BITCOIN WITNESS

Confidence Report

An on-device generation record

PROVENANCE VERIFICATION

SEED GENERATION

READ THIS FIRST

This records a Bitcoin seed generated on an offline device, with the address derivations it produces and a measured estimate of its randomness.

Important. It does not contain the seed words and cannot move money. It is safe to store.

Read the seed-entropy line before funding: a weak estimate means the seed is predictable and must not hold real value.

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 12:49:25 UTC
BACKUP FORMAT	BIP39 seed phrase (12 words)
SEED LENGTH	12 words
LANGUAGE	English
SEED ENTROPY	~0 of 128 bits (WEAK)
PASSPHRASE	No
MASTER FPR	3F635A63
NETWORK	Bitcoin mainnet
AIR-GAP	VERIFIED
VERSION	v1.0
SEED PATTERN	all symbols identical, a long repeated run, highly repetitive

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 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. Re-enter this seed phrase on a Bitcoin Witness appliance (or any BIP39-compatible wallet) to spend.

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	bc1qk0a9hr7wjfxeenz9nwenw9flhq0tmsf6vsgnn2
Receive #1	bc1qkd33yck74lg0kaq4tdcmu3hk4yruhjayxpe9ug
Receive #2	bc1qvr7e5aytd0hpmtaz2d443k364hprvqpm3lxr8w
Change #0	bc1q3pgnz3gszmccgxlrygmp086w8j5rkhynx7cckt
Change #1	bc1q3ws8shjjmwx8y9p2hq8rw3lphfj4mukgqxwjfr
Change #2	bc1qekq6vth07lx9dmshgaln4jjamyt0xx0gygytj5

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

Receive #0	1EjnS13zBgN6tUgy6U64qFeh53fyAeUsqE
Receive #1	15zqaY9cc57p9NaiWBjrFBm8TfXqMVo5Dj
Receive #2	1Q2KXT1i6fez5LpLNmDKPTZhPMpwD4hNDb
Change #0	1M7kDNYZ1pNM3pB8YCBBbvyQoQGReSB6XQ
Change #1	1CK6Nb7MkZ9ibNw6Uc6FVxrA4Swt3RHo1H
Change #2	1HtF9wHpS8sW57icbBhWFiikSkpnhXrzfh

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

Receive #0	3CfyLSjYFFV6MUAMh3auTK9kfpPscPCHth
Receive #1	31nD3MEioUDchu7bVaHUCdCa4vxxsqDYwu
Receive #2	32pqj8rgW1BdXK2Cygwn2JVYPnVRknfTE4
Change #0	3HBUdaW5PBJydoMWESpd7F1dbGzyUxb1D9
Change #1	3L5d9FqsxEMUZ7dAjPnawsMdCoKherC1EJ
Change #2	3PBzQzJnbyfXSZV1cwduhW2QkDhphyis1C

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

Receive #0	bc1p7hycyt2u4m90sm8fnchmuupwn40l6qmm42f3eqj5m30yyw6g4w2sxjyytr
Receive #1	bc1p538vprsd0rgfgzev5a4yxhgwe3hsqjkgcuq5vvza3uj737sfq6tqxlh8yc
Receive #2	bc1pe0a8jqwu928l0td3ec8gdz6xwhscjkwn39quswf6dun82azdykms5ujh4w
Change #0	bc1pu0zfg0q9arc0atzgurt3nlt6fzturjqp30jzkqanyh2q49p8khaqfp49m3
Change #1	bc1pfhamnyex4pwtd5vxpyr222apxr4ffr07mwhxjl9lkpr7gu8mahqqjlru95
Change #2	bc1pghgx8asrfrqm2qcfm2a57jxjecqzxulr7000wqlnt2mysvl0af2qnlkg7h

Bitcoin Witness. Verify, Attest, Inherit.

EXTENDED PUBLIC KEYS

zpub · BIP84, m/84'/0'/0'

```
zpub6rD5AGSXPTDMSnpmczjENMT3NvVF7q5MySww6uxitUsBYgkZLeBywrcwUWhW5YkeY2aS7xc45APPgfA6s6wWfG
2gnfABq6TDz9zqeMu2JCY
```

xpub · BIP44, m/44'/0'/0'

```
xpub6CfuVE8s2cAQijg7nqYKFoEu7AqkAfMNNMufV7utCmDjMjQZwM9RtN9PHxvBK4gkLWRyu8Xs6jh4TwRz8EYiFj
Wb8bxDMynAwyHZFxwzvkZ
```

ypub · BIP49, m/49'/0'/0'

```
ypub6XcubJFujNWud4hRW4oVs1P7kVUcPPYfw51p2rpM3FZfi77ATR9wQ7Cu9yxtFsKHFNTvLbd2MxS4CLtC1YXvCq
zbYnfDceSGDqUM33t2bAn
```

xpub · BIP86, m/86'/0'/0'

```
xpub6BjYQbzfdeKfrrP2B9uV4tZvUk7iHz5t8aGqgfMecXjnUi5iCohqsLvPAHPPaBBdwptNE4ETcfSnGfDgBJEJ4d
7gMEosnJQGdqp4BSXB8oy
```

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

BIP84

```
wpkh([3f635a63/84h/0h/0h]xpub6CYYYw6h668PkCSXxH9yxBG32zCMEb6N9DuVY8Ax8U7RSV86qKrrhjJfS6nL5
jSoikLpd1Qw9qgHv5vyRi7V4nfV3ymLfGpFShsYsFmQiT8/0/*)#9m66mdj4
```

BIP44

```
pkh([3f635a63/44h/0h/0h]xpub6CfuVE8s2cAQijg7nqYKFoEu7AqkAfMNNMufV7utCmDjMjQZwM9RtN9PHxvBK4
gkLWRyu8Xs6jh4TwRz8EYiFjWb8bxDMynAwyHZFxwzvkZ/0/*)#grjv3f3c
```

BIP49

```
sh(wpkh([3f635a63/49h/0h/0h]xpub6CneHdazagyRmmWJfi1sevHcaXLASmZB1xVbFTvTfFBnf1HwCkzNn3Ym8n
1JFxfMqjM7b82TuJ5WK4GdHr7uQcJzgSxo2jcmx7QheVtjHEC/0/*))#7m9dkcfn
```

BIP86

```
tr([3f635a63/86h/0h/0h]xpub6BjYQbzfdeKfrrP2B9uV4tZvUk7iHz5t8aGqgfMecXjnUi5iCohqsLvPAHPPaBB
dwptNE4ETcfSnGfDgBJEJ4d7gMEosnJQGdqp4BSXB8oy/0/*)#0a7zusl8
```

VERIFIED & DATED BY

WITNESS OR EXECUTOR

Bitcoin Witness. Verify, Attest, Inherit.

WARNINGS AND NOTES · THE RECORD'S OWN WORDS

> ENTROPY SOURCE · from 128 coin flips
>
> Assumes the throws were fair and independent. This device checked the numbers the user entered, not the throws behind them.

> PATTERN · (normal for test vectors; weak for a real wallet)