Kedify FIPS 140-3 Attestation

Release: `kedify/agent@v0.5.7`

Commit: `c5f64dd3fff641c4cb62ab261225cb79401aa904`

Generated date: `2026-05-19T10:59:13Z`

Summary

This document is a vendor self-attestation for the hardened container image variants published by Kedify in the release identified above. It describes the FIPS 140-3 cryptographic posture of those images for procurement teams and security questionnaires.

The cryptographic module embedded in Kedify binaries is the Go Cryptographic Module, and its CMVP status is tracked by the upstream Go team. The claim is FIPS Inside: each hardened Kedify binary embeds the validated module and routes approved cryptographic operations through it.

Cryptographic module

Item	Value
Module name	Go Cryptographic Module
Module version	`v1.0.0`
FIPS standard	FIPS 140-3
CMVP status	Tracked at https://go.dev/security/fips140
Build flag (Go)	`GOFIPS140=v1.0.0`
Required Go version	1.24 or later
External dependencies	None. The module is statically compiled into each Kedify binary.

The CMVP cert state for the Go Cryptographic Module changes as it moves through validation. The link above is the source of truth at any given moment.

Images in scope

The following images embed the Go FIPS 140-3 module and carry the OCI labels `io.kedify.crypto.module=go-fips140` and `io.kedify.crypto.version=v1.0.0`:

Image: `ghcr.io/kedify/agent`
Tag: `latest-hardened`
Digest: `sha256:94a04b044defe5f18f52b57eda598a353da42a5bfb4da543c5bf895694af755d`

Image: `ghcr.io/kedify/agent`
Tag: `v0.5.7-hardened`
Digest: `sha256:94a04b044defe5f18f52b57eda598a353da42a5bfb4da543c5bf895694af755d`

Manifest digests above are pinned to this release. They will not change for this tag; a future release of the same image will publish a new digest under its own tag.

Build evidence

For every hardened binary built for this release, `go version -m` reports the FIPS module is linked. The exact build settings are:

```
agent-hardened-amd64_linux_amd64_v1/bin/manager-hardened:
    build -buildmode=exe
    build CGO_ENABLED=0
    build GOARCH=amd64
    build GOFIPS140=v1.0.0-c2097c7c
    build GOOS=linux
    build vcs.revision=c5f64dd3fff641c4cb62ab261225cb79401aa904

agent-hardened-arm64_linux_arm64/bin/manager-hardened:
    build -buildmode=exe
    build CGO_ENABLED=0
    build GOARCH=arm64
    build GOFIPS140=v1.0.0-c2097c7c
    build GOOS=linux
    build vcs.revision=c5f64dd3fff641c4cb62ab261225cb79401aa904
```

Signing

Kedify signs this attestation document and the hardened container manifests listed above with a Cosign static keypair. The public key is published at https://docs.kedify.io/kedify-cosign.pub.

Verify the attestation document:

```
cosign verify-blob --key https://docs.kedify.io/kedify-cosign.pub \
  --signature kedify-fips-attestation-v0.5.7.md.sig kedify-fips-attestation-v0.5.7.md
```

Verify each hardened image manifest:

```
cosign verify --key https://docs.kedify.io/kedify-cosign.pub   ghcr.io/kedify/agent:latest-hardened

cosign verify --key https://docs.kedify.io/kedify-cosign.pub   ghcr.io/kedify/agent:v0.5.7-hardened
```

The signature establishes that the document or image was published by Kedify. The validated module's lab attestation is the upstream Go Cryptographic Module's CMVP record, linked above.

Reporting and contact

Security findings related to this attestation should be sent to support@kedify.io.

References

- Go Cryptographic Module CMVP status: https://go.dev/security/fips140
- Go FIPS 140-3 documentation: https://go.dev/doc/security/fips140
- Kedify FIPS compliance page: https://docs.kedify.io/security-and-compliance/fips/
- NIST CMVP program: https://csrc.nist.gov/projects/cryptographic-module-validation-program