

In P2PE, how do "hybrid" decryption environments differ from "hardware" decryption environments?

PCI SSC FAQ | Article 1248 | April 2020

In a hardware decryption environment, all decryption operations are performed only by PCI listed or FIPS approved HSMs.

In a hybrid decryption environment, the decryption of account data is performed on a "Host System", outside of an HSM. The solution provider's decryption environment may consist of multiple Host Systems in one or more locations. When the Host System is required to decrypt encrypted account data received from a POI, the account-data decryption key (DDK) is retrieved from a key store protected by the HSM, then passed to the Host System. The Host System temporarily retains account-data decryption keys (DDKs) in volatile memory for the purpose of decrypting account data. When the DDK reaches the end of its cryptoperiod, it will be erased from memory. These DDKs are the only keys permitted to exist in the clear outside of the HSM and only for the purpose of decrypting account data. All other cryptographic keys, functions and key management operations must still occur within the secure cryptographic devices (HSMs).

In both hardware and hybrid decryption environments, all HSMs used in the solution must be approved to either FIPS140-2 (or 140-3) Level 3 or higher, or to PTS HSM. Refer to the P2PE Standard for further information.

Source: <https://www.pcisecuritystandards.org/faqs/1248/>