5 May 2026

NATIONAL DIGITAL ID SYSTEM
CONSULTATION PAPER RESPONSE

1. INTRODUCTION

1.1 Spilsbury Holdings Limited t/a Aztec Labs ("**Aztec Labs**") welcomes the opportunity to respond to the "*Making public services work for you with your digital identity*" consultation paper issued by the Cabinet Office, presented to Parliament by the Chief Secretary to the Prime Minister at the Cabinet Office, dated March 2026 (the "**Consultation**").[1]

1.2 Aztec Labs is a UK-headquartered software development company building open-source, blockchain-based software with a focus on zero-knowledge proofs ("**ZKP**"), a form of advanced cryptography discussed in detail in this response. Aztec Labs has recently acquired and is developing ZKPassport ("**ZKPassport**"), an open-source, permissionless, and self-custodial digital identity system (available on iOS and Android) that uses the same International Civil Aviation Organization ("**ICAO**") open standards relied on globally in airports and border systems to authenticate electronic identity documents. ZKPassport enables individuals to prove specific facts about themselves (such as nationality, age, or document validity) directly from their government-issued electronic passport, national e-ID card, or electronic residence permit, without revealing any other personal information. The technology has been battle-tested in production, performing approximately 30,000 document checks and ZKP proofs.

2. THE CASE FOR PRIVACY-PRESERVING DIGITAL IDENTITY

2.1 The introduction of any national identity system raises fundamental questions about the relationship between the state and its citizens. While digital identity infrastructure, properly designed, can unlock significant efficiencies in public services and the wider economy, history demonstrates that identity systems introduced for limited purposes tend to expand in scope, creating risks to civil liberties and national security that persist long after the original justification has passed. Any new digital ID system must therefore be designed so that privacy protections are structural and technical, embedded in the architecture itself, rather than dependent on policy commitments alone.

2.2 The United Kingdom's ("**UK's**") own experience with identity cards illustrates this risk. The UK identity card was born of an emergency. On 1 September 1939 German tanks rolled into Poland; four days later, with the war four days old, Parliament passed the National Registration Act. The Act compelled everyone in Great Britain and Northern Ireland to register, to carry the resulting card at all times, to produce it on demand and to keep its details current. The data collected was sparse by modern standards: full name, date of birth, sex, marital status, occupation and residence. The scheme was meant to last only as long as the war.

2.3 It did not. When peace came in 1945, the cards stayed on. The Attlee (Labour) government justified them in turn as a tool for administering food rationing, for catching the estimated 20,000 (~0.05% of the total population)[2] wartime deserters still thought to be at large, and, more

---

[1] **Note**: http://www.gov.uk/government/consultations/making-public-services-work-for-you-with-your-digital-identity

[2] **Note**: The UK's population at the time was approximately 40,000,000. The estimated deserters were approximately 0.05% of the then population.

candidly, for the convenience of officialdom. By 1950 the ID card had quietly accumulated uses its drafters never imagined. It was demanded for medical treatment, for new passports, even for withdrawals from a Post Office savings account: a textbook instance of function creep. The police, who in law could only insist on the card when investigating a serious offence, in practice asked for it routinely; "*it is obvious that the police now, as a matter of routine, demand the production of national registration cards whenever they stop or interrogate a motorist for whatever cause*"[3]. Hundreds were prosecuted each year for failing to produce one.

2.4 The last of them was a man called Clarence Harry Willcock. On 7 December 1950 a constable named Harold Muckle pulled him over for speeding in London and asked to see his ID card. Willcock refused, reportedly saying '*I am a Liberal, and I am against this sort of thing*'. Willcock was convicted but appealed. In June 1951, the case came before a divisional bench of seven judges presided over by Lord Goddard, the Lord Chief Justice. The court upheld the conviction, but Goddard's judgment made plain his disdain for what successive governments had done with the Act. It '*was passed for security purposes; it was never passed for the purposes for which it is now apparently being used*', he wrote. Pressing wartime statutes into peacetime service, he warned, '*tends to turn law-abiding subjects into lawbreakers, which is a most undesirable state of affairs*'. Prosecutions collapsed. When Churchill's Conservatives returned to office that autumn they scrapped the cards on 21 February 1952, with Churchill declaring that the move would '*set the people free*'.

2.5 Three-quarters of a century on, the same instinct is on the march. On 25 September 2025 the current Labour government announced 'BritCard', a digital identity scheme for every adult resident of the United Kingdom, to be held on a smartphone and required of anyone starting a new job or renting a home. The justifications will sound familiar to any student of 1939: a state of emergency, this time over illegal migration; a promise of swifter access to public services; and assurances that the powers will not be misused.

