Module Supplemental Information – V2.0.0

- General
  - Was the module remotely tested?
  - Were changes made to the module to meet the 140-3 requirements?

- Cryptographic module specification
  - Does the module implement OTAR? – IG D.C
  - Does the module have a non-Approved mode? – Certificate Caveat and SP
  - Are there initialization steps required for the module? – Certificate Caveat and SP
  - Are there excluded components? – AS02.13, AS02.14
  - Does the module allow a degraded mode of operation? – AS02.25
  - Is PPA or PAI implemented? – IG 2.3.C
  - Are there embedded or bound modules? – IG 2.3.A
  - Are there any critical functions? – AS10.16, AS10.23, AS10.24, AS10.52
  - Is the module a sub-chip implementation? – IG 2.3.B
  - Are there any non-approved algorithms used in approved mode? – IG 2.4.A
  - Does the module have a non-compliant state?

- Cryptographic module interfaces
  - Is there an external input device? TE03.05.02, TE03.06.02, TE03.08.02, TE03.11.02
  - Is there an external output device? TE03.05.02, TE03.06.02, TE03.08.02, TE03.11.02
  - Is there a Trusted Channel? – IG 3.4.A
  - Is there a control output interface? – AS03.09, AS03.10

- Roles, services, and authentication
  - Does the module support concurrent operators? – AS04.02
  - Does the module use identity based authentication?
  - Does the module support role based authentication?
  - Does the module have a bypass capability? AS04.22, AS10.21-AS10.22; AS10.47-AS10.51
  - Is there a maintenance role? – AS04.07
  - Does the module support multi-factor based authentication? AS03.22
  - Can operators change roles? – AS04.38, AS04.42
  - Is there default information used for first-time authentication? AS04.46
  - Is a complete image replacement supported within software/firmware loading? – AS04.33-35

- Software/Firmware security
  - Does the module use an EDC for the software/firmware components of a hardware module? – AS05.06
  - Does the module allow external loading of firmware/software? – AS05.13
  - Does the module contain any non-reconfigurable memory? – IG 5.A
  - Does the module utilize Open Source software? – Annex B

- Physical security
  - Is there a maintenance access interface? – AS07.11,12,13
  - Are there any ventilation holes or slits? - AS07.20, AS07.25
  - Are there any removable cover/doors? – AS07.22, TE07.39.02,05, AS07.47, TE07.51.02,07,08, AS07.62, TE07.65.02,07,08
  - Are there tamper seals? – IG 7.3.A
  - Are there tamper seals applied by the module user? – Caveat
  - Does the module implement EFP or EFT mechanisms?

- Non-invasive security

- Sensitive security parameters management
    - Are there plaintext keys, CSPs or sensitive data output? – AS09.16/17
    - Does the module support manual/direct entry of SSPs? AS09.15, AS10.42 to 46, TE10.46.04
    - Is Split Knowledge Utilized? – AS09.21, AS09.22, AS09.23
    - Is One Time Programmable (OTP) memory used in the module? – IG 9.7.A

- Self-tests

- Life-cycle assurance
    - Are there any CVEs related to this module? – IG 11.A

- Mitigation of Other Attacks
    - Is the module designed to mitigate other attacks? – Section 12

- Approved Security Functions
    - Are any non-NIST curves used? – IG C.A