



Age Assurance Technology Trial

PART H

Parental Consent

August 2025



Funded by



Australian Government

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

Project by



Findings on Parental Consent

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

1

Parental consent systems **can be effectively applied** in Australia across different services and platforms.

2

Consent mechanisms offered **private, event-driven models** flowing from age assurance outputs; typically triggered at point of access.

3

Design approaches varied significantly across providers; evaluated systems ranged from lightweight verification to more formalised models involving ID checks.

4

Most **systems assumed conventional family structures**; did not routinely account for more complex guardianship arrangements.

5

Long-term consent logging practices varied, with **implications for privacy and transparency**.

6

Emerging innovations showed **potential to support more dynamic consent workflows**; may facilitate more responsive consent experiences.

7

Alignment with international standards was evident, though implementation maturity differed.

8

Consent was generally positioned as a **one-time event**, with limited ongoing interaction and designs focused on single transactions.

© 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 978-1-0681646-7-5



Table of contents

Introduction and Context



H.1	Introduction to Part H: Parental Consent	6
H.2	Executive Summary	8
H.3	Who Participated in the Trial of Parental Consent Technology	11

Context, Standards and Methodology



H.4	What is Parental Consent	14
H.5	Evaluation Approach for Parental Consent Systems	18

Detailed Analysis of Parental Consent Findings



H.6	Parental Consent Can Be Done	30
H.7	Inconsistent Verification of Parental Authority	42
H.8	Policy and Technological Readiness	48
H.9	Lack of Recognition for Evolving Child Capacities and Rights	53
H.10	Risks of Circumvention and Identity Weaknesses	55
H.11	Practice Statements and the Current State of Parental Consent Design	58
H.12	Security and Integrity of Parental Consent Mechanisms	61

H.13	Innovation and Emerging Practices in Parental Consent Systems	64
H.14	Data Handling and Privacy Practices in Parental Consent Systems	71
H.15	Inclusivity and Guardianship Complexity in Parental Consent Mechanisms	75
H.16	Systemic Challenges and Opportunities in the Development of Parental Consent Mechanisms	81
H.17	Contextual, Risk-Aligned Deployment of Parental Consent Mechanisms	88
H.18	Data Minimisation and the Privacy Risks of Persistent Consent Logging	92
H.19	Standards Based Approach to Consent Management	99



Age Assurance Technology Trial

PART H

Introduction and Overview

I



H.1 Introduction to Part H: Parental Consent


H.1.1 Part H of the Age Assurance Technology Trial focuses on parental consent – a form of age assurance where a parent or guardian confirms a child’s access to age-restricted goods, services or content, typically in digital environments. Unlike age estimation, inference or verification, parental consent does not seek to determine a user’s age directly. Instead, it relies on the intervention of a responsible adult, who attests to the child’s eligibility, often in response to an age-related trigger.

H.1.2 Parental consent operates downstream of other age assurance methods. A user is typically flagged as a child (or possible child) through inference, estimation or declared age, after which a parent or guardian is asked to approve access or authorise an account. Parental consent thus acts as a decision point – not a measurement tool – and must be implemented with clear evidence of adult identity, informed consent and safeguards to prevent coercion, misrepresentation or circumvention.

H.1.3 This part of the report examines how parental consent systems are designed, how they operate in real-world deployments and the extent to which they meet the requirements of emerging international standards – particularly ISO/IEC FDIS 27566-1¹ and IEEE 2089.1². These standards set functional expectations for parental involvement, identity binding, consent logging, data minimisation and the appropriate use of parental permissions across different risk contexts.

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.



H.1.4 The Trial was established to evaluate the technical feasibility and privacy implications of a wide range of age assurance methods in the Australian context. It does not make policy recommendations, nor does it seek to determine whether parental consent should be mandated for any particular use case. Rather, it addresses whether parental consent technologies are practically implementable, user-friendly, secure and reliable in supporting age assurance – particularly for children under regulatory thresholds such as 13, 15 or 18.

H.1.5 This report explores the strengths and challenges of parental consent as a method of age assurance, including:

- How the consent process is initiated and verified
- How parent-child relationships are authenticated
- What safeguards are in place to protect the child's and guardian's data
- How systems prevent misuse or false assertions of parental status

H.1.6 Importantly, we examine how well current technologies can balance the rights of children, responsibilities of guardians and expectations of relying parties, while ensuring the experience is accessible, inclusive and meaningful across diverse communities and service contexts.

H.2 Executive Summary

H.2.1 Parental consent mechanisms represent a widely recognised component of age assurance strategies, particularly in digital environments where children seek access to services or content subject to regulatory thresholds, such as those below the ages of 13 or 16. These mechanisms enable a responsible adult – typically a parent or legal guardian – to authorise a child’s participation in age-restricted environments, usually after an initial trigger such as self-declared age or inferred risk. Unlike parental controls, which are configured in advance and applied continuously, parental consent is typically event-based, requiring an affirmative, verifiable action by an adult at a specific point in the child’s user journey.

H.2.2 The Trial evaluated a range of parental consent systems currently deployed or in development across Australian and international contexts. It found that these systems are technically feasible and can be effectively deployed using existing infrastructure. Participating providers demonstrated varied approaches to capturing consent, including email-based verification, credit card micro-payments, digital identity checks and token-based authorisation. While many of these mechanisms were already operational, their implementation styles varied in rigour, user experience and alignment with international frameworks.

H.2.3 Across the evaluated systems, most implementations were designed around conventional, binary parent-child relationships. As a result, few consent models explicitly accommodated non-traditional caregiving arrangements, such as those involving foster carers, kinship care or shared parental responsibility. Similarly, most mechanisms were static in design, offering limited support for consent renewal, expiry or adaptation as the child matures. This often left little scope for recognising the evolving capacities of children or involving them meaningfully in the consent process.

Key Statistics About Parental Consent

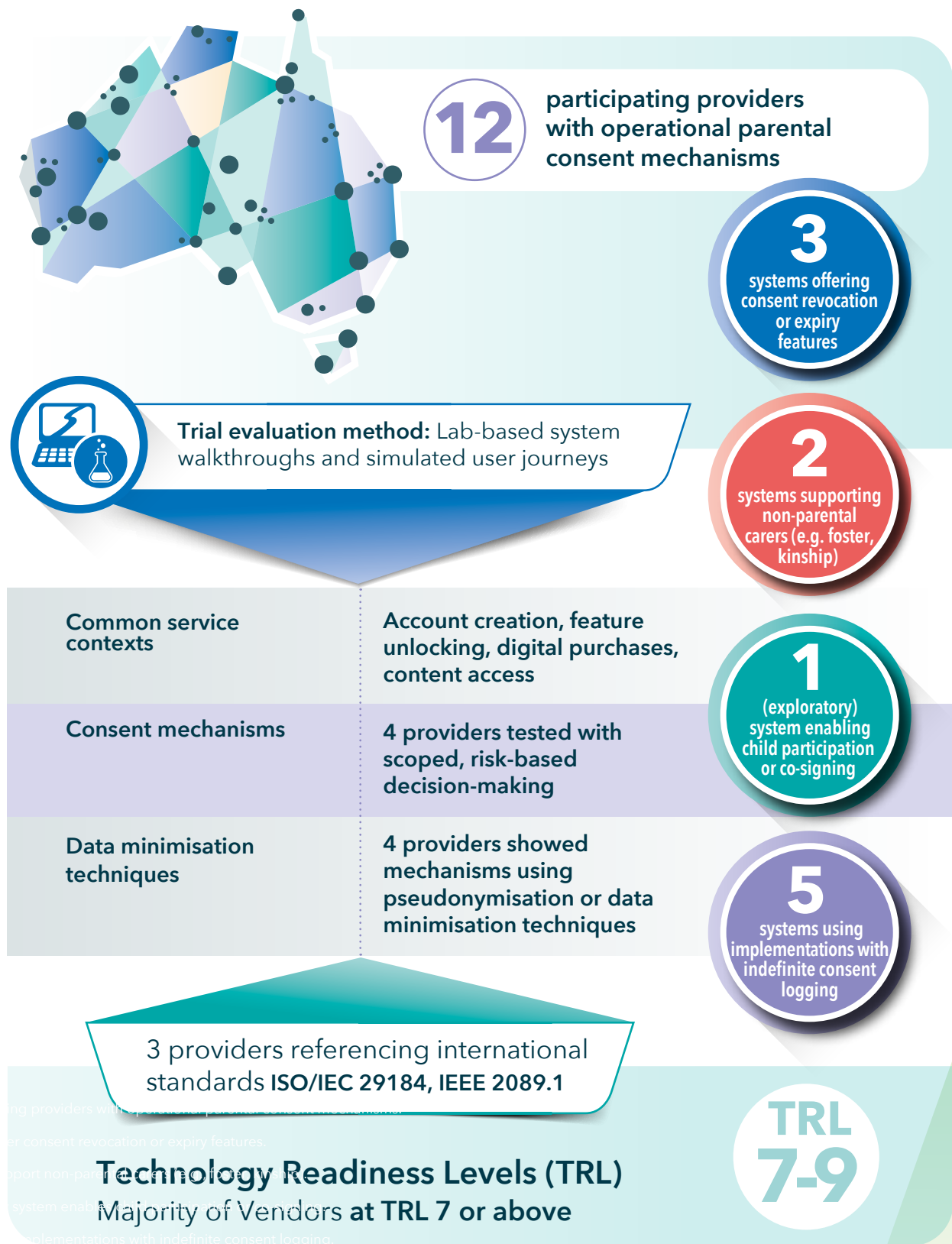


Figure H.2.1 Key Statistics from the Trial on Parental Consent

H.2.4 Verification of the adult's identity and legal authority varied in strength. Some systems relied primarily on self-declaration or account-based continuity, while others integrated more robust checks. Although several providers referenced alignment with standards such as ISO/IEC 29184 (Online privacy notices and consent) and IEEE 2089.1, practical application of principles like informed consent, accessibility and revocability differed across implementations.

H.2.5 Emerging innovations – such as scoped, time-bound consent signals and privacy-preserving credential frameworks – indicated a growing maturity in the field, but also revealed challenges related to interoperability and ecosystem fragmentation. The retention and use of consent logs also varied, with some systems demonstrating strong privacy-by-design features (such as pseudonymisation or limited signal exposure), while others retained long-term records without clear boundaries on scope or re-use. This variability has implications for the privacy and data protection of both children and guardians.

H.2.6 Overall, the Trial found that parental consent technologies are functionally mature and capable of supporting access governance where age-related restrictions apply. However, the consistency, inclusiveness and contextual adaptability of these mechanisms remains uneven. The findings suggest that while the technology underpinning parental consent is largely in place, further evolution in design, scope and implementation may be necessary to ensure these systems work equitably, proportionately and in support of both children's rights and service provider obligations.

H.3 Who Participated in the Trial of Parental Consent Technology





Age Assurance Technology Trial



PART H

Context, Standards and Methodology



H.4 What is Parental Consent

H.4.1 A parental consent mechanism is a process that enables a parent or legal guardian to provide or revoke permission for a child to access digital goods, content, services, venues or spaces.

H.4.2 Unlike parental control, which is configured in advance and operates continuously, parental consent arises in response to an age assurance trigger – typically when a child attempts to access something that requires age verification or compliance with legal or policy restrictions.

H.4.3 Parental consent mechanisms typically involve five stages:

1. Identifying the parent or guardian, usually via account credentials, digital ID or other verified identity tools
2. Binding the parent or guardian to the correct child, confirming their legal relationship
3. Capturing informed consent for a specific action, such as joining a service, purchasing digital goods or engaging with age-restricted content
4. Communicating consent status to the relying party or service provider, often through a verifiable token or signal that the child has parental permission for the requested access
5. Providing a facility for consent to be revoked

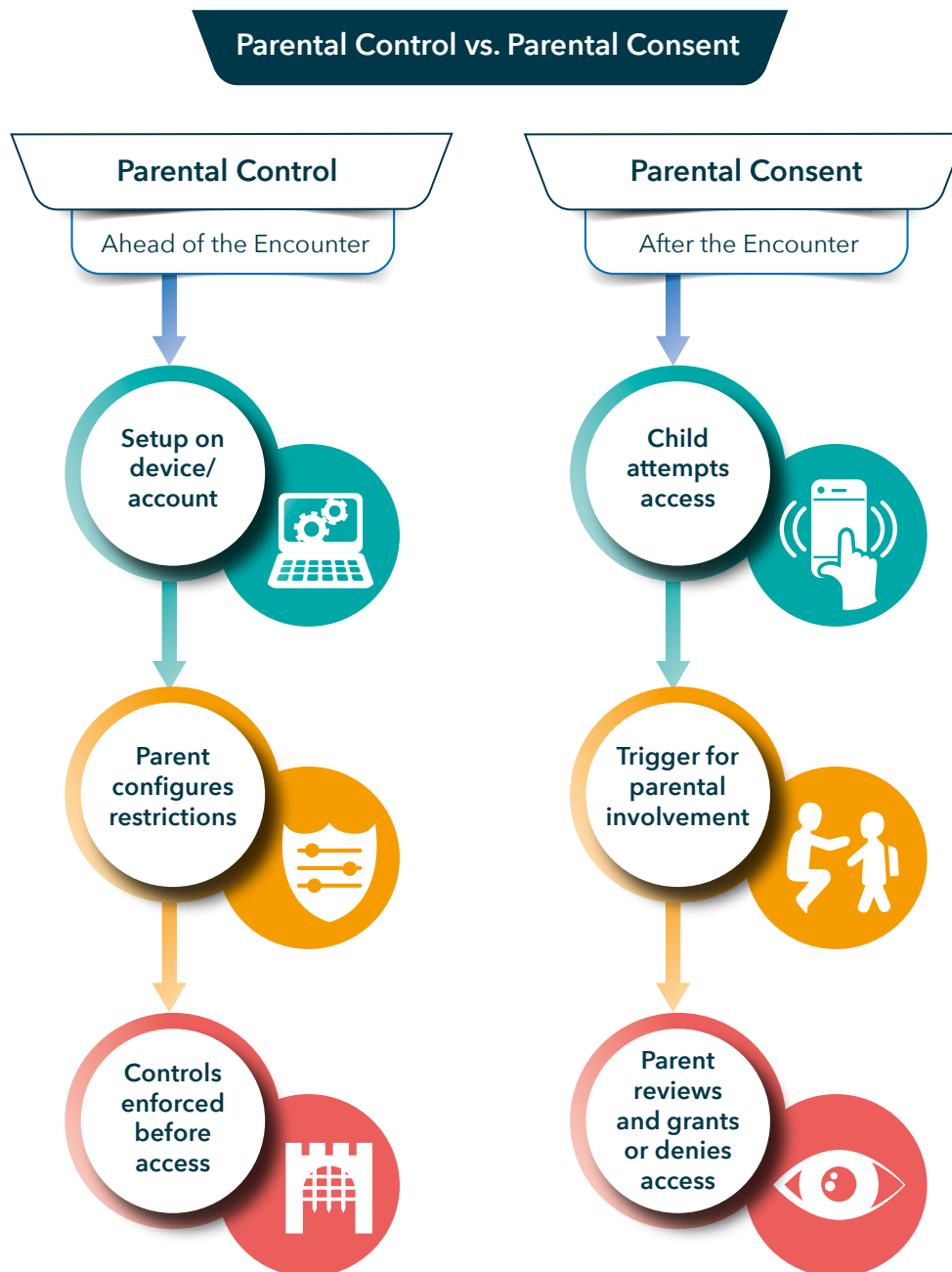


Figure H.4.1 Parental Control vs. Parental Consent



Figure H.4.2 Five Stages of Parental Consent

H.4.4 Parental consent mechanisms can be found in many online and offline services, such as:

- Online platforms: social media networks, multiplayer games, educational portals and content platforms often request guardian permission for children under a certain age
- Mobile and app ecosystems: app stores and in-app purchase systems may require verified consent before allowing downloads or transactions
- Offline environments: schools, healthcare providers or recreational venues (such as trampoline parks or soft play centres) may require guardian signatures or digital forms to authorise child participation in services or activities



H.5 Evaluation Approach for Parental Consent Systems

H.5.1 The evaluation of parental consent systems in the Trial was grounded in a structured, standards-informed methodology, designed to assess how these systems operate in practice and the extent to which they are usable, verifiable, secure and aligned with children's rights.

H.5.2 Parental consent was treated in the Trial as a distinct functional model that flows from – but is not itself – a form of age assurance. Consent mechanisms are typically triggered after an initial age-related determination has been made, such as through self-declaration, age verification or other assurance methods. Once a user is flagged as potentially under a defined age threshold, a parental or guardian approval process is initiated to confirm access. The evaluation therefore focused on how effectively these downstream mechanisms capture, transmit and manage parental authorisation – and how well they align with standards for security, usability, privacy and rights protection.







| Lab-based, simulated evaluation only

H.5.3 As with parental control systems, no live deployments or field trials of parental consent mechanisms were undertaken. This decision was based on strong ethical considerations: testing live consent systems could have inadvertently altered the access permissions of real children or families, particularly in systems that rely on persistent tokens, linked accounts or shared devices.