2.6 The lesson of Willcock's case, and of the UK's history with ID cards in general, is not that digital identity is intolerable; Estonia and others run such schemes without descending into surveillance states. The lesson is that architecture matters more so than rhetoric. A system designed in haste, with citizens' data pooled in central registers and accessed at the state's convenience, will erode privacy for whoever happens to be in office. Function creep is not a flaw in such a system but unfortunately its natural condition. A system designed deliberately, with cryptographic guarantees, data minimisation and the keys to a citizen's credentials in their own pocket rather than Whitehall's (or the contractors that Whitehall hired to build such a system, for that matter), can deliver the efficiency the government promises without the surveillance it disclaims wanting. ZKP technology provides exactly this guarantee: citizens can prove facts about themselves (such as their age, nationality, or right to work) without revealing any underlying personal data, and without that data ever leaving their own device. Critically, even if a future government were to seek to expand the scope of the digital ID system, the technical architecture itself would prevent it from being repurposed as a tool for mass surveillance or disproportionate data collection. The UK has tried the first approach before. It is time to try a better one.

2.7 ZKPs are one of several privacy-enhancing technologies ("**PET**") that could play a role in the digital ID system. However, ZKPs offer material advantages over other PETs, particularly in terms of their production readiness, interoperability with existing government infrastructure, and ability to provide cryptographically guaranteed data protection. We set out further context on ZKPs, and their proposed utility within the national digital ID system, below.

---

[3] **Note**: Lord Goddard CJ in Willcock v Muckle [1951] 2 KB 844.

3. BUILDING ON EXISTING GLOBAL STANDARDS

3.1 The UK does not need to design a digital identity infrastructure from scratch. The ICAO 9303 standard already provides a globally interoperable framework for electronic identity document authentication, relied upon by over 150 countries for e-passport gate systems.

3.2 The ICAO 9303 global standard began with the ICAO's Technical Advisory Group on Machine Readable Travel Documents, which was established in 1984, building on the 1980 standardisation of the Machine-Readable Zone. However, it was the post-9/11 security environment that produced binding international consensus. The 2003 New Orleans Resolution selected facial recognition as the globally interoperable biometric, and the United States used its Visa Waiver Program ("**VWP**") as leverage, under the Enhanced Border Security and Visa Entry Reform Act of 2002, VWP countries had to issue 9303-compliant biometric passports by 2006 or lose visa-free access. Belgium issued the first compliant ePassport in 2004; ICAO then extended the mandate to all member states by 2010, with non-compliant documents losing validity in 2015. The lesson is that international convergence on a single identity standard is not only achievable but already accomplished, under harder conditions, against stronger sovereignty objections, and within roughly a decade of serious effort. There is no need for the UK to reinvent the wheel.

3.3 ZKPassport is built directly on the ICAO trust chain (Country Signing Certification Authority, Document Signer, and chip data), the same cryptographic infrastructure that underpins immigration systems worldwide. This means that ZKPassport's identity verification carries the same level of assurance as a check at an e-passport gate, while adding the privacy benefits of zero-knowledge cryptography on top[4].

3.4 Internationally, the direction of travel is clear. The European Union Digital Identity ("**EUDI**") Wallet project, the reference implementation of eIDAS 2.0, is being built with age verification as a cornerstone use case. Importantly, the EUDI project's public GitHub repository includes a demo age verification component that uses Noir (Aztec Labs' open-source programming language) and Aztec's open-source zero-knowledge circuits, taken from ZKPassport's open-source library, for its zero-knowledge proof implementation. Aztec Labs has not (yet) been formally engaged by the EU on this, but the adoption of Noir and ZKPassport's circuits in the EUDI project's codebase speaks to the maturity and suitability of the technology. We are proud that our cutting edge and future proof technology 'Made in Britain' is being utilised by the EU. The EU's age verification app is now in pilot with seven front-runner Member States (France, Denmark, Greece, Italy, Spain, Cyprus and Ireland), with the architecture explicitly using zero-knowledge proofs over passport / ID data, matching completed on the user's device, and no personal data sent to any external server. All 27 Member States are due to offer EUDI Wallets by end of 2026 under eIDAS 2.0.

3.5 For the UK government, the practical implication is straightforward. The cryptographic standards, open-source tooling, and production-tested infrastructure needed to deliver a privacy-preserving digital ID system already exist and are in use. Importantly, they are 'Made in Britain'. ZKPassport is operational today, supports identity documents from over 130 countries, and its cryptographic backend (built on Noir) can be upgraded seamlessly as the technology evolves (to make it faster / more secure). By building on ZKP technology and the ICAO standard, the UK can move quickly, reduce development cost and risk, and ensure interoperability with international partners, rather than incurring the expense and delay of designing a bespoke solution.

3.6 For readers less familiar with the underlying technology: ZKPs are cryptographic techniques that allow one party (the 'prover') to demonstrate to another party (the 'verifier') that a given

---

4 **Note**: with modern cryptography and technology it is possible to take any existing ICAO compliant ID (including UK passports) and turn them into digital ID's that are opt in and privacy preserving.

statement is true without revealing any information beyond the truth of the statement itself. Although the underlying mathematics has existed for over 40 years, recent breakthroughs have made ZKPs practical for everyday applications, including digital identity verification, age verification, and regulatory compliance checks. In the context of a national digital ID, ZKPs enable a citizen to prove, for example, that they are over 18, that they hold a valid passport, or that they have the right to work in the UK, without revealing their date of birth, passport number, or any other personal data to the service provider.

