NEXILIS · ENCLAVE

PRODUCT BRIEF · APRIL 2026 · REVISION 1.0

The room inside the *app.*

Bank-grade encrypted communications embedded inside the host application — covering workforce, customer-to-customer, and named relationship-manager threads. One cryptographic fabric. One identity system. Sovereign-hostable.

> *Where trusted conversations live.*

PT EASYSOFT INDONESIA
JAKARTA — NEXILIS.IO

CONTENTS

Nexilis Enclave — *in ten movements.*

This brief is a technical and commercial reference for Nexilis Enclave — the secure-communications product in the Nexilis portfolio. It is written for chief information security officers, heads of workforce technology, heads of priority and private banking, and the procurement committees who evaluate them. It is organised so that a reader who has thirty minutes can read sections 01, 03, 04, and 09 and come away with a correct picture of what Enclave is, how it is built, and what it costs to own.

HOW TO READ THIS DOCUMENT

Sections 01 and 02 set up the category and define the product in plain language. Sections 03, 04, and 05 are the technical core — they belong to the security architect on the evaluation team. Section 06 is the composition story for procurement teams evaluating Enclave alongside Sentinel, Reach, and Plaza. Sections 07 and 08 are the competitive and regulatory frame. Sections 09 and 10 carry the commercial and operational detail a procurement lead needs to model the deal.

01 — THE PROBLEM

Conversations that leak *the institution.*

A bank's most sensitive conversations — the relationship manager advising a private-banking client on a succession plan, the fraud officer coordinating across three branches to freeze an account, the two treasury staff confirming a large-value instruction between themselves — do not happen where the bank thinks they do. They happen on the WhatsApp threads the staff already have open. They happen on SMS. They happen on the one consumer app everyone in the branch uses because it is easy. They happen, in short, in rooms the institution does not own.

This is not a failure of training. It is a failure of architecture. The institution has invested in core banking, in fraud systems, in mobile apps, in contact centres, in device management — and yet the conversations that move risk, relationship value, and regulatory liability still flow through external consumer channels because no one ever built the *internal* channel properly. The external channels are convenient. The internal ones, where they exist at all, are fragmented: a secure messaging app for the compliance team, an MDM for the field officers, a separate video platform for branch managers, a priority-banking CRM with its own comms pane that nobody uses. Four tools, four identity systems, four audit trails — so staff default to the one tool that works everywhere, which is the one the institution cannot see.

The consequences are no longer hypothetical

Between 2021 and 2025, the US Securities and Exchange Commission and Commodity Futures Trading Commission levied more than USD 3.5 billion in combined penalties — with additional actions by FINRA — against more than one hundred firms for a single category of failure: recordkeeping violations arising from staff conducting business communications on personal devices and consumer messaging platforms. The UK Financial Conduct Authority, the European Securities and Markets Authority, and the Monetary Authority of Singapore have opened parallel enforcement tracks. These are not edge cases. These are the largest and most sophisticated institutions in the world, losing billions, because their staff used WhatsApp to talk about work.

Indonesia is not exempt from this trajectory. Otoritas Jasa Keuangan's POJK 11/POJK. 03/2022 on the Implementation of Information Technology by Commercial Banks, and its implementing circular SEOJK 29/SEOJK.03/2022 on Cyber Security and Resilience for Commercial Banks, already require risk-based cyber-resilience governance. Bank Indonesia's SNAP SDK guidance pushes in the same direction for payments. The Personal Data Protection Act adds a lawful-basis and data-sovereignty overlay that commercial messaging platforms cannot satisfy. The regulator is not a question of *whether*, only of *when*, the enforcement window opens in Jakarta on the same category that cost Wall Street more than three-and-a-half billion dollars.

USD 3.5B+

PENALTIES (2021–2025)

Combined SEC and CFTC enforcement actions against more than one hundred firms for off-channel business communications, with further FINRA activity on top.

5–7

SYSTEMS PER CASE

Average number of disconnected platforms a single sensitive conversation crosses before resolution.

0

UNIFIED AUDIT OWNERS

Number of institutions examined during this review that were able to produce a single regulator-ready conversation record on demand.

The category the market has misnamed

For two decades the industry has framed this as a *secure-messaging* problem and sold secure-messaging products against it. That framing is incomplete. Secure messaging, as sold by the global incumbents, addresses one mode of the problem — staff-to-staff communication — and leaves the other two untouched. It does not address customer-to-customer conversations happening inside the bank's own app. It does not address the persistent one-to-one thread between a private-banking client and their relationship manager, where the franchise value of wealth management actually lives. And it does not provide the *single* cryptographic fabric across all three modes that makes audit, key rotation, and policy enforcement tractable for a regulated institution.

