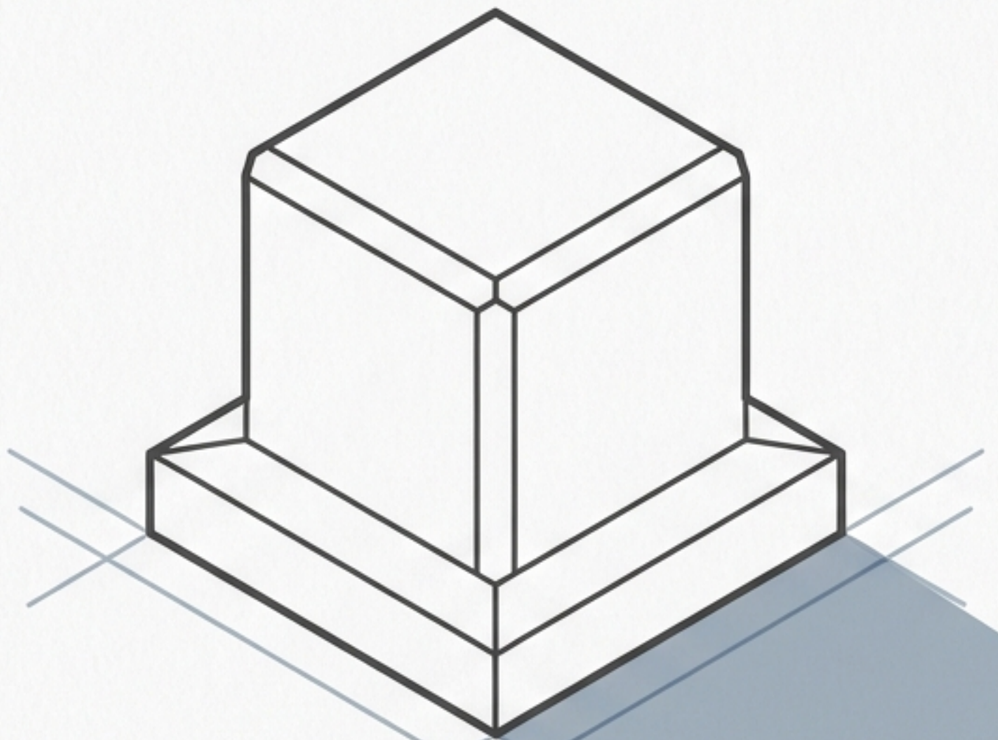
Credo: Building a Fortress for Regulated Identity

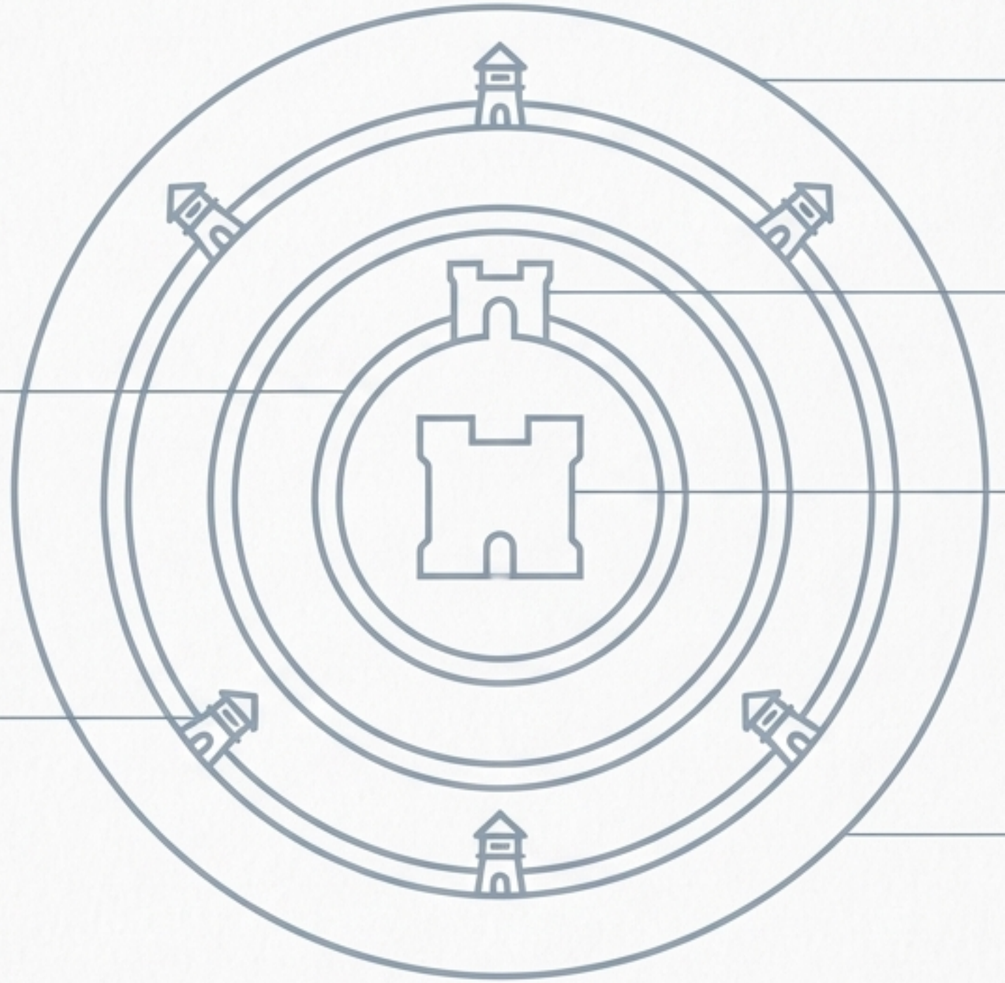
A review of the foundational capabilities delivered in Phase 0.