4. HOW ZKPS CAN DELIVER THE CONSULTATION'S OBJECTIVES

4.1 When it comes to the proposed national digital ID system, we think ZKPs are the best technology available to protect citizen privacy and maximise data security while still delivering on the government's goals of utility, inclusivity, and trust. Beyond the privacy benefits (and the boost to public confidence that comes with them), ZKPs can also drive real operational efficiencies across both public and private sector use cases.

4.2 To unlock these benefits, the digital ID system needs to be open to integrating privacy-enhancing technologies rather than locking in traditional, data-heavy approaches to identity verification. The system should let technology providers, including through the existing trust framework and digital verification services ("**DVS**") ecosystem, use ZKPs to meet the required identity verification and data protection standards. The Consultation's proposal to build on existing infrastructure, including GOV.UK One Login and the GOV.UK Wallet, and to work within the UK digital identity and attributes trust framework, provides a natural starting point for this.

4.3 This section looks at the practical benefits of using ZKPs in the digital ID system, organised around four themes: (i) trust and privacy first; (ii) optional adoption for citizens; (iii) efficiency in public services; and (iv) solving age verification. Taken together, these benefits make a strong case for embedding ZKP technology in the digital ID architecture, especially when you consider how ZKPs can simultaneously strengthen data privacy and deliver useful, inclusive digital identity services.

Trust and Privacy First: A Digital ID Rooted in Cryptography

4.4 The Consultation recognises that the digital ID system must be built with privacy as a core principle, following 'privacy by design and default' from the very start. We couldn't agree more and we think ZKP technology is the most effective way to make good on that commitment. A UK digital ID system rooted in zero-knowledge cryptography would let citizens control not just their data but their privacy in a way traditional approaches simply can't match. Instead of asking citizens to hand over personal data to be stored in centralised databases (creating 'honeypots' that invite cyberattack, a national security risk), a ZKP-based system lets citizens prove facts about themselves through cryptographic proofs, without the underlying data ever leaving their device. This approach is naturally aligned with the data minimisation principles in the UK GDPR and the Consultation's commitment to selective disclosure.

(a) ZKPassport is a production-ready example of this in action. It works entirely on-device, generating selective-disclosure proofs that service providers can verify without ever storing, transmitting, or touching the underlying identity data. It uses the same ICAO open standards infrastructure relied on globally in airports and border systems to authenticate electronic identity documents, and can confirm that a facial liveness check matches the biometric data stored in a document's NFC chip, proving 'the person presenting is the document holder' without revealing the actual face data. The result is state-grade assurance, anchored in official government-issued certificates and biometric-match attestations, with user-controlled, self-custodial privacy. Critically, ZKPassport is fully open-source and does not need any intermediary to check someone's passport and issue new credentials: all you need is your phone and an ICAO-compliant document (an electronic passport, national e-ID card, or electronic residence

permit). ZKPassport's cryptography backend is built using Noir, Aztec Labs's programming language, the same language and open-source circuits now appearing in the European Union's EUDI Wallet age verification pilot (as discussed further in section 3 below). The system is anchored on Ethereum, the most secure and trusted blockchain infrastructure in the world, providing a decentralised, tamper-proof foundation for identity attestations.

4.5 *Optional for Citizens: A Digital ID That Puts Individuals in Control*

We strongly support the Consultation's position that nobody should be legally required to have or present the digital ID, and that the system should be something people want to get rather than something they must have. ZKP technology reinforces this principle at a technical level. In a ZKP-based digital ID system, citizens are not passively enrolled into a surveillance architecture. Rather, they actively choose to generate and present cryptographic proofs of their identity attributes, on their own terms, from their own devices. Proof generation happens locally on the citizen's device, and no personal data is sent to or stored by any centralised entity. This gives people genuine control over when, where, and with whom they share information about themselves, going well beyond the selective disclosure the Consultation envisions. In an era of growing privacy awareness and increasing national security risks (with citizens data being leaked), amplified by the data risks associated with large-language models and autonomous agents, a ZKP-based approach ensures that the optional nature of the digital ID is baked into the technology, not just promised in policy documents.

4.6 *Issued for Efficiency; Not Emergency: Unlocking Modern Public Services*

(a) The Consultation sets out an ambitious vision for the digital ID to sit at the heart of next-generation digital public services, from streamlining child benefit administration to enabling proactive, personalised service delivery. ZKP technology can play a transformative role here. ZKPs can dramatically cut onboarding and verification times by letting citizens present reusable cryptographic credentials whenever they interact with a public service, enabling automated verification and reducing both manual review and scope for error. For example, a citizen could use ZKPassport to cryptographically prove their identity and eligibility to multiple government departments without going through a separate identity check with each one. This mirrors the 'tell us once' approach the Consultation highlights as a key goal.

(b) On top of that, ZKPs can significantly lower the administrative cost of identity verification across government. The Consultation notes that digital signatures enabled by Estonia's digital identity system save the nation an estimated 2% of GDP annually. A ZKP-enhanced digital ID system could deliver comparable, if not greater, efficiencies for the UK by eliminating duplicative identity checks, reducing fraud risk, and giving government services greater confidence in the identity of the people they serve, all while minimising (i) the personal data that needs to be processed and stored and (ii) data breaches which would lead to national security concerns.

