

# Delegation Trust Packet Profile

**Status:** Draft (Normative)

**Purpose:** Define the rules and invariants governing delegation of authority using chained Trust Packets.

## 1. Overview

Delegation allows an Issuer to grant limited authority to another entity without transferring identity or root control.

Delegation is expressed exclusively through Trust Packets.

## 2. Delegation Invariants

All delegation MUST satisfy:

- Explicit grant
- Scope reduction only
- Independent verifiability
- Temporal limitation

Authority MUST never expand across delegation boundaries.

## 3. Delegation Packet Structure

A Delegation Trust Packet MUST include:

- Reference to parent packet hash
- Delegated subject identity
- Explicit scope subset
- Expiration timestamp

## 4. Chain Validation Rules

Verifiers MUST:

1. Validate each packet independently
2. Validate chain order via hash references
3. Enforce monotonic scope reduction
4. Enforce expiration at every hop

Failure at any step invalidates the chain.

## 5. Revocation Propagation

Revocation of any packet in a chain invalidates all downstream packets.

Verifiers MUST check revocation status at each hop.

## 6. Example

Issuer → PSP → Device Agent

- Issuer grants `pay:amount<=100`
- PSP grants `pay:amount<=50`
- Device executes payment

Verifier confirms scope never expands.

## 7. Security Considerations

Delegation threats:

- Scope escalation
- Replay
- Stale delegation

Mitigations:

- Canonicalization
- Hash chaining
- Temporal bounds

## 8. Conformance

Implementations MUST enforce all delegation invariants.