AffixIO AFFIXIO

YES NO

Sandbox Contact Us

AffixIO Technical Paper · WP-009
June 2026
affix-io.com

AFFIXIO WHITE PAPER · WP-009

Privacy-Preserving Age Verification: Zero-Knowledge Proof of Age Threshold for the Online Safety Act and DSA

Check someone is old enough without learning how old they are.

AffixIO | United Kingdom | affix-io.com | June 2026

ABSTRACT

Age gates leak birthdays. AffixIO's threshold eligibility circuit proves a user meets a threshold without revealing date of birth or storing document images. Built for Online Safety Act and DSA age assurance with minimal data.

CONTENTS

SECTION 1

Introduction

Age verification is a solved problem in the sense that it is technically straightforward to verify a user's age using identity documents. It is an unsolved problem in the sense that every commercially deployed solution to date creates a privacy liability that is, for many users, more harmful than the risk it is designed to prevent. Users required to upload passport or driving licence images to an online service are required to trust that service with the most sensitive personal identity documents they possess, in order to access content that most services make available without restriction to desktop users.

The privacy critique of conventional age verification is well-established: Age Verification Coalition v. Ofcom, the Open Rights Group's campaigns, the ICO's 2019 age verification data protection concerns, and the child rights organisations who argued that invasive age verification would drive child users to less regulated environments rather than protecting them. These critiques have not prevented age verification regulation from advancing; they have simply left the privacy problem unresolved.

Zero-knowledge proof age verification resolves the privacy problem structurally. The user's date of birth is verified by an age verification service provider (AVP) that the user already trusts with their identity documents (a bank, a government identity service, or an established AVP). The AVP checks the date of birth against the service's age threshold and issues a signed binary token: this user satisfies the threshold. The AffixIO ZK circuit converts

this binary token into a ZK proof. The service receives only the proof. The service never sees the date of birth, the identity document, or the AVP's identity for the specific user. The proof is the age verification record.

SECTION 2

The Age Verification Privacy Problem

Conventional age verification creates three distinct privacy risks that ZK age verification eliminates.

Identity document exposure. The service receives a copy of the user's identity document. If the service is breached, identity documents are exposed. If the service is sold, identity documents change hands. Age verification databases are high-value breach targets because they link verified real identities to user accounts on specific services, including those whose use the data subject might prefer not to have linked to their real identity.

Cross-service tracking. If multiple services use the same AVP and that AVP shares user identifiers across services, user behaviour across services can be linked through the common identity anchor. The user who thought their activity on Service A was separate from Service B can be linked through the common verification record. This is a structural risk in any centralised AVP model.

Behavioural profiling. A service that receives a date of birth or age bracket as part of age verification can use that information for advertising targeting, content personalisation, and profiling beyond the verification purpose. This violates GDPR's purpose limitation principle, but may be difficult to detect in practice because the profiling use occurs internally after the verification data is received.

ZK age verification eliminates all three risks. The service never receives the date of birth, so there is nothing to breach. The ZK proof is stateless: two different services receiving proofs from the same user cannot link those proofs to a common identity without additional information not present in the

proof. The service receives only a binary output (over threshold / under threshold) and the proof, neither of which contains age bracket information usable for profiling.

SECTION 3

Regulatory Requirements

The UK Online Safety Act 2023 requires all user-to-user services and search services that are likely to be accessed by children and that carry harmful content to implement highly effective age assurance to prevent children from accessing such content. OFCOM's guidance defines the threshold for "highly effective age assurance" and identifies acceptable methods.

The EU Digital Services Act requires very large online platforms (VLOPs) to implement age assurance for services presenting systemic risks related to minors. Article 28 DSA prohibits VLOPs from processing personal data of minor users for advertising. Age assurance is a prerequisite for complying with the advertising restrictions.

OFCOM's age assurance guidance (published under the OSA) identifies several acceptable age assurance methods, including credit card checks, digital identity verification, and open banking-based age inference. Critically, the guidance specifies that age assurance methods must themselves be privacy-protecting: OFCOM has stated that methods that "unnecessarily process personal data" are not preferred and that privacy-preserving alternatives should be used where available. ZK age verification is directly responsive to this preference.

SECTION 4

The ZK Age Threshold Circuit

The AffixIO threshold eligibility circuit (so named because it also supports health condition threshold verification) implements a configurable age threshold check. The circuit takes three private inputs: the user's year of birth,

the current year (treated as a private input to prevent circuit output from varying by date), and the age threshold. The circuit produces a single public output: 1 if the threshold is satisfied, 0 if not.