(c) ZKPs also tackle fraud head-on, a major concern highlighted in the Consultation. Between June 2024 and 2025, fraud accounted for 44% of crime in England and Wales, with over 118,000 identity fraud cases reported to the National Fraud Database in the first half of 2025. A ZKP-based digital ID fundamentally changes the game: because personal data is never disclosed in the first place, there's nothing to steal, forge, or misuse. ZKP attestations are cryptographically secured and tamper-evident, making them inherently more resistant to the identity fraud that currently plagues physical document-based processes. This represents a step-change in the security of the UK's identity infrastructure.

Age Verification Solved: A Revolutionary Approach

4.7 A well-designed ZKP-based digital ID system has the potential to transform age verification. Over the last three years, a wave of regulation has turned age verification from a 'nice to have' into a legal mandate. In the UK, the Online Safety Act 2023 requires 'highly effective age assurance' for adult content and a widening list of social features, enforced by Ofcom with real financial penalties. The government's parallel consultation on children's safety online ('Growing Up in the Online World', open until 26 May 2026) has a statutory minimum age for social media, a higher age of digital consent, more robust age assurance mechanisms, and new age-related obligations on AI chatbots all on the table at once. In the EU, the Digital Services Act obliges platforms to protect minors, and the eIDAS 2.0 framework has put the EUDI Wallet on the critical path, with age verification as a cornerstone use case. In the US, the Supreme Court upheld Texas's age verification law in *Free Speech Coalition v. Paxton* in June 2025, and more than a dozen other states have introduced similar requirements. Australia has legislated a social media ban for under-16s. The Consultation itself acknowledges that proving age when purchasing alcohol will be an early use case for the digital ID, and more broadly highlights the importance of age verification across regulated sectors including online services, tobacco and vapes, and knife sales.

(a) Traditional age verification methods are not fit for this new regulatory reality. Self-declaration is trivially bypassed. Document-based checks (requiring users to photograph a passport or driving licence for server-side review) can be compromised through forged or borrowed IDs and create a toxic byproduct: a centralised database of verified government IDs. In October 2025, photographs of government IDs belonging to approximately 70,000 Discord users were exposed after a breach at verification vendor Persona. Biometric age estimation (where a selfie returns an estimated age range) avoids document collection but degrades in accuracy at the age boundaries that matter most (roughly 16 to 25), and some users object to biometric data being processed at all. The structural flaw shared by all legacy methods is over-disclosure: each one forces users to reveal substantially more about themselves than the question requires.

(b) ZKP-based age verification is designed to change that, answering only what is asked and learning nothing more. With ZKPassport, a citizen scans the NFC chip in their passport or e-ID card with their phone, and the app generates a cryptographic proof that they are over 18 (or any other required age threshold), without revealing their date of birth, name, or any other personal information. The service provider can verify the proof instantly, with cryptographic certainty, without ever accessing or storing any personal data. This is not theoretical: it is technically proven and operational today. The French Data Protection Authority (CNIL) has acknowledged zero-knowledge identity as a privacy-friendly model for online age verification, and the EU's own age verification pilot (discussed in section 3 above) uses the same zero-knowledge approach that ZKPassport has been running in production. Privacy-preserving approaches will dominate over time, because the alternative, a centralised database of verified government IDs attached to every platform anyone uses, is both a security liability and politically unsustainable.

(c) ZKPassport's age verification works across both Web2 and Web3 environments, making it a good fit for the full range of private sector use cases the Consultation has in mind, from purchasing age-restricted goods in shops to accessing age-restricted services online. Importantly, ZKPassport does not require any eyeball scanning or collection of personal biometric data; it works directly with legitimate government-issued document data, without revealing anything beyond the specific attribute being proved. Interoperability will matter more than any individual vendor in this space: the platforms that will succeed are those whose age proofs can be reused across the web. ZKPassport's architecture is designed for exactly this, and the same proof can be reused across many services without compounding the exposure of any one of them. A comparison of ZKPassport against other leading digital identity technologies (including traditional KYC providers and the EUDI Wallet) is set out in *Annex 1* to this response.

Data Minimisation and Cybersecurity

4.8 The Consultation rightly makes security a top priority, noting that cyber threats pose a growing risk to public services. ZKPs offer a uniquely powerful approach to cybersecurity in the digital identity context, precisely because they minimise the amount of sensitive data that needs to be stored and sent around in the first place.

(a) In a traditional digital ID system, centralised databases full of citizens' personal data, including biometrics, become prime targets for cyberattacks. These 'honeypots' pose serious personal and national security risks, and the Consultation acknowledges this. A ZKP-based architecture fundamentally eliminates the problem: personal data stays on the citizen's device and only cryptographic proofs are shared with service providers, so there is no centralised store of personal data to be compromised. Even if a verifier's system were breached, no personal data would be exposed, because none was collected. This is a fundamental shift in how digital identity security works, and it directly addresses the Consultation's commitment to building on cybersecurity best practice.

