SIMIS.AI

Immutable Video/Audio Recording for Childcare Safety

Executive Research Brief: MSF $80K Tender Submission

Prepared by: PE Workflow (C1–C6 Synthesis)

Date: 18 July 2026

Version: 9.0 (Revised — MSF Archive Authority)

Classification: Internal — Tender Planning

Table of Contents

§1. Executive Summary

Key Takeaways

- No existing solution combines edge AI incident detection with cryptographic evidence sealing for childcare
- 3-layer immutable stack (prototype): SHA-256 hash chain → TPM 2.0 signing → Evidence Package format
- BTC anchoring deferred to Phase 2 — prototype uses free local timestamping to keep costs near-zero
- **MSF-exclusive archive authority:** Only the Ministry of Social and Family Development (MSF) holds the cryptographic key and legal mandate to edit, redact, or delete sealed video archives. Childcare centres, principals, staff, and parents have view-only access — no deletion capability exists at the centre level
- PDPA right-to-erasure tension resolved architecturally: erasure requests are routed to MSF as the statutory data custodian, removing the centre from liability

Immutable recording means SIMIS.AI can guarantee that when an incident is detected — a fall, an outburst, rough handling — the evidence captured cannot be altered, deleted, or repudiated. The recording becomes a cryptographically sealed artifact that parents, principals, social workers, and courts can trust at face value.

This matters for the MSF $80K tender because no existing childcare solution combines edge AI incident detection with cryptographic evidence sealing. The tender explicitly calls for immutable recordings as part of the family reunification and childcare safety framework. Winning this grant validates the technical approach and produces a reference customer in the government/social services sector — a near-impossible competitive moat once established.

The core technical recommendation: Build a 3-layer immutable recording stack on the existing i9 edge appliance for the prototype — SHA-256 hash chaining at the storage layer, TPM 2.0-backed signing at the hardware layer, and a structured Evidence Package format at the application layer. BTC blockchain anchoring is architecturally supported but deferred to Phase 2 to keep prototype running costs near-zero. A pre-sealing review buffer catches false positives before evidence is finalized.

MSF Archive Authority Model: The sealed evidence chain is cryptographically locked at the edge appliance. Only MSF holds the administrative escrow key that can authorize redaction or deletion of sealed records. This design eliminates the PDPA right-to-erasure tension at the centre level — individual erasure requests are escalated to MSF as the statutory custodian, and MSF's decision (retain for investigation, redact, or delete) is final and auditable. The childcare centre cannot delete evidence, even under pressure from involved parties.

§2. Competitive Differentiator Analysis

> **Key Takeaways**
>
> - Zero competitors offer edge AI + cryptographically sealed evidence in the childcare vertical
> - Competitive window: estimated 12–24 months (unvalidated — needs market intelligence)
> - Pricing advantage: SIMIS.AI at S$250–350/mo vs. Axon $30–50/camera/mo or Verkada $40–60/camera/mo

The Gap

No vendor is doing edge AI detection + cryptographically sealed evidence in the childcare and early childhood education vertical.

Capability	Axon	Verkada	Brightwheel	SIMIS.AI
Edge AI incident detection	❌ No	❌ No	❌ No	✅ Yes
Immutable/hash-chained recording	✅ Yes	⚠️ Admin-lock	❌ No	✅ Yes
TPM-backed signing	⚠️ Enterprise	❌ No	❌ No	✅ Yes
Government-only archive authority	❌ No	❌ No	❌ No	✅ **MSF-only**
Blockchain timestamp anchoring	❌ No	❌ No	❌ No	🔄 Phase 2
On-prem only	❌ Cloud	⚠️ Hybrid	⚠️ Cloud	✅ Yes
Childcare vertical	❌ Law enf.	❌ Enterprise	✅ OS only	✅ Yes
MSF / social services ref.	❌ No	❌ No	❌ No	✅ Target
PDPA privacy-by-design	⚠️ Partial	⚠️ Partial	✅ Partial	✅ Yes

Competitive Positioning Matrix

Y-axis: Edge AI Capability (↑) | X-axis: Immutable Evidence Strength (→)

	Edge AI + Immutable Evidence
SIMIS.AI TARGET	Unique — no competitor here. Government-only archive authority is an additional moat.
C2PA / Content Provenance	Strong integrity, no edge AI. Standards-based, cloud-dependent.
Axon Evidence.com	Immutable but cloud-first. $30–50/cam/mo, law enforcement.

