ACSE RESEARCH SERIES · WP-04

The Dasa Mahavidya Profiles — Domain-Adaptive Cryptographic Defence

Complete reference for all 11 ACSE mutation profiles: domain, design rationale, benchmarks, crown jewel claims, and integration patterns

Author: Arul Raj · Patent IN202641070690 · June 2026
Primary Audience: Security Architects · Infrastructure Teams · System Integrators · Classification: Public Technical Paper

ABSTRACT

ACSE's 11 mutation profiles are not independent engines. They are 11 expressions of a single MutationEngineCore, each tuned to the threat model, compliance requirements, and performance constraints of a specific surface class. This paper describes each profile in depth — domain, core design insight, key mechanism, performance benchmark, crown jewel security claim, and integration pattern.

All profiles implement the Kali Invariant identically. They differ in what surface properties are mutated, at what granularity, and with what domain-specific validation logic. Swapping one profile for another in a running PME deployment requires changing a single registration call.

1. PROFILE ARCHITECTURE

1.1 The MutationTarget trait

Every profile implements the MutationTarget trait — a five-method interface that gives MutationEngineCore everything it needs to manage any surface:

(a) fingerprint() → [u8;32]: current observable surface state as SHA3-256 hash
(b) mutate(entropy: &[u8]) → MutationResult: apply mutation, return result
(c) validate(result: &MutationResult) → bool: profile-specific invariant check
(d) rollback(checkpoint: &Checkpoint): restore to pre-mutation state
(e) profile_id() → u8: ASMP profile identifier for audit frames

The engine calls these methods in the same order for every profile on every cycle. Profile-specific logic lives entirely inside the implementation — the engine is profile-agnostic.

1.2 Profile selection guide

Infrastructure Class	Recommended Profile	Profile ID	Key Reason
Financial services / payment processing	SquidShield	0x03	100% fingerprint uniqueness at transaction rates; snapshot+restore for audit
Healthcare / PHI / HIPAA	GlassFrog	0x08	Immutable audit chain alongside mutable surface; per-cycle compliance proof

Intrusion response / active attacker	MantisNet	0x01	Fastest mutation (10.31µs); full Patrol→Strike→Retreat→Harden→Recover state machine
Cloud workloads / elastic scaling	JellyNet	0x02	MVS guarantee at all load levels; calm→critical transition in 1.09µs
AD / credential surfaces / defence	KrakenNet	0x05	4-arm independent mutation; LSASS/AD credential surfaces rotate continuously
VPN / API deception / attacker capture	AnglerShield	0x06	Real endpoint hidden; deception lures; attacker captured at 3-probe threshold
Data vault / database access	NautilusVault	0x07	5× Fibonacci protection gradient; O(1) siphuncle verification
COLO / data centre / side-channel	ElectricEelGrid	0x09	Power side-channel defeat; 0.03% correlation — only product addressing COLO power observable
Cloud cooperative enclaves	ChameleonNet	0x04	Zero mutual information between attacker and ally channels
Nation-scale / 16-node distributed	LeviathanGrid	0x0A	16-node simultaneous mutation + full topology rewire in 143.9µs
Estate-wide orchestration	KaliCoreTarget	0xFF	One trigger fires all registered profiles simultaneously in <200µs

2. PROFILE REFERENCE — CORE TEN

Profile 0x01: 🦐 MantisNet — Intrusion Response

Latency p50	Throughput	Profile ID
10.31µs p50	79.7k/s	0x01

Core Design Insight: The mantis shrimp strikes faster than the human eye can track and has the most complex visual system in the animal kingdom. MantisNet applies the same principle to intrusion response: detect fast, strike faster, then harden before the attacker can adapt.

Key Mechanism: Five-state machine: Patrol (normal) → Strike (mutation aggression maximum) → Retreat (surface withdrawal) → Harden (fingerprint anchoring for forensics) → Recover (return to patrol). The full state machine cycle completes in 131.8µs. At 10.31µs per mutation, MantisNet is the fastest PME profile.

Crown Jewel Claim: 107/107 Forced Twitch detections in red team evaluation. MantisNet identifies attacker probe patterns via timing analysis and uses the probe itself to trigger mutation, causing the attacker's next observation to be a post-mutation surface.

