BCCS-ISR-2026-001

Internal Security Review

Smart contract security assessment of BCCSToken (ERC-20) and BCCSNodeLicense (ERC-721 Soulbound) deployed on Base Layer 2. Conducted by KRYONIS Sovereign Systems Limited.

OVERALL VERDICT: PASS

No critical or high severity issues found. Two low-severity operational notes and three informational observations documented with mitigations.

DOCUMENT	BCCS-ISR-2026-001 v1.0
DATE	April 15, 2026
REVIEWER	KRYONIS Sovereign Systems Limited
CLASSIFICATION	Public
COMPILER	solc v0.8.34 — optimization 200 runs
FRAMEWORK	OpenZeppelin Contracts v5.1.0
CHAIN	Base Layer 2 (Chain ID 8453)

Contracts Reviewed

VERIFICATION UNIT

$BCCS — ERC-20

Supply: 1,000,000,000 (fixed, non-mintable)

Pausable: Yes (owner only)

Permit: EIP-2612

Address: 0xb86174c4c1ca01f0639ce3067306bdf6eeba17a7

INFRASTRUCTURE ACCESS

Node License — ERC-721

Standard: EIP-5192 Soulbound

Tiers: 5 (Alpha – Epsilon)

```
Payment: USDC on Base

Address: 0x44B46f9D170ae8122cce71332884252934b66FBd
```

Findings Summary

0	0	0	2	3
CRITICAL	HIGH	MEDIUM	LOW	INFO

Detailed Findings

LOW-1

Single-Owner Dependency

Both contracts use a single-owner model. While ownership has been transferred to a Safe multisig, it is currently configured as 1-of-1. A compromised signer key could execute all owner functions.

Mitigation: Upgrade Safe to 2-of-3 threshold. No contract changes required.

LOW-2

No Timelock on Critical Functions

Critical functions (pause, setTreasury) execute immediately upon owner approval with no delay period for community review.

Mitigation: Implement TimelockController as intermediate owner in Phase 5.

INFO-1

No Explicit Burn Mechanism

BCCSToken has no dedicated burn() function. Tokens can be burned by sending to the zero address, but no convenience function exists. This is by design for the fixed-supply model.

INFO-2

Unlimited Batch Whitelist Size

The batchWhitelist() function accepts an unbounded array. Extremely large batches could exceed block gas limits. Mitigated by owner-only access and natural gas limits.

INFO-3

Internal Review Scope

This review was conducted internally by KRYONIS Sovereign Systems Limited. While it follows professional methodology and covers standard vulnerability classes, it does not constitute an independent third-party audit. External audit recommended before governance decentralization.

Key Verifications

PASS

Fixed Supply Integrity

No mint function exists post-deployment. Supply of 1,000,000,000 BCCS is permanently fixed. Confirmed by code inspection and BaseScan token tracker.

PASS

Soulbound Enforcement

All transfer vectors are blocked for non-mint/non-burn operations. EIP-5192 locked() returns true for all tokens. Covers transferFrom, safeTransferFrom, and approval-based transfers.

PASS

USDC Payment Security

Mint function protected by ReentrancyGuard. Follows checks-effects-interactions pattern. USDC on Base has no fee-on-transfer. All payments route directly to treasury.

PASS

Access Control

All privileged functions restricted to onlyOwner. Ownership transferred to Safe multisig. No backdoors, no hidden admin functions, no proxy upgradeability.

PASS

Tier Pricing Immutability

Tier prices and supply caps are set in the constructor and cannot be modified. No setter function exists for pricing. Purchasers have price certainty.

Disclaimer

This Internal Security Review is provided by KRYONIS Sovereign Systems Limited for informational purposes. It represents a good-faith assessment of the smart contract code at the time of review. This document does not constitute a guarantee of security, an independent third-party audit, or a warranty of any kind. Smart contracts carry inherent risks. KRYONIS Sovereign Systems Limited recommends that all participants conduct their own due diligence.

— KRYONIS Sovereign Systems Limited, Hong Kong © 2026