Age Estimation Test Report: /DigiChek

Introduction

This report summarizes the results of the independent evaluation of the Age Assurance Software Solution (referred to as the Target of Evaluation, or ToE), performed as part of the Age Assurance Technology Trial. The evaluation focused on the core properties required by ISO 27566-1: functionality, performance, privacy, security and acceptability.

The objective of this test was to assess the readiness and effectiveness of the solution in real-world conditions, to inform regulatory, industry and public stakeholders.

Disclaimer

The inclusion of this test report in the suite of Age Assurance Technology Trial (AATT) documents does not constitute endorsement, certification or approval of any product, service or provider. The findings are based on self-declared information, interviews and test results submitted by participating organisations, and while evaluated under structured criteria, not all claims have been independently verified in full by the Trial team.

This report reflects the status of the technology at the time of testing and within the scope of the Trial. No guarantee is given as to the completeness, accuracy or continued applicability of the findings. The Trial was a technical evaluation only and did not assess legal or regulatory compliance. Inclusion of a test report does not imply market readiness or regulatory acceptance. Any person considering the use of the technology described in this test report should ask the provider for up-to-date evidence of independent conformity assessment of their products or services and should not rely on this test report.

The AATT, Age Check Certification Scheme, nor any of the AATT contractors do not accept any liability for any statements or assessments relied upon in this test report.

Funded by

Australian Government
Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Project by

Age Check Certification Scheme

Amendment register

VERSION	VERSION DATE	AMENDMENT DESCRIPTION
0.9	30 June, 2025	Initial release
1.0	4 July, 2025	Approved for release
1.1	8 July 2025	Minor update to references

Approvals:
This document has been approved for release by:
Mark Pedersen

References

Document	Location (URL address or Other)
ALM Octane – Test Cases	Test Case Execution Dashboard

Glossary

Term	Meaning
ToE	Target of Evaluation

Target of Evaluation

Product Name and Provider

- **Product Name**: DigiChek
- **Provider Name**: DigiChek Pty Ltd
- **Version Number/Description**: Current at the time of testing

Provider's Practice Statement

The DigiChek **practice statement**—submitted as part of the Age Assurance Technology Trial (AATT)—outlines the operation and privacy safeguards of their age assurance system. Below is a detailed summary of the key points:

System Overview and Purpose
DigiChek Pty Ltd is an Age Assurance Provider responsible for delivering age assurance results to relying parties. The DigiChek solution enables precise, privacy-preserving, and secure age verification through a user-controlled key system. Its primary purpose is to empower individuals to confirm their age or identity without the need to share sensitive documents or personal credentials with querying organisations. This ensures individuals retain privacy while supporting organisations in meeting legal and regulatory obligations for managing age-restricted content and services.

DigiChek offers three core age assurance outcomes:

- Verification of exact age
- Confirmation of being over or under a certain age
- Confirmation of being within a specific age range

All verification occurs in person during profile creation, ensuring a trusted, intermediary-free foundation for future age assurance queries.

Methods and Confidence Indicators
Adults:
Verification is conducted by a DigiChek Registrar—an authorised agent of a third-party organisation registered and recognised by the Australian government. The Registrar confirms the user's identity using primary credentials compliant with the 100-point ID check. The verified information (name, date of birth, place of birth) is used to create a DigiChek profile.

Children:
Verification is facilitated by schools during enrolment. As part of this trusted process, schools submit the child's name, date of birth, and place of birth directly to DigiChek—no credentials or additional documents are shared.

Confidence Indicators:

Confidence is upheld through:

- In-person identity verification
- Use of immutable identity data
- A secure, user-generated DigiChek Key
- Cryptographically protected data handling

DigiChek calculates age based on the verified date of birth and responds with the age assurance outcome requested by the querying organisation.

Aligns with core **indicators of confidence** as defined in **ISO 27566**.

Binding and Workflow

When a user creates their DigiChek profile, they generate a **DigiChek Key** that consists of their date of birth (DDMMYYYY) followed by 4 to 10 user-selected characters. This Key:

- Is **permanently bound** to the user's DigiChek profile
- Can only be changed by the user
- Is **never transmitted or stored** outside the DigiChek system

To initiate an age or identity query:

- The querying organisation submits the user's name, date of birth, and place of birth
- The user provides their DigiChek Key

If the data matches the profile, DigiChek provides:

- Yes/No confirmation of profile existence
- Exact age, or Yes/No to an age-based query

Security questions, set and managed solely by the user, control access to and updates of the DigiChek Key.

Privacy and Data Handling

DigiChek is built with a privacy-by-design approach, focused on **data minimisation** and **user control,** in line **with ISO 27566-1:2025**. It stores only:

- Name
- Date of Birth
- Place of Birth

It **does not**:

- Collect or store government credentials, documents, or biometric data
- Share or transmit identifying information to querying organisations
- Receive additional data from third parties beyond the initial verified fields

Adults' credential and photo records are retained by the verifying third-party organisations—not DigiChek.

Children's information is sourced solely from schools, with no additional documentation provided.

Querying organisations receive only the age assurance result—not the underlying personal data and **Non-Disclosure of Exact Age**. DigiChek does not track user activity or digital behaviour, ensuring minimal digital footprints and mitigating risks of data over-sharing.

Accessibility and Usability

DigiChek is designed for universal access, is of **globally scalable design** and **designed for users of all ages**, regardless of:

- Age
- Device type
- Digital literacy level
- Language or cognitive capacity

Key usability features include:

- A simple key format (DOB + 4–10 characters), with full personalisation options
- Support for any language in key creation and security questions
- **Frictionless user experience** via device-agnostic design, compatible with legacy or adaptive hardware
- No requirement for high-speed connectivity or advanced technical skills

The system mimics the widely familiar **username/password model**, making it intuitive and accessible for all users—including children, neurodivergent individuals, and those in low-connectivity environments.