(b) ZKPs also help with the Consultation's proposals for protecting vulnerable and at-risk individuals. The Consultation identifies specific groups (victims of domestic abuse, people in witness protection, government staff in sensitive roles) whose data needs extra protection. A ZKP-based system provides this by default: because no personal data is disclosed during verification, there is no risk of a vulnerable individual's details being exposed through data breaches, system errors, or unauthorised access.

Third-Party Holder Services and the Trust Framework

4.9 The Consultation explores whether the digital ID could be stored in third-party digital wallets beyond the GOV.UK Wallet, provided they meet certain conditions including certification under the UK trust framework. We strongly support this, and ZKPassport is exactly the kind of technology that could operate as a complementary component within this ecosystem. Because ZKPassport is open-source and self-custodial, citizens keep full control of their identity data on their own device, while service providers can verify cryptographic proofs knowing they meet the required standards.

4.10 In this context, ZKPs could provide the robust programmatic verification the Consultation sees as essential for all digital ID transactions, confirming that digital IDs have not been faked, tampered with, or revoked, without requiring visual inspection and without creating additional data security risks. A summary of how ZKPs address the Consultation's key objectives is set out in Table 1 below, and our responses to specific Consultation questions are set out in Table 2.

TABLE 1: HOW ZKPS ADDRESS KEY DIGITAL ID CONSULTATION OBJECTIVES

For a broader view of how ZKPs can support the digital ID system's key objectives, *Table 1* below maps ZKP capabilities against the main use cases and challenges identified in the Consultation.

Consultation Objective	**Description / Challenge**	**How ZKPs / ZKPassport Can Help**
Age Verification		
The Consultation identifies age verification as an early use case for the digital ID, including proving age when purchasing alcohol, accessing age-restricted online services, and supporting the objectives of the Online Safety Act 2023. The government proposes that the digital ID will share only that a person is 'over-18' rather than their full date of birth.	Traditional age verification methods require users to present physical documents disclosing far more personal information than necessary. Online methods such as self-declaration are easily bypassed by minors. Biometric and AI-based approaches create additional privacy and data security risks.	Using ZKPassport, a citizen scans the NFC chip in their passport or e-ID card and generates a ZKP that they are over 18 (or any other required age threshold) without revealing their date of birth, name, or any other personal information. The proof is generated on-device and can be verified instantaneously by service providers without accessing or storing any personal data. This is the most privacy-preserving age verification method available and is already operational.
Right to Work Checks		
The Consultation proposes that, by the end of this Parliament, evidence must be checked digitally as part of a prescribed right to work check. The digital ID will have a central role in the UK's right to work regime.	Currently, right to work checks rely on a varied range of physical documents, which are susceptible to forgery. Manual checks are unreliable, and the process creates data security risks when copies of documents are stored by employers.	ZKPassport enables individuals to cryptographically prove their nationality and right to work status without disclosing their full passport data or other personal information to employers. This creates a digital audit trail, eliminates the risk of document forgery, minimises the personal data employers need to process, and significantly streamlines the recruitment process. ZKPassport can attest that a person holds a valid ICAO-compliant document confirming their nationality and, where applicable, immigration status.
Selective Disclosure / Data Minimisation		
The Consultation commits to data minimisation principles and selective disclosure as central features of the digital ID. The digital ID will share only the minimum information necessary for a given interaction.	When presenting physical identity documents, individuals have no choice but to disclose all printed information. Digital systems can improve on this, but	ZKPs provide the most advanced form of selective disclosure available. Rather than transmitting a subset of personal data, ZKPs allow citizens to prove specific facts (*e.g.*, 'I am over 18', 'I have the right to work in the UK', 'I am not on a sanctions list') without revealing *any*

Consultation Objective	Description / Challenge	How ZKPs / ZKPassport Can Help
	most approaches still require transmission and storage of personal data at some point in the verification chain.	underlying data. No personal data is transmitted, stored, or processed by the verifier at any stage. This goes beyond selective disclosure to achieve genuine zero-knowledge verification.
Fraud Prevention		
The Consultation identifies fraud as a national challenge. Fraud accounted for 44% of crime in England and Wales (June 2024 – 2025), with over 118,000 identity fraud cases reported to the National Fraud Database in the first half of 2025. AI-generated fake identities are an emerging threat.	Physical documents can be forged or stolen. Centralised databases of personal data are vulnerable to cyberattacks and data breaches. AI can be used by malicious actors to generate highly convincing fake identities, manipulate biometric data, and automate impersonation at scale.	ZKP-based identity attestations are cryptographically secured and tamper-evident. They cannot be forged, manipulated, or replicated by AI. Because personal data is never disclosed, there is no data to steal or misuse. ZKPassport's on-device proof generation means that even if a service provider's systems are compromised, no personal data is exposed. This fundamentally changes the fraud landscape.
Sanctions Screening and KYC/AML Compliance		
Sanctions and KYC/AML requirements apply across regulated sectors where the digital ID may be used, including financial services. The Consultation notes that the digital ID will support Know Your Customer checks as required under the Money Laundering Regulations.	Traditional KYC checks require individuals to disclose and transmit significant amounts of personal data to multiple service providers, creating data security risks and administrative burdens. Each interaction typically requires a separate verification, with no reusability.	ZKPassport enables individuals to prove their identity and sanctions compliance without revealing personal information. ZKPassport's sanctions-screening capability conducts checks against published sanctions lists using a Merkle tree-based non-membership proof, confirming that an individual is not on any sanctions list without revealing their identity. Separately, ZKPassport has been battle-tested in production, performing approximately 30,000 document checks and ZK proofs to ensure sybil-resistance for sequencers joining Aztec Network's decentralised testnet. The technology is here today.