Integration Pattern: `engine.register(Box::new(MantisNetTarget::new("perimeter")), "ids");`

Profile 0x02: 🪼 JellyNet — Elastic Infrastructure / Scaling

Latency p50	Throughput	Profile ID
12.90µs p50	82.1k/s	0x02

Core Design Insight: A jellyfish has no centralised control system yet coordinates complex movement across its entire body simultaneously. JellyNet applies this to elastic infrastructure: mutation behaviour adapts automatically to load level with no centralised coordination overhead.

Key Mechanism: MVS (Minimum Viable Surface) guarantee: at any load level from empty to capacity, JellyNet guarantees the minimum cryptographically necessary surface exposure. calm→critical state transition takes 1.09µs — faster than a network round-trip, meaning JellyNet adapts before an attacker can observe the transition.

Crown Jewel Claim: Mathematically guaranteed MVS at all load levels. The only profile that formally proves minimum surface exposure as a function of current load — not as a best-effort property but as a provable invariant.

Integration Pattern: `engine.register(Box::new(JellyNetTarget::new("api-gateway")), "cloud");`

Profile 0x03: 🦑 SquidShield — Finance / Payment Processing

Latency p50	Throughput	Profile ID
15.94µs p50	76.1k/s	0x03

Core Design Insight: A squid's chromatophores change colour faster than any predator can track, creating visual patterns that defeat recognition systems. SquidShield applies this to financial surfaces: transaction identifiers rotate so fast that a captured token is useless before it can be replayed.

Key Mechanism: Per-transaction cryptographic surface rotation with atomic snapshot+restore for audit. The snapshot operation (15.78µs) captures the pre-transaction surface state for dispute resolution while the post-transaction surface is already on its next fingerprint. PCI-DSS audit trail is maintained throughout.

Crown Jewel Claim: 100% fingerprint uniqueness at 76.1k transactions/second sustained over 1,000 consecutive cycles. Zero fingerprint collisions in the entire test suite. This is the property that makes credential replay and session hijacking structurally impossible at transaction rates.

Integration Pattern: `engine.register(Box::new(SquidShieldTarget::new("payment-api")), "fin");`

Profile 0x04: 🦎 ChameleonNet — Cloud Cooperative Enclaves

Latency p50	Throughput	Profile ID

23.15µs p50	38.8k/s	0x04

Core Design Insight: A chameleon's colour change is not camouflage — it's communication with conspecifics, invisible to predators who cannot interpret the signal. ChameleonNet creates a dual-channel surface: an ally channel visible only to authenticated peers, and an attacker channel that provides zero mutual information about the ally channel.

Key Mechanism: Dual-channel architecture: the ally channel rotates on a schedule known to authenticated peers; the attacker channel rotates independently with zero correlation to the ally channel. Proven zero mutual information between the two channels. An adversary who observes the attacker channel learns nothing about the ally channel fingerprint.

Crown Jewel Claim: Zero mutual information between attacker channel and ally channel — formally measurable property, not an assertion. The only profile providing cryptographically proven communication privacy to authenticated peers while presenting a completely uninformative surface to adversaries.

Integration Pattern: `engine.register(Box::new(ChameleonNetTarget::new("enclave-mesh")), "coop");`

Profile 0x05: 🦑 KrakenNet — Defence / Multi-Domain / AD Surfaces

Latency p50	Throughput	Profile ID
28.56µs p50	34.7k/s	0x05

Core Design Insight: The kraken's arms are independently controlled yet work in coordination, making it impossible to disable the creature by attacking any single arm. KrakenNet applies 4-arm independent mutation to Active Directory and credential surfaces: disabling one credential domain does not help an attacker build a model of another.

Key Mechanism: Four independently mutating arms: network topology, credential identifiers, AD structure fingerprints, and session tokens. Each arm rotates with its own entropy slice (statistically independent). Sever-and-regenerate operation (90.26µs) can replace a compromised arm entirely without disrupting the other three.

Crown Jewel Claim: AD/LSASS credential surfaces rotate every 28.56µs. An LSASS dump captured at time t is cryptographically stale at t+1. This directly defeats the credential harvesting phase common to every major enterprise breach of the past decade, including Change Healthcare, Stryker-Handala, and Colonial Pipeline.

Integration Pattern: `engine.register(Box::new(KrakenNetTarget::new("ad-surface")), "defence");`

Profile 0x06: 🎣 AnglerShield — API Security / Attacker Deception

Latency p50	Throughput	Profile ID
31.67µs p50	32.3k/s	0x06

Core Design Insight: An anglerfish hides its real body in darkness while displaying a luminous lure that attracts prey to a specific point. AnglerShield hides the real API endpoint behind a rotating cryptographic fingerprint while presenting four deception lures that capture and identify attackers.