The mission is to build a system where trust is the foundation, not a feature.

Credo is engineered from the ground up to be a **regulated identity and authorization system**. This requires a foundation that is not just functional, but demonstrably secure, auditable, and built with intention. Phase 0 was the deliberate construction of this foundation.

Our foundation is a deliberate, layered defense.



The Moat:
Perimeter Defenses

The Gatehouse:
Rules of Engagement

The Walls:
Sovereign Territories

The Keep:
Identity Core

The Watchtowers:
Long-Lived Patrols

The Moat:
Perimeter Defenses

The Keep: Forging the Identity Core

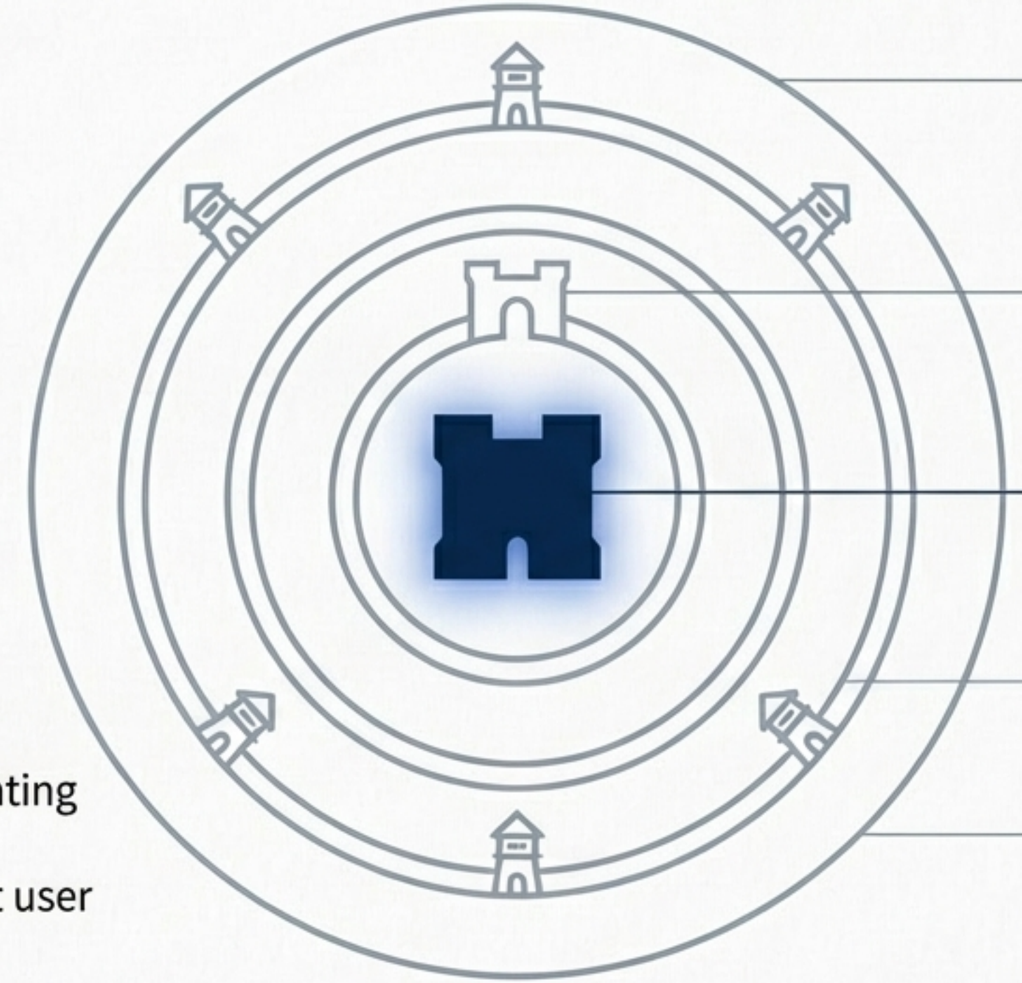
Any identity system must first answer one question flawlessly: “Who are you?”