TABLE 2 – RESPONSES TO THE CONSULTATION

Part	*Consultation Question*	*Aztec Labs / ZKPassport Response*
Part 1: Our Ambition	*1.0.Q1 — What do you think the main benefits will be, if any, for the government's new national digital ID system?*	The biggest benefit is the chance to build a digital identity system that's privacy-preserving by design, not just privacy-compliant as an afterthought. By embedding zero-knowledge proof technology into the digital ID architecture, the UK can give citizens genuine, cryptographically guaranteed control over their personal data. The practical benefits are huge: faster access to public services (digital signatures enabled by Estonia's digital ID save its economy an estimated 2% of GDP annually), streamlined right-to-work and age verification, and dramatically reduced fraud (identity fraud currently represents 59% of all cases filed to the Cifas National Fraud Database). Zero-knowledge proofs (ZKP) make all of this possible while actually collecting and sharing less data than traditional methods, a genuine win-win for citizens and government alike.
	1.0.Q3 — To what extent do you agree or disagree that the proposed system could help make it easier for people to prove who they are?	Strongly agree. ZKPassport already proves this is achievable today. During the onboarding of sequencers as part of bootstrapping the Aztec Network, ZKPassport performed approximately 30,000 document checks and ZK proofs, verifying identity attributes including age, nationality, and uniqueness, using nothing more than a smartphone and an ICAO-compliant electronic passport or e-ID. No uploading of documents, no third-party intermediaries, no centralised databases. Citizens simply scan their passport's NFC chip, and ZKPassport generates a cryptographic proof that they meet the relevant criteria, stored on-chain to prove verifiability. This is quicker, more private, and more secure than any paper-based or traditional digital verification method currently available.
Part 2: Our Approach	*2.1.Q1 — Are there technical issuance standards, beyond those already used by the GOV.UK Wallet, that we should be building the national digital ID to?*	Yes. The digital ID should embed ZKP generation and verification as a core technical standard. This would let citizens generate selective-disclosure proofs on their devices, proving specific attributes (like age or right-to-work status) without revealing underlying personal data. ZKPassport shows this is technically achievable today, using the same ICAO open standards infrastructure already relied on by HM Passport Office and international border systems. The digital ID should also support verifiable credentials standards compatible with ZKP-based selective disclosure, and technical standards should be designed for interoperability with emerging international standards, including those being developed by

Part	*Consultation Question*	*Aztec Labs / ZKPassport Response*
		the EU for its digital identity wallet, which uses Aztec Labs' zero-knowledge cryptography (including Noir, Aztec Labs's programming language).
	2.2.Q3 — Do you think people should be able to choose to store their national digital ID directly in holder services (digital wallets) other than the GOV.UK Wallet, that are certified to meet government standards?	Yes, strongly agree. Letting people choose certified third-party wallets reinforces the principle that the digital ID is optional and citizen-controlled. Open-source, self-custodial solutions like ZKPassport can provide equal or greater security than centralised wallets, precisely because they don't require personal data to be sent to or stored by any third party. As long as wallet providers are certified under the UK trust framework and meet the relevant security standards, citizens should be free to choose the wallet that best fits their needs and privacy preferences. This also encourages innovation and competition in the digital identity space.
Part 3: Useful	*3.3.Q1 — To what extent do you agree or disagree that the private sector and third parties should be able to use the digital ID alongside other options?*	Strongly agree. Private sector adoption is essential to making the digital ID genuinely useful, and age verification is the clearest near-term opportunity. The Consultation already recognises that the digital ID could be used for purchasing alcohol, accessing age-restricted websites, and other everyday transactions. ZKPassport can support all of these use cases today, with a single privacy-preserving proof that works across both online and offline contexts. A customer buying a bottle of wine could prove they're over 18 by tapping their phone, without revealing their name, date of birth, or any other personal information. The same proof works for online platforms, right-to-work checks, and KYC processes. This kind of interoperability between public and private sector use cases is exactly what will drive adoption.
	3.4.Q1 — Are there any additional challenges not captured in the Consultation that businesses would face in carrying out fully digital right to work checks for all new workers?	The main challenge is privacy. A fully digital right-to-work regime that relies on traditional verification methods would mean employers (or their service providers) routinely accessing and processing sensitive nationality, visa, and immigration data. This creates data protection risks, increases the compliance burden on businesses, and exposes individuals, particularly foreign nationals, to potential discrimination. ZKP technology solves this cleanly: an individual can prove they have the right to work in the UK without revealing their nationality, visa type, or immigration status. The employer gets the binary answer they need (right to work: yes/no), and nothing more. ZKPassport already supports this kind of selective

