



Verification Report

Bitcoin Balance and Control

CONFIDENTIAL — Prepared solely for the named recipient and their appointed auditor.
Redistribution without written consent from CertainKey is prohibited.

Prepared for	James Thompson & Sarah Thompson as Trustee for Thompson Family Superannuation Fund
ABN	51 824 753 196
Report Date	04/03/2026
Reference	CK-2025-EOFY-XMPL
Version	1.0



Contents

- 1** Executive Summary

- 2** Note to Auditors

- 3** Verification Results

- 4** Methodology

- 5** Regulatory Compliance

- 6** Limitations

- 7** Sign-off

- 8** Glossary

- A** Appendix: Wallet Descriptor Hash



1. Executive Summary

1.8534 BTC

VERIFIED BALANCE

AUD \$287,648

FIAT VALUATION

Pass (A+)

ASSESSMENT

Entity	Thompson Family Superannuation Fund (ABN 51 824 753 196)
Engagement	EOFY Proof of Holdings
Balance Snapshot	30 June 2025, 23:59 AEST (block height 895,421)
Balance	1.8534 BTC (AUD \$287,648 at AUD 155,200/BTC, 30 June 2025)
Key Control	3 of 3 key holders verified (2 required) – Exceeded
Descriptor Hash	9720a4c44d63192d02b4bd6ab0075f7d28813cc3b9cc5304e21a2c62a7fce a39



2. Note to Auditors

This report is designed to serve as **sufficient standalone evidence** of Bitcoin ownership, control, and valuation for SMSF audit purposes.

The cryptographic signature verification provides **mathematical proof** that the entity controls the wallet's private keys – a standard of evidence stronger than a conventional bank or exchange statement, which **relies solely on institutional attestation**.

The wallet descriptor (which encodes the wallet's addresses and key configuration) is **not included** in this report at the customer's request. The SHA-256 descriptor hash is provided so that, if the entity voluntarily discloses the descriptor, its integrity can be independently confirmed.

Note: Without the wallet descriptor, this report cannot be independently verified against the Bitcoin blockchain. Your auditor may require the descriptor to satisfy their evidence obligations under ASA 500 and GS 009. A full version of this report including the wallet descriptor and cryptographic signatures is available from the customer's CertainKey dashboard.

Standards Mapping

This table maps the evidence in this report to applicable Australian Auditing Standards assertions, for use in audit working papers.

AUDIT ASSERTION	STANDARD	EVIDENCE IN THIS REPORT
Existence	ASA 500.A31 GS 009 para 80	UTXO balance confirmed at block height 895,421 by scanning all derived wallet addresses against Bitcoin's public ledger
Rights & Obligations	ASA 500.A31	BIP-322/BIP-137 cryptographic signatures prove private key control – mathematically verifiable and unforgeable
External Confirmation	ASA 505	Balance sourced from Bitcoin blockchain via independent node infrastructure, not from client-supplied data
Valuation	AASB 13 ASA 540	AUD valuation derived from independent pricing source (Bitaroo) at snapshot date
Completeness	ASA 500.A5	SHA-256 descriptor hash enables cross-period consistency checks on wallet configuration
Integrity	ASA 500.A5	Report SHA-256 hash stored at generation – tamper-evident and publicly verifiable

Report Authenticity

A SHA-256 hash of this PDF is stored by CertainKey at the time of generation. To confirm this 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. Alternatively, compute the SHA-256 hash yourself and enter it manually.

Independent Verification

The underlying findings can also be verified independently, 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 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 this report.



3. Verification Results

Balance

Thompson Family Superannuation Fund held **1.8534 BTC** at block height **895,421**, confirmed by scanning all derived wallet addresses and summing confirmed on-chain transaction outputs up to the snapshot block.

BTC Balance	1.8534 BTC
Price per BTC	AUD 155,200 (Bitaroo, 30 June 2025)
Fiat Valuation	AUD \$287,648
As at	30 June 2025, 23:59 AEST

Key Control

Each key holder was issued a unique cryptographic challenge (`CK-895421-a7f3b2e1`), requiring them to produce a digital signature using their private key – proving control without moving funds.

NAME	ROLE	SIGNED	VERIFICATION
James Thompson	Trustee	Yes	Verified
Sarah Thompson	Trustee	Yes	Verified
Michael Thompson	Advisor	Yes	Verified

Quorum: 2 of 3 required – Exceeded (3/3 signed). **Rating: A+**

Evidence Summary

Descriptor Hash	9720a4c44d63192d02b4bd6ab0075f7d28813cc3b9cc5304e21a2c62a7fce a39
Block Height	895,421
Signing Challenge	<code>CK-895421-a7f3b2e1</code>
Signature Method	BIP-322 / BIP-137 (auto-detected)



Key Holder Fingerprints

Where provided, the master extended public key (xpub) fingerprints for each signer are listed below. These allow auditors to cross-reference key holder identity against the wallet descriptor without exposing sensitive key material.

