BITCOIN WITNESS

Confidence Report

A derived child-seed record

PROVENANCE VERIFICATION

BIP85 CHILD VERIFICATION

READ THIS FIRST

This records a child seed derived from a master seed under BIP85, re-entered on an offline device and matched back against that master.

Important. It does not contain the seed words and cannot move money.

Privacy. The extended public keys and addresses below cannot spend, but they reveal every past transaction and every future address of this account to anyone who holds them. Treat this report as financially sensitive, and share it only with people you intend to have that visibility.

WHAT WAS VERIFIED

DATE	2026-08-05 12:50:18 UTC
BACKUP FORMAT	BIP85 child (BIP39, 12 words)
SEED LENGTH	12 words
LANGUAGE	English
CHILD PASSPHRASE	No
CHILD'S OWN FPR	02E8BFF2
PARENT FPR	73C5DA0A
DERIVATION PATH	m/83696968'/39'/0'/12'/0'
NETWORK	Bitcoin mainnet
AIR-GAP	VERIFIED
VERSION	v1.0

PREPARED FOR & BY

WALLET OWNER

PREPARED FOR

PREPARED BY, DATE

REVIEWED BY, DATE

HOW TO RE-VERIFY · NO SEED REQUIRED

1. Import an extended public key on the following pages into a watch-only wallet on its stated derivation path (Sparrow accepts every key form) and confirm Receive #0 matches the address shown here for that path.
2. Re-derive this child on another BIP85 tool from your master seed, using the index / language / word count you INTENDED (not just the ones printed here) and the master passphrase if your wallet uses one. Confirm both that the master fingerprint matches your known wallet and that the re-derived child matches. Re-deriving from the values printed here only proves you copied them down; it cannot prove they were the ones you meant. A wrong one would derive a valid child of a DIFFERENT wallet.
3. Recompute the Report SHA-256 in the footer and confirm it matches — any change to the document changes the hash. Re-verify on the appliance: menu → Verify File Integrity, or run 'python3 confidence_report.py --verify <this-file>' (prints OK).

Recovery path. Either back up this child's own seed words directly (it is a standalone BIP39 wallet), or re-derive it from the master seed at the derivation path shown in the provenance block below.

Bitcoin Witness. Verify, Attest, Inherit.

APPENDIX — TECHNICAL RECORD

Address derivations for the same wallet under each standard it supports.

DERIVATION RESULTS

BIP84 m/84'/0'/0' Native SegWit (P2WPKH, bc1q...)

Receive #0	bc1qgt7wkrnz232usu755nn3e7g0glu7tje74cq42w
Receive #1	bc1q9cd5r8uutpdxwc9g9x2f58qy66e02020rrkdf6
Receive #2	bc1q6n7vyae7c7ymsc3l27medxauyk5cr38sqjrtxl
Change #0	bc1q6t09tfa9zr9qkxcvyvf82avvfqmtrytgeyjgcm
Change #1	bc1qrvgtalhfe7rddtae9hrxmrrhlt099j4k07x23w
Change #2	bc1qx5uc6hac4mwnd2uaxl2te9h8gdvzulrny7l0mq

BIP44 m/44'/0'/0' Legacy (P2PKH, 1...)

Receive #0	182BqSSdwn1d4BpGjnhiLxUMdG6GZc3nTn
Receive #1	1MSavsVZs5yMfz9gP9SJRWM8ckfpV27LcX
Receive #2	17GxKTxzAnnhExAKCZrY7TVGS69QkMGtt1
Change #0	1DrAXQDs6GREcXbvaWnUPmHr7R5ndo315H
Change #1	15vLdfCvav2aThV1VCrB9ZxTB3dnNkowud
Change #2	1GGYxhPVPsmdDP82hqmFAwNd5A3UxgAPVk

BIP49 m/49'/0'/0' Nested SegWit (P2SH-P2WPKH, 3...)

Receive #0	35vYVdBPQ2XCfh1u1XGo6nRCZg1RVWQqWu
Receive #1	3G2EEq8aCRNWjBSJ9bJ9Fy9PCaREgsTejL
Receive #2	37Z3zAYoYJHuGFcK4cPWo2D9aj75cWUg3u
Change #0	3KJLWJyXCLJcZ8dCQmwoZYtqcCiwY43qya
Change #1	34UvDVeNnBo2fTXWCJujjpAhnc5b1xjzid
Change #2	3PGESLQocAuWf3CgMtmWJ7up83idABwjBL

BIP86 m/86'/0'/0' Taproot (P2TR, bc1p...)

