TECHNICAL WHITEPAPER · JUNE 2026

VEMP

Verifiable Enterprise Messaging Protocol

Pre-Decryption Admission Control for Encrypted Communications

Yandeh™ Holdings Inc.

ABSTRACT

The Verifiable Enterprise Messaging Protocol (VEMP) defines a new layer of the communication security stack: pre-decryption admission control of encrypted communications under state-machine-governed release. This whitepaper sets out the architectural framing, governance principles, threat model, deployment relevance, and compliance mapping for the VEMP protocol category. It positions VEMP relative to existing communication-security categories — S/MIME and OpenPGP, TLS, secure email gateways, information rights management, secure portal architectures, zero-trust network access, and recent academic work in hierarchical governance and policy-compliant secure messaging — and identifies the layer at which VEMP operates as distinct from each. This document is a technical reference; specific claim language is held in the filed patent applications.

1. The Layer VEMP Defines

Existing communication-security architectures govern the channel, the envelope, or the rendered content. They do not govern whether a delivered encrypted communication should ever be decrypted in the recipient environment.

Transport-layer security protects the pipe between nodes. Once an encrypted object has been delivered, TLS has no further involvement. Encrypted email (S/MIME, OpenPGP) treats decryption-key possession or signature verification as the principal trust event; no admission state exists between message delivery and content access. Secure email gateways make a deliver-or-block decision at the mail-transfer boundary against transport authentication signals; they have no further involvement once delivery occurs. Information rights management applies controls to communications already inside the recipient environment, after decryption has occurred and the encrypted object's content is exposed to the recipient platform. Secure retrieval portals condition retrieval on HTTP authentication; once retrieved, content remains in the recipient's local cache and cannot be recalled. Zero-trust network access governs whether a user or device may reach a network resource; it does not govern whether a specific communication object should be decrypted at this time, under these conditions, by this recipient.

VEMP names the missing layer:

> ***Pre-decryption admission control.*** *The communication is delivered and held in a controlled state. Whether it is ever decrypted at all is gated by evaluation of artifact-bound preconditions against runtime conditions at the time of attempted access. Decryption keys are released by a protected-boundary key management service only upon affirmative state-machine advancement. Every governance event — admission, release, modification, revocation, failure — is recorded in a cryptographically signed, tamper-evident receipt.*

2. Architectural Components

VEMP introduces six coordinated mechanisms. None individually constitutes a new protocol category. Their combination does.

2.1 Two-plane communication architecture

A communication object is delivered into a *first communication plane* — the conventional mail-transport boundary, the network-delivery layer, or any delivery substrate. Admission into a *second communication plane* — the controlled environment in which content can be accessed — requires affirmative evaluation of the admission preconditions associated with the communication object. A communication that fails admission is retained in the first plane without any exposure of encrypted content to recipient systems. The dual-plane separation is structural rather than configurational; the second plane is not reachable by delivery of the outer envelope component alone.

2.2 Message authority artifact

Each communication object is associated with a structured message authority artifact that encodes the authorization conditions governing the communication: the authorized sender authority, the message classification, the cryptographic profile under which the communication may be admitted, the recipient eligibility conditions, the release preconditions, and the lineage control parameters applicable to derived communications. The artifact is cryptographically bound to the encrypted content such that any modification of either invalidates the binding. The artifact travels with the communication object.

2.3 Formally defined communication state machine

Each communication object has a state in a formally defined state machine. Representative states include *delivered*, *admission-pending*, *admitted*, *release-qualified*, *released*, *partially-released*, *reevaluation-pending*, *revoked*, and *expired*. Each transition between states requires affirmative evaluation of state-transition preconditions stored in association with the message authority artifact. The state machine is non-bypassable: no transition to a more permissive state occurs without validation of the applicable artifact-encoded preconditions.

2.4 Protected-boundary key management

Decryption keys for VEMP-governed communications are held within a protected execution boundary — a hardware security module, a trusted execution environment, a cloud-hosted key management service with tenant-isolated access controls, or any boundary implementation that prevents extraction of key material outside authorized processes. Key release is causally conditioned on the state machine

having advanced to a state in which release is permitted; the key management service does not release decryption keys absent the affirmative authorization signal from the admission evaluation component. Post-release revocation operates through invalidation of key material within the protected boundary, architecturally independent of recipient endpoint behavior.

