Pre-Access Legitimacy Requirement (PALR)

Definition
Pre-Access Legitimacy is the requirement that a system must not render sensitive surfaces or permit high-impact actions until the legitimacy of the acting user and the operational context has been explicitly resolved.

Rationale
Modern systems frequently proceed under assumed continuity of legitimacy (shared devices, cached sessions, ambient access). Downstream controls activate after exposure or commitment. PALR establishes legitimacy as a precondition, not a reaction.

Legitimacy States
Unresolved — legitimacy not established.
Provisional — only safe, non-sensitive surfaces permitted.
Resolved — sensitive access may proceed.
Expired — prior legitimacy no longer valid; system returns to Unresolved.

PALR Conformance Checklist

- Explicit legitimacy states independent of authentication.
- First-class Expired legitimacy state.
- Blocking of sensitive rendering until legitimacy is resolved.
- Defined Provisional safe-access mode.
- Legitimacy expiry triggers (time or event based).
- Explicit legitimacy resolution step.
- Minimal legitimacy trace for audit.
- Non-substitution of existing security layers.

Mapping to Existing Security Layers

PALR complements authentication, session management, step-up authentication, risk-based authentication, Zero Trust architectures, and monitoring systems by governing whether access may be treated as legitimate before sensitive surfaces or actions are available.