



Age Assurance Technology Trial

PART C

Age Verification

August 2025



Funded by



Australian Government

**Department of Infrastructure, Transport,
Regional Development, Communications, Sport and the Arts**

Project by



Findings on Age Verification

These are our headline findings. In line with the overall findings of the Trial, these findings relate specifically to the topic of age verification.

1

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

2

No substantial technological limitations preventing its implementation in the Australian context.

3

Providers' claims were independently assessed; are **accurate and reflective of real-world system performance**.

4

There is no single solution to age verification; a range of valid models exist, shaped by different contexts, needs and expectations.

5

The age verification sector in Australia is dynamic and innovative with active development and communication of verified age information.

6

We found **robust, privacy-focused and secure** data handling practices.

7

Age verification systems performed broadly **consistently across demographic groups**, including Indigenous populations.

8

Opportunities exist to enhance risk management and system capability, especially regarding real-time detection of lost or stolen documents.

9

Cybersecurity practices were strong across the sector with various threats addressed; continuous monitoring remains essential.

© Copyright of the Commonwealth of Australia

This document is available for reproduction on royalty-free, perpetual, attributed source, non-commercial rights to reproduce.

This permission allows for unlimited reproduction and distribution, provided that proper credit is given to the original author(s) and source. This grant applies to all formats and media worldwide. For queries about commercial use or the licence in general, please contact the publishers. All rights to materials on links are reserved to the author of those materials.

Accessibility Statement:

This report was produced in line with the accessibility guidelines found in the Australian Government Style Manual.

Legal Clearance Statement:

This report includes references to ISO standards through summarisation, referencing and reproduction of definitions only. While the material is not reproduced verbatim, ISO asserts copyright over its publications. For any further use or licensing queries, contact Standards Australia at: copyright@standards.org.au.

Published By:

Age Check Certification Scheme
Unit 321B Broadstone Mill, Broadstone Road
Stockport, United Kingdom, SK5 7DL

www.accscheme.com

ISBN 978-1-0681646-2-0



Table of contents

Introduction and Context

I

C.1	Introduction to Part C: Age Verification	6
C.2	Executive Summary	8
C.3	Who Participated in the Trial for Age Verification Technology	13

Context, Standards and Methodology

II

C.4	What is Age Verification	16
C.5	Approach For Age Verification Systems	17
C.6	Methodology and Technology Readiness Assessment	22

Detailed Analysis of Age Verification Providers

III

C.7	Age Verification Can Be Done	26
C.8	Accuracy of Age Verification in Mystery Shopper Testing	33
C.9	No Substantial Technological Limitations to Age Verification In Australia	35
C.10	Verified Practice Statements	39
C.11	Analysis of Approaches to Age Verification	45
C.12	Innovation and User-Centric Design in the Age Verification Sector	61
C.13	Privacy by Design and Data Minimisation in Age Verification	71

C.14	Demographic Consistency and Inclusion in Age Verification	81
C.15	Improving Data Access and Risk Management in Age Verification	88
C.16	Information Security In Age Verification Systems	94
C.17	Biometric Binding, Spoofing Mitigation and Document Integrity	98
C.18	Balancing Investigatory Preparedness with Privacy: Risks of Over-Retention of Data Used for Age Verification	106

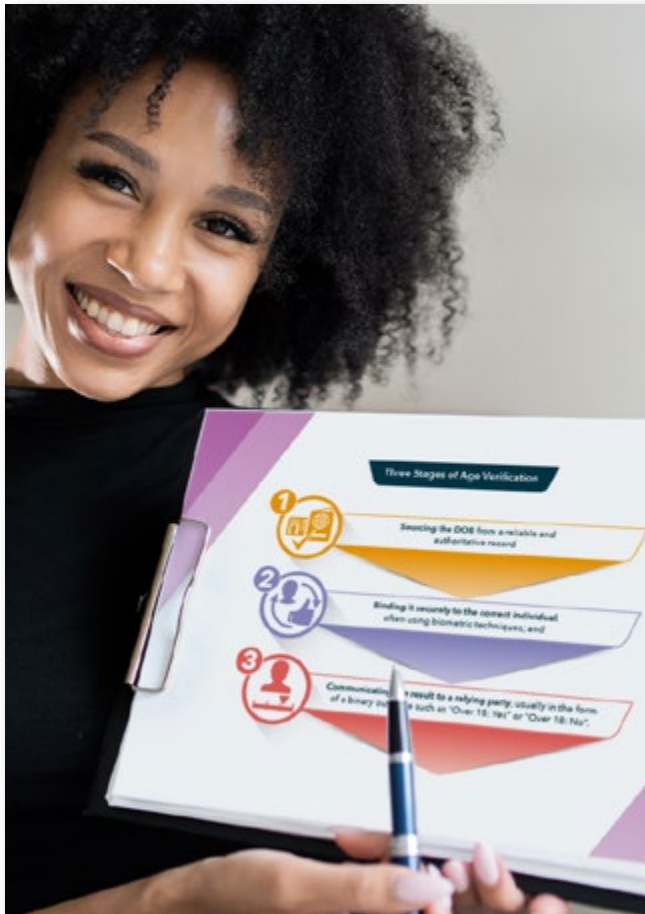


Age Assurance Technology Trial

I

PART C

Introduction and Overview



C.1 Introduction to Part C: Age Verification

C.1.1 Part C of the Age Assurance Technology Trial focuses specifically on age verification – the process of determining an individual’s age by referencing a verified date of birth and calculating their age from that known data point. Age verification represents the most direct and high-assurance form of age assurance and is already in widespread use across many regulated industries.

C.1.2 This section evaluates how age verification systems perform in the Australian context in terms of technical feasibility, reliability, inclusivity, privacy preservation and security and how they align with emerging international standards such as ISO/IEC FDIS 27566-1¹ and IEEE 2089.1². The technologies assessed include solutions using official identity documents, secure databases, customer account information and verified credentials, often supported by cryptographic or biometric binding techniques.

C.1.3 The Trial was established by the Australian Government through the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts (DITRDSCSA) to undertake an independent technological evaluation of a range of age assurance systems, in response to increasing public concern over children’s exposure to age-restricted online content, including pornography and harms on social media. The Trial explores whether technologies exist that can effectively verify age without unnecessarily compromising users’ privacy and how they perform under real-world conditions.

1. All references to ISO/IEC FDIS 27566-1 Standard throughout the suite of reports are referring to ISO/IEC FDIS 27566-1 – Information security, cybersecurity and privacy protection – Age assurance systems – Part 1: Framework.
2. All references to IEEE 2089.1 throughout the suite of reports are referring to IEEE 2089.1-2024 – IEEE Standard for Online Age Verification.

C.1.4 Through this part of the report, we present our findings on age verification technologies, including their accuracy, resilience to circumvention, handling of personal data and suitability for use across diverse populations. This analysis can support future efforts to inform best practices, certification and responsible deployment within Australia's evolving digital safety and privacy landscape.



C.2 Executive Summary

C.2.1 Age verification is a high-assurance method of age assurance that determines whether an individual is above or below a specific age threshold by comparing a verified date of birth (DOB) with a point in time – typically the current date.

C.2.2 Age verification can be done in Australia and is widely used in existing deployments. Australia has a robust foundation for verifying dates of birth, with authoritative government sources, consistent data management practices and secure access to identity records and documents. This framework supports reliable issuance and validation of birth date evidence across services, enhancing trust and integrity in age assurance and identity verification processes. Notwithstanding the robust foundation, there may be cultural and education barriers for age verification.

C.2.3 Our evaluation did not reveal any substantial technological limitations to the implementation of age verification technologies in Australia. Providers demonstrated compliance with recognised standards and deployed responsible, privacy-conscious approaches, incorporating strong data protection and security. The alignment of these technologies with emerging policy frameworks supports the deployment of effective and trustworthy systems for verifying age based on date of birth.

C.2.4 Privacy by-design and data minimisation were consistently observed across the participating providers. In most cases, systems were designed to avoid long-term storage of full identity or biometric information. Instead, they returned binary age outcomes or anonymised session tokens that could be reused across services. Several providers supported integration with privacy-focused digital wallets, allowing verified age credentials to be stored locally and reused with explicit consent. These approaches reflect close alignment with the draft ISO/IEC FDIS 27566-1 standard and demonstrate strong readiness for future conformity assessment and certification.

C.2.5 Demographic consistency was a key area of focus. The Trial found that systems generally performed well across diverse user groups, including First Nations and Torres Strait Islander Peoples. Some providers also made proactive efforts to include users who lack conventional identity documents, by supporting community-issued records or in-person onboarding processes. Nevertheless, gaps persist in remote and very remote communities where digital exclusion and lack of foundational credentials continue to limit access. While technically feasible, exact age verification for children is constrained by limited access to hard data; government-backed blind-access APIs to records (e.g., schools, healthcare) may be needed to improve precision.

C.2.6 Sector-specific tailoring was a notable strength across the Trial. Different sectors – such as gambling, adult content, education, retail and access to physical venues – require different levels of assurance, privacy and friction. Providers demonstrated flexibility and configurability in their systems, allowing them to be adapted to both high-risk and privacy-sensitive contexts. In high-assurance sectors such as gambling, providers incorporated document checks, facial biometrics and record-matching. In privacy-sensitive sectors like adult entertainment, the focus was on anonymous, one-time checks that avoided any persistent identity linkage.

C.2.7 Security and fraud resilience were also strong. Most providers operated ISO/IEC 27001-compliant systems, with encryption, multi-factor authentication and tamper detection. Biometric liveness checks were commonly implemented and aligned with ISO/IEC 30107 (presentation attack detection) standards, helping to guard against spoofing and deepfake risks. Systems were also generally effective at identifying document forgeries, including AI-generated fakes. However, several providers lacked the ability to check documents against live government databases to determine whether a document had been reported lost or stolen. The evaluation found that security against injection attacks – where malicious code or media bypasses the biometric capture process – is improving but still emerging.

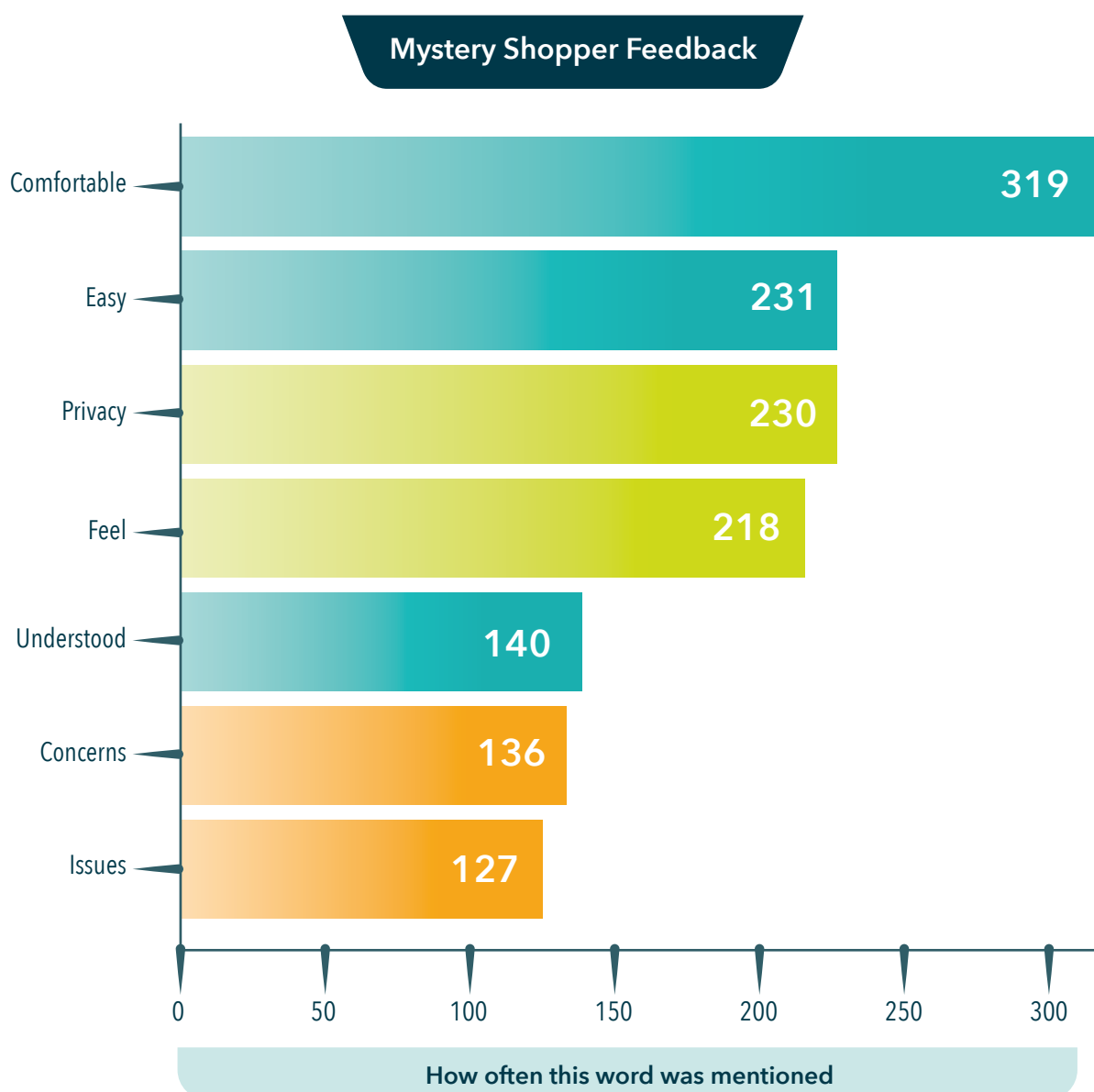


Figure C.2.1 Mystery Shopper Feedback

Key Statistics from the Trial

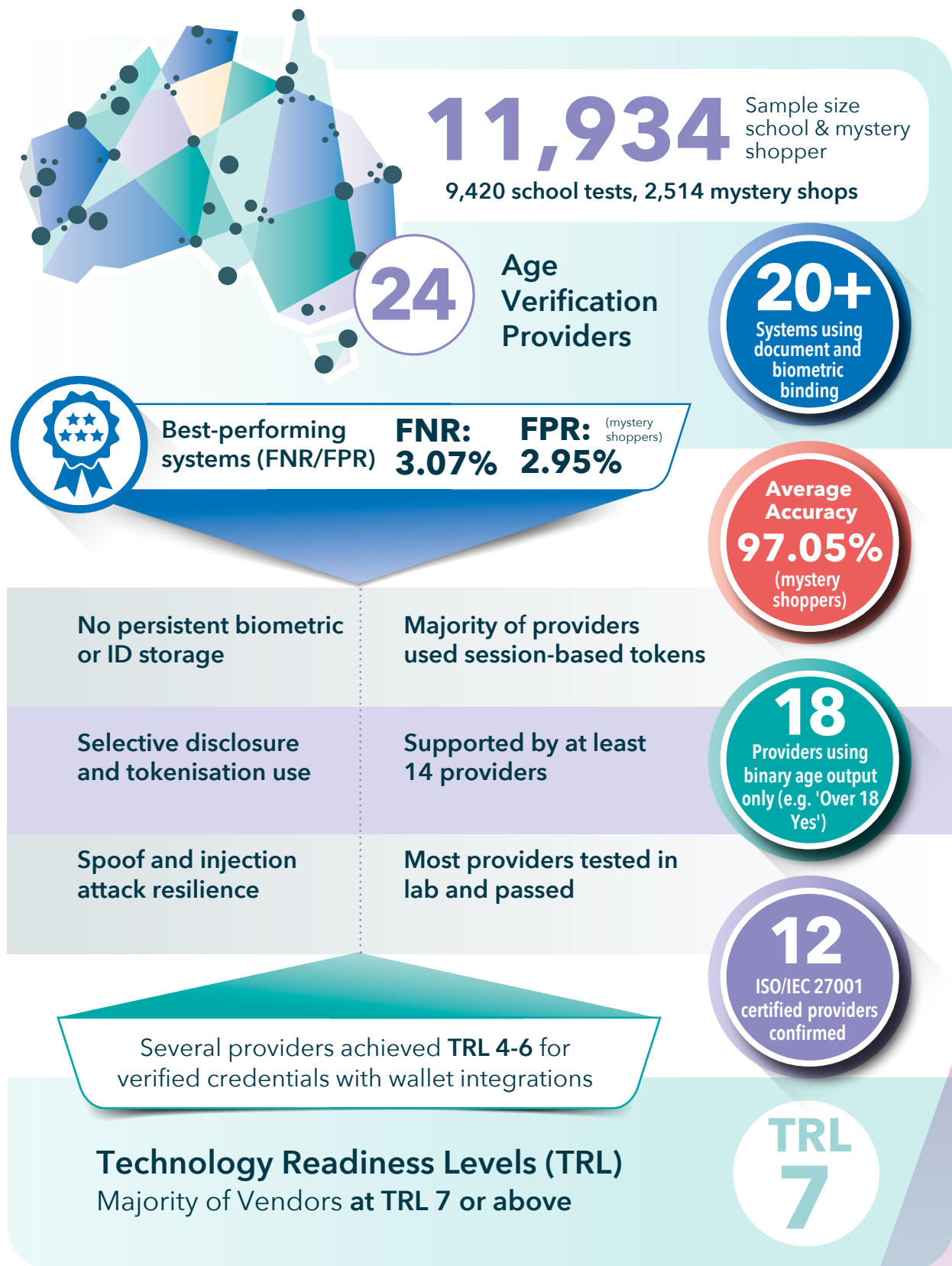


Figure C.2.2 Key Statistics from the Trial on Age Verification

C.2.8 While most providers followed clear data minimisation practices, the Trial identified a concerning trend among a minority of providers toward over-preparing for investigatory or forensic requests. This included the retention of full biometric or document data for all users, even when such retention was not required or requested. While these practices may be motivated by a desire to assist regulators or coroners in rare and serious circumstances, they carry significant privacy risks and require clearer regulatory guidance to ensure proportionality.