2.5 Lineage-bound constraint propagation

Constraints encoded in the message authority artifact of a root communication object propagate to derived communications — replies, forwards, delegations, and communications generated by AI agents or other automated processes acting on the root communication. A derived communication is bound to a cryptographic lineage continuity record generated at the admission of the root. Any derived communication that asserts authority exceeding the encoded ceiling — for example, an AI-agent-generated reply asserting an authority scope wider than the agent's permitted ceiling — is denied state-machine advancement regardless of whether the derivation was syntactically valid.

2.6 Verifiable receipt generation

Each governance event — admission, release, partial release, post-release modification, revocation, expiration, failure — produces a cryptographically signed, tamper-evident receipt. Receipts are typed to specific governance event categories, are bound to a specific communication object's state-machine record, and are appended to a hash-chained audit log replicated across multiple nodes. The receipt-generation function is integral to the protocol; it is not an optional logging facility added at deployment time.

3. Threat Model Catalog

VEMP addresses eight independently identifiable threat categories. Each is described below with the specific architectural mechanism by which VEMP addresses the threat.

3.1 Business email compromise and compromised sender domain

Threat. A compromised contractor or partner domain passes DKIM, SPF, and DMARC authentication with valid signatures. Gateway filtering accepts the communication because it is technically valid at the transport-authentication layer. The adversary's communications are indistinguishable from legitimate communications at that layer.

VEMP mechanism. VEMP evaluates the sender authority encoded in the message authority artifact against an approved authority record for the recipient domain. A compromised domain that has no approved record for the asserted message class, or that presents a class not authorized for that sender under the applicable policy, receives a hard-fail admission result. No content is exposed; a tamper-evident failure receipt is generated.

3.2 Post-compromise retroactive revocation

Threat. When a trusted sender is compromised after communications have already been delivered and read by recipients, no existing communication protocol provides a mechanism to revoke access to already-delivered content. Certificate revocation (CRL, OCSP) affects only future operations; previously decrypted content remains readable.

VEMP mechanism. Upon a qualifying post-release event — a sender-compromise indicator, a recipient-compromise indicator, a policy change — VEMP's post-release enforcement module signals the state-transition controller to roll back the communication state machine for affected communications and directs the protected-boundary key management service to invalidate the associated decryption keys. Revocation enforcement is complete within the propagation latency of the key management service, architecturally independent of recipient endpoint cooperation.

3.3 Harvest-now-decrypt-later on archived ciphertext

Threat. Adversaries collect encrypted communications at scale with the intent to decrypt them retrospectively once a cryptographically relevant quantum computer becomes available. Archived ciphertext protected only by classical algorithms becomes retroactively readable when the underlying primitive is broken.

VEMP mechanism. VEMP enforces hybrid post-quantum cryptographic profile compliance as a state-machine-gated admission prerequisite. The cryptographic profile field in the message authority artifact encodes a hybrid configuration combining classical and post-quantum algorithms. A communication that presents only a classical profile cannot advance from the admission-pending state regardless of algorithmic signature validity.

3.4 AI-agent and machine-originated communication abuse

Threat. AI agents and automated workloads generate and process communications. A compromised or malicious agent can generate communications asserting authority beyond its permitted scope, inject unauthorized content into existing threads, or escalate from a permitted role (summarization) to an unauthorized role (approval).

VEMP mechanism. VEMP's lineage tracking module evaluates every derived communication against a maximum-authority ceiling encoded in the lineage continuity record. An AI-agent-generated communication asserting authority exceeding its ceiling is denied state-machine advancement before any admission evaluation is performed. A tamper-evident lineage violation receipt is generated.

3.5 Thread hijacking and reply injection

Threat. Adversaries insert themselves into existing legitimate communication threads. A reply that continues an existing thread appears credible to recipients because it references prior genuine communications. No existing protocol verifies that a reply is a legitimate continuation of its parent communication.

VEMP mechanism. VEMP enforces cryptographic lineage continuity for all derived communications. Every reply, forward, and delegation is evaluated against the lineage continuity record generated at admission of the root communication. A reply from a sender not in the authorized participant set, or presenting a lineage identifier that does not match the thread's lineage record, is denied state-machine advancement.

