Age Assurance Technology Trial
Preliminary Findings Event
June 20th 2025

Tony Allen

Project Director

CEO, Age Check Certification Scheme & Digital ID Systems Certification

Funded by

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

Project by

Age Check Certification Scheme

Age Assurance Technology Trial

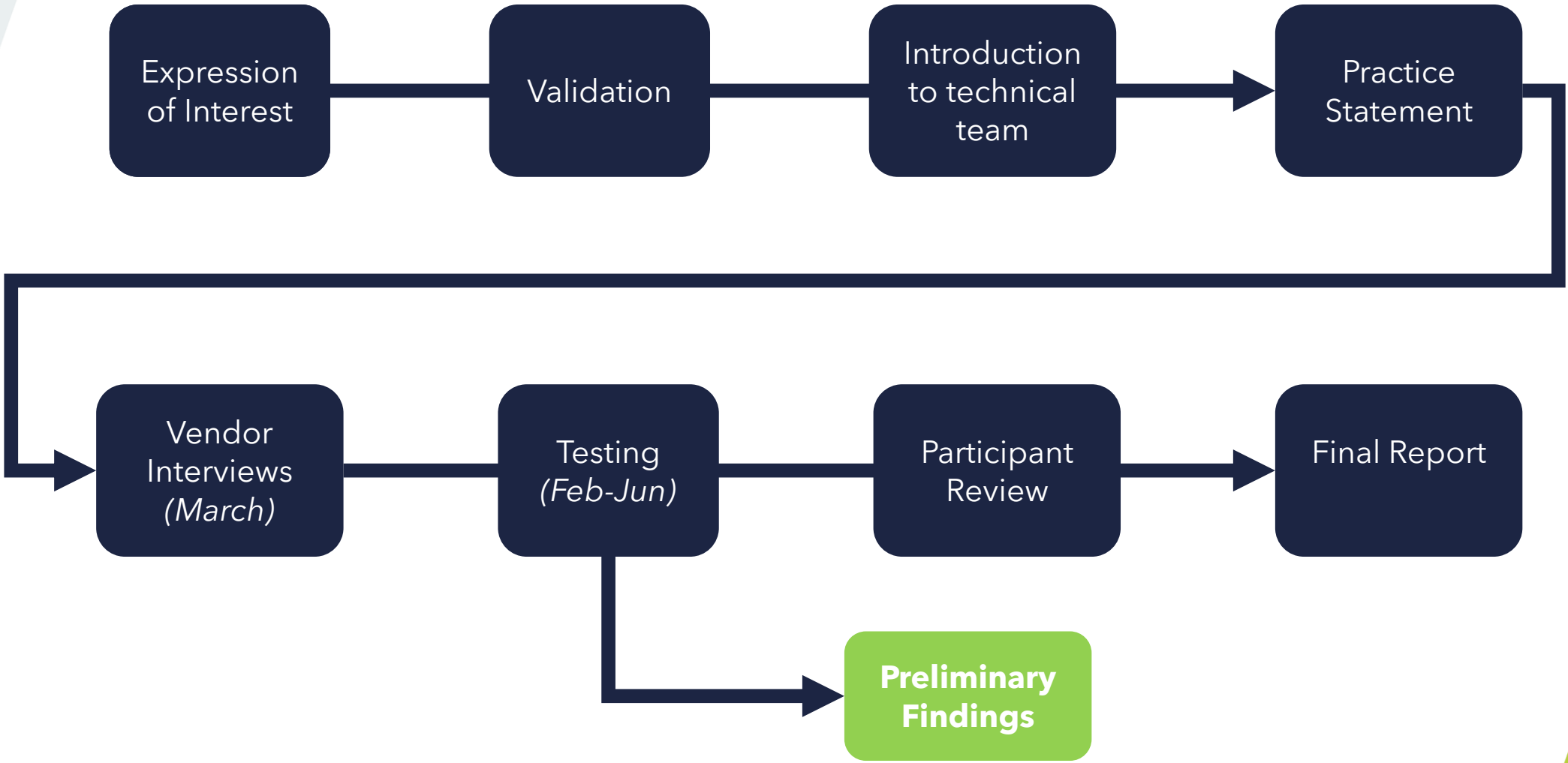
- 10:00am – Welcome
- 10:05am – Preliminary Findings
- 10:45am – Q&A
- 11:00am – Next Steps…

