

Email Execution Layer · Sender Policy

Infrastructure-Level Email Execution

What this is

The Email Execution Layer is a post-event execution component. It executes transactional or lifecycle emails only after a confirmed business event is received from the client system, such as payment success, license expiry, or access revocation. The layer does not generate events, make decisions, or initiate communication on its own.

The problem it solves

In many systems, email delivery logic is tightly coupled with business logic or UI layers. This leads to inconsistent sender identity, spoofing risks, unclear responsibility boundaries, and audit complexity. Sender identity is often passed dynamically per request, creating security and compliance issues.

Core principle

Sender identity is configuration-based, not request-based. Requests cannot override the sender identity. This removes runtime ambiguity and prevents unauthorized sender manipulation.

Built by Inna Kragh · LegalTechCounsellor / ContractBot.dk

Sender Identity Policy

Emails executed through the Email Execution Layer are delivered on behalf of the client's product, not on behalf of the execution provider. The provider never appears as the sender brand, sender domain, or communication party.

By default, emails are sent using a neutral, managed system domain with the client's product name displayed as the sender name. Custom sender domains are optional and available for enterprise use cases, subject to domain verification and one-time technical setup (SPF and DKIM).

The execution provider does not initiate communication, decide when emails are sent, or access user databases or payment systems. Execution occurs only after a confirmed event is received from the client system.

Sender Resolution Model

1. Input business event (confirmed)
2. Authorization via execution key (identity and permissions)
3. Configuration lookup (product name, sender mode, allowed events)
4. Execution: email sent on behalf of the client product (provider never appears)

Security note

Sender identity is resolved by configuration, not by request. This design prevents spoofing, removes runtime ambiguity, and supports audit and compliance requirements.

Available Sender Modes

Feature	Standard Sender (Default)	Branded Sender (Enterprise)
Sender name (From)	Client product name	Client product name
Sender email	notifications@system-domain.com	notifications@clientdomain.com
Client DNS setup	Not required	Required (SPF / DKIM)
Client email provider	Not required	Not required
Provider visible as sender	Never	Never
Typical use case	SaaS · internal systems · automation	Regulated environments · strict branding

Security and compliance note

The execution provider does not generate events, decide when emails are sent, or access user data beyond what is strictly necessary for execution. No marketing logic, tracking, or profiling is included.

Procurement one-liner: Sender identity is configuration-based, not request-based. That is why the execution layer is secure.