C.2.9 The age verification sector in Australia is highly dynamic and marked by innovation. Providers are actively developing new ways to verify age while reducing user friction and improving inclusivity. These include privacy-preserving cryptographic methods, reusable verified credentials, integration with mobile digital wallets and emerging support for blind-verification APIs that enable checks against government-held data without exposing user identity. Although some of these models remain at lower technology readiness levels, they signal a shift toward greater interoperability, reusability and user control.

C.2.10 In summary, age verification is a technically mature, privacy-conscious and inclusive method of age assurance. When implemented with strong safeguards, ethical oversight and adherence to international standards, it offers a viable and trustworthy solution for protecting children and enforcing age-based access controls in Australia's digital environment. Continued investment in inclusion, standardisation and user-centric innovation will help ensure that age verification systems remain fair, effective and widely accepted.

C.3 Who Participated in the Trial for Age Verification Technology





Age Assurance Technology Trial



PART C

Context, Standards and Methodology



C.4 What is Age Verification

C.4.1 Age verification is an age assurance method based on calculating the difference between a verified year or date of birth of an individual and a subsequent date.

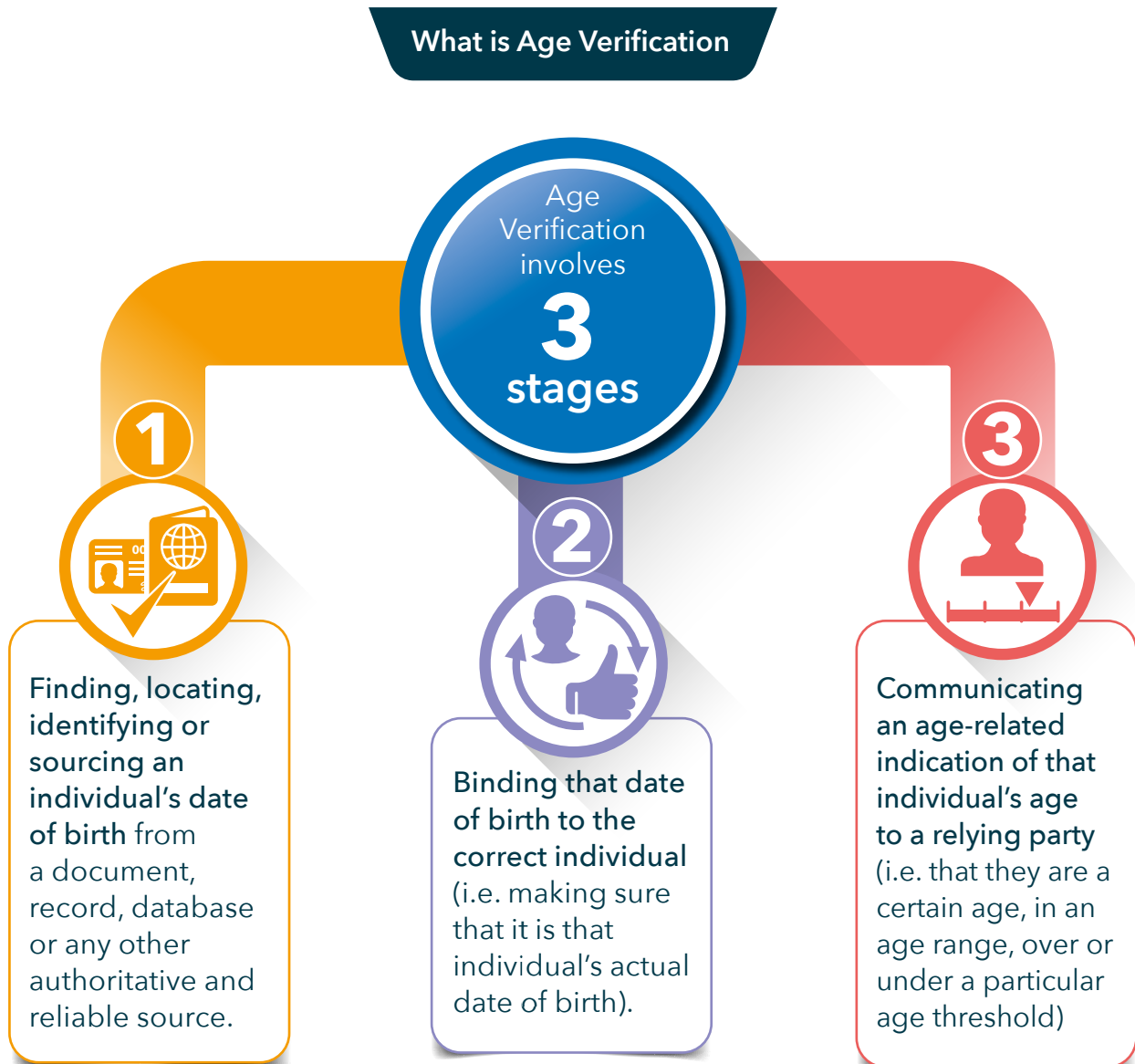


Figure C.4.1 What is Age Verification

C.5 Approach For Age Verification Systems






C.5.1 Age verification was assessed as a distinct category of age assurance with the goal of evaluating its readiness for use in online safety contexts requiring proof of being over thresholds such as 13, 16 or 18 years old.



Cross Reference: Part B - Methodology and Ethics

| International standards for age verification methods

C.5.2 The age verification evaluation was guided by internationally recognised standards including:

International Standards	
 ISO/IEC FDIS 27566-1	Framework for age assurance systems
 IEEE 2089.1	Standard for age verification
 ISO/IEC 25010 and 25040	Software quality models and evaluation processes
 ISO/IEC 29119	Software testing
 ISO/IEC 30107	Biometric presentation attack detection



ISO/IEC FDIS 27566-1

- Age Assurance Systems - Part 1: Framework

C.5.3 This draft international standard defines age verification as a sub-type of age assurance involving a verified date of birth (DOB). Key requirements include:

- Use of genuine, current and authoritative documents or records.
- Robust binding of the DOB to the specific individual.
- Support for selective disclosure (e.g. age threshold confirmation without revealing full DOB).
- Encouragement of privacy-by-design and use of cryptographic proofs.
- Inclusivity, particularly where formal ID documents may be unavailable.

C5.4 ISO/IEC FDIS 27566-1 positions age verification as a high-certainty, low-ambiguity method – but also one that is vulnerable to record falsification and identity theft, requiring strong countermeasures.



C.5.5 The standard outlines several key expectations for age verification systems:

ISO/IEC FDIS 27566-1	Criteria
Verification of source (Clause 4.3.2)	The identity document or data source must be genuine, current (not expired) and not revoked or falsified.
Binding to individual (Clause 5.3.2)	The system must ensure the date of birth belongs to the specific individual making the claim, often through biometric or cryptographic binding.
Privacy protection (Clause 7.3.2)	Systems should minimise data disclosure – communicating only what’s necessary (e.g., “Over 18”) without revealing full dates of birth.
Security (Clause 8.1)	Robust measures are required to prevent spoofing, forgery or misuse, including checks against stolen or falsified documents.
Inclusivity (Clause 9.2)	The framework encourages support for individuals who may lack conventional credentials by using alternative, trustworthy sources of verification.

C.5.6 The standard supports the use of selective disclosure and cryptographic proofs (such as those from digital wallets) to preserve privacy while still enabling age-related decisions to be made confidently. This aligns with global trends toward privacy-preserving and user-centric identity systems.

C.5.7 In essence, ISO/IEC FDIS 27566-1 positions age verification as the most direct and high-assurance method for determining an individual’s actual age but requires robust binding of that result to an individual and is, without effective countermeasures, prone to document or record falsification attack.

IEEE IEEE 2089.1 - Online Age Verification

C.5.8 IEEE 2089.1 provides an interoperability framework for online age checking systems, including definitions and processes for verifying DOBs. It emphasises:

- Minimising data collection
- Transparent disclosure to users
- Alignment with digital identity ecosystems

C.5.9 Both standards provide the backbone for future certification of age verification systems in Australia.





ISO/IEC 25010

C.5.10 Age verification systems were tested against criteria aligned to ISO/IEC 25010 and sector-specific needs:

ISO/IEC 25010	Criteria
Accuracy	How reliably the system determines whether a person is over a given age, using verified dates of birth.
Interoperability	Ability to integrate across services and platforms.
Reliability	Consistency of results across sessions and conditions.
Ease of use	Simplicity of the user journey, especially in verifying documents.
Bias minimisation	Fairness across demographic groups, including First Nations populations.
Privacy protection	Data minimisation and use of binary responses (e.g., "Over 18: Yes/No").
Data security	Protection against document fraud, spoofing and injection attacks.
Resistance to circumvention	Handling of forged documents and biometric spoofing.

C.6 Methodology and Technology Readiness Assessment

C.6.1 Methodology:

- Vendor interviews and declarations captured details of how dates of birth were sourced, verified and communicated.
- Structured testing involved deploying systems in controlled environments simulating typical user journeys.
- Technology Readiness Levels (TRLs) were assigned to benchmark maturity.
- Real-world use case alignment was prioritised over lab-only testing, to evaluate systems under plausible operational conditions.

C.6.2 Limitations and out-of-scope items.

While robust, the evaluation:

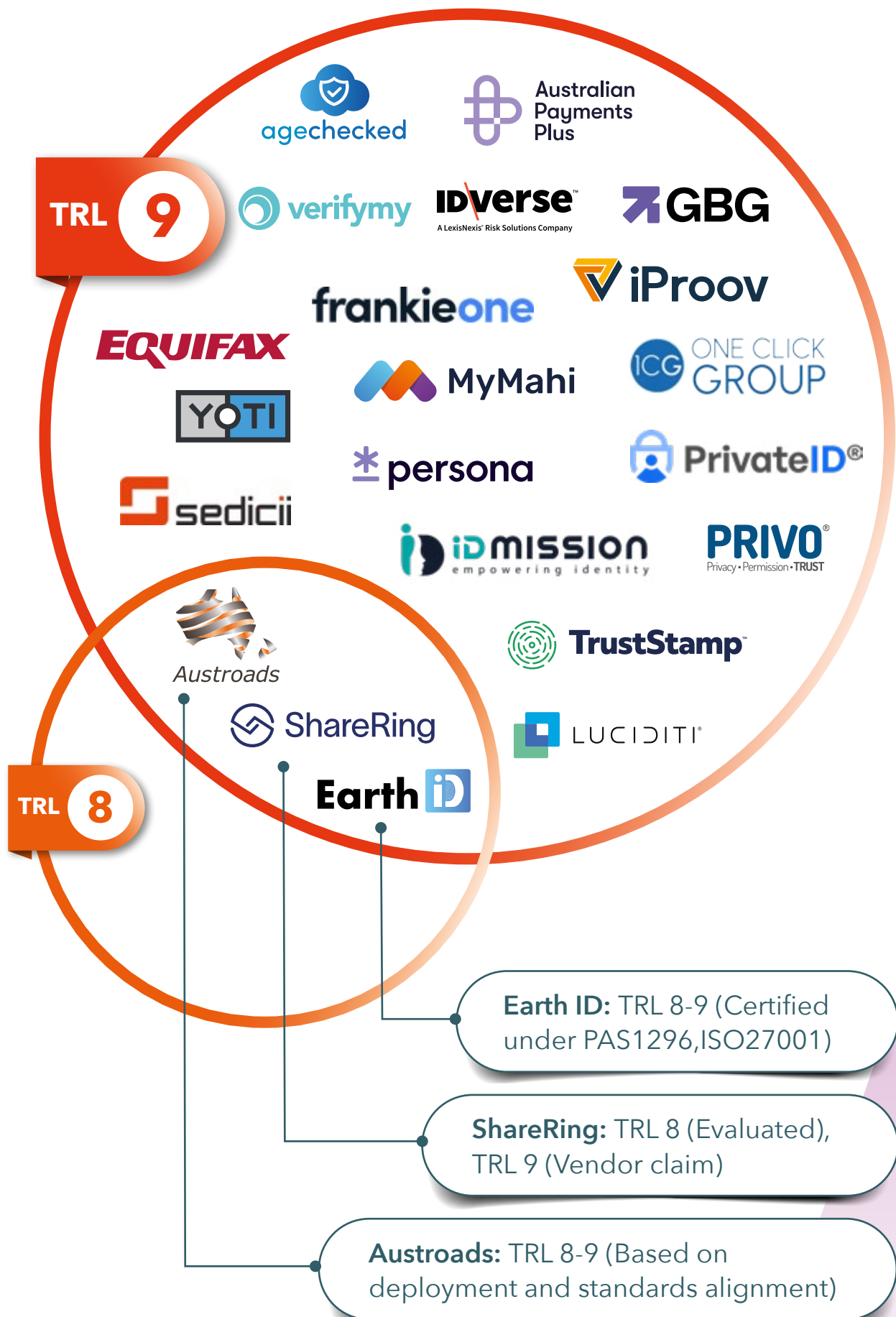
- Did not include volume stress testing, although degradation in performance for any reason during testing was noted. In some cases, the systems stopped working during individual tests.
- Did not conduct technical penetration testing or cryptographic audits (distinct from circumvention testing).
- Exact age determination (e.g., whether someone is 14 or 15) was out of scope; focus was on threshold-based verification (13+, 16+, 18+).

C.6.3 All of the providers of age verification technology were verified for their technology readiness. For an explanation of Technology Readiness Levels (TRLs), please refer back to the Part B - Methodology and Ethics Report, where this is explained in more detail.



Cross Reference: Part B - Methodology and Ethics

Technology readiness assessment for age verification systems





Age Assurance Technology Trial

III

PART C

Detailed Analysis of Age Verification Providers



C.7 Age Verification Can Be Done

| Summary finding

C.7.1 Age verification – based on calculating age from a verified date of birth – is technically and operationally feasible in Australia and can be implemented privately and effectively in line with emerging international standards.

| Detailed analysis

C.7.2 Age verification can be done in Australia and is widely used in existing deployments. Australia has a robust foundation for verifying dates of birth, with authoritative government sources, consistent data management practices and secure access to identity records and documents. This framework supports reliable issuance and validation of birth date evidence across services, enhancing trust and integrity in age assurance and identity verification processes. Notwithstanding the robust foundation, there may be cultural and education barriers for age verification.

| What age verification is and is not

C.7.3 Age verification is a method of age assurance that determines whether a person is above or below a given age threshold by comparing their verified date of birth (DOB) to the current date. It is the most direct method of age assurance, requiring authoritative evidence – such as a passport, driver's licence or official record – of an individual's DOB, which is then bound to the individual and used to generate an age-related signal (e.g. "Over 18: Yes/No") communicated to a relying party.

C.7.4 This method is commonly used in sectors where regulatory requirements mandate reliable age checks such as online gambling, digital identity onboarding or access to age-restricted content. It is distinct from estimative or behavioural approaches due to its binary, record-based logic.

C.7.5 It is important to distinguish age verification from other forms of age assurance. Age verification is specifically based on establishing and validating an individual's date or year of birth using authoritative evidence, such as a government-issued identity document, a verified record or a trusted account. It is not age estimation³, which infers age from biometric or behavioural characteristics, nor is it age inference⁴, which draws probabilistic conclusions about facts about individuals other than date of birth.

C.7.6 Age verification also operates independently of parental involvement – unlike parental consent⁵, which requires a guardian to affirm a child's access or parental control⁶, which pre-configures device or service restrictions based on child profiles. Age verification is also not self-declaration, where users input their age without validation, nor is it a content filter or moderation tool. It does not rely on subjective thresholds or platform internal logic but instead delivers a binary or confidence-based output grounded in verifiable evidence. This method offers the highest level of assurance among age assurance techniques, though it may introduce greater friction and raise specific privacy considerations.

3. See Part D – Age Estimation

4. See Part E – Age Inference

5. See Part G – Parental Consent

6. See Part H – Parental Control



Vendor Case Study

Website

digicheck.com

DigiChek is an age verification provider that uses document-based and data-driven techniques to assess user age, ensuring compliance and safety across digital platforms while aligning with international verification standards.

Three Key Facts

1

Verification is conducted by a DigiChek Registrar using primary credentials compliant with a 100-point ID check.

2

Verification is facilitated by schools during enrolment submitting the child's name, date of birth and place of birth.

3

The DigiChek system correctly completed 11 verification tests across a range of 13+ 16+ and 18+ users.

Strengths

Confidence is upheld through:

- In-person identity verification
- Use of immutable identity data
- A secure, user-generated DigiChek Key
- Cryptographically protected data handling
- Is permanently bound to the user's DigiChek profile

Practice Statement

ageassurance.com.au/v/dig/#PS

Privacy Policy

ageassurance.com.au/v/dig/#PP

Technology Trial Test Report

ageassurance.com.au/v/dig/#TR

Technology Trial Interview

ageassurance.com.au/v/dig/#VI

Summary of Results

DigiChek is effective in age verification for 13+, 16+ and 18+ users. The system demonstrated strong privacy protections, secure data handling and broad browser compatibility, with no personal data stored or transmitted during use.

| Why age verification is important

C.7.7 Date of Birth based age verification is a high-assurance method with minimal ambiguity. It offers regulators, service providers and users a clear, audit-ready basis for determining age, especially for legal thresholds (e.g. over 18 for adult content, alcohol purchase or gambling).