Part	*Consultation Question*	*Aztec Labs / ZKPassport Response*
		disclosure, and its integration with the ICAO trust chain means the underlying data is as authoritative as a passport check at the border.
Part 5: Trusted	*5.1.Q1 — Are there any additional measures, beyond the principles and standards set out in the Consultation, that we should consider to further protect user data?*	Yes. The strongest additional measure the government can adopt is a technical architecture that makes data misuse impossible by design, not just prohibited by policy. ZKP technology provides exactly this. When a citizen uses a ZKP to prove they're over 18, the service provider never receives their date of birth, name, or any other personal data. There's nothing to leak, nothing to breach, and nothing to misuse. We'd also recommend that all ZKP circuits used in the digital ID system be published as open-source code and subject to independent cryptographic audit.
	5.1.Q2 — How should the government ensure transparency around how national digital ID data is used?	The most effective way to ensure transparency is to use a technical architecture that makes excessive data collection impossible by design. ZKP technology does exactly this: because personal data is never sent to or stored by service providers, the question of how that data is later used simply doesn't arise. The government should publish open-source specifications for the ZKP circuits used in the digital ID system, so they can be independently audited by the public, privacy organisations, and the ICO. This provides mathematical, verifiable proof that the system works as described.
	5.2.Q1 — Are there any additional security safeguards that should be considered in relation to the national digital ID system?	Yes. We'd recommend integrating ZKP technology as a core security safeguard. A ZKP-based architecture shrinks the attack surface of the entire system by ensuring that sensitive personal data, including biometrics, is never centralised, transmitted, or stored outside the citizen's own device. This eliminates the risk of mass data breaches and 'honeypot' attacks. Anchoring identity attestations on Ethereum means the system benefits from decentralised, tamper-proof security properties, adding resilience against state-level threats and single points of failure. We also recommend that all ZKP circuits and verification logic be open-source and subject to independent cryptographic audit.
	5.3.Q1 — What do you think are the most important factors we need to consider in order to ensure alternative access routes are secure?	The most important factor is ensuring that alternative access routes maintain the same cryptographic guarantees as the standard digital route. Any alternative that falls back on visual inspection of documents or manual identity checks reintroduces the fraud vulnerabilities the digital ID is designed to eliminate. The Consultation rightly notes that identity fraud

Part	*Consultation Question*	*Aztec Labs / ZKPassport Response*
		represented 59% of all cases filed to the Cifas National Fraud Database in 2024. ZKP-based verification addresses this head-on: a ZKP is mathematically unforgeable, meaning it's impossible to create a valid proof without holding the genuine underlying credential. Even in offline or low-connectivity scenarios, ZKPassport's architecture supports the generation and verification of cryptographic proofs without requiring a real-time connection to a central database.

ANNEX 1 – COMPARISON OF DIGITAL IDENTITY TECHNOLOGIES[5]

	ZKPassport	Persona & Traditional KYC Providers	EUDI Wallet
		Overview	
Description	ZKPassport is an open-source identity verification solution that enables users to prove specific facts about themselves: age, nationality, personhood, without revealing any underlying personal data. It works by scanning the NFC chip embedded in a biometric passport or national ID using a smartphone, a private live face match, then generating a zero-knowledge proof entirely on-device. That proof can cryptographically demonstrate, for example, that the user is over 18, without disclosing their date of birth, name, or any other attribute.	Persona is a traditional identity verification platform for KYC, AML, and onboarding workflows. The product handles document checks, biometric liveness, and watchlist screening as a server-side SaaS. Users scan their documents and record the video of their face and upload to Persona servers where it gets verified and stored. There are other KYC providers like Sumsub, Entrust that work in a similar way.	EU-mandated digital identity wallet rolling out across all 27 member states. Each country issues its own wallet that meets common EU standards, so credentials work cross-border. Stores government ID, driving licence, diplomas, payment cards, and more. Supports selective disclosure of attributes; implementations may still reveal underlying data depending on credential format
Website	www.zkpassport.id	https://withpersona.com	https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/overview
		Core Architecture	
Core Technology Future Proof	✅Zero knowledge proofs ZK-SNARKs (Noir circuits) over ICAO-standard eMRTD NFC chip signed data. All computation on-device. Verifier receives a math proof, never raw data.	❌ Traditional identity verification (no ZK proofs) Document checks and face matching use Persona's closed-source ML models, supporting IDs from 200+ countries. All processing runs server-side. The verifying business gets the result plus, depending on its setup, the underlying personal data. ID issuer → Persona's servers →	🟡 Selective disclosure today via SD-JWT VC and ISO mdoc proves specific facts (over 18, EU resident) without revealing the underlying document. Zero-knowledge proofs and BBS+ signatures (better unlinkability) are flagged in the spec as planned but not yet live. Future-proof in design intent, but the privacy-

[5] **Note**: The table is intended to serve as a general frame of reference, rather than an exhaustive description and comparison of each digital identity technology.