- 2:00pm – Findings and Practice Statements released on www.ageassurance.com.au

Notes for the media:

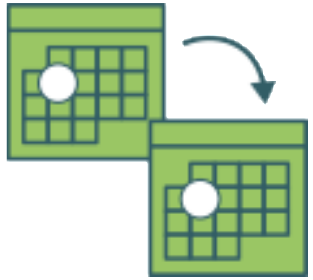
- This is a private briefing so should not be recorded for transmission
- The embargo on the news release issued in advance of this event has been lifted.

Reminder of the trial process



Age Assurance Methods

Age Verification Methods

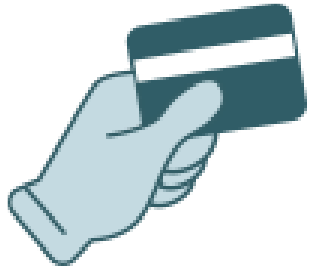


Calculating the difference between a verified year or date of birth of an individual and a subsequent date

Age Estimation Methods

Analysis of biological or behavioural features of humans that vary with age

Age Inference Methods



Verified information which indirectly implies that an individual is over or under a certain age or within an age range

Successive Validation

Additional Approaches

- Parental Controls
- Parental Consent
- Tech Stack Alternatives

Accreditation Layer	**ISO/IEC 17065:2012** Conformity assessment – Requirements for bodies certifying products, processes and services
Evaluation Model Layer	**ISO/IEC 25010:2023** Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Product quality model
Core Characteristics of Age Assurance Technologies Layer	**ISO/IEC DIS 27566-1:2025** Information security, cybersecurity and privacy protection – Age assurance systems – Part 1: Framework - *We will also apply Parts 2 & 3 as appropriate, but they remain in early stages of development*
Implementation Requirements and Testing & Metrics Layer	**IEEE 2089.1:2024** Standard for Online Age Verification ISO/IEC/IEEE 29119 series - Software testing

Age Assurance Systems - Framework

Clause 6
Functional Characteristics

Clause 7
Performance Characteristics

Clause 8
Privacy Characteristics

Clause 9
Security Characteristics

Clause 10
Acceptability Characteristics

Clause 11
Practice Statements

Technology Readiness Levels

- Analysis of the Technology Readiness Level is important for understanding the preliminary findings
- Each type of technology and each provider of that technology has had their TRL level reviewed
- This will help to place the results in context

A.÷ Structure of the Report

A.÷.÷ The Australian Age Assurance Technology Trial report consists of ten separate but interlinked reports, each examining a different aspect of age assurance technology. Together, they provide a comprehensive view of the trial's findings, methodologies and recommendations.

Part A: Main Report

A.÷.÷ Provides the overarching summary of findings across all technology types, including the Australian context, stakeholder engagement and forward-looking insights. Includes a summary of the analysis of age verification, estimation, inference, successive validation, parental consent, parental control and tech stack deployment.

Part B: Methodology and Ethics Approach

A.÷.÷ Outlines the research design, data collection, analysis methods, ethical framework and risk management strategies that underpinned the trial. Emphasises rigour, transparency and integrity in data handling and evaluation.

Part C: Age Verification

A.÷.÷ Explores technologies used to verify a user's date of birth using documents and biometrics. Includes technical, privacy and security analysis, as well as provider practice statements and readiness assessments.

Part D: Age Estimation

A.÷.÷ Evaluates systems that estimate age based on biometric or behavioural features. Assesses functional and performance characteristics, data protection implications and contextual suitability for Australian users.

Part E: Age Inference

A.÷.÷ Focuses on systems that infer age from user behaviour, digital footprints or contextual signals. Reviews effectiveness, ethical considerations and potential risks around profiling and inclusion.

Part F: Successive Validation

A.÷.÷ Examines layered or waterfall models where multiple age assurance methods are applied in sequence. Analyses their adaptability, escalation logic and proportionality in different risk settings.

