Whitepaper

Private Evidence

Zero-Knowledge Proofs and Their Potential

Authors
Bootsma, S.E. (Sven)
Ellen, F. (Fokel)
Otto, D.P. (David)
Sijpesteijn, T. (Thom)

TNO innovation for life

Contents

Introduction

Can you prove something without revealing the data behind it? Your personal data, your contacts, your preferences and your (online) behaviour are incredibly valuable. With many services tracking our every move, maintaining privacy can feel like an impossible challenge. One might argue, *"Just avoid services that collect personal data."* If you disagree with how a given platform handles your information, you could choose not to sign up. But in practice, the decision is rarely that straightforward. In many cases, individuals lack meaningful alternatives or face exclusion from essential services.

A clear example of this tension arises in the context of children accessing social media. While platforms are increasingly urged to restrict access for users under a certain age, verifying this requirement often means asking adolescents to upload official identity documents. In doing so, they reveal far more than just their age, such as their full name, the document number, and other sensitive details that are not necessary for the purpose of age verification. For parents, this raises a critical concern. Is it truly necessary to share so much personal information just so a teenager can access a social media app? And what guarantees are there that this data will not be stored, reused, or leaked?

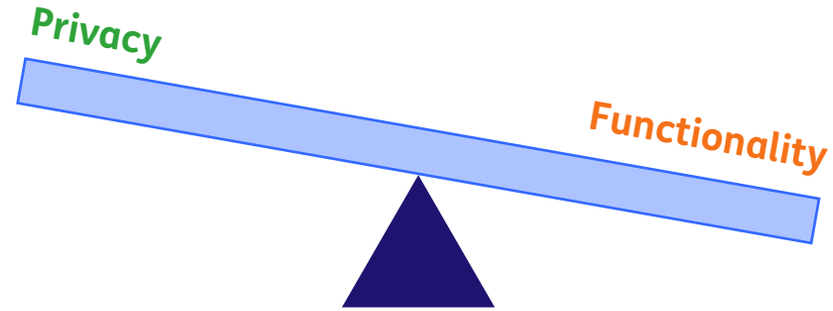
Zero-Knowledge Proofs (ZKPs) offer a privacy friendly alternative. Instead of handing over full documents, young users could prove they meet the age requirement without disclosing any additional personal information including their date of birth. This ensures that platforms receive the verification they need while young users retain control over what is shared.

In the first section, we will explain what ZKPs are and how they might be employed in the previously mentioned example of age verification by social media platforms. We will use compelling examples to show how ZKPs work. After that, we explore what kinds of knowledge can be proven using ZKPs, give examples of how they are already used in real-world applications, such as secure remote password protocols and digital wallets, and also look ahead to what will be possible in the near future, like verifying the correct training of an AI model.

Zero-knowledge proofs represent a new approach to data sharing. They allow individuals to prove eligibility without exposing personal data. Although the concept has been known for decades, recent advances have significantly improved ZKPs, enabling broader real-world adoption. To unlock the full potential of ZKPs, action is needed. In the final section, we outline how governments and businesses can lead, support, and adopt ZKPs to build more secure and privacy preserving systems.

Balancing privacy and functionality

Striking a balance between privacy and functionality is essential when sharing data. Governments and commercial entities often require data to provide services, for example to confirm that an individual is old enough to vote or that they earn enough money to qualify for a mortgage. However, individuals often have little control over how much data they have to share, leading to infringements on their privacy. Zero-knowledge proofs can offer a solution to this dilemma by allowing individuals to prove very specific statements without revealing anything beyond those statements. For instance, individuals can prove their age or income is above a certain threshold, without revealing their age of income itself – and without leaking any additional personal information.

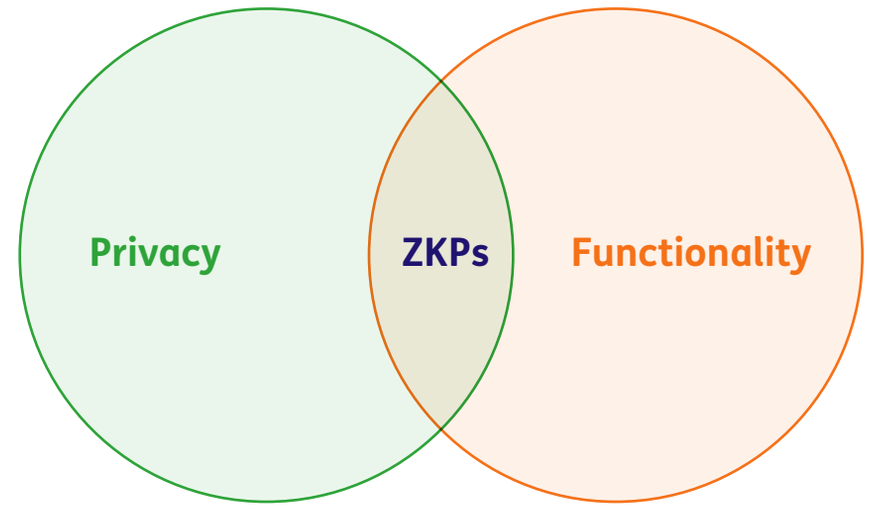


The challenge of balancing privacy protection and the practical need for data is readily visible in social media. In the EU, regulations such as the Digital Services Act (DSA) dictate the protection of minors from potentially harmful content. Australia even decided to ban the use of social media completely for users under 16. As a result, users have to prove that they are old enough to use a social-media platform, which, when implemented naively, involves sharing sensitive personal documents like an ID card. While a social-media platform is obligated to keep such documents safe, this safety is not guaranteed. Moreover, it gives a company information about a user that could potentially be used for other purposes than age verification. For example, their place of residence could be used to create targeted advertisements. This situation forces users into a position where they must make a stark choice: either share more data than you might be comfortable with, or have no access to a social-media platform.

