Information for Auditors

Bitcoin Balance and Control Verification for SMSFs

This guide explains how CertainKey verification reports work, what they prove, and how to independently verify their findings.

Issued by	CertainKey
Contact	certainkey@dpinkerton.com
Web	app.certainkey.dpinkerton.com

What is CertainKey?

CertainKey provides independent Bitcoin balance and control verification for self-managed superannuation funds (SMSFs). It produces a detailed verification report confirming how much Bitcoin a fund holds and that the fund's trustees control the wallet's private keys — without moving any funds.

What the Report Proves

Each CertainKey report establishes two things at a specific point in time (the "Balance Snapshot"):

1. **On-chain balance** — the exact amount of Bitcoin held in the wallet, derived from Bitcoin's public blockchain at a specific block height.
2. **Key control** — cryptographic proof that nominated key holders control the wallet's private keys, verified through digital signatures (BIP-322 / BIP-137).

The report also provides a fiat valuation in AUD using a recognised pricing source at the snapshot date.

Why Cryptographic Proof Is Stronger Than a Bank Statement

A traditional bank or exchange statement is an *institutional attestation* — you are trusting the issuer to report accurately. A CertainKey report is backed by *mathematical proof*:

> The **balance** is derived directly from Bitcoin's immutable public ledger. Any party with a Bitcoin node and the wallet descriptor can independently reproduce the exact same figure. **Key control** is proven via digital signatures against a unique challenge string. The verification is deterministic — it either passes or it doesn't. There is no discretion or judgement involved.

This makes the evidence self-verifying and independent of any single institution, including CertainKey itself.

The Wallet Descriptor Hash

The report includes a SHA-256 hash of the wallet descriptor rather than the descriptor itself. This is a deliberate privacy and security measure: the raw descriptor reveals all wallet addresses and full on-chain transaction history.

The hash allows verification without exposure:

- If the client voluntarily provides the descriptor, the auditor can compute the SHA-256 hash and confirm it matches the report.
- Requesting the raw descriptor should not be necessary for audit sign-off, and is discouraged as a matter of operational security.

Independent Verification

The findings in a CertainKey report can be independently verified without proprietary software or access to CertainKey:

Balance	Load the wallet descriptor into any Bitcoin full node or compatible wallet software and query the balance at the stated block height.
Signatures	Verify the digital signatures using open-source tools such as Bitcoin Core's `verifymessage` RPC, Sparrow Wallet, or any BIP-322-compatible verifier.
Descriptor hash	Compute the SHA-256 hash of the descriptor string (no trailing whitespace) and compare to the report.

Report Authenticity

A SHA-256 hash of each report PDF is stored by CertainKey at generation time. To confirm a report has not been altered, visit **app.certainkey.dpinkerton.com/verify** and drop the PDF into the verification page. The file is hashed locally in your browser and never leaves your device — only the hash is transmitted for comparison.

Alternatively, compute the SHA-256 hash yourself and enter it manually.

Regulatory Alignment

CertainKey reports are designed to satisfy:

- **ATO** requirements for SMSF cryptocurrency holdings documentation.
- **ASIC** guidance on digital asset custody and control evidence.
- **AASB 1056** reporting standards for superannuation entities and **AASB 13** fair value measurement requirements.

The report provides the balance, valuation, and proof of control evidence typically required for SMSF audit sign-off.

Contact

For auditor questions or to discuss a specific report:

Email	certainkey@dpinkerton.com
Web	app.certainkey.dpinkerton.com