

STAGE 1: INTERMEDIATE (Build Stage)

1. Specify Arguments

- Signature Algorithm: ML-DSA-65
- **TLS Group: X25519MLKEM768:X25519**
- OS: Alpine 3.21
- BASEDIR: /opt
- INSTALLDIR: \${BASEDIR}/nginx

2. Git Clone Dependencies

- liboqs (0.13.0)
- oqs-provider (0.9.0)
- **openssl (3.5.4)**
- nginx (1.28.0)
- **curl (8.11.1)**

3. Compile & Install

- **openssl 3.5.4 : including oqs-provider**
- liboqs Library : static link (liboqs.a)
- nginx (using SSL Module) : dynamic link to **openssl 3.5.4**
- oqs-provider : oqsprovider.so connected to MODULESDIR
- **curl: dynamic link to openssl 3.5.4**

4. Minimize Image

- strip: Binaries optimized

STAGE 2: RUNTIME (Final Image)

1. Copy

- nginx Binary + Config (\${INSTALLDIR})
- OpenSSL Binaries + Libs (\${OSSLDIR})
- OQS-Provider Module (.so)

2. Configure

- OPENSSL_CONF : openssl.cnf (PQC aktiviert)
- **DEFAULT_GROUPS : X25519MLKEM768:X25519**
- Logging : /dev/stdout, /dev/stderr

3. Secure

- Non-Root User : oqs (UID 1000)
- Ownership : oqs:oqs (\${INSTALLDIR})

4. Define

- ENTRYPOINT using nginx at container start