When implemented with privacy-preserving and proportional data practices, it strikes a balance between:

- Legal compliance
- User privacy
- Operational efficiency

Its use also enables trust in cross-sector digital ecosystems, such as when age-verified credentials are shared via digital wallets or interoperable identity systems.

| How have the evaluation team found that age verification can be done

C.7.8 Age verification systems using verified dates of birth are well established and technically mature in Australia. Providers demonstrated alignment with international standards, strong privacy-by-design and high usability. The systems are adaptable to diverse use cases and demographic contexts, with no substantial technological limitations to deployment identified across the Trial.



Vendor Case Study



Website

verifymy.io

Verifymy provides flexible AV solutions integrated with digital wallets, document verification and cross-jurisdictional datasets. It supports selective disclosure and privacy-first age checks, delivering binary outcomes (e.g., "Over 18: Yes") via APIs and reusable credentials for platforms such as gambling, e-commerce and education.

Three Key Facts

1

Lab testing confirmed strong functionality, with all test scenarios (e.g., expired, tampered and invalid documents).

2

Offers strong fallback options, such as biometric selfies or document upload, if initial checks fail.

3

Adaptive system can serve both high-assurance and low-friction use cases with configurable workflows.

Strengths

Mystery shopper testing showed high accuracy for ages below the Age 16 and 18 gates. Notably, false negative rates were high for 18-19-year-olds at the Age 18 gate (up to 50%), indicating some eligible users would be blocked and require fallback verification. For older adults (25+), FNR was 17%.

Practice Statement

ageassurance.com.au/v/vmy/#PS

Privacy Policy

ageassurance.com.au/v/vmy/#PP

Technology Trial Test Report

ageassurance.com.au/v/vmy/#TR

Technology Trial Interview

ageassurance.com.au/v/vmy/#VI

Summary of Results

Verifymy performed consistently well in interoperability, privacy and usability testing. Its digital wallet integration supported cross-platform verification. However, clarity around configuration for relying parties was needed to avoid misconfigured deployments. It is TRL 9, ISO-aligned and effective in both regulated and low-friction AV use cases.

C.7.9 Some providers demonstrated multi-tiered verification flows that escalated based on confidence level. Users near an age threshold were typically referred from estimation to document-based verification, enabling accurate and privacy-conscious decisions. Notably, multiple systems showed strong performance across First Nations and remote users through adaptive onboarding, local verification partners or fallback credential pathways. Real-world testing also confirmed robust spoofing and tamper resistance via biometric liveness, document security checks and cryptographic protections.

C.7.10 Each Vendor took part in an interview which evaluated their technology on key characteristics including Functionality, Performance, Privacy, Security and Acceptability. The Trial Team highlighted positive aspects and identified relevant issues.



C.8 Accuracy of Age Verification in Mystery Shopper Testing

C.8.1 To evaluate the real-world accuracy of age verification systems under typical user conditions, the Trial included a structured mystery shopper exercise. This involved 328 participants attempting to access age-restricted content or services using a sample of the participating age verification technologies. These tests simulated real-world scenarios in which users presented their actual age credentials or attempted to bypass verification.

| Key findings

- **False Negative Rate (FNR): 3.07%**

This represents instances where the system incorrectly denied access to users who were, in fact, above the required age threshold. These cases typically reflect edge conditions such as lighting challenges, ambiguous document images or conservative system thresholds.

- **False Positive Rate (FPR): 2.95%**

This reflects instances where users who were below the required age were incorrectly allowed access. These represent a key area of risk in the context of age-restricted online services, but the observed rate remained low.

- **Overall Accuracy: 97.05%**

This figure represents the combined proportion of correct acceptances and correct rejections. It demonstrates a high level of reliability, especially considering the diverse testing environments, device types and age thresholds involved.

| Interpretation

C.8.2 These results indicate that the participating age verification systems were generally highly accurate, with error rates below 3% in both directions. This level of performance is comparable to or better than many real-world identity verification deployments – especially those involving biometric liveness checks or age estimation techniques. That there is an error rate serves to remind that no technology is going to deliver 100% accuracy, at least not without significantly more inconvenience to users.

C.8.3 Importantly, these systems maintained this level of performance while also upholding strong privacy and data minimisation practices, often returning only binary “Over 18: Yes/No” results with no storage of sensitive personal data.

C.8.4 The low error rates found in the mystery shopper testing reinforce the finding that age verification systems are technically mature, operationally effective and capable of supporting regulatory and platform-level controls for age-restricted content. These systems are ready for broader deployment in sectors requiring robust, privacy-conscious age assurance.

C.9 No Substantial Technological Limitations to Age Verification In Australia

C.9.1 Our evaluation did not reveal any substantial technological limitations to the implementation of age verification technologies in Australia. Providers demonstrated compliance with recognised standards and deployed responsible, privacy-conscious approaches, incorporating strong data protection and security. The alignment of these technologies with emerging policy frameworks supports the deployment of effective and trustworthy systems for verifying age based on date of birth.

| What is meant by no technological limitations

C.9.2 The evaluation team found that age verification systems are technically feasible and deployable within the Australian context, without requiring new or unproven technologies. Service providers showed that these systems can be integrated into digital platforms, operated securely and privately and used by a wide range of end-users.

C.9.3 This includes technologies such as biometric selfie-to-ID document matching, NFC passport chip reading, blockchain-stored verifiable credentials and secure attribute exchange APIs. These methods were demonstrated to work reliably under test conditions, including with school-aged users and mystery shoppers.

C.9.4 While this report concludes that there are no substantial technological limitations to the implementation of age verification in Australia, this should be interpreted narrowly. It does not imply that age verification is universally appropriate in all use cases, cost-neutral or without operational considerations. Some edge-case challenges – such as verifying users without formal ID or supporting access in remote locations – may require further policy, infrastructure or community-based solutions rather than technological innovation.

C.9.5 Applying age verification for younger users becomes harder as they are progressively less likely to have an accessible data source for their verifiable age – if exact age verification is required for a policy affecting minors, then public authorities which tend to be the main source of comprehensive age data will need to facilitate greater, but obviously controlled, access.

Vendor Case Study



Website

risk.lexisnexis.com/products/idverse

IDVerse uses advanced AI for real-time age verification via biometric face matching, liveness detection and OCR. Offers strong spoof protection and compliance with global standards for diverse user groups.

Practice Statement

ageassurance.com.au/v/idv/#PS

Technology Trial Test Report

ageassurance.com.au/v/idv/#TR

Privacy Policy

ageassurance.com.au/v/idv/#PP

Technology Trial Interview

ageassurance.com.au/v/idv/#VI

Summary of Results

Top performer with strong biometric performance and security. Lab testing confirmed full functionality across devices, including robustness to expired or tampered IDs, invalid documents and identity mismatches. Met inclusivity and tamper resistance standards.

| Why is the absence of technological limitations important

C.9.6 In the context of regulatory reforms aimed at improving online safety – particularly for children and young people – governments and industry stakeholders require confidence that technological solutions can meet policy objectives without introducing disproportionate costs, security vulnerabilities or privacy harms.

C.9.7 This finding provides reassurance to decision-makers that:

- There are no fundamental research or development gaps that would prevent the national deployment of date-of-birth-based age verification technologies.
- Systems capable of enforcing compliance with policy-defined age thresholds (e.g. 13+, 16+, 18+) are already available and demonstrably effective.
- Responsible implementation, aligned with privacy-by-design principles and international standards, can uphold user privacy and data security.

| How does age verification technology align with policy objectives

C.9.8 The successful deployment of age verification systems within the Trial demonstrates a mature alignment between technology capabilities and regulatory objectives. This alignment is supported by:

- The availability of authoritative and verifiable date-of-birth data from identity documents (e.g. passports, driver's licences) and secure government records.
- A stable regulatory foundation for data protection and cybersecurity, including the Privacy Act 1988 and the development of national digital identity frameworks.
- Industry readiness to integrate with platforms such as the Australian Government Digital ID System (AGDIS) and Consumer Data Right (CDR), both of which enable privacy-preserving and standards-based identity verification.

| What does the evidence from the Trial show

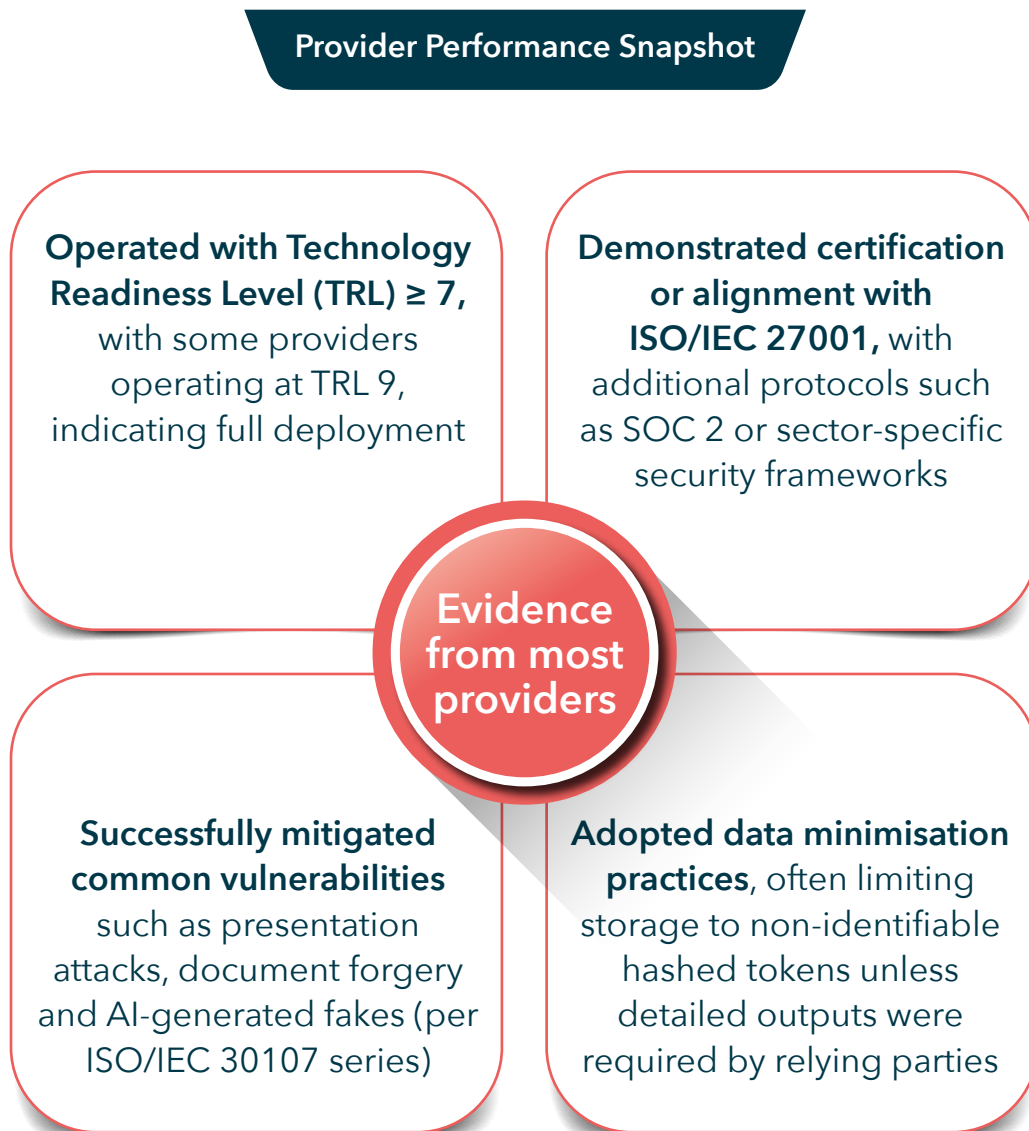


Figure C.9.1 Provider Performance Snapshot

C.10 Verified Practice Statements







C.10.1 A key part of the evaluation process involved reviewing practice statements submitted by age verification providers whose technologies had reached a Technology Readiness Level (TRL) of 7 or above indicating a high degree of operational readiness. This sample-based approach allowed the evaluation team to assess whether providers stated processes aligned with the capabilities demonstrated in structured testing.

C.10.2 The analysed statements described:

- how date of birth (DOB) information was secured, bound to individuals and verified.
- how data retention was minimised and disclosed; and
- how verification results (e.g. binary age assertions) were communicated to relying parties.

C.10.3 We identified opportunities to improve the clarity and consistency of configuration guidance – particularly for relying parties who integrate these solutions. Some documentation lacked implementation details or did not fully articulate the risks and controls applicable to third-party deployments.

C.10.4 The following table provides a comparison of practice statements and privacy policies for a sample of providers. The analysis found a high degree of consistency between what providers claimed and what their privacy policies enforced, concluding that the statements fairly reflected the technical and operational behaviour of the systems and were consistent with observed results across test environments.

Provider	Practice Statement Summary	Privacy Policy Summary	Consistent?
Verifymy	Selective disclosure via wallets, binary over-18 signals, minimal data retention.	Aligns with selective disclosure, no full DOB shared, strong on data minimisation.	
AgeChecked	Anonymised tokens, no PII storage unless needed, returns binary result.	Confirms anonymised accounts, non-retention of PII, binary results.	
Luciditi	Face estimation and document match, only returns threshold confirmations.	No full PII stored, encrypted app-only access, supports user deletion.	
ConnectID	Binary output, no PII passed to relying parties, user-controlled consent.	No PII seen by ConnectID, consent and transparency in dashboard.	
DigiChek	Uses user-generated key, holds only DOB/place of birth/name, strict control.	Holds only three identity fields, anonymised key-based logic, no full ID reused.	
EarthID	ZKPs and reusable credentials in personal wallet, no central storage.	Supports ZKPs, decentralised ID model, no central data retention.	

Vendor Case Study



Website

sharering.network

ShareRing uses blockchain to manage privacy-first identity and AV via OCR, biometrics and ePassports. Operates through the ShareRing Me app with decentralised, verifiable credential storage.

Practice Statement

ageassurance.com.au/v/shr/#PS

Technology Trial Test Report

ageassurance.com.au/v/shr/#TR

Privacy Policy

ageassurance.com.au/v/shr/#PP

Technology Trial Interview

ageassurance.com.au/v/shr/#VI**Summary of Results**

Excellent privacy and decentralised control. Blockchain UX may challenge less technical users. Requires onboarding support for vulnerable populations. Strong security and identity binding across NFC and document sources.

| How have age verification practice statements been assessed

C.10.5 Across the reviewed practice statements, three consistent and well-demonstrated technical features were observed:

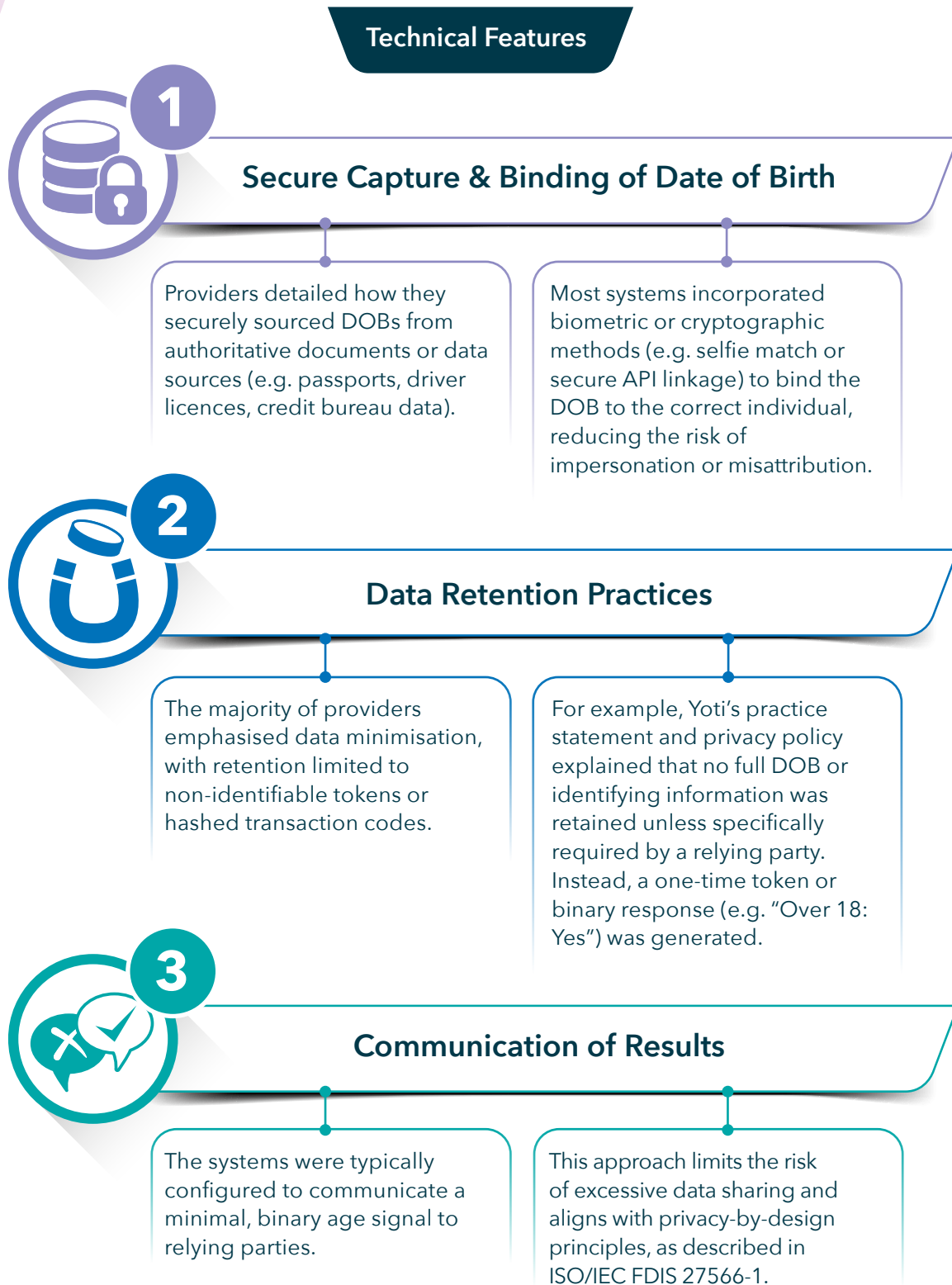


Figure C.10.1 Consistent and Recurring Features of Practice Statements

| What opportunities are there for improvement of age verification practice statements

C.10.6 While the submitted statements were largely strong, the evaluation identified one recurrent area for improvement.

