

Age Assurance Technology Trial

PART F Successive Validation

August 2025



Funded by



Australian Government

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

Project by



Findings on Successive Validation

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

1

Successive validation **can be done** in Australia and aligns with emerging international standards.

2

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

3

Successive validation systems demonstrated **internal consistency and standards alignment**, including alignment with ISO/IEC FDIS 27566-1.

4

There is no single configuration to successive validation; flexible models exist and approaches varied by risk context and use case.

5

An evolving and innovative sector is **actively exploring layered age assurance models**; an industry focused on inclusion is maturing.

6

Strong privacy-by-design principles were observed across successive validation stages.

7

Successive validation can **enhance demographic inclusion and reduce bias**, supporting users without formal ID.

8

Configuration and escalation logic would benefit from clearer standardisation and guidance.

9

Cybersecurity practices aligned with best practice and addressed emerging attack surfaces; various defences employed to protect against manipulation.

© 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 978-1-0681646-5-1



Table of contents

Introduction and Overview



F.1	Introduction to Part F: Successive Validation	6
F.2	Executive Summary	8
F.3	Who Participated in the Trial of Successive Validation Technology	13

Context, Standards and Methodology



F.4	What is Successive Validation	16
F.5	Evaluation Approach for Successive Validation Systems	20
F.6	Methodology	25

Detailed Analysis of Successive Validation Findings



F.7	Successive Validation Can Be Done	28
F.8	Technological Feasibility and Strategic Design of Successive Validation	36
F.9	Analysis of Practice Statements and Implementation Models	38
F.10	Successive Validation in Continuous Monitoring Models	43
F.11	Adoption of Successive Validation	48
F.12	Innovation and Delivery Models for Successive Validation	51

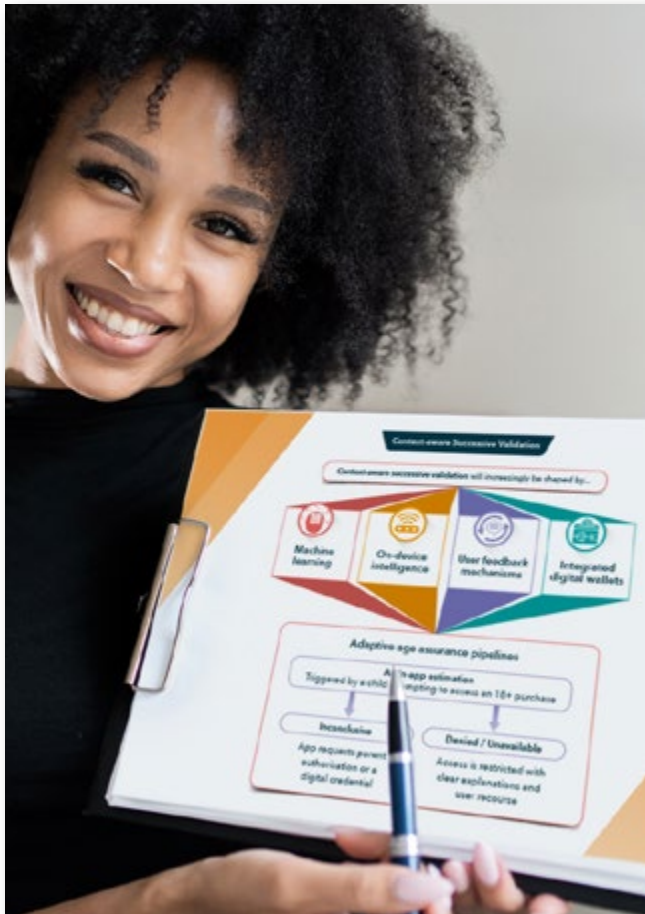
F.13	Privacy, Transparency and Data Handling in Successive Validation Models	54
F.14	Demographic Performance and Inclusion in Successive Validation	61
F.15	Future Potential of Seamless, Embedded Successive Validation	65
F.16	Interoperability and Privacy in Successive Validation	71
F.17	Attack Resilience in Successive Validation: Hill-Climb and Input Manipulation Defences	75
F.18	User Experience and Usability in Successive Validation	81
F.19	The Role of Relying Parties in Configuring Successive Validation	82
F.20	Cross-Border and Jurisdictional Considerations	84
F.21	Machine-Readable Outputs and Interoperable Signalling	86



Age Assurance Technology Trial

PART F Introduction and Overview

I



F.1 Introduction to Part F: Successive Validation

F.1.1 Part F of the Age Assurance Technology Trial focuses on successive validation, the process of combining two or more age assurance methods (such as age inference, age estimation and age verification) to reach a more accurate, risk-appropriate or confidence-boosted age-related decision. Defined in ISO/IEC FDIS 27566-1¹, successive validation supports the principle that age assurance should be proportionate to risk, enabling layered approaches where no single method alone is sufficient or contextually appropriate.

F.1.2 Successive validation plays a critical role in real-world deployments by balancing friction, privacy and assurance levels. For example, a platform may initially infer age based on behavioural signals, escalate to biometric estimation if the result is uncertain and offer verification as a fallback only in edge cases. This model allows services to manage trade-offs dynamically using the lightest effective method wherever possible and only requesting higher-assurance inputs when necessary.

F.1.3 This section of the report evaluates how successive validation has been implemented by Trial participants in the Australian context, examining technical feasibility, data flow, fallback logic, interoperability, privacy handling, demographic consistency and conformance with international standards particularly ISO/IEC FDIS 27566-1, which provides specific guidance on successive validation workflows and IEEE 2089.1², which supports consistency of age-related outputs across methods.

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.

F.1.4 Importantly, the Trial does not make policy recommendations or endorse specific technologies. The Trial’s purpose is to assess whether age assurance technologies, if required by regulation or business need, are technically deployable, effective and privacy-preserving. Whether age-based restrictions should apply and how they are enforced is a matter for policymakers. This report focuses instead on whether technology can support those decisions reliably and proportionately.

F.1.5 Through this part of the report, we present findings on multi-step and fallback age assurance systems, including how they can reduce error rates, improve inclusivity and support practical deployment in diverse operational contexts. This analysis contributes to the emerging evidence base for best practice, certification pathways and risk-responsive age assurance design within Australia’s evolving digital safety and privacy framework.



F.2 Executive Summary

F.2.1 This section of the Trial report examines the feasibility, implementation and implications of successive validation – a layered approach to age assurance in which multiple methods, such as age inference, age estimation and age verification, are applied in sequence to increase confidence in a user’s age. Successive validation enables services to begin with low-friction, privacy-preserving techniques and escalate only when uncertainty remains or the user appears close to a critical threshold. It reflects principles of proportionality and user sensitivity, offering an adaptable model for contexts where no single method alone is sufficient.

F.2.2 Drawing on practice statements, interviews, technical reviews and international standards – particularly ISO/IEC FDIS 27566-1 and IEEE 2089.1 – the Trial evaluated how successive validation has been deployed by technology providers within the Australian context. The assessment found that successive validation is both technically viable and operationally effective. Providers demonstrated considered and standards-aligned designs that escalated users through assurance steps based on risk, confidence levels and policy-defined thresholds. Configurations varied across services and sectors, but all shared a common emphasis on minimising unnecessary friction while ensuring appropriate assurance.

F.2.3 The report identifies emerging use cases, including dynamic validation flows embedded in platform-level monitoring systems. In particular, social media services are beginning to apply continuous assurance logic, using behavioural signals – or contra indicators – to detect discrepancies in declared age and trigger additional validation. This approach mirrors real-world escalation (e.g. a shopkeeper requesting ID when unsure of a customer’s age), but raises new questions around transparency, data minimisation and user control.

F.2.4 Privacy-by-design was a consistent theme across provider systems. Early stages of validation typically relied on anonymised, temporary signals that avoided persistent data collection. As validation progressed, providers demonstrated careful separation between operational, training and evaluation datasets and employed clear logic to limit data exposure to what was strictly necessary for each step. Where more intrusive methods – such as document verification or biometric analysis – were required, these were invoked only when prior stages yielded insufficient confidence.

F.2.5 Security protections were also robust. Systems included defences against spoofing, input manipulation and so-called “hill-climb” attacks. Rate-limiting, session binding and unpredictability in escalation logic helped prevent adversarial circumvention. Providers also addressed cross-method attack surfaces by securing the interfaces between validation steps and ensuring that age assurance outputs could not be tampered with during escalation.

F.2.6 The Trial found no evidence of systemic demographic bias in the configurations examined. Some providers had begun experimenting with culturally grounded assurance signals to address inclusivity, such as contextual cues that may be more accessible to First Nations users or individuals without conventional identity documents. These early efforts suggest that successive validation may offer a more equitable model of age assurance by enabling alternative pathways to demonstrate eligibility.

Opportunities for successive validation

F.2.7 While interoperability across platforms remains in its infancy, a number of providers are exploring how age signals – particularly from inference and estimation – can be made portable, privacy-respecting and policy-aligned. This is a critical next step to enable users to avoid repeating intrusive checks and to allow services to build consistent assurance without persistent profiling.

F.2.8 In summary, successive validation represents a mature and adaptable model of age assurance, well suited to the diverse risk environments encountered in Australia’s digital ecosystem. It allows systems to calibrate their assurance level in response to both contextual risk and user characteristics. When governed transparently and implemented in accordance with privacy and security best practices, successive validation has the potential to support inclusive, proportionate and scalable age assurance across sectors.



Key Statistics from the Trial on Successive Validation

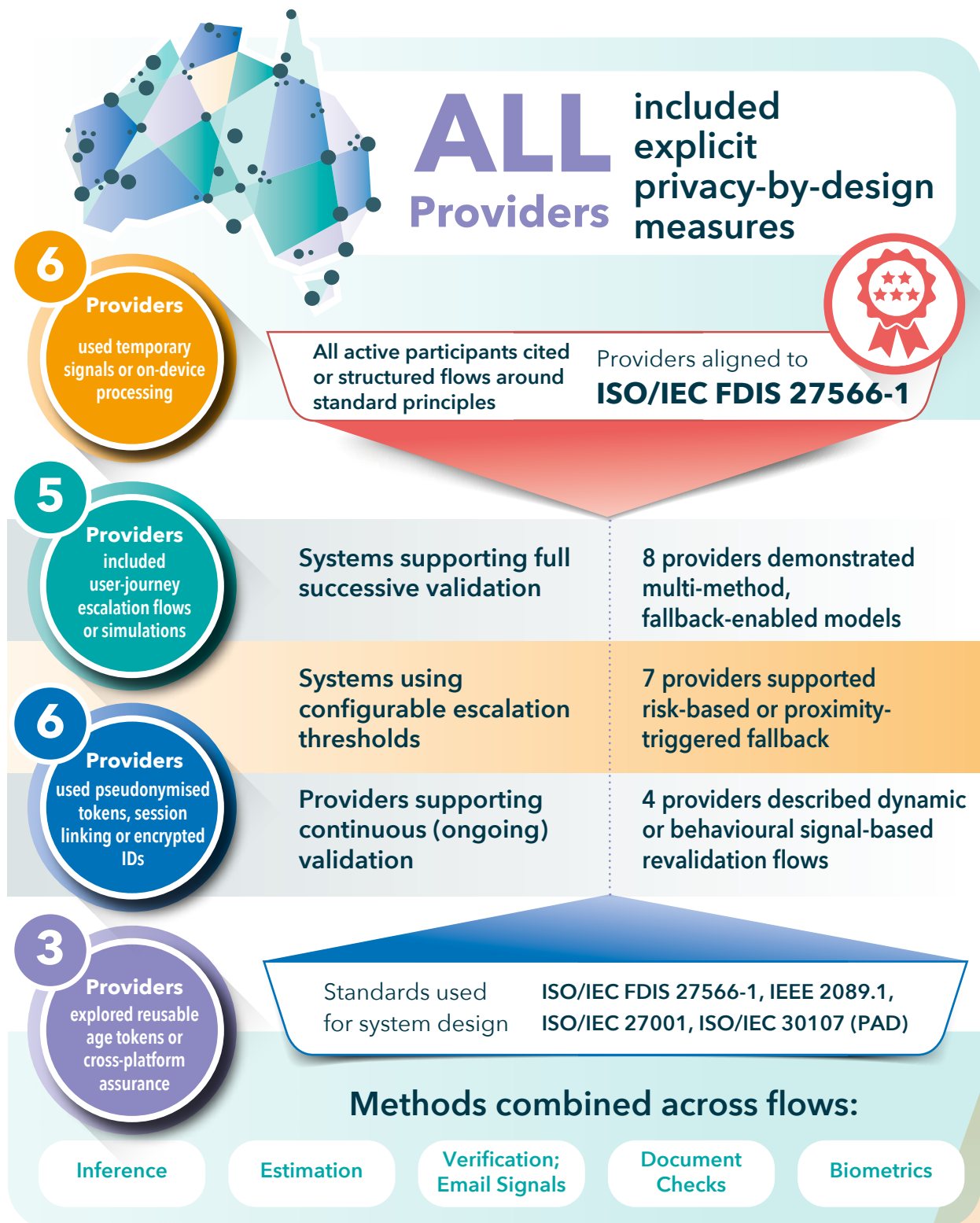


Figure F.2.1 Key Statistics from the Trial on Successive Validation



F.3 Who Participated in the Trial of Successive Validation Technology





Age Assurance Technology Trial



PART F

Context, Standards and Methodology



F.4 What is Successive Validation

F.4.1 Successive validation is a type of age assurance process where multiple independent methods – such as age inference, estimation and verification – are used sequentially to reach a confident age assurance result.

