BITCOIN WITNESS

Confidence Report

A watch-only account record

PROVENANCE VERIFICATION

EXTENDED PUBLIC KEY VERIFICATION

READ THIS FIRST

This records an extended public key read on an offline device.

Important. It holds no seed and cannot spend.

What this is for: this key alone does not say which script template its wallet uses, so this report shows four candidates and resolves none. Resolve the template first, then import the matching complete public descriptor to watch that account. Nothing here can spend.

Privacy. The extended public keys and addresses above 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

ACCOUNT KEY FPR	6CC9F252
PARENT FPR	155BCA59
KEY FORM	xpub
SCRIPT TYPE	Unresolved · 4 shown
NETWORK	Bitcoin mainnet
AIR-GAP	VERIFIED
CHECKED	2026-08-05 12:50:11 UTC

PREPARED FOR & BY

VERIFIED BY

PREPARED FOR

REVIEWED BY

DATE

HOW TO RE-VERIFY

None of these steps needs a network or an address lookup.

1. Best: use the public output descriptor your wallet exported. It states the script policy outright. Bitcoin Core prints descriptors with 'listdescriptors'. Its 'private' option defaults to false, which is the public form you want.
2. If no descriptor is available: on an air-gapped verifier that holds the seed, derive the candidate parent for each template above. Compare its fingerprint with this key's Parent Fingerprint, then derive the account child number recorded in this key and confirm that the resulting extended public key equals the one in this report. A match identifies a tested standard template for this account. It does not prove that no nonstandard path exists.
3. After the policy is resolved, import the matching pair of complete descriptors into a watch-only wallet that supports their script type, and confirm its Receive #0 matches the address shown here.
4. Recompute this report's SHA-256 and confirm it matches. This confirms that the report body has not changed since the hash was made. By itself, it does not identify who made the report or establish the key's path, policy, history, or balance. Re-verify on the appliance: menu -> Verify File Integrity, or run 'python3 confidence_report.py --verify <this-file>' (prints OK).

Bitcoin Witness. Verify, Attest, Inherit.

EXTENDED PUBLIC KEY

xpub (as supplied)

```
xpub6BosfCnifzxcFwrSzQiqu2DBVTshkCXacvNsWGYJVVhhawA7d4R5WSWGFNbi8Aw6ZRc1brxMyWMzG3DSSSSoek
kudhUd9yLb6qx39T9nMdj
```

WHAT THIS KEY SETTLES · THE RECORD'S OWN WORDS

This key does not record its script type, so four standard templates are shown. For a conventional single-sig wallet, one template will usually be the policy the wallet watches. An xpub alone cannot prove which one.

Each heading names a template and the standard path for that template, with the account number read from this key. None of them is a claim about this key's original derivation path. A wallet can deliberately use the same key material under more than one policy.

A multi-signature cosigner key can look exactly like this one. If that is what you pasted, none of the four templates applies and its addresses depend on the other cosigners. Verify it under Verify Extended Public Key, multisig mode, with your complete descriptor or cosigner file.

> Scope · this four-template view is intended for conventional single-key accounts. It does not determine multisig policy, nonstandard derivation paths, other script types beyond the four shown, account discovery, or the original wallet's gap limit. It covers this key's receive (/0/i) and change (/1/i) chains only, for the addresses shown. Other account numbers are not covered.

> Before using an address · do not hand one out as a receiving address until you have resolved the template. If these came from your own single-key account xpub and you hold the matching private keys, the coins at them remain spendable. Your current wallet may not discover them automatically, and a hardware signer may refuse to sign for an address whose script type or path does not match the policy it was set up with.

Bitcoin Witness. Verify, Attest, Inherit.

Native SegWit (P2WPKH)

BIP84 · m/84'/0'/0'

Receive #0	bc1qmxrw6qdh5g3ztfcwm0et5l8mvws4eva24kmp8m
Receive #1	bc1qdtsnq885fjjj2agaza36cnl0ztg32wvxqg5x0c
Receive #2	bc1qmansqj24utny54uag2ped8censfwnszplhg27m
Change #0	bc1qht5nernlk6pyytfy0q935y492rhlg28jhggde9
Change #1	bc1qyqrp7k29mppkq8s9x2y0u0t0sl3kz2w4sle8q4
Change #2	bc1qmwf4e47geyl564j258jpd3q2wteyldscpvldaq

COMPLETE DESCRIPTORS FOR THIS TEMPLATE

Import the pair, not one line. Each carries its own #checksum over its own text, so a receive descriptor cannot be edited into a change descriptor and keep its sum.

NATIVE SEGWIT RECEIVE #p54wed40

```
wpkh(xpub6BosfCnifzxcFwrSzQiqu2DBVTshkCXacvNsWGYJVVhhawA7d4R5WSWGFNbi8Aw6ZRc1brxMyWMzG3DSSSSoek
kudhUd9yLb6qx39T9nMdj/0/*)#p54wed40
```

NATIVE SEGWIT CHANGE #sqs0yc9h

```
wpkh(xpub6BosfCnifzxcFwrSzQiqu2DBVTshkCXacvNsWGYJVVhhawA7d4R5WSWGFNbi8Aw6ZRc1brxMyWMzG3DSSSSoek
kudhUd9yLb6qx39T9nMdj/1/*)#sqs0yc9h
```

VERIFIED & DATED BY

WITNESS OR EXECUTOR

Bitcoin Witness. Verify, Attest, Inherit.

