Zen Crypted Operating System

Технічна декларація

Заморожений базовий рівень Erlang/OTP 20 з LibreSSL 3.1.5 для контрольованого подальшого патчингу

На основі вимог високого рівня довіри

Для статичних Protection Domain seL4

Формалізовано згідно з практиками ISO/IEC/IEEE 29148

OS.1: Frozen Baseline Declaration
Erlang/OTP 20 + LibreSSL 3.1.5

Namdak Tonpa (maxim@synrc.com), Synrc Research

19 серпня 2026 р.

Анотація

This document formally declares a frozen software baseline consisting of Erlang/OTP 20 (final maintenance line) statically linked against LibreSSL 3.1.5. The freeze is instituted to enable rigorous, reviewable and reproducible further patching in high-assurance environments, particularly those employing the seL4 microkernel with static Protection Domains, single-core execution and a minimised cryptographic surface (including the synrc/ca pure-ASN.1 stack). The declaration establishes the precise component versions, the rationale for the freeze, the permitted scope of subsequent patches, the exact `:crypto` and `:public_key` call surface, and the governance principles under which any modifications may be introduced.

Зміст

1. Introduction

Modern cryptographic and runtime ecosystems evolve rapidly. Continuous upstream updates, while beneficial for general-purpose systems, introduce unacceptable variability and review burden for high-assurance, formally constrained or long-lived embedded deployments. In such contexts a deliberately frozen and fully characterised baseline is a prerequisite for meaningful security evaluation, deterministic behaviour and controlled remediation.

This paper declares the following frozen baseline:

- **Erlang/OTP 20** (final maintenance releases, including 20.3.8.x);
- **LibreSSL 3.1.5** (December 2020), used as the sole cryptographic provider via the OTP `crypto` NIF, preferably under static linkage.

The baseline is intended for systems that prioritise auditability, minimality and isolation (e.g. seL4 static Protection Domains) over access to the newest cryptographic primitives or protocol features.

2. Rationale for the Freeze

1. **Reviewability.** OTP 20 and LibreSSL 3.1.5 constitute a finite, historically bounded codebase. Their combined surface can be subjected to exhaustive manual and automated review.
2. **Reproducibility.** Exact source trees, build configurations and linkage methods can be archived and regenerated years later.
3. **Compatibility with constrained execution environments.** Single-core, non-SMP, statically linked builds of OTP 20 map cleanly onto seL4 Protection Domains with minimal capability sets.
4. **Controlled patching surface.** By freezing the major versions, all subsequent security or correctness fixes become explicit, localised patches against a known baseline.
5. **Alignment with existing high-assurance stacks.** The baseline is compatible with pure-Erlang ASN.1 approaches (exemplified by synrc/ca) that minimise reliance on high-level LibreSSL X.509 APIs while still requiring a stable cryptographic substrate.

3. Precise Baseline Definition

Component	Version / Identifier	Notes
Erlang/OTP	20.3.8.x (final)	SMP disabled or strictly limited; static NIFs preferred
`crypto`	OTP 20 corresponding	Sole interface to LibreSSL
`public_key`	OTP 20 corresponding	Retained for records and pkix helpers
`asn1`	OTP 20 corresponding	Required by public_key and synrc ASN.1 modules
LibreSSL	3.1.5	Static linking; unnecessary features disabled
Linkage	Static (preferred)	`libcrypto.a` linked into the crypto NIF
Higher-level stack	synrc/ca (or equivalent)	Pure-ASN.1 certificate authority layer

Табл. 1: Frozen baseline components.

Build flags for LibreSSL 3.1.5 shall exclude shared libraries, engines, deprecated protocols and non-essential ciphersuites where feasible. OTP shall be configured to avoid dynamic loading of the SSL library.

4. Scope of the Freeze

Frozen (immutable without formal amendment)

- Major and minor version of Erlang/OTP (20.x);
- Exact LibreSSL release (3.1.5);
- Core architectural decisions (single-core preference, static linkage, retention of `public_key`).

Permitted under controlled patching

- Security fixes addressing known CVEs or demonstrated vulnerabilities;
- Correctness patches required for deterministic behaviour on the target platform;
- Minimal adaptations required for seL4 integration or static Protection Domain constraints;
- Removal or disabling of unused code paths (attack-surface reduction);
- Documentation and build-system improvements that do not alter runtime semantics.

Any patch must be explicitly documented with rationale and risk analysis, applied against the frozen baseline, and subject to independent review before integration.

5. Cryptographic Call Surface

The following tables enumerate the exact entry points into the cryptographic substrate that are exercised by the synrc/ca + x509 stack when running on the frozen baseline.

