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	03/09/2026
Reference	CK-2025-EOFY-XMPL
Version	1.3

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	$287,647.68	Pass (A+)
VERIFIED BALANCE	FIAT VALUATION (AUD)	ASSESSMENT

Entity	Thompson Family Superannuation Fund (ABN 51 824 753 196)
Engagement	EOFY Proof of Holdings and Control
Balance Snapshot	30 June 2025, 23:51:07 AEST (block height 895,421)
Balance	**1.8534 BTC** (AUD $287,647.68 at AUD 155,200.00/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 provide evidence of Bitcoin **existence, control and valuation** that an SMSF auditor can verify independently, without reliance on CertainKey.

> 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 discloses the descriptor to you directly, its integrity can be confirmed against this report. The cryptographic signatures, signing addresses and derivation paths **are included**, so key control can be verified independently of the descriptor.

> **Note:** Without the wallet descriptor, the balance cannot be re-derived from the blockchain by a third party; it rests on CertainKey's scan of the descriptor and the funded addresses. Key control and descriptor-hash integrity can still be verified from this report. If the descriptor is needed, it can be obtained from the entity directly, or a version of this report including it 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 findings can be verified independently, without proprietary software or access to CertainKey:

- **Signatures:** The BIP-322/BIP-137 signatures, signing addresses and derivation paths are provided in this report. Verify each signature against the signing challenge using open-source tools such as Sparrow Wallet, Bitcoin Core's `verifymessage` RPC, or any BIP-322-compatible verifier.
- **Balance:** Requires the wallet descriptor, which the entity has chosen not to include here. If the entity provides it to you, load it into any Bitcoin full node or compatible wallet software and query the balance at the stated block height.
- **Descriptor hash:** If provided with the descriptor, compute its SHA-256 hash (including the trailing checksum, no trailing whitespace) and compare to this report to confirm it is the same wallet.

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.

Block 895,421 was mined at 23:51:07 AEST on 30 June 2025 (2025-06-30 13:51:07 UTC) and is the last block confirmed before 00:00 AEST on 1 July 2025. It therefore defines the holding as at the end of 30 June 2025.

BTC Balance	**1.8534 BTC**
Price per BTC	AUD 155,200.00 (Bitaroo)
Price Definition	Close of the Bitaroo BTC/AUD one-hour candle ending 00:00 AEST on 1 July 2025 (14:00 UTC, 2025-06-30).
Price Evidence	Retrieved 2025-07-02 14:12:38 UTC from `https://api.bitaroo.com.au/v2/price/2025-06-30/13`; value returned: `155200`
Fiat Valuation	**AUD $287,647.68** (1.8534 BTC × AUD 155,200.00, rounded to the cent)
As at	30 June 2025, 23:51:07 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.

KEY	NAME	ROLE	SIGNED	VERIFICATION
Key 1 `a1b2c3d4`	James Thompson	Trustee	Yes	Verified
Key 2 `e5f6a7b8`	Sarah Thompson	Trustee	Yes	Verified
Key 3 `c9d0e1f2`	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
Snapshot Block Time	23:51:07 AEST, 30 June 2025 (2025-06-30 13:51:07 UTC)
Snapshot Block Hash	`00000000000000000001a4c2e7d3f0b9c8a7e6d5c4b3a2918f7e6d5c4b3a2918`
Price Retrieved	2025-07-02 14:12:38 UTC from Bitaroo
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	KEY HOLDER	MASTER XPUB FINGERPRINT
Key 1	James Thompson	`a1b2c3d4`
Key 2	Sarah Thompson	`e5f6a7b8`
Key 3	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	KEY HOLDER	SIGNING ADDRESS AND PATH
Key 1 `a1b2c3d4`	James Thompson	`bc1qexample0addr0james0thompson0demo0report0only000000jt8m4s` Path: `m/48'/0'/0'/2'/0/0`
Key 2 `e5f6a7b8`	Sarah Thompson	`bc1qexample0addr0sarah0thompson0demo0report0only000000k7p2w` Path: `m/48'/0'/0'/2'/0/0`
Key 3 `c9d0e1f2`	Michael Thompson	`bc1qexample0addr0michael0thompson0demo0report0only0000q9x3r` Path: `m/48'/0'/0'/2'/0/0`