Solution/Capabilities

We implemented a robust, standards-based authentication and session management engine.

Proof Points

- OIDC-lite via OAuth 2.0 Authorization Code Flow (RFC 6749)
- Privacy-first device fingerprinting (SHA-256 hash, no PII)
- Admin-only, GDPR-compliant user deletion orchestration



The Walls: Establishing Sovereign Territories

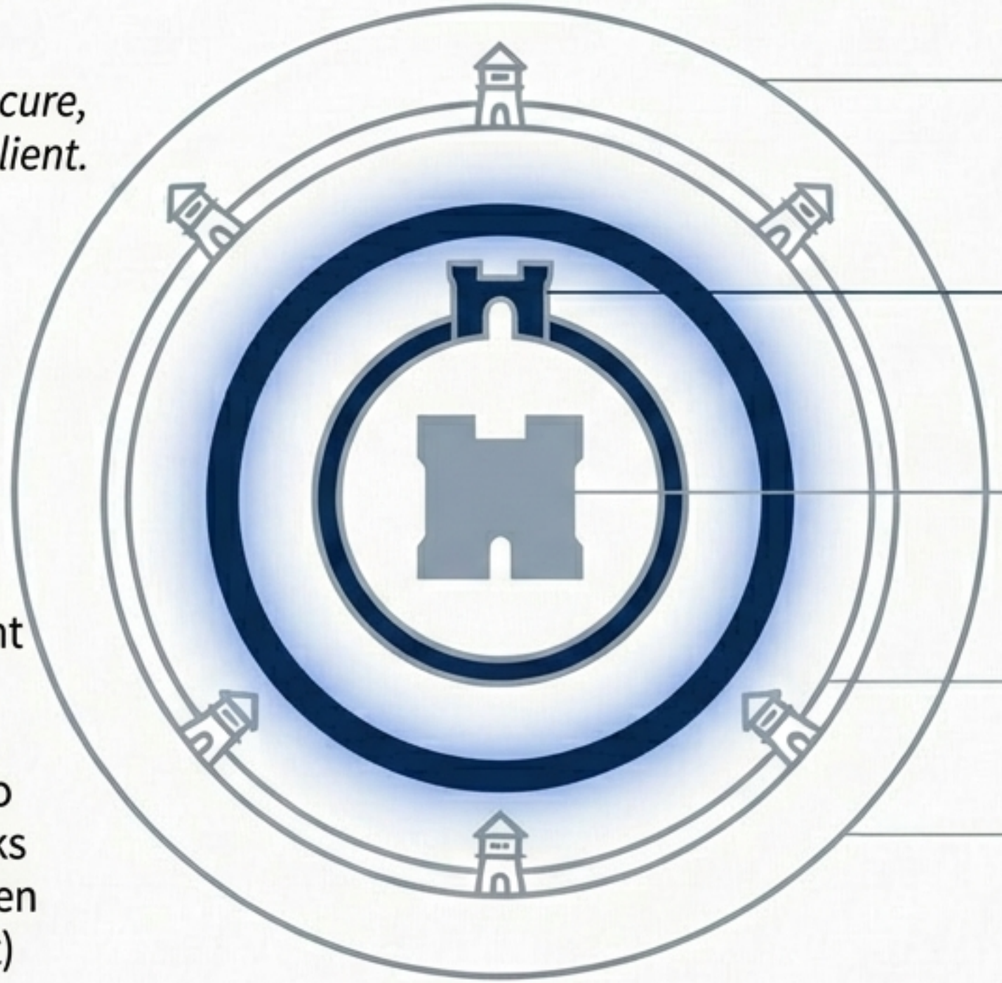
A login system is not an identity platform. True isolation requires secure, independent boundaries for each client.

