

National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme



**Interim Guidance
for
Evaluation of Self-Encrypting Drives for the
Hard Copy Device Protection Profile (HCD PP)**

6 November 2015

**9800 Savage Road, STE 6940, Ft. Meade, MD 20755-6940
Phone: (410) 854-4458 Fax: (410) 854-6615
E-mail: niap@niap-ccevs.org
<http://www.niap-ccevs.org>**

DESCRIPTION:

This guidance outlines an interim approach that allows for evaluation of Hard Copy Device products that implement Self Encryption Drives (SED) for secure data storage until Common Criteria evaluated SEDs are readily available.

BACKGROUND:

In February 2015, the Full Drive Encryption (FDE) international Technical Community (iTC) published the Encryption Engine (EE) collaborative Protection Profile (cPP). The cPP provides requirements for a component that securely encrypts data on a drive, to include a Self Encrypting Drive (SED). Because there are no evaluations completed against the FDE EE cPP, HCDs undergoing evaluation are currently unable to satisfy Security Functional Requirements (SFR) in the HCD Protection Profile necessitating use of an evaluated SED.

RESOLUTION:

HCDs may use SEDs that have received only a FIPS 140-2 (CMVP) certification. The HCD Security Target must list CMVP certificates for all SEDs providing security functionality used by the HCD.

EFFECTIVE DATE:

This guidance is implemented immediately.

FUTURE:

Version 2.0 of the FDE EE cPP is currently scheduled for publication in Q1 2016. NIAP will review this guidance for continued applicability following publication of FDE EE cPP version 2.0.

9800 Savage Road, STE 6940, Ft. Meade, MD 20755-6940
Phone: (410) 854-4458 Fax: (410) 854-6615
E-mail: niap@niap-ccevs.org
<http://www.niap-ccevs.org>