F.4.2 Sometimes referred to as a '**waterfall technique**', this process begins with a low-friction method (e.g. age inference or estimation). If the result is inconclusive – particularly near a threshold age (e.g. 18) – the system escalates to another method. This might involve collecting contextual data for inference or requesting biometric estimation. If uncertainty remains, it may culminate in a full documentary age verification.

F.4.3 It is most commonly triggered when a user appears close to a threshold age – such as someone just over 18 – where higher confidence is needed to confirm eligibility for accessing age-restricted content, products, venues or services. Example flow:

1. Start with age inference from contextual signals (e.g. email age or device settings);
2. If the result is uncertain or near a critical threshold, trigger facial age estimation;
3. If that too is inconclusive, request full age verification (e.g. upload of a government-issued ID).

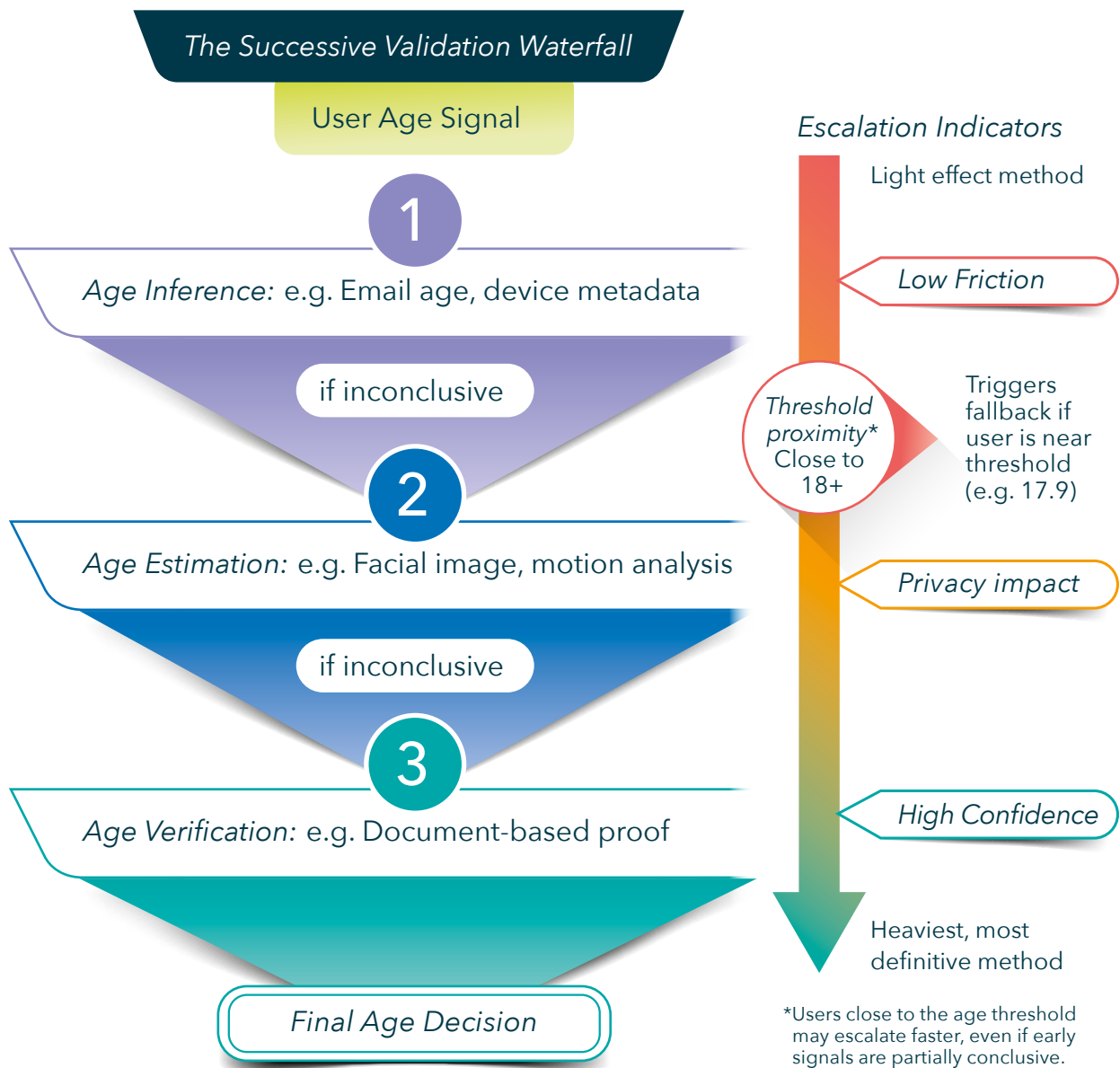


Figure F.4.1 The Successive Validation Waterfall

F.4.4 This approach is governed by risk and proportionality. The closer a user appears to the threshold, the more likely additional steps are required. When well-designed, successive validation:

- Applies the lightest effective method first;
- Escalates only when necessary; and
- Supports data minimisation by avoiding unnecessary collection and retention.

| Successive validation happens in real life: buying alcohol offline vs. online

F.4.5 Successive validation is a well-established practice in offline settings, such as age checks when purchasing alcohol. An initial, low-intrusion assessment is used to make a judgement, with further verification only required if the initial signal is ambiguous.

F.4.6 This principle is equally applicable in digital environments. The following flow diagram (see Figure F.4.2) illustrates how the online successive validation process mirrors the offline process. If the initial result is inconclusive or near the threshold, the system requests additional evidence, such as uploading an ID document. This tiered approach balances privacy, proportionality, and effectiveness.

Vendor Case Study



Website

rightcrowd.com

Starts with facial estimation, escalates to document checks if confidence is low or age is near threshold; supports multi-doc workflows and liveness fallback.

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.

Successive Validation Happens Offline Too

This is successive validation. We already use it offline.
Online age assurance is simply a digital version of the same process.

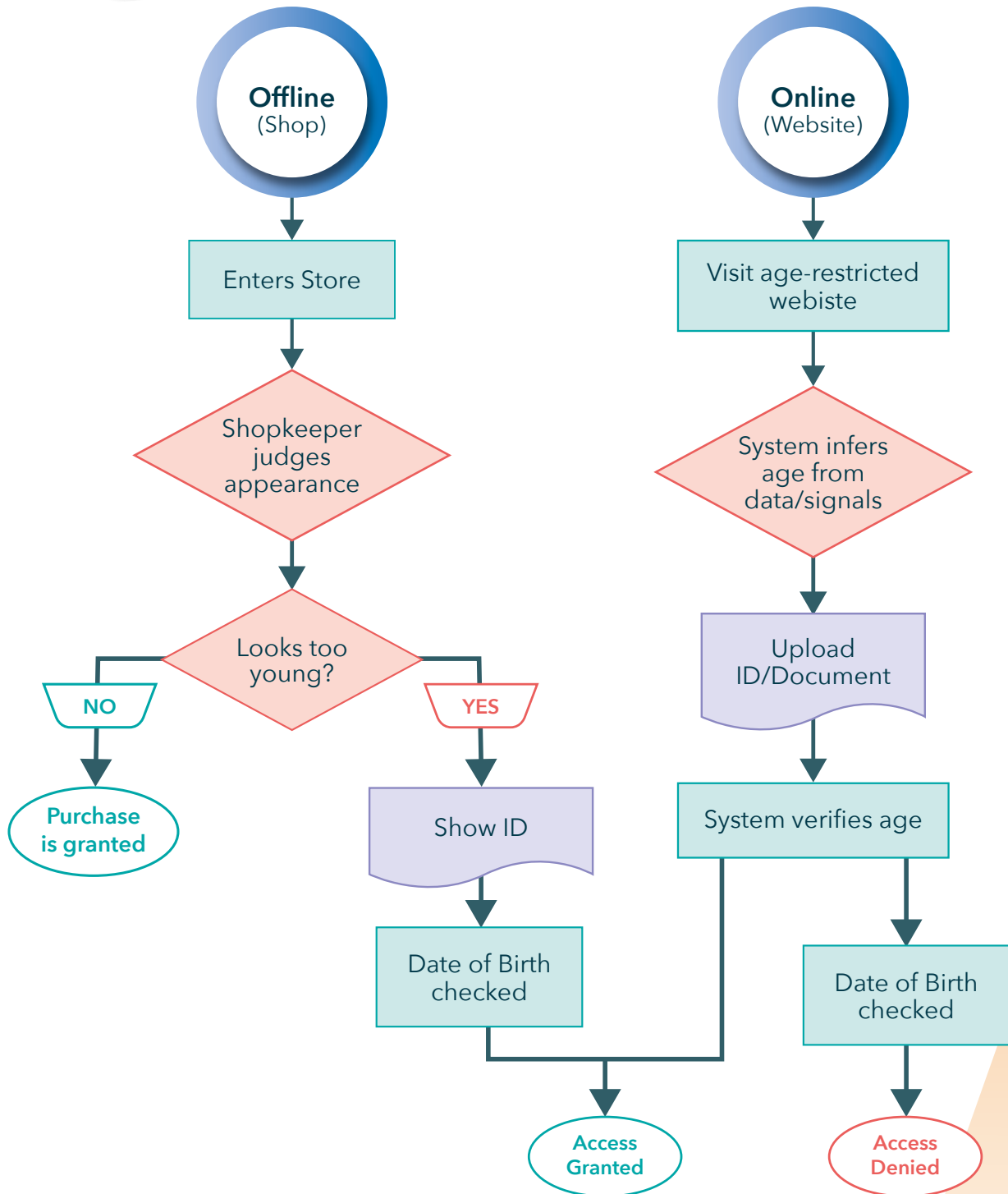


Figure F.4.2 Successive Validation Happens Offline Too

F.5 Evaluation Approach for Successive Validation Systems

F.5.1 The evaluation of successive validation systems in this Trial was primarily a desktop-based, standards-aligned assessment, drawing on documentation, practice statements and provider interviews rather than full-system live testing. This approach reflects the nature of successive validation itself, which is not a single technology, but a composite process that escalates between multiple age assurance methods (e.g. inference, estimation, verification) in response to uncertainty or proximity to age thresholds.

F.5.2 Successive validation was treated as a composite, policy-driven configuration and evaluated based on how well providers described their ability to escalate in a technically sound, proportionate and privacy-preserving way.






F.5.3 Although individual components of age assurance (such as facial estimation or ID document verification) were tested in isolation through earlier parts of the Trial, successive validation as a full chain was not tested operationally in end-to-end deployments.



International standards for successive validation methods

F.5.4 Standards-based assessment framework

The evaluation aligned with internationally recognised standards, including:

International Standards	
 ISO/IEC FDIS 27566-1	Framework for age assurance systems, including layered and fallback techniques.
 IEEE 2089.1	Standard for online age checking, including age signal interoperability.
 ISO/IEC 25010 & 25040	Software quality models and evaluation principles.
 ISO/IEC 29119	Software testing approaches and test documentation.
 ISO/IEC 30107	Biometric presentation attack detection (relevant to escalation to facial estimation and verification stages).



