Certification process

“Are we on the right track?”

Fabien Deboyser
ICMC 2017 – May 17th 2017
C13c
A little look to FIPS 140 history

- **January 11th 1994** - Signature of FIPS 140-1 by the US government. FIPS 140-1 becomes mandatory for the protection of sensitive data.

- **July 17th 1995** - NIST established the CMVP to validates FIPS 140-1 for Cryptographic Modules. CMVP is a joint effort between NIST and CSE.

- **May 25th 2001** - FIPS 140-2 is released and supersedes FIPS 140-1.

- CMVP is studying the adoption of ISO/IEC 19790 as a revision of FIPS 140-2.

“The more you know about the past, the better prepared you are for the future”

*Theodore Roosevelt*
Why do we do FIPS 140 certification daddy?
FIPS 140 certification

- Computer Security Act of 1987 and FISMA 2002
  Mandatory standard by the US government for the protection of sensitive information

- Requested by customers for compliance and audits, requested in the call for tenders

- FIPS 140-2 is “recognized by the market”
Come and join us 😊
FIPS 140 certification process

**Developer**
- Develops product and documentation
- Engage the laboratory
- Run the CAVP testing

**Laboratory**
- Performs the evaluation
- Performs functional and physical testing

**CMVP**
- Review the report and Security Policy

Source: CMVP website
Certification process in details

Development

- Lab selection
- SOW
- Product development
- Doc preparation

Evaluation

- Review of the evidence
- CAVP
- Functional testing
- Physical testing

Certification

- Review of the evaluation report
- Update of the SP

FIPS pending
Which IG is applicable?

Is it in the FIPS scope?

What do we do?

When will CMVP begin processing?

When will I have my certificate?

Source: wikimedia
360° look

- Based on my experience with
  - Common Criteria FR, ES & UK schemes
  - PCI-PTS

- Let’s have a look at other certification practices to see what might benefit FIPS 140

“We cannot solve our problems with the same thinking we used when we created them”
Albert Einstein

It is a great invention!!! But ... does it comply with all government guidelines?
Kick-off meetings

Kick-off meeting

Meeting pre-evaluation with all 3 parties (in CC “RE0”)

Benefits:
- All 3 parties agree on workload & scope
- Certification Body is aware of the work
- Review of applicable documents

End of evaluation

Meeting pre-certification with all 3 parties (in CC “REINT”)

Benefits:
- Presentation of the evaluation report to the certifier
- Highlight of the results

Source pixabay
Test plan validation

Validation of the test plan by all 3 parties

Benefits

- Testing is performed based on an agreed test plan
- Maximizes the predictability of test cycles and certification timelines

Source: pixabay
Evaluation report

Evaluation Report owned by the developer and the laboratory

Common practice in all certification and is template based

Benefits:

- Developer reviews the report and validates the accuracy which helps the certification
- IP sharing is properly managed
- Comments from the certifier is done on a shared document
- Supports better communication on comments done by the certifier

Source: pixabay
Meeting with all stakeholders on update of the scheme

Common practice in other certification. Form of a regular, ideally face-to-face meeting with stakeholders

Benefits:

- All parties can give feedback to the proposed updates (particularly vendor point of view)
- Ability to anticipate the change
- Getting to know each other
Future work

- Certification update framework
  - Working group ongoing on this subject
  - “Revalidation in response to CVE”

- Evolution of the FIPS 140 supporting documents at a speed “that can be followed”

- “Agile” certification
Thank you!!

Fabien Deboyser
Security Certification Engineer
Thales e-Security - Plantation Florida
Fabien.deboyser@thalesesec.com