C.10.7 The management of system configuration and the clarity of implementation guidance provided to relying parties.



Summary of configuration management requirements (ISO/IEC FDIS 27566-1)

- Age assurance providers must share standard configuration settings with relying parties upon request.
- Specific settings may be tailored by mutual agreement.
- Configuration settings should clarify:
 - Whether user-controlled settings are available.
 - How these settings affect system functionality, performance, privacy, security and user acceptability.
 - Who holds the authority to change configurations.
 - How changes are planned, controlled and audited – following practices such as those in ISO 10007.

C.10.8 This issue encompasses:

- How age verification systems are deployed or embedded into third-party platforms.
- The role of default vs. configurable options in determining privacy, data flows and user experience.
- The risks introduced when relying parties misconfigure privacy settings, age thresholds or audit logging.

C.10.9 Improved documentation and clearer integration playbooks would support more consistent and privacy-preserving deployments, particularly for small-to-medium enterprises that may not have in-house technical expertise.

Vendor Case Study


Website

frankieone.com

Aggregates age assurance services, enabling inference through third-party integrations; supports orchestration logic for fallback, confidence thresholds and multi-vendor identity decisioning.

Practice Statement

ageassurance.com.au/v/fra/#PS

Technology Trial Test Report

ageassurance.com.au/v/fra/#TR

Privacy Policy

ageassurance.com.au/v/fra/#PP

Technology Trial Interview

ageassurance.com.au/v/fra/#VI

Summary of Results

Strong fraud prevention and high assurance. Aggregator platform integrating third-party inference and IDV solutions. Supports inference via partners and orchestration logic but does not offer native age inference capability. Strong on configuration and delivery; TRL reflects reliance on external providers.

C.11 Analysis of Approaches to Age Verification

C.11.1 There are a wide range of age verification technologies that source date of birth data from documents (such as passport or driving licence scans), from records (such as credit reference or utility databases), from customer account data (such as from banks or financial institutions) or from authoritative sources (such as government or school data). We found that each age verification service provider had built and optimised their system for the specific needs of their clients and tailored their approach in line with the regulatory environment and the risk profile of the sectors that they specialised in. These needs varied across sectors with more privacy intrusive data needed for sectors like gambling (to guard against money laundering as an example) than other sectors like adult entertainment (where user privacy is paramount).

C.11.2 These approaches can broadly be grouped into:

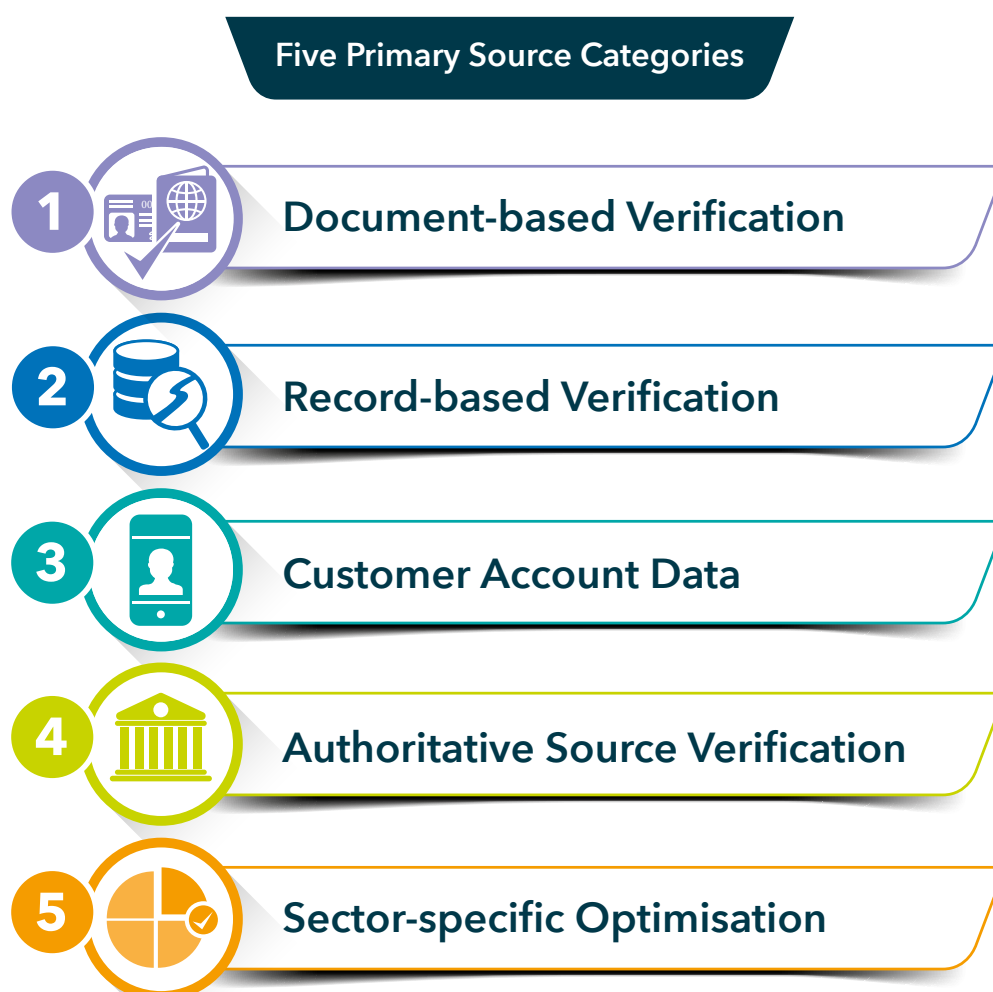


Figure C11.1 Five Primary Source Categories

1



Document-based Verification

C.11.3 Many systems extract date of birth data from scanned or photographed identity documents such as:

- Passports
- Driver licences
- National or student identity cards

C.11.4 These systems typically employ:

- Optical Character Recognition (OCR) to extract data
- Liveness detection and biometric 'selfie match' to bind the document to the presenting user
- Forgery and AI-generated fake detection measures (per ISO/IEC 30107)⁷



C.11.5 Document-based methods are widespread, particularly in direct-to-consumer and regulated markets like online gambling, but are dependent on document availability and quality.

7. ISO/IEC 30107-1: 2023 Information technology – Biometric presentation attack detection is a Framework standard that establishes terms and definitions that are useful in the specification, characterisation and evaluation of presentation attack detection methods.

Vendor Case Study



Website

luciditi.co.uk

Luciditi provides facial age estimation, document verification via selfie-ID match, NFC passport reading and open banking or telco records, with fallback to a reusable digital ID app.

Three Key Facts

1

Privacy-preserving design; user-held encryption; fast integration; supports verification, estimation, inference.

2

Verified users across 13+, 16+ and 18+ thresholds with high accuracy. Consistently verified Indigenous and non-Indigenous users accurately.

3

High document capture success rate across varied devices. Designed for low-friction UX with fallback.

Strengths

Passed all controlled test scenarios, including:

- Poor lighting and low-quality selfies
- Face partially obscured by glasses, hats or scarves
- Expired or altered documents
- Liveness challenge using spoof images or pre-recorded selfies

Practice Statement

ageassurance.com.au/v/luc/#PS

Privacy Policy

ageassurance.com.au/v/luc/#PP

Technology Trial Test Report

ageassurance.com.au/v/luc/#TR

Technology Trial Interview

ageassurance.com.au/v/luc/#VI

Summary of Results

Luciditi demonstrated a mature, privacy-conscious and standards-aligned approach to document-based age verification. It met or exceeded test expectations across OCR accuracy, biometric binding, spoofing resilience and user inclusion. Its system offers a robust model for regulated and high-assurance age verification use cases.

2



Record-based Verification

C.11.6 Some providers draw on a user's DOB retrieved from existing records, such as:

- Credit reference agency databases
- Utility account records
- Schools or education records
- Telecommunications or mobile operator data

C.11.7 These approaches involve matching user-submitted information against known records and are often used for background verification in finance, telecommunications or public service platforms. While these methods can offer high assurance, they may raise privacy and data access concerns if not properly scoped.





Vendor Case Study

Website

agechecked.com

AgeChecked uses data matching, credit reference checks, electoral rolls, facial age estimation, document verification with liveness detection and adult-linked credit card checks in a cascading process.

Three Key Facts

1

Modular verification; privacy by design; anonymised tokens; multiple methods (data, document, facial).

2

Secure data handling, transparency in age determination and delivers binary signals like "Over 18: Yes/No" to relying parties.

3

Demonstrated high true positive rates across 16+ and 18+ thresholds using record-matching.

Strengths

Low-friction UX: Instant match from known records; minimal user input required for key retail, gambling and online marketplaces
No Biometric or ID Upload Needed: Suitable for users without access to conventional ID.

Practice Statement

ageassurance.com.au/v/age/#PS

Privacy Policy

ageassurance.com.au/v/age/#PP

Technology Trial Test Report

ageassurance.com.au/v/age/#TR

Technology Trial Interview

ageassurance.com.au/v/age/#VI

Summary of Results

AgeChecked exemplified how record-based age verification can offer high assurance while respecting privacy. It successfully matched user data against trusted databases, avoiding excessive data collection. Its design supports regulatory compliance, rapid deployment and strong fallback mechanisms, making it well-suited for both regulated markets and low-barrier online environments.

3



Customer Account Data

C.11.8 In some sectors – particularly banking, fintech and e-commerce – age verification can leverage customer account metadata, where the date of birth was captured during prior Know Your Customer (KYC) processes. This model is:

- Fast and frictionless
- Typically low in additional user interaction
- Highly dependent on the original quality, maintenance and accuracy of the captured data

C.11.9 Such reuse could be accompanied by robust identity binding and audit trails to ensure legitimacy and prevent fraud.



Vendor Case Study



Website

auspayplus.com.au

ConnectID relies on banks' KYC-verified date of birth to return yes/no age assertions; the peer to peer exchange model ensures that no Personal Identity information is ever visible to ConnectID; in addition, the model ensures only consented minimal data (e.g. over 18) is shared.

Three Key Facts

1

KYC-verified DOB and identity data from major banks: Commonwealth Bank, National Australia Bank, Westpack and ANZ Plus.

2

User is redirected to their bank's app or portal to authenticate and consent to share an age assertion.

3

ConnectID facilitates the secure P2P transfer verified via pairwise identifiers without ever seeing or storing user data.

Strengths

Successfully deployed with relying parties for real-world use cases:

- Same-day alcohol delivery verification (NSW Liquor Act)
- Knife sale restriction enforcement (Queensland Jack's Law)
- Onboarding with Telco SIM card activation

Practice Statement

ageassurance.com.au/v/app/#PS

Privacy Policy

ageassurance.com.au/v/app/#PP

Technology Trial Test Report

ageassurance.com.au/v/app/#TR

Technology Trial Interview

ageassurance.com.au/v/app/#VI

Summary of Results

ConnectID provides a model for fast, accurate and private age verification using existing customer account data. By leveraging KYC-verified DOBs from banks and enforcing user-controlled consent flows, ConnectID ensures high assurance with minimal friction. Its federated architecture, regulatory alignment and zero data retention approach make it ideal for sectors demanding both security and usability.

4



Authoritative Source Verification

C.11.10 Some of the most privacy-preserving and secure implementations rely on direct access to authoritative data, such as:

- Digital wallets of holders of verified credentials
- Government ID verification services
- Birth and education records (where accessible)
- Public registries and trusted data holders

C.11.11 These models typically use API-based “match/no match” queries that do not return the full DOB, but confirm if the submitted data aligns with a known record. This method minimises unnecessary data sharing and is well-aligned with the selective disclosure principles as set out in ISO/IEC FDIS 27566-1.





Austroads

Vendor Case Study

Website

austroads.gov.au

Austroads manages the National Exchange of Vehicle and Driver Information System (NEVDIS) and is pioneering Mobile Driver Licence (mDL) standards. It enables verified credentials and selective age attestations via government-issued IDs and secure registries. Austroad's ecosystem combines national-scale infrastructure with ISO-compliant design.

Three Key Facts

1

Mobile Driver Licences (mDLs) issued by states and territories (ISO/IEC 18013-5 compliant).

2

User consents to share a digitally signed age claim (e.g., "Over 18") through a mobile wallet.

3

Relying party queries a government API or wallet service for a "match/no match" check - no DOB is returned.

Strengths

- High trustworthiness due to government-backed credentialing
- International standards compliance ensures future-proofing
- Strong alignment with ISO/IEC FDIS 27566-1 for selective disclosure and user-centric identity

Practice Statement

ageassurance.com.au/v/aus/#PS

Privacy Policy

ageassurance.com.au/v/aus/#PP

Technology Trial Test Report

ageassurance.com.au/v/aus/#TR

Technology Trial Interview

ageassurance.com.au/v/aus/#VI

Summary of Results

An authoritative source verification model: secure, decentralised and privacy-preserving. By leveraging government-issued digital credential and realtime API validation, it eliminates the need to transmit sensitive identity data. Austroad's ecosystem offers a trusted foundation for age assurance with minimal friction or exposure.

5

Sector-specific Optimisation

C.11.12 Across the Trial, it became clear that no single age verification method fits all contexts. Providers have tailored their technologies to meet the distinct commercial, regulatory and user-experience demands of specific sectors. These sector-aware strategies reflect a mature and adaptive ecosystem that balances privacy, assurance, usability and compliance.

Online gambling

C.11.13 In the online gambling sector, high-assurance verification is a regulatory necessity, driven by anti-money laundering (AML) laws and responsible gambling obligations. Providers such as Verifymy, GBG and AgeChecked have developed robust systems that integrate:

- Document-based verification using passports and driver licences,
- Biometric selfie matching with liveness detection, and
- Authoritative record checks, including credit reference and electoral data.

C.11.14 For example, Verifymy demonstrated flexible integration with UK and Australian data sources and is already used in gambling onboarding. GBG's ID3global platform combines real-time forgery detection with robust risk analytics, while AgeChecked uses a multi-layered waterfall approach, starting with record checks and progressing to facial estimation or document upload as needed. These methods, while more privacy-intrusive, are accepted in exchange for greater assurance.

Vendor Case Study



Website

gbg.com/en

GBG offers a real-time, multi-layered age verification system combining document checks, facial biometrics, credit agency data and liveness detection. Their solution includes in-person verification options and supports facial age estimation for users aged 6+, without retaining personally identifiable information (PII), making it suitable across multiple regulated sectors.

Three Key Facts

1

Document + facial biometrics with spoof detection (iBeta certified). Configurable privacy options for minimal disclosure.

2

Deployed in high-assurance settings like gambling, finance and AML/KYC onboarding, with low false acceptance rates.

3

Mention retaining additional data or supporting detailed audit trails when required by regulation (e.g., AML or forensic tracing).

Strengths

Highly accurate and fast, even under low lighting and varied image conditions in real-world testing environments.

Flexible integration with client systems via APIs and SDKs, enabling easy deployment at scale.

Practice Statement

ageassurance.com.au/v/gbg/#PS

Privacy Policy

ageassurance.com.au/v/gbg/#PP

Technology Trial Test Report

ageassurance.com.au/v/gbg/#TR

Technology Trial Interview

ageassurance.com.au/v/gbg/#VI

Summary of Results

GBG performed well in live testing, demonstrating strong accuracy and fraud detection capabilities. It was especially effective in online gambling and retail sectors. However, guidance for relying parties was limited, creating a risk of privacy misconfiguration. The system is TRL 9, with ISO-aligned privacy and data minimisation features.

Adult entertainment

C.11.15 In contrast, the adult content sector prioritises user anonymity and frictionless access. Here, systems are optimised for privacy and simplicity:

- Yoti, for example, uses one-time age confirmation based on facial estimation or document check, with only a binary “Over 18: Yes” result returned.
- AgeChecked supports anonymous sessions using pseudonymised tokens and does not retain personally identifiable information.
- Luciditi enables minimal data disclosure using digital credentials embedded in privacy-centric mobile identity wallets.

C.11.16 In this domain, persistent identifiers are avoided and age checks are often designed to function without user profiling, ensuring low-friction user experience with strong privacy guarantees.



Access to physical venues

C.11.17 In the physical access sector – such as entry to bars, nightclubs, age-restricted events or licensed venues – age verification must be fast, frictionless and reliable under time-sensitive and often low-light conditions. Here, systems are optimised for offline operation, minimal personal data exposure and integration with physical infrastructure like gates or handheld scanners:

- RightCrowd, for example, provides device-based credentials that verify age without transmitting personal information. These are used for gate access and can operate without biometric input, prioritising speed and security in physical settings.
- ShareRing supports QR code or NFC-based credentials derived from document scans and selfie matches, storing only hashed identifiers on the blockchain. This enables verified “Over 18” assertions that are unlinkable and usable without network access.
- Luciditi offers privacy-centric mobile credentials that can be shown visually or presented digitally, including through digital wallets or event apps, ensuring compatibility with human and machine verification workflows.

C.11.18 In this domain, persistent identifiers are minimised and the emphasis is on local verification, offline fallback and interoperability with event or venue systems. The result is a high-trust, low-friction experience that respects user privacy while ensuring legal compliance at the door.

