BITCOIN WITNESS

Confidence Report

A Shamir backup record

PROVENANCE VERIFICATION

SLIP-39 BACKUP VERIFICATION

READ THIS FIRST

This is proof that a SLIP-39 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 SLIP-39 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 12:49:29 UTC
BACKUP FORMAT	SLIP-39 Shamir backup
SEED LENGTH	256-bit (32 bytes)
PASSPHRASE	No
MASTER FPR	9C121355
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. Recombine at least the threshold number of SLIP-39 shares on a SLIP-39-capable signer (Trezor / Keystone / this appliance) 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	bc1q3nqaaxmxp7ewkndlma066sq5kvunwl0ggcwyut
Receive #1	bc1q6erk3jrsvlwrwv3t7xy53qmkepuk2q0svtmfjj
Receive #2	bc1qan9c7dchc75x3wmtdc5ffzea0lyne56hjpxf3q
Change #0	bc1qxgv4c334vcmyepcu9v6k6wk7ag533em26cf0fe
Change #1	bc1qftd5uk03lm5f687a33vnd7jpsp0vpecl8ls6lc
Change #2	bc1q6g84mj3ad0vrp4gvhvzhx5jvsjxgasd6utu7c9

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

Receive #0	1MyFfopF44URaxZMTV5rWRCJUx6De1571G
Receive #1	1JBbKrvCjmVTXfz8kT5EvphpGqQ3AeHPGy
Receive #2	1HdB8BttUgMh3aHaePqNgk8NXWTAtM5VFv
Change #0	1Gyzuy37x2B9jADvEmRFivCcbxCZKGMrQq
Change #1	1B7X7F3ERm1pXj94G31fMJ9Hg5zR1AN5XJ
Change #2	17iMYvjkDA5CZpbGYdAaSPMmoLwgeAhpLG

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

Receive #0	3G3HrQ7DrNJLm8gMrLHTeeD5DdzgeoScRJ
Receive #1	3HgGV4fhXz8GZYVMRT1tj9WoUdMQMDrGvw
Receive #2	3Ktkg2Zkiba5GstBXb5BeRQMnAegS4Z74m
Change #0	3BdrAbZCo9BCmzP1nmpEVyGXMB9JF4MJ1L
Change #1	3GFSjHbSRGZZavmY7YTm9UJfDbmJdpCeMA
Change #2	3EygwPaHDMAmYZBEodwjMedJjh39y8X7xC

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

Receive #0	bc1prg26pl2atv2q0g5yty2jrcjpx79j7u5p8afh48m9ge4lat5szhuqhtd0ps
Receive #1	bc1pld0uzdfwxudqrky2p5stch0w78leqhtnmpfdrg6xacu49vyp9h3s9n9hh0
Receive #2	bc1pqfthg3mr9pku4na6acz67hcznk9tlpc7ar5dd9khftttpg4rr2vq45wq9z
Change #0	bc1p4jxf8zs0kc95cuvfxnvkh73pmgej6k7ylw2m7nf35pvzgnkc9xgq9l95c9
Change #1	bc1ph09swm5rtmhf29un0lrkz0vh92l2ealyjv9etvvypd42ujdgd36sqtafs6
Change #2	bc1pztvranzkeel89ymdnqv8g8as93qcg539vhzqh6j02lttk3pstp5quaj37c

Bitcoin Witness. Verify, Attest, Inherit.

EXTENDED PUBLIC KEYS

zpub · BIP84, m/84'/0'/0'

```
zpub6qVekdL37kqSi7rE38MzChBkZkFpWu2ksGDurmw93epWBxBie5UVWC1v3uPEDjQGvEqvt4G67NbuPx511ca5MqLSdMSDcknc8rUB3FKHWEY
```

xpub · BIP44, m/44'/0'/0'

```
xpub6C1MWRF7pThTTdibR74ynf4VfqpmkFmq6Ne2Tj7u5aBavsaf1qbtEn5rPLBgo54KVLi2WoppCn21X2xddoSBKrNWVbS1fdVKuSVgYrgdHeP
```

ypub · BIP49, m/49'/0'/0'

```
ypub6X9R2VHhtMJ9WnEQLtPV3MhycNZBru5NYLGMEXwUwG1X1EvgLGhwYWEMJNwEDbNsK5GtzB5kD4mje51wcn69xjADc6UE8f8W6Tw9CP3Aitw
```

xpub · BIP86, m/86'/0'/0'

```
xpub6C9dF6ZKmy9LsHZdhy39FN4BLvfWySfHosSQpb3x6kHULzzV2UsTUPvecJHJ1QYrgWVX5gsBxzRN5EQhQohAzBAsdHavnjNAAYVvRhEb8BL
```

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

BIP84

```
wpkh([9c121355/84h/0h/0h]xpub6Bq89HzCpPkV1XTzNQnjnWzkDoxvdf3m33BUHz9NHe4k5kZG8m9NG4he1VU4Dv6S6xcKP74yC3todNqsaDk3mMyEtg3NSw9dbQLtG6GENzg/0/*)#67reqfhq
```

BIP44

```
pkh([9c121355/44h/0h/0h]xpub6C1MWRF7pThTTdibR74ynf4VfqpmkFmq6Ne2Tj7u5aBavsaf1qbtEn5rPLBgo54KVLi2WoppCn21X2xddoSBKrNWVbS1fdVKuSVgYrgdHeP/0/*)#4uu306d0
```

BIP49

```
sh(wpkh([9c121355/49h/0h/0h]xpub6CK9ipcnjfkffV3HWXbrqGcUSQQjvH5sdDk8T93bZFddx97T5cYNvSaDHAyeDgiwuSA6EhVBkQRBknQNu5g9AVUcjkmoYkK1pjsVon7x1Ac/0/*))#5fl0wcku
```

BIP86

```
tr([9c121355/86h/0h/0h]xpub6C9dF6ZKmy9LsHZdhy39FN4BLvfWySfHosSQpb3x6kHULzzV2UsTUPvecJHJ1QYrgWVX5gsBxzRN5EQhQohAzBAsdHavnjNAAYVvRhEb8BL/0/*)#hxvy5nmy
```

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.