Solution/Capabilities

We built a multi-tenant architecture where clients and users exist within isolated domains.

Proof Points

- Tenant and Client Management APIs with lifecycle controls (activate/deactivate)
- Strict redirect URI validation to prevent open redirector attacks
- Per-tenant issuer URLs for token isolation (RFC 8414 Compliant)



The Gatehouse: Defining the Rules of Engagement

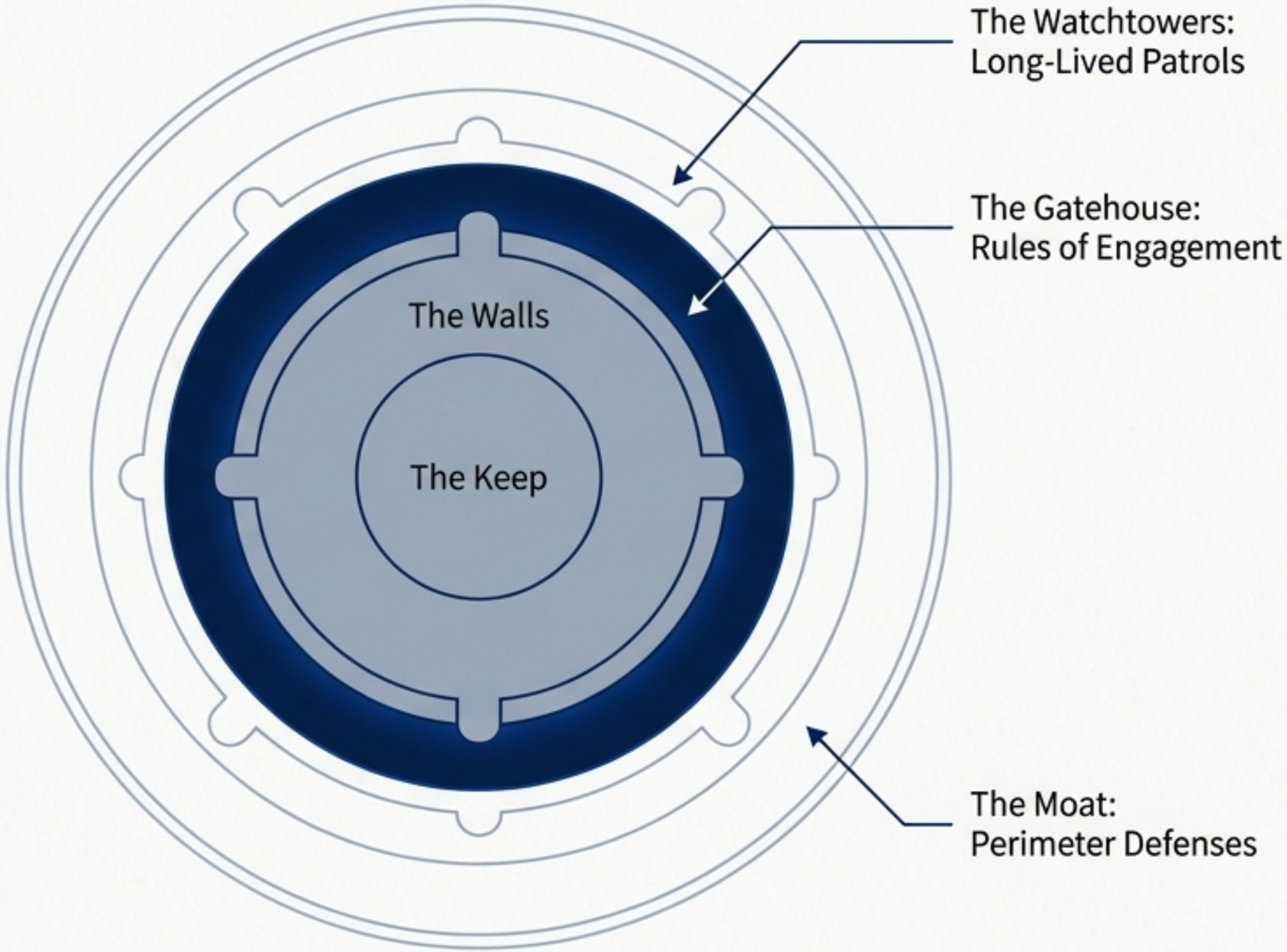
In regulated domains, access is not enough. We must prove that every action was explicitly permitted, for a specific purpose.