H.5.4 Instead, the evaluation used lab-based simulations, structured walkthroughs and provider-submitted evidence, allowing for consistent assessment of system capabilities without risking unintended consequences for users.

| Standards referenced

H.5.5 The evaluation was aligned with international frameworks relevant to consent governance, age assurance, software quality and digital rights:

International Standards	
 ISO/IEC FDIS 27566-1	Framework for age assurance systems
 ISO/IEC 29146	Access management (including delegation and guardian control relationships)
 ISO/IEC 29184	Online privacy notices and consent
 IEEE 2089.1	Age-appropriate digital services framework
 ISO/IEC 25010 & 25040	Software product quality models and evaluation criteria
 ISO/IEC 29119	Software testing standards

| International Standards for Parental Consent Methods

H.5.6 Parental consent mechanisms are a critical component prompted by the output of age assurance frameworks, particularly where access to digital services by children requires active authorisation from a parent or guardian. Several international standards provide guidance on the design, implementation and governance of these mechanisms to ensure they are secure, transparent and rights-respecting.



ISO/IEC 29184:2020 - Online privacy notices and consent

H.5.7 ISO/IEC 29184 provides a formal framework for managing online privacy notices and obtaining user consent, including mechanisms relevant to parental consent in digital environments. While not specific to age assurance, the standard outlines clear requirements for consent flows involving minors and third parties, including:



ISO/IEC 29184	Criteria
Clear, Understandable Notices	Organisations must ensure that privacy notices – including those directed to parents – are concise, intelligible and tailored to the digital literacy of the audience, including children.
Informed Consent	Consent must be based on a clear explanation of what data is collected, for what purpose and how it will be processed or shared. For parental consent, this includes specifying the scope of permission and its implications for the child.
Verifiability	Where a guardian's consent is required (e.g., for children under a certain age), the organisation must implement mechanisms to verify that the person granting consent has the authority to do so.
Withdrawal and Revocation	Parents must be able to revoke consent easily and systems should support timely and effective withdrawal mechanisms that apply to the child's data access or participation.
Record-Keeping and Accountability	Systems should log consent events in an auditable manner, enabling compliance with legal and regulatory frameworks and offering transparency to both regulators and end users.

H.5.8 By aligning parental consent flows with ISO/IEC 29184, service providers can ensure that their processes uphold international expectations around clarity, fairness and verifiability – crucial elements for responsible age assurance.

IEEE IEEE 2089.1 - Age-appropriate digital services framework

H.5.9 IEEE 2089.1 provides further structure by offering a risk-based framework for age-appropriate digital service design. In the context of parental consent, it highlights:

IEEE 2089.1	Criteria
Risk-Proportionate Design	Consent requirements should reflect the nature and sensitivity of the service or content being accessed. Higher-risk activities (e.g., social media use, location tracking) may warrant more robust parental validation.
Transparency and Inclusivity	Consent mechanisms should be understandable and accessible to parents and guardians across diverse cultural and literacy backgrounds.
Ongoing Oversight	Parental consent is not a one-time event; systems should provide mechanisms for ongoing oversight, notification and role-based participation.

H.5.10 Together, ISO/IEC 29184 and IEEE 2089.1 provide a robust framework for implementing parental consent mechanisms in digital environments. These standards support service providers in designing consent systems that are legally compliant, technically secure and practically accessible - while also respecting the rights of children and parents alike.

| Sources of evidence

H.5.11 The evaluation drew on four main sources of input:

- Practice statements submitted by providers, outlining system design, consent workflows, verification methods and data handling practices
- Vendor interviews, used to clarify implementation approaches and explore edge cases such as revocation, multi-child households and out-of-home care
- System walkthroughs and demonstrations, including simulated user journeys based on typical parent-child interaction scenarios
- Publicly available documentation, such as privacy policies, consent disclosures and user guidance materials

H.5.12 No real children, guardians or end-user accounts were involved in this part of the Trial.



Evaluation criteria



ISO/IEC 25010

H.5.13 Systems were assessed against a consistent set of attributes adapted from ISO/IEC 25010 and related standards:

ISO/IEC 25010	Criteria
Authenticity of parental binding	Whether the system reliably linked the consenting adult to the correct child (e.g. via shared credentials, ID verification, secure tokens).
Usability	Accessibility, clarity and ease-of-use of the consent process for parents and guardians.
Auditability and revocation	Whether systems recorded consent actions appropriately and provided meaningful options for withdrawal or expiry.
Privacy and data minimisation	The degree to which both parent and child data were protected, with minimal collection and retention.
Security	Protections against impersonation, circumvention or misuse of the consent mechanism.
Interoperability	The extent to which consent status could be integrated into wider age assurance or identity management systems.
Compliance support	Alignment with regulatory expectations for verifiable, informed and freely given consent.



| Scope and limitations

H.5.14 The evaluation of parental consent systems was designed to assess technical feasibility, design alignment with standards and potential implementation risks. However, significant limitations applied due to the inherent sensitivity of consent relationships and the ethical implications of interfering with live systems used by real families.

H.5.15 Specifically:

- No real-world deployments or field trials were undertaken. All testing was conducted in controlled, lab-based environments or simulated journeys. This decision was made to avoid the risk of altering a real child's access permissions, triggering unintended notifications or affecting persistent consent records stored across services.
- Verification of parental identity and legal authority was not tested in practice. While many systems claimed to verify guardianship via ID checks, payment methods or account linking, the Trial did not attempt to independently validate whether these mechanisms reliably confirmed legal responsibility under relevant laws (e.g., for non-parental carers or shared custody arrangements).
- Revocation, dispute and edge-case scenarios were not simulated. The Trial did not test what happens when consent is contested, revoked or lapses over time. Insights into these behaviours are based solely on provider descriptions and policy documents.
- Children's participation in the consent process was not directly observed. The evaluation considered how systems were designed to accommodate children's evolving capacities and rights (e.g. UNCRC³ Articles 5 and 12), but did not engage with children or families to validate how those features worked in practice.

3. *The UNCRC is a legally binding agreement which outlines the fundamental rights of every child, regardless of their race, religion or abilities. Australia became a signatory to the UNCRC on 22 August 1990 and ratified it on 17 December 1990.*

- Legal validity of the consent mechanisms was outside scope. The Trial did not assess whether the consent collected met the legal thresholds under domestic or international child protection and privacy laws. The focus was on technical implementation, not legal sufficiency.
- No behavioural testing was performed. The evaluation did not explore how children or parents interact with consent prompts under real conditions – including issues of digital literacy, comprehension or power dynamics in decision-making.

H.5.16 These limitations are critical to interpreting the findings. While the Trial was able to assess how parental consent mechanisms are intended to operate, it was not designed to capture their real-world reliability, impact on families or alignment with lived experience. Future evaluation may require staged, consented trials involving family groups under more controlled but realistic conditions.



Age Assurance Technology Trial

PART H

Detailed Analysis of Parental Consent Findings



H.6 Parental Consent Can Be Done

| Summary finding

H.6.1 Parental consent mechanisms are viable and implementable in Australia. The Trial found that a number of providers had established functional, secure and user-friendly parental consent pathways, particularly for onboarding child users into online services. These solutions provided real-time opportunities for adults to approve or decline access, enhancing parental oversight while preserving user autonomy.



| Detailed analysis

H.6.2 Parental consent mechanisms operate downstream of age assurance processes, typically following self-declaration or inference that a user is under a defined threshold. They do not establish age directly but instead provide a formal pathway for adult approval where such access is required.

H.6.3 Parental consent, as defined in this report and consistent with ISO/IEC 29184:2020, refers to a process by which a parent or guardian is presented with a clear, understandable privacy notice and is able to provide informed, verifiable consent for a child's engagement with a digital activity or service. Unlike age verification, which determines a user's age through direct evidence, parental consent mechanisms rely on transparency, comprehension and user-agency - focusing on whether the parent or guardian has been clearly informed and has genuinely authorised the child's access.

H.6.4 While ISO/IEC FDIS 27566-1 (Age Assurance Systems Framework) explicitly excludes parental consent from its functional scope, it refers implementers to complementary standards for guidance on privacy, notice and consent mechanisms - chief among them ISO/IEC 29184.

H.6.5 Several Trial participants demonstrated working implementations of standards-aligned parental consent workflows, including:

- Verifiable email or SMS confirmation loops, where the parent was notified of a child's request and completed a verification action to authorise access.
- Micro-payment validation, using a nominal, refundable charge to a known adult-held payment method to verify the user's role and authority.
- ID-based verification, with the parent's identity confirmed through credential checks before authorising the child's participation.
- Time-limited, revocable consent tokens, supporting consent that could expire, be withdrawn or be scoped to a specific context.

H.6.6 These implementations reflected key principles set out in ISO/IEC 29184, including:

- Transparency and accessibility of privacy notices: Parents received clear, timely explanations of what data would be collected, how it would be used and their rights to control that data.
- Comprehension and choice: Consent was obtained via mechanisms that offered a genuine opportunity for informed agreement, in accessible and understandable formats.
- Verifiability of consent: Systems captured not just that consent was given, but that it was linked to a recognisable and valid user pathway (e.g., known email, verified ID or payment credential).
- Ability to withdraw or revoke consent: Consistent with the right to withdraw under ISO 29184, consent was not treated as permanent or indefinite and parents were offered options to revoke it.

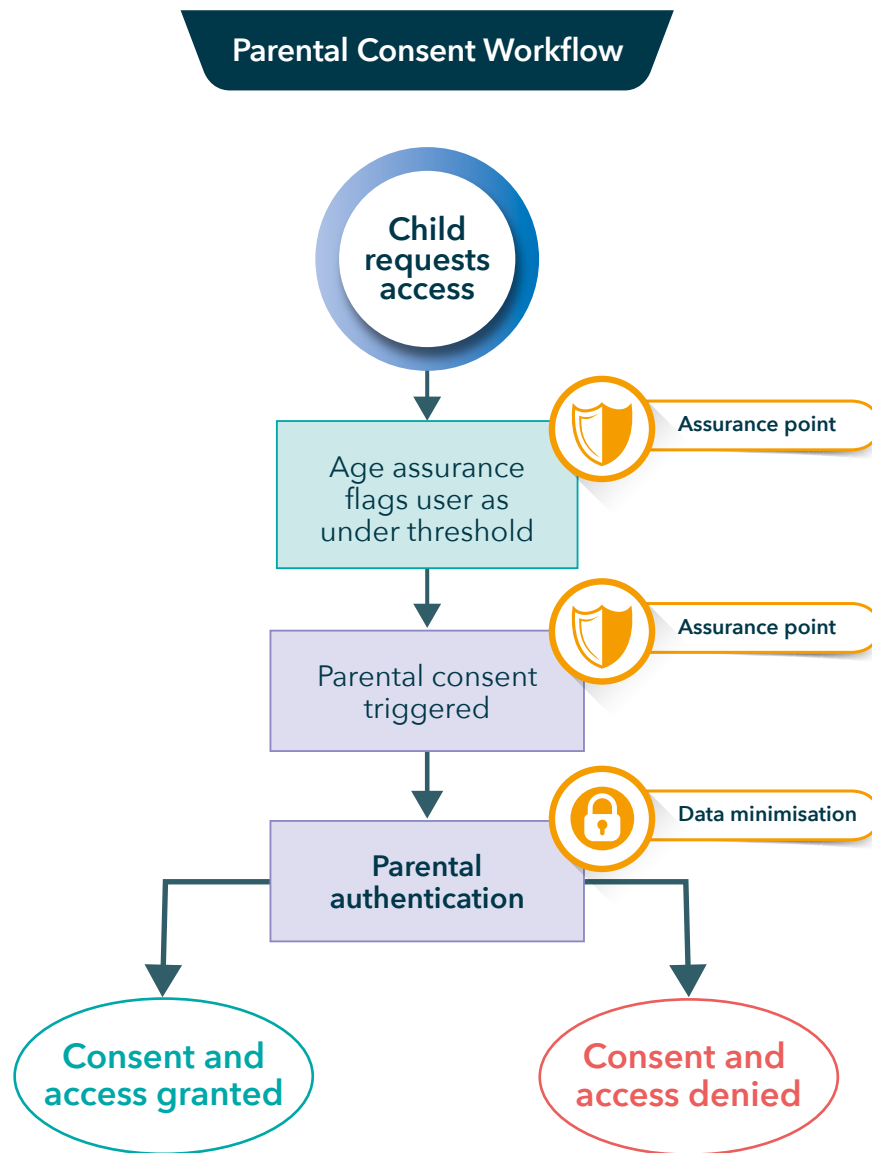


Figure H.6.1 Parental Consent Workflow

H.6.7 In the Australian context, these mechanisms align well with:

- The Family Law Act 1975, which defines parental responsibility and supports legal recognition of consent given by a parent or guardian.
- High rates of digital literacy and smartphone usage among Australian families, enabling multi-channel parental engagement.
- Emerging interoperable digital identity frameworks, which could enhance the scalability and reliability of parental consent mechanisms.

H.6.8 However, the Trial also highlighted risks and usability challenges. Overly complex or privacy-intrusive consent flows may discourage use or reduce trust, while weak, unverifiable processes may fail to withstand legal or regulatory scrutiny.

| Insights from the evaluation

H.6.9 The evaluation identified several attributes and design approaches that appeared to support more effective, trustworthy and rights-respecting parental consent mechanisms. These included:

- Clear and transparent consent interfaces: Consent forms and user flows were most usable when they were concise, visually accessible and adapted to the literacy levels of both parents and children.
- Dynamic and revocable consent models: Some systems allowed parents to set time limits, restrict feature access or issue consent for specific purposes, rather than granting open-ended approval. These approaches were better aligned with evolving contexts and user expectations.
- Context-specific scoping and expiry: Consent mechanisms that included automatic expiry, time-bound access or service-specific permissions appeared to reduce the risk of long-term profiling or consent reuse beyond the original intent.

- Separation of authentication from consent: Systems that distinguished between identity verification (proving who the parent is) and consent (actively authorising a child's access) provided clearer assurance pathways. Verifying identity alone was not treated as sufficient.

H.6.10 Together, these design elements align closely with the intent of ISO/IEC 29184 and IEEE 2089.1, which describe functional requirements for parental involvement, clarity of consent flows and proportional safeguards. While not all features were implemented consistently across providers, the Trial found strong interest in improving the usability, scope and accountability of parental consent systems in line with these international standards.

H.6.11 These findings are based on lab-based evaluation only. Real-world testing of child interaction, consent durability and family dynamics was outside the scope of the Trial and insights into usability and revocation are based on provider claims, not observed behaviour.

| What parental consent is and is not

H.6.12 Parental consent, in the context of age assurance, refers to a verifiable, affirmative decision made by a parent or legal guardian to allow a child under a regulatory age threshold (such as 13) to access a specific good, service, content, venue or space. It is typically triggered after an age assurance process identifies that the user is a child, prompting a decision from the parent or guardian. Consent must be active, informed, specific to the context and authenticated through reliable mechanisms – such as identity verification, payment method confirmation or cryptographically secure authorisation.

H.6.13 Parental consent is not simply the presence of a shared device or co-use of an account, nor is it a passive configuration set at the time of device purchase or service registration. It is also not equivalent to parental control, which is the pre-emptive management or restriction of a child's access to content or services. While parental control is proactive and configured ahead of a potential encounter, parental consent is reactive, occurring at or after the point of attempted access and requiring a clear, verifiable approval. It is also distinct from self-declaration by either the child or the parent, where no verification or binding to the consenting party takes place.

| Why parental consent is important

H.6.14 Parental consent plays a crucial role in safeguarding children's rights and welfare in digital and physical environments. It provides a legal and ethical mechanism for involving a parent or guardian in decisions about a child's access to age-restricted goods, services, content, venues or spaces. Where a child is below a defined regulatory threshold – commonly 13 in privacy and digital safety legislation – parental consent serves as the gatekeeping step that aligns with legal obligations and best practice in child protection.

H.6.15 This process ensures that parents or guardians are informed and empowered to make choices about their child's digital experiences, helping to enforce boundaries that children may not fully understand themselves. It also provides an important layer of accountability for service providers, ensuring that children's data is not processed unlawfully and that they are not inadvertently exposed to harmful or developmentally inappropriate material.

H.6.16 Moreover, well-implemented parental consent systems support transparency and trust between families and digital platforms. They give parents visibility into their child's interactions and allow them to assess and approve access on a case-by-case basis. This is particularly relevant in online services where risks vary by context – such as social media, gaming or educational platforms – and a nuanced, human decision may be more appropriate than a purely algorithmic one.

H.6.17 By embedding verifiable parental consent into services that rely on age assurance mechanisms, service providers can better comply with legal frameworks like the Children's Online Privacy Protection Act (COPPA)⁴ or Australia's own Privacy Act⁵, while also respecting family autonomy and promoting responsible digital citizenship.

4. *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.*
5. *The Privacy Act 1988 was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations with an annual turnover of more than \$3 million, and some other organisations, handle personal information.*

| How technically ready are parental consent systems

H.6.18 Parental consent systems assessed during the Trial demonstrated varying levels of technological maturity, with several solutions already operational and embedded within commercial offerings. Most systems were assessed at Technology Readiness Level (TRL) 8 or 9, indicating they are either fully deployed or approaching widespread use in production environments.

