National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Shift5, Inc. Software File-Based Encryption

Report Number: CCEVS-VR-VID11663-2026
Dated: July 28, 2026
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson
Lisa Mitchell
Jaemond Reyes
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Reed Eberly
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This Validation Report (VR) documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of Shift5, Inc. Software File-Based Encryption solution provided by Shift5, Inc. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in July 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements of the:

- *PP-Configuration for Application Software and File Encryption*, Version 1.1, 07 April 2022 (CFG_APP-FE_v1.1) which includes the:
    - Base PP: *Protection Profile for Application Software*, Version 1.4, 7 October 2021 (ASPP14)
    - PP-Module: *PP-Module for File Encryption*, Version 1.0, 25 July 2019 (FE10)
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 (PKGTLS11).

The TOE is the Shift5, Inc. Software File-Based Encryption (Shift5 SW FBE) version 1.3. The TOE, identified in this VR, has been evaluated at a NIAP approved CCTL using the *Common Methodology for IT Security Evaluation* (Version 3.1, Rev 5) for conformance to the *Common Criteria for IT Security Evaluation* (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR and the Assurance Activities Report (AAR). The Validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The technical information included in this report was obtained from the *Shift5, Inc. Software File-Based Encryption Security Target*, version 0.4, July 23, 2026 and analysis performed by the Validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST: describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The PP/PP-Module to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Shift5 Software File-Based Encryption version 1.3
Protection Profile	*PP-Configuration for Application Software and File Encryption*, Version 1.1, 07 April 2022 (CFG_APP-FE_v1.1) which includes the: • Base PP: *Protection Profile for Application Software*, Version 1.4, 7 October 2021 (ASPP14) • PP-Module: *PP-Module for File Encryption*, Version 1.0, 25 July 2019 (FE10) *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 (PKGTLS11).
ST	*Shift5, Inc. Software File-Based Encryption Security Target*, version 0.4, July 23, 2026
Evaluation Technical Report	*Evaluation Technical Report for Shift5 Software File-Based*, version 0.2, July 23, 2026
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	Shift5, Inc.

Item	Identifier
Developer	Shift5, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Lisa Mitchell, Jaemond Reyes, Lori Sarem

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE provides software File-based Encryption within the computer systems in which it operates.

For the purposes of evaluation, the TOE was evaluated for its compatibility with Shift5's hardware platforms running a proprietary SUSE Micro Linux 6-based operating system. The TOE was fully tested running on a Shift5 Manifold hardware running the SUSE Linux Micro 6.0-based platform image and an internal Rancher Government Solutions Rancher Kubernetes Engine 2 (RKE2) running on an Atom C3708 CPU.

3.1 TOE Description

The Shift5 SW FBE is an OCI-containerized software application that Shift5 distributes as a part of their proprietary OS images for their supported hardware platforms (such as their Manifold product line). The TOE provides file-based encryption for designated files and accepts an administratively provided passphrase to enable its file encryption service or decrypt requested files.

The TOE consists of multiple inner processes. The TOE WebUI binds to a local address and provides an HTTPS interface for administrators to login or configure the TOE. The administrator provides the file-encryption passphrase through the command line and starts the file encryption services through the WebUI on the system. Upon unlocking the TOE Data at Rest Protection (DARP) service, the TOE derives the necessary key values, encrypts data using 256-bit AES-XTS, and writes the encrypted results to disk. Lastly, the TOE also has a separate, command-line interface used for decrypting data. The decryption utility takes in the same file-encryption passphrase, validates the password against a saved fingerprint, decrypts the FEK from file metadata, and saves the decrypted file data to a new file.

The Manifold product used for testing also features a separate full-drive encryption layer that is bundled with the TOE Platform, however that is outside the scope of this evaluation and is evaluated separately. Similarly, the TOE features multiple modes of operation, however the TOE requires that only its attended mode of operation is used in order to be compliant with the evaluated configuration. The attended mode of operation is enabled upon default installation of the TOE, which disables all non-attended, or non-password-based modes of authentication.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

The Product is a locally managed system that provides FBE protection for persistent data stored to an internally monitored directory.

3.4 Physical Boundaries

The TOE is a containerized software application that is designed to operate inside the Shift5 hardware product lines and interact with the host operating system and additionally installed software. The boundary of the software application is the singular, containerized image pertaining to the FBE solution, distributed by Shift5 as a part of their platform OS.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security management
5. Privacy
6. Protection of the TSF
7. Trusted path/channels

4.1 Cryptographic support

The TOE uses Automated Cryptographic Validation Test System (ACVTS)-validated cryptographic algorithm implementations, provided by two crypto libraries managed by the TOE developer. All these cryptographic libraries are installed with the TOE, to support key generation and derivation, encryption/decryption, and establishment of trusted channels to protect data in transit. Using these cryptographic libraries, the TOE implements a file-based encryption scheme to protect sensitive data at rest. The TOE implements a HTTPS/TLS server to securely provide an administrator WebUI used to manage the TOE. The TOE also relies on direct links to hardware entropy provided by Intel CPUs with RDSEED instructions to generate entropy that is used as input data for each of the TOE's deterministic random bit generator (DRBG).

