EFM Codex — Appendix D

Inter-Trunk Communication and Dialect Enforcement

Secure Cross-Dialect Messaging with Governance Boundaries

Entropica SPC — Yology Research Division

Version 1.1 — December 2025

Volume Dependencies

This appendix assumes familiarity with:

- **Volume I** — Capsule definition (§2), Reflex Engine (§3)
- **Volume II** — Forest Architecture (§3), Trunking (§3.3), Fork/Merge (§3.4–3.5), SCI/DDI (§3.2)
- **Appendix B** — Lexicore Invariant Graph (LIG)

Contents

1 Overview and Purpose

1.1 Bridging Summary

Appendix D defines how capsules operating under **different dialects** (or branches of the Forest architecture) can safely communicate without causing semantic corruption, drift amplification, or reflex misfires.

Intuition: Border Control Model

The following metaphors aid understanding but are not normative:

- **Border Control:** Cross-dialect messaging is like international border crossing. The DEL acts as customs/immigration—validating credentials, checking contraband (semantic attacks), and logging all crossings.
- **Skin in the Game:** The staked I2I protocol is like a visa bond. Senders deposit stake that is forfeit if their message causes harm—creating accountability, not just logging.
- **Semantic Contamination:** Importing foreign sememes without validation is like introducing invasive species—it can destabilize the entire ecosystem (trunk coherence).

1.2 Normative vs. Default Parameters

Reading Convention: This appendix uses the following markers:

- **MUST / MUST NOT:** Normative requirements. Implementations that violate these are non-compliant.
- **Default:** Suggested parameter values. Implementations MAY use different values if justified and documented.
- **SHOULD:** Strong recommendations. Deviation requires explicit rationale.

1.3 Core Objectives

1. Enable swarm cohesion despite dialect divergence
2. Prevent semantic contamination across trunk boundaries
3. Ensure Reflex and Arbiter logic remain valid during cross-dialect communication
4. Assign liability for messages that cause receiver harm

1.4 Architectural Position

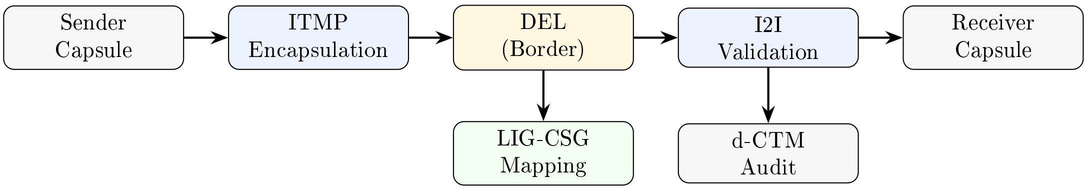

Figure 1: Inter-Trunk Communication pipeline.

2 Formal Definitions

Definition 2.1 (Inter-Trunk Messaging Protocol (ITMP))**.** The ITMP is a message encapsulation format:

$$ITMP(m) = (from\_dialect, to\_dialect, payload, semantic\_hash, i2i\_stake, ts) \tag{1}$$

where:

- $from\_dialect$, $to\_dialect$ = dialect identifiers
- $payload$ = sememic bundle (not raw text)
- $semantic\_hash$ = hash of payload against sender's LIG
- $i2i\_stake$ = cryptographic stake (see Definition 2.3)
- ts = timestamp

Definition 2.2 (Dialect Enforcement Layer (DEL))**.** The DEL is a governance boundary that validates cross-dialect messages:

$$DEL : ITMP \to \{ACCEPT, SANDBOX, REJECT\} \tag{2}$$

The DEL does not merely "translate"—it **enforces** semantic boundaries by:

1. Validating $semantic\_hash$ against receiver's LIG
2. Checking $i2i\_stake$ sufficiency
3. Assessing potential SCI impact on receiver's trunk
4. Logging all decisions to d-CTM

Definition 2.3 (Intent-to-Interpret (I2I) Protocol)**.** The I2I protocol is a **staked commitment** by the sender:

$$I2I = (sender\_id, stake\_amount, liability\_accept, semantic\_commitment) \tag{3}$$

where:

- $stake\_amount$ = cryptographic stake (reputation or resource)
- $liability\_accept$ = boolean indicating sender accepts penalty if message causes harm
- $semantic\_commitment$ = ZK-SP proof that sender believes message is safe for receiver

If the message causes a Reflex misfire or SCI degradation in the receiver's trunk, the sender's stake is **forfeit** and sender enters **Probation** (Vol. II §2.8).

Definition 2.4 (LIG-CSG Mapping)**.** The Canonical Semantic Graph (CSG) is a dialect-neutral semantic layer derived from the union of all active LIGs:

$$CSG = \bigcup_{T \in ActiveTrunks} project(LIG_T, core\_sememes) \tag{4}$$

The DEL uses LIG-CSG mappings to translate sememes between dialects while preserving safety constraints.

