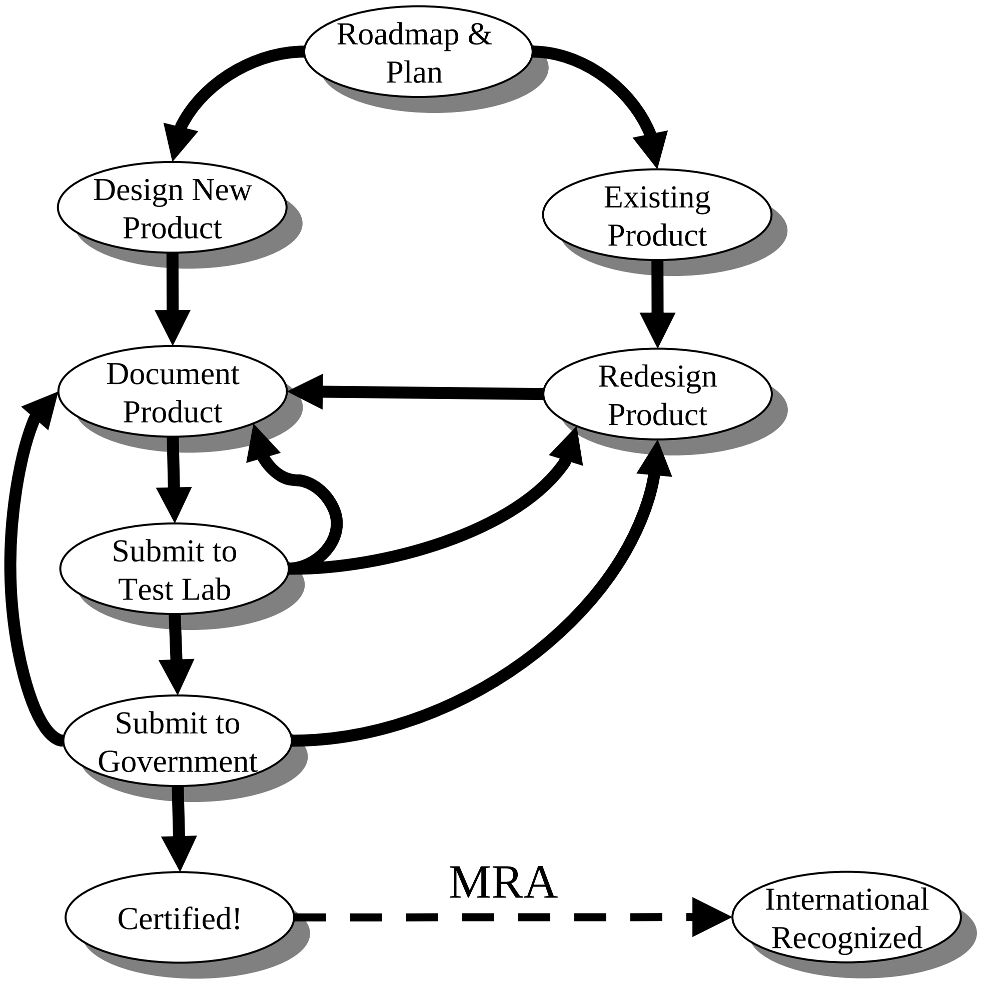
FIPS 140-2 Basics

- Focus on Cryptographic Modules - Cryptographic Boundary
- The FIPS Standard
  - 69 pages, with another 22 pages of annexes
- Derived Test Requirements
  - 122 pages of DTRs
- Implementation Guidance
  - 45 pages of interpretations of questioned requirements
- Algorithm Testing Program