4.2 User data protection

The TOE implements functionality to encrypt sensitive data through its file-based encryption scheme. To manage this service, the TOE utilizes command-line level utilities and provides a WebUI interface to enable the file encryption service and manage administrator passphrases. Outside of the network connectivity used by the WebUI and by the user to check for updates, the TOE makes no access to any special hardware or sensitive data repository. The TOE properly protects all data at rest and destroys all references to sensitive and plaintext data upon transitioning to a powered off state.

4.3 Identification and authentication

The TOE provides user authorization based on a file-encryption passphrase to protect the keys used for file-based encryption.

4.4 Security management

The TOE requires a file-encryption passphrase, a WebUI access passphrase, a webserver certificate and private key, and a web credential passphrase used to encrypt the webserver private key in storage. The TOE provides default credentials for the WebUI access credentials that must be changed after first login before the WebUI provides any functionality. For all remaining credentials, the TOE does not provide any default values, and they are configured by the user during the initial provisioning. The TOE provides two management interfaces: a WebUI which

can enable/disable the encryption service, and a local console connection which the administrator can use to provide passwords, start the WebUI interface, manage files, and access the separately managed decryption utility. The TOE relies on a new file-encryption passphrase each time the encryption service is started and that same passphrase can be used to later decrypt any files protected during that instance. By default, the TOE is configured with file permissions to protect itself and its data from unauthorized access.

4.5 Privacy

The TOE does not transmit personally identifiable information (PII) over any network interfaces.

4.6 Protection of the TSF

The TOE protects itself against exploitation by implementing address space layout randomization (ASLR) and by not allocating any memory region for both write and execute permission. The TOE uses standard, well-documented APIs and includes third-party libraries used to perform its functions. As a part of the evaluation process, the vendor provided a SBOM listing all the integrated 3rd party libraries to NIAP for approval.

The TOE provides the ability to check the version of the TOE as well as to check for TOE updates through its WebUI. TOE software is digitally signed and distributed as a part of the operating system. Updates to the TOE containerized application are signed such that the application platform can cryptographically verify them prior to installation. The TOE does not update its own binary code in any way and when removed, all traces of the TOE application software are deleted.

4.7 Trusted path/channels

The TOE protects communications between itself and a remote administrator using the WebUI interface with TLS/HTTPS.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 (ASPP14)
- *PP-Module for File Encryption*, Version 1.0, 25 July 2019 (FE10)
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 (PKGTLS11)

That information has not been reproduced here and the ASPP14/FE10/PKGTLS11 should be consulted if there is interest in that material.

5.2 Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP14/FE10/PKGTLS11 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the ASPP14/FE10/PKGTLS11 and performed by the Evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- The TOE consists solely of software and relies on its operational environment for supporting security functionality, as identified in the ST.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ASPP14/FE10/PKGTLS11 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- *Shift5 File – Based Encryption (FBE) Administrator Guidance Document (AGD)*, Version 1.3, April 2026

To use the product in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation team. It is derived from information contained in the proprietary *Detailed Test Report for Shift5, Inc. Software File-Based Encryption*, Version 0.2, July 23, 2026 (DTR), as summarized in the evaluation *Assurance Activity Report for Shift5, Inc. Software File-Based Encryption*, Version 0.2, July 23, 2026 (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the ASPP14/FE10/PKGTLS11 including the tests associated with optional requirements. The AAR, in sections 1.1 and 3.4.1, lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The containerized TOE application was fully tested on a Shift5 Manifold hardware running the SUSE Linux Micro 6.0-based platform image and an internal Rancher Government Solutions Rancher Kubernetes Engine 2 (RKE2) running on an Atom C3708 CPU.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Shift5 SW FBE TOE to be Part 2 extended, and to meet the SARs contained in the ASPP14/FE10/PKGTLS11.

9.1 Evaluation of the Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Shift5 Software File-Based Encryption version 1.3 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and product guidance document. Additionally, the Evaluation team performed the assurance activities specified in the ASPP14/FE10/PKGTLS11 related to the examination of the information contained in the TSS.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guide was assessed during the design and testing phases of the evaluation to ensure it was complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted

in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the ASPP14/FE10/PKGTLS11 and recorded the results in the DTR, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the DTR prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities.

The Evaluation team searched the MITRE CVE Database, National Vulnerability Database, and CVE details (https://www.cve.org/, https://web.nvd.nist.gov/vuln/search, and https://www.cvedetails.com/vulnerability-search.php) and Known Vulnerability Exploit Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) on 7/17/2026.

