BITCOIN WITNESS

Backup & Inheritance

An heir & estate record

BACKUP ASSEMBLY

SECRET-FREE · ASSEMBLED & VERIFIED 2026-08-05

READ THIS FIRST

If you are holding this, someone arranged their Bitcoin so that you would not have to take its existence on faith. This folder was produced by a Bitcoin Witness appliance for an heir or estate attorney. It holds only secret-free material: one or more watch-only Confidence Reports, an optional encrypted share-holder map, and a MANIFEST.sha256.

The seed and backup shares are not here. Nothing here can move the coins. It shows the wallet exists and was checked — a backup convenience, not a security upgrade over multisig.

This cover is a summary. Every claim on it is stated in full in INSTRUCTIONS.txt and PACKAGE-INFO.txt in this folder. Where they differ, the files govern.

WHAT IS ENCLOSED

REPORTS	7
REPORT FILES	14 (.txt + .pdf)
SHARE-HOLDER MAP	Present, encrypted
SIGNATURE	Signed

WHAT IT CAN AND CANNOT DO

SEE BALANCES	Yes, watch-only
MOVE COINS	No
SEED OR SHARES INSIDE	None
BACKUP SCHEMES	BIP39 · SLIP-39 · Codex32

WHAT TO DO WITH THIS PACKAGE

- **Today.** Run the two folder checks on page 3, then import every extended public key the reports list, not just the first, into a watch-only wallet to see the balance (step 1). No secret is needed for any of this.
- **Later.** When it is time to move the coins, gather the shares held elsewhere, follow each report's Recovery path, and restore the wallet (step 2).
- **Where to keep it.** Keep this package with the will. Treat it as financially sensitive: it reveals balances and addresses, though it can never spend. The share-holder map, which names people, is encrypted.

PREPARED FOR & BY

WALLET OWNER

PREPARED FOR

PREPARED BY, DATE

REVIEWED BY, DATE

DATE HANDED OVER

Bitcoin Witness. Verify, Attest, Inherit.

TO USE THE PACKAGE, ONCE THE PAGE 3 CHECKS PASS

1 **See the funds (no seed required)**

Import every extended public key the Confidence Reports list, not just the first.

A wallet holds funds under several address types, and importing only one can show a zero balance while the others hold the funds. Sparrow accepts every key form; Bitcoin Core needs the output descriptor each report prints, not the key itself; Electrum has no Taproot.

2 **To recover (spend)**

Follow the "Recovery path:" line in each Confidence Report

Each report that verifies a seed backup names the scheme and the procedure, for example reassemble the number of SLIP-39 or Codex32 shares the report names. Collect the shares that were distributed separately, reassemble per that line, and restore using the wallet and procedure that "Recovery path:" line names — it is not always a BIP39 wallet, since an Electrum, SLIP-39 or Codex32 backup restores differently. Not every report is a backup. An xpub, Multisig or Message report carries a "What this is for:" line instead, because those cannot recover or spend on their own.

3 **Share-holder map (if present)**

Decrypt share-holder-map.gpg with the passphrase the operator gave you separately. INSTRUCTIONS.txt has the command.

It is metadata only (who holds which share). Encrypted because it names people. Decrypt with the passphrase the operator gave you separately.

STANDARDS VERIFIED AGAINST

BIP32 · BIP39 · BIP48 · BIP67 · BIP-93 · BIP137 · BIP322 · BIP380 · SLIP-132 · SLIP39

PRIVACY

This folder contains extended public keys. An extended public key reveals every past transaction and every future address of that account, though it cannot spend. Treat this folder as financially sensitive and share it only with people you intend to have that visibility.

Bitcoin Witness. Verify, Attest, Inherit.

IN THIS PACKAGE

Rows 1 to 7 are the Confidence Reports, one per check, each shipping a .txt and a matching .pdf. A dash means the file is not listed in MANIFEST.sha256.

#	FILE	WALLET	WHAT IT IS
1	Seed Verification	73C5DA0A	a seed checked against its own addresses
2	Seed Generation	3F635A63	a seed generated on the appliance
3	SLIP-39 Backup	9C121355	a share backup of its own wallet
4	Codex32 Backup	3F3521A6	a second share backup, its own wallet
5	Extended Public Key Verification	FD13AAC9	row 1's BIP84 account key, watch-only
6	Multisig Verification	ARZS0ZEH	watch-only, cannot recover alone
7	Message Verification	NOFP	a signed statement, not a backup
8	INSTRUCTIONS.txt		how to read this package, .txt + matching .pdf
9	PACKAGE-INFO.txt		what this is and is not, plus the standards checked
10	share-holder-map.gpg		who holds which share, encrypted (it names people)
–	MANIFEST.sha256		sha256 of every listed file; not itself listed
–	MANIFEST.sha256.asc		signature file for the manifest, if signed; not itself listed
–	SIGNING-KEY.pub.asc		the signing key, if enclosed; not itself listed

BEFORE YOU TRUST ANY INCLUDED FILE

Check the folder **twice**: once that every listed file still matches the fingerprint recorded for it, and once that nothing extra has been added. INSTRUCTIONS.txt gives both commands, and MANIFEST.sha256 is the list they read.

A file that is not on that list is **not covered** by either check. The list itself, its signature file and any enclosed public key are the expected exceptions; treat anything else unlisted as untrusted.

If a signature file (MANIFEST.sha256.asc) is present, the folder is **signed**, and verifying it tells you who assembled it once you hold the signer's public key. An enclosed key proves nothing by itself: anyone able to alter the folder could replace that key and sign again. Confirm the signer's fingerprint **by phone, in person, or another way you already trust**.

WHAT THESE CHECKS DO NOT COVER

Passing both checks shows only that the files match a list shipped beside them. It cannot show who made them, and it cannot detect someone who changed a file and rebuilt the list to match. A verified signature names whoever assembled the package; it does not prove the appliance that built it was untampered. Until a signature is verified, or the operator confirms the contents with you by phone, in person, or another way you already trust, treat the package as unverified.

Each Confidence Report also carries its own fingerprint, taken over the report body rather than the whole file, so a plain whole-file check will not match it and that mismatch is expected. Each report's own "How to re-verify" section gives the command.

Bitcoin Witness. Verify, Attest, Inherit.

DEMO ONLY

Example data. In a real package this is `share-holder-map.gpg`, encrypted because it names people and **never printed**. It is shown decrypted here only to illustrate the format.

WHO HOLDS WHICH SHARE

SHARE	HOLDER & WHERE
1 of 3	**Alice** · SLIP-39 · safe deposit box (Zurich)
2 of 3	**Bob** · estate attorney · sealed
3 of 3	**Carol** · sibling · sealed envelope

TO RECOVER

Collect at least the threshold number of shares each report names, from the holders above and follow the "Recovery path:" line each Confidence Report carries. The shares themselves are never in this package.

Bitcoin Witness. Verify, Attest, Inherit.