Vendor Case Study



Website

rightcrowd.com

Primarily an enterprise physical access platform, RightCrowd uses device-bound credentials for gate control. Minimal age verification capability; focused on on-site access security rather than online AV.

Practice Statement

ageassurance.com.au/v/rig/#PS

Technology Trial Test Report

ageassurance.com.au/v/rig/#TR

Privacy Policy

ageassurance.com.au/v/rig/#PP

Technology Trial Interview

ageassurance.com.au/v/rig/#VI

Summary of Results

Effective for physical access and security workflows. Not designed for online or consumer-based AV. Limited application to age assurance sectors. Best suited to enterprise environments with existing ID infrastructure.



Digital Identity and eGovernment

C.11.19 In the digital identity and eGovernment sector, age verification is increasingly integrated into national identity frameworks and digital wallet ecosystems. These implementations prioritise trust, auditability and data minimisation:

- ConnectID (Australian Payments Plus) uses customer account data from KYC-verified banks to return binary age assertions (e.g., "Over 18"), with no DOB or identity data shared. The process is fully consent-based, with peer-to-peer exchanges between the bank and relying party and no central data storage.
- Austroads supports authoritative source verification via digital credentials embedded in mobile driver licences (mDLs). These credentials allow selective disclosure, such as "Over 18" confirmation, without revealing the full DOB. The system was successfully tested in both online and offline environments and is live in Queensland.

C.11.20 These implementations represent the leading edge of standards-aligned privacy engineering, using frameworks such as ISO/IEC FDIS 27566-1 and ISO/IEC 18013-5 (mobile driving licence standards) to ensure trust and interoperability across platforms.

A mature, adaptive ecosystem

C.11.21 Throughout the Trial, providers demonstrated a strong capacity to configure and orchestrate verification flows based on sector needs. For example:

- Fallback mechanisms such as selfie-based estimation were used when authoritative record checks failed.
- Credential reuse via digital wallets was tested successfully in Austroads' cross-jurisdictional demonstrations.
- Systems like Luciditi and Yoti showed modularity that allows rapid integration into high-risk sectors or privacy-sensitive environments alike.

C.11.22 As age verification continues to evolve in Australia, we can expect greater emphasis on cross-sector interoperability, verified credential reuse and selective disclosure, driven by privacy legislation, user expectations and international best practices.

C.12 Innovation and User-Centric Design in the Age Verification Sector

C.12.1 We found a vibrant, creative and innovative age verification service sector with both technologically advanced and deployed solutions. The service providers demonstrated a continuous commitment to improvement, with many seeking:

- New ways to verify dates of birth.
- More advanced and friction-reducing approaches to binding results to individuals.
- A focus on smoother user journeys minimising barriers to entry to age restricted goods, services, content, venues or spaces whilst retaining their effectiveness.



Vendor Case Study



Website

egdc.com.au

Focuses on youth gaming environments. Performs manual ID checks at in-person events and plans to launch a privacy-sensitive tokenised ID system using gesture-based spoof resistance, minimal data retention and community trust principles for underage users.

Practice Statement

ageassurance.com.au/v/ede/#PS

Technology Trial Test Report

ageassurance.com.au/v/ede/#TR

Privacy Policy

ageassurance.com.au/v/ede/#PP

Technology Trial Interview

ageassurance.com.au/v/ede/#VI

Summary of Results

System shows strong youth sector alignment and local trust-building. Prototype phase limits scalability and cross-sector applicability. Video call spoofing detection was innovative but needs broader testing. Broader deployment and digital interoperability remain underdeveloped.

C.12.2 The Trial observed that Australia's age verification sector is not only technologically mature, but also dynamic and forward-looking. Providers are demonstrating a strong commitment to continuous innovation, aiming to improve accuracy, inclusivity and user experience while upholding privacy, security and regulatory alignment.

C.12.3 Rather than treating age verification as a static, compliance-focused function, service providers are investing in R&D, iterative refinement and user-focused design, making solutions more effective and more acceptable to the individuals and organisations that rely on them.

| New approaches to verifying date of birth

C.12.4 While traditional document- and record-based verification remains dominant, providers are experimenting with and implementing novel methods to source and validate DOB data, including:

- Direct API-based verification with government registries and authoritative sources
- Use of community or alternative records to support users without formal identity documents (e.g. in First Nations communities)
- Integration with digital wallets and mobile credentials, such as digital driver licences, to support privacy-preserving retrieval and re-use of DOB

C.12.5 These approaches reflect a shift from one-off checks to more modular, reusable and interoperable age assurance models.



Example of a New Approach to Age Verification

The **National Exchange of Vehicle and Driver Information System** (NEVDIS) is a secure, nationally coordinated database operated by Austroads, containing verified driver licence data from all Australian states and territories.

Because NEVDIS records include authoritative, government-issued identity data, including date of birth (DOB), it presents a powerful and privacy-conscious source for age verification.

In age assurance contexts, NEVDIS can be accessed via API-based “match/no match” queries, where a user’s submitted information (e.g. licence number and name) is checked against NEVDIS records to confirm if they are over a given age threshold (e.g. Over 18). Crucially, this model:

- Does not return the full DOB, reducing unnecessary data exposure;
- Offers real-time verification from a trusted source; and
- Aligns with ISO/IEC FDIS 27566-1 principles of selective disclosure and minimal data handling.

As part of the Trial, NEVDIS was identified as a high-assurance mechanism that could support scalable, privacy-respecting age checks across retail, online services and public sector use cases.

Vendor Case Study



Website

myearth.id

EarthID provides decentralised, blockchain-based age verification solutions that prioritise user privacy, data security and consent-driven identity sharing, aligning with international standards for trustworthy digital age assurance systems.

Practice Statement

ageassurance.com.au/v/ear/#PS

Technology Trial Test Report

ageassurance.com.au/v/ear/#TR

Privacy Policy

ageassurance.com.au/v/ear/#PP

Technology Trial Interview

ageassurance.com.au/v/ear/#VI

Summary of Results

EarthID demonstrated a privacy-focused, decentralised age verification solution using blockchain technology and emphasised user consent and data minimisation. Evaluation noted strengths in security and transparency, though further detail on technical deployment, scalability and integration with relying parties was recommended for improvement.

| Friction-reducing binding and identity matching

C.12.6 Binding the verified DOB to the correct individual – traditionally achieved via biometric “selfie match” or document matching – is also evolving. Providers are:

- Streamlining biometric matching workflows through liveness detection and rapid face comparison
- Using cryptographic binding in conjunction with device trust signals and secure elements (e.g. secure enclaves or chip-based IDs)
- Exploring token-based identity representations that can be matched without persisting any PII

C.12.7 These innovations support fast, secure and less intrusive identity binding, particularly valuable in mobile-first use cases and time-sensitive transactions.



IDVerse[™]
A LexisNexis® Risk Solutions Company

IDVerse provides identity verification and age assurance services with a focus on automated biometrics, cryptographic security and zero-data persistence. In the Trial, IDVerse demonstrated a highly optimised system for frictionless, secure identity binding, particularly suited to digital onboarding and mobile-first scenarios.

Vendor Case Study



Website

yoti.com

Yoti provides low-friction, high-trust verification with one-time and reusable tokens. A standout example of minimising user friction while maintaining assurance comes from Yoti, whose platform consistently prioritised privacy, simplicity and user control throughout the Trial.

Three Key Facts

1

"Over 18" binary checks: Yoti enables users to prove they are over a certain age without ever sharing their full date of birth.

2

One-time, session-based tokens users receive a pseudonymous token that can be used to access age-restricted content or services.

3

Mobile interface presents concise, user-friendly explanations of what data will be shared, with whom and for what purpose, empowering informed choices.

Strengths

Privacy and Assurance in Balance.

Yoti's system complies with ISO/IEC FDIS 27566-1 by using:

- Hashed, non-linkable identifiers
- No persistent identity profiles unless explicitly required
- Privacy by design, ensuring minimal data is retained

Practice Statement

ageassurance.com.au/v/yot/#PS

Privacy Policy

ageassurance.com.au/v/yot/#PP

Technology Trial Test Report

ageassurance.com.au/v/yot/#TR

Technology Trial Interview

ageassurance.com.au/v/yot/#VI

Summary of Results

Yoti excelled in frictionless, privacy-focused AV. No full DOBs were retained, only session-based tokens. One of the most privacy-forward platforms in the Trial.



| Focus on smoother user journeys

C.12.8 One of the most promising developments across the sector is a strong focus on minimising friction for users while maintaining assurance levels. Providers are simplifying user journeys by:

- Offering “over X” checks rather than requiring users to share full DOBs with relying parties
- Reducing steps in verification flows (e.g. pre-filled ID scans, reusable identity profiles)
- Providing clearer user awareness and friendly interfaces that explain what data is shared, with whom and why

C.12.9 For example, several providers offer one-time, session-based verification tokens that can be presented to multiple relying parties without repeated identity exposure. This model enables low-friction, high-trust access to restricted content or services without compromising privacy.

| Sector diversity and responsiveness

C.12.10 The sector includes a wide range of provider types – from established identity verification companies to emerging startups. This diversity is driving experimentation and rapid iteration, including:

- Cross-platform age verification Software Development Kits and Application Interfaces.
- Integration with parental control signals, where applicable.
- Deployment of AI to support fraud detection and automated decision-making.

C.12.11 In highly regulated sectors like gambling and fintech, providers are also embedding age verification more deeply within broader anti-money laundering/know your customer compliance frameworks, ensuring seamless integration with other trust signals.

C.12.12 Australia's age verification ecosystem is marked by creativity, adaptability and a strong ethos of user protection. Providers are not only meeting current regulatory and market requirements but are actively advancing the state of the art in how age can be verified securely, respectfully and with minimal friction.



C.12.13 Examples of AV Providers that support diversity of approach:

Provider	Type	Cross-Platform SDK/API	Parental Control Signals	AI for Fraud Detection	Embedded in AML/KYC Workflows
GBG (ID3global)	Established ID verification provider	Yes	Not specified	Yes	Yes
Verifymy	Established ID verification provider	Yes	Not specified	Yes	Yes
Yoti	Privacy-first ID Provider	Yes	Supported in broader platform	Yes	Partial (Yoti KYC toolkit)
Luciditi	Privacy-focused identity platform	Yes	Not specified	Yes	No
ConnectID	Federated identity exchange	Yes	Not applicable	No	Yes (via banks)
AgeChecked	Hybrid verification service	Yes	Not specified	Yes	Yes
IDVerse	AI-driven ID verification provider	Yes	Not specified	Yes	Yes
Austroads	Government-backed infrastructure	Partial (government integration)	No	No	No
PRIVO	Child privacy-focused provider	Web SDK (US-based)	Native parental consent	Yes	No
FrankieOne	Orchestration layer	Yes	Not Applicable	Risk and fraud scoring	Yes

C.13 Privacy by Design and Data Minimisation in Age Verification

C.13.1 We found robust understanding of and internal policy decisions regarding, the handling of personal information by independent age verification service providers. They all displayed a focus on data minimisation and privacy by design and most providers only retained a secure (hashed) transaction code that did not contain personally identifiable information. Unless relying parties required more detailed information perhaps as a result of a regulatory requirement, most providers simply provided a binary 'Yes/No' answer to a question such as, is this person over 18?

C.13.2 The evaluation found that independent age verification service providers demonstrated a strong and consistent commitment to privacy by design, data minimisation and secure data handling. These practices were embedded both at the technical architecture level and in the providers' internal policies, aligning closely with the principles and requirements outlined in ISO/IEC FDIS 27566-1, the emerging international standard for age assurance systems.



| Why is privacy by design important

C.13.3 Privacy by design and data minimisation are critical to age verification because they ensure that verifying a person's age does not require unnecessary exposure of their identity or personal information. Age verification often involves sensitive data – such as official documents or biometric identifiers – and without strong safeguards, these systems risk enabling over-collection, long-term tracking or secondary misuse of personal data. By embedding privacy protections into the architecture of these systems from the outset and by limiting data collection to only what is strictly necessary (e.g., a binary “Over 18: Yes/No” response), providers can deliver effective age assurance while upholding individuals' rights, reducing compliance burdens and fostering public trust. These principles are central to international standards such as ISO/IEC FDIS 27566-1, which emphasise proportionality, transparency and user control as essential components of responsible age assurance.

C.13.4 This standard emphasises that age assurance systems should not collect or disclose more information than is strictly necessary to fulfil their intended purpose. It advocates for:

- Use of binary or threshold-based responses (e.g., “Is this person over 18?”)
- Avoidance of sharing full dates of birth, unless absolutely required
- Support for selective disclosure and cryptographic proofs
- Secure, non-identifiable transaction records
- Design approaches that minimise privacy risks throughout the system lifecycle

C.13.5 The Trial found that Australian-based and international providers participating in the evaluation largely conformed to these principles in practice.



Vendor Case Study

Website

oneclickgroup.com.au

One Click Group delivers decentralised, mobile-first identity with encrypted device-bound tokens. Uses facial recognition and liveness detection to securely bind age to the user without server-side data storage.

Practice Statement

ageassurance.com.au/v/one/#PS

Technology Trial Test Report

ageassurance.com.au/v/one/#TR

Privacy Policy

ageassurance.com.au/v/one/#PP

Technology Trial Interview

ageassurance.com.au/v/one/#VI

Summary of Results

Excellent privacy and decentralised model. KYC-heavy defaults may over-collect data. Lacks tailored UX for youth and vulnerable users. Technically sound and well-suited for privacy-sensitive applications, with potential for improved configurability.

| How is privacy by design being implemented

C.13.6 Providers implemented privacy-first design in several key areas:

- **Data minimisation by default:** Most systems were architected to return only a simple confirmation of age threshold status (e.g., over 13, over 18), rather than sharing a user's full DOB or other identifying information.
- **Non-persistent identifiers:** In most cases, no persistent or personally identifiable information (PII) was retained following a successful verification. Instead, providers retained only a hashed transaction code or token that could be referenced in future audits or for troubleshooting – without exposing user identity.
- **User transparency and control:** Several providers offered clear consent flows, allowing users to understand what data was being shared, how long it would be retained and who would receive it. This aligns with ISO/IEC FDIS 27566-1's emphasis on transparency and accountability.

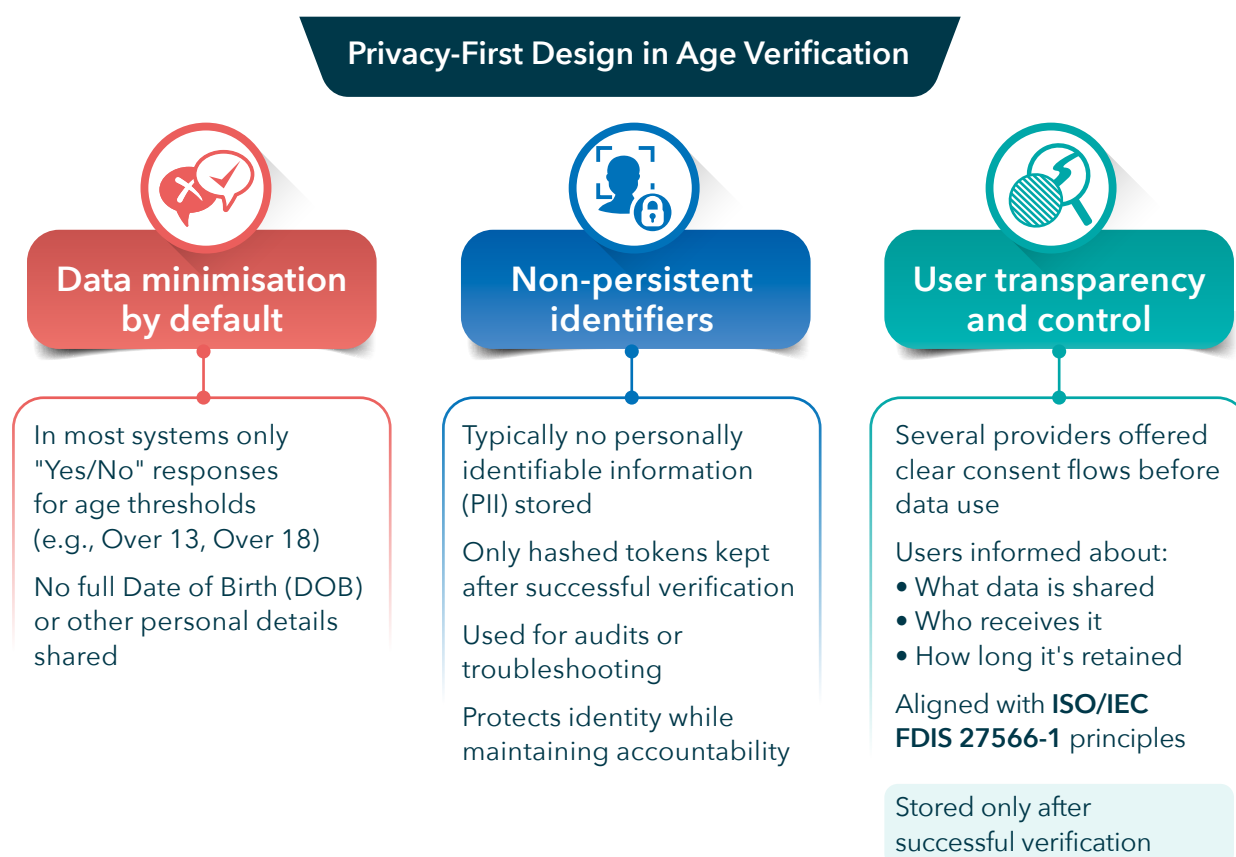


Figure C.13.1 Providers Implemented Privacy-First Design in 3 Key Areas

| What examples are there from Trial participants

- **Yoti:** Their age verification system uses a one-time facial scan and document verification, followed by a binary output to the relying party (e.g., "Over 18: Yes"). According to their privacy policy and practice statement, no biometric data or full identity details are retained and only a secure hash of the transaction is stored for audit purposes.
- **Verifymy:** This provider offers integration with digital wallets and relies on selective disclosure protocols, which allow the user to present a cryptographically verified age claim without sharing the underlying date of birth or identity.
- **GBG:** In regulated sectors such as financial services, GBG systems are capable of providing detailed outputs if required (e.g., full DOB for AML checks), but their systems are configurable to default to minimal disclosures for age-only checks, as expected in lower-risk scenarios.