Solution/Capabilities

A granular, purpose-based consent system that enforces rules at the API level.

Proof Points

- Purpose-specific, time-bound, and fully auditable consent records
- Idempotent grant logic (5-min window) to prevent audit noise from UI retries
- Internal `**consentService.Require()**` check enforces consent before sensitive operations



The Watchtowers: Enabling Long-Lived Patrols

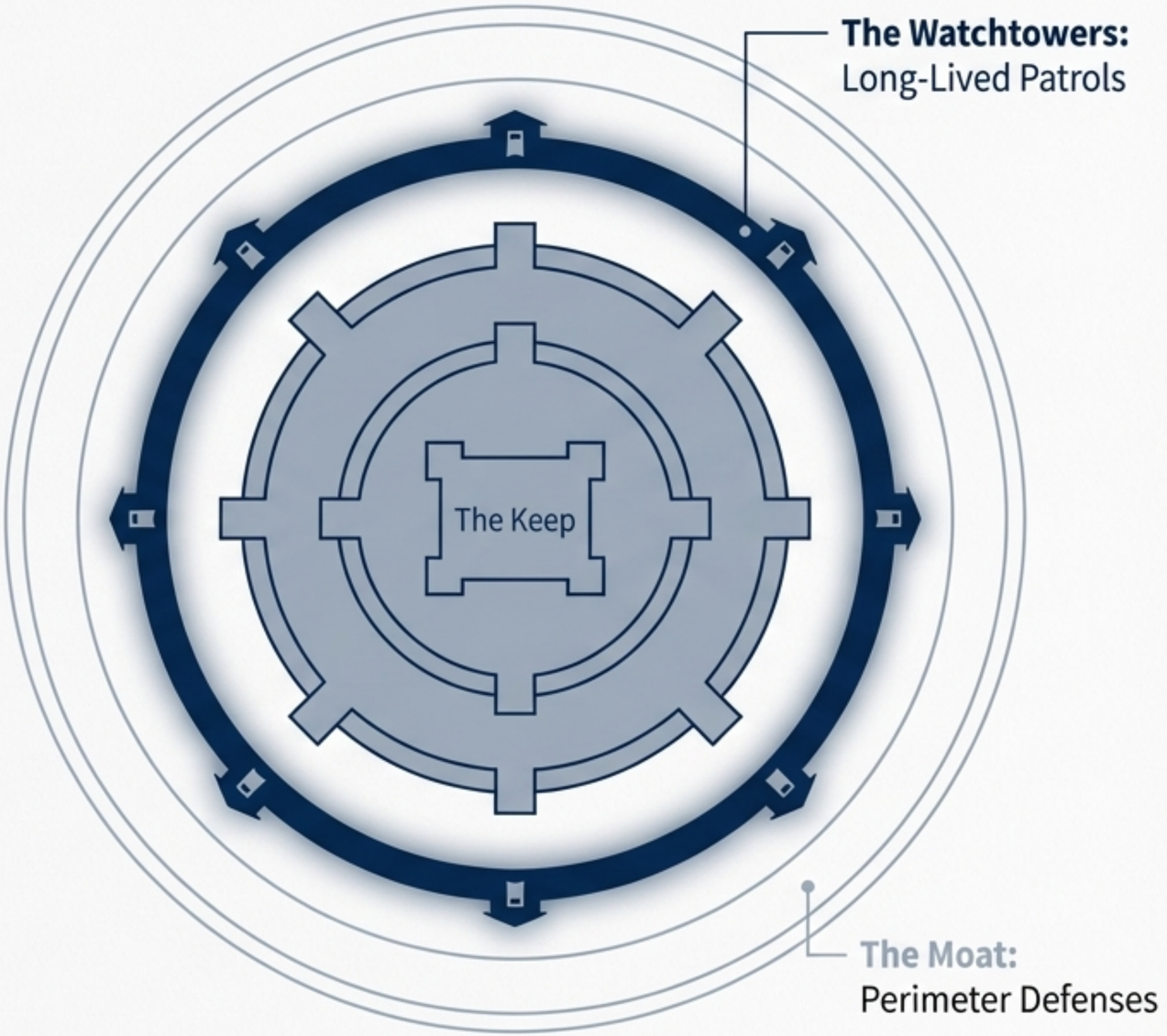
Short-lived tokens are secure but create a poor user experience. Users need to maintain sessions without constant re-authentication.