Validation Services

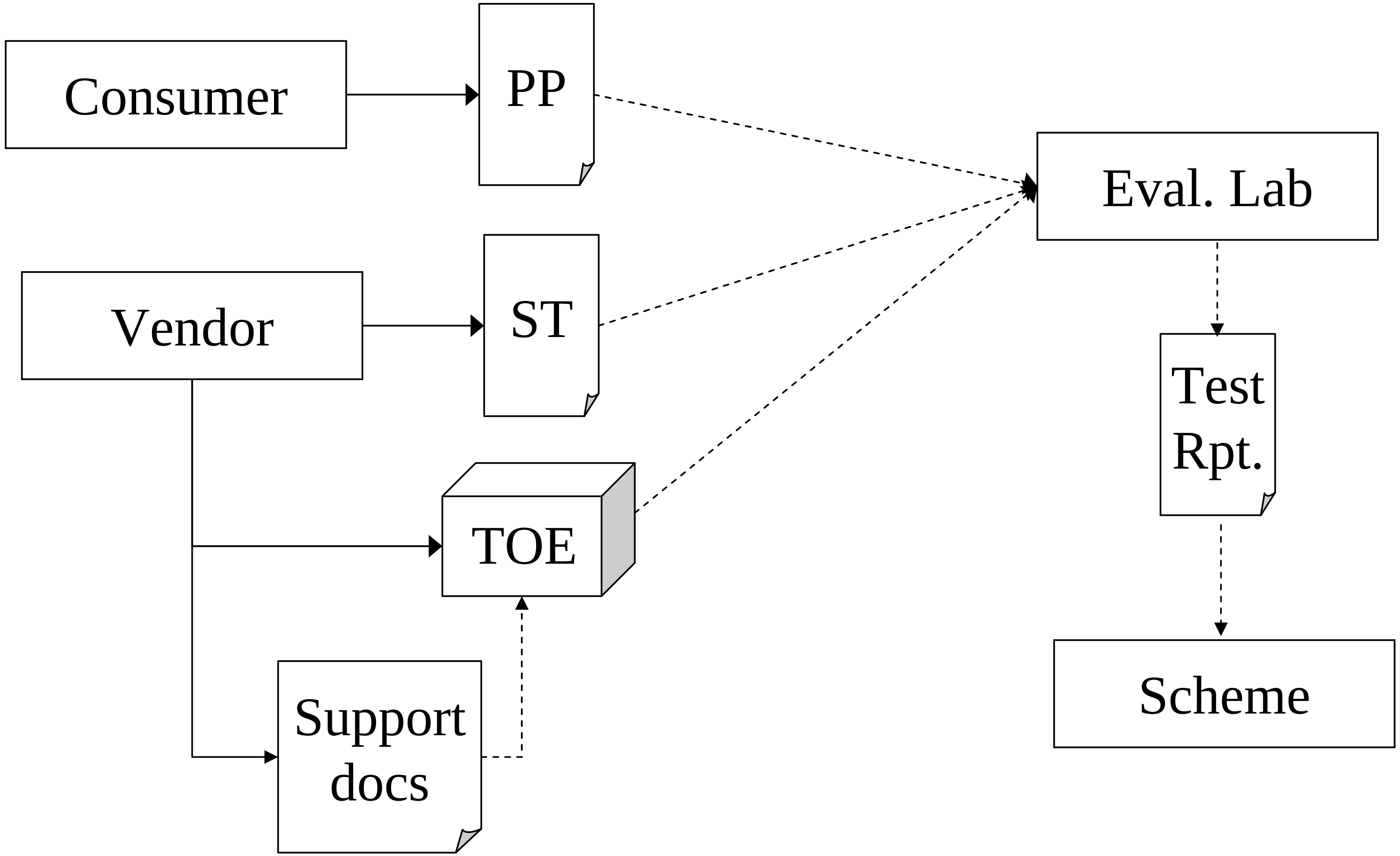
- Training
  - Consultants
  - Schemes
- Evidence Preparation
  - Internal Staff
  - Generic Documentation Companies
  - Consultants
- Evaluation
  - Accredited Labs

Validation Process



http://www.corsec.com

Document Flow



Supporting Documents

- **Configuration Management Document**
- **Delivery Procedures**
- **Install and Setup Procedures**
- **Functional Specification**
- **High Level Design**
- **Low Level Design**
- **Correspondence Analyses Document**
- **Admin and User Guides**
- **Test Coverage Evidence Document**
- **Vulnerabilities Analysis**

Planning a Successful Effort

- Learn about Common Criteria
- Determine Customer Requirements
  - PP, EAL, MRA
  - Coordinate with the Sales Staff
- Study Competitor's Efforts
- Target a Protection Profile (No PP)
- Selecting the TOE Boundary
- Target Evaluation Assurance Level
- Define Timelines and Milestones
- Which Scheme to Use

- PreEvaluation Consulting Effort (Assessment)

PreEvaluation Steps

- Design for Requirements
  - CEM – Common Evaluation Methodology
  - Interpretations -
    - http://www.commoncriteria.org/cc/ccinterps/ccInterps.html
  - Requirements Affect Development Process
- Document for Assurance Requirements
- Realistic Time Schedules
  - Labs Find Problems and Issues

Evaluation Steps

- Evaluation Contracting
  - Fixed Prices
- Documentation Updates
- Responding to Evaluation Questions
- Monitor Evaluation Schedule