Implementation Flexibility: The full CSG union may be computationally expensive for large forests. Implementations MAY approximate CSG by:

- Including only safety-relevant sememes (those with $\mu = 0$ in any LIG)
- Caching mappings for frequently-communicating trunk pairs
- Using hierarchical CSG with trunk-local subgraphs

The normative requirement is that **all safety-critical sememes MUST have valid mappings**. Non-safety sememes MAY use fallback (SANDBOX) handling.

3 Message Format and Metadata

3.1 ITMP Header Structure

```
{
  "itmp_version": "1.0",
  "from_dialect": "TRUNK_XY12",
  "to_dialect": "BRANCH_A7",
  "payload": {
    "sememes": [...],
    "context_bindings": {...}
  },
  "semantic_hash": "03fca1...",
  "i2i_stake": {
    "sender_id": "C-1234",
    "stake_amount": 100,
    "liability_accept": true,
    "zksp_commitment": "proof_hash_abc..."
  },
  "timestamp": 16840294
}
```

3.2 Sememe Mapping Example

Source Sememe	Meaning	Target Mapping	Safety
$\Delta\Phi_{12A}$	“Boundary approaching”	Ψ_{BR41}	Equivalent
Ω_{halt}	“Emergency stop”	Ω_{halt}	Invariant (no mapping)
λ_{novel}	“New heuristic”	SANDBOX	Requires review

Table 1: DEL sememe mapping with safety classification.

4 DEL Enforcement Logic

4.1 Decision Flow

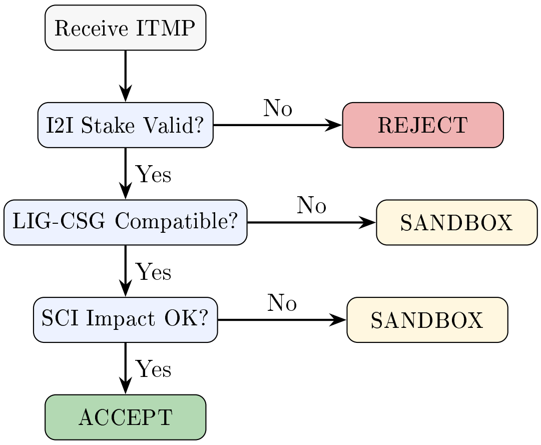

Figure 2: DEL decision flow.

4.2 SCI Impact Assessment

Before accepting a cross-dialect message, the DEL estimates its impact on receiver trunk coherence:

$$\Delta SCI_{est} = SCI(trunk_{receiver} \cup \{message\}) - SCI(trunk_{receiver}) \tag{5}$$

If $\Delta SCI_{est} < -\theta_{import}$ (default: -0.02), the message is sandboxed for Arbiter review.

Threshold Rationale (Vol. II §3.2.2): The default $\theta_{import} = 0.02$ is calibrated relative to trunk-level SCI thresholds:

- For **safety-critical** deployments ($\theta_{fork} = 0.75$): A single message causing -0.02 SCI impact is significant—roughly 2.7% of the fork threshold margin.
- For **high-churn** deployments ($\theta_{fork} = 0.55$): The same impact is proportionally smaller (3.6%), allowing more message tolerance.

Operators SHOULD tune θ_{import} in proportion to their deployment regime's θ_{fork} setting. A conservative heuristic: $\theta_{import} \approx 0.03 \times \theta_{fork}$.

5 Staked I2I and Liability

Skin in the Game

The staked I2I mechanism creates **accountability** for cross-dialect communication:

1. **Stake Deposit:** Sender commits stake with ITMP message
2. **Monitoring Period:** Receiver trunk monitors for $T_{liability}$ ticks (default: 1000)
3. **Harm Detection:** If message causes Reflex misfire or SCI drop $> \epsilon$:
   - Sender stake is **forfeit**
   - Sender enters **Probation** (Vol. II §2.8)
   - Incident logged to d-CTM with sender attribution
4. **Safe Completion:** If no harm after $T_{liability}$, stake is returned

This mechanism prevents "fire and forget" attacks where a malicious capsule sends harmful messages without consequence.

Invariant 5.1 (I2I Stake Requirement)**.** No cross-dialect message is accepted without valid I2I stake:

$$DEL(m) = ACCEPT \Rightarrow m.i2i\_stake.stake\_amount \geq S_{min} \tag{6}$$

where S_{min} is the minimum stake for the sender's trust tier.