Solution/Capabilities

A complete token lifecycle management system compliant with modern security standards.

Proof Points

- Secure token refresh via Refresh Token Rotation (RFC 6749)
- RFC 7009-compliant token revocation for secure logout
- Full session management: list, revoke specific sessions, and global logout



The Moat: Building the Perimeter Defenses

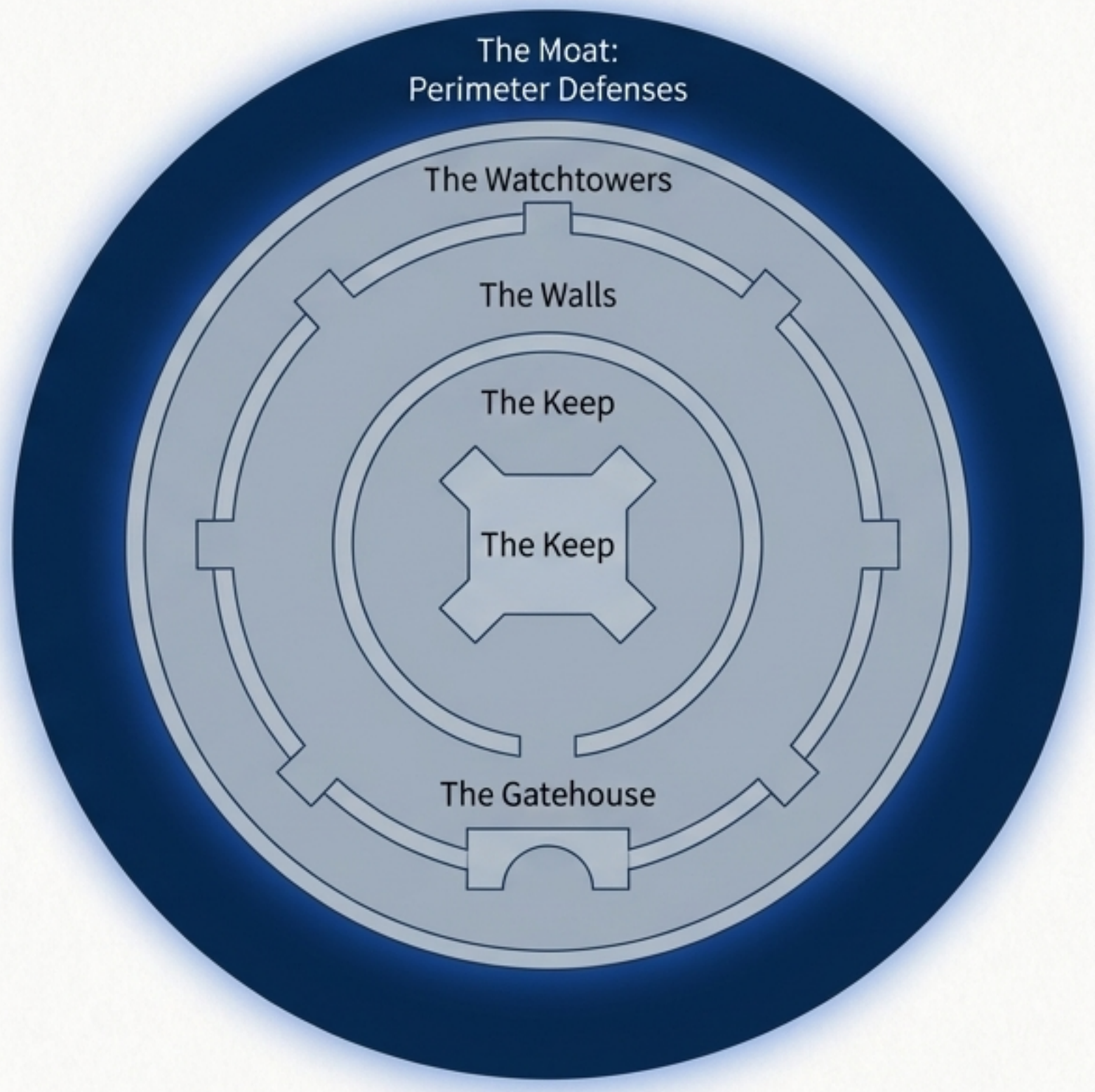
A secure fortress is a valuable target. It requires proactive defenses to repel automated attacks and prevent abuse.

