Delivery & verification

Every release of the Ophir engine reaches you as one file, with a checksum and a signature beside it. Your team confirms both with two commands, using tools already on a locked-down host. This document sets out what arrives, how to check it, and how the release was made.

It takes about five minutes to read.

What you receive

Each release is delivered offline. It needs no registry and no internet connection on your side.

`ophir-engine-<version>.tar`	The engine as a container image, saved to a single file
`ophir-engine-<version>.tar.sha256`	The SHA-256 checksum of that file
`ophir-engine-<version>.tar.sig`	A detached ECDSA P-256 signature over that file, made with Ophir's delivery key
`VERIFY.md`	These verification steps, shipped with every release

The version is pinned for your engagement. What runs in production is the file you verified, loaded from disk.

Verify it in two commands

Both commands use stock OpenSSL and the standard checksum tool. There is nothing to install.

```
shasum -a 256 -c ophir-engine-<version>.tar.sha256
openssl dgst -sha256 -verify signing.pub \
  -signature ophir-engine-<version>.tar.sig ophir-engine-<version>.tar
```

Expected output: `OK`, then `Verified OK`.

The first command confirms the file arrived intact. The second confirms it is the file Ophir signed. If either prints anything else, do not deploy: contact us, and keep the file as received.

The delivery key

The signature is checked against the public half of Ophir's delivery key, signing.pub. It ships with every release and is published on this site. Its fingerprint, the SHA-256 of the public key in DER form, is:

```
113d 5b85 279e 8fc8 c236 6523 1446 e7f3 bc68 7150 b324 5c61 d3b2 f814 2484 7eb5
```

Confirm the fingerprint through a second channel before you rely on it: it is also printed in your engagement schedule. To compute it from the copy of the key you hold:

```
openssl pkey -pubin -in signing.pub -outform DER | shasum -a 256
```

The private half of the key is held by Ophir alone. It is stored encrypted and is not in any repository or build system.

How a release is made

- Every change to the engine runs the automated test suite. One of those tests generates synthetic data with known faults planted in it, and requires the engine's findings to equal the faults that were planted.
- The container image is then built and run against the bundled reference scenario.
- Signing is done by a named person at the point of delivery. It is a deliberate act, not a step in an automated pipeline.
- The release script checks its own signature as soon as it is made, and stops with an error if the signing key is absent. An unsigned release cannot be produced by it.

What runs inside your environment

- The engine is written in Python and uses the standard library only. It carries no third-party packages.
- It runs as an unprivileged user on a read-only filesystem, and writes only to a temporary directory and the store you mount for it.
- It needs no internet egress.
- Credentials come from your vault at run time. They are never in the image, the configuration files or the logs.

The deployment design for your estate is prepared with your security team and shared under a mutual NDA.

Deploying, and recovering

- A release is loaded, verified and started inside your change window, through your change board.
- A restore drill, redeploying from the verified file and restoring the database, is run once before go-live.
- The engine fails safe: if it stops, your existing manual process continues.
- The operations runbook for your deployment is complete before the parallel run is signed off.

See the output first

The sample evidence pack and suspense ledger on the due-diligence shelf are the engine's output from its reference run, on synthetic data. They are the files a release produces, in the form your operations team and your examiner would receive them.

Questions on this document: hello@ophirdigital.com.

Ophir Controls is a trading style of Ophir Digital Ltd, a company registered in England and Wales, company number 17338110. Registered office: Mansion House, Manchester Road, Altrincham, Cheshire, England, WA14 4RW.