H.6.19 Participants such as PRIVO, Qoria and Assure ID showcased end-to-end consent workflows that included identity verification, parent-child account linking and revocable authorisation signals. These implementations were designed to align with existing regulatory frameworks and were supported by dashboards or credentials to enable real-time parental oversight.

H.6.20 Other participants, such as R2 Labs, Sedicii and TrustElevate, presented technically advanced models – including cryptographic consent tokens, zero-knowledge proofs and verifiable parental credentials – that offer high privacy and security assurances. While innovative, these systems typically required broader ecosystem integration or relying-party adoption to reach full deployment maturity.

H.6.21 Overall, the Trial found that there are no fundamental technological barriers to implementing secure, verifiable parental consent systems in Australia. However, real-world readiness depends on factors such as platform interoperability, standardisation and service provider willingness to adopt externally issued consent signals. Continued progress will rely on improving alignment between back-end infrastructure, identity frameworks and inclusive user interfaces that accommodate the diversity of parental roles and caregiving contexts.

H.6.22 Parental consent technologies are therefore technically viable and increasingly sophisticated, offering a strong foundation for scalable, risk-responsive and rights-aware age assurance in digital services. The table below summarises the assessed TRL status of participating solutions.



Figure H.6.2 TRL

Technology Readiness Assessment for Parental Consent Systems

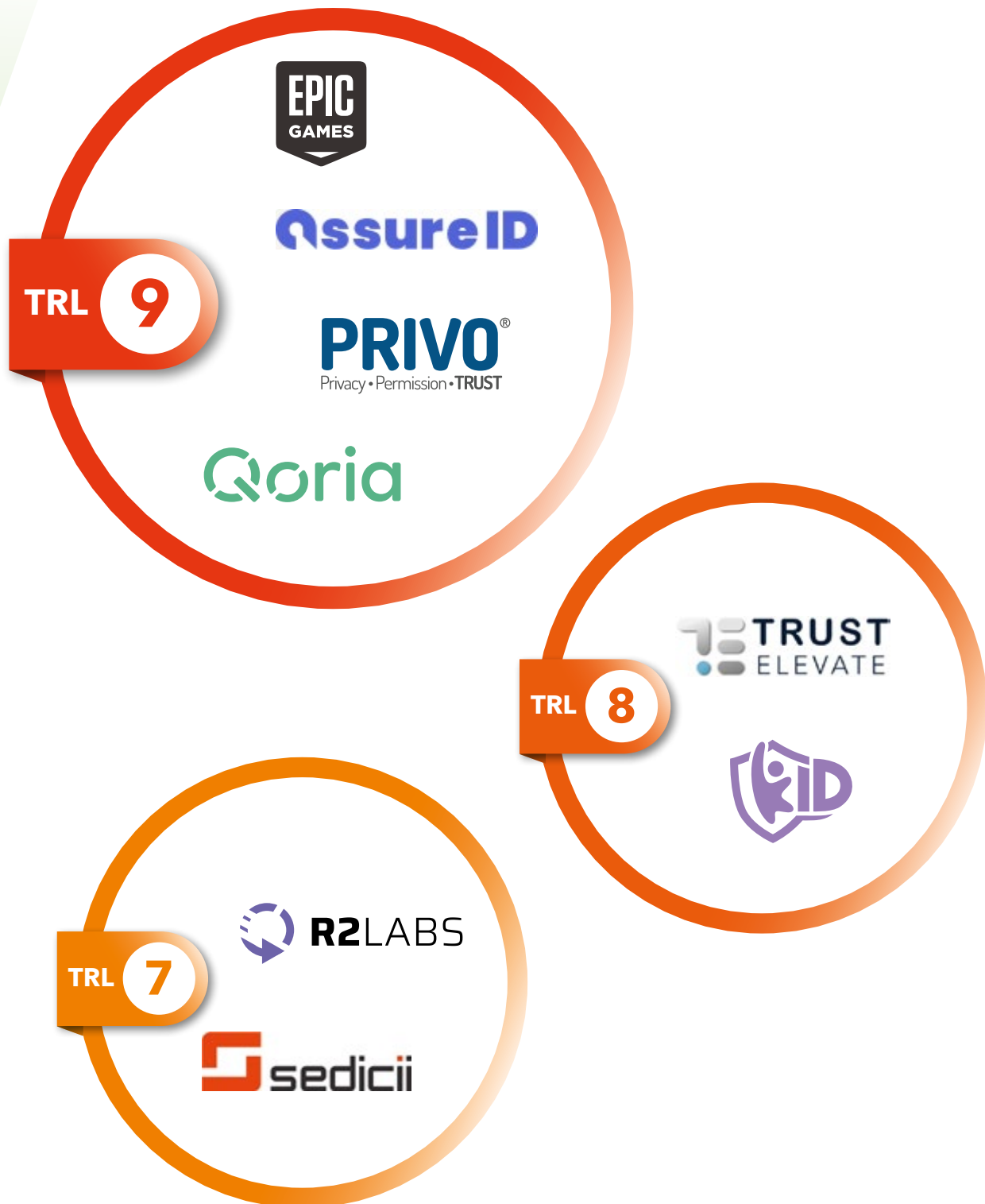


Figure H.6.3 Technology Readiness Assessment for Parental Consent Systems

Provider	Notes
Assure ID	Browser-based parental consent system in live production; consent linked via PIN-based access.
k-ID	Operational credentialing service: consent requires relying party implementation support.
PRIVO	Commercial platform with verified parental workflows and token-based consent signalling.
Qoria	Fully deployed system in education settings; supports parent account linkage and filtering.
R2 Labs	Issues cryptographically secure consent tokens; strong privacy model but less ecosystem uptake.
Sedicii	Implements zero-knowledge proofs for parental consent; technically sophisticated but limited integration scope.
TrustElevate	Demonstrated live workflows and feature-level consent with verifiable parental binding.

H.7 Inconsistent Verification of Parental Authority

H.7.1 Many consent systems lacked consistency and clarity in how they verified parental authority or confirmed the parent-child relationship. In several cases, self-declared authority was accepted without verification, raising concerns about the integrity and legal validity of the consent.

H.7.2 Most systems relied on static or single-instance consent, with few mechanisms in place for reviewing, updating or withdrawing consent as the child's circumstances changed. This rigidity is particularly problematic in fast-changing digital environments where children's developmental capacity – and the associated level of risk – can shift rapidly.

H.7.3 Parental consent systems are needed when the outcome of an age assurance process indicates that parental or guardian approval is needed for the child user to proceed to utilise the services. We found no technological barriers to this in Australia.

H.7.4 Service providers and policymakers demonstrated thoughtful consideration in deploying these systems to help manage access to age-restricted goods, services, content, venues or spaces – particularly for younger children.

H.7.5 A significant challenge observed during the Trial was the inconsistent verification of parental authority across different systems. While most platforms correctly identified when parental consent was required – typically triggered by an age assurance result indicating the user was under a set threshold (e.g., under 13 or under 16) – the methods for verifying that the individual granting consent was a legitimate parent or guardian varied widely.

H.7.6 In many cases, self-declared consent was accepted without verification. For instance, systems would allow a user to enter an email address purportedly belonging to a parent and consider a click-through or check-box affirmation as sufficient consent. This raises serious concerns about the legal robustness and reliability of such mechanisms. Without robust binding between the adult and child (e.g., via shared account credentials, verifiable identity documents or payment instruments), the system may fail to meet regulatory expectations for verifiable parental consent under privacy laws.

H.7.7 ISO/IEC 29184 stresses the importance of clear, accessible and transparent notice and consent processes, including verifiability of both notice delivery and consent origin. In practice, few systems provided evidence that the parent had truly received, understood and affirmatively responded to the consent request.

H.7.8 One exception was PRIVO, which demonstrated a multi-method approach to verifying parental authority, including identity document upload, credit card verification and scoped consent management via a parent dashboard. Consent events were logged and could be reviewed or revoked, providing clearer alignment with the verifiability expectations set out in ISO/IEC 29184. While not universal across participants, such implementations show that robust verification of parental authority is achievable using currently available technologies.

Vendor Case Study



Website

privo.com

PRIVO (Privacy Vaults Online) participated in the Trial as a provider of verifiable parental consent infrastructure. Its platform is designed to enable digital services to obtain, manage and audit parental consent across multiple child-facing environments. PRIVO's solution was notable for its multi-method approach to verifying parental identity and authority, its support for scoped and revocable consent and its alignment with key international standards including ISO/IEC 29184 and COPPA.

Three Key Facts

1

PRIVO links verified adults to child users, managing consent with secure, token-based, privacy-focused signals.

2

PRIVO's dashboard empowers parents to manage, revoke, and monitor consent, ensuring transparency and ongoing control.

3

PRIVO's audit trail logs detailed consent events, ensuring accountability, compliance, and alignment with global standards.

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

PRIVO's implementation demonstrates that it is possible to:

- Reliably verify parental authority using accessible, multi-method workflows
- Bind parents to children across diverse service contexts
- Enable meaningful consent management and revocation
- Comply with both privacy law and ethical standards around child rights

| Static vs. dynamic consent models

H.7.9 Another key finding was that most systems operated on a static or one-time consent model. Once given, consent was often treated as permanent, with limited or no mechanisms for:

- Revisiting or renewing consent
- Adjusting consent scope based on the child's development
- Withdrawing consent as risks or use cases evolved

H.7.10 This lack of flexibility is increasingly problematic in dynamic digital environments. Children's needs, maturity and use of technology change rapidly - often within short timeframes. Parental consent systems must therefore evolve beyond simple "yes/no" gating mechanisms and move toward dynamic consent architectures that reflect the child's growing capacity and the changing nature of digital risk.

H.7.11 Features such as consent dashboards, revocable tokens and event-triggered notifications (e.g. when a child attempts to use a new feature or app) offer pathways to more nuanced, rights-respecting models.

| Static vs. dynamic consent models table

H.7.12 These are examples of static vs dynamic consent models:

Provider	Consent Model	Evidence / Notes
Apple	Static	Consent via Family Sharing; no expiry or renewal mechanisms observed. No revocation features.
Epic Games KWS	Partially Dynamic	Offers real-time parent approvals and configurable permissions; some support for per-feature access control.
Google	Static	Family Link consent is granted at account setup; changes require full reconfiguration, not dynamic renewal.
k-ID	Partially Dynamic	Supports consent tokens and revocation signals but relies on relying parties to implement expiry logic.
PRIVO	Dynamic	Offers scoped, revocable consent via parent dashboard; supports time-limited and contextual approvals.
R2 Labs	Dynamic	Issues revocable, cryptographic tokens tied to child identity; designed for context-bound, expiring access.
Sedicii	Dynamic	Enables privacy-preserving, event-triggered access based on parental authorisation; no static binding assumed.
TrustElevate	Dynamic	Supports revocable, per-feature consent tokens; aligned with evolving capacity principles.

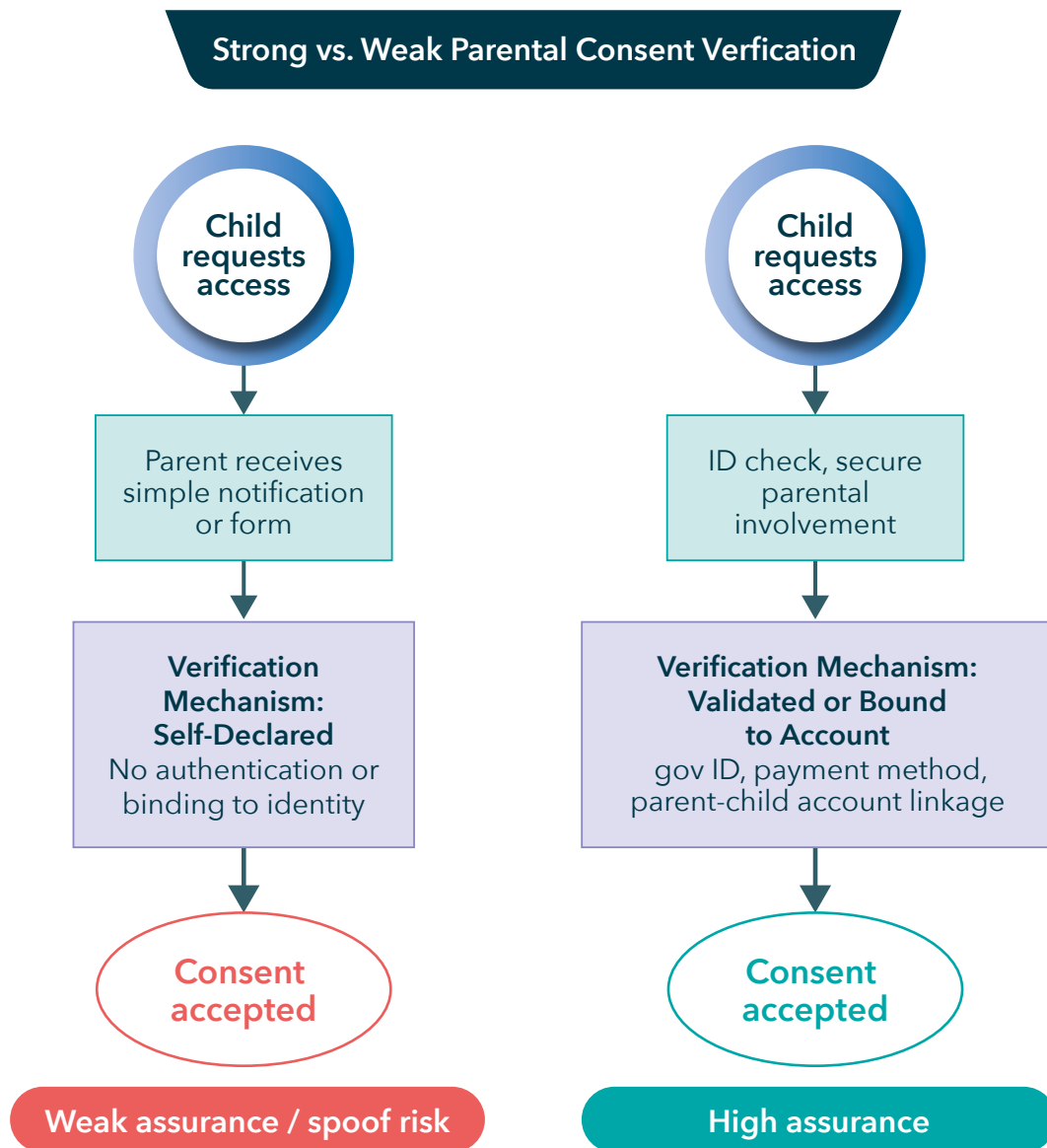


Figure H.7.1 Strong vs. Weak Parental Consent Verification

H.8 Policy and Technological Readiness

H.8.1 From a technological perspective, the Trial found no substantial technological limitations to the implementation of parental consent mechanisms in Australia. Participants demonstrated a variety of functional approaches, including email-based confirmation loops, payment verification, mobile authentication and third-party identity checks. These systems were capable of capturing, storing and transmitting verifiable consent signals in a way that could be integrated into digital service workflows.

H.8.2 Service providers and policymakers showed thoughtful engagement with the problem space, particularly in contexts involving children under key regulatory thresholds. Consent systems were typically deployed at decision points – such as registration, content access or purchase – and offered flexible triggers for obtaining adult approval.

H.8.3 However, legal and policy alignment remains less developed. In the absence of a national standard for verifying parental identity or defining how long consent records should be retained, questions remain about:

- The legal sufficiency of self-asserted consent
- The privacy implications of persistent consent logs
- And the extent to which providers can reliably demonstrate compliance with evolving child privacy and data protection laws

H.8.4 Further clarity may be needed to support consistent implementation, especially where consent mechanisms are used to satisfy regulatory requirements around children's data, access controls or digital participation.

H.8.5 Parental consent mechanisms – when well designed, verifiable and aligned with children’s rights – offer a compelling, human-centred approach to managing children’s experiences in digital environments. While implementation challenges exist, the foundational logic of verified parental consent is strong: it is user-aware, ethically grounded and technically feasible. In an ecosystem increasingly reliant on automated systems to govern access, verified parental consent stands out as a mechanism that respects human agency, protects children and builds shared responsibility between platforms, families and policymakers.

