

Developer Documentation

A Who To Guide

Erin Connor, Mark Gauvreau, and Samuel E. Moore
EWA-Canada
20 September 2006

Presenter: Erin Connor (econnor@ewa-canada.com)

Overview

- Introduction To EWA-Canada
- Documentation Development Considerations
- Example Rules for Deciding Recommended Author
- Example Recommendations for EAL 4+
- Summary

- What we do
 - Lab
 - Common Criteria Evaluation – Canadian Scheme
 - FIPS 140-2 Cryptographic Module Testing – CMVP
 - Point of Sale Terminal & Encrypted PIN Pad Certification
 - Interac Financial Services Network
 - Payment Card Industry PED
 - Payment Terminal Security (PoS Terminals)
 - Documentation Development Assistance to Vendors
 - Managed Security Services
 - Information Assurance Consulting
 - Site Security Audit and Vulnerability/Penetration Testing

Documentation Development Considerations

Factors

We identified a set of five factors that we felt would have a significant impact on deciding who should be selected to produce the evaluation evidence documentation.

Rating Scheme

A simple rating scheme of Low, Medium, High was used for each factor to assess its applicability to each documentation family in the security assurance requirements up to EAL 4+ (FLR).

Following slides discuss each factor and its rating scheme

Documentation Development Considerations, Cont'd

EM - Existing Material

If material already exists, particularly if it is reasonably well developed, it may be advantageous for the individual(s) who developed it to complete the documentation.

Rating Scheme

L (Low) = unlikely to exist

M (Medium) = may exist

H (High) = probably exists

Documentation Development Considerations, Cont'd

IP - Retained Intellectual Property

One of the benefits of developing documentation, particularly design documentation, is that it leads to a better understanding of the product. If this understanding is obtained by an outside consultant, the developer may not gain as much benefit from the documentation development exercise.

Rating Scheme

L (Low) = developer team unlikely to receive much value from generating the documentation

M (Medium) = developer team may get good information

H (High) = developer team would get valuable information from generating the documentation

Documentation Development Considerations, Cont'd

CC - Specific Common Criteria Knowledge Needed

Some of the documents require a detailed familiarity with the Common Criteria terminology and expectations for document content and format. If these are outsourced, the development team is not required to obtain the depth of knowledge and experience to produce them.

Rating Scheme

L (Low) = document could be constructed with minimal instruction on CC (e.g., template & brief instructions)

M (Medium) = some instruction or familiarity with the CC needed

H (High) = significant training and experience with the CC would be needed

Documentation Development Considerations, Cont'd

DI – Detailed Developer Input

Some of the documents (e.g., low-level design) require detailed knowledge of the product. These might best be done by the developers themselves or by employees who are able to interact closely with them at their convenience.

Rating Scheme

- L (Low) = document could be constructed with minimal interaction with developers (e.g., few hours discussion)
- M (Medium) = moderate amount of interaction with developers needed (e.g., few discussions of a few hours each)
- H (High) = significant interaction with developers would be needed (e.g., several to many discussions lasting several hours each)

Documentation Development Considerations, Cont'd

RA – Internal Resource Availability

Developer may have limited internal resources that can be applied to documentation development. For example, resources may be focused on product development activities to “get the next release out.” Developer may also prefer to have external help to produce evaluation documentation, regardless of the availability of internal resources.

Rating Scheme

Since the availability of internal resources and the desire for external help varies greatly among developers, and may well outweigh all other considerations, this factor has not been rated. Rather, full availability of internal resources has been assumed.

Who To Rules

Recommended Producer (RP)

- “D” means Developer, “C” means Consultant/Lab and “J” means Joint effort of Developer and Consultant/Lab.

Rules

1. If EM = H, then RP = D
2. If IP = H, then RP = D
3. If CC = H, then RP = C
4. If DI = {M | H} & CC = L, then RP = D
5. If DI = M & CC = M, then RP = J
6. Two are forced to be Joint with the Lab, namely:
 - ADV_IMP.1 code sample selected jointly and provided by developer
 - ATE_IND.2 supported by developer and conducted by Lab
7. Else RP = D

Configuration management

Identifier	Family Name	EM	IP	CC	DI	RP
ACM_AUT	CM automation	M	H	L	M	D
ACM_CAP	CM Capabilities	M	H	L	M	D
ACM_SCP	CM Scope	M	H	L	M	D

ADO Who To

Delivery & operation

Identifier	Family Name	EM	IP	CC	DI	RP
ADO_DEL	Delivery	L	L	L	M	D
ADO_IGS	Installation, Generation & Startup	H	L	L	M	D

Development

Identifier	Family Name	EM	IP	CC	DI	RP
ADV_FSP	Functional Specification	L	M	M	M	J
ADV_HLD	High level design	L	M	M	M	J
ADV_LLD	Low level design	L	H	L	H	D
ADV_IMP	Implementation representation	-	-	-	-	J
ADV_RCR	Representation correspondence	L	L	M	M	J
ADV_SPM	Security Policy Model	L	L	H	L	C

Guidance

Identifier	Family Name	EM	IP	CC	DI	RP
AGD_ADM	Administrator guidance	H	L	L	L	D
AGD_USR	User guidance	H	L	L	H	D

Life cycle support

Identifier	Family Name	EM	IP	CC	DI	RP
ALC_DVS	Development security	L	H	L	L	D
ALC_FLR	Flaw remediation	M	H	L	L	D
ALC_LCD	Life cycle definition	M	H	L	L	D
ALC_TAT	Tools & techniques	M	H	L	M	D

Tests

Identifier	Family Name	EM	IP	CC	DI	RP
ATE_COV	Coverage	L	L	L	M	D
ATE_DPT	Depth	L	L	L	M	D
ATE_FUN	Functional Tests	H	H	L	M	D
ATE_IND	Independent Testing	-	-	-	-	J

Vulnerability assessment

Identifier	Family Name	EM	IP	CC	DI	RP
AVA_MSU	Misuse – Validation of analysis	L	L	H	L	C
AVA_SOF	Strength of TOE security functions	L	L	H	L	C
AVA_VLA	Vulnerability analysis	L	M	H	L	C

Additional Thoughts

- A Gap Analysis to determine what, if any, material already exists must be the first step in the process
 - For this presentation we have used an assumed rating for Existing Material based on previous experience
- Less than full internal resource availability to support documentation production may cause Developer items to move into the Joint or Consultant/Lab category
 - There will always be a requirement for some developer input and interaction with the documentation team
- Schedule and Cost considerations will also have an impact on any decision

Summary

- Identified a set of documentation development factors
 - Existing material
 - Retained intellectual property
 - Specific CC knowledge requirements
 - Detailed developer input
 - Internal resource availability
- Rated on a High, Medium, Low scale of “applicability”
 - For this analysis assumed full internal resource availability as needed

Summary Cont'd

- Rules defined to determine Who To produce recommendations for required evidence documentation
- Using rules, “recommended producer” for each assurance class/family up to EAL 4+ identified
- Some assurance families are automatically joint efforts between developer and lab
- A documentation gap analysis is a necessary first step
- Lower internal resource availability may cause Developer items to move into the Joint or Consultant/Lab category
- Each developer and evaluation will be different

Questions



For further information:
econnor@ewa-canada.com

Your Trusted Partner