The correct framing is not *secure messaging*. It is *containment*: the institution building a room, inside the application it already owns, where every conversation of consequence happens under one identity system, one audit trail, and one policy engine — and cannot happen anywhere else. That room is an enclave. This product is Nexilis Enclave.

02 — THE PRODUCT

What Enclave is, *in one paragraph.*

Nexilis Enclave is an embedded communications fabric — a software layer that sits inside the institution's existing mobile application and delivers bank-grade encrypted messaging, voice, video, group threads, and file exchange across three modes: workforce to workforce, customer to customer, and customer to a named workforce counterpart. Every conversation carried over Enclave is bound to a verified identity, observed by a single policy engine, recorded in a single regulator-ready audit stream, and encrypted end-to-end under keys the institution — not a foreign vendor — is able to rotate, escrow, and retire. The product can be embedded into an existing banking app, deployed as a white-label companion app, or delivered as a hardened sovereign build for government and defence.

What Enclave replaces

- The WhatsApp group used by a regional manager and nine branch heads to coordinate a product rollout.
- The SMS thread between a relationship manager and a private-banking client about a structured product.
- The consumer video-call app used by a compliance officer to interview a new high-net-worth applicant.
- The informal payment-memo message a customer sends a family member about a transfer, today done on a social network.
- The point-to-point enterprise-messaging tools (Wickr, Element, Signal Enterprise, Threema Work) a security team licenses to solve only the workforce slice of the problem.
- The embedded-chat SDKs (Sendbird, Stream, CometChat) a product team licenses to solve only the customer slice.
- The bespoke relationship-manager chat panel inside a CRM, which most staff abandon within six months.

What makes Enclave different

ONE FABRIC

Three modes, one cryptographic surface.

Workforce-to-workforce, customer-to-customer, and customer-to-named-workforce all share the same key hierarchy, the same identity primitives, the same audit stream, and the same policy engine. This is what no point-solution competitor delivers, and it is what makes regulatory proof possible.

ONE IDENTITY

Bound to the institution's own identity graph.

Every participant — staff or customer — authenticates against the institution's identity provider (for staff) or the institution's digital-onboarding KYC record (for customers). No Enclave conversation is possible without a verified, bound, enrolable party on both sides.

EMBEDDED

Inside the app the user already opened.

Enclave ships as an SDK that embeds inside the bank's existing mobile application, or as a white-label companion app where an embedded deployment is not feasible. Users do not install a second app. They do not change habit. They open the bank app and find a room already built.

SOVEREIGN

The institution holds the keys.

Enclave is built by PT Easysoft Indonesia on a deliberately minimised and fully disclosed cryptographic supply chain — standard-defined primitives from auditable, widely reviewed sources, with no closed-source or unreviewed third-party code in the ciphertext path. The institution can host the control plane, the relay, and the key management service in its own data centre or sovereign cloud. No foreign vendor holds escrow over the ciphertext.

> *Nexilis Enclave is bank-grade encrypted communications embedded inside the app — covering workforce, customer-to-customer, and named relationship-manager threads. One fabric, one identity, sovereign-hostable.*

PORTFOLIO POSITIONING — NEXILIS PRODUCT ARCHITECTURE, APRIL 2026

03 — THE THREE MODES

Workforce. Customer. *Named counterpart.*

Most secure-communications products address one mode and leave the other two to other vendors. Enclave carries all three on one fabric. The three modes are distinct in purpose, user interface, and commercial metric — but they share the same cryptographic primitives, the same identity provider, and the same policy plane. This section defines each mode, the persona it serves, and the operational pattern it replaces.

W ↔ W

Workforce to workforce

Encrypted, identity-bound communication between staff.

Direct and group messaging, voice and video calls, file exchange, and broadcast channels between authenticated workforce users — head office to branch, compliance to front line, treasury desk to operations.

Competes with Wickr, Signal Enterprise, Element, Salt, Threema Work, and the workforce-comms module of Microsoft Teams.

C ↔ C

Customer to customer

Encrypted peer-to-peer inside the bank's own app.

Encrypted conversations between two verified customers of the institution — payment memos, transfer confirmations, referrals, community banking groups, family-account coordination.

Competes with Sendbird, Stream, and CometChat, none of which carry identity verification at the bank's KYC level and none of which share a key hierarchy with workforce comms.

