BITCOIN WITNESS

Confidence Report

A multisig policy record

PROVENANCE VERIFICATION

MULTISIG VERIFICATION

READ THIS FIRST

This is proof that a multisig wallet policy, its cosigner keys and address derivations were independently checked on an offline device.

Important. It contains no private keys and cannot move money. It is safe to store and to share with cosigners.

What this is for: the wallet policy (the signing rule, e.g. 2-of-3, plus the cosigner keys and the descriptor). Spending needs this descriptor plus signatures from the threshold number of cosigners, whose keys are held separately and are not in this package.

Privacy. The extended public keys, addresses, and descriptor below cannot spend, but they reveal every past transaction and every future address of this wallet to anyone who holds them, and the descriptor also reveals the quorum, the number of cosigners, and that these keys form one wallet. 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 12:49:26 UTC
POLICY	2-of-3 P2WSH [sortedmulti (BIP67)]
IMPORTED VIA	Output descriptor (BIP380)
DESCRIPTOR #	#arzs0zeh
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. Re-import the full descriptor (with its #checksum) and all cosigner keys from the following pages into Sparrow / Bitcoin Core / Specter.
2. Confirm Receive #0 matches the address shown here, and that every cosigner is present in the same policy.
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. Spending needs this descriptor plus signatures from the threshold number of cosigners. The restore instructions, with the wallet-specific descriptor form, are printed with the derivation results.

Bitcoin Witness. Verify, Attest, Inherit.

APPENDIX — TECHNICAL RECORD

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

DERIVATION RESULTS

2-of-3 P2WSH multisig

Receive #0	bc1q40554ue6za9jxt9el2p29gvt73yzqskzcr6at2ywp953wasvrdcs34m8a0
Receive #1	bc1q87w6nsgz8hcl8ak2snvsg5h82k3p9ktru9ahkvggkktqkpqqrdeqntyqqr
Receive #2	bc1qwjl6t576ul2wmj53fsqq37dljmca9wcm2ysnduq2thvcp936ej0s9tn2hm
Change #0	bc1qm8uzztwlr78rlpyzuk3j7mhquy4a0uhe0ha5gh3lu63velmkn8cs2gf8ka
Change #1	bc1qzz30gmsz9yshaxvd0hvgt3jjcr9yes4d6zdnjmwfygnc5ymev26s2g60eg
Change #2	bc1qrty8zpmf543jncr67udd37y0f2eh8nnz3d28yun30znqs97qszys3f78xd

> To restore this watch-only wallet: import the descriptor below into Sparrow (which accepts SLIP-132 and multi-path descriptors); for Bitcoin Core / Specter / Ledger use the CANONICAL (plain-xpub) form when shown. Every cosigner must be present and in the same policy.

Bitcoin Witness. Verify, Attest, Inherit.

COSIGNERS · FINGERPRINTS AND KEYS ARE CLAIMED BY THE DESCRIPTOR — CONFIRM OUT-OF-BAND

#1 · master fp 73c5da0a (xpub) · origin (claimed) m/48h/0h/0h/2h THIS DEVICE

```
xpub6DkFAXWQ2dHxq2vatrt9qyA3bXYU4ToWQwCHbf5XB2mSTexcHZCeKS1VZYcPoBd5X8yVcbXFHJR9R8UCVpt82VX1VhR28mCyxUFL4r6KFrf
```

#2 · master fp 3f635a63 (xpub) · origin (claimed) m/48h/0h/0h/2h

```
xpub6FHZCoNb3tg3o1GAJQxSwgFNF8mLRtTk2GgkF7n5rwzoxBhUEdFWa8cyZRHqytAzKZWsKz8627cQEMCCfR5GDSv6yXegqirpgDUX41Pxybr
```

#3 · master fp 5436d724 (xpub) · origin (claimed) m/48h/0h/0h/2h

```
xpub6E79FaRWLSJCAgA2jDHRvyrWKwT6aSmR685zptzyYPvmUd44omcxZ1NAzDtbdFBvEADjcVbV4NzTDwQeU6oiSV9KGiMSWhjANZjbfUHkm3Y
```

Descriptor checksum · #arzs0zeh (VALID) (a multisig wallet has no single master fingerprint; the BIP380 descriptor checksum is the wallet's fingerprint.)

FULL DESCRIPTOR · as entered; its #checksum matches this descriptor

Confirm this WHOLE string (keys, order, threshold, #checksum) with every cosigner through a separate channel before funding:

```
wsh(sortedmulti(2,
[73c5da0a/48h/0h/0h/2h]xpub6DkFAXWQ2dHxq2vatrt9qyA3bXYU4ToWQwCHbf5XB2mSTexcHZCeKS1VZYcPoBd5X8yVcbXFHJR9R8UCVpt82VX1VhR28mCyxUFL4r6KFrf/0/*,
[3f635a63/48h/0h/0h/2h]xpub6FHZCoNb3tg3o1GAJQxSwgFNF8mLRtTk2GgkF7n5rwzoxBhUEdFWa8cyZRHqytAzKZWsKz8627cQEMCCfR5GDSv6yXegqirpgDUX41Pxybr/0/*,
[5436d724/48h/0h/0h/2h]xpub6E79FaRWLSJCAgA2jDHRvyrWKwT6aSmR685zptzyYPvmUd44omcxZ1NAzDtbdFBvEADjcVbV4NzTDwQeU6oiSV9KGiMSWhjANZjbfUHkm3Y/0/*))#arzs0zeh
```

VERIFIED & DATED BY

WITNESS OR EXECUTOR

Bitcoin Witness. Verify, Attest, Inherit.

WARNINGS AND NOTES · THE RECORD'S OWN WORDS

> COSIGNER FP · 'master fp' is CLAIMED by the descriptor and is unverified: it is the value the cosigner's own wallet shows, and this appliance cannot recompute it. Confirm it with the cosigner.

> DESCRIPTOR · a swapped cosigner key also derives clean-looking addresses. Confirm the WHOLE descriptor (keys, order, threshold, #checksum) through a separate trusted channel such as a phone call or in person.

Bitcoin Witness. Verify, Attest, Inherit.