The following search terms were used: "Shift5", "Manifold", "SUSE Linux Micro", "Intel Atom C3708", "Data at rest protection", "Alping ca-certificates", "chainguard", "wolfi", "glibc", "stdlib", "golang", "apk", "apk/libselinux", "apk/lvm2", "apk/pcre2", "apk/popt", "apk/userspace-rcu", "apk/util-linux@", "apk/json-c", "alexedwards/scs/v2", "awnumar/memcall", "awnumar/memguard", "beorn7/perks", "ccoveille/go-safecast", "cespare/xxhash/v2", "fsnotify/fsnotify", "go-logr/logr", "goccy/go-yaml", "golang-migrate/migrate/v4", "google/go-sev-guest", "google/go-tpm-tools", "google/logger", "google/uuid", "hashicorp/errwrap", "hashicorp/go-multierror", "hashicorp/hcl", "justinas/alice", "justinas/nosurf", "lmittmann/tint", "magiconair/properties", "mattn/go-isatty", "mitchellh/mapstructure", "moby/sys/mountinfo", "moby/sys/userns", "munnerz/goautoneg", "pborman/uuid", "pelletier/go-toml/v2", "pkg/errors", "prometheus/client_golang", "prometheus/client_model", "prometheus/common", "prometheus/procfs", "remyoudompheng/bigfft", "rs/cors", "sagikazarmark/slog-shim", "spf13", "spf13/afero", "spf13/cast", "spf13/cobra", "spf13/pflag", "spf13/viper", "subosito/gotenv", "urfave/cli/v3", "veqryn/slog-context", "go.uber.org/atomic", "go.uber.org/automaxprocs",

"go.yaml.in/yaml/v2", "golang.org/x/crypto", "golang.org/x/sys", "golang.org/x/text", "google.golang.org/protobuf", "gopkg.in/ini.v1", "gopkg.in/yaml.v3", "k8s.io/klog/v2", "k8s.io/mount-utils", "k8s.io/utils", "modernc.org/libc", "modernc.org/mathutil", "modernc.org/memory", "modernc.org/sqlite", "stdlib", "pk/inih", "openssl", "linux kernel 6.11.3", "util-linux", and “libgcrypt”.

The results of these searches did not identify any vulnerabilities applicable to the TOE.

The Shift5, Inc. Software File-Based Encrypton evaluation included the Vendor submission of a Software Bill of Materials (SBOM) for analysis, per NIAP policy. The SBOM provided a comprehensive listing of the third-party library components contained in the TOE. The SBOM was used in vulnerability analysis during the evaluation period and was updated by the Vendor as requested by NIAP.

The conclusion drawn from the vulnerability analysis is that no residual TOE vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.7 Summary of Evaluation Results

The Evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The Validation team’s assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Shift5 File – Based Encryption (FBE) Administrator Guidance Document (AGD)* listed in the Documentation section of this VR. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore, should not be relied upon to configure or operate the TOE as evaluated.

The Validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST and only that functionality was evaluated. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness. Specifically, the CLI is enabled locally and is protected through normal OS-level accounts. These protections are outside the TOE boundary.

It is also noted that TOE requires that only its attended mode of operation be used in the evaluated configuration. During default installation of the TOE, all non-attended or non-password-based modes of authentication are disabled.

In addition, for the purposes of this evaluation, the TOE is compatible with any of the SUSE Linux Micro 6-based images Shift5 provides for their product line that ship with the TOE pre-installed. It is not evaluated as a separate container to be used by other products.

Per NIAP/CCEVS Publication #6, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

The Validation team also strongly recommends that all TOE platforms in the operational environment are kept up to date with patches as they are released.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Shift5, Inc. Software File-Based Encryption Security Target*, Version 0.4, July 23, 2026.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation team used the following documents to produce this VR:

[1] *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, April 2017.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.

[4] *Protection Profile for Application Software*, Version 1.4, 7 October 2021 (ASPP14).

[5] *PP-Module for File Encryption*, Version 1.0, 25 July 2019 (FE10).

[6] *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 (PKGTLS11).

[7] *Shift5, Inc. Software File-Based Encryption Security Target*, Version 0.4, July 23, 2026 (ST).

[8] *Shift5 File-Based (FBE) Administrator Guidance Document (AGD)*, Version 1.3, April 2026 (AGD).

[9] *Assurance Activity Report for Shift5, Inc. Software File-Based Encryption*, Version 0.2, July 23, 2026 (AAR).

[10] *Detailed Test Report for Shift5, Inc. Software File-Based Encryption*, Version 0.2, July 23, 2026 (DTR).

[11] *Evaluation Technical Report for Shift5 Software File-Based Encryption*, Version 0.2, July 23, 2026 (ETR).