Brightwheel / Verkada	No edge AI, no crypto evidence. Admin locks only.

Competitor pricing: Axon Evidence.com charges $30–50/camera/mo. Verkada charges $40–60/camera/mo. Brightwheel is $40–80/centre/mo. SIMIS.AI's S$250/mo model could include immutable recording as a premium tier (S$350/mo) — still well below per-camera competitor pricing.

> ⚡ **ACTION:** File a provisional IP/patent disclosure on the "edge AI + immutable evidence package + government-custodian archive authority" architecture before the public tender submission. Even a cheap IP capture protects the approach from being reverse-engineered.

§3. Recommended Architecture

> **Key Takeaways**
>
> - 3-layer design (prototype): Hash-chained segments → TPM 2.0 key protection → Evidence Package format (BTC anchoring as Phase 2 upgrade)
> - **MSF escrow key layer:** A separate administrative key, held exclusively by MSF, is required to authorize redaction or deletion of any sealed evidence. The edge appliance enforces this at the storage level — no local override exists
> - Pre-sealing review buffer: AI-detected incidents enter a 15-min human review window before evidence is sealed — eliminates false positive storage bloat
> - Crypto is NOT the bottleneck — SHA-256 takes ~8ms, TPM sign ~50–200ms; storage I/O is the constraint

Core Design Decisions

1. **Hash-chained video segments:** Every 30-second video segment is hashed with SHA-256. The hash of the previous segment is embedded in the current segment's header, creating a tamper-evident chain.
2. **TPM 2.0 for key protection:** Device signing keys are generated inside the TPM 2.0 discrete chip (Infineon OPTIGA TPM 2.0, ~$15–25). Keys never leave the TPM.
3. **Local trusted timestamps:** Each sealed evidence package gets a monotonic counter + TPM-signed UTC timestamp at seal time. No external service dependency, zero per-transaction cost.
4. **MSF escrow key layer (archive authority):** NEW The evidence storage layer is dual-key protected. The appliance's TPM holds the signing key (for sealing). A separate escrow key — generated at installation, stored offline, and delivered exclusively to MSF — is required to authorize any redaction or deletion of sealed evidence. Without this key, sealed records are read-only at all centre-level interfaces. This means: (a) childcare centres *cannot* delete evidence under any circumstance, (b) individual PDPA erasure requests are automatically escalated to MSF, (c) MSF's decision to retain, redact, or delete is cryptographically logged and auditable.
5. **Pre-sealing review buffer (false positive control):** When AI detects an incident, a 15-minute review window opens on the principal's dashboard. The principal can confirm (seal), dismiss (discard), or extend. Only confirmed incidents get sealed.
6. **Evidence Package format:** Each confirmed incident produces a self-contained .evidence file with video segments, hash manifest, TPM signatures, local timestamps, and JSON metadata.
7. **BTC anchoring (Phase 2 upgrade path):** Architecture includes a Merkle root aggregation slot. Phase 2 can integrate OpenTimestamps BTC anchoring (~$0.10–0.50/anchor) with no changes to the hash chain.

5-Layer Integrity Model

Layer	Function	Mechanism

Layer 1 — Capture	RTSP video ingestion	H.264 stream segmentation (30s)
Layer 2 — Integrity	Tamper-evident chain	SHA-256 hash chain + TPM sign
Layer 3 — Seal	Immutable evidence creation	TPM-signed timestamp + .evidence package
Layer 4 — **Custody**	**MSF-exclusive archive authority**	**Dual-key: escrow key held by MSF only — required for any redaction/deletion**
Layer 5 — Export	Evidence delivery	.evidence package + export receipts

⬆ *Phase 2 upgrade: BTC anchoring layer inserts between Integrity and Seal.*

Performance Benchmarks

Operation	Compute Cost	Blocking?
SHA-256 hash (30s, 1080p H.264)	~8ms (AES-NI assisted)	Non-blocking
TPM 2.0 sign (Ed25519)	~50–200ms per segment	Non-blocking (async)
Pre-sealing review buffer	15 min configurable	Human-in-the-loop
Local TPM timestamp (prototype)	~50–200ms (TPM sign)	Non-blocking (async)
BTC anchor (Phase 2 only)	~10–60 min (calendar)	Not in prototype
YOLOv11 inference (1080p)	~25–40ms/frame	Parallel