C ↔ W

Customer to named workforce

Persistent identity-bound thread with a named staff counterpart.

The one-to-one thread that lives for years between a private-banking client and their relationship manager, or between a corporate-banking client and their named account officer. Persistent, identity-bound, audit-captured.

No standalone competitor addresses this correctly — today it lives inside a CRM chat panel no one uses, or worse, on WhatsApp.

The boundary rule: relationship versus service moment

Because the customer-to-workforce axis overlaps with a contact centre, the boundary between Enclave and Nexilis Reach is stated as a rule the institution can enforce in product design. **Enclave is identity-bound, persistent, and tied to a named counterpart** — a relationship manager, an account officer, a private-banking concierge. **Reach is queue-bound, transactional, and routed to whichever agent is free.** Both can live in the same bank application, using the same underlying comms primitives — Reach's messaging transport runs on the Enclave fabric — but the products are sold on different metrics: Enclave on seats and persistent threads, Reach on conversations and engagement outcomes.

> **WHY THE THREE-MODE FABRIC MATTERS COMMERCIALLY**
>
> A workforce-only secure-messaging purchase solves one vector. A customer-chat-SDK purchase solves another. A relationship-manager CRM purchase pretends to solve a third. Three vendors, three contracts, three audit systems, three sets of key escrow, three renewal cycles. Enclave is one contract. That consolidation, on its own, is why the commercial evaluation simplifies well before the technical review begins.

Which mode to activate first

Most institutions activate Enclave in one of three entry patterns. A **regulatory-pressured bank** typically activates W↔W first to close the SEC-style enforcement risk on off-channel comms. A **priority- or private-banking franchise** typically activates C↔W-named first to bring the relationship-manager thread inside the institution's audit perimeter. A **consumer-scale digital bank** typically activates C↔C first to deepen engagement inside the app and reduce dependence on external social-messaging platforms. The three-mode fabric supports all three sequences without architectural change.

04 — ARCHITECTURE

The six-layer *enclave fabric.*

Enclave is a layered product. The layers are not marketing artefacts — they correspond to the engineering teams, the interface contracts, and the control-plane responsibilities that the institution's integrators will encounter. Each layer is independently testable, independently upgradable, and independently auditable. Sentinel's hardening envelope applies below Layer 1; Reach and the host banking application sit above Layer 6.

L1 Identity & Attestation	**Who is on each end of the conversation.** FIDO2 / passkey for staff, institution KYC anchor for customers, device attestation via Play Integrity and iOS App Attest, session binding. Every participant in every conversation is bound to a verified, attested identity on an attested device before a single byte of plaintext exists.
L2 Key Management	**How keys are generated, sealed, and rotated.** Per-install device keys sealed to hardware trust (Android Keystore with StrongBox or TEE; iOS Secure Enclave). Per-thread message keys derived via Double Ratchet. Per-session transport keys delivered via double-envelope. Institution-owned KMS for escrow, rotation, and retirement.
L3 Transport & Relay	**The carrier.** Metadata-minimised relay, forward-secret session establishment, mutual TLS to institution-hosted edge, no plaintext ever present on the server. Works across low-bandwidth, metered, and intermittently connected networks.
L4 Conversation Primitives	**Chat, voice, video, groups, files.** One-to-one and group messaging with delivery and read receipts, encrypted voice and video with SRTP, group-call up to institutional policy cap, encrypted file exchange with DLP hooks, self-destructing and confidential-view messages, broadcast channels.
L5 Policy & DLP	**What is allowed to happen.** Risk-adaptive policy engine — attributes and conditions evaluated at every action (send, forward, screenshot, export, save, open-on-device). DLP with lexical, pattern, and content classification. Safe-view, watermarking, clipboard and export control. Policies attached to role, to thread, and to conversation content.
L6 Evidence & Audit	**The regulator-ready record.** Unified timeline per participant, per thread, per case. Tamper-evident log chain, hash-sealed records, exportable in regulator-ready formats. Supports the full off-channel-communications evidentiary bar as defined by US SEC, UK FCA, and ESMA rulings, and maps forward to anticipated OJK electronic-communications recordkeeping requirements.

WHAT IS NOT ENCLAVE

Device hardening, root and jailbreak detection, malware scanning, anti-tamper, and DEX protection are *not* in Enclave. Those are Sentinel's job. Enclave assumes Sentinel runs below it and consumes Sentinel's device-posture signal to feed Layer 5 policy decisions. The two products ship together in the Trusted Channel and TrustLink bundles.

