Verification Report

Bitcoin Balance and Control

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

1.8534 BTC	AUD $287,648	Pass (A+)
VERIFIED BALANCE	FIAT VALUATION	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	`9720a4c44d63192d02b4bd6ab0075f7d28813cc3b9cc5304e21a2c62a7fcea39`

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 **included in Appendix B** to facilitate independent verification. The cryptographic signatures used to prove key control are also included, along with the BIP-32 derivation path for each signing address.

This report is designed to provide sufficient appropriate audit evidence under ASA 500, enabling direct verification of holdings against the Bitcoin blockchain without reliance on a service organisation report (ASA 402 / ASAE 3402). All findings can be independently reproduced using open-source tools.

The SHA-256 descriptor hash is also provided in the Executive Summary for cross-reference.

> **Confidentiality:** The wallet descriptor should be treated with the same confidentiality as a bank account number. It reveals all wallet addresses and on-chain transaction history but does not enable spending. This report should only be shared with the entity's appointed auditor.

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

This report includes all the data needed for full independent verification, without proprietary software or access to CertainKey:

- **Balance:** The wallet descriptor is provided in Appendix B. Load it into any Bitcoin full node or compatible wallet software and query the balance at the stated block height.
- **Signatures:** The BIP-322/BIP-137 signatures and derivation paths are provided in this report. Derive each signing address from the descriptor at the stated path and verify the signature against the signing challenge using open-source tools such as Sparrow Wallet or any BIP-322-compatible verifier.
- **Descriptor hash:** The full descriptor and its SHA-256 hash are provided in Appendix B. Compute the hash independently to confirm integrity.

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	`9720a4c44d63192d02b4bd6ab0075f7d28813cc3b9cc5304e21a2c62a7fcea39`
Block Height	895,421
Signing Challenge	`CK-895421-a7f3b2e1`
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`

Cryptographic Signatures

The following BIP-322/BIP-137 signatures were provided by key holders in response to the signing challenge `CK-895421-a7f3b2e1`. Each signature can be independently verified using open-source tools.

KEY HOLDER	SIGNING ADDRESS	SIGNATURE
James Thompson	`bc1qexample0addr0james0thompson0demo0report0only000000jt8m4s` Path: `m/48'/0'/0'/2'/0/0`	`AkcwRAIgT3Y6mVzWqB5FxPl8kR2hU4jN7bwKd9sFjLpQcA0RMnICIGxH8vN5dWkYr3qJlB7tZ0sP6mC4XjD9eUoKfE2AxhBASEDxR4vP7bNk3mQwL5fYjT8aK0cZ6hU2dW9gS1eXpI4rVo=`
Sarah Thompson	`bc1qexample0addr0sarah0thompson0demo0report0only000000k7p2w` Path: `m/48'/0'/0'/2'/0/0`	`AkcwRAIgJm8uN4bRx5dHwK7jLfQ3gP0sT6cV9aY2eUoS1hXkI8MCIFtG3vZ0rWpD6mE5nYqJ7wB4xC9fKaHlU8dSjN2eRoLASECpK7mT4vN0xR3qW8bFjH6sY5gU9aD2cZlE1dXoI3wSf=`
Michael Thompson	`bc1qexample0addr0michael0thompson0demo0report0only0000q9x3r` Path: `m/48'/0'/0'/2'/0/0`	`AkcwRAIgQk5rL2bN8xH3dF7jT0wP6mC4sV9aYeUoKfG1hXkI8RMCIGpD6vZ0rWtN3qJ7wB4mE5nYsC9fKaHlU8dSjQ2eRoLASEBwM3nT4vK7xR0bFjH6qW8sY5gU9aD2cZlE1dXpI3rSf=`

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

The wallet descriptor and cryptographic signatures are included in this report. All other sensitive 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.

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
```

Appendix B: Wallet Descriptor & Signatures

The wallet descriptor below is included to enable full independent verification by the appointed auditor.

> **Confidentiality Notice:** The wallet descriptor should be treated with the same confidentiality as a bank account number. While it does not grant the ability to spend funds, it reveals all wallet addresses and enables surveillance of the wallet's complete on-chain transaction history. This appendix should not be shared beyond the entity's appointed auditor.

Wallet Descriptor

```
BSMS 1.0
wsh(sortedmulti(2,[a1b2c3d4/48h/0h/0h/2h]xpub6BosfCnifzxcFwrSzQiqu2DBVTshkCXacvNsWGYRVVStYCA
nTPHAgj7KCAB7KhcefeNEbDHsGJQw8WHkJGQZfpQNbTCojfkCGDEHr6DJWbDk,[e5f6a7b8/48h/0h/0h/2h]xpub6C6
nQwHaWbSrzs5tZ1q7m5R9cPK9eSPWNcXN2EFesiZoXAL6Tp5vE5vFHqXUnqxAQPKs7C3PB7D5jqYFFqxaJpkB6JqH5Hp
UXW5dB3fEQFd,[c9d0e1f2/48h/0h/0h/2h]xpub6CatWdiZiodmUeTDp8LT5or8nmbKNcuyvz7WyksVFkEqfjzCUrFy
95KDCCZ2e7s5Y5sE3Y8ERf9PpC6zCLqJxhgDSauRq7MxmDFPx3FqPvb))
/0/*,/1/*
bc1q9example0address0placeholder0for0demo0report0only000pv8wjt
```

SHA-256: `9720a4c44d63192d02b4bd6ab0075f7d28813cc3b9cc5304e21a2c62a7fcea39`

Load this descriptor into any Bitcoin full node or compatible wallet software (e.g. Sparrow Wallet, Bitcoin Core) to independently derive all wallet addresses and verify the balance at the stated block height.

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.