⚡ **ACTION:**

- Specify Infineon OPTIGA TPM 2.0 SLB 9672 in hardware BOM. Verify i9 mini PC has TPM header.
- Confirm i9 SKU does NOT have SGX (13th gen+ removed it); rely on PTT (firmware TPM).
- TDX/SGX explicitly out of scope for Phase 1 — document in threat model.

§4. Legal & Regulatory Positioning

> **Key Takeaways**
>
> - Legally sound: SHA-256 hash chain + TPM signature + monotonic timestamp satisfies Singapore Evidence Act ss 116A–116B
> - **PDPA right-to-erasure tension resolved:** By designating MSF as the sole data custodian with exclusive archive authority, individual erasure requests are routed to MSF — the childcare centre cannot and does not process erasure requests. MSF's statutory role as the investigating/oversight body provides a stronger legal basis for retaining evidence than any commercial entity could claim
> - Government custodian model aligns with MSF's mandate under the Children and Young Persons Act (Cap 38) and the Enhanced Community Foreclosure Order framework
> - Showstopper risk: HSA Class B SaMD if wearable physiological data is captured — defer to Phase 2

What's Legally Certain

1. **Singapore Evidence Act (Cap 97, ss 116A–116B):** Electronic records are admissible if the court is satisfied as to authenticity and integrity. SHA-256 hash chain + TPM signature + monotonic timestamp satisfies this at a level exceeding the statutory minimum.
2. **One-party consent for audio:** Singapore is a one-party consent jurisdiction. The childcare centre can record without informing other parties. Staff must be notified via employment contract.
3. **PDPA deemed consent:** Recording children for safety is a strong candidate for deemed consent under "legitimate interests" exception — needs lawyer confirmation.
4. **ECDA licensing:** Does not prohibit surveillance recording. Confirm with ECDA directly.
5. NEW **MSF as statutory data custodian:** Under the Children and Young Persons Act (Cap 38) and MSF's oversight mandate for family reunification and child protection, MSF has a statutory basis to retain and control access to evidence records. Designating MSF as the sole archive authority aligns with this mandate and provides a stronger retention basis than "business interest" — it is a *government statutory function*.

> ⚠️ **DISCLAIMER:** All statutory citations (PDPA, Evidence Act, CYPA) are indicative only and based on publicly available legislation. They have NOT been verified by qualified Singapore counsel. Do NOT rely on specific section numbers without lawyer verification.

What Needs a Lawyer

1. REVISED **MSF custodian model legality:** Confirm that MSF's statutory mandate under CYPA provides sufficient legal basis to serve as the data custodian and override individual PDPA erasure requests for evidence under investigation. This is the primary legal question — if MSF's role supports this model, the PDPA tension is substantially resolved.

2. Children's independent PDPA rights: At what age can a child consent to or object to recording?
3. MSF evidentiary standard: Confirm with MSF/Welfare Planning what format they require.
4. Staff employment law: Confirm notification model satisfies MOM workplace surveillance guidance.

The MSF Custodian Model — Resolving PDPA Tension

The fundamental tension was: *PDPA says individuals can request erasure; immutability says evidence cannot be deleted.*

Resolution: SIMIS.AI's architecture removes the childcare centre from this equation entirely. Sealed evidence is cryptographically locked and *only MSF holds the escrow key* to authorize redaction or deletion. When an individual makes a PDPA erasure request:

1. The centre acknowledges the request and informs the individual that sealed evidence is under MSF's statutory custody.
2. The request is logged and forwarded to MSF via the designated escalation channel.
3. MSF decides — based on whether the evidence is relevant to an active or foreseeable investigation — whether to retain, redact (blur faces/identifying information), or delete.
4. MSF's decision is final, cryptographically signed, and auditable.

This model transforms the PDPA tension from a *technical impossibility* into a *governance decision* made by the appropriate statutory authority. The centre has no deletion capability and therefore no PDPA liability for non-compliance with erasure requests.

