ECSEC Laboratory

Cryptographic Algorithm Validation Program (CAVP) Implementation Procedures

1. Objective

   Describe the procedures to be followed to obtain the CAVP. The procedure is for acquisition by ECSEC Laboratory.

2. Implementation procedure

   Step1: Listen for product information and encryption algorithms (ECSEC Lab)

   Step2: Respond with an estimate of acquisition costs (ECSEC Lab)

   Step3: Order (Vendor)

   Step4: Determine the cryptographic algorithm (Vendor)

   ECSEC Lab provides Vendor with a file to select the parameter for testing cryptographic algorithm. Vendor fills out the form and submit it to ECSEC Lab.

   Using Pre-TEST Environment

   Step5: Provide "request files" for each cryptographic algorithm (ECSEC Lab)

   Vendor must create a tool that reads "request files", sends it to the target implementation, receives the result from the target implementation, and writes it out in the specified format ("response files").

   The formats are shown in links for each algorithms of "Supported Algorithms" on the https://pages.nist.gov/ACVP/.

   ECSEC Lab can provide sample files (both "request files" and "response files").

   Step6: Using the provided "request files", execute cryptographic functions (encryption/decryption, hash computation, signature generation/verification, etc.) of the target implementation, and return the result ("response files") to ECSEC Lab (Vendor)

   Step7: Validate "response files" (ECSEC Lab)

Step8: If successful, the program will be moved to the TEST Environment (ECSEC Lab)
If it fails, return to step5 and the process will be conducted again (Step6, Step7) with new request files.

Using TEST Environment

Step9: Provide "request files" for each cryptographic algorithm (ECSEC Lab)

Step10: Using the provided "request files", perform encryption and return the result ("response files") to ECSEC Lab (Vendor)
If necessary, ECSEC lab visits the test site to verify information provided by Vendor.

Step11: Validate "response files" (ECSEC Lab)

Step12: If successful, apply to NIST for certificate (ECSEC Lab)
If it fails, return to Step9 and the process will be conducted again (Step10, Step11) with new request files.

Step13: To be listed on the CAVP website