OpenVPT — Verified Person & Age Token

Version 1.1 · Public Working Draft · Whitelist & Trust Model Overview

This document provides a high-level overview of the OpenVPT protocol and its whitelist-based trust model used by digital platforms to validate verified personhood and age group signals without exposing identity data.

Purpose

OpenVPT enables platforms to distinguish real human users from bots, synthetic identities, and underage accounts using cryptographically verifiable tokens issued by trusted Identity Providers.

Why verified personhood matters

The modern internet was never designed to reliably distinguish a real human from automated or coordinated entities. As a result, platforms increasingly face large-scale abuse including bot amplification, fake engagement, deepfake impersonation, and underage access to restricted services.

Traditional identity verification approaches attempt to solve these problems by collecting and storing sensitive personal data. This creates privacy risks, regulatory burden, and user friction — while often exceeding what platforms actually need.

OpenVPT introduces a different model: proof of verified personhood and age group without revealing legal identity. Platforms receive only minimal, cryptographically verifiable signals — not documents or personal records — enabling safer online spaces without mass identity exposure.

Whitelist and Trust Policy concept

OpenVPT deliberately separates the technical protocol from trust decisions. Each platform defines its own Trust Policy, including a whitelist of accepted issuers, minimum assurance levels, and policy profiles appropriate for its jurisdiction and risk model.

What platforms actually validate

When validating an OpenVPT token, platforms do not evaluate a user’s identity. Instead, they verify a compact set of signals required for access control and safety decisions:

- Verified personhood (verified_person = true)
- Verified age bracket (e.g. age_over_18 = true)
- Trust or assurance level meeting platform requirements
- Token issuer included in the platform’s whitelist
- Token validity, signature, and revocation status

Example minimal claims

{ verified_person: true, age_over_18: true, trust_level: 4 }

How it works

1. An Identity Provider verifies a natural person using approved methods.
2. The provider issues a Verified Person & Age Token (VPT).
3. The Relying Party validates the token according to its Trust Policy whitelist.

Privacy guarantees

OpenVPT tokens never contain name, date of birth, address, national identifier, or document numbers. Only boolean or bracketed verification signals are shared.

Status and alignment

OpenVPT 1.1 is a Public Working Draft aligned with eIDAS 2.0 and EU Digital Identity Wallet principles. This document is intended for evaluation, feedback, and pilot discussions.

Author: Vojtěch Sejkora · License: Apache 2.0 · 2025
https://openvpt.dev