C.13.7 These examples demonstrate how configurability and context-sensitive deployment enable providers to support a wide range of use cases while still adhering to the minimum data principle.



Vendor Case Study



Website

privo.com

PRIVO provides privacy-focused, parental consent-based AV services using facial estimation, document checks and guardian approval workflows. COPPA-certified and focused on protecting children in online services and educational contexts.

Practice Statement

ageassurance.com.au/v/pvo/#PS

Technology Trial Test Report

ageassurance.com.au/v/pvo/#TR

Privacy Policy

ageassurance.com.au/v/pvo/#PP

Technology Trial Interview

ageassurance.com.au/v/pvo/#VI

Summary of Results

Robust privacy protocols and high assurance for under-13 use. US-centric framework limits direct Australian applicability. Excellent for family-focused platforms. Zero knowledge proof use and secure credential handling were standout features in its category.

| How does this align with ISO/IEC FDIS 27566-1 requirements

C.13.8 ISO/IEC FDIS 27566-1 specifies the following key requirements that were met or exceeded by providers:

ISO/IEC FDIS 27566-1	Criteria
Data Minimisation (Clause 5.6)	Systems should disclose only the information required to make an age-based decision.
Privacy and Security (Clause 5.3)	Providers must apply privacy by design, ensuring that personal data is collected and processed lawfully, fairly and transparently.
Output Control (Clause 5.4)	Age signals should be communicated in a privacy-protective way (e.g., binary assertions or cryptographic tokens).
Selective Disclosure (Clause 6.2)	Systems should support the use of derived credentials or proofs that confirm age without revealing the DOB itself.

C.13.9 Across the Trial, providers demonstrated high fidelity to these design and policy requirements, indicating strong readiness for future conformity assessment and certification once the ISO standard is finalised.

C.13.10 The Trial confirmed that privacy by design is a foundational principle in the implementation of age verification systems. Providers consistently adopted practices that minimise data exposure and empower users, while maintaining regulatory compliance and system reliability. These privacy-focused approaches not only meet the expectations of ISO/IEC FDIS 27566-1 but also help build public trust in the broader age assurance ecosystem.

C.13.11 Most privacy policies confirm data minimisation and purpose-limited use.

C.13.12 However, in some providers, especially those with configurable output options, there are provisions where:

- More data can be collected or shared (e.g., full DOB or ID scan) based on relying party requirements.
- While configurable, this places a privacy burden on the relying party and may blur separation if not clearly documented or enforced.



C.13.13 A sample of ten age verification providers and how their privacy policies align with the characteristics shown in ISO/IEC FDIS 27566-1.

Provider	Binary Response	Minimal Data Retention	No Full DOB Shared	Selective Disclosure	Transparency and User Control	ISO/IEC FDIS 27566-1 Alignment
Yoti	Yes	Hashed transaction only	Yes	Yes	Yes	Strong
Verifymy	Yes	Yes (cryptographically verified claim)	Yes	Yes (via wallets)	Yes	Strong
GBG	Configurable	Depends on configuration	Default is Yes	Supported	Yes	Strong
AgeChecked	Yes	Anonymised only	Yes (unless required)	Yes	Yes	Strong
Luciditi	Yes	Yes, configurable	Yes (threshold confirmation only)	Yes	Yes	Strong
ConnectID	Yes	No PII retained by ConnectID	Yes	Yes	Yes (consent dashboards)	Strong
DigiChek	Yes	Only name, DOB and place of birth	Only if required by relying party	Yes	Yes	Strong
EarthID	Yes	No central storage	Yes	Yes (ZKPs)	Yes	Strong
Private Identity	Yes	Homomorphic token only; no biometric or PII retained	Yes	Yes (FHE-based verification)	Yes	Strong
PRIVO	Yes	Depends on method; session tokens or pseudonymous identifiers used	Only shared if method selected by user requires it	Yes (various methods including credit card, document ID)	Yes	Strong

Vendor Case Study



Website

privateid.com

PrivateID implements face/voice/fingerprint authentication via fully homomorphic encryption, eliminating central data storage. Offers secure, device-local identity verification with privacy and security at the forefront of its design philosophy.

Practice Statement

ageassurance.com.au/v/pid/#PS

Technology Trial Test Report

ageassurance.com.au/v/pid/#TR

Privacy Policy

ageassurance.com.au/v/pid/#PP

Technology Trial Interview

ageassurance.com.au/v/pid/#VI

Summary of Results

Excellent cryptographic privacy and minimal data exposure. Complex UX may hinder accessibility for lower-literacy users. A strong solution for high-risk or enterprise use cases, though onboarding simplification would help general adoption.

C.14 Demographic Consistency and Inclusion in Age Verification

C.14.1 Age verification service providers use demographic-neutral tools to verify age but some also make proactive efforts to include those without formal identity documents, such as certain First Nations and Torres Strait Islander peoples. This includes seeking access to alternative or community-based records, ensuring more inclusive and accurate verification across Australia's diverse populations. However, there may be cultural and education barriers for individuals who need to seek verification of their age, particularly where this involves regulatory or judicial applications or processes. Where age verification service providers are using biometric comparison (sometimes called a 'selfie match') to verify the holder of a document or record, we found they performed broadly consistently across the demographic groups assessed.

C.14.2 This finding reflects not only technical maturity but also an awareness of the social and cultural dimensions of identity assurance, aligning with the inclusivity and equity objectives set out in ISO/IEC FDIS 27566-1.

| Why demographic consistency matters

C.14.3 Demographic consistency in age verification is vital to maintaining fairness, accuracy and public trust. If systems work less effectively for certain groups – whether due to skin tone, cultural presentation or lack of identity documentation – those individuals may face disproportionate exclusion from digital services or experience invasive or repeated verification requests. This not only undermines user dignity and fairness but also increases the risk of digital exclusion – particularly for Aboriginal and Torres Strait Islander communities and other groups with diverse cultural or access needs. ISO/IEC FDIS 27566-1 recognises this and its guidance on inclusive design serves as a framework to mitigate these risks and promote equal access to digital age-restricted environments.

| Proactive inclusion of underserved populations

C.14.4 In accordance with ISO/IEC FDIS 27566-1 which addresses inclusivity and fairness (Clause 9.2), providers are encouraged to design and implement systems that are inclusive of users with limited access to conventional identity credentials. During the evaluation, we observed several promising approaches, including:

- Use of alternative or community-based records to establish DOB (e.g. school records, health services data or community verification processes)
- Outreach and consultation efforts with community organisations to understand barriers and co-design solutions
- Technical flexibility in integrating non-standard data sources where reliability could be demonstrated and legally permitted

C.14.5 Such efforts contribute to a more inclusive age assurance ecosystem, where individuals are not excluded simply because they fall outside conventional administrative systems. Here are some examples from the vendor interviews about approaches to these issues:

Use of Alternative or Community-Based Records	
DigiChek	Uses school enrolment records for children and community verification through in-person registrars for adults lacking formal ID.
Austroads	Highlighted ongoing work to support community-based credentials and is exploring credential issuance beyond driver licensing.
Verifymy	Capable of integrating authoritative data sources and has shown flexibility in configuring verification pathways for different sectors, including those with limited formal ID.

Outreach and Consultation with Community Organisations

Austroads	Conducted “on-country” testing with First Nations communities in Queensland to ensure facial recognition and liveness checks were not biased or exclusionary.
ConnectID (Australian Payments Plus)	Plans to include state governments and community-trusted identity providers in its scheme to increase inclusivity and culturally sensitive identity verification options.
Luciditi	While direct consultation wasn’t reported, their system includes configurable language files and accessibility UI, showing an openness to localisation and potential future community collaboration.

Technical Flexibility for Non-Standard Data Sources

Yoti	Supports age verification using digital wallets and one-time tokens, including credentials issued by trusted community or government sources without exposing full DOB.
Verifymy	Integrates with UK and Australian authoritative data sources and is adaptable to non-document-based flows when legally permissible.
Austroads	Demonstrated infrastructure to support digital age credentials using verifiable claims (e.g., “Over 18”) without requiring full document sharing.

| Performance across demographic groups

C.14.6 In systems using biometric comparison (e.g. 'selfie match') to bind identity documents to individuals, the evaluation assessed the performance of technologies across a diverse range of user demographics. The results indicated that biometric components generally performed broadly consistently across the demographic groups assessed, with no statistically significant evidence of accuracy degradation based on ethnicity, gender or age.

C.14.7 This finding is consistent with the demographic-neutrality principle embedded in ISO/IEC FDIS 27566-1, which requires that age assurance systems:

- Be designed and tested to avoid discriminatory outcomes
- Support equity of access and performance across populations
- Monitor and mitigate any observed disparities in effectiveness

C.14.8 Providers with biometric components also implemented presentation attack detection measures in line with ISO/IEC 30107-3 (biometric presentation attack standards), further ensuring reliability and resilience against spoofing across all user groups.

| Access to digital identity and demographic consistency

C.14.9 Ensuring equitable access to age verification services requires specific attention to the persistent digital identity and infrastructure gaps experienced by many First Nations communities in Australia. These gaps impact both the technical feasibility of age verification and the cultural appropriateness of current identity frameworks.

C.14.10 Research described on the next two pages has shown that individuals in remote and very remote areas frequently lack access to the core documents – such as birth certificates or driver’s licences – needed to participate in standard age verification processes.

C.14.11 A 2024 report by AusPay+ (Trial participant) underscores these challenges, identifying that many Aboriginal and Torres Strait Islander people face systemic barriers to obtaining identity documents.

Vendor Case Study



TruAnon
Digital Identity

Website

truanon.com

TruAnon delivers anonymous age verification with no biometric or document use. Uses cryptographic hashes and digital signatures to confirm age status without identifying the individual.

Practice Statement

ageassurance.com.au/v/tru/#PS

Technology Trial Test Report

ageassurance.com.au/v/tru/#TR

Privacy Policy

ageassurance.com.au/v/tru/#PP

Technology Trial Interview

ageassurance.com.au/v/tru/#VI

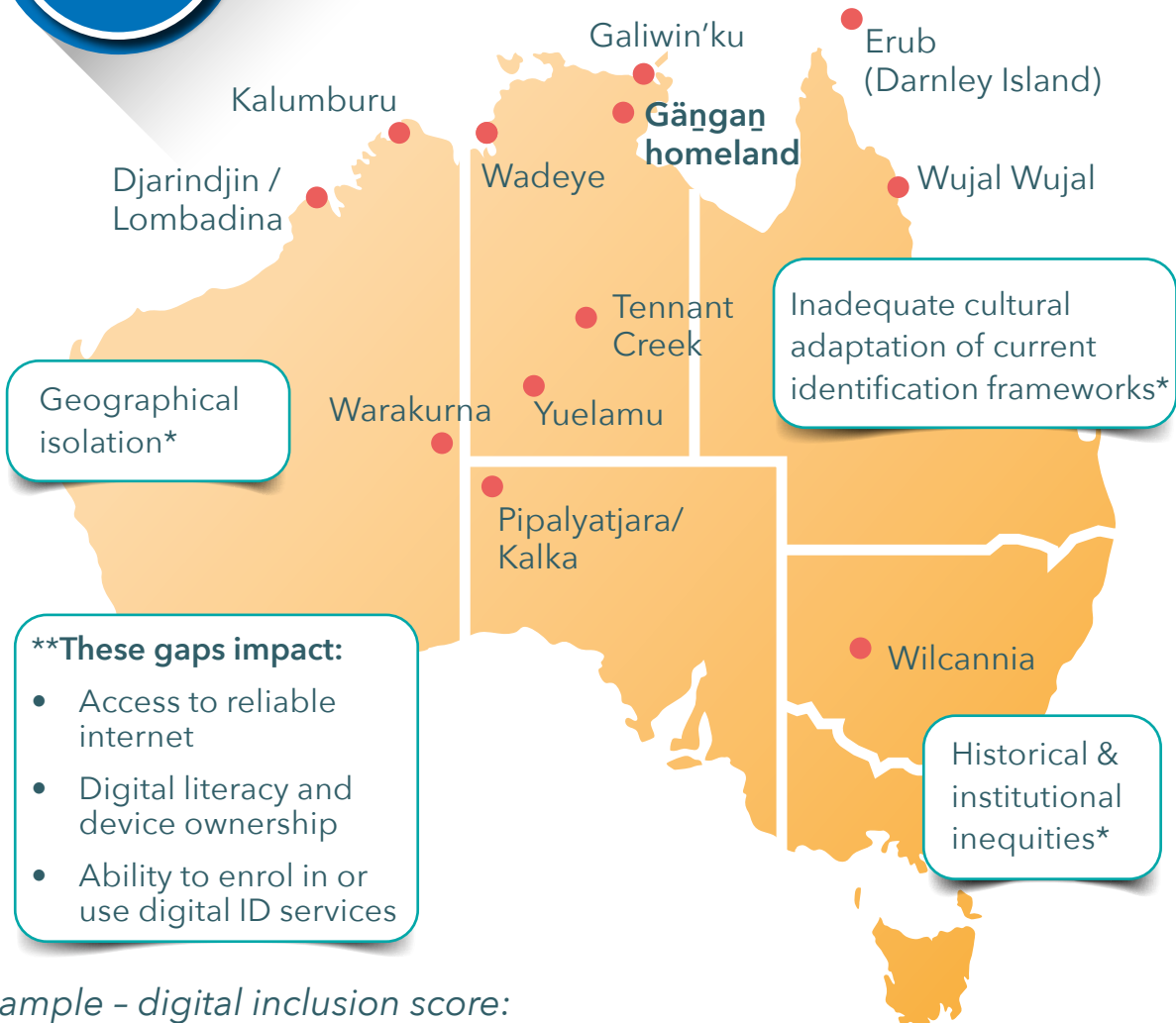
Summary of Results

Privacy maximised but assurance and user trust limited unless embedded properly. Highly secure architecture, but lack of identifiers may hinder acceptance. Good fit for anonymity-critical applications like adult content access.

Digital Inclusion and Infrastructure Gaps

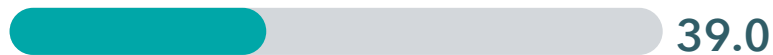
25+
point gap

between First Nations people and non-Indigenous Australians in very remote areas.



Example - digital inclusion score:

Gängan homeland



National Average



The Mapping the Digital Gap project (RMIT, Telstra, ADM+S) highlights significant disparities in digital access

** The Australian Digital Inclusion Index (ADII) 2023

* Source: AusPay+, "Identity in Crisis", 2024

Figure C.14.1 Digital Inclusion and Infrastructure Gaps

| Impact of the gaps

C.14.12 The impact of the gaps could be:

- Access to reliable internet
- Digital literacy and device ownership
- Ability to enrol in or use digital ID services

Sources: Mapping the Digital Gap, 2023; ADII 2023

| Implications for Age Verification

C.14.13 Without adequate connectivity, documentation or support, users in these communities are at risk of:

- Being excluded from digital services that rely on age verification
- Facing repeated or invasive checks
- Losing autonomy due to misaligned ID frameworks

C.14.14 These challenges must be addressed to ensure that age verification systems uphold demographic consistency and do not inadvertently amplify digital exclusion.

mappingthedigitalgap.com.au

C.15 Improving Data Access and Risk Management in Age Verification

C.15.1 There is scope for technological improvement and enhancing the management of risk in age verification systems particularly relating to access to reliable data. Only some of the age verification systems were able to detect if a presented document had been reported as lost or stolen by reference to authoritative sources. This may only be partially rectified by biometric comparison of the holder to the document. Most were effective at spotting forgeries and counterfeits (including advanced artificial intelligence generated presentation attacks).

C.15.2 The systems could be enhanced, where proportionate to the use case in mind, through one-way blind access to government verification of data - where an application programming interface (API) could be used to provide a 'MATCH/NO MATCH' response to data held by government or an authoritative source, based on that captured from the document or record presented by the individual. In addition, the systems may benefit from securing and analysing verified credentials from data holder services (like digital wallets), which also provide an opportunity for the results of an age verification system to be stored for reuse in such services.

C.15.3 While the age verification systems assessed in the Trial were generally robust and standards-aligned, the evaluation identified clear opportunities for technological improvement, particularly in relation to accessing and validating reliable source data. Effective age verification depends not only on technical processing but also on the authenticity, accuracy and timeliness of the data used to verify a person's date of birth.

C.15.4 This finding aligns with key provisions in ISO/IEC FDIS 27566-1, particularly:

ISO/IEC FDIS 27566-1	Criteria
Clause 5.2 (Data Source Assurance)	Which calls for the use of genuine, valid and current data from trusted sources.
Clause 5.5 (Resilience and Security)	Requiring systems to guard against data manipulation, forgery or substitution.
Clause 6.3 (Risk Management)	Emphasising the importance of system-level safeguards, particularly when data cannot be fully validated.

| Opportunities for improvement

Blind government verification APIs

C.15.5 The evaluation supports a one-way blind verification model, in which an age verification system could:

- Capture DOB and document metadata from the user.
- Transmit it securely via an API to a government service.
- Receive a “MATCH/NO MATCH” response—without revealing the user’s identity to the government or exposing government records to the provider.