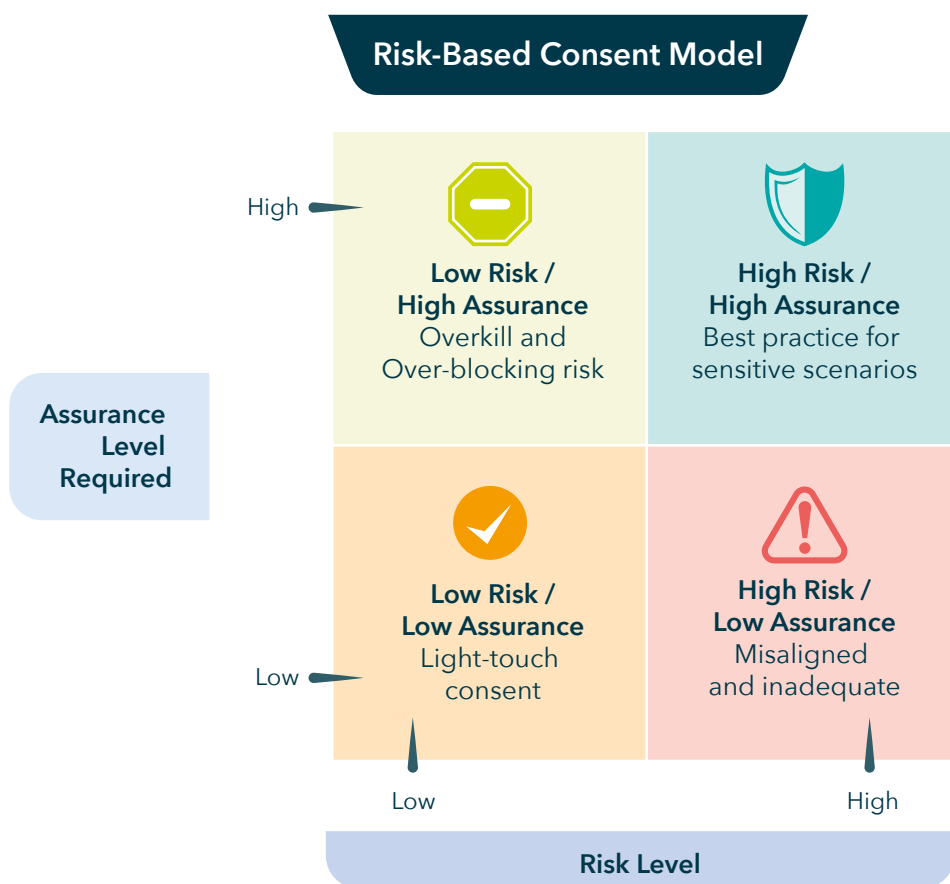


Figure H.8.1 Risk-Based Consent Model

H.8.6 Critical risk factors in parental consent need to be considered:

1. **Human oversight at critical decision points**

Unlike automated age gates or inferred signals, parental consent places a real person – usually someone who knows the child intimately – at the centre of the decision. This supports more contextual and ethical judgments about access to services, platforms or content. Rather than guessing age or maturity, the system explicitly invites a parent or guardian to participate in a decision aligned with the child’s needs, family values and developmental stage.

2. **Legal clarity and ethical alignment**

Verified parental consent aligns well with established legal doctrines in child protection and privacy, including:

- COPPA (in the U.S.)
- Article 8 of the GDPR⁶ (in the EU)
- And similar protections under Australia’s Privacy Act

These frameworks recognise that children require additional safeguards and that parental authority can provide a lawful basis for data processing or digital access in a way that age estimation alone cannot.

6. *The General Data Protection Regulation was put into effect by the European Union on 25th May 2018. Though passed by the EU, it imposes obligations onto organisations anywhere, so long as they target or collect data related to people in the EU.*

3. **Trust and transparency between families and platforms**

Consent mechanisms create a traceable interaction between the platform and the family. This opens up channels for transparency, giving parents:

- Clear notice of what the child wants to do
- Control over whether to allow it
- Visibility into how their child's data and engagement are being handled

This two-way model can build greater trust in online services, particularly where automated systems may seem opaque or unaccountable.

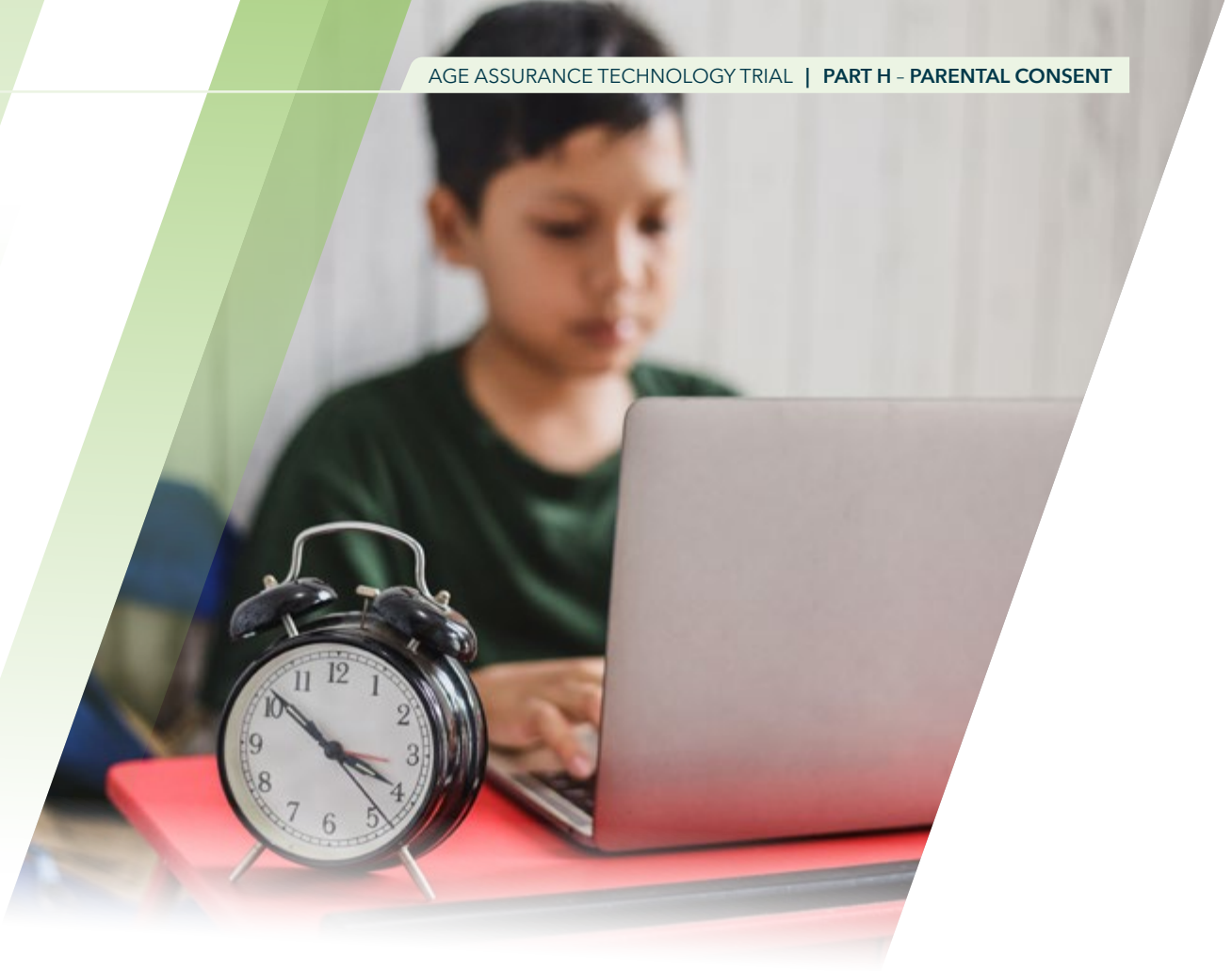
4. **Flexibility across risk contexts**

Parental consent mechanisms create a traceable interaction between the platform and the family. This opens up channels for transparency, giving parents clear notice of what the child wants to do, control over whether to allow it and visibility into how their child's data and engagement are being handled. Importantly, consent mechanisms are typically triggered at the point of access – such as during registration, content selection or purchase – meaning they are highly proximate to the moment of risk.

As discussed in Part J (Tech Stack), this risk-proximity is critical: systems that intervene too early or too generically may fail to capture meaningful risk, while those that respond too late may allow harmful exposure. Parental consent offers one of the most situationally aware, timely and proportionate mechanisms for involving a parent or guardian in a child's digital experience – particularly where the risk relates to content maturity, peer interaction or data disclosure. It enables real-time, human judgement precisely when it matters most.



Cross Reference: Part J - Tech Stack



5. **Compatibility with evolving identity and credential ecosystems**

Modern consent frameworks (e.g. PRIVO, TrustElevate, R2 Labs) increasingly use digital credentials, tokens and verifiable identifiers. This makes parental consent interoperable with existing digital identity ecosystems, potentially allowing for:

- Consent to be scoped and time-limited
- Access to be revoked easily
- Audit trails to be maintained securely and efficiently

Such technical maturity shows that verified parental consent can scale with future platform architectures and privacy standards.

6. **Respect for family autonomy and diverse parenting models**

At its best, parental consent empowers families to make decisions on their own terms, respecting cultural norms, religious beliefs and parenting styles. It avoids a one-size-fits-all approach and allows parents and guardians – not algorithms – to decide what's appropriate for their child.

H.9 Lack of Recognition for Evolving Child Capacities and Rights

H.9.1 As with parental controls, few systems demonstrated adequate recognition of the evolving capacities and rights of children, particularly adolescents. In many implementations, consent mechanisms did not provide a way for the child to be involved in or informed about the decision, nor did they consider the balance between protection and participation as outlined in the UN Convention on the Rights of the Child (UNCRC). In most cases, the consent of the child was assumed and ongoing and there was little opportunity for children to revoke consent, even if their parents had not.

H.9.2 Risks of circumvention were observed, particularly where children could easily create multiple accounts, spoof age declarations or bypass consent requests using alternative devices. Without robust identity binding and session controls, consent systems risk being tokenistic or ineffective in real-world application.

H.9.3 One of the most significant shortcomings observed in the Trial was the limited recognition by parental consent systems of the evolving capacities of children, particularly adolescents. While the requirement for parental consent is essential in safeguarding younger users, many systems failed to balance this protective function with the child's growing autonomy and right to participate in decisions affecting them – principles enshrined in Article 5 and Article 12 of the UN Convention on the Rights of the Child (UNCRC).

H.9.4 In most cases, once parental consent was granted, the child user was neither informed nor actively involved in the decision and there were no mechanisms to allow the child to object or revoke that consent. This lack of transparency toward the child effectively rendered their agency invisible within the process. It also creates an imbalance between the right to protection and the right to participation, privacy and freedom of expression – especially for adolescents nearing the threshold of legal independence.

H.9.5 International guidance, including ISO/IEC 29184, highlights the need for accessible, understandable and age-appropriate notices in consent processes. While many systems did provide clear interfaces for the parent or guardian, there was little evidence that these principles were extended to child users themselves. This absence undermines the educational value of the consent process and weakens digital literacy by failing to involve children in discussions about their rights, data use or permissions.



H.10 Risks of Circumvention and Identity Weaknesses

H.10.1 The Trial also identified common circumvention vectors in systems that did not implement strong identity binding or session management. In particular:

- Children were able to bypass consent mechanisms by creating multiple accounts, either on the same platform or across devices
- Some systems relied solely on self-declared age, without verifying the declared birth date or linking it to any persistent identifier
- In shared device environments (such as tablets or home computers), it was possible for children to use an authenticated session established by an adult, thereby skipping the consent process entirely

H.10.2 These issues reflect a lack of binding between the consent token and the individual child user, a critical technical requirement for effective and enforceable parental consent. Without strong session controls, authentication measures or behavioural analysis to detect inconsistent activity, parental consent risks becoming a symbolic step rather than a meaningful safeguard.

H.10.3 To prevent circumvention and reinforce user trust, systems should:

- Implement session-level identity validation, especially when toggling between child and adult profiles
- Use device fingerprinting, behavioural analysis or secure tokens to persistently associate consent with a specific user and context
- Enable child-facing dashboards or interfaces to increase transparency and allow children to understand, question or withdraw consent in age-appropriate ways

H.10.4 To address these concerns, future development of parental consent systems should:

- Acknowledge and implement the evolving capacities principle by enabling co-consent or consultation models for older children
- Introduce granular and revocable consent options, including those initiated by the child themselves
- Provide child-friendly notices and feedback loops explaining what consent means, how it affects them and how they can exercise their rights
- Strengthen identity binding and circumvention resistance, especially for services operating near critical age thresholds (e.g., under 13 or under 16)

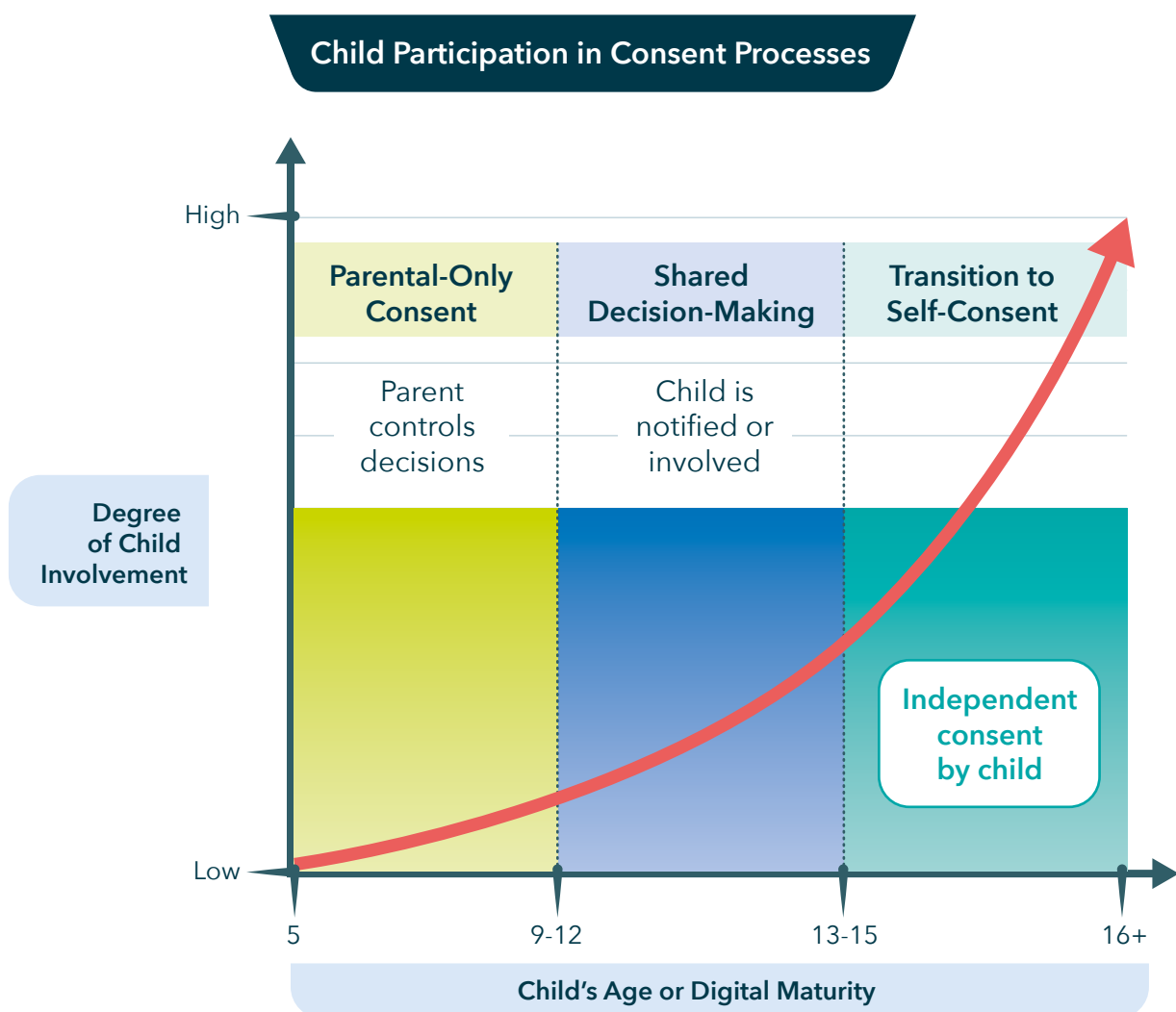


Figure H.10.1 Child Participation in Consent Processes – Maturity Curve

Vendor Case Study



Website

trustelevate.com

TrustElevate participated in the Trial as a provider of identity and age assurance services with built-in parental consent mechanisms. Unlike many systems that treat parental consent as a static, one-time gatekeeping event, TrustElevate's approach demonstrated a clear awareness of the evolving capacities of children, as recognised in the UN Convention on the Rights of the Child (UNCRC).

Three Key Facts

1

Relies on robust identity verification of both parent and child, using verifiable credentials issued through secure, privacy-preserving methods.

2

Supports revocable consent tokens, allowing parents to withdraw permission or update boundaries as circumstances change.

3

Instead of granting or denying access to a service in total, parents can authorise use of specific components.

Practice Statement

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

Technology Trial Test Report

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

Privacy Policy

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

Technology Trial Interview

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

Summary of Results

TrustElevate demonstrates that parental consent systems can go beyond static permission models to reflect the realities of children's development, digital participation and rights. While not all features are currently active, the system architecture, documentation and design intent strongly reflect best practice principles.

H.11 Practice Statements and the Current State of Parental Consent Design

H.11.1 Although ISO/IEC FDIS 27566-1 – the standard underpinning practice statement development in the Trial – explicitly excludes parental consent from its functional scope, several participating providers nonetheless submitted voluntary descriptions of how they manage parental consent in practice. These statements were not subject to formal certification and varied in depth and format, but they offer a useful snapshot of how parental consent is currently being approached across different sectors.