Key Mechanism: Real endpoint cryptographically hidden behind surface rotation. Four configurable lure endpoints that look attractive to reconnaissance tools. Attacker capture occurs at the 3-probe threshold: an IP address that probes any lure three times is classified as an active attacker and triggers KaliCore escalation to Hunter state.

Crown Jewel Claim: Probe capture at 3-probe threshold: 107/107 attacker self-identifications in red team evaluation. AnglerShield turns active reconnaissance into an attacker liability — every probe brings the attacker one step closer to self-identification and one step further from a usable model.

Integration Pattern: `engine.register(Box::new(AnglerShieldTarget::new("public-api")), "api");`

Profile 0x07: 🐚 NautilusVault — Data Vault / Database Access

Latency p50	Throughput	Profile ID
37.96µs p50	27.3k/s	0x07

Core Design Insight: A nautilus shell is a Fibonacci spiral of sequentially sealed chambers, each requiring the organism to be at the correct stage of development to access. NautilusVault applies this to data vault access: each layer of data has a cryptographic protection gradient that increases with data sensitivity.

Key Mechanism: Five-layer Fibonacci protection gradient: outer layers (metadata) rotate at highest rate, inner layers (sensitive PII/PHI) rotate at the highest cryptographic strength. The siphuncle — the continuous tube connecting all chambers — provides O(1) vault integrity verification (8.024µs) without requiring full vault traversal.

Crown Jewel Claim: O(1) vault integrity verification in 8.024µs — independent of vault size. A vault containing 100M records can be verified in the same time as a vault containing 100 records. This makes continuous integrity checking practical at any scale.

Integration Pattern: `engine.register(Box::new(NautilusVaultTarget::new("phi-store")), "vault");`

Profile 0x08: 🐸 GlassFrog — Healthcare / HIPAA / Audit-Intensive

Latency p50	Throughput	Profile ID
56.84µs p50	2,540/s*	0x08

Core Design Insight:

Key Mechanism:

Crown Jewel Claim:

Integration Pattern:

**Low throughput by design — each mutation cycle appends a cryptographic HIPAA/GDPR compliance proof to the immutable audit chain. Rate is set by compliance requirements, not hardware limits.*

Core Design Insight: A glass frog has transparent skin — its internal organs are permanently visible while the frog itself remains alive and functional. GlassFrog makes the audit chain permanently visible and immutable while the surface itself continues to mutate. Regulators can verify the complete mutation history; attackers cannot exploit it.

Key Mechanism: Dual-state architecture: the observable surface mutates on every cycle (Kali Invariant maintained); the audit chain is cryptographically immutable. Each mutation cycle produces a HIPAA/GDPR compliance proof appended to the chain. The proof attests that: (a) the surface mutated, (b) the previous state was compliant, (c) the new state is compliant, and (d) no PHI was exposed during the transition.

Crown Jewel Claim: The only mutation profile that provides HIPAA/GDPR audit compliance as a cryptographic proof rather than a log entry. The proof is machine-verifiable by any regulator with the chain public key. No manual audit interpretation required.

Integration Pattern: `engine.register(Box::new(GlassFrogTarget::new("phi-api")), "hipaa");`

Profile 0x09: ⚡ ElectricEelGrid — COLO / Data Centre / Side-Channel

Latency p50	Throughput	Profile ID
58.33µs (Sachs)	82.0k/s (Sachs)	0x09

Core Design Insight:

Key Mechanism:

Crown Jewel Claim:

Integration Pattern:

†Sachs (steady-state) mode. All benchmarks commodity x86_64. Hunter and Main Organ modes increase mutation rate at reduced throughput as threat escalates.

Core Design Insight: An electric eel generates high-voltage pulses not just for offence but as a continuous electromagnetic field used for navigation and prey detection. ElectricEelGrid models this: the workload itself emits observable signals (power consumption, thermal patterns, electromagnetic emissions) that a COLO attacker can exploit. ElectricEelGrid's mutation randomises these signals as a primary security property.

Key Mechanism: Computational workload randomisation alongside surface mutation. Each mutation cycle randomises the timing, intensity, and pattern of computational operations so that cross-correlation between observable workload signals and internal state approaches zero. Power proof operation completes in 1.595µs.