05 — CRYPTOGRAPHIC MODEL

Keys, devices, *and provenance.*

The cryptographic design of Enclave is built to withstand a specific class of regulated-institution evaluation — one where the CISO's team will read the key-derivation chain, one where the internal audit team will test evidence replay, and one where the state security agency's technical reviewer will ask where every key in the system ultimately lives. This section summarises the model at the level a technical evaluator needs; a detailed cryptographic specification is provided under NDA.

Identity anchors and device binding

Every Enclave participant — whether workforce or customer — is rooted in an identity anchor. For workforce, that anchor is the institution's identity provider: OIDC or SAML, with FIDO2 passkey as the authenticator. For customers, the anchor is the institution's own digital-onboarding KYC record — the same identity bound to the customer's banking relationship. Both anchors commit to a per-install device public key at first enrolment. That device key is generated in hardware — Android Keystore with StrongBox where available or the trusted execution environment otherwise, and iOS Secure Enclave — and never leaves the device.

Message and session key hierarchy

Message-layer encryption uses a Double Ratchet construction, seeded from a prekey exchange at first contact between two identities. Every message uses a fresh chain key; compromise of a single device at time t cannot decrypt messages exchanged before t (forward secrecy) and cannot decrypt messages exchanged after t once the ratchet has advanced (post-compromise security). Session transport to the relay uses a mutual-TLS channel with per-session ephemeral keys; bulk ciphertext is AEAD under AES-256-GCM or ChaCha20-Poly1305 depending on platform policy.

Sovereign key management

The institution operates an Enclave KMS — deployable on-premises, in sovereign cloud, or in Telkom Sigma — which holds the institution's signing keys, the relay's signing keys, and the policy-signature keys. The institution can escrow, rotate, or retire any key in the hier-

archy without vendor dependency. Nexilis as a vendor does not hold cryptographic escrow over any institution's ciphertext; the audit of this claim is structural, not contractual, because the relay is explicitly designed to be unable to decrypt message payloads.

CRYPTO PROVENANCE — THE SOVEREIGNTY CLAIM

The cryptographic primitives used in Enclave — AES-GCM, ChaCha20-Poly1305, X25519, Ed25519, HKDF, and the Double Ratchet — are standards-defined. The implementation is built by PT Easysoft Indonesia on a deliberately minimised cryptographic supply chain drawing from auditable, widely reviewed sources; the complete Software Bill of Materials for the ciphertext path, together with per-component provenance and upstream versions, is disclosed in full to qualified institutional evaluators under NDA. The product contains no closed-source or unreviewed third-party code in the ciphertext path. This is the claim behind the sovereign-hostable positioning and is testable by independent review.

Evidence and replay

Every conversation event — send, receive, forward, screenshot attempt, export, policy decision — is captured into a tamper-evident log chain on the Layer-6 evidence plane. Each entry is individually hash-sealed and chained to its predecessor; the chain's root is sealed periodically into an append-only ledger that can be externally witnessed. On demand, the institution can replay a full case timeline — every participant, every action, every policy decision — into a regulator-ready export. This is the capability that today's fragmented channel stack cannot produce and that US SEC enforcement actions have demonstrated regulators will demand.

06 — PORTFOLIO COMPOSITION

Enclave inside the *Nexilis portfolio.*

Enclave is sold three ways: standalone, as a component of two vertical platforms (Trusted Channel for BFSI and TrustLink for government and defence), and as a component of a sharp bundle aimed at relationship-led banks (the Relationship Banking Stack). The composition logic is deliberate — every Nexilis product can be sold alone, but each vertical platform packages the set that a particular market buys as a unit.

BFSI VERTICAL

Trusted Channel

`Sentinel + Enclave + Reach`

The full banking stack. Sentinel hardens the device and the session; Enclave carries every sensitive conversation; Reach carries the service-moment and outbound engagement traffic. One contract, one integration, one commercial partner for the full mobile-first trusted lane.

GOVERNMENT & DEFENCE

TrustLink

`Sentinel + Enclave`

The sovereign workforce stack. Sentinel guarantees device integrity in BYOD and mixed-device field environments; Enclave carries command, coordination, and classified-adjacent communications. Reach is out of scope — government buyers do not buy customer contact-centre infrastructure from this vendor.

PRIORITY & PRIVATE

Relationship Banking Stack

`Sentinel + Enclave`

A focused bundle for BPDs, private banks, and priority-banking franchises where the relationship-manager thread is the franchise asset. Sentinel hardens the RM's and the client's device; Enclave carries the named persistent C↔W thread with a regulator-ready audit stream.