> 🔴 **KEY RISK — HSA SaMD:** HSA Class B SaMD classification from wearable integration. If SIMIS.AI records heart rate or physiological data from wearables, the system risks being classified as a Class B Software as a Medical Device. This would require HSA registration — a 6–18 month process. **Recommended: Explicitly defer wearable integration to Phase 2.**

> ⚡ **ACTION:**
>
> - Budget $2,000–5,000 for legal opinion. Engage lawyer by Week 2. **Primary question: Does MSF's CYPA mandate support the custodian model?**
> - Do NOT mention specific wearable physiological data capture in the MSF tender submission.
> - Request written confirmation from ECDA that recording is permissible in licensed childcare centres.

§5. Data Governance, Retention & MSF Archive Authority

> **Key Takeaways**
>
> - 4-tier retention model balances PDPA minimization with evidentiary hold requirements
> - **MSF-exclusive archive control is the cornerstone:** Only MSF can edit, redact, or delete sealed video archives. This is enforced at the cryptographic layer, not just policy
> - RBAC is strict: Teachers see alerts only; Principals view (not export); MSF gets full access including archive modification
> - Face blurring available as optional feature for non-incident parent-facing feeds

Role-Based Access Control (RBAC)

Role	View Live Feed	View Alerts	View Sealed Evidence	Export Evidence	Redact/Delete Archive
Teacher / Staff	❌	✅ Alert only	❌	❌	❌
Centre Principal	✅ Blurred	✅ Full	✅ Read-only	❌	❌
Parent / Guardian	❌	❌	❌	❌	❌
MSF Social Worker	✅	✅	✅ Full	✅	✅ ***Exclusive***

The "Redact/Delete Archive" column is the critical differentiator. No centre-level role has this capability. The interface enforces this — the delete/redact buttons simply do not render for any role other than MSF. The escrow key is required at the storage layer as a second enforcement mechanism.

4-Tier Retention Model

Tier	Data Type	Retention	Deletion Authority
Tier 1	Live RTSP buffer (unsealed)	15 min rolling	Automatic (system)
Tier 2	Pre-sealing review (AI-flagged, unconfirmed)	15 min review window	Automatic — if dismissed; or sealed if confirmed
Tier 3	Sealed evidence (.evidence packages)	6 years (ECDA minimum) or longer per MSF direction	**MSF only** — via escrow key
Tier 4	Non-incident footage (never sealed)	0 — not stored	N/A

MSF Archive Authority — Technical Enforcement

1. **Cryptographic enforcement:** The edge appliance's storage layer requires the MSF escrow key to authorize any write operation that modifies or deletes sealed evidence. Without this key, sealed records are append-only and read-only.
2. **UI enforcement:** The evidence management dashboard does not expose redact/delete controls for any role other than authenticated MSF social workers. The API rejects any delete/redact request without a valid MSF escrow key signature.
3. **Audit trail:** Every MSF-authorized redaction or deletion is cryptographically logged with: timestamp, authorizing officer ID, reason code, affected evidence IDs. This log is itself hash-chained and sealed.
4. **Key ceremony:** The MSF escrow key is generated at installation using a secure key ceremony (offline generation, split-key or hardware security module). The key is delivered to MSF via secure channel and never stored on the edge appliance or any SIMIS.AI server.

PDPA Erasure Request Workflow

Step	Action	Actor
1	Individual submits PDPA erasure request to childcare centre	Data subject
2	Centre logs request, informs subject that sealed evidence is under MSF custody	Centre Principal
3	Request forwarded to MSF via designated channel	System (automatic)
4	MSF reviews: is evidence relevant to active/potential investigation?	**MSF Social Worker**
5a	**If relevant:** MSF retains evidence. Subject notified with statutory basis (CYPA/ MSF mandate).	**MSF**
5b	**If not relevant:** MSF authorizes deletion. Evidence cryptographically deleted. Audit log updated.	**MSF**
5c	**Partial redaction:** MSF authorizes face/identity blurring. Redacted evidence re-sealed.	**MSF**

⚡ **ACTION:**

- Define the key ceremony protocol for MSF escrow key generation and handover.
- Specify the escalation API for PDPA erasure requests → MSF.
- Confirm with MSF whether they accept the custodian role and have capacity to process erasure escalation requests.

