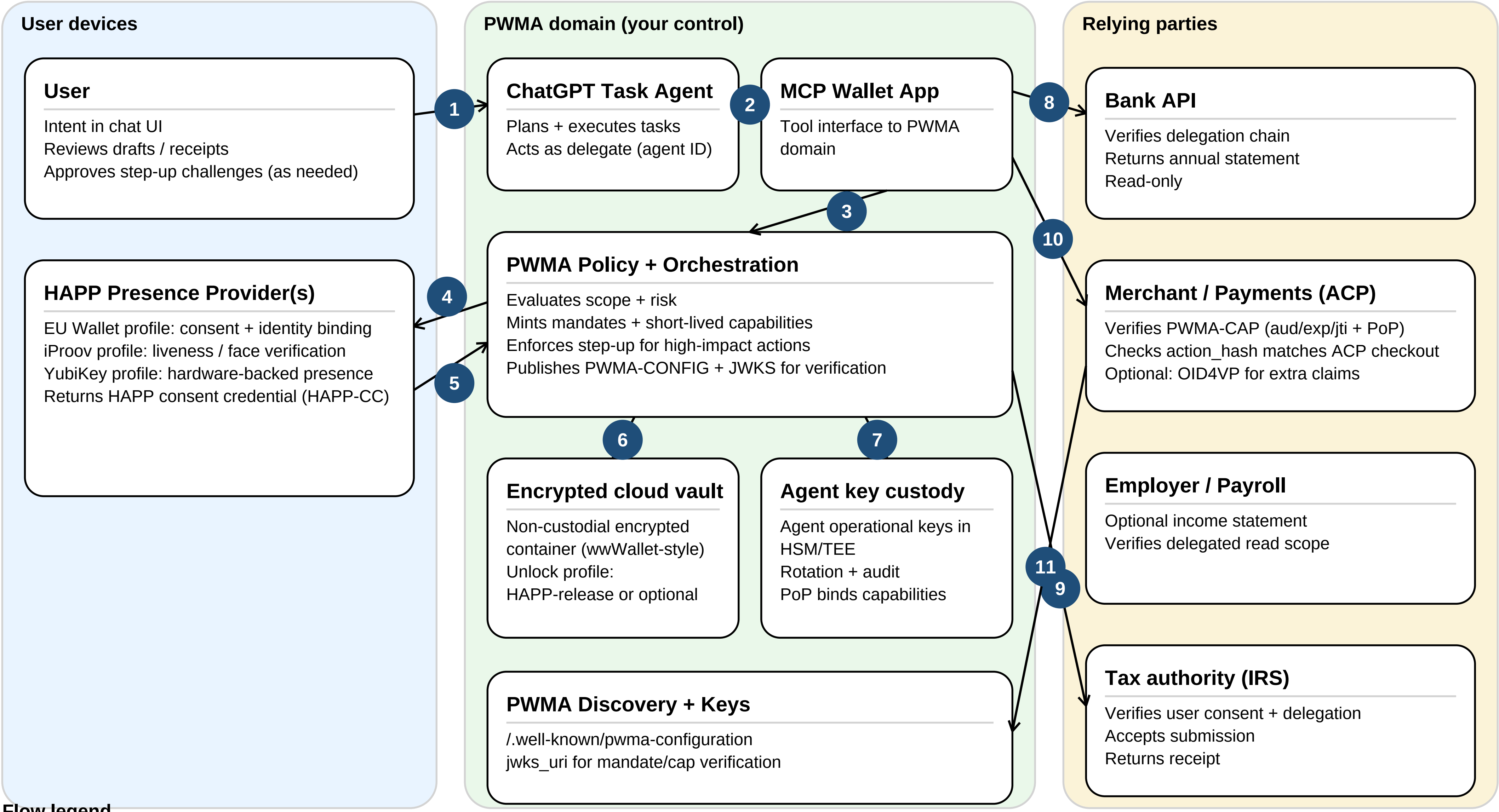
PWMA Wallet Architecture for ChatGPT (MCP Wallet App + HAPP Step-up)

Trust boundaries, key custody, and RP verification (PWMA discovery/JWKS + ACP action hashing)



User devices

User

Intent in chat UI
Reviews drafts / receipts
Approves step-up challenges (as needed)

HAPP Presence Provider(s)

EU Wallet profile: consent + identity binding
iProov profile: liveness / face verification
YubiKey profile: hardware-backed presence
Returns HAPP consent credential (HAPP-CC)

PWMA domain (your control)

ChatGPT Task Agent

Plans + executes tasks
Acts as delegate (agent ID)

MCP Wallet App

Tool interface to PWMA domain

PWMA Policy + Orchestration

Evaluates scope + risk
Mints mandates + short-lived capabilities
Enforces step-up for high-impact actions
Publishes PWMA-CONFIG + JWKS for verification

Encrypted cloud vault

Non-custodial encrypted container (wwWallet-style)
Unlock profile:
HAPP-release or optional

Agent key custody

Agent operational keys in HSM/TEE
Rotation + audit
PoP binds capabilities

PWMA Discovery + Keys

/.well-known/pwma-configuration
jwks_uri for mandate/cap verification

Relying parties

Bank API

Verifies delegation chain
Returns annual statement
Read-only

Merchant / Payments (ACP)

Verifies PWMA-CAP (aud/exp/jti + PoP)
Checks action_hash matches ACP checkout
Optional: OID4VP for extra claims

Employer / Payroll

Optional income statement
Verifies delegated read scope

Tax authority (IRS)

Verifies user consent + delegation
Accepts submission
Returns receipt

Flow legend

1 Intent in chat
2 Agent requests mandate/capability via MCP
3 PWMA policy evaluates request
4 Step-up elicitation via HAPP presence provider
5 User signs approval / consent (HAPP-CC)
6 Persist mandate/delegation + receipts (encrypted vault)
7 Mint short-lived capability bound to agent keys (PoP)
8 Fetch evidence (bank/employer) using delegation
9 Submit high-impact action with user consent + delegation
10 Purchase/checkout under envelope (ACP action_hash)
11 RPs fetch PWMA-CONFIG + JWKS to verify mandates/caps