May 20, 2022

HashiCorp
101 2nd St #575
San Francisco, CA
94105

To Whom It May Concern:

Leidos completed its conformance review of the HashiCorp Vault **v1.10.0+ent FIPS Enabled** build (the "Product") on May 13, 2022; and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic module:

- BoringCrypto (FIPS 140-2 Cert. #3678). This will be referred to as the "Integrated Cryptographic Module" throughout the remainder of this document.

Specifically, under the following assumptions:

1. The operator of Vault does not utilize the Transits Secret Engine with external AES-GCM initialization vectors (IVs)

Leidos' review confirmed that the Integrated Cryptographic Module is properly being leveraged for, but not limited to, the following features and use cases:

1. The Vault application programming interface (API) Client uses the Integrated Cryptographic Module to configure and establish transport layer security (TLS) connections, validate the state header format, create TLS listeners, generate cryptographic keys, produce certificate authority (CA) certificates, and to hash plugin files.
2. The Vault plugin helper uses the Integrated Cryptographic Module to configure and establish TLS connections between the Vault plugins and the server.
3. The Vault secure shell (SSH) agent uses the Integrated Cryptographic Module to configure SSH connections.
4. Vault's built-in App ID authentication method uses the Integrated Cryptographic Module to calculate and store hashes of App IDs and User IDs.
5. Vault's built-in App Role authentication method uses the Integrated Cryptographic Module to calculate and store hash-based message authentication code (HMAC) digests of Role Names and Secret IDs.
6. Vault's built-in Amazon web services (AWS) authentication method uses the Integrated Cryptographic Module to verify digital signatures to confirm instance identities, produce HMAC digests to produce role tags, perform symmetric and asymmetric encryption and decryption, and perform Approved digital signature generations and verifications.
7. Vault's built-in TLS certificate authentication method uses the Integrated Cryptographic Module to check the validity of the client's TLS certificate in that it is signed by a trusted certificate authority.
8. Vault uses the Integrated Cryptographic Module to generate random/dynamic database passwords.
9. Vault's public key infrastructure (PKI) secrets engine uses the Integrated Cryptographic Module for certificate management operations including generating certificates, signing certificates, building certificate revocation lists, and parsing information from certificates.
10. Vault's SSH secrets engine uses the Integrated Cryptographic Module for certificate management operations including generating key pairs and certificates, signing certificates, and validating signing keys.
11. Vault's Transit secrets engine uses the Integrated Cryptographic Module to provide cryptographic operations as a service, inclusive of key generation, encryption and decryption, hashing, HMAC generation and verification, and digital signature generation and verification.
12. Vault uses the Integrated Cryptographic Module to perform hashing operations to add objects (keys) to a Merkle tree for replication.

13. The Vault agent uses the Integrated Cryptographic Module for TLS communication, to generate and derive cryptographic keys and to perform encryption and decryption operations.
14. Vault uses the Integrated Cryptographic Module to configure and establish TLS connections with multiple physical storage backends (including but not limited to Consul, Aerospike, Cassandra, MySQL, Raft, ZooKeeper, InfluxDB, and MongoDB) as well as to generate keys and certificates.
15. The Vault SDK libraries use the Integrated Cryptographic Module to provide a set of utility/helper functions for developing Vault plugins that are integrated into Vault, inclusive of functions to parse information from certificates, generate and compare key pairs, generate serial numbers, generate certificates and certificate signing requests (CSRs), and sign certificates.
16. Vault's key policy engine uses the Integrated Cryptographic Module to provide a set of utility/helper functions for cryptographic operations such as deriving and generating keys, performing encryption and decryption, and generating and verifying digital signatures. These functions are used by other Vault features such as the Key/Value secrets engine, Transit secrets engine, and Transform secrets engine.
17. Vault uses the Integrated Cryptographic Module to perform key generation as well as encryption and decryption operations for its barrier functionality.
18. Vault uses the Integrated Cryptographic Module for TLS activity, including but limited to the creation of TLS connections and listeners for replication and incoming API requests as well as to perform related operations such as forwarding TLS replication requests as part of the Raft consensus algorithm, client-side TLS authentication, TLS key pair and certificate generation, lookups for client, server, and CA certificates, performing encryption and decryption, and verifying HMAC digests on signed tokens.
19. Vault uses the Integrated Cryptographic Module in the context of write-ahead logging (WAL) to calculate HMAC digests of the WAL state and to provide the hashing function for Merkle trees.
20. Vault uses the Integrated Cryptographic Module to perform audit log hashing.
21. The Product will not operate if the Integrated Cryptographic Module is missing or altered.

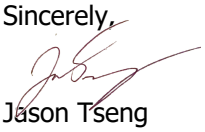
Details of Leidos' review, which consisted of source code review and operational testing, are obtainable by special request.

Please note that for this review, Leidos only examined the Product features referenced above and while the Product may contain other features or functionality, Leidos did not examine these during its review and makes no claims or representations regarding them. Furthermore, the Cryptographic Module Validation Program (CMVP) has not independently reviewed Leidos' analysis, testing, or results.

The intention of this letter is to provide independent opinion that the Product correctly integrates and uses validated cryptographic modules within the scope of claims indicated above. Leidos offers no warranties or guarantees with respect to the above-described compliance review. This letter does not imply a Leidos certification or product endorsement.

Please let us know if you have any questions.

Sincerely,



Jason Tseng
Leidos Cryptographic and Security Testing Laboratory (CSTL) Lab Director