Receive #0	bc1p9mvfaxkylnxjflv9udw9qlht9c24puwej8qlq3akg0rpu73eccesg5sxpt
Receive #1	bc1perxj5cyagd6gg68kgqd3k7pp4qkgakpqg377mme5p9mrqlakdkxs2xj2x2
Receive #2	bc1pc87mtuwc2zlkc7gk9gmantlr6fttqgaue75tl6uecgttc577tm2s57mqu6
Change #0	bc1pg7uz40yznhxpa2uahu77vm066whulk5g4vcev8u5sfmrqxwcsmpsdsqkc3
Change #1	bc1p2kzhgflgm99d8c0lun3f77yh7pc2gwxg6q7q67u728zmcq865qzsrkkmcs
Change #2	bc1pufzv2mv60f0968f7yu5npm30yues8yukjnqm3fv05r4hr89x3emshxcgwl

Bitcoin Witness. Verify, Attest, Inherit.

EXTENDED PUBLIC KEYS

zpub · BIP84, m/84'/0'/0'

```
zpub6qhgoKmWmN3JLGKQpsPx8cWqGtPUNG41jBciEyGyUohwuQFhWxwCaFUxs15a1oasowvUmMGPB8176fxgomAvNH
ogKYi5fitq98kawiQDvyn
```

xpub · BIP44, m/44'/0'/0'

```
xpub6C3iaws1AqizjXde5LsbUwhVPgKfc84NGXTcfhJ5DnRsYceSfSzPLby7MnWsQB8gxNVA2k5Pt5icZKENys4dTH
ifyhXFrGDzfqFip4NAp4M
```

ypub · BIP49, m/49'/0'/0'

```
ypub6XfeTDY6xYj9zTwH6QmAacAGY5MqwPDXpnemTPgpz68H66i5Hn4Ap9AnhPEf3QgLAoUXckr9RVBqzdkkZB1vYR
LJazyxPZz8vQvYKBggHM4
```

xpub · BIP86, m/86'/0'/0'

```
xpub6DLdFKeBhjghPHuf3WXbEgTp6x6bi8mmzpQFf7JfKfbQ81DShYYHis74wt5rbdjxFUxKQ2o7zkkQfi2VoUkqRq
EB6Z8r9WsQ5HPumjrFFBf
```

OUTPUT DESCRIPTORS · RECEIVE /0/*; CHANGE /1/*

BIP84

```
wpkh([02e8bff2/84h/0h/0h]xpub6C3ABzRgTzxLdfwBA9phiSKpvx6aV251txaGgBVCinxBoCdF1ec5L8AgpbAQ1
zH2zfgsGQ5GFoJ1L6jZNNLtmpSUasKEVuFrbgdJAYacaEp/0/*)#ga5rupx0
```

BIP44

```
pkh([02e8bff2/44h/0h/0h]xpub6C3iaws1AqizjXde5LsbUwhVPgKfc84NGXTcfhJ5DnRsYceSfSzPLby7MnWsQB
8gxNVA2k5Pt5icZKENys4dTHifyhXFrGDzfqFip4NAp4M/0/*)#drf9de0p
```

BIP49

```
sh(wpkh([02e8bff2/49h/0h/0h]xpub6CqP9YsBosBg9AkAG3yYNX4mN7DPzmE2ug8Yfznwc5kQ2ztr37tcC5WegB
H53W2QmAMisHFaxpqJ7M9BqUbukBehifHXofAeegrtvgTKwg8/0/*))#sv5q9ncl
```

BIP86

```
tr([02e8bff2/86h/0h/0h]xpub6DLdFKeBhjghPHuf3WXbEgTp6x6bi8mmzpQFf7JfKfbQ81DShYYHis74wt5rbdj
xFUxKQ2o7zkkQfi2VoUkqRqEB6Z8r9WsQ5HPumjrFFBf/0/*)#f4cerpqs
```

VERIFIED & DATED BY

WITNESS OR EXECUTOR

Bitcoin Witness. Verify, Attest, Inherit.

WARNINGS AND NOTES · THE RECORD'S OWN WORDS

> NOTE · any BIP39 passphrase you later apply to this child is a separate secret. BIP85 re-derivation reproduces only the child words, not that passphrase, so back it up separately.

> MASTER PASSPHRASE · (assumed empty: no master BIP39 passphrase applied)

> BIP85 INDEX · 0

> WORD COUNT · 12

Bitcoin Witness. Verify, Attest, Inherit.