Enclave sold standalone

Enclave is also available as a standalone product. A security team that has already standardised on other mobile-security and engagement vendors can license Enclave as the communications fabric alone, integrating it against its existing identity provider, its existing

audit systems, and its existing banking application. A standalone deployment is a natural step for institutions that are part-way through a multi-year contract with an incumbent secure-messaging vendor and are beginning to look at the renewal. Enclave's three-mode fabric is the architectural differentiator no workforce-only product is structured to provide, and the standalone licence makes it possible to introduce that fabric without waiting for the incumbent term to expire.

Path to a fuller deployment from a standalone start

A standalone Enclave deployment typically surfaces, during evaluation, a set of adjacent questions the institution does not intend to leave unanswered. The question of device-posture trust — *what happens if the device is rooted, what happens if the app is tampered with, what happens if a keyboard-injection attack captures a plaintext draft* — sits in Sentinel's territory, and institutions that have completed an Enclave evaluation are typically in a position to open the Sentinel conversation within six months. The question of service-moment traffic — the inbound ticket that belongs in the same trusted channel as the sensitive conversation — sits in Reach's territory, and is the third adjacency an institution is usually ready to close once the first two are in place.

> **ONE NOTE ON PROCUREMENT LANGUAGE**
>
> Buyers and procurement teams sometimes ask whether Enclave is "the secure-messaging module" of Trusted Channel or a standalone product. The answer is both — and the correct framing is that Enclave is a product in its own right, addressed and sold by itself, and that Trusted Channel is a bundled commercial offering composed of three of Nexilis's standalone products. The same SKU structure applies as to Microsoft's portfolio, where Teams is both a standalone product and a component of Microsoft 365.

07 — COMPETITIVE FRAME

Why none of the incumbents *cover all three modes.*

Enclave does not compete against a single incumbent. It competes against the unavoidable vendor sprawl that a regulated institution today has to assemble because no single product on the market delivers all three communications modes on one cryptographic fabric. The table below is the competitive landscape as an institutional evaluation would assemble it.

COMPETITOR	PRIMARY MODE	W↔W	C↔C	C↔W-NAMED	STRUCTURAL GAP VERSUS ENCLAVE
AWS Wickr (SaaS) / Wickr Enterprise (self-hosted)	W↔W	YES	NO	NO	Workforce-only across both tiers. No customer-facing surface. No embedding into a banking app. AWS Wickr (cloud) relies on AWS regions; Wickr Enterprise is self-hostable but is a general-purpose secure-messaging product rather than an institution-anchored, KYC-bound embedded fabric. Sovereignty posture for the cloud tier does not meet Indonesian BFSI data-residency expectations; the self-hosted tier addresses hosting but not the customer-side modes.
Signal Enterprise / Element	W↔W	YES	NO	NO	Workforce only. No identity binding to an institution's KYC record. No policy engine mature enough for BFSI DLP. Consumer-lineage brand heritage that complicates institutional evaluation.
	W↔W	YES	NO	NO	Workforce only. Stronger

COMPETITOR	PRIMARY MODE	W↔W	C↔C	C↔W-NAMED	STRUCTURAL GAP VERSUS ENCLAVE
Salt Communications / Threema Work					enterprise posture than Signal-lineage peers but identical structural gap on the customer-side modes.
Microsoft Teams	W↔W	YES	NO	NO	Office-productivity-lineage. Not designed for embedding in a third-party banking app. Sovereignty and data-residency caveats in Indonesia. No customer-side surface.
Sendbird / Stream / CometChat	C↔C	NO	YES	PARTIAL	Customer-chat SDKs. No identity anchor to a bank's KYC record. No workforce surface. No institutional audit model. Relay is vendor-hosted; ciphertext sovereignty story does not exist.
Twilio Conversations	Transport	PARTIAL	YES	PARTIAL	Plumbing, not a product. No enclave posture, no identity model, no audit surface, no sovereign option. A developer tool for building parts of what Enclave ships as a product.