Crown Jewel Claim: The only available product defending the power side-channel in COLO environments. Red team cross-correlation of workload vs power observations: 0.03% deviation — below the measurable threshold

for side-channel exploitation. This property has no equivalent in any other commercial or research security product.

Integration Pattern: `engine.register(Box::new(ElectricEelGridTarget::new("dc-node")), "colo");`

Profile 0x0A: 🐉 LeviathanGrid — Nation-Scale / 16-Node Distributed

Latency p50	Throughput	Profile ID
143.9µs p50	7.07k/s	0x0A

Core Design Insight: The leviathan of myth was so vast that its movement changed the topology of the sea itself. LeviathanGrid applies scale as a security property: a 16-node distributed grid mutates simultaneously, rewiring its entire observable topology on every cycle. An attacker mapping the topology at time t finds a different topology at t+1.

Key Mechanism: 16-node simultaneous mutation with full topology rewire. Grand hash computation — SHA3-256 of all 16 node fingerprints combined — completes in O(1) time (43.75µs) regardless of individual fingerprint sizes. This provides an estate-level integrity check: a single value that confirms all 16 nodes mutated correctly and in sync.

Crown Jewel Claim: 16-node simultaneous mutation in 143.9µs — the entire distributed grid rotates before a single network round-trip completes. The SolarWinds attack required 14 months of patient topology mapping across thousands of nodes. LeviathanGrid makes that model permanently stale every 143.9µs.

Integration Pattern: `engine.register(Box::new(LeviathanGridTarget::new("nation-grid")), "scale");`

3. KALICORETARGET — PROFILE 0XFF

KaliCoreTarget is the meta-profile that orchestrates all registered profiles simultaneously. It is not a surface profile — it has no domain-specific mutation logic. It is the governing orchestration layer that receives a single trigger and fans it out to all registered MutationTarget implementations.

3.1 Estate-wide rotation

When KaliCoreTarget receives a mutation trigger, it calls trigger_mutation() on every registered profile in a single scheduling window. The scheduling window completes in under 200 microseconds for any combination of profiles. This is the coordinated defence property: an attacker cannot observe a pre-rotation state on any surface after a KaliCoreTarget trigger.

Operation	Time	What it achieves
Single profile mutation (MantisNet)	10.31µs	Fastest single-surface rotation
All 10 core profiles simultaneously	< 200µs (estate-wide)	No surface in the estate survives the trigger
16-node LeviathanGrid grand hash	43.75µs	Full distributed topology integrity check

GlassFrog HIPAA audit chain verify	164.3µs	Full compliance proof chain verification

3.2 ProVerif-verified orchestration

The KaliCoreTarget orchestration model was analysed as part of the cascade authentication model in ProVerif. The verified property: all registered profiles receive the mutation trigger within the scheduling window, and no profile can receive a trigger from KaliCoreTarget that it could not independently verify as originating from a valid KaliCoreTarget instance. Result: formally correct.

4. CROSS-PROFILE CONSIDERATIONS

4.1 Entropy independence

When multiple profiles are registered simultaneously, each receives a statistically independent entropy slice from the EntropyManager: SHA3-256(entropy_bundle || profile_id || target_id || cycle_seq). No profile's mutation inputs can be inferred from another's, even if they share the same entropy pool.

4.2 Profile combinations

Profiles are designed to be deployed in combination. A typical enterprise deployment might register SquidShield (payment surfaces), GlassFrog (PHI surfaces), AnglerShield (API surfaces), KrakenNet (AD surfaces), and KaliCoreTarget (estate-wide orchestration) simultaneously. Each profile operates independently; KaliCoreTarget can trigger all of them together.

4.3 TEE adapter compatibility

All 11 profiles are compatible with all 5 TEE adapters. The profile implementation is adapter-agnostic — it calls the TEE adapter trait and receives an attestation quote without knowing which hardware produced it. Profile selection and TEE adapter selection are completely independent deployment decisions.

5. CONCLUSION

The 11 ACSE profiles cover the full spectrum of enterprise surface classes — from the fastest intrusion response (MantisNet at 10.31µs) to the most scalable distributed defence (LeviathanGrid at 16-node simultaneous rotation) to the most compliance-rigorous (GlassFrog with per-cycle HIPAA/GDPR proof). Every profile enforces the Kali Invariant. No profile requires application code changes to swap.

The crown jewel claims listed in this paper are not marketing assertions. They are technical properties verifiable against the test suite, the Criterion benchmarks, and the red-team results documented in WP-05.