Circuit implementation omitted from public documentation.

The circuit does not receive the exact date of birth (day and month), only the birth year. This means the circuit can over-verify (a user born in December of the threshold year will pass even if they have not yet reached the threshold birthday) but cannot under-verify. The conservative direction is deliberate: a user who is one month short of the threshold is more likely to be mislabelled as satisfying it (a risk to the child protection purpose) than one who is months over the threshold. Operators who require more precise threshold enforcement can use day-of-year inputs at the cost of revealing slightly more information about the date of birth.

> **Privacy property:** The threshold eligibility circuit receives the birth year, not the full date of birth. The ZK proof certifies the output without revealing the birth year. The online service receives only the binary output (1 or 0) and the proof. No year of birth is transmitted to the service.

SECTION 5

Interface with Age Verification Providers

The ZK age circuit does not perform age verification independently. It consumes the output of an existing AVP. The integration architecture has three parties: the online service (which needs age verification), the AVP (which verifies age from identity documents), and the AffixIO ZK circuit (which converts the AVP's output into a ZK proof).

The flow is as follows. The user is redirected to the AVP's verification flow, where they complete identity verification using their chosen method (document upload, open banking, digital identity). The AVP verifies that the user satisfies the service's threshold. The AVP issues a signed binary token: `{"threshold": N, "satisfied": true, "issued_at": ""}`. This token is

returned to the AffixIO ZK service (not to the online service). The ZK service extracts the birth year from the AVP's back-end verification record (accessible via API, not the user-facing token), generates witnesses, and generates a proof. The proof is returned to the online service as the age verification record.

The online service never receives the AVP's verification record or the user's birth year. The online service receives only the ZK proof and can verify it against the published verification key. The AVP never communicates directly with the online service: all communication is mediated by the AffixIO ZK service.

SECTION 6

The Age Verification Record

The age verification record stored in AffixIO's governance layer has the following fields: proof digest, circuit identifier (`threshold module v1`), threshold satisfied (YES or NO), threshold value (e.g., 18), Merkle leaf hash, signed Merkle root, and timestamp. It does not contain the user's birth year, name, document type, or any other personal data.

The record serves as the compliance evidence for Online Safety Act purposes. It demonstrates that an age assurance check was performed, that it used a ZK circuit (the circuit identifier specifies which circuit and version), that it was performed at a specific time, and that it produced a specific result. The completeness of the age verification audit trail can be verified by examining the Merkle tree: every age verification event corresponds to a leaf in the tree, and the signed roots confirm the completeness and ordering of those leaves.

SECTION 7

Double-Spend Prevention

A critical requirement for age verification is that a single age verification cannot be reused across multiple accounts or sessions. A user who passes age verification once must not be able to share their proof with others to enable those others to access age-restricted content without verification. This is the ZK equivalent of credential sharing.

AffixIO's double-spend prevention mechanism (described in detail in WP-014) applies to age verification proofs. Each proof is associated with a proof digest that is derived from a session-specific nonce included in the verification request. The nonce is generated by the online service and is unique per session. A proof generated for one session cannot be presented as valid for a different session, because the nonce in the proof would not match the nonce expected by the service for that session. The proof is bound to the specific session for which it was generated and cannot be reused.

SECTION 8

GDPR Analysis

The ZK age verification system has a significantly simpler GDPR profile than conventional age verification. The online service does not receive personal data as part of age verification. The service is not a personal data controller in respect of the verification data. The lawful basis for the verification is not data protection consent from the user (which would create withdrawal rights and other obligations) but the legitimate interests of the service in complying with age assurance regulation.

The AVP remains a data controller for the identity verification it performs. The AffixIO ZK service processes the AVP's output in the course of generating the proof but does not retain personal data. The GDPR Article 25 analysis for the ZK layer is as described in WP-008: the schema has no fields for personal data, so the by-design and by-default requirements are satisfied structurally.

The age verification record (proof digest, circuit identifier, threshold, Merkle anchor) does not constitute personal data in the ordinary sense. It is not linked to a user identity by the online service. The online service knows that a specific session passed age verification at a specific time; it does not know whose session it was in terms of real-world identity. This is a materially different GDPR position from conventional age verification, where the service knows both that a session passed verification and whose identity document was used.