5.1. Direct / Primary :crypto Calls

Function	Typical form	Used for	Called from
:crypto.generate_key/2	generate_key(:ecdh, Curve) or via public_key	EC key pair generation	X509.PrivateKey.new_ec/1 → CA.CSR.root/2, server/2, client/2
:crypto.generate_key/3	generate_key(:eddsa, Curve, Priv)	EdDSA public derivation	x509 (Ed25519/Ed448; secondary for secp focus)
:crypto.sign/4	sign(Algorithm, DigestType, Msg, Key)	ECDSA / RSA signatures	CSR & certificate signing (via x509/public_key)
:crypto.verify/5	verify(Algorithm, DigestType, Msg, Sig, Key)	Signature verification	X509.CSR.valid?/1, certificate checks
:crypto.strong_rand_bytes/1	strong_rand_bytes(N)	Serial numbers, IVs, nonces, salt	Certificate serials, AES IVs, key encryption
:crypto.compute_key/4	compute_key(:ecdh, OthersPub, MyPriv, Curve)	ECDH shared secret	CA.AES shared-secret helpers
:crypto.crypto_one_time/4-5	crypto_one_time(Cipher, Key, IV, Data, Flag)	AES-256-ECB/CBC/GCM/CCM	CA.AES encrypt/decrypt
:crypto.hash/2	hash(sha256 | sha384 | ..., Data)	Digests for signatures / HKDF	Indirect via public_key/x509 and CA.HKDF/CA.KDF
:crypto.hmac/3	HMAC (OTP 20 equivalent)	HKDF / key derivation	CA.HKDF / CA.KDF paths
:crypto.privkey_to_pubkey/2	(engine / modern path)	Derive public from private	X509.PublicKey.derive/1 (engine case)

5.2. Calls Mediated by :public_key

These constitute the most common path inside synrc/ca.

:public_key function	Ultimately uses	Purpose in synrc/ca + x509
public_key:generate_key/1	:crypto.generate_key	X509.PrivateKey.new_ec/1, new_rsa/1
public_key:sign/3 or /4	:crypto.sign	Certificate & CSR signing
public_key:verify/4 or /5	:crypto.verify	CSR / signature validation
public_key:pkix_sign/2	:crypto.sign	Older-style certificate signing
public_key:pem_encode/1, pem_decode/1	mostly pure + crypto for encrypted PEM	Key & certificate PEM I/O in CA.CSR
public_key:pkix_encode/3, pkix_decode_cert/2	ASN.1 + crypto for signatures	DER handling in CMP/EST replies
public_key:der_encode/2, der_decode/2	ASN.1 only	Structure manipulation (no direct crypto)

5.3. Recommended Minimal Whitelist

For the smallest practical attack surface that still supports the full EC-focused synrc/ca functionality on the frozen baseline, the following entry points are sufficient:

```
:crypto.generate_key/2
:crypto.sign/4
:crypto.verify/5
:crypto.strong_rand_bytes/1
:crypto.hash/2
:crypto.compute_key/4          % only if CA.AES / ECDH retained
:crypto.crypto_one_time/5      % only if AES support retained
```

All higher-level certificate structure handling remains in pure Erlang ASN.1 modules and does not enlarge the cryptographic TCB.

6. Patching Policy and Governance

1. **No silent upgrades.** Version numbers of the baseline components remain fixed. Patches are recorded as delta sets against the declared baseline.
2. **Whitelisting of cryptographic entry points.** The `:crypto` NIF surface should be restricted to the minimal set listed in Section 5.3.
3. **Traceability.** Every binary artefact must be accompanied by exact source hashes, full build configuration, list of applied patches, and a mapping of high-level operations to LibreSSL functions.
4. **Exception process.** Introduction of any newer cryptographic algorithm or protocol feature requires a formal amendment to this declaration and a re-evaluation of the isolation and review arguments.

7. Security Considerations and Residual Risk

LibreSSL 3.1.5 post-dates the Heartbleed vulnerability and removes a substantial amount of legacy OpenSSL complexity. Nevertheless it is a 2020-era library and therefore carries residual risk relative to contemporary cryptographic practice. The freeze accepts this risk in exchange for a stable, reviewable foundation.

Mitigations inherent in the intended deployment model include:

- Strong isolation via seL4 static Protection Domains;
- Aggressive reduction of network and protocol attack surface;
- Preference for pure-ASN.1 certificate handling (synrc/ca style);
- Capability minimisation and single-core execution.

The baseline does *not* claim to provide state-of-the-art cryptographic agility. It claims only to provide a well-defined, frozen and patchable foundation upon which higher-assurance arguments can be constructed.

8. Conclusion

We hereby declare Erlang/OTP 20 together with LibreSSL 3.1.5 as a frozen baseline for further controlled patching. This declaration prioritises reviewability, reproducibility and compatibility with high-assurance isolation mechanisms over continuous upstream evolution. All subsequent work on systems adopting this baseline shall treat the stated versions as immutable reference points, with any modifications introduced solely through explicit, reviewed patches.

This freeze is intentional, documented and subject to formal governance. It constitutes a deliberate engineering decision in favour of long-term inspectability and deterministic behaviour.

References (indicative)

- Erlang/OTP 20 release and maintenance documentation.
- LibreSSL 3.1.5 release notes and change log.
- seL4 Reference Manual and Protection Domain model.
- synrc/ca technical description and ASN.1 module set.
- Analyses of OTP `crypto` NIF surfaces and LibreSSL linkage practices.