

OPENAGE

OpenAge Practice Statement

ISO 27566-1

Executive Summary

In our increasingly digital world, users are frequently asked to prove their age to access online content and services. This process is often repetitive, inconvenient, and raises significant privacy and security concerns as users are required to share sensitive personal data multiple times. The OpenAge Initiative addresses this challenge with *AgeKeys*, a privacy-preserving, reusable age assurance solution designed for global interoperability.

An AgeKey functions as a trusted age proof, allowing users to verify their age once and then reuse that verification credential across different digital services without repeatedly sharing their personal information. This approach dramatically reduces friction for users and minimizes data sharing, creating a safer and more seamless online experience.

AgeKeys are built on two core principles: the separation of issuance and reuse, and the strict segregation of information. An AgeKey is fundamentally a combination of two elements:

1. A user-held passkey, which is a secure credential stored on a user's device (such as a phone or computer) based on the global WebAuthn/FIDO2 standard.
2. A minimal age signal (e.g., "over 18" or an age bracket) issued by an Age Assurance Provider.

The process is simple:

- **Creation (One-Time Event)**: A user completes an age assurance process, for example on agekey.org or on a participating platform or service. An AgeKey can then be created, securely binding the verified age signal to the user's passkey on their device.
- **Reuse (Lightweight and Repeatable)**: To access another Age-Restricted Platform or Service, the user simply authenticates with their AgeKey. The AgeKey provides the Age-Restricted Platform or Service with a simple "pass" or "fail" answer based on its age policy, without sharing the user's actual age or identity.

A key innovation of AgeKey is its ability to enable *double anonymity* by strictly separating the information that each party sees during an age assurance process. This ensures that each party in the flow only learns what it strictly needs to perform its role. No single actor has enough information to link a user's identity, their age signal, and the specific services they are accessing. This architectural design means that a user's identity, their age, and their browsing habits cannot be linked together by any single party, providing a powerful layer of privacy.

- **Age-Restricted Platform or Service:** knows the service being accessed and ultimately allows/blocks access, but receives only a confirmation (pass/fail) of whether the user is above their established age threshold.
- **Age Assurance Orchestrator**: knows which Age-Restricted Platform or Service is requesting an age signal, but does not know the identity of the user, recognize them across sessions, or learn their age.
- **OpenAge (AgeKey Manager)**: recognizes and evaluates the AgeKey against the

requested age threshold, but does not know which Age-Restricted Platform or Service the user is accessing.

AgeKeys are designed and engineered to meet high regulatory and international standards across different areas of assessment:

- **Functionality:** Built on the open and interoperable OpenID Connect (OIDC) standard, AgeKey allows a user to verify once and reuse their credential across any participating platform or service, significantly reducing user friction.
- **Performance**: The reuse of an AgeKey is extremely fast, typically taking only about 3 seconds from initiation to delivery of a result to the Age Assurance Orchestrator.
- **Privacy**: This is the cornerstone of the system. By design, AgeKey minimizes data collection enabling compliance with the double-anonymity principle set by regulators such as the French ARCOM. It does not process or store the information provided by users to prove their age (e.g. face scan, passport, bank details). The participating platform or service only receives the result of that process.
- **Security**: AgeKey leverages the strong, phishing-resistant security of modern passkey technology. The results delivered to services are cryptographically signed to ensure their authenticity and integrity. OpenAge's security practices are regularly audited, and have been recognised by international certifications such as ISO/IEC 27001.
- **Accessibility and Inclusion**: AgeKey is a globally deployed solution, already operating in highly regulated markets. It is technology neutral and can support any type of age assurance method. This variety allows users, including those with disabilities, to select the most usable method that accommodates their individual preferences and needs. AgeKey is designed to be user-friendly and intuitive, and is supported by various publicly available resources to ensure transparency.

The secure operation of AgeKey relies on the assumptions that (i) users access the service from a personal device whose operating system and primary browser natively support passkey authentication; (ii) the passkey ecosystem (OS, platform account, authenticator) is secure as designed; (iii) Age Assurance Orchestrators correctly configure AgeKey and API calls to meet their compliance requirements; (iv) Age Assurance Providers supply accurate age signals; (v) a stable internet connection exists for all parties. These factors are outside the certified scope of AgeKey, which focuses on the secure orchestration of the compliance workflow. AgeKey effectiveness has been independently tested and evaluated in the Australian Government's Age Assurance Technology Trial, where it achieved a high Technology Readiness Level (TRL) of 8.

On this basis, AgeKey operates as a rule-based, deterministic orchestration layer, technology and demographic-neutral by design, granting effectiveness classification: Strict.

Further details about the OpenAge Initiative and AgeKey are available at https://openageinitiative.org/, https://agekey.org/, in our Developer Documentation at https://docs.agekey.org/, and on k-ID Privacy and Security Center at security.k-id.com.