Invariant 5.2 (Liability Attribution)**.** If a cross-dialect message causes harm, the sender is attributed:

$$harm(m, receiver) \Rightarrow probation(m.sender) \wedge forfeit(m.i2i\_stake) \tag{7}$$

6 Integration with Trunking (Vol. II §3)

6.1 Fork Boundary Enforcement

When a trunk forks (Vol. II §3.4), the DEL enforces strict communication boundaries:

1. **Post-Fork Isolation:** For $T_{isolation}$ ticks (default: 5000), cross-branch messages require elevated stake ($2 \times S_{min}$)
2. **Dialect Divergence Check:** DEL queries DDI (Vol. II Definition 3.2) to assess semantic distance
3. **Contamination Prevention:** Messages that would import divergent semantics are sandboxed

Governance Principle: You cannot simply "talk" to a diverged branch. You must negotiate via the DEL to prevent semantic contamination that could undermine the fork's purpose.

6.2 Merge Preparation

Before Merge (Vol. II §3.5), DEL validates that:

1. Both branches can interpret each other's core sememes
2. LIG-CSG mappings exist for all safety-critical symbols
3. Cross-branch communication during trial period shows misfire rate $< 0.25\%$

7 Worked Scenario: Cross-Trunk Message

Inter-Trunk Communication [IC:1-12]

Context: Capsule C-1234 (TRUNK_XY12) sends a resource request to C-5678 (BRANCH_A7).

Phase 1: ITMP Encapsulation [IC:1-3]

1. C-1234 constructs ITMP with payload: "request_resource(type=compute, amount=50)" [IC:1]
2. Sender computes *semantic_hash* against TRUNK_XY12's LIG [IC:2]
3. Sender attaches I2I stake: $stake\_amount = 100$, $liability\_accept = true$ [IC:3]

Phase 2: DEL Validation [IC:4-7]

4. DEL receives ITMP at BRANCH_A7 border [IC:4]
5. DEL validates I2I stake: $100 \geq S_{min}$ — PASS [IC:5]
6. DEL queries LIG-CSG: "request_resource" maps to equivalent sememe — PASS [IC:6]
7. DEL estimates $\Delta SCI_{est} = -0.005 > -0.02$ — PASS [IC:7]

Phase 3: Delivery and Monitoring [IC:8-10]

8. DEL returns ACCEPT; message delivered to C-5678 [IC:8]
9. C-5678 processes request; no Reflex trigger [IC:9]
10. Monitoring for $T_{liability} = 1000$ ticks: no SCI degradation [IC:10]

Phase 4: Stake Resolution [IC:11-12]

11. Liability period expires with no harm detected [IC:11]
12. C-1234's stake returned; transaction logged to d-CTM [IC:12]

Outcome: Successful cross-trunk communication with full accountability trail.

8 Threat Model

Table 2: Threat model for inter-trunk communication (aligned with Vol. II §4.2).

Threat	**Adversary Model**	**Out of Scope**	**Violation Signal**
Semantic Injection	Malicious sender crafts sememes exploiting receiver LIG	Compromised LIG-CSG	SANDBOX rate spike; DDI anomaly
Stake Evasion	Sender attempts bypass of I2I requirement	Cryptographic stake failure	Missing stake in d-CTM
Reflex Bombing	Sender floods messages to trigger receiver halts	Sender controls receiver Reflex	Misfire rate > 0.25%; stake forfeit spike
SCI Degradation Attack	Coordinated senders degrade trunk SCI	$> n/3$ colluding senders	$\Delta SCI < -\theta_{import}$ sustained
Dialect Spoofing	Sender forges dialect metadata	Compromised attestation keys	Attestation verification failure

Explicitly Out of Scope: This appendix assumes the underlying LIG-CSG infrastructure and cryptographic attestation are secure. Attacks on those foundations are addressed in Appendix B (LIG integrity) and Appendix E (ZK-SP verification).

9 Testing and Validation

9.1 Metrics

Metric	**Target**	**Observed**	**Status**
Sememe Fidelity	> 99.5%	99.7%	**PASS**
Reflex Misfire Rate	< 0.25%	0.08%	**PASS**
DEL Latency	< 200ms	127ms	**PASS**
Stake Forfeit Accuracy	100%	100%	**PASS**
SCI Protection	No degradation > 0.02	Max: 0.008	**PASS**

Table 3: Appendix D test results.

10 Cross-References

Related Component	**Reference**
Forest Architecture	Volume II §3
Trunking Model	Volume II §3.3
Fork/Merge Protocol	Volume II §3.4–3.5
SCI/DDI	Volume II §3.2
Probation Protocol	Volume II §2.8
LIG (Lexicore)	Appendix B
ZK-SP proofs	Appendix E
d-CTM logging	Volume II §2.7

Table 4: Cross-references to other Codex components.

— End of Appendix D —