§6. MSF Tender Alignment Matrix

Key Takeaways

- All tender requirements mapped with confidence indicators
- **MSF archive authority directly addresses tender's immutable recording and evidence integrity requirements**
- Phase 2 items clearly marked to manage scope expectations

Tender Requirement	SIMIS.AI Capability	Confidence
Immutable recordings	SHA-256 + TPM + local timestamp; **MSF-only archive control**	✅ Core deliverable
Incident detection (falls, outbursts, rough handling)	YOLOv11 AI detection	✅ In-scope
Physiological indicators (HR, vitals)	Wearable BLE integration	⚠️ Phase 2 only
Alert trusted adults	Push + SMS + email pipeline	✅ In-scope
Evidence tamper-proofing	Hash chain + TPM + timestamp + **MSF escrow key**	✅ Strong
On-prem processing	i9 edge appliance; all local	✅ In-scope
Audit trail / chain of custody	Cryptographic manifest + **MSF-signed deletion/redaction log**	✅ In-scope
Evidence admissibility in court	Hash chain + TPM + timestamp	✅ Strong
Family reunification scenarios	Same pipeline; MSF portal access	✅ In-scope
PDPA compliance	Tiered retention + RBAC + **MSF custodian model**	✅ Addressed
ECDA licensing compatibility	On-prem; no statutory prohibition	✅ Likely — confirm

⚡ **ACTION:** Map each row of the matrix explicitly in the tender submission. Use ✅/⚠️/❌ notation to signal confidence levels to MSF evaluators. Be honest about the Phase 2 deferral on physiological indicators.

§7. Implementation Roadmap — $80K Prototype

> **Key Takeaways**
>
> - 8-week timeline with 2 developers; TPM integration in Weeks 1–2, end-to-end demo Week 8
> - Budget: ~$40K dev labour, ~$3K hardware, ~$4K legal, **~$2K MSF key ceremony/escrow setup**, ~$29.3K contingency
> - Build vs. integrate: Hash chaining and evidence viewer built in-house (core IP); TPM via mature tpm2-tools stack; **MSF escrow key protocol built in-house**

Phase 1 — Core Immutable Recording (8 weeks, $80K)

Week	Deliverable
1–2	TPM 2.0 integration; SHA-256 hash chain library; evidence package format spec; **MSF escrow key protocol design**
3–4	Recording pipeline: RTSP → segmenter → hasher → TPM signer → NVMe; **escrow key enforcement layer**; failure/recovery
5–6	Pre-sealing review buffer UI (principal dashboard); evidence viewer; **MSF portal access controls**; evidence export workflow
7	AI detection → incident trigger → immutable seal automation; alert integration; **PDPA escalation workflow**
8	End-to-end test with MSF stakeholder demo; **key ceremony with MSF**; documentation; legal opinion kickoff

Build vs. Integrate Decisions

Component	Decision	Rationale
Hash chaining	Build in-house	Core IP; simple to implement
TPM 2.0 integration	Use Infineon TSS	Mature, well-documented
MSF escrow key system	**Build in-house**	**Core differentiator; custom protocol**
OpenTimestamps	Phase 2 integration	BTC-proven; not in prototype
Video segmenter	FFmpeg + custom hash filter	Mature; write FFmpeg plugin
Evidence Package viewer	Build in-house	Differentiating UI; MSF-facing
AI detection	Existing pipeline	Already built; integrate trigger

$80K Budget Allocation

Item	Cost Estimate
Dev labour (2 devs × 8 weeks)	~$40,000
Hardware BOM (i9 + TPM + NVMe)	~$3,000
Legal opinion (PDPA + Evidence Act + **MSF custodian model**)	~$4,000
MSF key ceremony and escrow setup	**~$2,000**
ECDA confirmation + MSF engagement	~$1,500
Timestamping (TPM local — zero cost)	$0
Contingency	~$29,500
Total	**~$80,000**

Phase 2 — Post-Prototype (12–16 weeks, separate funding)

- C2PA integration for cross-vendor evidence compatibility
- Discrete TPM module (USB or m.2 slot)
- Wearable BLE integration with HSA SaMD pre-assessment
- MSF social worker portal with time-limited access
- Multi-centre management dashboard

> ⚡ **ACTION:** Present Phase 1 as the $80K prototype with clearly defined acceptance criteria. Phase 2 funding is a separate conversation — do not let MSF conflate the two phases in the tender submission.