H.11.2 Across the submissions, several common features were observed:

- Clear articulation of consent capture points, typically following an age declaration or inference
- Use of standard communication channels, such as email, pop-up requests or linked device approvals
- Data minimisation practices, including use of tokenised or hashed records to store consent outcomes
- Reliance on self-declared authority, where consent is granted by an adult whose relationship to the child is not independently verified

H.11.3 These approaches reflect a general trend toward low-friction consent mechanisms that favour speed and usability, particularly at onboarding or registration stages. In lower-risk contexts, such models may be sufficient to meet basic legal requirements.

H.11.4 However, the statements also revealed some emerging points of good practice and growing awareness of ethical and rights-based considerations:

- A few providers referenced revocation pathways or dashboard interfaces that allow parents to review and update consent over time
- Some described mechanisms for scoped or feature-specific permissions, which allow more granular control than simple all-or-nothing approval
- One or two referenced alignments with international frameworks, such as ISO/IEC 29184 or the UNCRC, particularly in recognising the importance of transparency and informed choice

H.11.5 Notably, while most practice statements were written with the parent or service provider as the primary user, there was limited detail on how children themselves were involved in the process – either through child-facing notices, information about consent outcomes or opportunities to object or participate. As discussed in earlier sections, this remains a key area for future development.

H.11.6 Overall, the practice statements point to a sector in transition: moving from basic, compliance-oriented models toward more dynamic, rights-aligned systems. While no single provider demonstrated full maturity across all dimensions of best practice, the statements submitted to the Trial show increasing attention to:

- Data minimisation and verifiability
- Modular and context-aware consent
- And the broader ethical obligations of involving parents and children in meaningful, proportionate ways

H.11.7 As standards evolve and interoperability frameworks emerge, practice statements may play a valuable role in codifying sector norms, benchmarking consent maturity and guiding continuous improvement in this space.

H.11.8 Analysis table of practice statements

Provider	Consent Capture Method	Data Minimisation	Verifiability of Parent Identity	Revocation Support	Child Participation or Notification	Granular / Feature Consent
Apple	Family Sharing email approval	Moderate	Weak	None	No	No
Epic Games KWS	Pop-up approval, ParentGraph	Good	Moderate	Partial	No	Yes
Google	Credit card validation via Family Link	Moderate	Moderate	Manual only	No	No
k-ID	Credential token approval	Good	Depends on RP	Signalled, RP dependent	Yes, where parental consent requested by child	Depth of implementation determined by RP
PRIVO	Email/ID/ payment verification	Good	Strong	Full dashboard	Planned	Yes
R2 Labs	Cryptographic tokens	Strong	Strong	Token-based	No	Yes
Sedicii	Zero-knowledge signals	Strong	Moderate	Token-based	No	Yes
TrustElevate	Feature-level consent token	Good	Strong	Supported	Planned	Yes

H.12 Security and Integrity of Parental Consent Mechanisms

H.12.1 Parental consent systems rely on the secure identification of a parent or guardian, the binding of that authority to the correct child and the issuance of a valid, enforceable signal authorising access to age-restricted services. The Trial found that while many systems demonstrated strong user experience design, security assurance varied considerably, with some implementations more vulnerable to impersonation, circumvention or unauthorised access than others.

H.12.2 For parental consent systems to be effective and trustworthy, the following steps are essential to consider:

- Authentication of the consenting party: Linking the adult providing the consent to a real-world identity, ideally confirmed through multi-factor authentication, credential checks or payment verification
- Binding between child and guardian: Reliably establishing that the consenting adult has legal or custodial authority over the specific child user – not just general access to the device or account
- Tamper-proof consent signals: Once issued, cryptographically securing consent signals and resisting them to replay, forgery or man-in-the-middle interception
- Secure data transmission and storage: Encrypting any data associated with consent – including tokens, audit trails or confirmation logs in transit and at rest, with role-based access controls applied
- Revocation and audit integrity: Supporting revocation and dispute resolution via consent logs and status flags, without enabling manipulation or deletion by unauthorised actors

| Risks identified

H.12.3 The Trial observed several implementation risks, including:

- Self-declared consent without robust authentication (e.g., entering any email address and clicking a link)
- No verification of parent-child relationship, relying solely on shared devices or accounts.
- Lack of integrity checks on consent tokens, meaning they could be reused or spoofed
- No support for revocation or rollback, even in cases of error or dispute.

H.12.4 These gaps raise concerns under both privacy law and child safety frameworks. A failure to secure consent workflows could result in unauthorised access by children, misuse of parental credentials or breaches of legally required protections.

H.12.5 Security is not an optional feature of parental consent – it is foundational. Without robust controls to authenticate the parent, bind to the child and protect the integrity of the consent signal, these mechanisms risk being easily bypassed or abused. Future development must prioritise security as a core function, supported by encryption, credentialing frameworks and tamper-resistant protocols that uphold both legal and ethical responsibilities.

| Summary of security and privacy claims by a sample of providers

H.12.6 This is a summary of security and privacy claims by a sample of providers:

Provider	ISO 27001 Certified	SOC 2 Type II	Other Certifications or Claims	Key Security Measures
PRIVO	Yes (BSI Certified)	Yes (4 years, A-LIGN)	EU-US DPF , PAS 1296 ⁷ (in progress), PCI bi-monthly audit	Encryption at rest, SSL ⁸ transmission, data minimisation, quarterly security board review
Sedicii	Yes (2022)	Not listed	Penetration testing	HTTPS default, encrypted storage, Privacy by Design, inclusive policies
Qoria	Aligned with NIST	SOC 2 ⁹ aligned	Not stated	Encryption, anonymised usage data, regular privacy reviews, NIST-based security protocols
SafeGen	In progress (ISO 27001 & ISO/IEC FDIS 27566-1)	Not listed	GDPR, COPPA alignment; ACCS certification planned	Token-based authentication, data minimisation, hashed data, no biometric or PII retention
k-ID	In progress (ISO 27001 & 27701)	In progress	ESRB privacy certified Kids Seal , ACCS 0:2021 & 3:2021	No child PII stored, DSR-enabled ¹⁰ , encrypted access, role-based control

7. PAS 1296:2018 is a Code of Practice for Online Age Verification service providers developed by the British Standards Institute and the Digital Policy Alliance.
8. SSL stands for Secure Sockets Layer. It's a cryptographic protocol that establishes a secure, encrypted connection between a user's browser and a server.
9. 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.
10. This means Data Subject Access Request-enabled.

H.13 Innovation and Emerging Practices in Parental Consent Systems

H.13.1 We identified ongoing vibrancy, creativity and innovation within the parental consent ecosystem, driven by demand from platforms, service providers and regulators seeking to ensure compliant and age-appropriate access in increasingly complex digital environments. While parental consent mechanisms are a well-established requirement under data protection and child safety laws, the Trial observed a renewed focus on usability, trust and seamless integration across services.

H.13.2 Within many digital services, parental consent functionality is beginning to be more deeply embedded into registration flows, identity verification processes and account management interfaces, with the goal of reducing friction while ensuring validity. Some providers are exploring real-time consent prompts, digital credentialing and token-based consent signals to improve both the user experience and compliance assurance. These emerging approaches aim to support clearer communication with guardians and to reduce administrative complexity for platforms.

H.13.3 The Trial identified ongoing innovation and active development within the parental consent ecosystem, responding to rising expectations from platforms, service providers, regulators and caregivers for secure, usable and compliant consent workflows. Although parental consent requirements have long been embedded in legislation – such as under Australia’s Privacy Act, COPPA in the United States or GDPR in the EU – what is changing is the design maturity and integration depth of these mechanisms.

H.13.4 Providers participating in the Trial demonstrated new approaches to embedding consent into existing user journeys, such as:

- Integrated registration flows where age is declared or inferred and, if under a threshold, a parent or guardian is prompted in real-time for consent via linked devices or family account structures
- Token-based consent signals, where an authenticated parent triggers a consent payload that is temporarily stored, cryptographically secured and made available to the relying service – without storing full PII (personally identifiable information)
- Digital wallet integration for parental consent credentials: one Trial participant showed how consent can be issued as a verifiable credential that the child can store and present when required, reducing the need for repeated re-validation across services
- Real-time confirmation mechanisms, such as one-time passcodes (OTP) sent to a parent's device, which link the approval action to both the child's session and the adult's identity in a short-lived, auditable format

H.13.5 For example, one provider deployed a micro-payment verification model: when a child attempted to register for an online service, a nominal charge (e.g. \$0.01) was applied to a credit card registered to an adult. The process served both to verify the adult's age and establish a proof-of-consent record while refunding the charge immediately. This method is widely considered acceptable under global data protection guidance, where more robust verification is required for high-risk services.

H.13.6 Another platform adopted progressive consent flows, in which guardians could set content-level permissions (e.g., video chat, messaging, location sharing) rather than granting full access. These controls could be reviewed and adjusted over time – aligning better with the principle of evolving capacity under the UNCRC and offering a granular model of child autonomy.



Epic's Kids Web Services (KWS)

Epic's Kids Web Services (KWS) supports a federated approach to parental consent across participating games and platforms. It was one of the few systems in the Trial to demonstrate:

- Real-time parental consent prompts triggered dynamically when a child attempts to engage with age-gated features.
- Multiple verification methods, including email confirmation, micro-payment and integration with credentialing services like ParentGraph.
- Feature-level configuration, allowing guardians to set permissions across different gameplay or communication functions (e.g., voice chat, messaging).
- An API-first architecture, enabling third-party developers to reuse consent status across platforms without re-verifying the parent.

While Epic's model still relies on external partners to maintain the child-parent binding over time, its implementation demonstrated high usability, risk responsiveness and good integration with age verification signals – a strong example of embedded, event-triggered consent workflows that reduce friction without sacrificing oversight.

| Reducing friction and enhancing trust

H.13.7 The trend observed across submissions was a shift away from single-instance, email-only consent requests toward multi-factor, integrated and time-sensitive systems. This reflects both technological maturation and an acknowledgment that guardians often expect:

- Clear visibility over what their child is engaging with
- Confidence that consent is meaningful, not merely a formality
- Minimal administrative burden, especially when managing consent across multiple platforms

H.13.8 Providers highlighted that improvements in parental trust correlated with transparency of communication - e.g., simple language in consent prompts, context-aware risk descriptions and explainer overlays for both children and adults. These design choices enhance informed decision-making and help avoid the common pitfalls of passive or uninformed approval.

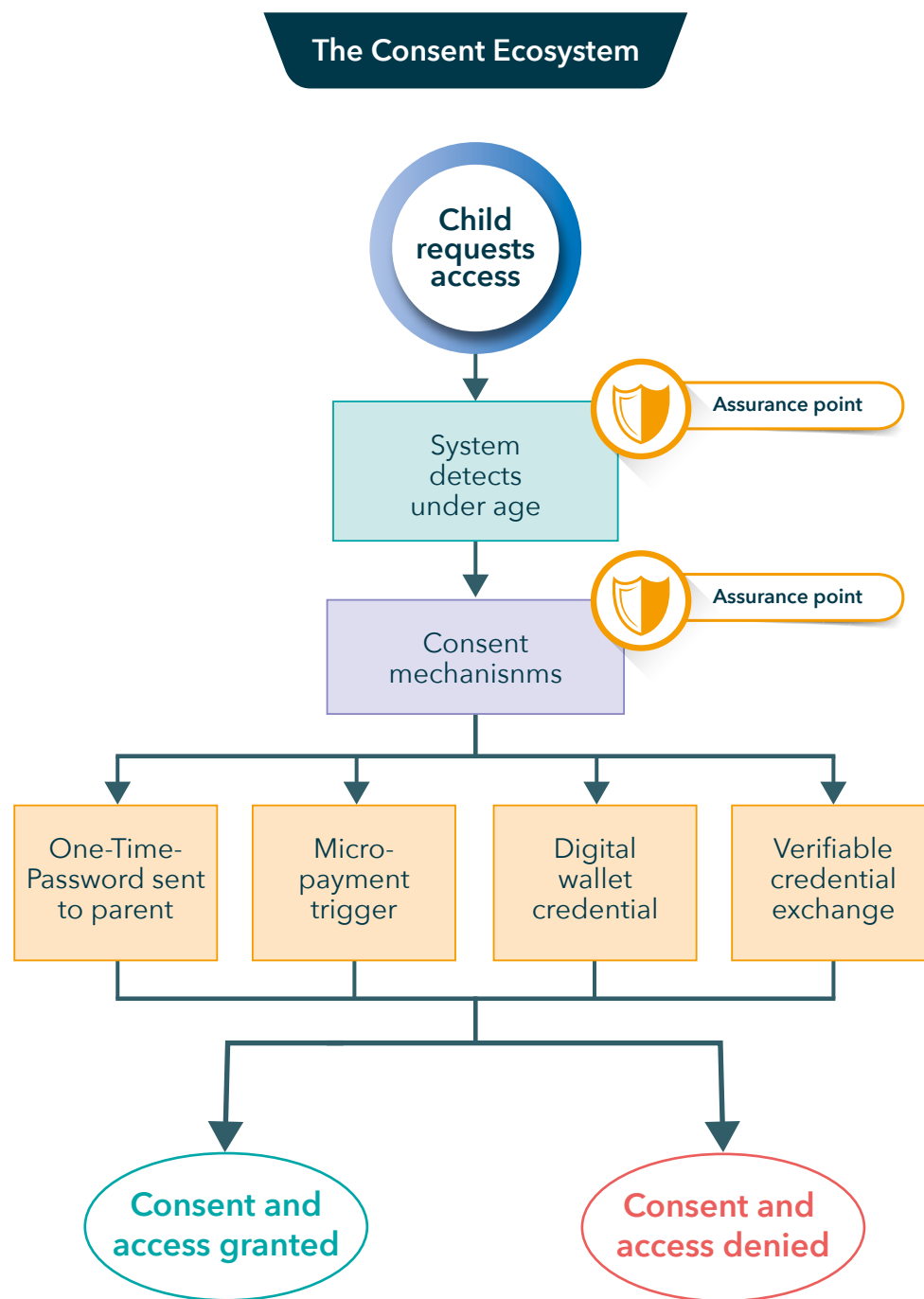


Figure H.13.1 Consent Ecosystem Flowchart



k-ID - Consent Tokens and Interoperable Identity Signals

k-ID presented a novel intermediary model built around child-centric digital credentials.

The system issues a verified identity and consent token for each child, which can then be presented to participating services.

Key features include:

- Verifiable parental consent signals, issued via the k-ID platform, using trusted account credentials and optional document checks.
- Token-based interoperability, allowing a child to access multiple services without re-requesting consent – provided the token remains valid.
- Auditability and selective disclosure, where relying parties receive only the minimum necessary signal (e.g., “parental consent granted”), not full personal data.
- Support for revocation and session expiry, although implementation is dependent on the third-party service integrating the token.

While k-ID does not directly handle child-facing interfaces, it is a promising identity-layer solution that prioritises privacy, scalability and technical flexibility – especially well-suited for app ecosystems or multi-platform child services.

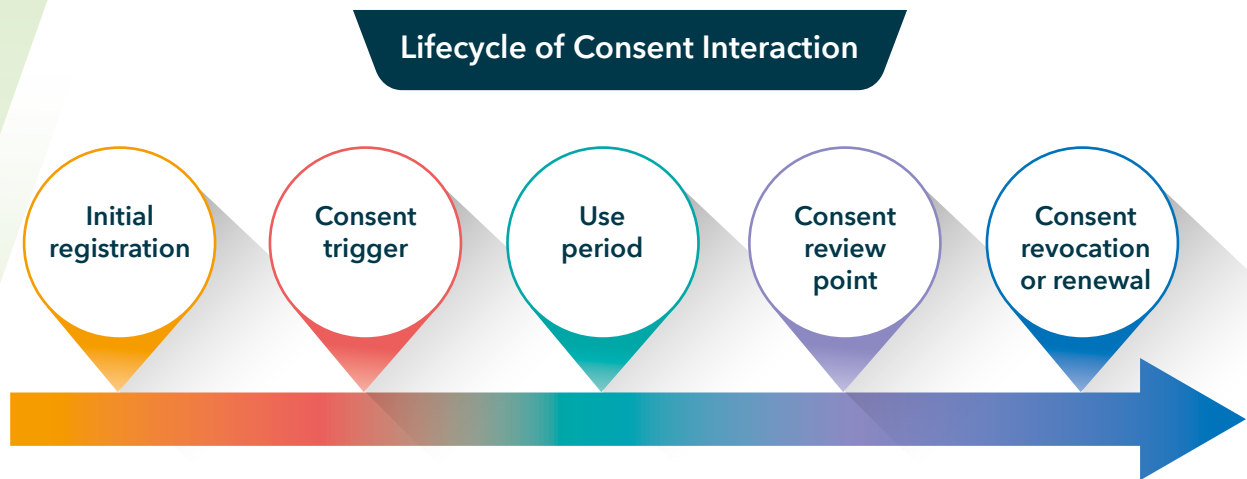


Figure H.13.2 *Lifecycle of Consent Interaction*

| Implications for best practice and standardisation

H.13.9 These developments align closely with the guidance in ISO/IEC 29184:2020, which outlines best practices for online privacy notices and consent mechanisms, including:

- Real-time consent prompts and clear notice prior to data collection
- Multi-layered transparency to ensure both adult and child users understand the implications
- Time-bound consent lifecycles, with the ability to revoke or modify permission
- Interoperable consent records, potentially delivered via verifiable credentials or federated identity frameworks

H.13.10 As these systems mature, service providers should continue to evaluate and test usability, inclusivity and child rights compliance, especially where AI-driven systems or cross-platform tokens are used to manage consent signals at scale.