3.6 Malicious attachment delivery

Threat. Ransomware and malware are delivered via email attachments. Sandbox scanning detects known signatures but fails against novel variants. Once a message is delivered and opened, attachments are in the recipient's operating environment and may execute.

VEMP mechanism. VEMP supports per-attachment release control. Attachments may be configured to require secondary authorization before release, separately from the message body. A communication may enter a partially-released state in which the recipient accesses the message body while attachments

remain in the second communication plane pending attachment-specific release conditions.

3.7 Insider exfiltration via unauthorized forwarding

Threat. An authorized recipient may forward a sensitive communication to unauthorized parties. Conventional information rights management attempts to prevent forwarding through client-side policy enforcement, which depends on the recipient's mail client respecting the policy and can be circumvented.

VEMP mechanism. VEMP enforces forwarding restrictions at the admission layer of the second communication plane rather than through client-side policy. A derived communication that names a non-authorized participant as the next recipient cannot advance from the admission-pending state. The enforcement is at the protocol layer and does not depend on client cooperation.

3.8 Absence of non-repudiable compliance audit evidence

Threat. Regulated industries and government agencies must demonstrate that communications were accessed only by authorized parties under verified conditions at specific times. Server-side log entries are alterable and do not constitute cryptographically verifiable governance evidence.

VEMP mechanism. VEMP generates a cryptographically signed, tamper-evident receipt for every governed state transition and governance event. Each receipt is signed within the protected-boundary key management service and is appended to a hash-chained audit log replicated across multiple nodes. The hash chain provides mathematical proof that no receipt has been modified or deleted; any modification invalidates the chain from the altered entry forward.

4. Position Relative to Existing Architectures

The architectural distinction between VEMP and existing communication-security architectures is summarized in the table below across five governance-critical dimensions.

Dimension	Existing communication-security architectures	VEMP
Trust event	One-time: key possession, signature verification, or point-of-access authentication. Trust is established once.	Continuous: artifact-bound state-machine advancement with precondition validation at every transition throughout the full communication lifecycle.
Operational timing	Transit-time (TLS, DKIM) or point-of-access (S/MIME verification, portal authentication). No mechanism operates after delivery and before decryption.	Entire lifecycle. Admission and release gates operate after delivery and before any decryption.
Revocation mechanism	Forward-only. Certificate revocation affects future operations only. No mechanism withdraws access to already-delivered or already-decrypted content.	Retroactive. Protected-boundary key invalidation withdraws access to already-delivered content within bounded enforcement latency, independent of endpoint behavior.
Audit evidence	None mandated at the protocol level. Server-side log entries are alterable.	Cryptographically signed, tamper-evident receipts for every state transition, appended to a hash-chained audit log replicated across multiple nodes.
Governance location	In the protocol engine, policy server, gateway, or IRM platform — external to and separable from the communication object.	In the communication object itself. The message authority artifact is cryptographically bound to the encrypted content and travels with it.

Table 1. Architectural comparison across five governance-critical dimensions.

5. Distinctions From Adjacent Categories

VEMP is positioned relative to seven adjacent architectures. Each is a credible comparison; in each case the comparison shows architectural difference rather than overlap.

S/MIME and OpenPGP

Encryption and signing are incidental to VEMP. S/MIME and OpenPGP treat decryption-key possession or signature verification as the principal trust event. Neither defines an admission state between delivery and access. VEMP's mechanism operates before any decryption occurs.

Transport-layer security (TLS)

TLS governs the channel between nodes. Once delivery completes, TLS has no further involvement. VEMP operates above the transport layer entirely; the outer communication plane may use TLS for channel security, but VEMP's mechanisms are orthogonal to it.

Secure email gateway filtering

Gateways make a deliver-or-block decision at the mail-transfer boundary against transport authentication signals. A gateway decides whether a message arrives. VEMP decides whether a delivered message is ever admitted into a controlled communication plane. Different operations, different layers, different threat coverage.

Information rights management and data loss prevention

IRM platforms apply controls to communications after they have been accepted into the recipient environment and decrypted. VEMP's admission evaluation occurs before any content exposure to the recipient environment. The separation is architectural, not merely temporal.

Secure message retrieval portals

Portal architectures condition retrieval on HTTP authentication at a web endpoint. Once retrieved, content remains in the recipient's local cache and cannot be recalled. VEMP's revocation is implemented as protected-boundary key invalidation, which renders content inaccessible on all recipient systems within bounded enforcement latency regardless of caching or portal availability.