C.15.6 This model supports:

- Minimal disclosure, consistent with ISO/IEC FDIS 27566-1 Clause 6.1 (Selective Disclosure).
- Privacy-preserving architecture, avoiding centralised identity tracking.
- Improved confidence in document legitimacy.

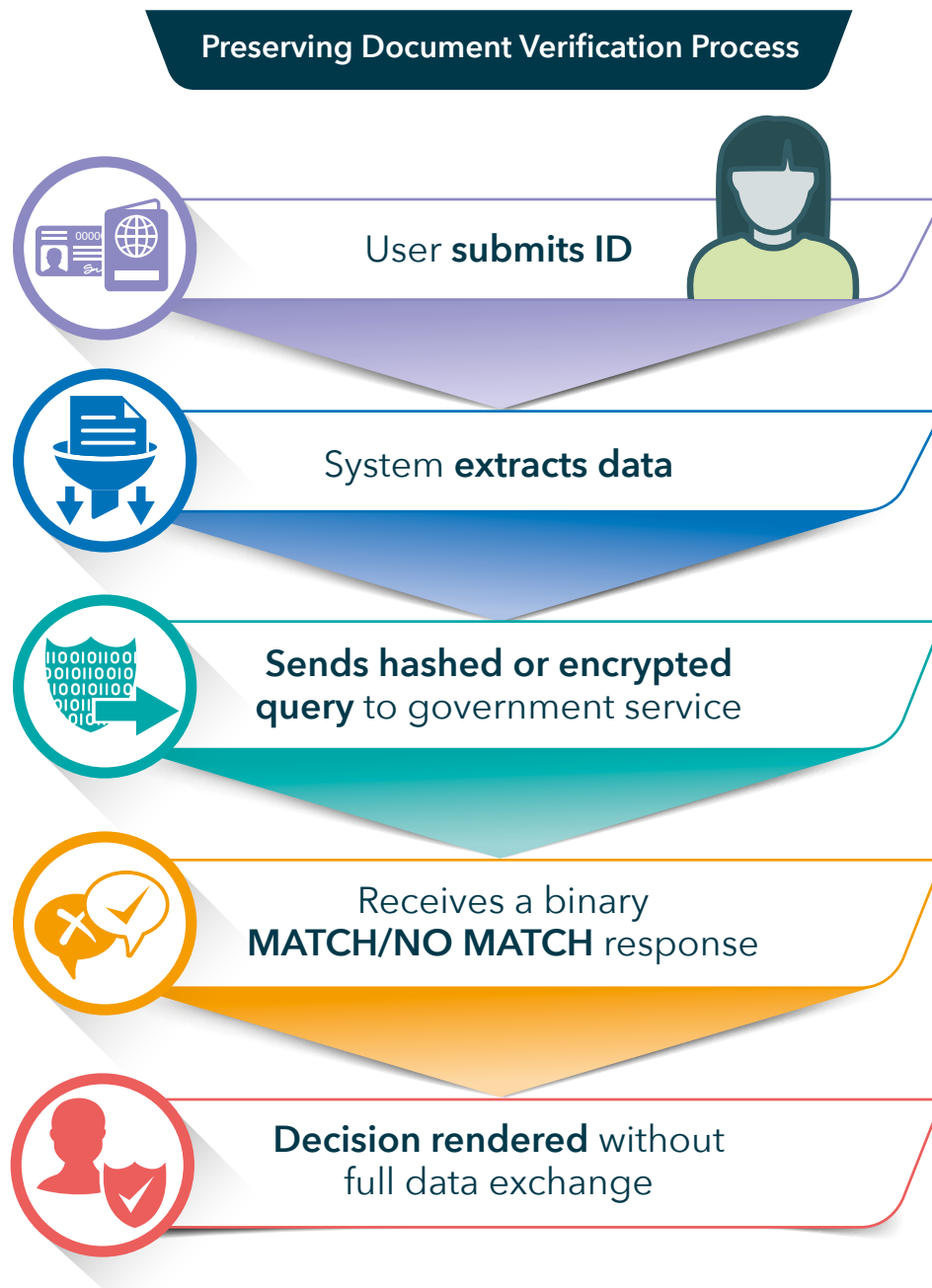


Figure C.15.1 Preserving Document Verification Process

Integration with verified credential ecosystems

C.15.7 A second enhancement area is integration with digital wallets and verified credential holders, such as:

- Mobile driver licences (mDLs)
- Government-verified identity wallets
- Reusable, cryptographically signed age tokens.

C.15.8 These systems allow verified DOB data to be:

- Stored securely on the user's device
- Reused with consent across services
- Updated or revoked as needed.

C.15.9 This aligns with the vision set out in ISO/IEC FDIS 27566-1 for privacy-preserving reusability and supports more efficient age assurance across platforms.

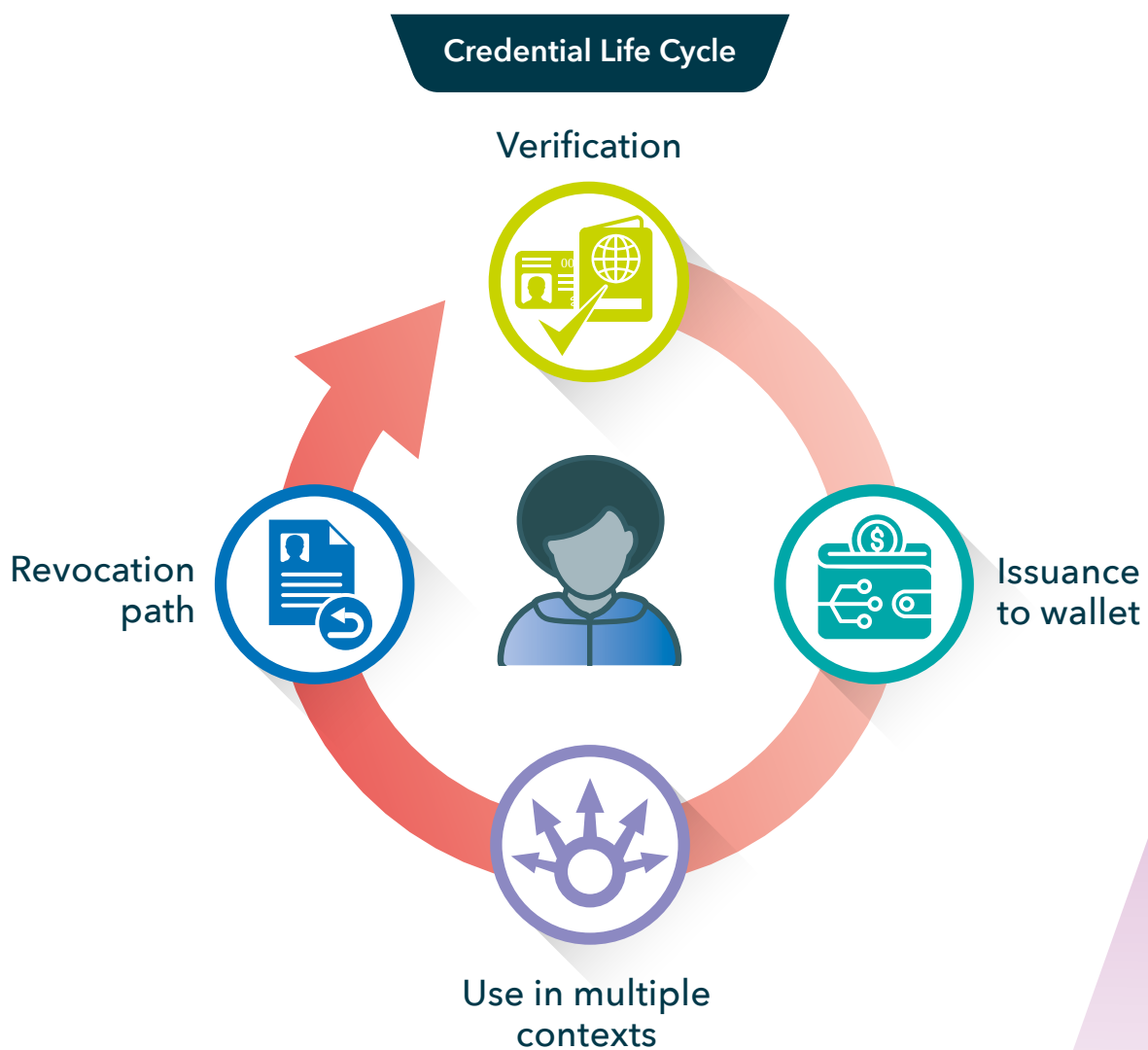


Figure C.15.2 *Credential Life Cycle*

| What examples are there from Trial participants

- **Trust Stamp** specialises in irreversible, non-Personal Health Information biometric hashing, creating persistent but untraceable tokens that can be used for repeated age verification across services. This supports token-based reuse: A user can verify age once and present the resulting token across relying parties without repeating document or biometric steps. No PII stored: Tokens contain no personal data, aligning with privacy-by-design and selective disclosure models.
- **FrankieOne** is an orchestration platform that integrates with banks, government registries, telcos and utilities for identity and DOB verification. This connects to authoritative sources to validate submitted data against real-world records. Particularly useful in financial and AML/KYC-sensitive contexts like fintech and gambling.
- **Sedicii** enables age and identity verification using zero-knowledge proofs, allowing a user to prove they meet a criterion (e.g. "Over 18") without revealing underlying data like DOB. This embeds privacy-preserving cryptographic logic at the protocol level. Supports federated identity reuse and has proposed models for integration with national ID and banking data without data leakage.

Vendor Case Study



Website

sedicii.com

Sedicii uses document scanning with biometric selfie matching or zero-knowledge proofs if no ID available. Issues single-use, unlinkable binary credentials (e.g. Over 18) without identity exposure.

Practice Statement

ageassurance.com.au/v/sed/#PS

Technology Trial Test Report

ageassurance.com.au/v/sed/#TR

Privacy Policy

ageassurance.com.au/v/sed/#PP

Technology Trial Interview

ageassurance.com.au/v/sed/#VI

Summary of Results

Sedicii enables age and identity verification using zero-knowledge proofs, allowing a user to prove they meet a criterion (e.g. "Over 18") without revealing underlying data like DOB. This embeds privacy-preserving cryptographic logic at the protocol level. Supports federated identity reuse and has proposed models for integration with national ID and banking data without data leakage.

C.16 Information Security In Age Verification Systems

C.16.1 We found that the age verification systems were generally secure and consistent with information security standards. Most of the providers were able to demonstrate ISO/IEC 27001:2022 certified information security management and some had other supplementary security protocols (such as SoC2 or Fintech-level security).



Cross Reference: *Part K - Glossary, Bibliography & Literature Review*

- **ISO/IEC 27001:2022 Certification:** Most providers held up-to-date certification, which covers governance of information assets, access controls, encryption policies, vulnerability management and regular auditing procedures.
- **SOC 2 Compliance:** Some providers operated under Service Organization Control (SOC 2) Type II frameworks, ensuring the continuous monitoring of systems for confidentiality, availability and integrity - particularly relevant in financial and regulated sectors.
- **Fintech-Level Security Measures:** For providers operating in high-risk environments such as gambling or online finance, we observed:
 - End-to-end encryption of data in transit and at rest.
 - Role-based access controls and multi-factor authentication for staff and partners.
 - Secure application development practices (e.g. OWASP Top 10 compliance).
 - Real-time anomaly detection and intrusion prevention systems.

C.16.2 This strong security posture is particularly significant in the age verification context, where systems routinely handle identity documents, biometric data and age-related attributes. Such data, if compromised, could result in privacy violations, identity fraud or profiling of individuals. Ensuring that this information is collected, stored and processed securely is a baseline requirement for user trust and regulatory compliance.

| Security requirements under ISO/IEC FDIS 27566-1

C.16.3 ISO/IEC FDIS 27566-1 sets out specific obligations for age assurance systems with respect to security, many of which were demonstrably met by the providers participating in the Trial. Relevant clauses include:

ISO/IEC FDIS 27566-1	Criteria
Privacy and Security (Clause 5.3)	Privacy and Security: Requires systems to implement appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure, alteration or destruction. This includes adherence to recognised security frameworks such as ISO/IEC 27001.
System Resilience (Clause 5.5)	System Resilience: Emphasises the need for systems to remain secure and functional in the face of anticipated threats, including presentation attacks, forgery and injection attempts.
Risk Management and Security Controls (Clause 6.3)	Risk Management and Security Controls: Requires risk-based approaches to information security, including incident response, threat modelling and secure design practices.

| Security in the age verification context

C.16.4 Age verification involves distinct security challenges not always present in broader identity systems. These include:

- Handling biometric inputs (e.g. facial comparison for selfie match) and associated risks of spoofing or deepfake injection.
- Validating identity documents, where AI-generated forgeries must be detected with high reliability.
- Ensuring secure, minimal retention, as many providers aim to avoid long-term storage of identifying information – often returning only a binary “Yes/No” result to relying parties.

C.16.5 In this context, strong information security is not simply about infrastructure protection – it is essential to:

- Maintain the trust of end users, particularly young people and their guardians
- Protect against the misuse of sensitive data, such as sharing a verified age credential outside its intended purpose
- Ensure auditability and integrity of the verification process, especially when decisions have regulatory or legal consequences



Certification Status	Vendor
ISO 27001 Certified	AgeChecked Austroads ConnectID EarthID Equifax FrankieOne GBG PLC IDMission IDVerse iProov Luciditi MyMahi Persona PRIVO RightCrowd Sedicii ShareRing Verifymy Yoti
Not certified / Not yet certified / Planned	DigiChek Eden Game Development Centre Trust Stamp VerifyChain
Not confirmed	One Click Group Private Identity Qoria Trust Elevate

C.17 Biometric Binding, Spoofing Mitigation and Document Integrity

C.17.1 We found that providers were increasingly aware of injection attack vectors, whereby the user is able to bypass the sensor on the device (such as a camera) and inject code or images into the age assurance system workflow. International standards in this respect are developing (see ISO/IEC AWI 25456 - Biometric Data Injection Attack Detection), but providers were able to demonstrate some resilience to this type of attack.

What are a Presentation Attack (to a Sensor) and a Video Injection Attack (Bypassing the Sensor)

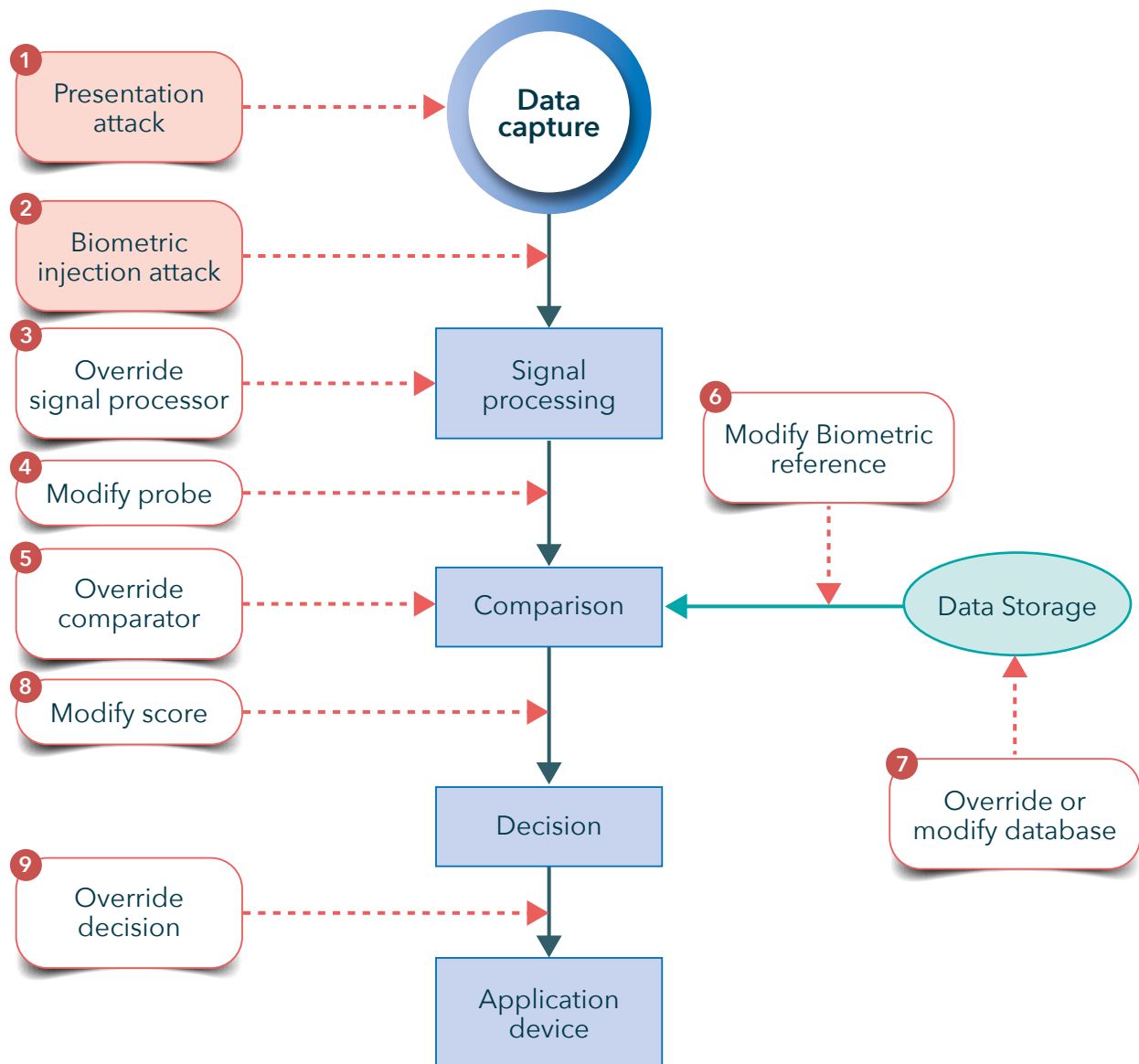


Figure C.17.1 What are a Presentation Attack and a Video Injection Attack

C.17.2 The providers assessed were able to identify fake, forged or counterfeit documents, including those generated by advanced artificial intelligence systems. Although they may pass casual visual inspection by door staff, bar staff or shop workers, our assessment is that they are unlikely to pose a threat to computer-based analysis.