Intermediate Wins

- In-Evaluation List - US
    - ST
    - Lab Contract
    - EAP
    - KickOff Meeting
- Letters from Consultant/Laboratories
- Lower Evaluation (EAL1)
    - Quick Cert Program
    - Fall Back Position
- Test against a ST only (No PP)
    - No Functional Design

Benefits of Evaluation

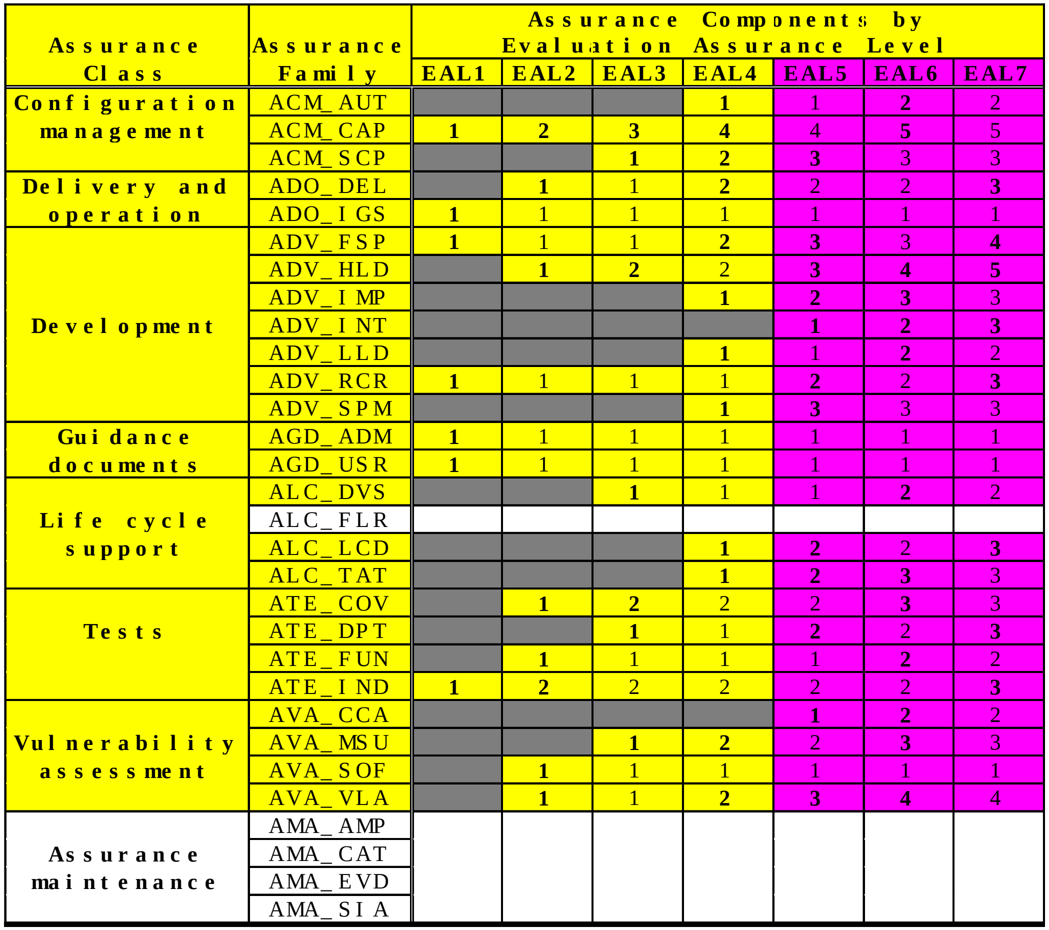
- Third Party Evaluation
  - Lends credibility to your marketing claims
  - Discover issues not discovered internally
- Mutual Recognition
  - Accepted in multiple countries
  - Accepted in multiple industries
- Limited Access Markets
  - Requirement in several markets
- Documentation
  - More detailed security documentation
  - Consolidation of design and process documentation

FAQ

- How long? – How much?
  - Developing Market Space
- Do I Need to do the Whole Thing Again? - Certification Maintenance
- Which Product Should I Certify?
- I have multiple similar products, how should I pursue validation?
- Which Level Should I Target?

http://www.corsec.com

EAL Chart



Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life cycle support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4
Assurance maintenance	AMA_AMP							
	AMA_CAT							
	AMA_EVD							
	AMA_SIA							

http://www.corsec.com

More Information

Corsec Security, Inc.
10340 Democracy Lane
Suite 201
Fairfax, VA 22030

P: (703)267-6050
F: (703)267-6810

http://www.corsec.com

- Local Schemes
- Local Labs
- www.commoncriteria.org

http://www.corsec.com

http://www.corsec.com