

ISO 27566-1 Practice Statement

Solution Owner: Eden Game Development Centre

Eden Game Development Centre is a(n) Age Assurance Provider (an entity responsible for providing age assurance results to a relying party)

This is a practice statement for the age assurance solution known as Verified Accounts

The system and practice statement are kept under continuous and regular review in the following way:

With key components being developed and tested as part of our governance approach, we are establishing a framework for continuous and structured review, including oversight by senior management. This will ensure that the system evolves in alignment with regulatory requirements, privacy and security standards, and emerging best practices.

Top management will play a central role in reviewing performance data, audit findings, and user feedback at regular intervals. These reviews will guide improvements and ensure the system remains effective, transparent, and responsive as it moves toward full deployment.

This solution is designed to test the following age eligibility requirements:

Age eligibility is determined through verification of official documentation provided by the user, which is automatically cross referenced with authoritative government databases. This ensures a clear and objective determination of whether the individual meets the required age threshold. There is no ambiguity in age assessment, as it relies solely on factual data derived from official sources. The age requirement criteria are established by the relevant policymakers, service providers, or regulatory authorities, and our system complies with those mandates. Any intermediaries involved in processing or validating this information are vetted and operate under strict accountability protocols.

This solution utilizes the following Age assurance components:

The system uses a two-step age assurance process. First, the user submits identity and age documentation, which is automatically compared against government records to confirm its authenticity and accuracy. This verification step is strictly based on primary credentials such as birth certificates or passports. No age estimation, inference, or behavioral analysis is used at any point. Second, a live video call is scheduled with a trained verifier to confirm that the individual presenting the documents matches the provided information. This final confirmation links the individual to the verified account, ensuring a high level of confidence in the result.

This solution delivers results to meet the following Indicators of confidence:

We aim to achieve 80% age assurance confidence for 20% of the effort. The initial document and data verification against government databases ensures that the information provided is 100% genuine. The follow-up video verification adds an additional layer of assurance by confirming the person's identity visually and interactively. This process creates a level of certainty equivalent to setting up a bank account or obtaining a driver's license in person. It is not technically feasible to guarantee that the verified user is the only person using the account at all times, attempts to enforce such a standard would require excessive intrusiveness and would not be proportionate to the legal, privacy and human rights considerations involved. Exponential costs for marginal gains.

The solution applies the following Binding process:

The verified account is bound to the individual through a two stage process: initial document verification and a video call with a responsible verifier. Each verifier is accountable for their confirmations, and any repeated verification errors are investigated. If necessary, corrective actions are taken.

Binding beyond the verified individual account to the real-time user is not technically feasible without disproportionate intrusion or surveillance.

If I have 100% age assurance confidence verified, then while watching a youtube video hand my phone to my child the real time person using the phone is not the correct individual and bypasses the age assurance.

There is no reasonable way to “bind the process” to the degree of dealing with handing a phone to the person next to you or a person swapping in the seat on the PC, that couldn’t also be beaten by someone who was equally unreasonably dedicated to bypassing it.

The solution achieves Privacy and data protection as follows:

All personal data collected for the purpose of age assurance is strictly limited to what is necessary for verification. Data is processed solely to fulfill legal and policy requirements and is stored securely in accordance with applicable data protection laws. Personally identifiable information is not used for any unrelated purpose and is only retained as long as necessary to meet regulatory requirements. Users are informed of their rights, including access to their data, the ability to challenge inaccuracies, and protections against automated decision-making. Data handling processes include strong encryption and breach protocols to ensure integrity and accountability.

Organisations may request the age of a verified account but it is up to the individual to accept or deny that request to allow the individuals to decide who receives what information.

The solution demonstrates ease of use as follows:

The age assurance system is designed to be simple and familiar. For most users, the experience mirrors existing account systems. Signing in is the same as usual via username and password. The only additional steps occur at account creation, where users upload their identification documents and participate in a brief video verification call. These tasks are straightforward and manageable for anyone with basic digital skills. The system is accessible to users of varying ages and does not complicate or hinder typical usage of digital services.

By design. One of the core goals is to be as easy to use and non burdensome on users as possible to make adoption as easy as possible and even desirable.

Security measures applied to the solution are as follows:

The system employs standard, secure practices including encryption of all sensitive data and the option for users to enable two-factor authentication. Only the minimum necessary personal information is collected to fulfill age assurance requirements. All system interactions and data flows are logged and monitored to ensure full traceability and security compliance.

The solution protects human rights in the following ways:

The system is designed to be inclusive, non-discriminatory, and respectful of user rights. It does not, by itself, restrict access to any services. Service providers, governments, and organizations determine how they use verified age information, and users can choose whether or not to share their age assurance details. Any decision to restrict access based on age is the responsibility of the service provider. Users retain full control over whether they participate, and any improper use of age verification to discriminate can be addressed through standard legal and compliance channels.

The solution has been subject to audit, certification and review in the following ways:

The system's operations are fully auditable. Every action taken within the verification process is logged, including data submission, document checks, and verifier confirmations. When implemented, the system will be subject to periodic review and third-party audit to ensure compliance with data protection laws, verification standards, and ethical practices. These audits will include full documentation of auditor qualifications, audit dates, and findings, supporting transparency and continuous improvement.

Primary Contact Details

Lead Contact

[REDACTED]

Lead Contact Email

[REDACTED]

Lead Contact Phone (with country code)

[REDACTED]