ISO/IEC FDIS 27566-1

F.5.5 ISO/IEC FDIS 27566-1 defines successive validation as a structured approach within age assurance where multiple independent methods such as age inference, age estimation and age verification are applied sequentially or in combination to increase the confidence of an age-related decision. It is used particularly where a single method alone is insufficient to meet a required level of assurance or where risk-based escalation is required.

F.5.6 Successive validation is not a distinct technology but a composite process and the standard outlines key expectations for how layered age assurance workflows should be designed and deployed:

ISO/IEC FDIS 27566-1	Criteria
Risk-appropriate layering	Systems should apply the lightest effective method first (such as inference or estimation) and escalate only when that result is inconclusive, near-threshold or contradicted by other signals. This ensures privacy preservation and proportionality.
Independence of methods	Each method used in the chain should function independently and be capable of delivering its own justified output. This guards against systemic bias and over-reliance on any one type of signal.
Confidence escalation logic	Successive validation must be based on clear, documented logic for escalation. For example, a relying party might specify that estimation confidence below 80% for users appearing between 17-19 years old triggers document verification.

ISO/IEC FDIS 27566-1	Criteria
Privacy-by-design	Systems must limit data collection at each stage and avoid accumulating unnecessary user information. Earlier methods (like inference) should not precondition or bias later methods (like verification).
Selective disclosure	Each validation step should only communicate what is necessary for the decision. For example, an "Over 18" flag should be passed forward, not a full age or raw biometric input from previous steps.
Security and binding	When combining outputs from multiple methods, strong mechanisms (e.g. secure tokens or session binding) must be used to ensure results correspond to the same user throughout the validation chain.
Inclusivity and fallback	The model supports individuals who may lack formal credentials by allowing them to be verified using alternative signals or to start with inference and move only to document-based verification if required.

F.5.7 ISO/IEC FDIS 27566-1 also encourages the use of interoperable and privacy-preserving components, such as verified credentials and digital wallets, within successive validation workflows. This enables users to re-use age-assurance results securely across platforms without repeating intrusive checks.

F.5.8 In essence, successive validation is the practical application of proportionality it mirrors real-world decisions (as seen in offline retail settings) and allows for flexible, confidence-based approaches to age assurance. When implemented according to standards, it offers a balanced and user-centric way to manage age-related access across diverse digital environments.



ISO/IEC 25010

F.5.9 From these standards, a tailored evaluation framework was applied to assess whether successive validation configurations (as described by providers) addressed key quality dimensions:

ISO/IEC 25010	Criteria
Effectiveness of escalation logic	Is the flow from one method to the next clearly defined and risk-responsive?
Accuracy and confidence layering	How are low-confidence results handled between steps?
Interoperability	Can methods be integrated across systems or vendors securely?
Friction minimisation	Are users only escalated when necessary?
Privacy and data minimisation	Is data collection limited and well-separated at each stage?
Bias minimisation	Are fallback paths inclusive and demographically consistent?
Security	Are validation chains protected from manipulation or spoofing?
Transparency and configuration	Can relying parties tailor fallback triggers appropriately?

F.6 Methodology

F.6.1 The assessment combined multiple non-live evidence sources:

- **Practice Statement Analysis** - Examined how providers described escalation pathways, fallback triggers and confidence logic.
- **Simulated User Journeys** - Reviewed illustrative flows showing how a user might escalate through a layered model under different risk contexts.
- **Technology Readiness Levels (TRLs)** - Assigned to the implementation maturity of successive validation logic (both individual components and chains).
- **Threshold Sensitivity Review** - Focused on how systems are configured to respond to users near critical age thresholds (e.g. 13, 16, 18), where fallback is most often required.

Limitations and scope

F.6.2 The evaluation was evidence-based but not operational in nature. The following activities were not conducted for successive validation as a complete chain:

- No live workflow testing of layered validation in production or field environments.
- No performance stress testing at scale.
- No penetration testing or cryptographic audit beyond reviewing circumvention resilience in standalone methods.
- No testing of cross-platform identity binding or re-use of age signals across different relying parties (noted as an emerging area with limited current deployment).



Age Assurance Technology Trial



PART F

Detailed Analysis of Successive Validation Findings



F.7 Successive Validation Can Be Done

| Summary finding

F.7.1 Successive validation can be effectively designed and applied within the Australian context. The Trial found that layered age assurance models – combining low-friction inference or estimation with fallback to higher-assurance verification – can be proportionate, privacy-conscious and adaptable to different risk environments.

F.7.2 This approach offers inclusion opportunities for young people near age thresholds, particularly where formal credentials may be lacking. However, the potential for scope creep, over-collection and cumulative privacy impacts increases as users are escalated through multiple steps – especially when fallback becomes the norm rather than the exception.







| What successive validation is and is not

F.7.3 Successive validation is a method of age assurance that involves using two or more independent techniques in sequence to reach a confident age-related decision. It is described in ISO/IEC FDIS 27566-1 as a layered or “fallback” approach, often used when a single method such as age inference, estimation or verification does not yield a sufficiently confident or risk-appropriate result on its own.

F.7.4 At its core, successive validation is:

Successive validation is...

-  **A risk-responsive model:** The method used escalates in line with the likelihood of harm or the proximity of the user to a critical age threshold (e.g. 18).
-  **A privacy-preserving strategy:** It begins with the least intrusive method, such as inference from contextual signals and only proceeds to more intrusive steps, like document verification, if earlier results are inconclusive.
-  **A real-world mirror:** It reflects how age checks are already conducted in physical environments such as a shopkeeper visually assessing a customer and requesting ID only when necessary.
-  **A flexible deployment framework:** It allows relying parties to tailor assurance flows according to sector needs, regulatory requirements and the technical maturity of the methods used.

F.7.5 Successive validation is not a single technology or necessarily a standalone product. Instead, it is a workflow or strategy that combines existing age assurance methods age inference, age estimation and age verification within a single decision framework.

F.7.6 It is also:

Successive validation is NOT...

- ✗ **Not an all-in-one solution:** It relies on each component (inference, estimation, verification) being independently reliable, secure and properly implemented.
- ✗ **Not a duplication of effort:** Effective successive validation avoids redundant checks by only escalating, when necessary, based on clearly defined triggers or thresholds.
- ✗ **Not always linear:** While often represented as a “waterfall” from low- to high-assurance methods, some implementations may use parallel signals or allow re-entry to earlier steps under certain conditions.
- ✗ **Not inherently high-friction:** When well-designed, most users complete the process at the first or second step reserving higher-friction steps for edge cases or high-risk scenarios.
- ✗ **Not a licence for data accumulation:** Escalation must still respect data minimisation and proportionality principles. Using more than one method does not justify retaining or aggregating all inputs unless strictly necessary and clearly disclosed.

F.7.7 Successive validation is a design principle, not necessarily a product. It recognises that no single method works perfectly for all users, in all contexts, at all times. Instead, it provides a structured way to combine methods based on risk, user experience and system confidence delivering flexibility without compromising standards. When implemented correctly, successive validation supports inclusion, fairness and trust in digital age-restricted environments.

F.7.8 Key requirements relevant to successive validation include:

ISO/IEC FDIS 27566-1	Criteria
Risk-based layering	Systems should apply the least intrusive method first (e.g. age inference or estimation) and escalate to stronger methods (e.g. document-based verification) only when justified by uncertainty or proximity to a threshold age.
Independence and modularity	Each component method in a successive validation flow must be independently capable of producing a compliant output, avoiding dependency loops.
Data minimisation and separation	Data collected at one stage must not automatically be shared or retained into later stages unless necessary and justified.
Proportionality and user transparency	Escalation must be explainable to users and decisions based on confidence thresholds should be auditable and fair.
Inclusivity	The model should support diverse user populations, including those without formal ID, by allowing inference or estimation to succeed before requiring verification.

F.7.9 ISO/IEC FDIS 27566-1 positions successive validation as a flexible and inclusive model for age assurance capable of accommodating uncertainty, diverse user contexts and escalating regulatory requirements while enforcing strict privacy and data governance boundaries at each step.

Vendor Case Study*Website*luciditi.co.uk

Begins with facial estimation and passive liveness; escalates to document-based verification or re-usable digital identity where estimation is inconclusive or fails liveness.

Practice Statementageassurance.com.au/v/luc/#PS*Technology Trial Test Report*ageassurance.com.au/v/luc/#TR*Privacy Policy*ageassurance.com.au/v/luc/#PP*Technology Trial Interview*ageassurance.com.au/v/luc/#VI**Summary of Results**

Luciditi platform supports inference, estimation and verification. Claims of interoperability and real-world integration; however, specific details of age inference deployment were limited to interview insights rather than practice statement-level granularity.

| Supporting inclusion

F.7.10 A key advantage of successive validation is its potential to support inclusion, particularly for:

- Young people near legal thresholds who may lack formal ID.
- Users from communities with limited access to credentials, including some First Nations individuals or recent migrants; and
- Minors seeking access to age-appropriate services, who may otherwise face exclusion due to the absence of a single definitive age indicator.

F.7.11 By enabling users to demonstrate eligibility through multiple pathways, successive validation supports fairer, more accessible digital environments.

| Risks and limitations

F.7.12 However, successive validation is not without trade-offs. As users move through multiple layers, there is an increased risk of cumulative data collection, especially when:

- Outputs from early stages are stored unnecessarily
- Systems are not designed with clear data minimisation logic
- Relying parties use fallback stages as default rather than exception



F.7.13 This creates a risk of scope creep, where data collected for one purpose (e.g. age estimation) is retained or reused in ways that exceed the original consent or need, particularly for users close to the age threshold who are more likely to be escalated.

F.7.14 To mitigate these concerns, the Trial observed that leading providers employed:

- One-time signals, destroyed after use.
- Clear separation of signals across layers.
- Escalation rules based on configurable thresholds, rather than automated profiling; and
- Robust adherence to privacy-by-design principles outlined in ISO/IEC FDIS 27566-1, including:

ISO/IEC FDIS 27566-1	
Clause 6.4	Data minimisation
Clause 6.5	Context-aware assurance
Clause 7.1	Separation of duties across functional layers.



Provider	Mitigation Strategy	Evidence from Practice Statement
Relevant ISO/IEC FDIS 27566-1 - Clause 6.4 - Data minimisation		
		"All processing occurs on-device... no PII or images are transmitted or stored."
	Robust adherence to privacy-by-design principles	"Only essential data collected. Face maps and IP addresses deleted post-check."
	One-time signals, destroyed after use	"Facial image is temporarily processed... immediately deleted after age estimation."
Relevant ISO/IEC FDIS 27566-1 - Clause 6.5 - Context-aware assurance		
		"Assurance level is configured by the relying party based on legal or risk context."
		"Step-up to ID verification triggered only when configured thresholds are met."
	Escalation rules based on configurable thresholds	"Escalation occurs when the estimated age is within a policy-defined buffer zone near thresholds."
Relevant ISO/IEC FDIS 27566-1 - Clause 7.1 - Separation of duties		
	Clear separation of signals across layers	"No PII is stored between steps... pseudonymous session tokens are used for binding."
		"Separate workflows for document checks, facial estimation and email-based signals... signals do not contaminate one another."
		"Inference, estimation and verification modules are functionally separated; no data reused across layers."

F.8 Technological Feasibility and Strategic Design of Successive Validation

F.8.1 Approaches to successive validation, as a combination of other approaches, do not face substantial technological limitations to implementation in Australia.

F.8.2 Service providers and policymakers demonstrated thoughtful planning in combining multiple methods to meet age related eligibility requirements. Each step in the validation sequence – particularly near age thresholds – balances privacy, data security and effectiveness and tended to deploy the least privacy intrusive method first.

F.8.3 Successive validation, as a combination of age inference, estimation and verification methods, does not face any substantial technological limitations to implementation in Australia. On the contrary, the Trial found that these approaches represent a technically mature and operationally flexible solution for contexts where a single method is insufficient to reach a confident age-related decision.

