BITCOIN WITNESS

Confidence Report

A Codex32 backup record

PROVENANCE VERIFICATION

CODEX32 BACKUP VERIFICATION

READ THIS FIRST

This is proof that a Codex32 (BIP-93) checksummed Shamir backup and its address derivations were independently checked on an offline device.

Important. It contains no shares and no secret material, and cannot move money. It is safe to store.

If you have inherited this, keep it with the sealed Codex32 shares or contact your estate attorney. Recovery needs the threshold number of shares, not this document.

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 12:49:32 UTC
BACKUP FORMAT	Codex32 (BIP-93) checksummed Shamir backup
SEED LENGTH	128-bit (16 bytes)
PASSPHRASE	No
MASTER FPR	3F3521A6
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 SHARES REQUIRED

1. Import an extended public key from the following pages into a watch-only wallet on its stated derivation path (Sparrow accepts every key form), or re-run Bitcoin Witness with the same seed.
2. Confirm Receive #0 matches the address shown here for that path.
3. Recompute the Report SHA-256 in the footer and confirm it matches — any change to the document changes the hash. If the document is independently GPG signed, verify that signature also. Re-verify on the appliance: menu → Verify File Integrity, or run 'python3 confidence_report.py --verify <this-file>' (prints OK).

Recovery path. Reassemble at least the threshold number of Codex32 shares (or decode the single unshared secret, if it was never split) on a Codex32-capable tool to recover the master seed identified 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	bc1q7uzj59wd9d67gft8kqstg3v5hmaa7hyl9r8h8a
Receive #1	bc1q8k4n9770x3s82c88uapdw3geacty6hhhnwht6q
Receive #2	bc1q38eu7p3gt0pyt2jgr5hyhvlnkyp7fghx0el8r3
Change #0	bc1q440s4qd5fvsmstnm6v23ec30e66pycm99k4xsl
Change #1	bc1q3kdq4ep4n0l3y0wmp4kfjqwrpzf6q6stlnnmd4
Change #2	bc1qaagql6lyfycp2tjqhthhga3yqsm7x88n22pa8c

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

Receive #0	1CNuaUyfrQ2SZgLH3XqnEfjEgcYqahmBVo
Receive #1	1LfNeGZTG6f659GsZEDddWvSEYtmiPFs5g
Receive #2	1LphA8av8cyX5SmDhsgP7ZnxfaJ5oqV1vu
Change #0	1CzfjiGc4Vkqo8DXrJX5GPtz3RtFUrZrQn
Change #1	1MBzHEFn1p5F6V3DrNuvR6GxUknF9qujVp
Change #2	1Cs9R1u94oFtGFDGLEiQLaU6iuabrkGBTX

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

Receive #0	3EUgDVX8TyfJ5XUkjBNjU6uxSFoyvP29cP
Receive #1	39ryLtX6x7FZ3Di67B7E4anroGeee6wrcF
Receive #2	3CHZpPNuua5snZrdMeVzmKCCud4C6SbR5B
Change #0	3CtjNUgazzNiRGquot225BoVT6q7XXUyLU
Change #1	3BaFmvk3sHaHiwoTk9FzoN34YRgQcEvjYX
Change #2	33j8PPzdiaXXoQAtJpHj7sp7xoqadn6ZV6

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

Receive #0	bc1padsq8nvjdwlmcuqz2zkymwrf6ch5v2cu4fgtu9krwv36j6h5073qxupm3r
Receive #1	bc1puvwu0hpdce3kw8e4lc8p4wdhphelq8ndcnx0wv5qd2vdhtla6c3sx9dr27
Receive #2	bc1px8ahj5zxzyx32ssj3yj3zl7f2cqmw357030tuj4wt5sgnj9hk2qqxmq9z9
Change #0	bc1pvrn60uq748v7yaxw36n6m43ht5rc9r688kfk0y4w27e66236cgssgr5gy4
Change #1	bc1pr9tp0lu0xagt4k3asnvrt0l5pfg40fzncgrtyn2d7xxx9xgh7d6qqad5lh
Change #2	bc1pp04p4ym4695yxwlxllfel4emue0jsl4jvcf3d9c0nz4h8rxy9pzqx5hg2y

Bitcoin Witness. Verify, Attest, Inherit.

EXTENDED PUBLIC KEYS

zpub · BIP84, m/84'/0'/0'

```
zpub6r3E7pmeTRE9gdigEuHqh1rBq18TxcG12fw2yTfjGLCP44aKb43vc36nN8x5LrAhUuY4Mka2DW5KFLzkyvExfpJhbURzz6imNgoTd1Lxt2z
```

xpub · BIP44, m/44'/0'/0'

```
xpub6CeZ5XxHp6rXSwi2GCi7UT25rswWQtoPvj36MbzRBr3QEoEmBFNGgnMy329ZMkfjRKBZHtKKpYfpkrPWohTjHZZn7y1NR9EHnojaGLKdMAR
```

ypub · BIP49, m/49'/0'/0'

```
ypub6XyonJJAgauoGDZyHWD2uE19tS4jss2vukCgtJM8EiUvZZbR4yjmpLMbVvLmTt9ENXXteWBSgRYq7QWVknZbVmKE4iXims5K9NyGSHtSVsh
```

xpub · BIP86, m/86'/0'/0'

```
xpub6C5pT77VWNhWvrB3TqSEbpm7NCpMYEzbJreYbB68RCUoAMkT7rdhafinmdKL4M5275TyDqNAWCnssYnDNaPoXMiAg3sWvCgAiYqY8dHk1k4
```

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

BIP84

```
wpkh([3f3521a6/84h/0h/0h]xpub6CNhWVRpA49Bz3LSaBibGqfBV4qa5NH1CStbQfsxWKScwrws5jioMunWKj2uM2rrfdJSroNuJBNDUmmdYXQw5LwVro39pH5nqEgAqrzTPyc/0/*)#qtaver0u
```

BIP44

```
pkh([3f3521a6/44h/0h/0h]xpub6CeZ5XxHp6rXSwi2GCi7UT25rswWQtoPvj36MbzRBr3QEoEmBFNGgnMy329ZMkfjRKBZHtKKpYfpkrPWohTjHZZn7y1NR9EHnojaGLKdMAR/0/*)#5vm2rpnp
```

BIP49

```
sh(wpkh([3f3521a6/49h/0h/0h]xpub6D9YUddFXuNKQvNrT9RQh8ueiTvHwF3RzdgU6uTEri73WTnBpKaDCGhTUiPBTyVJxtR5u2atDmCHE7tw369ahXddCNqJBxFpseud3j7pjX8/0/*))#wyucfucx
```

BIP86

```
tr([3f3521a6/86h/0h/0h]xpub6C5pT77VWNhWvrB3TqSEbpm7NCpMYEzbJreYbB68RCUoAMkT7rdhafinmdKL4M5275TyDqNAWCnssYnDNaPoXMiAg3sWvCgAiYqY8dHk1k4/0/*)#5xg6uvfv
```

VERIFIED & DATED BY

WITNESS OR EXECUTOR

Bitcoin Witness. Verify, Attest, Inherit.

WARNINGS AND NOTES · THE RECORD'S OWN WORDS

> NOTE · the recovered secret is a BIP32 seed: feed it DIRECTLY to the wallet (do not run it through the BIP39 passphrase / seed-stretching step).

Bitcoin Witness. Verify, Attest, Inherit.