Signature

```
AkcwRAIgT3Y6mVzWqB5FxPl8kR2hU4jN7bwKd9sFjLpQcA0RMnICIGxH8vN5dWkYr3qJlB7tZ0sP6mC4XjD9eUoKfE2AxhBASEDxR4vP7bNk3mQwL5fYjT8aK0cZ6hU2dW9gS1eXpI4rVo=
```

Signature

```
AkcwRAIgJm8uN4bRx5dHwK7jLfQ3gP0sT6cV9aY2eUoS1hXkI8MCIFtG3vZ0rWpD6mE5nYqJ7wB4xC9fKaHlU8dSjN2eRoLASECpK7mT4vN0xR3qW8bFjH6sY5gU9aD2cZlE1dXoI3wSf=
```

Signature

```
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 cryptographic signatures are included in this report; the wallet descriptor is not. 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 has been prepared with regard to:

- **ATO** documentation expectations for SMSF cryptocurrency holdings.
- **ASIC** guidance on digital asset custody and control evidence.
- **AASB 13** fair value measurement, as applied to superannuation entities reporting under **AASB 1056**.

Whether this report constitutes sufficient appropriate audit evidence for a particular engagement is a matter for the appointed auditor.

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, published at app.certainkey.dpinkerton.com/privacy.

7. Sign-off

> Thompson Family Superannuation Fund held **1.8534 BTC**, valued at **AUD $287,647.68**, 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.dpinkerton.com/verify** — the PDF is hashed locally in your browser and never uploaded.

Prepared by

David Pinkerton — Principal Verifier, CertainKey

03/09/2026

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

03/09/2026

Revision History

All versions issued under this reference, in order. Version is the report template in use, as printed on that PDF's cover.

VERSION	DATE	REASON
1.3	03/09/2026	Report issued.

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. The hash covers the complete descriptor string exactly as exported by the wallet, **including the trailing** `#checksum`, with no trailing whitespace or newline. On a Unix system: `printf '%s' '<descriptor>' | sha256sum`

Example

A 2-of-3 native SegWit multisig in the format used by Sparrow Wallet, Coldcard and Bitcoin Core (BIP-48 account paths, `<0;1>` multipath for receive and change). The keys are test keys generated for this example; the descriptor is valid and can be loaded into wallet software.

Input descriptor

```
wsh(sortedmulti(2,[0b74e0c6/48h/0h/0h/2h]xpub6E11tnmw33QMAY9Zqj9PEMiUiLgWrhEguPf6aFyMZmfS46Lmef1yu
1C1d79ctYs6wUznWJ5DXChrL5FnBkSSxnsXSEoa7xoWGw9KtwVvL8p/<0;1>/*,[8519dfb7/48h/0h/0h/2h]xpub6FPqyGhJ
vuXVvpY1riyBUSs7nFUUx5se25CAaQSsyM1MF5noqp5d2umUFAdEsupMvDmdHwJXLzS5gFGFgtKACmAJJFmkjwb1XR5QE7CR2q
g/<0;1>/*,[f6aa67f5/48h/0h/0h/2h]xpub6EXuhirsLMommXP2SqKvKgYGGCotASScxZDnCGqDoJDqd96VA3fba1UmXukYB
QKQZnXoGVtHr5J8d6NMBP4D1bzY2KWorrFnEEw17RppzeZ/<0;1>/*))#tvwh57lx
```

SHA-256 hash

```
c134575c7d5fcc7600a58a320bf396ec653cf75a56523f1e7a78b258ac7e4290
```

Report Authentication

This report's integrity can be verified by comparing its SHA-256 hash against CertainKey's records. The file's own hash cannot be printed inside the file, since doing so would change it. A checksum file (`CK-2025-EOFY-XMPL.pdf.sha256`) is available to the customer from their CertainKey dashboard and can be checked offline with `sha256sum -c`.

VERIFY THIS REPORT

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