F.8.4 Successive validation is already supported by the infrastructure and technologies commonly used in digital service environments, including:

- Biometric estimation tools
- Transactional inference engines using contextual data
- Verified document-based age checks
- Secure API integration layers for cross-system communication

F.8.5 All components assessed during the Trial were found to be readily deployable and interoperable, with providers demonstrating strong alignment with international standards (particularly ISO/IEC FDIS 27566-1 and IEEE 2089.1) regarding escalation logic, data handling and decision transparency.

| Strategic design and deployment

F.8.6 The Trial observed that service providers and policymakers had given careful and informed consideration to how successive validation could be implemented in ways that are effective, proportionate and ethically sound. Key findings included:

Successive validation implementation:

Privacy-first sequencing	Most implementations began with low-friction, privacy-preserving methods such as age inference or facial estimation. Escalation to more intrusive methods – like document verification – occurred only when early results were inconclusive or when users appeared close to a critical threshold (e.g. ages 17–19 in an 18+ system).
Confidence-based escalation	Escalation decisions were typically guided by confidence scores or policy-defined buffer zones. For example, many systems declined to rely solely on estimation when predicted ages fell within ± 2 years of a threshold. This ensured predictable and accountable fallback logic.
Balance of risk and user experience	Deployments were tailored to context: non-financial services (e.g. streaming) prioritised user experience, using inference and estimation as primary methods. In contrast, more regulated industries escalated quickly to full verification to meet compliance or licensing needs.
System modularity	Providers designed their validation chains with modular, plug-and-play architecture – enabling integration with third-party inference tools or verification APIs without compromising security, data minimisation or interoperability.

F.9 Analysis of Practice Statements and Implementation Models

F.9.1 The Trial primarily reviewed practice statements from independent third-party age assurance providers, who offer modular services capable of being integrated into relying parties' platforms. These systems were typically designed to deliver transactional successive validation, where users progress through age inference, estimation and verification at a defined moment of access (e.g. entering an age-restricted website, purchasing alcohol online).

























F.9.2 Some providers also described how their systems could be configured to support ongoing or dynamic revalidation – for example, by triggering reassessment based on behavioural anomalies, time intervals or data updates. These features may support more continuous assurance models, although this was not a distinct focus of the Trial.

F.9.3 Across the statements received, common patterns included:

- Privacy-first sequencing: Beginning with the least intrusive method and escalating only when necessary
- Confidence-based fallback: Using thresholds, policy buffers and scoring to determine escalation
- Modular architecture: Allowing for API-based orchestration between inference, estimation and verification tools
- Audit and control mechanisms: Some providers described internal logging or controls for how and when fallback is triggered

F.9.4 These patterns align with successive validation principles described in ISO/IEC FDIS 27566-1, including layered design, context-aware assurance and escalation proportional to risk.

F.9.5 Successive validation provider comparison:

Provider	Supports Transactional Successive Validation	Indicates Capability for Ongoing/ Dynamic Validation	Notes
			Starts with data inference, escalates to doc checks; transactional model.
			Supports multiple data inputs; mentions behavioural monitoring.
			Inference to document flow; transactional only.
			Confidence scoring, modular fallback; includes dynamic reassessment triggers.
			On-device estimation; no dynamic or continuous claims.
			Facial estimation with fallback to docs; no ongoing validation described.
			Email/facial inference, threshold-based escalation; notes ongoing signal use.
			Modular system with facial estimation, reusable ID; ongoing re-check described.

| Transparency and public trust

F.9.6 One of the most important findings from the Trial was the clarity and transparency with which providers described their successive validation processes. When layered systems include:

- Clear escalation triggers (e.g. buffer zones near threshold ages),
- Limited and purpose-specific data retention and
- Explicit fallback protocols and how they foster greater public trust in how age is determined.

F.9.7 This transparency is especially important for:

- Youth users near threshold ages, who are most likely to be escalated.
- Parents and guardians, who expect clear policies about how a child's age is validated.
- Regulators, who require assurance on proportionality, necessity and privacy compliance.

F.9.8 Practice statements demonstrated that successive validation is no longer an abstract policy idea, but a practical, evolving model. Whether deployed at the point of access or embedded into user workflows, systems showed layered capability, strong privacy architecture and standards-aligned design. These choices support more inclusive, flexible and proportionate age assurance, particularly in high-sensitivity sectors.



Website

withpersona.com

Persona orchestrates flows using selfie-based estimation first, escalating to document or NFC verification only when age proximity or quality issues trigger risk-based fallback.

Practice Statement

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

Technology Trial Test Report

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

Privacy Policy

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

Technology Trial Interview

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

Summary of Results

Supports user opt-out and clear user interface, strong performance with First Nations youth in school trials, demographic audit trails supported. MAE ranged from 0.86 to 3.31 across different cohorts; strong at 13+ thresholds. Accuracy varied more widely for under-13 users.



Note on platform-based successive validation

F.9.9 While no social media platforms submitted practice statements to this Trial, it is known from public sources that platforms may use successive validation dynamically – monitoring user behaviour for contra-indicators of declared age. If signals suggest inconsistency (e.g. language, connections, payment patterns), users may be prompted to reconfirm their age or escalate to verification.

F.9.10 This continuous validation model, though effective for policy enforcement, presents elevated privacy risks, such as:

- Over-collection from unrelated behaviours
- Persistent profiling
- Scope creep into areas not directly related to age assurance

F.9.11 Balancing this approach requires clear governance, strict data minimisation and transparency about how and when age re-validation is triggered.

F.10 Successive Validation in Continuous Monitoring Models

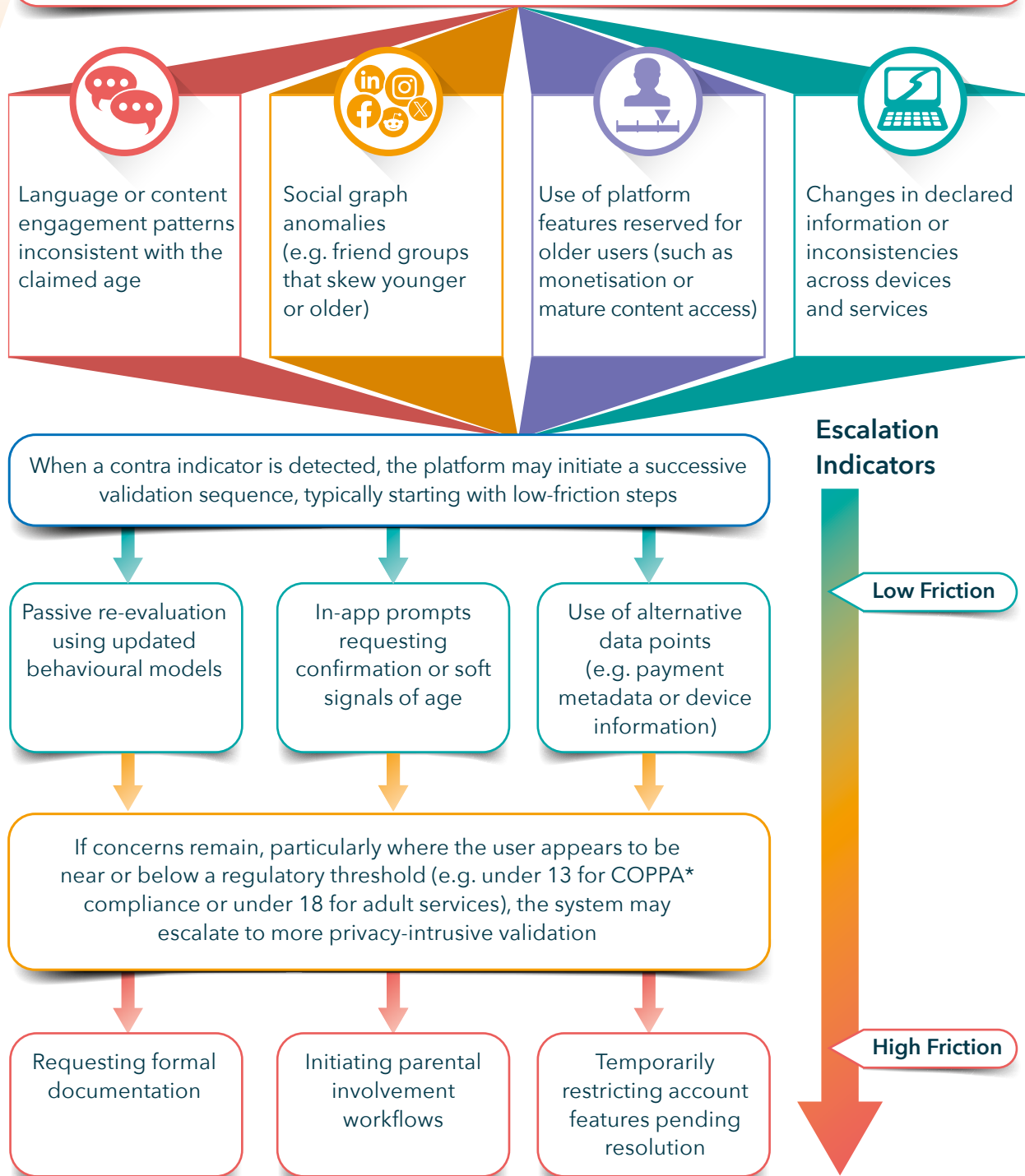
F.10.1 During the Trial, a distinct model of successive validation emerged among large online platforms, particularly social media companies, which rely on ongoing behavioural monitoring rather than discrete point-of-access age checks. These systems use continuous age assurance processes to enforce compliance with age-related policies even long after a user's initial account creation or self-declaration of age.

F.10.2 This layered validation process aligns with the principles of ISO/IEC FDIS 27566-1, which allows for context-specific escalation based on emerging risk, while mandating privacy-preserving and proportionate handling of user data.



Successive Validation in Continuous Monitoring Models

Contra indicators signals behaviours that may conflict with the user's previously declared age



* The Children's Online Privacy Protection Act, or COPPA, is a law that was passed by the United States Congress in 1998 with the aim of protecting the privacy and personally identifying information of children under the age of 13 who use online services.

Figure F.10.1 Successive Validation in Continuous Monitoring Models

| Distant-from-risk validation

F.10.3 While this model is effective for platform-wide policy enforcement, it carries inherent privacy risks due to its distance from the original point of age-related harm. Continuous monitoring across the platform may:

- Result in collateral intrusion capturing behavioural signals unrelated to age-based concerns
- Lead to over-collection or unnecessary aggregation of user data
- Introduce scope creep, where data collected for age assurance is later repurposed
- Erode user trust if escalation pathways and data use policies are not clearly communicated

F.10.4 This contrasts with risk-proximate successive validation, where age assurance is performed at the point of access to age-restricted content, services or purchases thus containing both the purpose and scope of data collection.

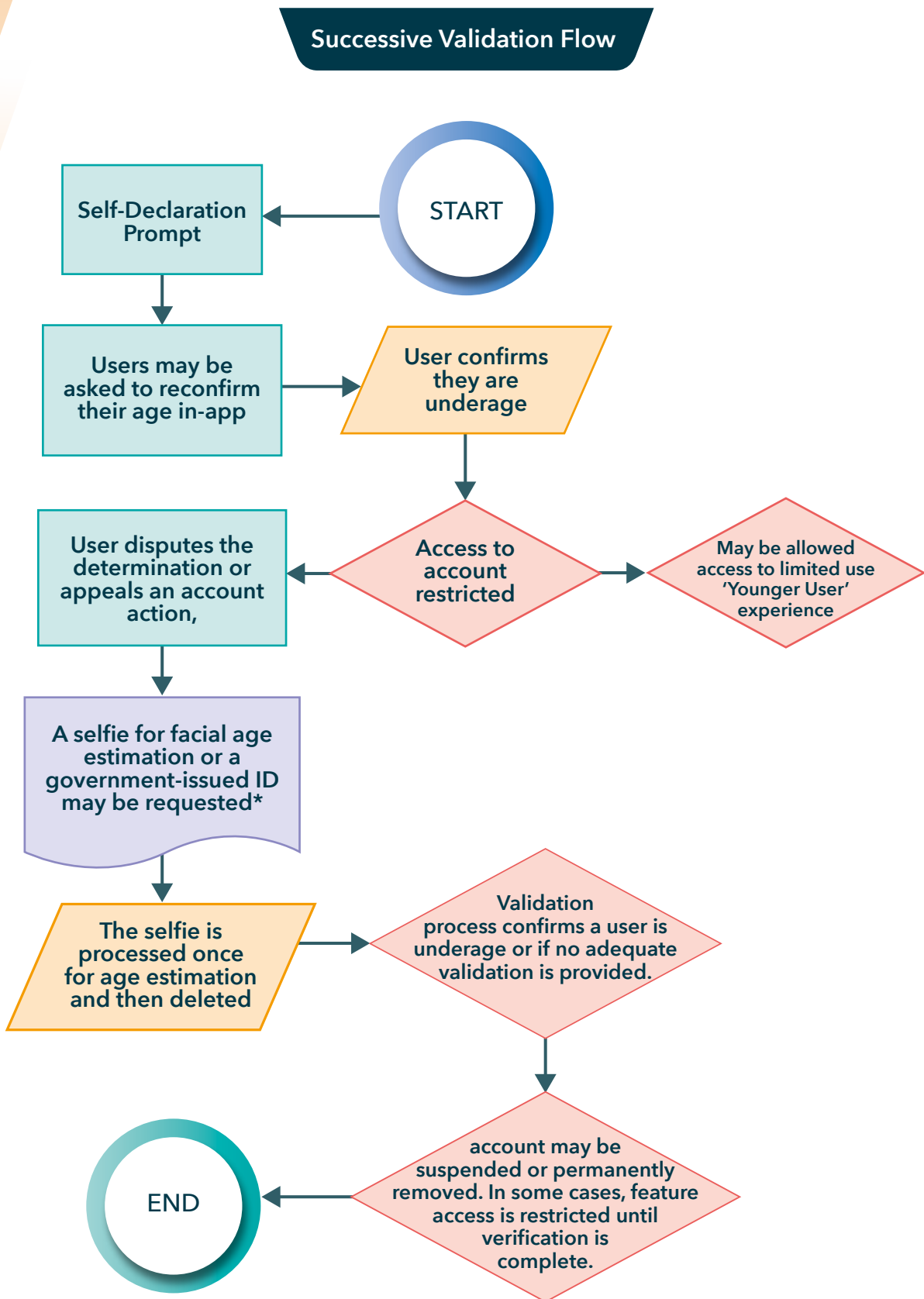


Figure F.10.2 Successive Validation Flow

| Balancing safety and privacy

F.10.5 To address these risks, platforms deploying continuous successive validation must implement:

- Clear governance frameworks to limit data use to age assurance purposes
- Transparent escalation criteria, so users understand when and why their age may be re-evaluated
- Minimisation and separation of data used for inference from broader profiling systems
- Granular auditability to ensure that successive validation is applied fairly and consistently

F.10.6 Although not formally evaluated in the Trial, continuous successive validation is an emerging norm in large platforms' compliance ecosystems. When aligned with the proportionality, data minimisation and transparency principles of ISO/IEC FDIS 27566-1, it can support robust, ethical age assurance – particularly for child safety.

F.11 Adoption of Successive Validation

F.11.1 We found limited use of successive validation, with many Trial participants providing single-type or single-flow age assurance methods. However, the small number of multi-type or multi-flow providers had a good range of available techniques and implemented data minimised successive in-flow data collection to avoid repetition and to prompt through a user journey the data needed as they flow from one age assurance method to another.

F.11.2 This type of service is very context specific, and we did not identify one provider that offered a fully comprehensive approach incorporating all potential options, but there are certainly providers with an extensive range of options available.

F.11.3 The Trial's analysis revealed that, while successive validation is a conceptually mature and standards-aligned approach, its practical implementation across Trial participants remains limited. The majority of providers participating in the Trial offered single-type or single-flow age assurance systems, typically focused on a specific method such as age estimation, inference or document-based verification used independently of others.

F.11.4 This single-method focus reflects the sector-specific origins of many systems. For example:

Method	Deployment
Age Estimation Tools	Frequently deployed in content platforms and gaming environments.
Age Verification Services	More common in finance, e-commerce and regulated sectors.
Age Inference Tools	Often embedded in existing user account workflows or CRM ³ platforms.

3. CRM platforms refers to Customer Relationship Management platforms.

| Multi-flow systems and successive pathways

F.11.5 A smaller subset of participating providers did implement multi-method, in-flow age assurance systems capable of performing successive validation by escalating from one method to another within a user journey. These systems showed promising characteristics, including:

- Contextual method switching, where a system automatically escalates from age inference to estimation or verification depending on confidence scores or threshold proximity
- User journey-based orchestration, with just-in-time data collection, meaning that additional personal data is only requested if required for the next stage of validation
- Minimised repetition, avoiding duplicate requests for the same input (e.g., no need to upload ID again if already presented earlier in the flow)

F.11.6 However, no provider in the Trial presented a comprehensive, plug-and-play system covering all possible age assurance methods. The multi-method offerings tended to be modular or customisable, with a strong dependence on:

- The sector and use case in which the service is deployed
- The privacy expectations and user demographic
- The commercial model and integration capacity of the relying party

F.11.7 Some providers, particularly those offering age assurance as a platform or orchestration service, had made significant progress in integrating multiple capabilities, such as age estimation followed by document verification or inference followed by parent/guardian escalation, but these were not yet universally deployed across all relying parties or contexts.

F.11.8 The Trial confirms that successive validation is technically feasible and partially in use across participating services, particularly among providers with a focus on orchestration, privacy preservation and dynamic risk-based workflows. However, wider adoption and standardisation of successive validation pathways is needed to unlock the full benefits of layered, context-aware age assurance. This may include:

- Template-driven integration models to support relying parties with limited development capacity
- Standards-based fallback logic, aligned to ISO/IEC FDIS 27566-1 and IEEE 2089.1
- Clearer pathways for certification or benchmarking of multi-method, data-minimising flows

F.11.9 As age assurance policy frameworks mature, the availability and integration of modular, extensible and user-centric successive validation models will be essential for delivering proportionate, inclusive and effective outcomes across sectors.

F.12 Innovation and Delivery Models for Successive Validation

F.12.1 Successive validation is supported by an innovative and responsive sector, but one that is split between the orchestration of multiple providers through a hub or portal and those that are building successive tools in a single workflow for users to graduate through.

F.12.2 We identified strong demand from relying parties to build and integrate successive validation workflows, combining inference, user-declared data and, when needed, documentary evidence. The pipeline of innovation suggests this layered model will continue to improve and diversify.

F.12.3 The Trial found that successive validation is supported by a dynamic and responsive age assurance sector, actively developing new methods and integration strategies to meet the needs of service providers and regulators. However, this sector is currently divided into two primary implementation models:

1. **Hub-Orchestration Providers** – These services act as integrators or platforms that coordinate multiple, often independent, age assurance methods via APIs or plug-in components. In these cases, the successive validation process is managed centrally, but the individual methods (e.g. age estimation, inference, verification) may come from different providers or modules.
2. **Single-Provider Workflows** – These systems offer a vertically integrated solution, where a user is guided through a predefined flow within a single provider's ecosystem. The process typically begins with low-friction methods (e.g. inference or estimation) and escalates, if necessary, to higher-assurance techniques like document verification without leaving the provider's environment.

| Market demand for layered assurance

F.12.4 During the evaluation, the Trial observed strong and growing interest from relying parties in building and integrating layered age assurance workflows. Relying parties particularly in sectors such as social platforms, online retail and content access expressed clear preference for solutions that:

- Start with privacy-preserving, low-friction methods, such as age inference from metadata
- Prompt users for progressively more definitive data only if initial methods yield uncertain or inconclusive results
- Allow for fallback to documentary evidence, including digital credentials or identity verification, where age-related eligibility decisions require high confidence

F.12.5 This demand reflects the recognition that no single method suits all users or contexts and that successful deployment depends on adaptive and proportional models that account for:

- The nature of the age-restricted service
- The proximity of the user to the threshold age
- The sensitivity of the data involved

| Pipeline of innovation

F.12.6 The sector's innovation pipeline suggests successive validation workflows will continue to evolve and diversify, with key areas of growth including:

- Smarter orchestration engines, capable of selecting the optimal method based on user context, confidence thresholds or consent preferences
- Privacy-preserving linkages between signals, enabling data to be reused across layers without redundancy
- Interoperability with digital wallets and holder services, enabling previously validated results to be reused across services and devices
- Configurable risk templates for relying parties, helping them to define escalation logic appropriate to their compliance obligations and risk appetite

F.12.7 These trends indicate a maturing ecosystem, where successive validation is becoming not only feasible, but also increasingly attractive as a user-centric, compliant and scalable approach to age assurance.

F.12.8 The Trial confirms that successive validation is not only technically viable but also driven by clear market demand and a strong innovation trajectory. The dual track of orchestration hubs and all-in-one workflow providers ensures flexibility of implementation, while also encouraging competition and continuous improvement. As age assurance policies evolve, this layered approach backed by responsive industry capabilities will be central to delivering effective and inclusive age-related access controls in both regulated and commercial contexts.

F.13 Privacy, Transparency and Data Handling in Successive Validation Models

F.13.1 Within social media platforms, successive validation is often embedded directly into internal systems continuously analysing user behaviour and metadata to infer age and detect contra indicators. When inconsistencies arise, the platform escalates validation steps – ranging from prompts for self-declaration to requests for supporting evidence – all within a seamless user experience. This integrated approach enables real-time decision-making but also raises challenges around transparency, data minimisation and the potential for overreach. As platforms refine these models, balancing effectiveness with user privacy and proportionality will be critical to sustaining trust and regulatory alignment.

F.13.2 We found robust understanding of and internal policy decisions regarding the handling of personal information within successive validation approaches to age assurance – particularly where early stages rely on signals from an individual’s digital footprint, such as behavioural patterns, service usage or contextual indicators. Providers demonstrated clear separation between operational use, training and validation datasets, ensuring that privacy safeguards were maintained throughout the layered process.

F.13.3 Initial inference stages were typically low intrusion, with signals anonymised, securely processed and not retained in a form that could re-identify individuals. Most providers stored only non-identifying transaction codes and some had begun developing privacy-preserving techniques based solely on indirect indicators like browsing habits or interaction sequences.

F.13.4 As successive validation escalates – moving from inference to user-declared information and, if necessary, documentary evidence – privacy considerations remain central. Independent providers showed strong design practices that minimise unnecessary data exposure until higher-assurance steps are warranted. This layered approach allows relying parties to align privacy impact with the level of risk, reflecting a mature and user-focused commitment to proportionate age assurance.

Social media platforms

F.13.5 Although social media platforms did not formally participate in this part of the Trial, publicly available information suggests that they are adopting a continuous validation model, in which:

- Age inference is embedded into internal monitoring systems.
- Contra indicators (e.g. language use, content engagement, social graph patterns) are used to reassess age.
- Users may be escalated through successive steps - from soft prompts to document verification - if inconsistencies are detected.

F.13.6 While this integrated model enables real-time enforcement, it raises heightened concerns around:

- Scope creep.
- Over-collection of behavioural data.
- And opacity of escalation criteria.

F.13.7 These risks highlight the importance of governance, transparency and data separation in continuous successive validation.

Vendor Case Study



Website

privateid.com

PrivateID performs real-time, on-device facial estimation with step-up to ID scan and selfie match where user is near threshold or liveness/confidence requirements are unmet.