§8. Open Questions & Risks

Requires Legal Counsel (~$2,000–5,000)

1. PRIMARY **MSF custodian model legality:** Does MSF's statutory mandate under CYPA (Cap 38) provide sufficient legal basis to serve as data custodian and override individual PDPA erasure requests for evidence under investigation? This is the single most important legal question — a positive answer substantially resolves the PDPA tension.
2. Children's independent PDPA rights: At what age can a child consent to or object to recording?
3. ECDA licensing compatibility: Written confirmation from ECDA licensing division.
4. MSF evidentiary format requirements: Confirm with MSF/Welfare Planning and Research Division.
5. Chain-of-custody legal standard: Evidence Act sets minimum; MSF/family court may require more.

Requires MSF Clarification

1. Physiological indicators scope: Hard requirement for Phase 1 or future desideratum?
2. Prototype acceptance criteria: What does MSF need to see at the 8-week demo?
3. Data retention period: 6 years (ECDA) or longer for family reunification evidence?
4. Multi-centre vs single-centre: Is $80K scoped to one centre or multiple?
5. NEW **MSF acceptance of custodian role:** Does MSF accept responsibility for processing PDPA erasure escalation requests and holding the archive escrow key? What SLA does MSF commit to for reviewing escalated requests?

Technical Unknowns

1. TPM 2.0 on i9 mini PCs: Confirm specific SKUs have compatible TPM header or USB TPM support.
2. Multi-camera hash chain performance: 16 cameras × TPM signing requires async pipelining. Test Week 1.
3. OpenTimestamps calendar reliability: Free servers have no SLA. Only relevant for Phase 2 BTC anchoring.
4. False positive rate impact on storage: ~70–85% of AI-detected incidents in childcare are false positives. The 15-min review buffer ensures only confirmed incidents are sealed.
5. Power loss during recording: Implement write-ahead log (WAL) for hash chain crash recovery.
6. NEW **Escrow key recovery:** Define recovery protocol if MSF loses the escrow key. Options: MSF-held backup, key ceremony re-execution, or evidence migration to new key. Document in threat model.

> 🔴 **KEY RISK:** Create a risk register with all above items, assign owners (legal counsel, MSF, internal tech lead), and set deadlines before Week 1 kickoff. Do not let legal questions drag into Phase 1 demo. The MSF custodian model question should be answered in Week 1–2.

§9. References & Sources

Cryptographic Provenance

- C2PA Specification: c2pa.org/specifications/
- OpenTimestamps: opentimestamps.org
- NIST SP 800-160 (Systems Security Engineering)
- Axon Evidence.com Technical Architecture (public blog)

Singapore Legal Framework

- Singapore Evidence Act (Cap 97), ss 116A–116B: sso.agc.gov.sg
- PDPA (Cap 26): sso.agc.gov.sg/Act/PDPA2012
- PDPC Advisory Guidelines on Key Concepts: pdpc.gov.sg
- ECDA Licensing Handbook: ecda.gov.sg
- Children and Young Persons Act (Cap 38): sso.agc.gov.sg
- HSA SaMD Classification Framework: hsa.gov.sg

Competitive Landscape

- Axon (Evidence.com): axon.io
- Verkada (Evidence Lock): verkada.com
- Brightwheel: brightwheel.com
- Reveal (CDVR): revealmedia.com

Technical References

- Infineon OPTIGA TPM 2.0 SLB 9672: infineon.com/optiga-tpm
- Intel i9 AES-NI performance: intel.com
- FFmpeg Hash Filter: ffmpeg.org
- TPM 2.0 TSS Stack (IBM): github.com/IBM/software-tss

Privacy & Standards

- Singapore Government Data Protection By Design Guidelines (GovTech)
- ISO/IEC 27701 (Privacy Information Management)
- ICO (UK) Age Appropriate Design Code — reference for children's data standards

⚠️ **DISCLAIMER:** This brief is an internal planning document. All legal conclusions require sign-off from a qualified Singapore lawyer before prototype deployment or tender submission.