KEY HOLDER	MASTER XPUB FINGERPRINT
James Thompson	a1b2c3d4
Sarah Thompson	e5f6a7b8
Michael Thompson	c9d0e1f2



4. Methodology

Balance Verification

Thompson Family Superannuation Fund supplied their wallet descriptor via the CertainKey platform. CertainKey derived all wallet addresses from the descriptor and computed the balance from confirmed on-chain transactions up to the snapshot block height. Balance data is sourced from Bitcoin's public ledger via CertainKey's own full Bitcoin node infrastructure, with independent public servers as fallbacks.

Signature Verification

Signatures were accepted in ECDSA (BIP-137/Electrum) or BIP-322 (Generic Signed Message) format and verified using CertainKey's verification engine, which auto-detects signature formats across Legacy, Wrapped SegWit, Native SegWit, and Taproot address types.

Data Handling

All sensitive wallet descriptor and key data is purged 90 days after report generation, in accordance with the Australian Privacy Act 1988 (Cth). The wallet descriptor hash is retained as a one-way cryptographic output that protects privacy while allowing verification.

5. Regulatory Compliance

This report is 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.

6. Limitations

- **Point in time:** This report reflects balance and control status solely as at the Balance Snapshot. Balances are subject to change after this point.
- **Fiat valuation:** Relies on third-party pricing data from Bitaroo, Australia's biggest bitcoin-only exchange.
- **Scope:** This is a targeted verification of Bitcoin holdings, not a comprehensive financial audit.
- **Privacy:** All personal and financial data is handled in accordance with the Australian Privacy Act 1988 (Cth) and CertainKey's privacy policy.



7. Sign-off

Thompson Family Superannuation Fund held **1.8534 BTC**, valued at **AUD \$287,648**, as at the Balance Snapshot (30 June 2025, block height 895,421). Key control was verified by 3 of 3 key holders. Assessment: **Pass (A+)**.

A SHA-256 hash of this PDF is stored by CertainKey for tamper detection. Verify at app.certainkey.com.au/verify – the PDF is hashed locally in your browser and never uploaded.

Prepared by

David Pinkerton – Principal Verifier, CertainKey

04/03/2026

certainkey@dpinkerton.com

Customer Acknowledgement

The undersigned confirms that the information provided to CertainKey was complete and accurate to the best of their knowledge, and acknowledges the findings and limitations of this report.

A handwritten signature in black ink, appearing as a series of connected loops and curves.

James Thompson, Trustee

04/03/2026



8. Glossary

Balance Snapshot

The specific date, time, and Bitcoin block height at which the balance was confirmed. All figures in this report are accurate as at this point only.

BIP-137 / BIP-322

Bitcoin Improvement Proposals defining methods for signing a message with a Bitcoin private key to prove address ownership, without moving funds.

Block Height

A sequential number identifying a specific block on the Bitcoin blockchain. Block heights are exact and immutable, making them the definitive reference point for balance verification.

Multi-Signature (Multisig) Wallet

A Bitcoin wallet requiring multiple private key signatures (e.g., 2 of 3) to authorise transactions.

Quorum

The minimum number of key holder signatures required to authorise a transaction from a multi-signature wallet.

SHA-256

A cryptographic hash function producing a fixed-length 256-bit output from any input. Used for the wallet descriptor hash and PDF authentication hash.

Wallet Descriptor

A standardised string that fully describes a Bitcoin wallet's configuration, including its keys and signing requirements. See Appendix A.

Xpub (Extended Public Key)

A public key from which child public keys and Bitcoin addresses can be derived. The "master xpub fingerprint" is a short identifier (8 hex characters) derived from the root key.



Appendix A: Wallet Descriptor Hash

The wallet descriptor is a standardised text string that fully describes a Bitcoin wallet's configuration – including its type, required number of signers, and each signer's extended public key and derivation path. Because this string contains sensitive information, it is hashed using SHA-256 to protect privacy while still allowing verification.

Anyone with the exact descriptor can recompute the hash to confirm it matches the one published in this report. To verify, compute the SHA-256 hash of the descriptor string (with no trailing whitespace or newline) and compare the output.

Example

Input descriptor

```
sh(multi(2,[fingerprint1/48'/0'/0']xpub1,  
[fingerprint2/48'/0'/0']xpub2,  
[fingerprint3/48'/0'/0']xpub3))
```

SHA-256 hash

```
7d5b07fad41588dde313e8e83c53436dbed0923f1af26a318fa9a1eff1fe6478
```



Report Authentication

This report's integrity can be verified by comparing its SHA-256 hash against CertainKey's records.

VERIFY THIS REPORT

Visit app.certainkey.com.au/verify and drop the PDF to confirm authenticity.