COMPETITOR	PRIMARY MODE	W↔W	C↔C	C↔W-NAMED	STRUCTURAL GAP VERSUS ENCLAVE
CRM chat panels (Salesforce, Dynamics)	C↔W-named	NO	NO	PARTIAL	A chat surface welded onto a CRM. Low adoption in practice. No end-to-end encryption. No audit surface that survives a regulator's examination.
Nexilis Enclave	**All three**	YES	YES	YES	**Three modes on one fabric. Institution-anchored identity. Sovereign KMS. In-house crypto path with no foreign library dependency.**

Where the competition is strongest

Two competitors warrant specific treatment. Wickr is a mature and capable product on the workforce mode alone, and an institution already operating under a multi-year Wickr contract is unlikely to reopen the question on comparison alone. The architectural case, rather, is that a single-mode workforce platform addresses one-third of the sensitive-conversation problem — the customer-to-customer and customer-to-named-workforce modes remain outside its scope, typically handled by separate stacks with separate key hierarchies and separate audit systems. Enclave consolidates the three modes into one cryptographic fabric, one identity model, and one audit stream; the total cost of ownership across the three lines falls below the combined cost of three stacked vendors within the first renewal cycle.

08 — REGULATORY MAPPING

Off-channel enforcement and *the POJK / PDP stack.*

Enclave is designed to satisfy three concentric regulatory frames: the global off-channel-communications precedent (SEC, CFTC, FCA, ESMA, MAS); the Indonesian financial-services framework (OJK POJK 11/POJK.03/2022 and its implementing circular SEOJK 29/SEOJK.03/2022, Bank Indonesia SNAP SDK); and the Indonesian data-protection and data-sovereignty overlay (UU PDP). Each control in Enclave maps to one or more requirements in each frame.

REGULATORY REQUIREMENT	JURISDICTION / SOURCE	ENCLAVE CONTROL MAPPING
Recordkeeping of business electronic communications	SEC Rule 17a-4 CFTC Regulation 1.31	Layer 6 tamper-evident log chain; per-participant, per-thread, per-case timelines; regulator-ready export formats.
Prohibition on off-channel business communications for registered personnel	SEC enforcement pattern 2021–2025 FCA SYSC 10A	Policy-plane enforcement of permitted-channel policy at device level; exception logging; staff-channel-of-record captured in Enclave.
IT governance and risk-based cybersecurity framework	POJK 11/POJK.03/2022 (IT Implementation by Commercial Banks)	Risk-adaptive Layer-5 policy engine; attestation-driven access; evidence of control effectiveness in Layer 6.
Cyber security and resilience controls, incident reporting	SEOJK 29/SEOJK.03/2022 (Cyber Security & Resilience for Commercial Banks)	End-to-end encryption; device attestation; session binding; institution-held keys; sovereign hosting option; cyber-

REGULATORY REQUIREMENT	JURISDICTION / SOURCE	ENCLAVE CONTROL MAPPING
		incident event stream into the Layer-6 evidence plane for 24-hour initial notification and 5-day detailed reporting.
Payment-system data governance	BI SNAP / BI PBI 23/6/PBI/2021	Domestic-residency deployment; no cross-border ciphertext; institution-controlled key lifecycle.
Lawful basis for personal-data processing in electronic communications	UU PDP (Indonesia)	Customer identity anchored to KYC record with lawful-basis stamp; data-minimisation in relay metadata; deletion and portability APIs.
Cross-border data-transfer controls	UU PDP Article 55–57	Sovereign-hosted KMS and relay; no foreign-jurisdiction escrow; no cross-border transfer of ciphertext or plaintext.

REGULATORY REQUIREMENT	JURISDICTION / SOURCE	ENCLAVE CONTROL MAPPING
Critical-information-infrastructure obligations	PP 71/2019 & BSSN guidance	On-premises and sovereign-cloud deployment; disclosed Software Bill of Materials and cryptographic supply chain; no closed-source or unreviewed third-party code in the ciphertext path.

THE INDONESIAN ENFORCEMENT OUTLOOK

OJK has not yet opened a publicised off-channel-communications enforcement track comparable to the US SEC's 2021–2025 action line. The direction of travel across the published authority and guidance is nevertheless clear: POJK 11/POJK.03/2022 establishes the IT-governance authority, SEOJK 29/SEOJK.03/2022 tightens the cyber-resilience and incident-reporting expectation, and OJK's informal guidance on electronic-communications governance is moving. The enforcement window is a question of when, not whether. Institutions that move before the window opens are positioned; institutions that wait will move under penalty.

What Enclave does not claim

Enclave does not claim to discharge the institution's regulatory obligations — no vendor product can. Enclave claims to provide the controls the institution needs in order to discharge those obligations, and to produce the evidence the institution needs when a regulator asks. The distinction is important: the responsibility stays with the institution, and Enclave is architected to make that responsibility tractable.