	ZKPassport	Persona & Traditional KYC Providers	EUDI Wallet
	ICAO PKI → issuing state CSCA certificate → passport chip signature. Trust = you trust the state that issued a passport. Aligned with emerging privacy-first regulatory trends.	the business. Trust = you trust Persona, their security, and how the business handles your data. Aligned with current KYC/AML frameworks; evolving toward data minimisation,	enhancing crypto isn't shipping in v1.
Issuer	Works with existing passports and ID cards issued by governments	Uses existing ID documents	Different levels of attestations issued by trusted providers - governments, universities, employers, etc.
Trust Anchor	Government PKI + Cryptography	Vendor Judgement	Issuer Signature
Open-source	✅ https://github.com/zkpassport	❌ Closed-source SaaS	✅Spec is open - https://github.com/eu-digital-identity-wallet
Use cases	Proof-of-personhood, age verification, sanctions screening, liveness check	Age verification, sanctions screening, liveness check	Age verification, custom credentials
Used in production	✅Used by a couple organizations to verify age and uniqueness. Used by Aztec Foundation token sale to conduct sanctions screening..	✅ Used at scale by OpenAI, LinkedIn, Twilio, Square, Etsy, Gusto, and Udemy for KYC, age checks, and onboarding.	🟡 Pilots running in Germany, France, Italy, Spain, Netherlands, Sweden, Poland, and others. France Identité is being upgraded into an EUDI Wallet. Member states must offer wallets to citizens by December 2026, but most experts expect that deadline to slip for several countries. Real adoption is early
Onboarding	🟢 Works with any biometric passport or compatible national ID a user already holds, so onboarding is a one-time NFC scan on their own phone with no enrolment infrastructure required.	🟡 Onboarding is a guided document scan and selfie flow that works with the broadest range of IDs and the lowest hardware bar, but each integrating business runs its own onboarding so users repeat the process across services.	🟡 Each Member State stands up its own onboarding pipeline tied to national PID issuance, meaning users must re-onboard from scratch into a state-issued wallet even if they already hold a valid passport or national ID, and non-citizens/non-residents of the issuing state are excluded by design.

	ZKPassport	Persona & Traditional KYC Providers	EUDI Wallet
Interoperable between Web2 and Web3	✅ Proofs are easily verifiable both offline and with blockchain technology.	🟡 Strong Web2 integration via API, webhooks, and SDKs. Web3 support is limited to reading wallet risk data from Chainalysis and reusable KYC via Persona Connect. Verification still runs off-chain on Persona's servers and cannot be checked by a smart contract.	🟡 Strong Web2 interoperability designed for use across EU public services, banks, telcos, and online platforms. Web3 fit is unclear. The spec doesn't mention blockchain integration, and there's no clear path for using EUDI credentials in dApps today, though nothing technically prevents it.
Cross-border usability	✅ Global (passport-based)	❌ Vendor-dependent	🟡 EU
Privacy and Security			
Data Sharing Model	✅ Proof only. Eg: proof that the user is above 18 without revealing DOB	❌ Full document	✅ Selected attributes. Eg: only DOB.
Privacy from issuer	✅ Yes	❌ No	🟡 Likely yes, but implementations are pending.
User Control	✅ Users are in full control of their data and what they want to prove. User initiates every proof using their government ID. Data lives solely on their phone.	❌ The user submits documents and selfies through Persona's flow. The user does not hold the credential. Data retention is set by the business. Users can request deletion via the business.	✅ Users decide which credentials to share, with whom, and for what purpose.
Biometric Liveness	✅ Relies on a simple open-source (MIT licence) machine learning model for local private face matching, which helps ensure the liveness check is accurate and matches the person on the government issued ID.	✅ Selfie and video liveness using Persona's own ML, with gesture guidance and multi-frame analysis. Designed to defeat photos, masks, and deepfakes. Effective in production, though the model is closed-source and the check runs on Persona's servers, not the user's phone.	🟡 Liveness checks happen during initial enrolment to bind the wallet to the holder. Standards reference EU biometric and anti-spoofing requirements, but implementation is left to each member state, so quality will vary.

	ZKPassport	Persona & Traditional KYC Providers	EUDI Wallet
Age Verification			
Private	✅ Predicate-level disclosure - Users prove they are above 18 without revealing their exact DOB. The service learns literally only whether the user passes the age threshold.	❌ The service receives the verification result plus, depending on integration setup, names, dates of birth, document numbers, and other personal data. Persona itself sees all of it during processing. The user has no cryptographic guarantee that less data than required is shared with the business.	🟡 Selective disclosure allows users to reveal only DOB without revealing other credentials; but implementations might not have predicate-level disclosure.
Regulatory fit	✅ Architecturally fully aligned with data minimisation mandates in UK Online Safety Act, EU Digital Services Act, and US KOSA proposals. No behavioural profile created.	🟡 Strong fit with traditional KYC and AML rules (FinCEN, FCA, MAS) because that's what the product was built for. Less aligned with newer data minimisation laws, which favour systems that share less data.	✅ EUDI is the regulation. eIDAS 2.0 makes it mandatory across the EU by December 2026.