H.14 Data Handling and Privacy Practices in Parental Consent Systems

H.14.1 The Trial found that most parental consent systems implemented privacy-conscious data handling practices, particularly at the point of consent capture. In contexts where children required guardian approval to access services, providers applied a range of technical and procedural safeguards to protect both child and parent information – consistent with Australian privacy principles and international standards such as ISO/IEC 29184.

H.14.2 Across practice statements and technical submissions, the following trends were observed:

1. **Data separation and role clarity**

Many systems maintained a clear separation between:

- Verification data (e.g. parent contact info)
- Consent metadata (e.g. timestamp, method used)
- Child operational data (e.g. platform usage post-consent)

This separation reduces risk of misuse or overreach – particularly where consent data could otherwise be misapplied to analytics, advertising or profiling.

Vendor Case Study

**R2LABS**

Website

r2-labs.io

R2 Labs provides consent tokens tied to child identity using cryptographic proofs; supports revocation but not ongoing behavioural oversight or content filtering.

Three Key Facts

1

Temporary logs (e.g. OTPs) are automatically deleted within 30 days, ensuring minimal data retention.

2

Consent tokens are cryptographically signed/stored client-side, enabling real-time validation without exposing parental or child identity to third-party services.

3

Tokens are valid only for a limited duration, after which access is automatically denied unless refreshed – reinforcing time-bound and revocable consent.

Strengths

- Avoids static, permanent consent states,
- Provides meaningful withdrawal functionality,
- Enables low-friction, privacy-first compliance without sacrificing parental control.

Practice Statement

ageassurance.com.au/v/r2l/#PS

Privacy Policy

ageassurance.com.au/v/r2l/#PP

Technology Trial Test Report

ageassurance.com.au/v/r2l/#TR

Technology Trial Interview

ageassurance.com.au/v/r2l/#VI

Summary of Results

The system balances auditability (via immutable logging) with user rights (via revocable mechanisms), offering a compelling model for future adoption.

2. **Data minimisation and pseudonymisation**

Providers generally collected only what was necessary to establish consent – such as a parent’s email address, a one-time payment token or confirmation of relationship. Several participants issued pseudonymised consent tokens, allowing third-party platforms to validate the existence of valid consent without receiving personal identifiers.

In one case, a provider used cryptographically signed, short-lived tokens, stored client-side, to enable access without transmitting parental data to external systems – a strong example of privacy-by-design in action.

3. **Storage, access control and retention**

Consent records were typically stored in encrypted, access-controlled environments, with access limited to authorised staff or systems. However, retention policies varied widely. In many cases, consent was treated as indefinite, with no built-in expiry, sunset clause or re-validation mechanism – raising potential concerns about data over-retention or long-term consent drift.

4. **Opportunities for improvement**

While consent capture itself was generally privacy-aware, several systems lacked:

- Dashboards for parents to manage or withdraw consent
- Automated expiry or re-validation logic tied to the child’s age or changing use
- Child-facing transparency about how their data was governed post-consent

These limitations suggest that while technical safeguards were strong at the point of collection, consent lifecycle management remains underdeveloped – particularly in systems that treat consent as a one-time event.



Figure H.14.1 Consent Data Lifecycle

H.15 Inclusivity and Guardianship Complexity in Parental Consent Mechanisms

H.15.1 The Trial found that parental consent mechanisms generally operate consistently across demographic groups in terms of technical design and service implementation. However, variability in family structures, cultural norms and legal guardianship arrangements significantly affects how these mechanisms function in practice. Most systems assume a conventional model in which a parent or guardian is readily available, digitally literate and legally authorised to provide consent on behalf of the child. While this may hold true for many families, such assumptions do not always reflect the realities of more complex care arrangements.

H.15.2 A notable challenge arises in the context of children in out-of-home care (OOHC), including those in foster care, kinship care or residential care. In these situations, consent may need to be provided by an authorised carer, child safety officer or other state-appointed guardian, rather than a biological parent. The Trial found that most parental consent systems do not currently account for this distinction, offering limited flexibility to reflect diverse legal guardianship models. This creates risks of either unauthorised individuals providing consent or eligible carers being excluded from the process due to system constraints.

H.15.3 Furthermore, digital services often lack mechanisms for verifying or registering alternative consent authorities, such as a government agency or a designated key worker. As a result, children in looked after care may face barriers to accessing age-appropriate digital services or may be inadvertently excluded from online experiences that their peers can access with ease. This can reinforce existing digital inequalities, particularly for children already experiencing social, emotional or educational disadvantage.

H.15.4 Culturally, the Trial also observed that assumptions about parent-child relationships may not align with the lived experiences of children in some Indigenous and multicultural communities. For example, caregiving responsibilities may be shared among extended family or community members who may not be recognised by formal consent systems. Without mechanisms to reflect these broader understandings of guardianship, well-intentioned consent requirements risk becoming exclusionary or administratively burdensome.

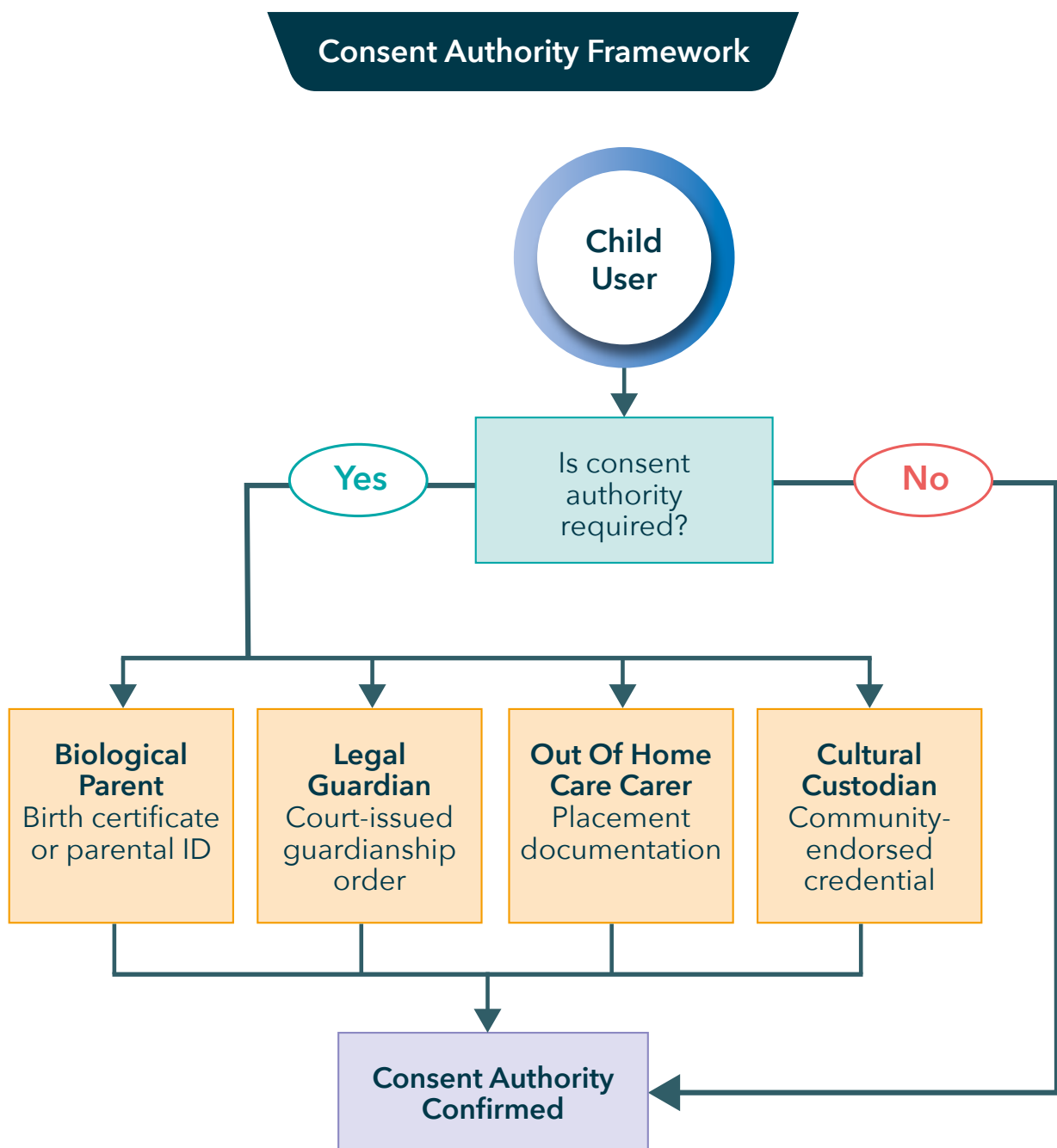


Figure H.15.1 Consent Authority Framework

H.15.5 The Trial found that while parental consent mechanisms were generally technically consistent across demographic groups, their practical implementation often failed to account for the diversity of family structures, caregiving models and legal guardianship arrangements in Australia. This has significant implications for the accessibility, fairness and real-world effectiveness of consent-based age assurance systems.

| Assumptions of the conventional parent-guardian model

H.15.6 Most of the systems examined in the Trial operated under a default assumption: that a child's legal guardian is a digitally literate biological parent, readily available and clearly authorised to give consent. While this may be true for many families, it does not reflect the full range of family circumstances, particularly those involving complex caregiving arrangements or state involvement.

H.15.7 This narrow design framework results in reduced inclusivity, inadvertently excluding or disadvantaging families where digital access is shared, legal authority is delegated or caregiving is communal or dynamic. In practice, many systems lacked configurable options for recognising alternative legal guardianship, such as kinship carers, grandparents or culturally recognised custodians.

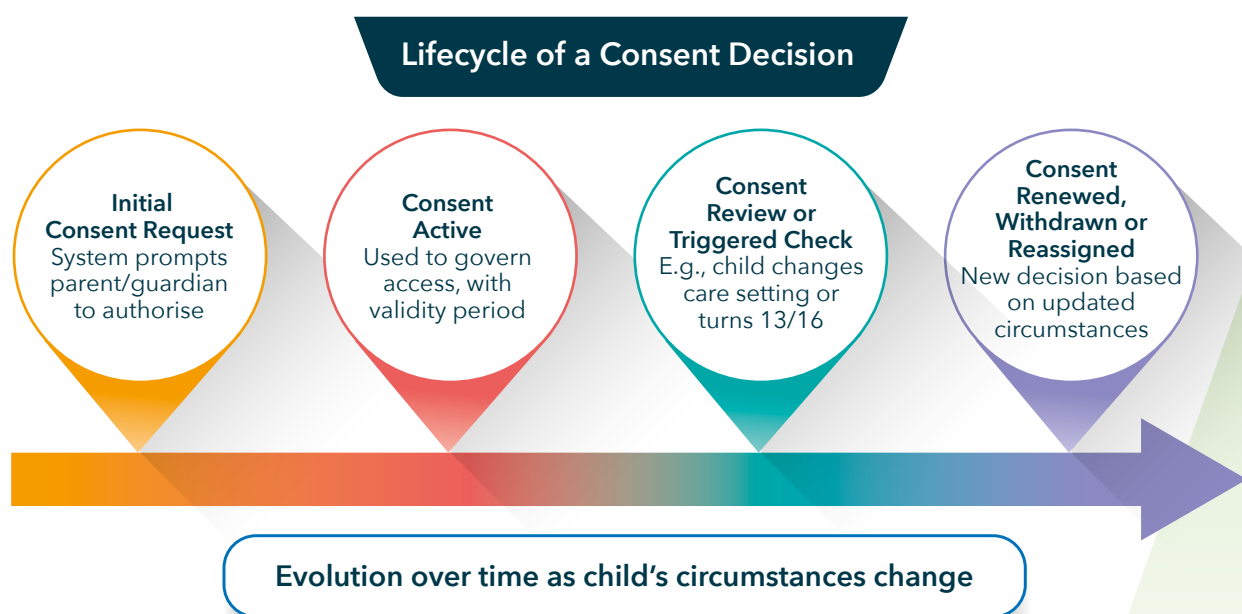


Figure H.15.2 Lifecycle of a Consent Decision

| Children in Out-Of-Home Care (OOHC)

H.15.8 A significant cohort affected by these limitations are children living in Out-of-Home Care (OOHC), including foster care, kinship care and residential care arrangements. In such cases, parental responsibility may reside with state-appointed carers, child protection authorities or designated case workers – not the child’s birth parents.

H.15.9 The Trial found that few if any parental consent systems were capable of:

- Registering or verifying consent from authorised government or NGO carers
- Providing flexible user interfaces for uploading supporting documentation
- Offering role-based access that distinguishes between legal guardian types

H.15.10 This absence of flexibility introduces two critical risks:

- Unauthorised consent may be given by an individual with no formal authority
- Barriers to access may prevent children from using age-appropriate services because the system does not recognise their carer as a valid consentor

H.15.11 This gap may exacerbate digital exclusion among already vulnerable children, contributing to wider inequalities in access to education, entertainment, communication and support services.

Gaps in Consent Recognition for Out-of-Home Care



Figure H.15.3 Gaps in Consent Recognition for Out-of-Home Care

| Cultural Variability in Guardianship

H.15.12 Beyond formal legal guardianship, the Trial also identified cultural mismatches between mainstream parental consent mechanisms and the caregiving practices of First Nations and multicultural communities. In many Aboriginal and Torres Strait Islander Peoples communities, caregiving is often shared across extended family networks and is shaped by deep cultural obligations and communal responsibility.

H.15.13 Current parental consent models do not adequately support:

- Multiple concurrent carers, such as aunties or grandparents, recognised by community but not by law.
- Community-based guardianship, where no single individual holds exclusive parental authority.
- Respect for culturally grounded parenting models, which may not map neatly onto Western-style account structures.

H.15.14 As a result, consent workflows may be confusing, exclusionary or misaligned with the realities of care, leading to either denial of access or pressure to fabricate consent via workaround methods (e.g., misdeclaring relationship roles).

H.15.15 To ensure inclusive, lawful and equitable parental consent systems, developers and policymakers should consider:

- Implementing role-based access controls that allow for flexible assignment of guardian rights.
- Supporting case manager consent protocols through integration with verified registries of OOHHC carers.
- Enabling multi-carer approval pathways to reflect community caregiving structures.
- Designing culturally sensitive interfaces with community-informed language and guidance.

H.16 Systemic Challenges and Opportunities in the Development of Parental Consent Mechanisms

H.16.1 The Trial identified several key challenges in the development of parental consent systems. Many require real-time communication, identity verification and secure consent record storage, but current digital identity infrastructure and credentialing systems remain fragmented, making implementations complex and difficult for both families and providers.

H.16.2 Emerging solutions – such as digital wallets, verified credentials and in-app dynamic consent frameworks – show promise for enabling more flexible, portable and secure consent experiences, especially across platforms. However, concerns remain about persistent logging of consent events, which could contribute to long-term digital profiling of children and families if not properly governed.

H.16.3 To ensure these systems evolve effectively, greater interoperability, privacy safeguards and alignment with diverse caregiving arrangements will be essential. Continued innovation must focus on creating consent mechanisms that are adaptive, inclusive and respectful of both the child's rights and the family's context.

H.16.4 The Trial identified a number of structural and implementation challenges associated with the current and emerging landscape of parental consent systems. As digital services increasingly require verifiable consent mechanisms for compliance with child safety and data protection laws, the limitations of today's infrastructure and identity ecosystems pose meaningful barriers to usability, scalability and child-rights alignment.