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.

| Real-time escalation within platform workflows

F.13.8 When contra indicators are detected, platforms typically escalate validation steps in a seamless, real-time user journey. This may involve:

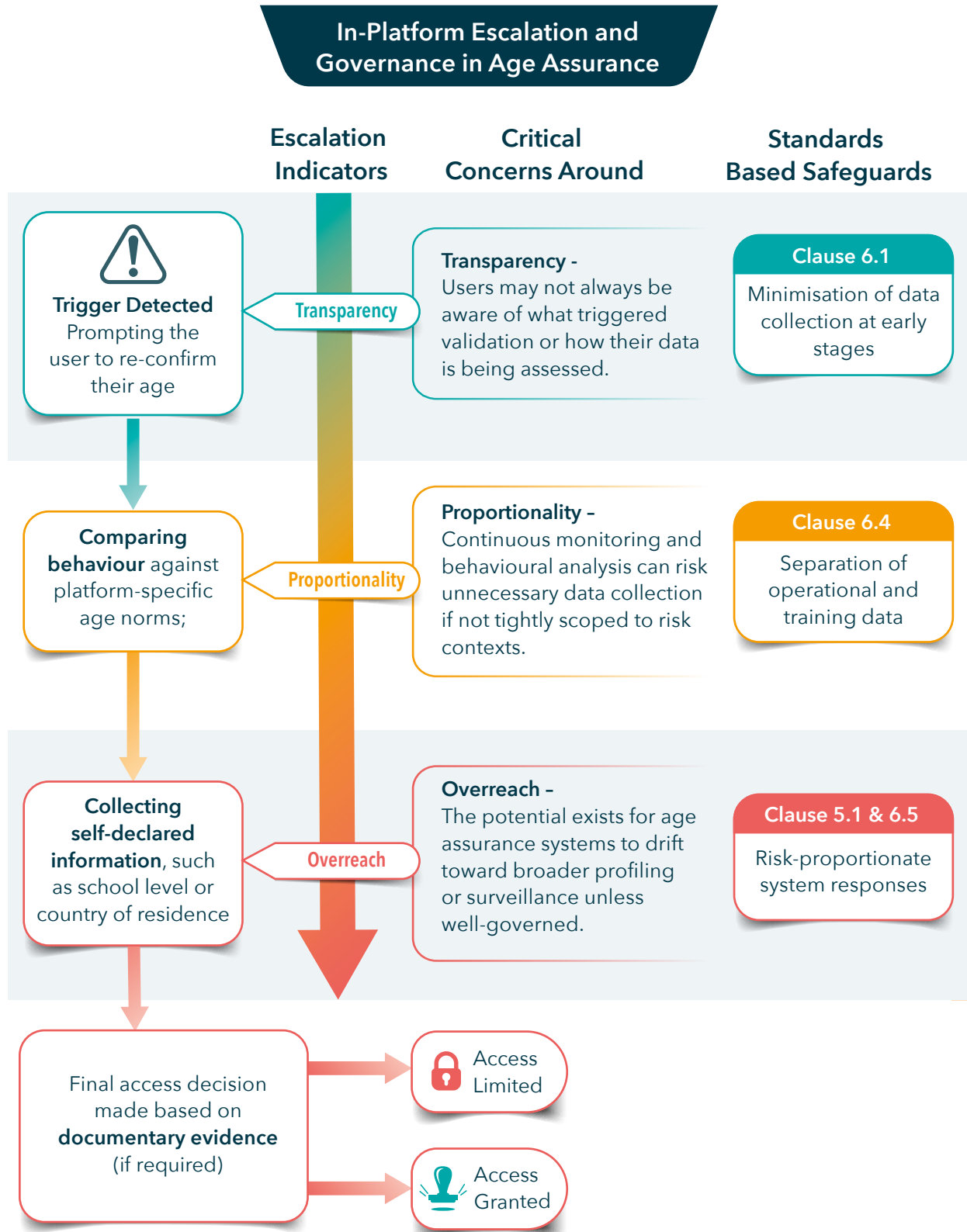


Figure F.13.1 In-Platform Escalation and Governance in Age Assurance

| Independent provider practices and layered privacy safeguards

F.13.9 Among third-party providers participating in the Trial, we observed strong privacy-aware design principles throughout the successive validation process:

- Early-stage inference methods relied on anonymised and context-specific signals, processed locally or temporarily and not retained in ways that could re-identify individuals
- Most providers retained only non-identifying transaction codes (e.g. hashed tokens or session identifiers) as audit or compliance artefacts
- A few services are actively developing privacy-preserving models based solely on indirect indicators such as browser behaviour, interface interactions or device metadata eliminating the need for biometric or identity-based data in early steps

F.13.10 As validation escalated e.g., from inference to user declarations or verified documents access to more sensitive information was triggered only, when necessary, with design practices aimed at:

- Reducing friction for compliant users
- Preserving user anonymity until higher assurance was required
- Enabling data reuse only within the same session or purpose

F.13.11 This layered approach supports the principle of graduated data exposure, enabling relying parties to meet their risk and compliance obligations without defaulting to high-intrusion methods. It aligns with the privacy engineering guidance outlined in IEEE 2089.1, particularly with respect to:

- Limiting unnecessary personal data transfer
- Enabling user control and consent at each validation layer
- Supporting auditability and justification for each escalation step

F.13.12 Successive validation offers a practical and privacy-conscious way to align the level of data exposure with the level of age-related risk, especially in environments like social platforms where user behaviour may evolve over time. The Trial found that when designed carefully, whether within continuous monitoring models or third-party orchestration tools, successive validation can uphold robust data protection while improving age assurance outcomes. Future improvements should continue to focus on:

- Clear user messaging and justification for validation escalation
- Greater transparency in risk models and trigger mechanisms
- Consistent standards alignment for training, storage and audit processes across all layers of the validation pathway.



Vendor Case Study

Website

agechecked.com

AgeChecked implements a modular, standards-aligned model of successive validation that escalates validation based on context, risk and client preference. Their approach is characterised by low-friction entry points (e.g. age inference or user-declared data), escalating only when confidence is insufficient.

Three Key Facts

1

Uses a privacy-first sequence: inference document check facial biometrics, each validation layer is separated to avoid data overreach.

2

Just-in-time data collection ensures that additional personal data is only collected when the system escalates.

3

Clients can customise thresholds, allowing the model to adapt across sectors such as online retail and gaming.

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 exemplifies modular orchestration, offering reusable APIs while ensuring data minimisation and session-bound signal use. Their emphasis on contextual escalation reflects ISO/IEC FDIS 27566-1 Clause 6.5 and supports flexible integration by relying parties.

F.14 Demographic Performance and Inclusion in Successive Validation

F.14.1 Successive validation offers important inclusion advantages by allowing users to progress through a series of methods – such as inference, self-declaration and verification – rather than relying on a single form of identity. This approach can help mitigate the exclusion of individuals who lack formal credentials or digital histories, including young people, rural users or those from underrepresented communities.

| Potential for demographic fairness

F.14.2 While the Trial did not conduct formal demographic performance testing across full successive validation chains, participating providers emphasised:

- The ability to fallback to alternative methods when one step produced uncertain or inconclusive results.
- The use of low-intrusion, context-aware signals at early stages.
- The importance of proportionality and configurability to support diverse user needs.

F.14.3 These features allow successive validation to act as a failsafe mechanism – if one method is less reliable for a particular demographic group, another can confirm or override it. This aligns with fairness expectations in IEEE 2089.1, which supports graduated assurance and demographic resilience.

| Supporting inclusion without formal credentials

F.14.4 Successive validation pathways are particularly well-suited to contexts where users may not hold formal ID. For example:

1. Start with contextual inference (e.g. device metadata, interaction patterns).
2. Progress to user-declared data (e.g. school level, location, parent/guardian relationship).
3. Escalate to document verification only if needed.

F.14.5 This model supports inclusion by avoiding early disqualification, while still enabling compliant decisions. It aligns with ISO/IEC FDIS 27566-1 Clause 6.4, which calls for:

- Avoidance of unnecessary exclusion.
- Use of fallback mechanisms.
- Proportionality in data handling.

| Culturally responsive design (emerging opportunity)

F.14.6 While not implemented in current systems reviewed in the Trial, there is emerging potential for culturally grounded age inference techniques, particularly in Indigenous contexts. For example:

- Community-aligned applications could use structured knowledge (e.g. local flora/fauna, tribal customs or heritage practices) to estimate age bands.
- These responses, combined with contextual signals, might support early-stage validation in remote areas where formal documentation is limited.

F.14.7 Such approaches would require community co-design, ethical safeguards and robust testing, but represent a promising path toward more respectful and inclusive digital safety systems.

F.14.8 Successive validation supports a more equitable model of age assurance by:

- Offering layered methods that reduce dependency on any one technique.
- Avoiding early exclusion of users without ID.
- Supporting context-aware design across diverse communities.

F.14.9 To enhance this further, future work should explore:

- Transparent user messaging and escalation justification.
- Consistent standards for fairness and audit across all layers.
- Further research into culturally relevant and demographically inclusive inference methods.

F.14.10 An additional consideration is whether the logic that determines escalation (e.g. buffer zones, confidence thresholds) performs equally across demographic groups.

F.14.11 While most providers emphasised low-bias performance in age estimation and verification components, fewer reported testing whether:

- Some groups are more likely to be escalated (e.g. certain ethnicities, device types, language users).
- Fallback rules are tuned equally across user cohorts.
- Validation success rates differ depending on socio-economic or geographic factors.

F.14.12 Successive validation offers resilience – by allowing alternative methods if one fails – but systematic over-escalation for specific groups may still occur if thresholds are not fairly calibrated.

F.14.13 Some providers indicated plans to monitor escalation rates by demographic marker (where legally permissible), while others noted the use of statistical parity checks during model training. These efforts align with fairness guidance in IEEE 2089.1 and evolving AI governance frameworks.





F.15 Future Potential of Seamless, Embedded Successive Validation

F.15.1 The Trial's assessment of age assurance technologies identified significant future potential for successive validation to evolve into seamless, context-aware workflows, embedded directly within the digital experiences of users. This trend reflects a broader industry shift towards "ambient" age assurance a model where validation occurs fluidly within the user journey, rather than as a disruptive or standalone checkpoint.

F.15.2 Looking ahead, we see considerable potential for successive validation to evolve into seamless, context-aware workflows embedded within everyday digital experiences, such as apps, games or online purchases - making age assurance both more effective and less intrusive over time.

F.15.3 Emerging prototypes and early-stage deployments observed during the Trial suggest that successive validation can be integrated into:



Figure F.15.1 *Successive Validation Integration Points*

F.15.4 Rather than front-loading friction or requiring users to submit high-assurance documentation upfront, successive validation enables progressive escalation only when a higher level of assurance is needed. This aligns with the principle of risk-proportionate design set out in ISO/IEC FDIS 27566-1 (Clause 5.1) and supports:

- Minimal disruption to the user experience
- Proportional data collection based on the nature of the content or service
- Real-time decision-making at the point of risk, rather than across the whole platform

Vendor Case Study



Website

verifymy.io

Verifymy delivers a privacy-aware escalation path combining document matching, facial age estimation and contextual inference. Escalation occurs when the confidence score falls within a defined “grey zone” around regulatory thresholds.

Three Key Facts

1

Adopts IEEE 2089.1 principles on minimal disclosure and traceable fallback.

2

Triggers facial estimation only if uncertainty exists.

3

Initiates with passive signals like email tenure or metadata.

Strengths

- Begins with email or facial age estimation.
- Escalates only if confidence falls within a policy-defined buffer.
- All fallback logic is threshold-based, with immediate deletion of sensitive inputs (e.g. face maps, IP addresses).

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's well-defined buffer zones and audit trails represent best practice for policy-aligned fallback handling and escalation transparency, ensuring that decision-making is justifiable and minimised in terms of user friction.

| Context-aware and adaptive escalation

F.15.5 Context-aware successive validation will increasingly be shaped by:

- Machine learning models that assess risk dynamically based on interaction patterns or user behaviour.
- On-device intelligence that performs local inference before escalating to server-side verification.
- User feedback mechanisms to fine-tune thresholds for validation escalation.
- Integrated digital wallets that store previously validated age signals, reducing redundancy.

F.15.6 These innovations will help build adaptive age assurance pipelines, where:

- A child attempting to access an 18+ purchase triggers an in-app estimation.
- If inconclusive, the app requests parent authorisation or a digital credential.
- If denied or unavailable, access is respectfully restricted with clear explanations and user recourse.