C.17.3 A critical function of many age verification systems is the ability to securely bind a verified date of birth to the correct individual. This is most commonly achieved through biometric comparison, where a live facial image (a “selfie”) is matched to the photograph embedded within a government-issued identity document. This process enables the system to confirm that the person presenting the document is indeed its legitimate holder, satisfying a core requirement of ISO/IEC FDIS 27566-1 Clause 5.6 – Binding.

Vendor Case Study



Website

idmission.com

IDmission delivers biometric-based ID and age verification via selfie matching, document scans and fallback vouching. Offers a global, mobile-first SDK with inclusive options for users lacking traditional identity documents.

Practice Statement

ageassurance.com.au/v/idm/#PS

Technology Trial Test Report

ageassurance.com.au/v/idm/#TR

Privacy Policy

ageassurance.com.au/v/idm/#PP

Technology Trial Interview

ageassurance.com.au/v/idm/#VI

Summary of Results

High TRL, inclusive and efficient.

AI-driven verification performed well, but privacy documentation lacked detail. Streamlined onboarding and global applicability are strong points. Could enhance trust through clearer policy articulation on data use.

| Trustworthiness of input data

C.17.4 The evaluation found that providers have adopted advanced and standards-aligned methods to manage spoofing, AI-based fraud and data injection attacks, with strong performance across the systems tested.

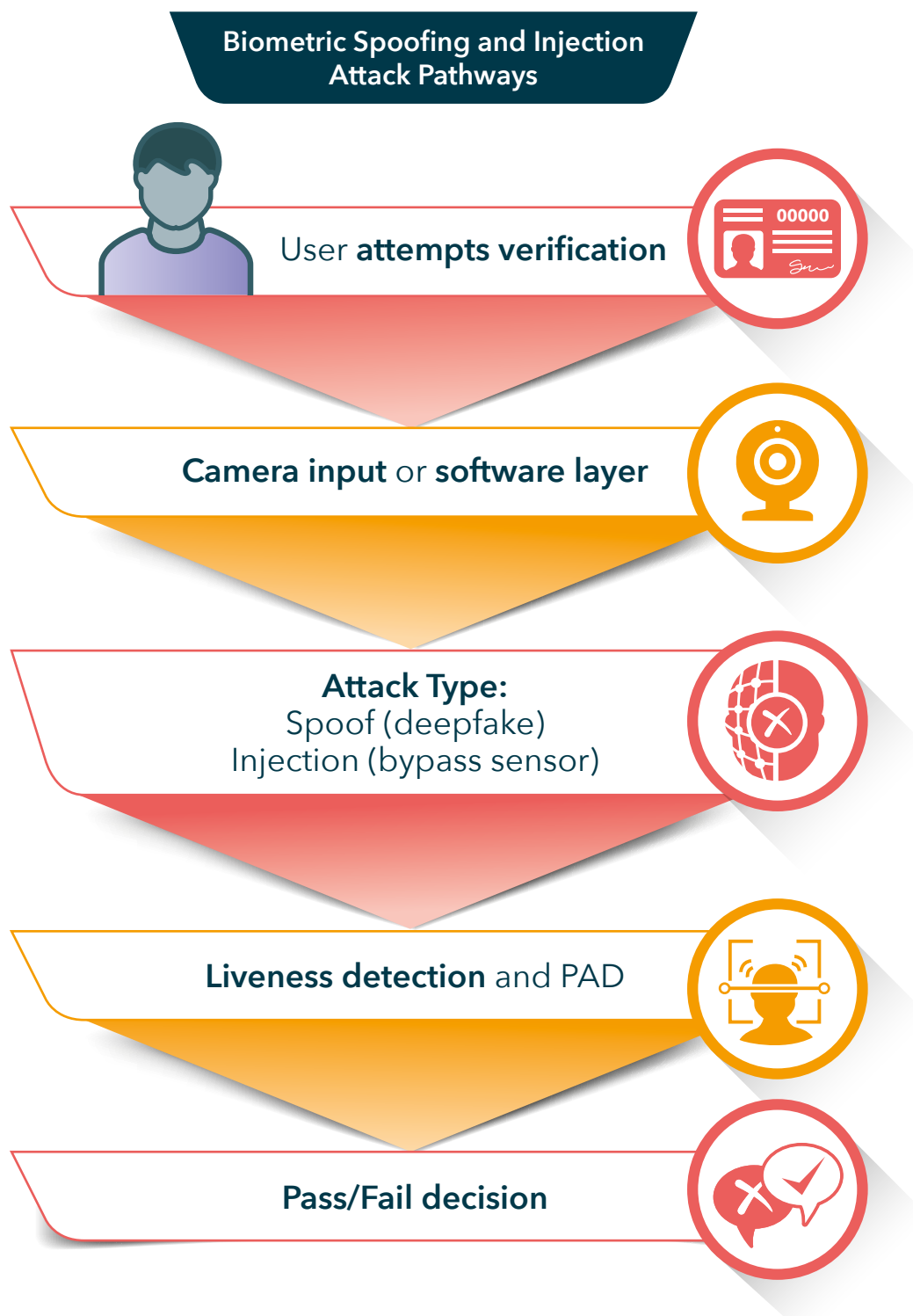


Figure C.17.2 Biometric Spoofing and Injection Attack Pathways

| Biometric comparison and presentation attack detection

C.17.5 The majority of participating providers implemented facial biometric matching tools to support document binding, with liveness detection and quality control processes designed to prevent common forms of presentation attacks. These techniques were implemented in line with the ISO/IEC 30107 series, which defines best practices for Biometric Presentation Attack Detection (PAD).

C.17.6 Presentation attacks may include:

- Static image presentation (e.g. printed photos).
- Replay attacks using video or animation.
- AI-generated synthetic faces or deepfakes.

C.17.7 The systems tested deployed countermeasures such as:

- Active liveness checks (e.g. blinking, head movements).
- Passive liveness detection using machine learning.
- Confidence scoring and risk flagging for manual review.

C.17.8 These features significantly reduce the chance of successful spoofing. While no system is entirely immune, it was evident that most providers met or exceeded PAD resilience thresholds recommended in ISO/IEC 30107-3. Importantly, systems were tested across a range of demographic conditions and environmental settings and demonstrated consistently high match accuracy without measurable bias.

| Injection attack awareness and response

C.17.9 The evaluation also identified growing provider awareness of injection attack vectors, whereby malicious users attempt to bypass sensors (such as cameras or scanners) and inject synthetic images or code directly into the age verification workflow. These attacks differ from spoofing in that they seek to subvert the system at the software or protocol level, potentially evading all biometric or liveness detection steps. Although specific countermeasures for these threats are still evolving, several providers showed early adoption of protections such as:

- Secure runtime environments for biometric capture,
- Tamper detection mechanisms in native mobile apps,
- Content authenticity validation using embedded metadata and source integrity checks.

C.17.10 This aligns with the direction of ISO/IEC AWI 25456 – Biometric Data Injection Attack Detection, a developing standard which aims to formalise countermeasures for this emerging threat type. While the standard remains in draft form, the readiness of providers to anticipate and address such risks is a strong indicator of security maturity.

| Document forgery and AI-generated fakes

C.17.11 Another critical component of system integrity is the ability to detect fake, forged or AI-generated identity documents. These may be convincingly fabricated and could pass a casual visual inspection by human reviewers in offline settings (e.g. bar staff or security personnel). However, the systems tested demonstrated high levels of resilience against such attacks using:

- Optical security feature detection (e.g. holograms, watermarks).
- AI-trained classifiers to identify document anomalies.
- Metadata validation and tamper detection.
- Database cross-referencing against known templates and document libraries.

C.17.12 Several providers integrated forensic-level document analysis tools and flagged irregularities in real time, improving both automation and reliability in high-risk sectors like gambling, fintech and adult content.

C.17.13 The assessment confirms that modern age verification systems incorporate sophisticated and standards-aligned techniques to protect against biometric spoofing, data injection and document forgery. The use of ISO/IEC 30107-compliant liveness detection, early alignment with ISO/IEC AWI 25456 and strong document integrity measures collectively ensure that systems are not only effective at verifying age, but also resilient to manipulation.

C.17.14 These defences are essential for ensuring trust in digital age assurance ecosystems and must remain central to the ongoing development of secure, privacy-preserving age verification tools.

C.17.15 Sample of providers approach to detection:

Provider	Biometric Binding and Description	Spoofing Detection	Injection Attack Mitigation	Document Forgery Detection
IDMission	Biometric face match, liveness detection, document verification	Yes	Not specified	Yes
Veridas	Deep learning face match, Renewable Biometric References	Yes	Yes	Yes
Yoti	Facial match from document verification with liveness	Yes	Yes	Yes
GBG	Liveness checks (iBeta certified), Vision AI	Yes	Yes	Yes
IDVerse	ISO/IEC 30107-3 certified liveness and spoof resistance	Yes	Not specified	Yes
Veridas	Injection attack mitigation in fraud systems	Yes	Yes	Yes
Trust Stamp	Fraud prevention and audit trails include injection protection	Yes	Yes	Partial
PrivateID	Forensic-level document and metadata analysis		Not specified	Yes

Vendor Case Study



Website

app.verifychain.io

VerifyChain combines ID document checks, selfie face match, liveness detection and fallback facial age estimation. Stores only blockchain transaction logs, no personally identifiable information, privacy-preserving, no reuse of data.

Three Key Facts

1

Uses unlinked tokens for binary age assertions. No PII or persistent data stored.

2

Full transaction log stored on chain, with no personal identity traceability.

3

Needs validation for interoperability and standards conformance.

Strengths

- No persistent storage of biometric or ID data.
- Promotes user sovereignty by separating identity from verification using decentralised architecture.
- Built-in spoofing and injection attack detection, including biometric liveness verification.

Practice Statement

ageassurance.com.au/v/ver/#PS

Privacy Policy

ageassurance.com.au/v/ver/#PP

Technology Trial Test Report

ageassurance.com.au/v/ver/#TR

Technology Trial Interview

ageassurance.com.au/v/ver/#VI

Summary of Results

VerifyChain is a promising, privacy-centric AV platform still maturing in real-world deployment. It demonstrated resilience to spoofing and strong data protection, but its interoperability and user onboarding experience need improvement. It provides strong technical foundations for future growth in regulated or privacy-sensitive digital environments.

C.18 Balancing Investigatory Preparedness with Privacy: Risks of Over-Retention of Data Used for Age Verification

C.18.1 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. However, the sector could benefit from clearer regulatory guidance to ensure that this practice remains the norm and to prevent gradual drift towards persistent data retention or cumulative behavioural tracking. Independent age assurance providers would benefit from explicit frameworks that balance investigatory needs with privacy-preserving design.

C.18.2 During the Trial evaluation, we found evidence of a trend among some age verification providers toward building tools that enable detailed audit trails capable of supporting future investigations by regulators, law enforcement agencies or coroners. These audit mechanisms sometimes involved the retention of original biometric images (e.g. selfies) or copies of identity documents, in secure or encrypted logs.

C.18.3 Although these measures may be motivated by a well-intentioned desire to assist in exceptional cases – such as the death of a minor following access to harmful content – they carry significant privacy and security risks if not carefully limited by legal necessity, clear governance and proportionality principles. The use of tested (ideally independently and therefore certified) age verification systems should be sufficient as a defence, even if the specific case was an error within the expected margin.

| Practice statement analysis:

C.18.4 The Trial evaluated the practice statements for indications of data collection for law enforcement purposes:

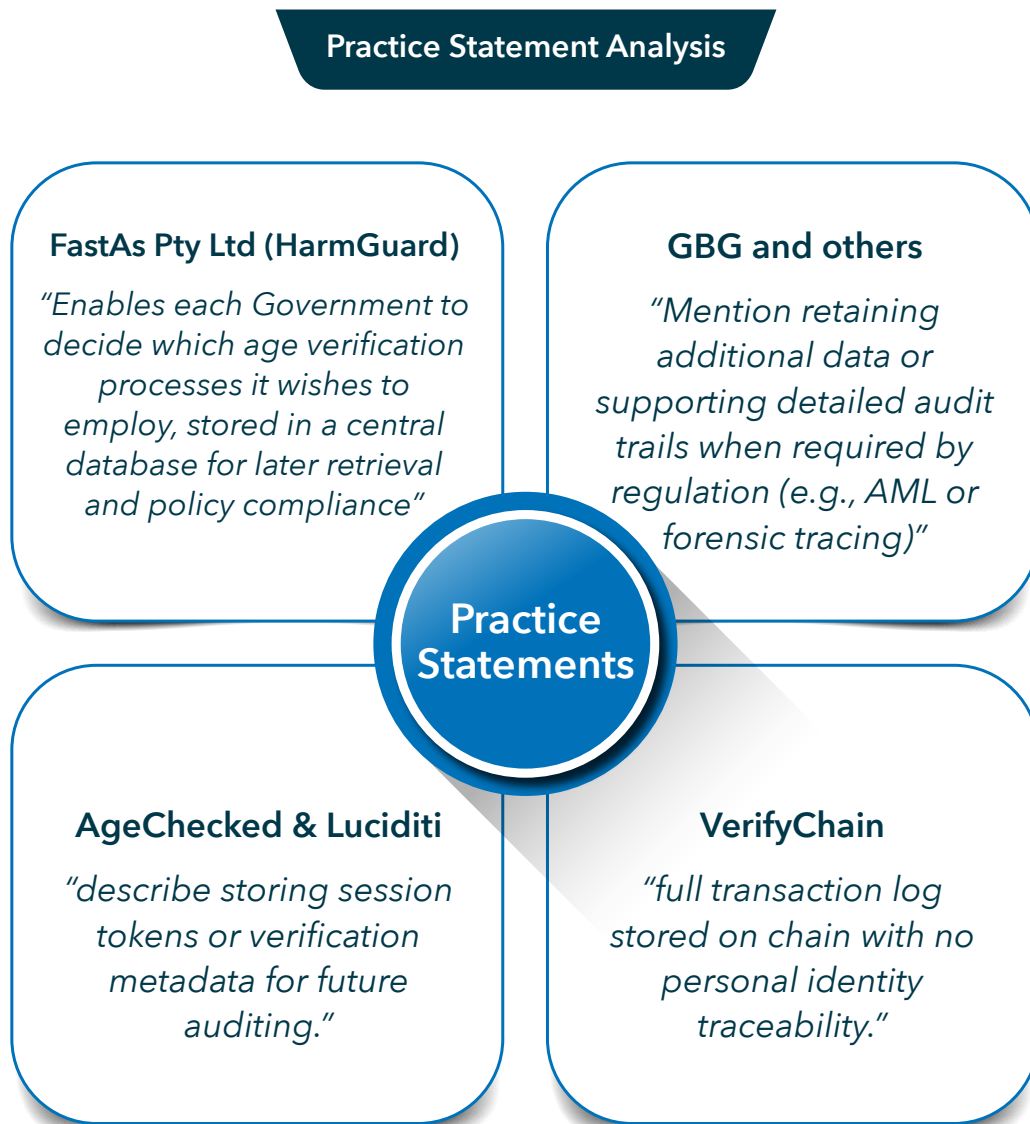


Figure C.18.1 Practice Statement Analysis

C.18.5 While lawful and often configurable, this could conflict with strict data minimisation unless clearly scoped and consented to.

| Core privacy concern

C.18.6 The issue at the heart of this finding is not that audit trails exist per se, but rather that:

- Systems are being configured to retain full, reconstructable identity and biometric data for all users, regardless of risk, regulatory context or outcome.
- This architecture anticipates rare and tragic edge cases – for example, a coroner wanting to verify how a person passed an age check before suicide – but applies a surveillance-level response to the entire user population.

C.18.7 In effect, every user may be subject to indefinite logging “just in case” one case warrants investigatory review. This undermines the principle of data minimisation and creates a persistent, latent risk that secure data stores containing highly sensitive materials (like biometric images) could be compromised, misused or accessed under vague or overly broad investigatory powers.

Lawful Audit Trail vs Over-Retention Risk

Lawful Audit Trail	Over-Retention Risk
Short-term logs	Persistent biometric storage
Anonymised tokens	Full document images
Purpose-limited access	General investigatory access
Regulator access on legal basis	Unbounded retention duration

| Regulatory clarity

C.18.8 This area would benefit from explicit regulatory or statutory guidance clarifying:

- When and how data should be retained for investigatory purposes.
- The lawful conditions under which law enforcement or coronial authorities may request access.
- The technical and governance constraints that should be placed on retention (e.g. encryption, time limits, redaction or unlinkable tokenisation).
- Prohibited practices, such as blanket retention of biometric imagery without consent or necessity.

C.18.9 While investigatory access is important in specific, serious contexts, the generalised retention of sensitive identity and biometric data for all users could be a disproportionate response that creates systemic privacy and security risks. Age verification providers – particularly those operating as independent, trust-marked services – require clear, enforceable frameworks that support exceptional investigatory needs without building surveillance into the fabric of everyday age assurance.

C.18.10 This is not just a technical challenge, but a governance and design imperative, central to ensuring that age verification systems remain safe, proportionate and rights-respecting by default.

9 781068 164620 >