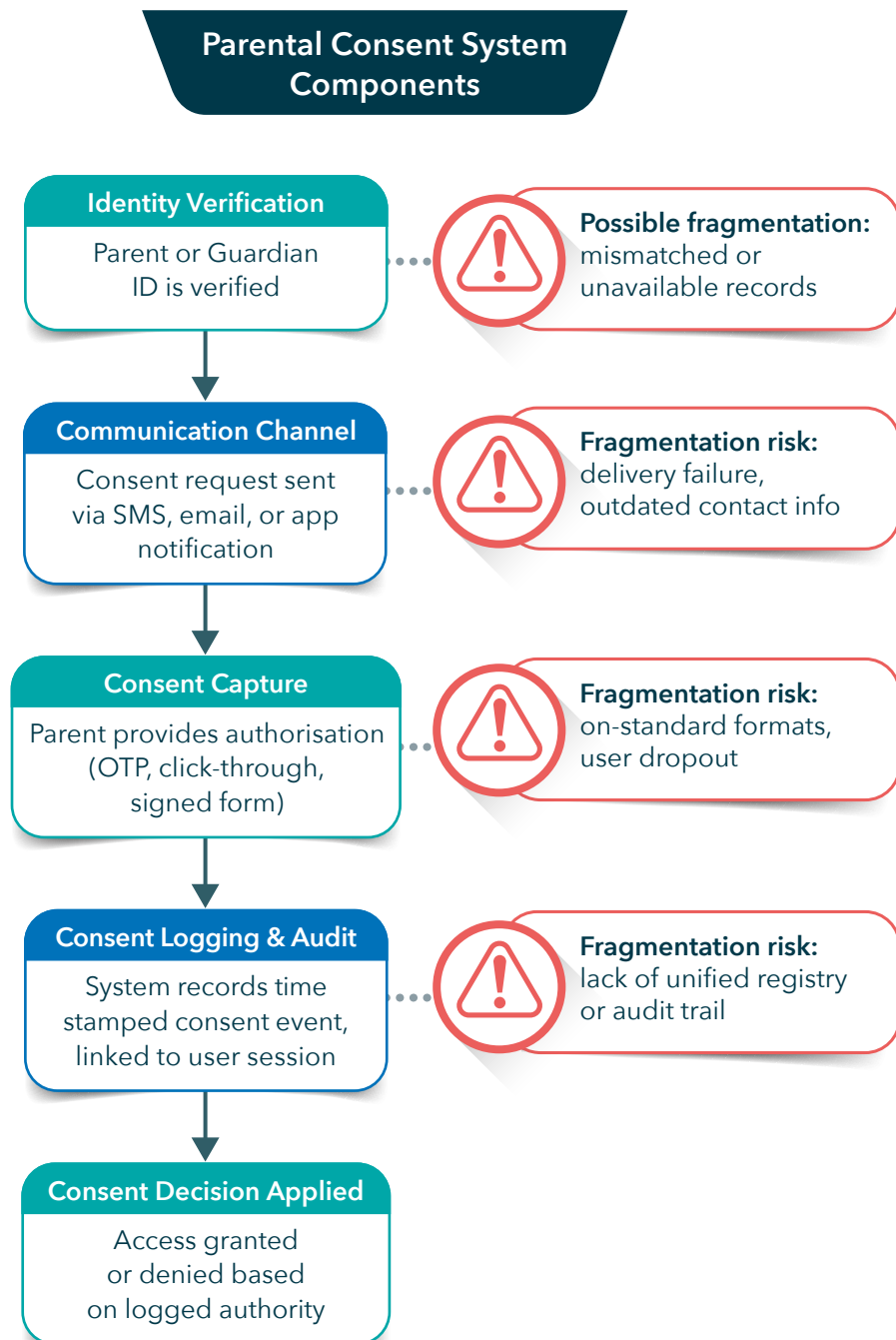


Figure H.16.1 Lifecycle of a Consent Decision

| Fragmentation of digital infrastructure

H.16.5 Parental consent mechanisms often rely on real-time coordination between multiple elements:

- Parental identity verification
- Communication with the guardian (e.g., email, SMS, app notification)
- Binding of consent to the child's account or session
- Secure logging and audit of consent events

H.16.6 The Trial observed that while many individual components are technologically mature, the integration between them remains fragmented. There is no consistent framework across platforms, devices or services for:

- Verifying that the adult is a legitimate parent or legal guardian
- Storing and managing consent records in a privacy-preserving manner
- Ensuring that consent is valid, revocable and portable across digital ecosystems

H.16.7 This complexity introduces friction for parents and raises risks of unverified or incomplete consent, particularly in time-sensitive, transactional or high-volume service contexts.

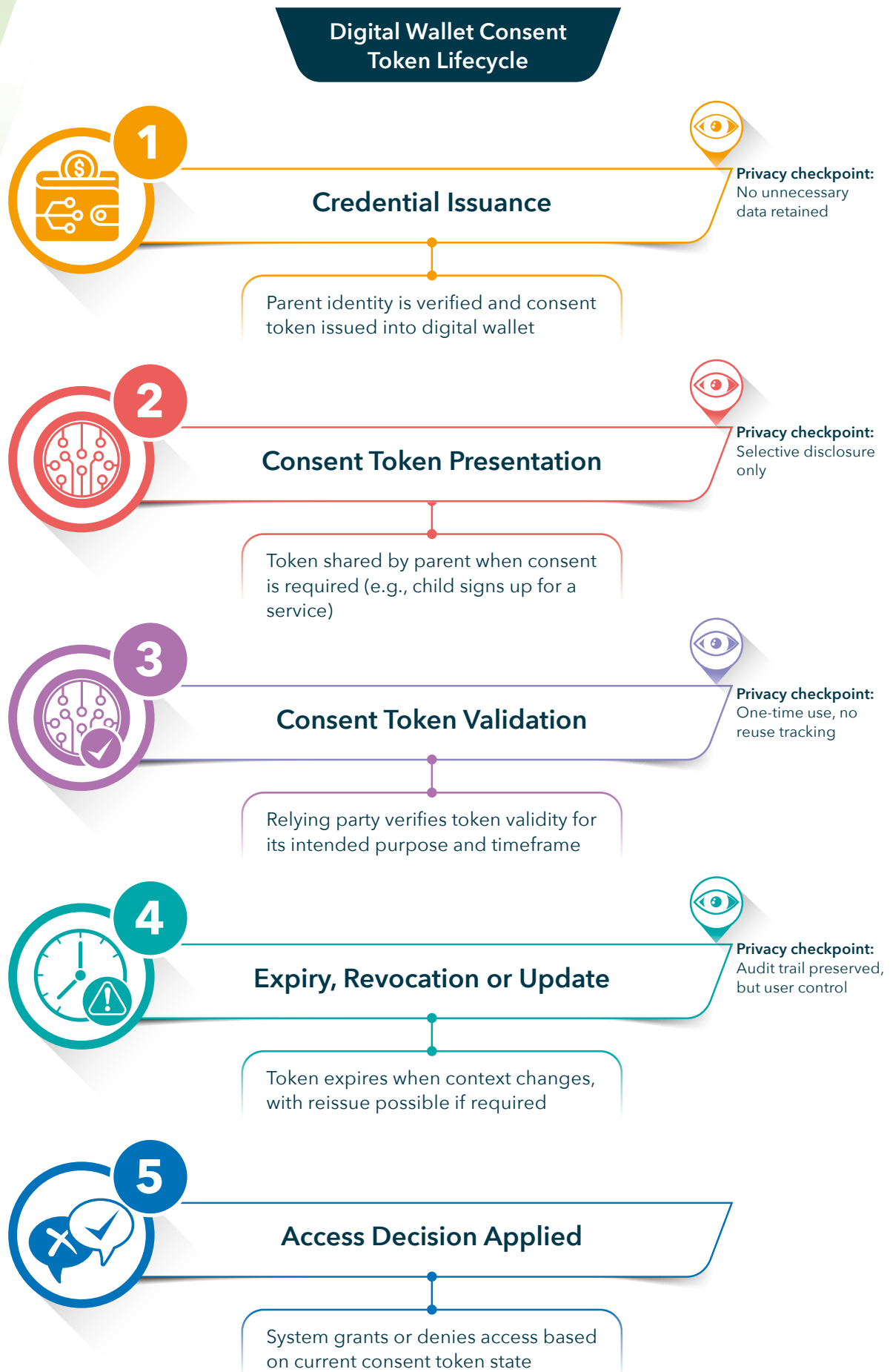


Figure H.16.2 Digital Wallet Consent Token Lifecycle

| Promise and pitfalls of emerging consent technologies

H.16.8 The Trial noted early adoption of emerging consent enablement tools that could address several of these limitations. These include:

- Digital wallets: Where verifiable credentials (e.g., “parent of child X”) can be presented securely to services
- Dynamic consent interfaces: Built into apps to allow real-time, in-flow decisions by parents
- Token-based signalling: Where third-party services can validate that consent has been granted without receiving identifying data

H.16.9 These developments offer the potential to reduce friction, enhance trust and enable more granular control over consent parameters, such as scope, duration and revocability.

H.16.10 However, they also raise new concerns, particularly around:

- Persistent logging of consent events, which if not properly governed, could contribute to long-term profiling of families and children
- The risk of interoperability gaps, where a consent token from one ecosystem is not recognised by another, undermining the scalability of the solution
- Unclear boundaries between consent and surveillance, especially when consent metadata is tied to behavioural analytics or advertising systems

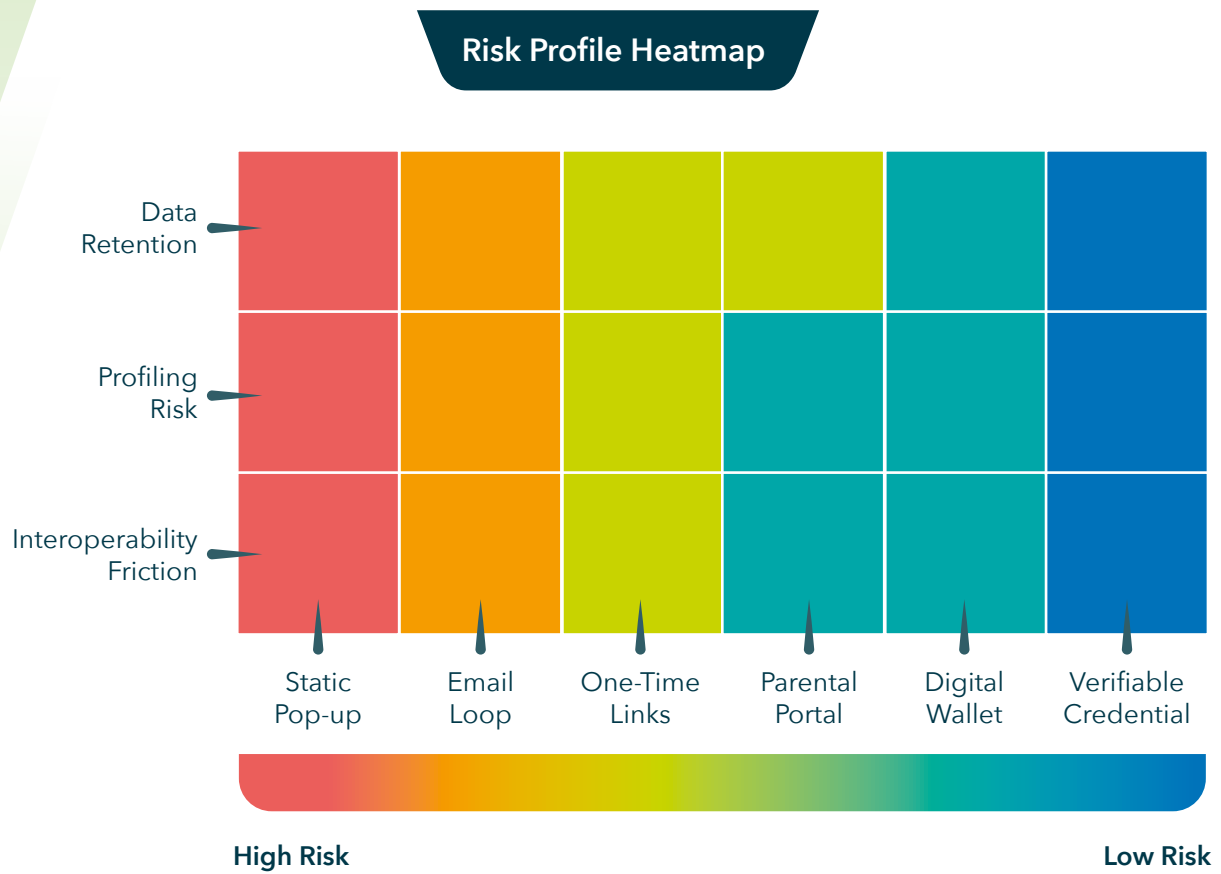


Figure H.16.3 Risk Profile Heatmap

| Future development

H.16.11 To ensure that parental consent mechanisms evolve in a way that supports trust, privacy and inclusion, the Trial highlights the following priorities:

- Interoperability and open standards: Consent systems should be able to interface across platforms using shared, privacy-preserving protocols
- Modular identity and role frameworks: Rather than assuming one model of guardianship, systems should support configurable roles for carers, foster parents or cultural custodians
- Dynamic, revocable and child-aware consent: Consent should not be a one-time checkbox. Systems should support time-limited approval, renewal prompts and age-appropriate feedback loops with the child
- Minimisation of metadata retention: Systems should avoid accumulating unnecessary logs of consent interactions that could be exploited for profiling or commercial purposes

H.17 Contextual, Risk-Aligned Deployment of Parental Consent Mechanisms

H.17.1 Unlike parental controls, which are often configured at the device, operating system or network level, parental consent is usually triggered in response to a particular access request – such as signing up for a service, making a purchase or accessing restricted content. As such, consent is contextual and event-driven, rather than persistently active across platforms or services. While this approach helps ensure consent is relevant and proportionate to the activity, it also presents challenges for interoperability and consistency across different digital environments. The Trial did not find widespread deployment of parental consent mechanisms at the stack level, highlighting an opportunity for more integrated, cross-platform approaches in the future – so long as they preserve user autonomy, legal integrity and privacy.

H.17.2 A key advantage of parental consent mechanisms being deployed at the moment a child attempts to access a specific age-restricted activity, service or piece of content is that the request for parental involvement occurs immediately before a decision must be made about access, making the process highly proximate to the actual risk. Unlike parental controls, which are pre-set and often apply broadly across an entire device or platform, parental consent is event-triggered and context-specific.

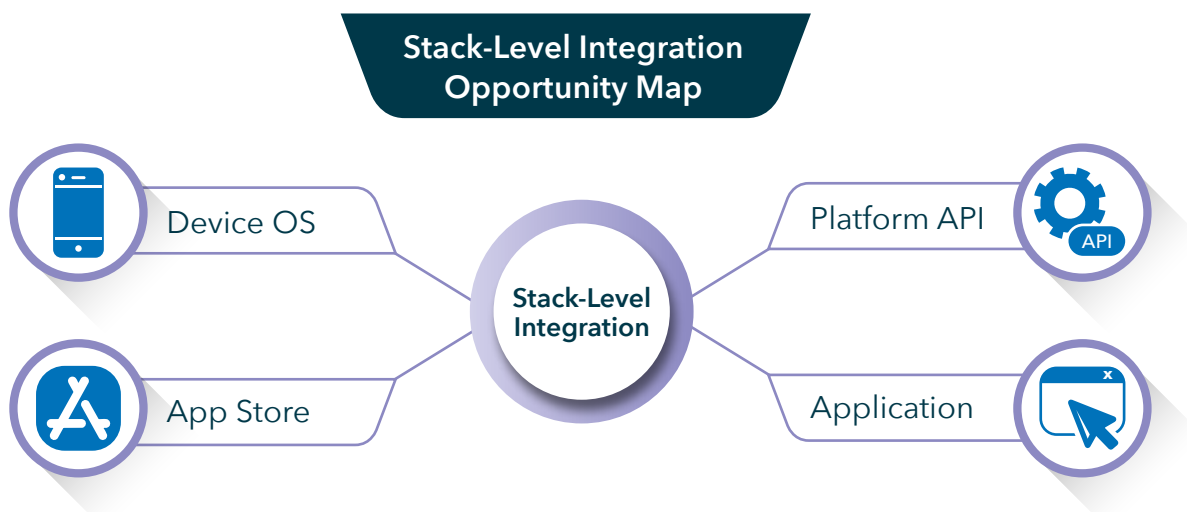


Figure H.17.1 Stack-Level Integration Opportunity Map

| Examples from Trial participants

H.17.3 Several participants in the Trial provided working implementations of real-time, risk-aligned parental consent workflows. Examples included:

- Video streaming platforms that trigger a consent prompt when a child tries to play a film classified above the child's self-declared age, requiring guardian verification before access is granted
- Educational tools that ask for parental confirmation before enabling communication features or location tracking – features that carry heightened privacy considerations
- Gaming platforms that require a parent to approve purchases or account creation based on inferred age from device metadata or previous user behaviour

H.17.4 In each of these cases, the consent request was tightly bound to the action itself, making it easier for the parent to assess the context and relevance of the request.

| Advantages of risk-proximate consent

H.17.5 This risk-aligned approach to parental consent presents several operational and ethical benefits:

- Improved legitimacy and trust: Parents are more likely to see the request as justified and timely, increasing the likelihood of engagement and valid consent
- Clearer communication with the child: Because the request is tied to a specific action, children can understand why consent is needed in that moment, reducing perceptions of arbitrary control or overreach
- Minimised surveillance: Unlike continuous parental monitoring, contextual consent avoids the need for broad data collection or pre-emptive restriction, helping to maintain the child's right to privacy and digital exploration
- Support for autonomy: By limiting consent prompts to high-risk actions, systems can avoid over-regulation and allow children to build independence in low-risk digital contexts

H.17.6 Despite these strengths, the Trial found that most parental consent systems operate as isolated implementations – effective for their specific use case, but lacking interoperability across services. As a result, there is no common infrastructure for issuing or verifying consent tokens across platforms, which could lead to repetitive user experiences or fragmented consent histories.

H.17.7 Furthermore, this contextual design does not yet extend across the broader technology stack. For example, there were no observed implementations of consent workflows embedded at the operating system, app-store or device provisioning level. This gap presents an opportunity for further development – where consent mechanisms could be more portable, secure and cross-platform while still preserving their event-specific character.