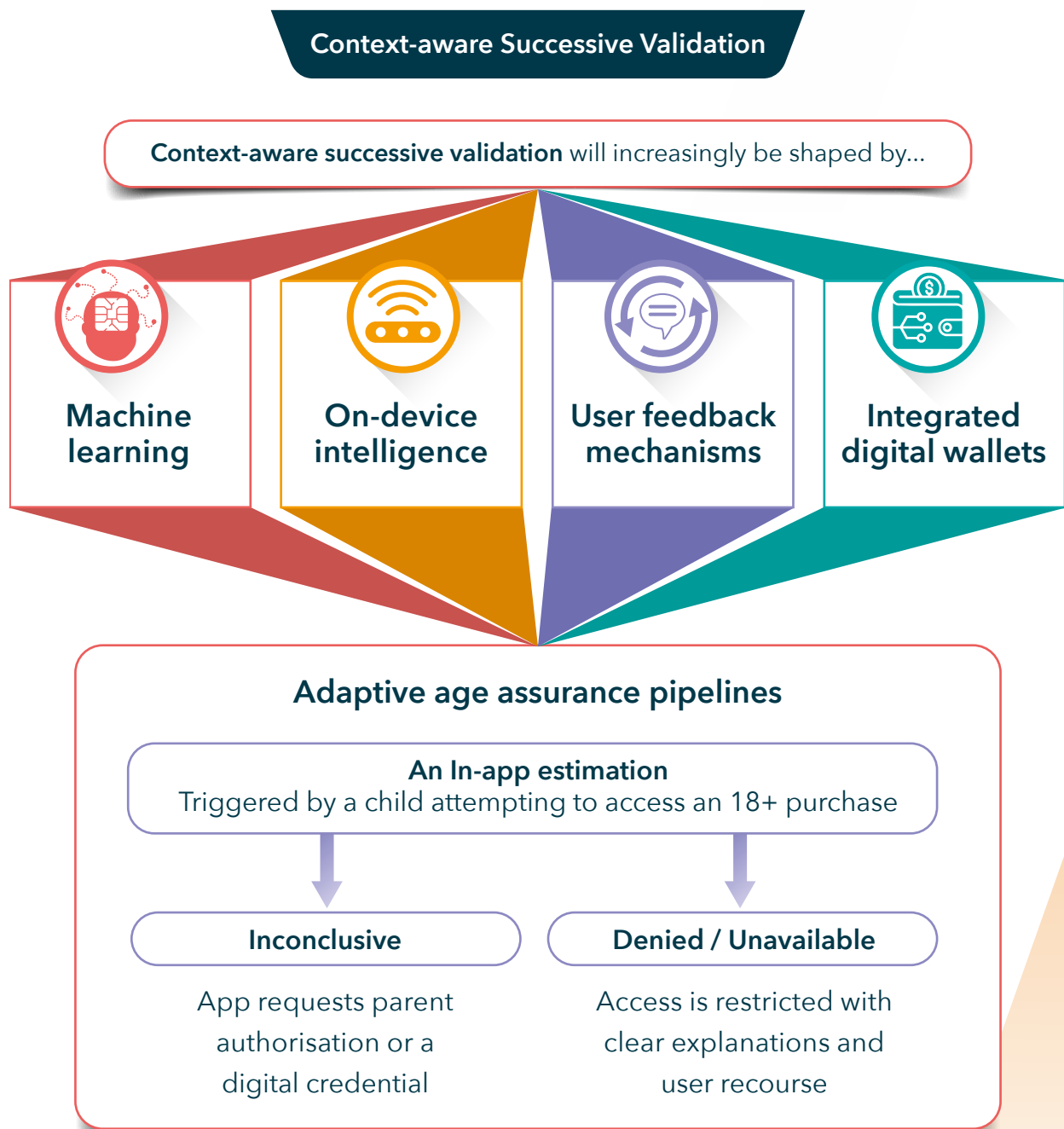


Figure F.15.2 Context-aware Successive Validation

| Minimising intrusion while maximising confidence

F.15.7 When designed correctly, successive validation offers a model for “privacy-first” assurance: rather than assuming maximum data collection is necessary, it embraces graduated data disclosure based on what is needed, when and why.

F.15.8 Such approaches are particularly well-suited to:

- Low-to-medium risk contexts, where a binary “Yes/No” response may suffice
- User populations with limited access to identity documents
- Digital services wishing to preserve user trust while fulfilling compliance obligations

F.15.9 Looking forward, the Trial anticipates that successive validation will move beyond standalone solutions and become a foundational capability within digital environments, offering:

- Flexibility for service providers to tailor assurance to their context
- Increased inclusivity for users, particularly young people and those without ID
- Reduced friction and stronger privacy protections, all without sacrificing regulatory compliance

F.15.10 As digital services grow more sophisticated, successive validation stands as a practical and responsible model for embedding age assurance into the everyday digital fabric quietly effective, contextually appropriate and aligned with emerging standards and user expectations.

F.16 Interoperability and Privacy in Successive Validation

F.16.1 To support effective successive validation, interoperability must be balanced with privacy-by-design principles. Systems should enable single-use or context-limited credentials, ensuring that age signals remain proportionate, relevant and non-transferable across unrelated use cases. As technology matures, clearer standards and governance will be essential to unlock the benefits of stack-integrated signals while safeguarding individual rights.

F.16.2 As successive validation methods evolve, the ability to interoperate across platforms, services and devices is becoming increasingly important especially for users navigating multiple digital environments that require proof of age. However, the interoperability of age assurance signals must be carefully balanced with privacy-by-design principles, to avoid overreach, scope creep or unintended surveillance.

F.16.3 In practice, interoperability enables convenience such as carrying an age assurance signal from one service to another (e.g. from a verified platform into a game or digital wallet). But if not tightly scoped, shared age signals could be misused or repurposed in ways that exceed their original purpose.

F.16.4 To mitigate this, successive validation systems should:

- Generate single-use or context-bound credentials
- Ensure data minimisation, only signalling age when necessary (e.g. "Over 18: Yes/No")
- Avoid persistent identifiers that could be linked across services
- Implement expiry and revocation mechanisms for age tokens

F.16.5 These principles are reinforced by ISO/IEC FDIS 27566-1, which encourages:

Clause	Safeguard Focus
Clause 6.1	Selective disclosure of age attributes
Clause 5.1-6.5	Contextual appropriateness and proportionality
Clause 6.3.2	Avoidance of cumulative digital footprint

F.16.6 For instance, a signal stating that a user is “likely over 18” for accessing an online forum should not automatically be re-used for advertising eligibility, gambling access or financial profiling without explicit consent and purpose limitation.

| Governance and the role of standards

F.16.7 As successive validation matures and stack-integrated models gain adoption where signals flow between age estimation tools, parental control layers, inference systems and digital wallets standards and certification mechanisms will be critical. These will help define:

- What constitutes a trustworthy age signal.
- How signals can be scoped and trusted without becoming transferable identifiers.
- What limits apply to downstream use, especially where sensitive inferences are made.

F.16.8 This work is already supported by:

- IEEE 2089.1, which sets baseline interoperability and disclosure practices.
- Ongoing developments in trust frameworks for digital identity ecosystems.
- Privacy-preserving cryptographic techniques, such as zero-knowledge proofs or verifiable credentials, which allow users to demonstrate eligibility without revealing sensitive data.

F.16.9 To support effective, scalable and responsible successive validation, interoperability must be built with privacy as a foundation, not an afterthought. This means:

- Embedding granular control over signal use.
- Enabling user awareness and revocability.
- Aligning technical implementation with strong governance and audit frameworks.



By doing so, Australia can develop trustworthy, standards-compliant age assurance infrastructure that supports innovation while preserving individual rights in both public and commercial digital contexts.

Vendor Case Study



Website

yoti.com

Yoti offers one of the most expansive successive validation suites, with twelve independent validation methods including facial estimation, digital credentials, document checks and ID reuse via digital wallets.

Three Key Facts

1

Flow from selfie based estimation to any other form of verification based around a document.

2

Offers embedded SDKs and APIs for sector specific integration.

3

Provides end-user visibility and control, aligned with data minimisation practices.

Strengths

- Clear documentation and transparency in logic
- Fully operational SDKs and browser-based integrations
- High relevance for low-friction, privacy-focused age gates

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's user-controlled Digital ID reuse feature exemplifies future-forward successive validation, enabling scalable, privacy-preserving portability across services while reducing redundant data collection.

F.17 Attack Resilience in Successive Validation: Hill-Climb and Input Manipulation Defences

F.17.1 The Trial found that successive validation systems demonstrated strong alignment with established security standards, including ISO/IEC 27001:2022 and, in some cases, SOC 2⁴ or Fintech-grade security protocols. Providers also presented evidence of structured penetration testing and secure systems engineering.

F.17.2 This section focuses on validation-specific threat models – particularly those that target the layered nature of successive validation systems, such as hill-climb attacks and input manipulation.

| Hill-climb attacks

F.17.3 A hill-climb attack involves a user systematically adjusting their inputs to incrementally increase their chances of validation success. By observing system responses – such as when a borderline result advances to the next stage – an attacker can iteratively “tune” their behaviour or data to move toward a successful outcome.

F.17.4 Examples include:

- Repeatedly modifying declared age or device/browser settings
- Adjusting behaviour to mimic threshold-passing users
- Cycling through identity documents to probe system tolerances

4. SOC 2 stands for System and Organization Controls 2. SOC 2 is a security framework that specifies how organisations should protect customer data from unauthorized access, security incidents and other vulnerabilities.

F.17.5 Providers have deployed multiple defences, including:

- Rate limiting to restrict repeated attempts
- Randomised workflows to reduce pattern predictability
- Feedback suppression, obscuring why a step failed
- Risk scoring and anomaly detection to flag unusual user flows

F.17.6 These measures obfuscate system thresholds, making it difficult to reverse-engineer escalation logic or optimise attacks.

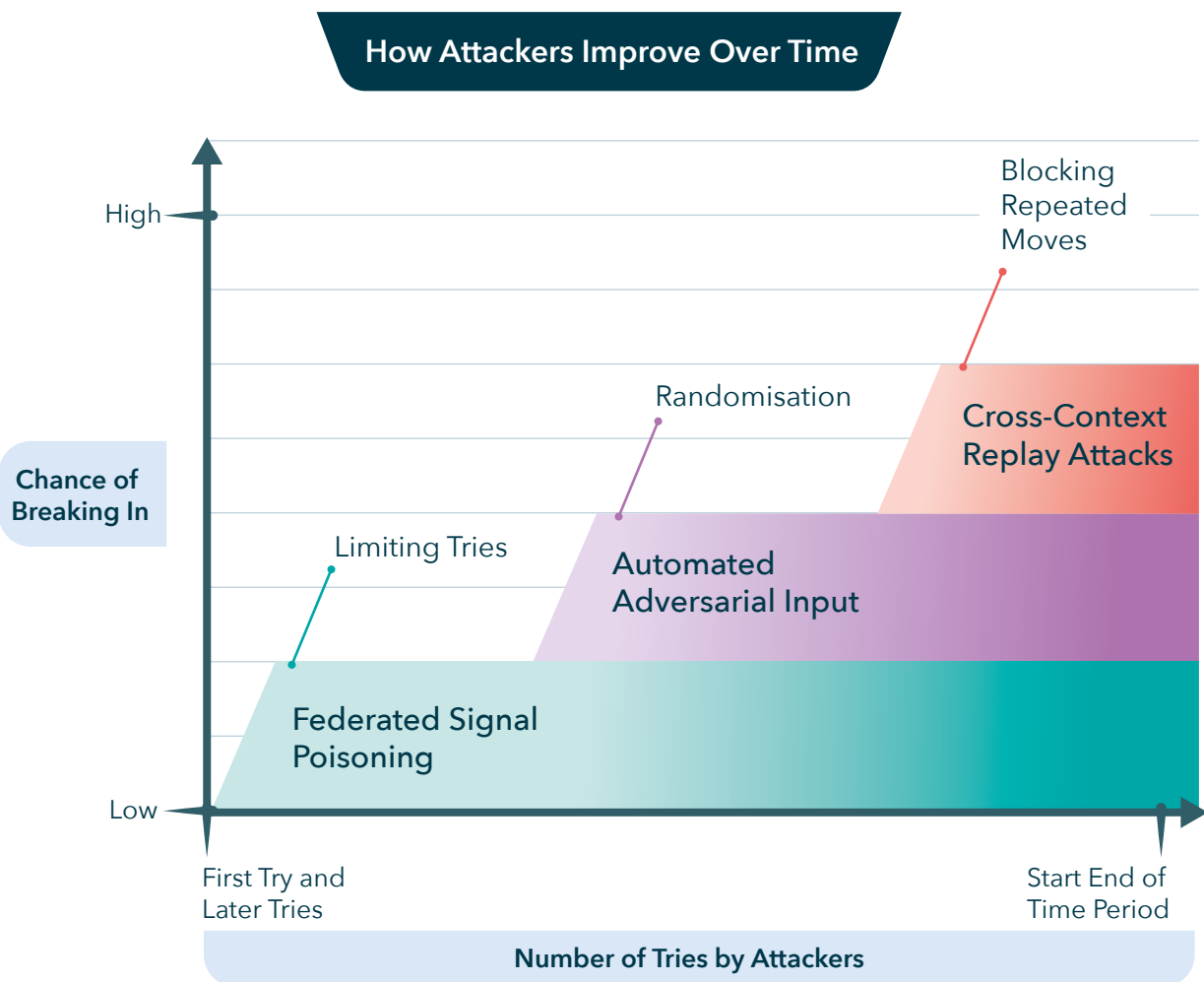


Figure F.17.1 How Attackers Improve Over Time

| Input manipulation and data injection attacks

F.17.7 Another class of threat involves the deliberate creation of false or misleading digital signals, crafted to mimic the behaviours of older or eligible users. Potential tactics include:

- Automated scripts that simulate “typical adult” browsing behaviour
- Injection of device or metadata artefacts associated with verified users
- Use of AI-generated interaction sequences or bot-driven activity profiles

F.17.8 While not commonly observed at scale, these attacks are technically feasible. Providers reported:

- Early-stage defences, such as anomaly detection and statistical baselining
- Input validation constraints, limiting acceptable inference data types
- Environmental separation between inference and verification layers to prevent signal reuse



Figure F.17.2 False Digital Footprint Attack Lifecycle

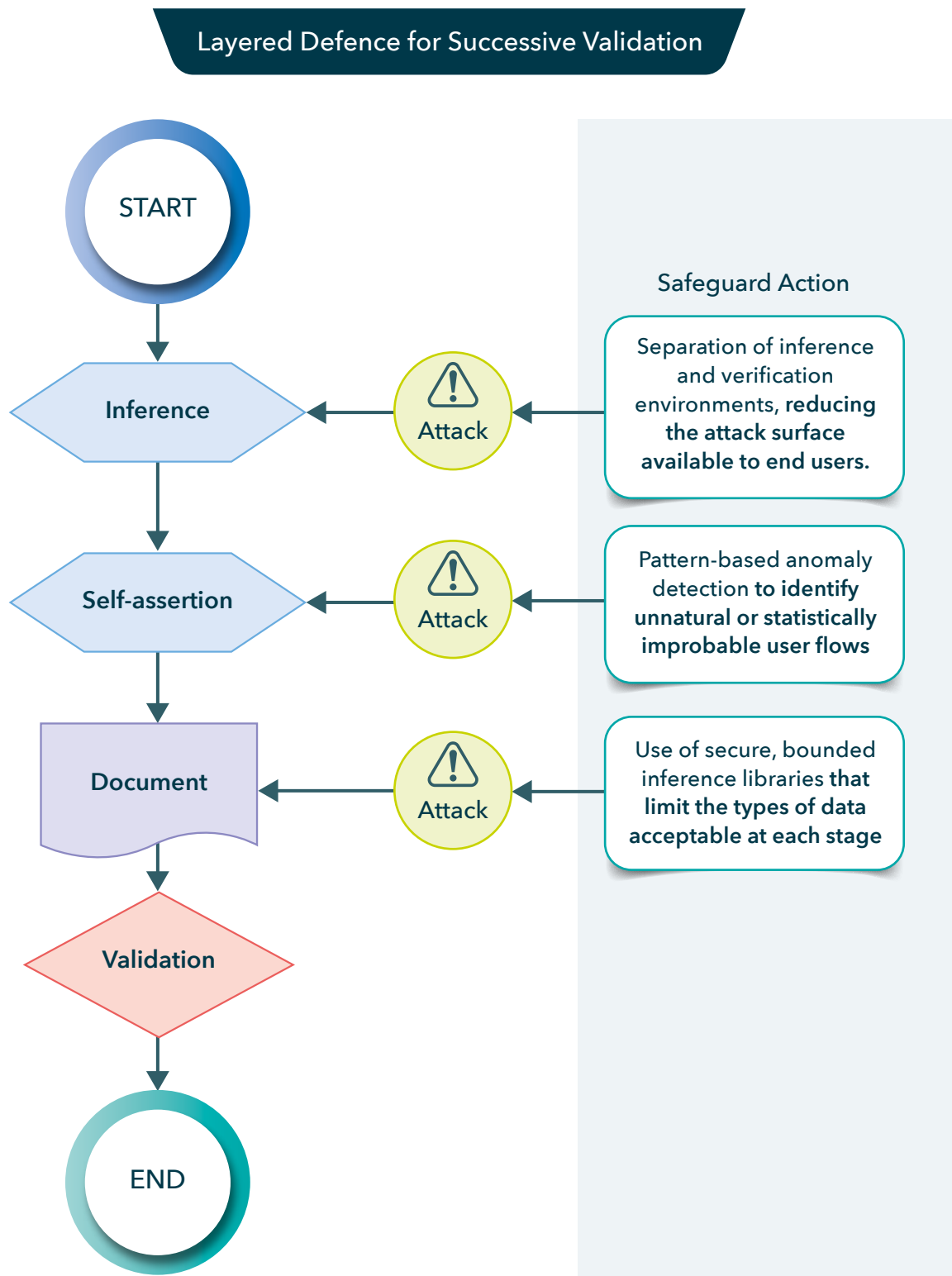


Figure F.17.3 Layered Defence for Successive Validation

| Scalability and threat likelihood

F.17.9 The Trial found that the effort, sophistication and coordination needed to construct a convincing false footprint across successive stages remains high, reducing the risk of scalable abuse. However, as age assurance systems become more integrated across services, threat surfaces will expand.

F.17.10 Future risk models may include:

- Federated signal poisoning across loosely governed platforms
- AI-driven adversarial input generation
- Cross-context replay attacks, particularly in low-friction integrations.

F.17.11 The Trial confirms that current successive validation systems exhibit strong defensive design, with proactive mitigation of manipulation risks unique to layered age assurance. While future threats may grow more sophisticated, especially with cross-platform signal reuse and AI-enhanced spoofing, today's systems show:

- Appropriate resilience to known threats
- Mature countermeasure strategies
- And a clear path for further improvement through standards-based governance, collaborative testing and transparent escalation control

F.18 User Experience and Usability in Successive Validation

F.18.1 While successive validation is technically robust and privacy-preserving, its success also depends on the usability and clarity of the user journey. Layered validation methods – such as inference, estimation and document checks – can introduce friction or confusion if not carefully designed.

F.18.2 During the Trial, providers highlighted the importance of:

- Clear escalation messaging: Users benefit from being told why they are being asked to provide additional information.
- Step-by-step guidance: Validation flows with intuitive, mobile-friendly interfaces reduced abandonment rates.
- Accessibility features: Support for users with lower digital literacy, limited English proficiency or device limitations was considered crucial in low-friction stages.

F.18.3 While validation accuracy is important, so too is the user's perception of fairness and effort required. Systems that clearly communicate their purpose, minimise repetition and explain fallback steps foster higher trust and completion rates – particularly among younger users or those unfamiliar with digital identity processes.

F.19 The Role of Relying Parties in Configuring Successive Validation

F.19.1 Successive validation workflows are typically deployed through a collaboration between age assurance providers and relying parties (e.g. website operators, app developers, content platforms). While providers offer the technical tools, it is often the relying party who:

- Determines which methods are activated.
- Sets thresholds for escalation (e.g. what counts as “borderline” in an age estimation).
- Decides whether document upload is mandatory or optional.

F.19.2 Providers participating in the Trial offered configurable templates or policy engines that allow relying parties to align successive validation flows with:

- Jurisdictional requirements (e.g. 18+ for adult content; 13+ for social media participation).
- Sectoral norms (e.g. stricter checks in fintech, lighter checks in gaming).
- Business goals (e.g. lower friction for user acquisition vs. higher certainty for compliance).

F.19.3 This flexibility allows successive validation to adapt to a wide range of operational contexts but also places responsibility on relying parties to configure flows appropriately and ensure compliance with data minimisation and proportionality principles.

Standard ISO/IEC FDIS 27566-1		
Clause	Title	Criteria
Clause 5.1	Proportionality and risk-based assurance	F8.13 describes how relying parties configure flows based on content risk, user base and jurisdiction.
Clause 6.5	Context-aware assurance	Recognises that different sectors (e.g. gaming, fintech) require different configurations - reflected here.
Clause 7.4	Configuration management	Requires age assurance systems to support flexible configuration of thresholds, methods and escalation.
Clause 7.4.1-7.4.3	Configuration rules, limits and documentation	Aligns with your text's recognition that relying parties decide activation logic and escalation paths.
Clause 6.4	Data minimisation and privacy	F8.13 ties configuration directly to minimising data use and ensuring proportionality.

F.20 Cross-Border and Jurisdictional Considerations

F.20.1 Successive validation methods are increasingly used in cross-border digital environments, where age thresholds, verification practices and data protection laws vary widely. Providers offering validation services to global platforms must consider:

- Different age thresholds: For example, 13 (US COPPA), 14 (South Korea), 16 (EU GDPR for consent), 18 (various regulated services)
- Variations in document types and formats: ID cards accepted in one country may not be machine-readable or trusted in another
- Localisation of fallback processes: Inference and estimation models may need to be tuned for regional devices, languages or user behaviours

F.20.2 Some providers reported adapting their validation logic to suit local requirements – either through region-specific rulesets or jurisdiction-aware orchestration layers. Others allowed relying parties to configure fallback flows based on geolocation or declared country of residence.

F.20.3 While successive validation offers global scalability, interoperability across legal and cultural contexts requires ongoing alignment with local regulation and user expectations.



Website

equifax.co.uk

Equifax integrates facial biometrics, document data and behavioural/fraud signals; escalates confidence through multiple data sources with configured fallback logic and weighted scoring.

Practice Statement

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

Technology Trial Test Report

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

Privacy Policy

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

Technology Trial Interview

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

Summary of Results

Equifax demonstrated effective age inference using transaction data, achieving reliable over-18 classification without biometrics. Systems operated efficiently via secure APIs, maintaining privacy through pseudonymised processing.

F.21 Machine-Readable Outputs and Interoperable Signalling

F.21.1 A key feature of successive validation is the generation of machine-readable outputs that indicate whether a user meets the age requirement and at what confidence level. These outputs are increasingly used across systems – such as integrating an estimated age result into a digital wallet or exporting a validated age attribute to a third-party relying party.






F.21.2 During the Trial, providers described a range of output formats, including:

- Boolean flags (e.g. “Over 18: Yes/No”)
- Confidence scores (e.g. “Estimated 18.7 years, confidence 96%”)
- Tiered assurance levels (e.g. Level 1: inference only; Level 3: verified with ID)

F.21.3 Some providers are aligning outputs with emerging standards such as:

- Verifiable Credentials (W3C) for digital wallets
- IEEE 2089.1 for age signal representation and interoperability
- National trust frameworks for attribute sharing

F.21.4 The format, scope and validity of these outputs are critical for enabling cross-service interoperability, user portability and privacy-preserving reuse of age validation without repeated data collection.

Provider	Output Format	Confidence Indicator	Interoperability Standards/Integration	Binding and Privacy Safeguards
	"Over 18: Yes/No", age band classification, assurance tier	Yes – configurable by relying party based on context	Supports IEEE 2089.1 and ISO/IEC FDIS 27566-1; designed to be flexible to relying party configuration	Uses pseudonymous session tokens or anonymised identifiers for output delivery
	JSON response with age estimation, DOB from OCR and face match results	Yes – age estimation subtask, OCR-based DOB, face match confidence	Modular response outputs for integration into client workflows	System outputs results for client interpretation, promoting flexibility and privacy-preserving workflows
	Boolean flags, age band pass/fail with audit metadata	Yes – certified MAE for age estimation; high-verification for ID checks	EAL-2 Challenge 25 tested; interoperable through Open Banking and document scan APIs	Passive liveness, document matching and clear thresholds for step-up escalation
	Numerical confidence score, boolean age thresholds, tiered result levels	Yes – includes Mean Absolute Error (MAE), image quality, confidence level	Supports binding via on-device selfie-to-ID match, secure tokens and W3C Verifiable Credentials	On-device processing, facial match, optional persistent link for compliance purposes
	Age over X result; fallback between facial estimation and document verification	Yes – configurable by relying party based on context	Planned future banded output; system can integrate multiple methods per relying party needs	Use of session-bound identifiers; document upload and biometric used in layered steps

Commissioned by the **Australian Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts**, the Trial assessed 48 vendors and over 60 distinct technologies across various sectors, including social media, gaming, adult content and online retail. Through lab-based testing, interviews, analysis, school-based trials and mystery shopper evaluations, the Trial investigated how well different solutions could confirm, estimate or imply a user's age in ways that are secure, privacy-preserving and inclusive.

Can age assurance be done? The answer – based on thousands of data points, stakeholder interviews and international standards – is **yes, it can.** While no single solution fits all contexts, the Trial found that a wide variety of technologies already meet meaningful thresholds for accuracy, security and privacy when carefully selected and implemented. The report offers a comprehensive evidence base to support regulators, industry leaders and the broader public in shaping a safer, age-appropriate digital environment for all Australians.

@AgeCheckCert

