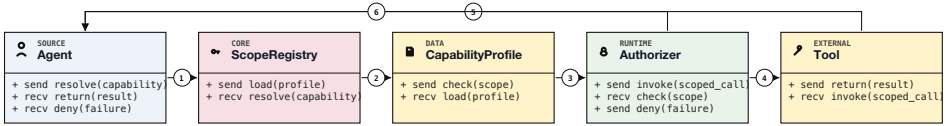
P25 Scope-based authorization and profiles

Primitive · A² A2 · registry role collaboration

Bind capabilities to explicit scopes.

STRUCTURE · PARTICIPANT COLLABORATION



PATTERN INTERFACE

context
A caller invokes a method or service with an operator, session, or agent identity.

trigger
Capability is checked against a requested scope.

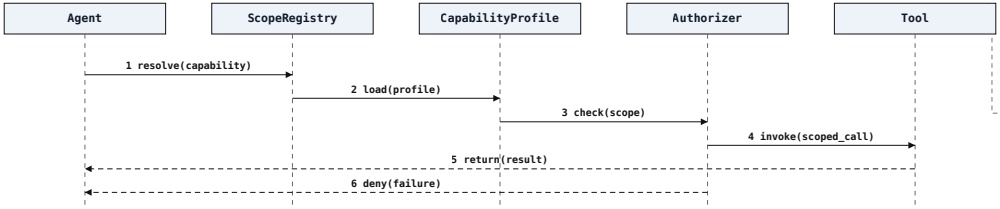
structure
Scope identity, profile, grant and revocation state, and resolution function.

effect
The call is permitted only if the principal currently holds a covering scope.

CONTRACT ANNOTATIONS

requires	Principal identity and requested capability are explicit.
ensures	Authorization is evaluated at the call boundary and records the covering scope.
invariant	Scopes are not inherited beyond declared containment or lifetime.
violation	Missing, expired, revoked, or cross-scope capabilities are denied explicitly.

INTERACTION



MESSAGE TRACE `1 resolve(capability) → 2 load(profile) → 3 check(scope) → 4 invoke(scoped_call) → 5 return(result) → 6 deny(failure)`

Evidence: 41/41 repositories, 36/36 families; 41 trajectories (20 multi-checkpoint); exact audit: not sampled.

Variation: Method scopes, roles, session grants, profiles, and delegated identities.

Negative control: A boolean admin flag is not a scope model.