Zero-trust network access

ZTNA governs whether a user or device may reach a network resource. VEMP governs whether a specific communication object may be admitted and released within the controlled communication plane. ZTNA addresses resource access; VEMP addresses communication object governance. Complementary, not overlapping.

Hierarchical governance and policy-compliant secure messaging (academic)

Recent academic work on hierarchical governance for end-to-end-encrypted messaging and on policy-compliant secure messaging addresses post-delivery content moderation and content-policy predicate systems. Both operate after decryption has occurred. VEMP operates before any decryption, with key release conditioned on protected-boundary-enforced state-machine advancement through artifact-stored precondition records.

6. Deployment Relevance

VEMP is relevant to deployment contexts in which the conventional separation between message delivery and content access is itself a security boundary that must be enforced at the protocol level rather than at the policy or client layers.

Enterprise communication platforms

Organizations operating sensitive communication infrastructure — financial services, healthcare, legal, defense contractors — require enforcement that operates independently of client cooperation. VEMP's pre-decryption admission and protected-boundary key release model satisfies this requirement: content cannot be accessed unless and until the state machine advances; revocation operates without endpoint cooperation.

Government and sovereign communication

Government and sovereign deployments require non-repudiable evidence of who accessed what, when, and under what conditions. VEMP's verifiable receipt generation, hash-chained audit log, and cryptographic profile compliance directly support the evidence requirements of regulated communication environments operating under CNSA 2.0 and ISO/IEC 42001 frameworks. Federated multi-domain deployment patterns support sovereign and air-gapped configurations.

Regulated industries operating under EU AI Act

Article 17 of Regulation (EU) 2024/1689 requires high-risk AI system providers to establish, document, and maintain quality management covering the full design and deployment lifecycle. VEMP's state-machine-bound verifiable receipts provide technical artifacts that demonstrate continuous governance of AI-agent-mediated communications under the regulation's obligations.

Post-quantum migration programs

VEMP's algorithm-agnostic functional framing — cryptographic profile compliance as a state-machine-gated prerequisite rather than a fixed algorithm requirement — preserves the verification properties across classical, hybrid, and CNSA 2.0 deployments. Enterprises operating under post-quantum migration mandates can adopt VEMP and migrate cryptographic profiles incrementally without protocol-level redesign.

7. Compliance Mapping

VEMP provides protocol-level mechanisms that directly support compliance with the principal communication-governance requirements across major frameworks.

Framework	Requirement category	VEMP mechanism
SOC 2 (Trust Services Criteria)	Logical access, monitoring, encryption, change management	State-machine-gated admission with verifiable receipts; protected-boundary key release; hash-chained audit log.
ISO/IEC 27001	Information security controls covering communication and operations security	Artifact-bound admission evaluation; lineage-bound constraint propagation; tamper-evident governance event records.
NIST SP 800-53 (Rev. 5)	Access control (AC), audit and accountability (AU), system and communications protection (SC)	Per-communication authorization evaluation (AC); cryptographically signed governance receipts (AU); pre-decryption admission with protected-boundary key release (SC).
FedRAMP	Federal authorization-to-operate requirements for cloud services	Inherits SP 800-53 control coverage; protected-boundary key management supports FIPS 140-validated key management requirements.
CMMC (Level 2 and 3)	Cybersecurity Maturity Model Certification for defense industrial base	Per-communication admission control; cryptographic non-repudiation of governance events; lineage governance over AI-agent-mediated communications.
EU AI Act Article 17	Quality management system for high-risk AI systems	State-machine-bound governance receipts for AI-agent communications; lineage propagation enforcing authority ceilings on derived communications.
ISO/IEC 42001:2023	AI management system standard	Verifiable receipts as technical evidence of governance controls operating on AI-agent communications throughout their lifecycle.
CNSA 2.0	Commercial National Security Algorithm Suite 2.0 for U.S. National Security Systems	Cryptographic profile compliance as a state-machine-gated admission prerequisite; hybrid post-quantum configuration supported as standard policy.

Table 2. VEMP mechanism mapping to principal communication-governance frameworks.