Solution/Capabilities

A multi-faceted rate limiting and abuse prevention middleware.

Proof Points

- Sliding window algorithm limits requests per-IP, per-User, and per-Client
- OWASP-compliant authentication protections (progressive backoff, account lockout)
- Bounded Fail-Open policy with in-memory fallback for high availability



Phase 0 Complete: The Foundation is Secure.

- **Identity Core**: Secure, standards-based authentication.
- **Sovereign Territories**: Full multi-tenancy and client isolation.
- **Rules of Engagement**: Granular, auditable consent management.
- **Long-Lived Patrols**: Complete token refresh and revocation lifecycle.
- **Perimeter Defenses**: Robust rate limiting and abuse prevention.

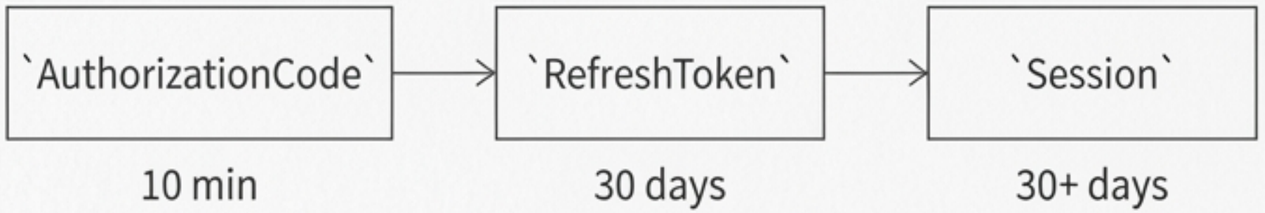
7
PRDs Delivered

~60-80
Hours of Focused Effort

21
Calendar Days from Start to Finish

Inside the Walls: A Foundation Built for Scale

The design of our token and session management system showcases our commitment to robust, maintainable architecture.



Core Decision:
We explicitly separated `AuthorizationCode`, `RefreshToken`, and `Session` into distinct models with independent lifecycles.

Rationale:

- **Clear Lifetime Boundaries**: Codes (10 min), RefreshTokens (30 days), Sessions (30+ days).
- **Independent Cleanup**: Expired codes are deleted without touching active sessions.
- **Privacy-First**: Hashed device fingerprints instead of raw PII.
- **Reduced Memory Footprint**: No dead fields occupying space after their purpose is served.

The Horizon: With the Foundations Secure, We Build the Core Identity Plane.

Phase 0 provides the secure, operational bedrock required for Phase 1, which will deliver Credo's core value proposition.

What's Next (Phase 1):

- Registry Integration (PRD-003)
- Verifiable Credentials (PRD-004)
- Decision Engine (PRD-005)
- Audit & Compliance Baseline (PRD-006)