09 — COMMERCIAL STRUCTURE

Foundation. Growth. *Enterprise.*

Enclave is packaged in a three-tier ladder mirroring Sentinel and Reach — Foundation, Growth, and Enterprise — structured so institutions can begin at Foundation with a single mode and expand as governance scope, scale, and sovereignty requirements deepen. The commercial metric at Foundation and Growth is active seats or active customers; the commercial metric at Enterprise is a committed platform fee with a seat band. Pricing below is a reference range; the actual commercial structure is set in the quotation against the institution's specific seat profile, deployment topology, and support tier.

TIER 01 · FOUNDATION

Foundation

Activate one mode; prove the fabric.

- One communications mode — typically W↔W or C↔W-named.
- Chat, voice, group up to policy cap.
- Institution identity provider integration.
- Policy engine at baseline control set.
- Audit export at monthly cadence.
- Standard SLA; business-hours support.
- Shared-tenant relay; sovereign-cloud option available.

TIER 02 · GROWTH

Growth

Activate two modes; add video, DLP, engagement.

- Two communications modes on one fabric.
- Full audio, video, groups, broadcast channels.
- DLP engine with lexical and pattern classifiers.
- Policy engine with risk-adaptive attributes.
- Audit export at weekly cadence; continuous streaming to SIEM.
- Enhanced SLA; extended-hours support.
- Dedicated relay tenancy; on-premises option.

TIER 03 · ENTERPRISE

Enterprise

All three modes; sovereign KMS; full governance.

- All three communications modes on one fabric.
- Sovereign KMS in the institution's data centre.
- Full DLP with content-classification and watermarking.
- Custom policy library with regulatory export packs.
- Continuous SIEM streaming and case-replay export.
- 24×7 premium support with on-site response option.
- Dedicated cryptographic advisory and annual control audit.

Commercial metrics and sizing

For the workforce mode, Enclave is sized on named authenticated seats. For the customer-to-customer mode, Enclave is sized on the addressable active-customer population of the host application — with a pricing grade that falls sharply at scale (above 500k customers the per-customer unit is a fraction of the workforce seat cost). For the customer-to-named-workforce mode, Enclave is sized on the number of named relationship-management pairings — typically the priority- or private-banking RM book. A typical three-mode deal for a

mid-tier Indonesian BPD (2,000 workforce, 800,000 customers, 120 RM pairings) prices at Growth tier in the mid- to high-single-digit IDR billion range per annum, before sovereign-hosting surcharges.

Add-ons available at any tier

- **Sovereign-hosting surcharge** — on-premises or in-country sovereign cloud; includes KMS co-residency and sealed relay.
- **Premium cryptographic audit** — annual independent review of implementation, key lifecycle, and evidence integrity.
- **Regulatory-pack updates** — continuous delivery of policy templates tracking OJK, BI, and BSSN regulatory evolution.
- **Relationship-Manager Concierge integration** — deep integration with the institution's CRM for the C↔W-named thread.
- **Defence-grade communications pack** — incremental hardening and custom policy library for TrustLink-deployed configurations.

10 — DEPLOYMENT & SUPPORT

Deployment, operations, *and support.*

Enclave is delivered in one of three deployment topologies — embedded SDK, white-label companion app, or sovereign build — and runs in one of three hosting modes. The choice of topology is determined by the institution's existing mobile application estate and integration appetite; the choice of hosting mode is determined by regulatory requirement and sovereignty preference.

Three deployment topologies

TOPOLOGY A

Embedded SDK

Enclave embeds as an SDK inside the institution's existing mobile banking application. Minimum application-footprint impact; maximum user-experience continuity. Preferred for institutions with a mature internal app team. Integration effort is measured in weeks for Foundation, not quarters.

TOPOLOGY B

White-label companion app

Enclave ships as a separate institution-branded mobile application, signed under the institution's developer account. Used when the host banking app cannot absorb additional surface for business or architectural reasons. Common for workforce-only deployments where the user population is staff, not customers.

TOPOLOGY C

Sovereign / defence build

Custom-hardened build produced against an institution-specific protection profile. Reduced feature set in exchange for elevated assurance — no analytics, no crash telemetry, no external third-party dependencies. Used for TrustLink deployments in government, defence, and critical-infrastructure contexts.

HOSTING

Three hosting modes

Shared sovereign cloud (Telkom Sigma, Biznet, or equivalent in-country operator), dedicated sovereign cloud, or full on-premises. The KMS and the evidence plane are always co-resident with the chosen relay tier; plaintext never crosses the institution's sovereignty boundary.