SECTION 9

OFCOM Age Assurance Framework Alignment

OFCOM's Age Assurance Technology Report identifies the key attributes of effective age assurance: accuracy (correctly identifying under-18 users), privacy (not processing more personal data than necessary), security (preventing circumvention), and accessibility (not excluding users who lack certain identity documents). ZK age verification scores well on all four dimensions.

On accuracy, the ZK circuit's output depends directly on the AVP's verification, which uses the same document-based verification as conventional approaches. Accuracy is as high as the underlying AVP's accuracy. On privacy, ZK age verification is the best available approach: no personal data reaches the online service. On security, the session-nonce binding and double-spend prevention mechanisms address the main circumvention vectors. On accessibility, ZK age verification is compatible with any AVP, including open banking, government identity, and document upload methods, so users can choose the method most accessible to them.

SECTION 10

DSA Alignment

The Digital Services Act's age assurance requirements for VLOPs apply specifically to systemic risks related to minors. Article 28 DSA prohibits profiling of minors and requires VLOPs to take measures to protect minors. ZK age verification is particularly well-aligned with Article 28 DSA because it provides age assurance without enabling the VLOP to link a verified age to a user identity, preventing the profiling-of-minors risk that arises when conventional age verification creates a database linking user accounts to verified ages.

The DSA Delegated Regulation on risk management requires VLOPs to conduct risk assessments for systemic risks including risks to minors. A VLOP that deploys ZK age verification can demonstrate in its risk assessment that its age assurance mechanism does not itself create privacy risks for the minor users it is designed to protect, which is a stronger compliance position than a VLOP that deploys conventional age verification and must separately assess the privacy risk of its age verification database.

SECTION 11

Implementation Guide

The minimum implementation for ZK age verification requires three components: an AVP integration (the AffixIO SDK provides adaptors for major UK and EU AVPs), the AffixIO threshold eligibility ZK circuit deployed as a microservice, and an age verification record schema in the online service's session management layer.

STEP	COMPONENT	ACTION	DATA HANDLED
1	Online service	Generate session nonce; redirect user to AVP	Session token (no PII)
2	AVP	Verify user age from identity document	PII (remains with AVP)
3	AVP	Return birth year to AffixIO ZK service via signed API call	Birth year (in transit)
4	AffixIO ZK service	Generate threshold eligibility proof; anchor in Merkle tree	Birth year (in memory only, discarded)
5	AffixIO ZK service	Return proof digest and YES/NO outcome to online service	Proof (no PII)
6	Online service	Store proof digest; admit or deny access based on outcome	Proof digest (no PII)

The entire flow takes approximately 2-3 seconds including AVP verification time. The ZK proof generation step (step 4) adds approximately 500 ms to the AVP's own verification time, which is typically 1-2 seconds. Users experience the verification as a single redirect flow to the AVP and back; the ZK proof generation is transparent to the user experience.

SECTION 12

Conclusion

Privacy-preserving age verification using ZK proofs resolves the fundamental tension between age assurance regulation and user privacy that has made conventional age verification controversial. The technical architecture is straightforward: the AVP verifies age and provides a birth year to the ZK service; the ZK service generates a proof; the online service receives only the proof. No identity document details, no date of birth, and no personal data reach the online service.

The regulatory alignment is strong. ZK age verification satisfies OFCOM's accuracy, privacy, security, and accessibility criteria for age assurance under the Online Safety Act. It aligns with the DSA's minor protection requirements better than conventional alternatives by eliminating the profiling risk created by age verification databases. Its GDPR position is significantly simpler than conventional approaches because the online service is not a personal data controller in respect of age verification data.

AffixIO's threshold eligibility circuit is available as part of the open ZK circuit library and can be deployed with any OFCOM-compliant AVP. The double-spend prevention mechanism ensures that age verification proofs cannot be shared across sessions or users.

Related reading

- WP-017: ZK Selective Disclosure for eIDAS 2.0 and the EUDI Wallet
- WP-008: Zero-Knowledge Proofs as GDPR Article 25 Infrastructure
- WP-014: Double-Spend Prevention for Zero-Knowledge Proofs

Frequently asked questions

Do you store dates of birth?

No. The circuit outputs a yes/no against a configured threshold; no DOB field exists in the audit schema.

Which regulations drive demand?

UK Online Safety Act age assurance, EU Digital Services Act, and GDPR data minimisation principles.

Can proofs be reused?

Spent-proof registries prevent replay across sessions when one-time age checks are required.