Part G: Parental Control

A.÷.÷ Investigates pre-configured restrictions across devices, platforms or services. Analyses the effectiveness, overreach risks and alignment with children's evolving rights and capacities

Part H: Parental Consent

A.÷.÷ Reviews mechanisms for obtaining guardian permission at the point of access. Considers legal integrity, usability and inclusion across diverse family and care arrangements.

Part J: Technology Stack Deployment

A.÷.÷ Assesses how age assurance is embedded across layers of the digital ecosystem - device, OS, network or app-level. Explores scalability, integration challenges and future potential.

Part K: Literature Review and Bibliography

A.÷.÷ A comprehensive review of academic research, standards, laws, media and advocacy literature relevant to age assurance technologies in Australia and internationally.

Assessment Criteria

1. **Accuracy:** How well the technology can detect a user's age. Assessing the variance of accuracy across different environmental conditions and contexts (including culturally diverse Australian settings)

2. **Interoperability:** Usability across multiple online platforms common in Australia

3. **Reliability:** Consistent performance under Australian conditions (including varied internet access and device usage)

4. **Ease of use:** Usability for all Australians, considering digital literary differences

5. **Minimisation of bias:** Including racial and cultural bias minimisation, essential for Australia's diverse and multicultural society

6. **Protection of privacy:** Compliance with Australian privacy principles (and cultural expectations of privacy)

Assessment Criteria (Continued)

7. **Human rights protections:** Including accessibility for all users, especially those with disabilities, as well as applicable rights under the UN Convention on the Rights of the Child (UNCRC)

8. **Data security:** How well the technology safeguards users' personal information from unauthorised access, breaches or theft

9. **Circumvention:** Resistance to certain kinds of attacks – Clause 9 of ISO 27566-1, including Biometric Presentation and Spoofing Attacks

10. **Technology Readiness Level (TRL):** Ensuring the technology was sufficiently mature for meaningful testing.

Preliminary Findings

About the Preliminary Findings

- The preliminary findings are a set of twelve observations based on the first phases of the Trial's evaluation.
  - They highlight broad patterns and trends seen across all the technologies under test.
  - These findings are not policy recommendations or final conclusions; they are intended to provide transparency and early insights to stakeholders and the public.
  - The preliminary findings summarise high-level observations only.
  - They were also used to enable the project team to complete the challenge and validation phase of the Trial.
  - These findings are intended to enable an early understanding of the likely structure of the final report.
  - More detailed technical assessments, including vendor-specific performance data, will be included in the Trial's final report, which will be released after fair opportunity to respond has been provided to trial participants on their individual findings. This is standard practice in a technology trial drawing conclusions about the performance of individual products.

The preliminary findings may change in the final report.

The interim report's findings address a number of topics

Technological Feasibility	No Major Barriers	Independent Validation	No One-Size-Fits-All
Innovation	Privacy Practices	Demographic Fairness	Room for Improvement
Limitations of Parental Controls	Cybersecurity Compliance	Data Retention Risk	Alignment with Standards

Age assurance can be done in Australia privately, efficiently and effectively.

- Age assurance can be done in Australia - our analysis of age assurance systems in the context of Australia demonstrates how they can be private, robust and effective.
- There is a plethora of choice available for providers of age-restricted goods, content, services, venues or spaces to select the most appropriate systems for their use case with reference to emerging international standards for age assurance.

No substantial technological barriers preventing its implementation to meet policy goals.

- Our evaluation did not reveal any substantial technological limitations that would prevent age assurance systems being used in response to age-related eligibility requirements established by policy makers.
- We identified careful, critical thinking by providers on the development and deployment of age assurance systems, considering efficacy, privacy, data and security concerns.
- Some systems were easier for initial implementation and use than others, but the systems of all technology providers with a technology readiness level (TRL) of 7 or above were eventually capable of integration to a user journey

Provider claims have been independently validated against the project's evaluation criteria.

- We found that the practice statements provided by age assurance providers with a TRL of 7 or above fairly reflected the technological capabilities of their products, processes or services (to the extent applicable to the project's evaluation criteria).
- Some of the practice statements provided have needed to be clarified or developed during the course of the Trial, but we observed that they offer a useful option for transparency of the capabilities of the available age assurance systems.
- Those with a TRL below 7 will need further analysis when their systems mature.