Integration and onboarding

A typical Foundation deployment — one mode, one integration point, shared sovereign-cloud hosting — onboards in six to ten weeks from contract signing to first live conversation. A Growth deployment — two modes, SIEM integration, dedicated tenant — typically lands at twelve to sixteen weeks. A full Enterprise deployment with sovereign KMS and on-premises relay is a three- to five-month program. The deployment team is composed of Nexilis platform engineers, a dedicated solutions architect, the institution's own identity and mobile-app teams, and where relevant the institution's preferred systems integrator.

Support and service levels

SERVICE LEVEL	FOUNDATION	GROWTH	ENTERPRISE
Support hours	Business	Extended	24 × 7
Severity-1 response	4h	1h	15m
Severity-1 workaround	24h	8h	4h
Target availability	99.5%	99.9%	99.95%
Dedicated solutions architect	—	Fractional	Named
Annual cryptographic review	—	Optional add-on	Included
On-site response option	—	—	Included (Jakarta / Bandung / Surabaya)

REFERENCE ARCHITECTURE BACKING THE ENTERPRISE SLA

The 99.95% availability target at Enterprise tier is supported by a documented reference architecture: active-active deployment across two in-country availability zones, synchronous replication of the evidence plane, asynchronous replication of the relay state, and automated failover under a measured recovery-time objective of fifteen minutes for the control plane and sixty seconds for the relay. The target availability and severity-response times are backed by an Indonesia-based 24×7 support operation with Bahasa Indonesia and English coverage, fielded by PT Easysoft Indonesia platform engineers escalating to named solutions architects. The full reference-architecture specification, the HA/DR run-book, and the staffing model for each tier are included in the technical-evaluation package provided under NDA.

Evidence, certifications, and deployment references

A product brief is the first document in an institutional evaluation; it is not the last. The evidence that backs the claims in this brief — deployment references, certification status, penetration-test summaries, cryptographic audit reports, the Software Bill of Materials,

the HA/DR reference architecture, and the policy-library source — is assembled into a separate Technical Evaluation Companion, released to qualified institutional evaluators under mutual non-disclosure.

CERTIFICATION POSTURE

Enclave's certification posture is tracked openly and included in every technical-evaluation pack. The current status across the certifications most commonly asked about in Indonesian BFSI and government evaluation is: ISO/IEC 27001 — in scope, audit cycle active; SOC 2 Type II — in scope, reporting period active; PCI-DSS (relevant for BFSI scope) — assessment in progress; BSSN evaluation (relevant for TrustLink / critical-information-infrastructure deployments) — submission in progress; FIPS 140-3 cryptographic module validation — planned for the post-quantum migration cycle. The up-to-date certification matrix, including the assessor name, audit period, and accessible attestation letter for each line, is provided in the technical-evaluation pack. Where a certification is not yet held, the expected attainment date and the compensating controls relied upon in the interim are documented alongside.

DEPLOYMENT REFERENCES

Nexilis Enclave is a product of a young and focused vendor, and its deployment base reflects that: the product is in the earliest institutional deployments in Indonesian BFSI and in qualified-pilot engagements with Indonesian government and defence stakeholders at the time of this brief. Specific deployment references, named or anonymised at the institution's preference, are shared with qualified evaluators under NDA. PT Easysoft Indonesia is transparent about the pre-reference stage of certain engagements and commits that any claim made in the evaluation conversation is grounded in a traceable customer case or a declared gap; no customer evidence is presented that does not exist.

POST-QUANTUM READINESS

Enclave's cryptographic road-map tracks NIST's post-quantum standards (FIPS 203 ML-KEM, FIPS 204 ML-DSA, FIPS 205 SLH-DSA, finalised August 2024). The crypto-agility architecture of the product permits hybrid-classical and post-quantum schemes to be delivered as a policy-library update rather than a breaking engine change. The migration timeline, hybrid scheme details, and test-vector status are documented in the technical-evaluation pack.

Upgrade path and version policy

Enclave is delivered on a continuous-delivery cadence with a quarterly long-term-support release that institutions can pin against change-management and audit cycles. Security fixes are delivered out-of-band on critical severity and do not disturb the LTS line. Policy-library and regulatory-pack updates are delivered independently of the platform release, so an institution can accept a regulatory refresh without accepting an engine upgrade.

End of Product Brief. This document is intended for institutional evaluation under mutual non-disclosure. Architectural details, cryptographic specifications, adversarial audit findings, and control-mapping appendices are provided as a technical-evaluation package to qualified evaluators on request. For commercial enquiries, procurement discussions, and proof-of-concept scoping, contact PT Easysoft Indonesia at **info@nexilis.io**.