Figure H.17.2 Consent Deployment Comparison Chart

H.18 Data Minimisation and the Privacy Risks of Persistent Consent Logging

H.18.1 While parental consent mechanisms are designed to be specific, time-bound and related to a particular access request, the cumulative effect of storing consent records over time can contribute to the creation of a persistent digital footprint. Each logged instance of parental approval – whether for signing up to a platform, accessing age-restricted content or making a purchase – can reveal patterns about a child’s development, interests and online behaviour. When these records are retained indefinitely or collected across services, they begin to form a detailed behavioural profile, even if unintentionally.

H.18.2 Although parental consent is not inherently intrusive, if consent logs are not properly governed, they may include sensitive metadata – such as timestamps, service types, device identifiers or even inferred maturity levels. Over time, this information can be used to draw inferences about a child’s age, habits and life stage, potentially exposing them to privacy risks or targeted profiling. If improperly shared, insecurely stored or used beyond the original purpose, these records could become a vulnerability point for misuse – by advertisers, third parties or in more concerning scenarios, by those seeking to manipulate or exploit the child. To mitigate these risks, systems must ensure that consent records are minimal, time-limited and purpose-bound, with clear policies for secure deletion and safeguards to prevent secondary use.

H.18.3 Parental consent mechanisms are fundamentally intended to be specific, time-bound and proportionate to a particular access request – such as signing up to a platform, authorising an in-app purchase or approving the use of an age-restricted feature. However, the cumulative storage of these consent records can have unintended consequences, particularly when not governed by clear limits on retention, reuse or scope.

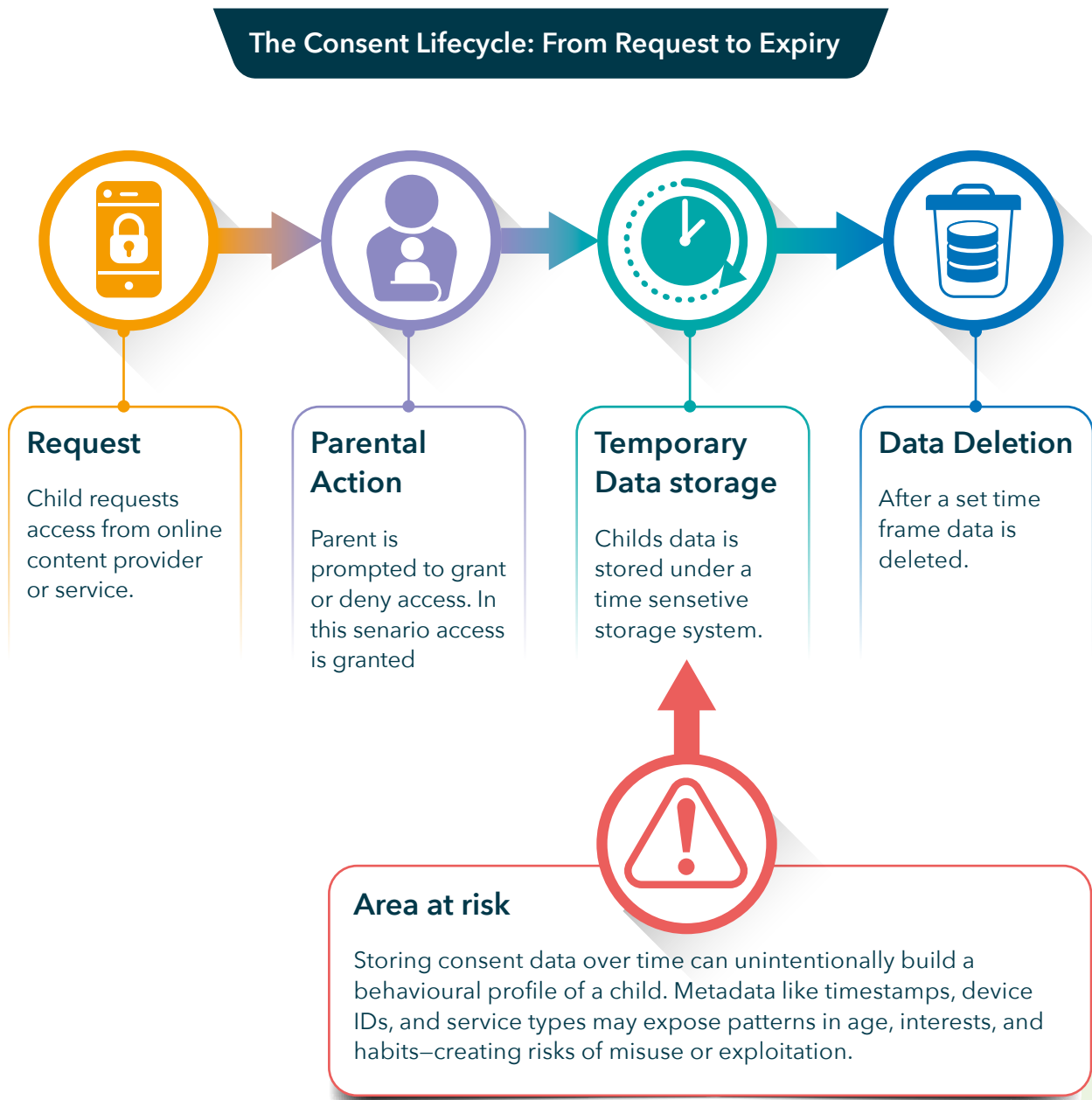


Figure H.18.1 Consent Lifecycle Flow

Vendor Case Study

*Website*sedicii.com

Sedicii offers one of the most privacy-preserving approaches to parental consent observed during the Trial, with a strong emphasis on data minimisation, selective disclosure and avoidance of persistent logging.

Practice Statementageassurance.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's model directly addresses a core risk identified: that repeated logging of consent events can unintentionally build up sensitive behavioural profiles of children over time. By design, Sedicii avoids this accumulation altogether.

| Digital footprint created by consent logs

H.18.4 Each instance of parental consent, even when isolated, can carry metadata – including the timestamp, device ID, type of service accessed or the inferred age threshold of the child. Over time, if consent logs are retained across multiple services or environments, they may begin to form a persistent behavioural profile. This profile may indirectly reflect:

- A child's evolving maturity or digital autonomy
- Shifts in content access over time (e.g. games to social media)
- Parental comfort with certain types of content or platforms
- Patterns of interaction across digital services and platforms

H.18.5 Even though consent itself is not inherently privacy-invasive, the surrounding data associated with it – especially if collected and stored without strict limitations – can become sensitive and revealing.

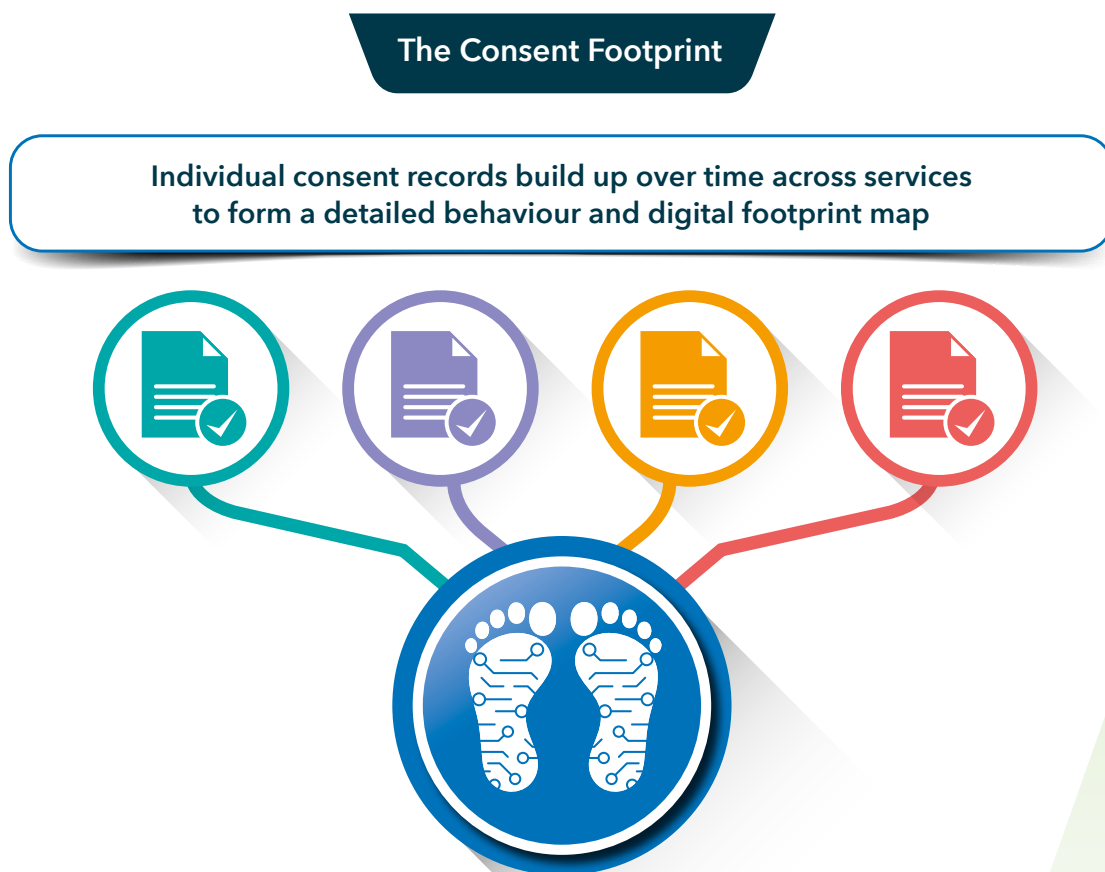


Figure H.18.2 Digital Footprint Accumulation

| Risks from poor governance or secondary use

H.18.6 Parental consent records can pose a substantial privacy and security risk if they are:

- Retained indefinitely
- Insecurely stored
- Shared across unrelated services
- Used for secondary purposes (e.g., behavioural profiling, targeted advertising or analytics)

H.18.7 In the most concerning scenarios, bad actors could access such records (via data breaches or insufficient authentication protocols) and reconstruct highly detailed behavioural profiles of children, increasing their vulnerability to:

- Manipulative advertising
- Targeted misinformation
- Grooming or exploitation based on inferred preferences, habits or vulnerabilities

H.18.8 This risk is particularly acute in contexts where consent metadata includes identifiers or is linked to the child's persistent account across platforms.

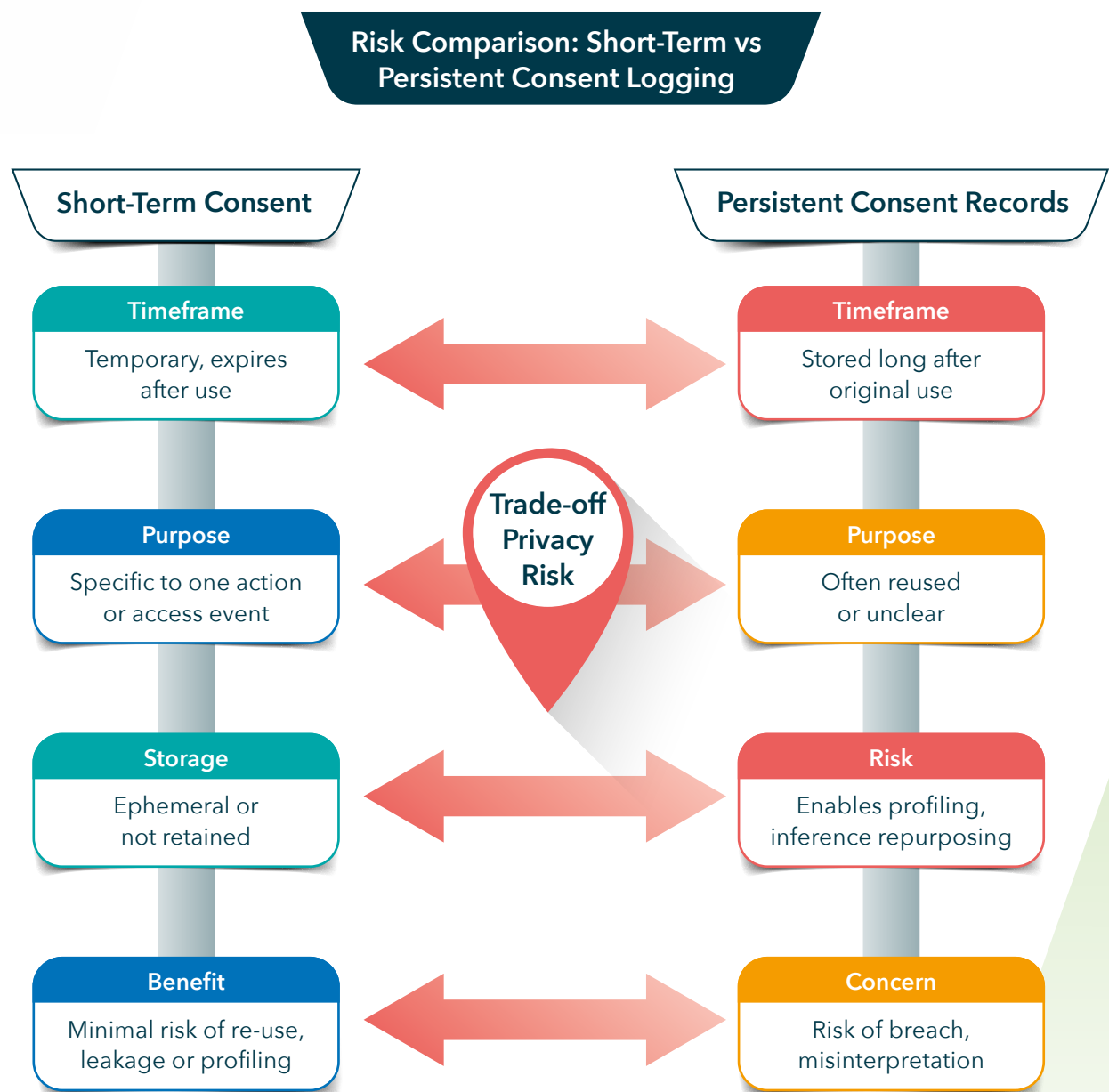


Figure H.18.3 Risk Comparison

| Good practice and mitigation

H.18.9 To avoid these risks, parental consent mechanisms are best developed in alignment with data minimisation and privacy-by-design principles. This includes:

- Time-limited consent records: Retaining records only for the duration necessary to support regulatory or operational requirements.
- Scoped consent: Restricting each record to the specific activity approved and prevent cross-context reuse.
- Secure deletion protocols: Establishing lifecycle management for consent data, with automated expiry and user-accessible revocation.
- Anonymisation and pseudonymisation: Replacing identifiable consent metadata with secure tokens or cryptographic references wherever possible.
- Transparency for families: Allowing parents to review, manage and revoke previous consents and ensure that children can eventually assume control as their digital maturity increases.



H.19 Standards Based Approach to Consent Management

H.19.1 The standards-based approach adopted by the Trial presented both opportunities and limitations when examining parental consent mechanisms. Unlike parental controls, where few dedicated standards exist, we were able to identify an established international standard that offers practical guidance relevant to the design and implementation of parental consent systems: ISO/IEC 29184:2020 – Online privacy notices and consent.

H.19.2 This standard, while not written exclusively for parental consent, provides clear expectations for how digital services should obtain and manage consent, particularly where users may have limited capacity – such as children. It sets out good practice for the presentation of online privacy notices and the obtaining of informed, meaningful and revocable consent in a transparent and accountable way.

H.19.3 In the context of parental consent, ISO/IEC 29184:2020 is particularly useful because it:

- Recognises that children may lack the legal or developmental capacity to provide valid consent themselves.
- Recommends that in such cases, consent must be obtained from a legally authorised representative, such as a parent or guardian.
- Emphasises the importance of clear, age-appropriate and accessible interfaces, enabling both the child and the parent to understand what is being agreed to.
- Requires that consent be revocable at any time and that systems provide easy mechanisms for withdrawal.
- Encourages organisations to maintain audit trails that record who provided consent, when, for what purpose and under what conditions.
- Promotes data minimisation, specifying that only information necessary for the consent process should be collected and stored.

H.19.4 Although the standard does not mandate specific technical implementations, it provides a strong foundation for building secure, user-friendly and compliant parental consent mechanisms, particularly in digital services aimed at or accessible to children.

H.19.5 The Trial found that none of the participating providers directly referenced this standard or demonstrated full alignment with its principles. Most parental consent systems we examined varied widely in their approach and maturity. In many cases, parental authority was assumed or inferred rather than verified and consent was treated as a one-time event, with limited options for review or withdrawal.

H.19.6 Overall, ISO/IEC 29184:2020 offers a relevant and valuable reference point for improving the design and delivery of parental consent mechanisms, helping services to strike a better balance between compliance, usability and the evolving rights and capacities of children in digital environments. However, further awareness and uptake of the standard are needed to drive consistency and quality across the sector.



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



AVID Certification Services Ltd t/a Age
Check Certification Scheme, registered in
England 14865982 • Unit 321 Broadstone
Mill, Broadstone Road, Stockport, SK5 7DL,
United Kingdom • ABN 76 211 462 157



9 781068 164675 >