Getting Value for Money from Your Certification Investment

ICMC16 Ottawa, Canada

18-20 May 2016

Presented by Alan Gornall

RYCOMBE CONSULTING

Introduction

- I provide certification support to my clients: compliance audit, design, implementation, testing, documentation, project management
- I have over 25 years of certification experience and have completed over 50 certifications
- Issue addressed by this presentation: How to cost effectively maintain the relevance of a module's FIPS 140-2 certification.

Evaluations are Version Specific

- Problem: If you make a change you are no longer certified.
- Solution: Don’t make changes or certify those changes.

I Don’t Want to Make Changes

- Options:
  - Have a “government” version that you recertify regularly but infrequently (once every year, for example)
  - Choose your cryptographic boundary carefully

Module Embodiments

- Hardware (sub-chip, single chip, multiple-chip embedded, multiple-chip standalone),
- Firmware,
- Software,
- Hybrid

Cryptographic Boundary

- FIPS 140-2, Section 4.1, paragraph 2:

A cryptographic boundary shall consist of an explicitly defined perimeter that establishes the physical bounds of a cryptographic module. If a cryptographic module consists of software or firmware components, the cryptographic boundary shall contain the processor(s) and other hardware components that store and protect the software and firmware components. *Hardware, software, and firmware components of a cryptographic module can be excluded from the requirements of this standard if shown that these components do not affect the security of the module*

Module Scope

- A cryptographic module is not necessarily the whole product. It just needs to contain the FIPS 140-2 security relevant functionality. As a minimum, it needs to contain at least one approved function (Annex A).
- Choosing the boundary carefully can result in a module with great longevity.

Anticipate Recertification

- Within a module, identify which areas of code are security relevant and which are not. Go to the file level if you have time, but usually simply identifying folders with security relevant code in can be all that is required.

Adding Relevance

- Even if your module is technically portable, CMVP will not make any statement about its fitness for purpose if ported to a non-certified platform (not tested during evaluation).
- Decide if want to consider portable modules or certifying the same module in multiple operational environments and/or CPUs.

Making Changes to a Certified Module

- There are many re-validation scenarios. These are fully described in IG G.8. Today I am going to talk about two of these: 1SUB and 3SUB.
- 1SUB (letter upgrade): Non security-relevant changes.
- 3SUB: Small number of security-relevant changes: 3SUB

3SUB

- 5SUB – new evaluation
- 3SUB – re-evaluation. Reduced scope, cheaper than a 5SUB

1SUB

- Letter upgrade. At its simplest may just be an impact analysis of the changes presented to a test lab, who in turn write to the CMVP to add the new version to the existing certificate.
- Easier if you have anticipated recertification. Excluding areas as not security relevant during the original evaluation makes life easier when doing your impact analysis of changes, especially when trying to justify that a 1SUB rather than 3SUB is required.
- Also gets you credit with a lab as it shows you have thought about the issue in advance and are not just justifying your argument after the fact.

1SUB v 3SUB

- 1SUB – requires conformance to the guidance at the time of the original certification and does not go through the CMVP queue and so is quick, typically less than a month.
- 3SUB – requires conformance to current guidance and goes through the main queue. This is a re-validation, so all of the validation boxes need to be checked.

Draft IG G.x Report Submissions encompassing Multiple Modules

- Restrictions on number of module variants that may be submitted on a single test report.
- Consideration given to differences in platforms such as not submitting mobile and server platforms on a single certificate.
- Not clear what effect this will have on adding a new operational environment to a module using a 3SUB.

Conclusion

- Don’t treat evaluation as a one-off event
- Anticipate recertification
- Control module scope
- Choose evaluated configurations carefully

Contact Details

Alan Gornall

Rycombe Consulting Limited

alan.gornall@rycombe.com

+44 1273 476366

RYCOMBE

CONSULTING