A wide range of approaches exist, but there is no one-size-fits-all solution for all contexts.

- We found a plethora of approaches that fit different use cases in different ways, but we did not find a single ubiquitous solution that would suit all use cases, nor did we find solutions that were guaranteed to be effective in all deployments.
- The range of possibilities across the trial participants demonstrate a rich and rapidly evolving range of services which can be tailored and effective depending on each specified context of use.

We found a dynamic, innovative and evolving age assurance service sector.

- We found a vibrant, creative and innovative age assurance service sector with both technologically advanced and deployed solutions and a pipeline of new technologies transitioning from research to minimum viable product to testing and deployment stages indicating an evolving choice and future opportunities for developers.
- We found private-sector investment and opportunities for growth within the age assurance service sector.

We found robust, appropriate and secure data handling practices.

- We found robust understanding of and internal policy decisions regarding the handling of personal information by trial participants.
- The privacy policies and practice statements collated for the Trial demonstrate a strong commitment to privacy by design principles, with consideration of what data was to be collected, stored, shared and then disposed of.
- Separating age assurance services from those of relying parties was useful as trial participants providing age assurance services more clearly only used data for the necessary and consented purpose of providing an age assurance result.

Systems performed consistently across demographics groups, including Indigenous populations.

- The systems under test performed broadly consistently across demographic groups assessed and despite an acknowledged deficit in training age analysis systems with data about Indigenous populations, we found no discernible difference in the outcomes for First Nations and Torres Strait Islander peoples and other multi-cultural communities using the age assurance systems.
- We found some systems performed better than others, but overall variances across race and gender did not deviate by more than the permitted tolerances set out in IEEE 2089.1.

There is scope to enhance usability, risk management and system interoperability.

- We found opportunities for technological improvement including improving ease of use for the average person and enhancing the management of risk in age assurance systems.
- This could include through one-way blind access to verification of government documents, enabling connection to data holder services (like digital wallets) or improving the handling of a child's digital footprint as examples.

There are limitations to parental control systems particularly during adolescence.

- We found that parental control and consent systems can be done and can be effective when first introduced, however, we found limited evidence that they:
  - could cope with the evolving capacity of children (particularly through adolescence),
  - were able to enhance the rights of children to participate in the breadth of digital experiences,
  - were effective and secure in the management of a child's digital footprint.

Systems generally align with cybersecurity best practice, but vigilance is required.

- We found that the systems were generally secure and consistent with information security standards, with developers actively addressing known attack vectors including AI-generated spoofing and forgeries.
- However, the rapidly evolving threat environment means that these systems - while presently fairly robust - cannot be considered infallible and must be continuously monitored and improved. Privacy compliance must be similarly monitored.

Unnecessary data retention may occur in anticipation of future regulatory needs.

- We found some concerning evidence that in the absence of specific guidance, service providers were over-anticipating the eventual needs of regulators about providing personal information for future investigations.
- Some providers were found to be building tools to enable regulators, law enforcement or Coroners to retrace the actions taken by individuals to verify their age which could lead to increased risk of privacy breaches due to unnecessary and disproportionate collection and retention of data.

Providers are aligning to emerging international standards around age assurance

- The standards-based approach adopted by the trial, including through the ISO/IEC FDIS 27566 Series, the IEEE 2089.1 and the ISO/IEC 25000 series (the Product Quality Model) all provide a strong basis for the development of accreditation of conformity assessment and subsequent certification of individual age assurance providers in accordance with Australia's standards and conformance infrastructure.

Stakeholder Engagement

Professor Jon Rouse

Questions

Next steps…

Final Report
Publication plans

- Draft Final Report will be submitted to government on time by the end of June
- Procedural Fairness process required before publication
  - Each participant can review and comment wherever the report refers to them
- Publication date will be determined by the Minister

- Practice Statements are available on our website www.ageassurance.com.au

Age Check Certification Scheme

@AgeCheckCert

+44 161 443 4111
info@accscheme.com

You can find us here