Security and Certification

DigiChek employs a **decentralised security model** with layered protections:

1. No centralised database—credentials are stored separately
2. User ownership of DigiChek Key and security controls
3. Verified identity required for profile creation
4. Encrypted communication and tamper-proof data
5. Reduced liability for relying on organisations by avoiding document handling
6. Protection against identity theft—identity data is useless without the Key
7. Minimal exposure—no expansion of the user's digital footprint
8. Strong privacy controls—no biometric, behavioural, or financial data involved

DigiChek is advancing toward **formal certification** under international standards. It currently aligns with:

- The General Data Protection Regulation (GDPR)
- The EU Digital Services Act
- The European Data Protection Board Statement 1/2025 on Age Assurance

Follows ISO/IEC 27566-1:2025 guidance on privacy and security.

Governance and Review

DigiChek's system and practice statement **actively prepares for Audits** and undergo **continuous and regular review** by senior management and the development team. These reviews are prompted by:

- Functional updates in response to client needs
- Legislative or regulatory changes
- Internal quality assurance and compliance monitoring

The system maintains compliance with the **13 Australian Privacy Principles (APPs)**, with demonstrated controls over:

- Transparency
- User consent and control
- Prevention of unsolicited data collection
- Avoidance of government identifiers
- Security of immutable identity data
- ***and demonstrates alignment with industry standards and frameworks***

This governance framework ensures DigiChek remains secure, lawful, fair, and inclusive—particularly for children, marginalised individuals, and privacy-conscious users—while upholding fundamental rights including **privacy**, **autonomy**, and **equitable access**.

Technology Readiness Assessment (TRL)

TRL	Definition
TRL 1	**Basic Research**: Initial scientific research has been conducted. Principles are qualitatively postulated and observed. Focus is on new discovery rather than applications.
TRL 2	**Applied Research**: Initial practical applications are identified. Potential of material or process to solve a problem, satisfy a need or find application is confirmed.
TRL 3	**Critical Function or Proof of Concept Established**: Applied research advances and early stage development begins. Studies and laboratory measurements validate an
TRL 4	**Lab Testing/Validation of Alpha Prototype Component/Process**: Design, development and lab testing of components/processes. Results provide evidence that performance targets may be attainable based on projected or modelled systems.
TRL 5	**Laboratory Testing of Integrated/Semi-Integrated System**: System Component and/or process validation is achieved in a relevant environment.
TRL 6	**Prototype System Verified**: System/process prototype demonstration in an operational environment (beta prototype system level).
TRL 7	**Integrated Pilot System Demonstrated**: System/process prototype demonstration in an operational environment (integrated pilot system level).
TRL 8	**System Incorporated in Commercial Design**: Actual system/process completed and qualified through test and demonstration (pre-commercial demonstration).
TRL 9	**System Proven and Ready for Full Commercial Deployment**: Actual system proven through successful operations in operating environment and ready for full commercial deployment.

The vendor rates the ToE to be at TRL 5.

Testing Scope and Approach

The evaluation process followed principles defined in ISO/IEC 29119-2:2023, utilizing a single test level to structure the required test activities:

- Acceptance testing

Testing comprised the following activities:

- Requested providers to demonstrate their services as part of the evaluation process.
- Developed a set of test scenarios based on the initial demonstration and system capabilities.
- **Shared the test scenarios with the provider** in advance to ensure preparedness and transparency.
- **Facilitated a follow-up session** where the provider executed the test scenarios using their live website.
- **Recorded the scenario** for virtual reference, documentation, and further review.
- **Testing approach focused on real-world use cases** to validate functionality, reliability, and user experience.

Static reviews were used on evaluation of features relating to privacy, data security, compliance with human rights requirements and technology readiness assessment. Dynamic testing of these features for each participating technology was beyond the scope of the current trial; however dynamic testing of these features is recommended for any technology being deployed.

Static reviews comprised a review of the provider's practice statement and interviews with the provider to clarify any additional details.

Test Schedule

Testing was conducted between 20th May,2025 and 20th June,2025

Evaluation Results

The Age assurance scenarios are listed in the table below.

Test Sceanrios	Results
Create DigiChek Key for 13+ User	Pass
Create DigiChek Key for 16+ User	Pass
Create DigiChek Key for 18+ User	Pass
Validate 13+ Age Using Stored DigiChek Key	Pass
Validate 16+ Age Using Stored DigiChek Key	Pass
Validate 18+ Age Using Stored DigiChek Key	Pass
Validate Cross-Browser and Site Compatibility (Chrome, Firefox, Safari, Edge)	Pass
Validate DigiChek Key does not store any personal information (e.g. name, ID number)	Pass
Validate No Personal Data Transmission During Use (no personally identifiable information is sent during DigiChek Key verification.)	Pass
Validate No Personal information or Excessive Data Stored on Backend	Pass
Validate Required Documents for DigiChek Key Creation (e.g., ID, bank record, third-party provider)	Pass

Evaluator Observations

Overall, usability of the system could be considered acceptable based on feedback from the demonstration and testers observations.

Strict governance and privacy protocols were identified and documented.

Robust data protection and business needs only access to view data has been clearly documented and demonstrated.

Based on the testing conducted, the ToE demonstrates the capabilities described in the practice statement and is aligned to the claimed TRL.

Vendor Comments on Evaluation Results

TBC