8. Toward Standards Engagement

VEMP names a layer that has not been addressed by existing communication standards. IETF working groups on workload identity (WIMSE) and supply-chain transparency (SCITT) address adjacent identity and artifact-attestation layers. IETF email security work continues to refine S/MIME (RFC 8551) and OpenPGP (RFC 4880). NIST guidance on zero-trust (SP 800-207) and access control (SP 800-53) addresses access architecture; none specifies a protocol-level admission mechanism operating before decryption with state-machine-bound governance receipts.

Yandeh Holdings Inc. is positioned to engage standards bodies, industry consortiums, and federal initiatives — including the NIST CAISI AI Agent Standards Initiative and related NCCoE efforts on agent identity and authorization — on VEMP as a candidate reference architecture for the pre-decryption admission control layer. Engagement is structured case-by-case under appropriate confidentiality arrangements.

9. The Category, Briefly

VEMP defines a protocol category — pre-decryption admission control of encrypted communications under state-machine-governed release — that does not have an existing standards-track home. The category's six coordinated mechanisms (two-plane architecture, message authority artifact, communication state machine, protected-boundary key management, lineage-bound constraint propagation, verifiable receipt generation) form an inseparable system. The category addresses threats — business email compromise on legitimately authenticated domains, post-compromise retroactive access withdrawal, harvest-now-decrypt-later attacks on archived ciphertext, AI-agent and machine-originated communication abuse, thread hijacking, malicious attachment delivery, insider exfiltration, and absence of non-repudiable compliance evidence — that existing categories cannot fully address from their own architectural positions. The category is implementable today with standard cryptographic primitives, widely deployed protected-boundary key management infrastructures, and specified post-quantum algorithms.

> ***Patent notice.*** *The subject matter of this whitepaper is based on pending U.S. patent applications filed by Yandeh Holdings Inc., including the Verifiable Enterprise Messaging Protocol (VEMP) parent application and the Admission Before Decryption continuation. The Yandeh Holdings protocol portfolio also includes the Autonomous Machine Identity and Authority Protocol (AMIAP / XAP) family covering execution authority for autonomous systems, addressed in separate publications. Specific claim language is held in the filed applications and is not reproduced in this whitepaper. Commercial engagement: info@yandehgroup.com.*

CONTACT

info@yandehgroup.com

REFERENCES

Ramsdell, B., & Turner, S. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification. IETF RFC 8551, 2019.

Callas, J., Donnerhacke, L., Finney, H., Shaw, D., & Thayer, R. OpenPGP Message Format. IETF RFC 4880, 2007.

Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. IETF RFC 8446, 2018.

Hardt, D. (ed.). The OAuth 2.0 Authorization Framework. IETF RFC 6749, 2012.

NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology, Revision 5, 2020.

NIST SP 800-207, Zero Trust Architecture. National Institute of Standards and Technology, 2020.

NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. National Institute of Standards and Technology, 2011.

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems. International Organization for Standardization, 2022.

ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system. International Organization for Standardization, December 2023.

Regulation (EU) 2024/1689, Artificial Intelligence Act. European Parliament and Council, 13 June 2024.

NSA Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). National Security Agency, 2022, updated 2024.

NIST FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). National Institute of Standards and Technology, 2024.

NIST FIPS 204, Module-Lattice-Based Digital Signature Standard (ML-DSA). National Institute of Standards and Technology, 2024.

Birkholz, H., Delignat-Lavaud, A., Fournet, C., Deshpande, Y., & Lasker, S. An Architecture for Trustworthy and Transparent Digital Supply Chains. IETF draft-ietf-scitt-architecture-22, October 2025.

Salowey, J., Rosomakho, Y., & Tschofenig, H. Workload Identity in a Multi System Environment (WIMSE) Architecture. IETF draft-ietf-wimse-arch-06, September 2025.

Namavari, A., et al. Private Hierarchical Governance for Encrypted Messaging. Proceedings of the 2024 IEEE Symposium on Security and Privacy, 2024.

Alwen, J., et al. Policy Compliant Secure Messaging. Advances in Cryptology — ASIACRYPT 2025, Lecture Notes in Computer Science Vol. 16246.

NIST Center for AI Standards and Innovation (CAISI). AI Agent Standards Initiative. National Institute of Standards and Technology, February 2026.

Yandeh Holdings Inc. XAP — Execution Authority Protocol: A New Protocol Category for Machine Governance. Category Definition Paper, April 2026.