Legacy (P2PKH)

BIP44 · m/44'/0'/0'

Receive #0	1LqBGSKuX5yYUonjxT5qGfpUsXKYYWeabA
Receive #1	1Ak8PffB2meyfYnbXZR9EGfLfFZVpzJvQP
Receive #2	1MNF5RSaabFwcbtJirJwKnDytsXXEsVsNb
Change #0	1J3J6EvPrv8q6AC3VCjWV45Uf3nssNMRtH
Change #1	13vKxXzHXXd8HquAYdpkJoi9ULVXUgfpS5
Change #2	1M21Wx1nGrHMPaz52N2En7c624nzL4MYTk

COMPLETE DESCRIPTORS FOR THIS TEMPLATE

Import the pair, not one line. Each carries its own #checksum over its own text, so a receive descriptor cannot be edited into a change descriptor and keep its sum.

LEGACY RECEIVE #t3qu2qap

```
pkh(xpub6BosfCnifzxcFwrSzQiqu2DBVTshkCXacvNsWGYJVVhhawA7d4R5WSWGFNbi8Aw6ZRc1brxMyWMzG3DSSSSoekkudhUd9yLb6qx39T9nMdj/0/*)#t3qu2qap
```

LEGACY CHANGE #699ah4de

```
pkh(xpub6BosfCnifzxcFwrSzQiqu2DBVTshkCXacvNsWGYJVVhhawA7d4R5WSWGFNbi8Aw6ZRc1brxMyWMzG3DSSSSoekkudhUd9yLb6qx39T9nMdj/1/*)#699ah4de
```

VERIFIED & DATED BY

WITNESS OR EXECUTOR

Bitcoin Witness. Verify, Attest, Inherit.

Nested SegWit (P2SH-P2WPKH)

BIP49 · m/49'/0'/0'

Receive #0	3HkzTaFbEMWeJPLyNCNhPyGfZsVLDwdD3G
Receive #1	3FYpNH4eWWmqqrvcbjWpvSJYybEaGmCwZi
Receive #2	3Qnpgq3UEaRRqXNmMBJZCDmVmCHQUmshaF
Change #0	36NJG8MkpBmKgVtA6L6W84EJYgakGMFKrF
Change #1	3Dym98YyPWgkspSGhSFBYq4r1BfqZRMK3J
Change #2	3FjPxhz4t2ARYRJ1DG9w2VNY7kNN2BG3WH

COMPLETE DESCRIPTORS FOR THIS TEMPLATE

Import the pair, not one line. Each carries its own #checksum over its own text, so a receive descriptor cannot be edited into a change descriptor and keep its sum.

NESTED SEGWIT RECEIVE #qj2n09pq

```
sh(wpkh(xpub6BosfCnifzxcFwrSzQiqu2DBVTshkCXacvNsWGYJVVhhawA7d4R5WSWGFNbi8Aw6ZRc1brxMyWMzG3DSSSSoekkudhUd9yLb6qx39T9nMdj/0/*))#qj2n09pq
```

NESTED SEGWIT CHANGE #x3zk5g25

```
sh(wpkh(xpub6BosfCnifzxcFwrSzQiqu2DBVTshkCXacvNsWGYJVVhhawA7d4R5WSWGFNbi8Aw6ZRc1brxMyWMzG3DSSSSoekkudhUd9yLb6qx39T9nMdj/1/*))#x3zk5g25
```

VERIFIED & DATED BY

WITNESS OR EXECUTOR

Bitcoin Witness. Verify, Attest, Inherit.

Taproot (P2TR)

BIP86 · m/86'/0'/0'

Receive #0	bc1plguuppjuw5uk2rpyjnnzvwsuvy5ctswns9fsvhrvn4qt04ns4nmscf9eqf
Receive #1	bc1p03dpkjmygsql7hzjdzjndkh25rfrnqmhc7skd9vl665ukydyv3hq79e4za
Receive #2	bc1pwtd9c04vlkkuhr92d74pkjmr4ven7dl49n0vfpj6hmj0j2v988fsu7dgx0
Change #0	bc1p0ru6ym5zwtpvwhp2u8wqm4tjvaavler670wyhrly33fh08ph2qlqmvgjpk
Change #1	bc1pmpssmtjec5708kwupczxwjhqx66shy7qzwdv4t93nrzy6grvttvsaqatvh
Change #2	bc1pmkvz9gs2uukv88ufah582sjplfwadpa0xp9zypq9rae3rcjgn3lqjp0dr9

COMPLETE DESCRIPTORS FOR THIS TEMPLATE

Import the pair, not one line. Each carries its own #checksum over its own text, so a receive descriptor cannot be edited into a change descriptor and keep its sum.

TAPROOT RECEIVE #d3k2meqx

```
tr(xpub6BosfCnifzxcFwrSzQiqu2DBVTshkCXacvNsWGYJVVhhawA7d4R5WSWGFNbi8Aw6ZRc1brxMyWMzG3DSSSSoekkudhUd9yLb6qx39T9nMdj/0/*)#d3k2meqx
```

TAPROOT CHANGE #u9ntxvs7

```
tr(xpub6BosfCnifzxcFwrSzQiqu2DBVTshkCXacvNsWGYJVVhhawA7d4R5WSWGFNbi8Aw6ZRc1brxMyWMzG3DSSSSoekkudhUd9yLb6qx39T9nMdj/1/*)#u9ntxvs7
```

VERIFIED & DATED BY

WITNESS OR EXECUTOR

Bitcoin Witness. Verify, Attest, Inherit.