Zero-knowledge proofs (ZKPs) offer a solution to this dilemma by allowing someone to prove a statement, such as <this user is at least 16 years old>, without revealing additional personal information. They work through a cryptographic process in which a user sends out claims that they could only make if they had an ID document proving they are over 16, without revealing anything else about the documentation. This solution assures a social-media company that the user has not lied about being above the age threshold, while the user is assured that the company has not obtained additional personal information. In general, zero-knowledge proofs allow a person to prove that a statement is true, without revealing anything else. As a result, zero-knowledge proofs can protect user privacy and provide a functional amount of data for a company, without forcing a trade-off between the two.

Zero-knowledge proofs allow someone to prove a statement is true, without revealing anything else.

Zero-knowledge proofs have many applications beyond age verification. ZKP solutions are already used in processes such as user authentication, cryptocurrency transactions and securely proving personal details in digital wallets. They are also opening doors to new applications, such as privacy-friendly mortgage approval and cryptographically verifiable training of AI models. As zero-knowledge proofs develop and are adopted more widely, they pave the way for a fundamentally different approach to data sharing and trust—one where individuals can prove statements without surrendering private information, working together with policy makers and systems designers toward stronger, more resilient digital ecosystems.



How do zero-knowledge proofs work?

Zero-knowledge proofs let someone prove that a statement is true without revealing any other information. While that might sound impossible at first, it works thanks to clever mathematical techniques. To make this idea more concrete, we will start by walking through the age verification example from the introduction. After that, we will look at a more intuitive example.

Suppose Peggy is 16 years old and wants to be able to use a social-media account on the fictitious platform Veeva. Veeva requires Peggy to prove that she is 16 in order to access their services. Veeva prefers not to collect sensitive personal data such as identification documents, as this could increase the risk of data breaches that would cause legal problems for the company. Therefore, Veeva has decided to use zero-knowledge proofs for age verification, so that they find out nothing about Peggy except the fact that she is at least 16 years old.

A zero-knowledge proof has four main ingredients:

1. a *prover*: Peggy
2. a *verifier*: Veeva
3. some *secret data*: for example, Peggy's national ID card
4. and a *statement* about the data that will be proven: *<Peggy is at least 16 years old>*

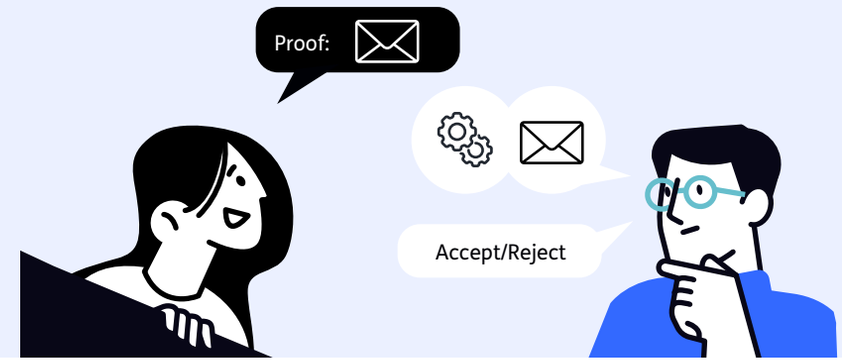
The general goal of a zero-knowledge proof is to prove a statement about the secret data without revealing anything else about the secret data, i.e. proving that Peggy is at least 16 years old without Veeva receiving her national ID card. Note that the statement can only be proven by someone that has the secret data, so Peggy would not be able to make a proof about her age if she did not have a valid ID card.

The protocol proceeds in three general steps, as follows.

Step 1: **Announce the claim**
Firstly, the prover announces what claim they are going to prove. In our age-verification example, this means that Peggy announces that she is going to prove the statement *"Peggy is at least 16 years old"*.

Step 2: Communicate & calculate
In the second step, the prover and the verifier communicate back and forth. The verifier may ask the prover certain mathematical questions or give them some specific numbers to use in their calculations. These questions are designed so that someone who doesn't actually know the secret data would have a hard time answering them correctly. The prover then uses both their secret data and the information from the verifier to do some calculations which will result in a proof.

Step 3: Send & verify proof
In the last step, the prover sends their proof to the verifier, and the verifier performs some calculations to check whether the proof was correct. In our example, this means that Peggy sends her proof that she is at least 16 years old, and Veeva checks the validity of the proof. If Peggy's proof is correct, Veeva accepts that Peggy is at least 16 and is allowed to use their services. Otherwise, Veeva rejects the proof.



In practice, Peggy and Veeva use mathematical encodings of the statement *<Peggy is at least 16 years old>* and the secret data (Peggy's ID card). These encodings allow the Peggy to perform calculations on the encoding of her ID card that *she would only have been able to perform if she had that ID card.* However, while Veeva is able to check that those calculations confirm the statement *<Peggy is at least 16 years old>*, the platform is not able to get any more information about Peggy's ID card, preserving her privacy.

The way zero-knowledge proofs work for applications such as age verification is complicated, because of the required mathematical machinery. However, there exist many examples of zero-knowledge proofs that are more intuitive, such as the story of the colour blind friend.

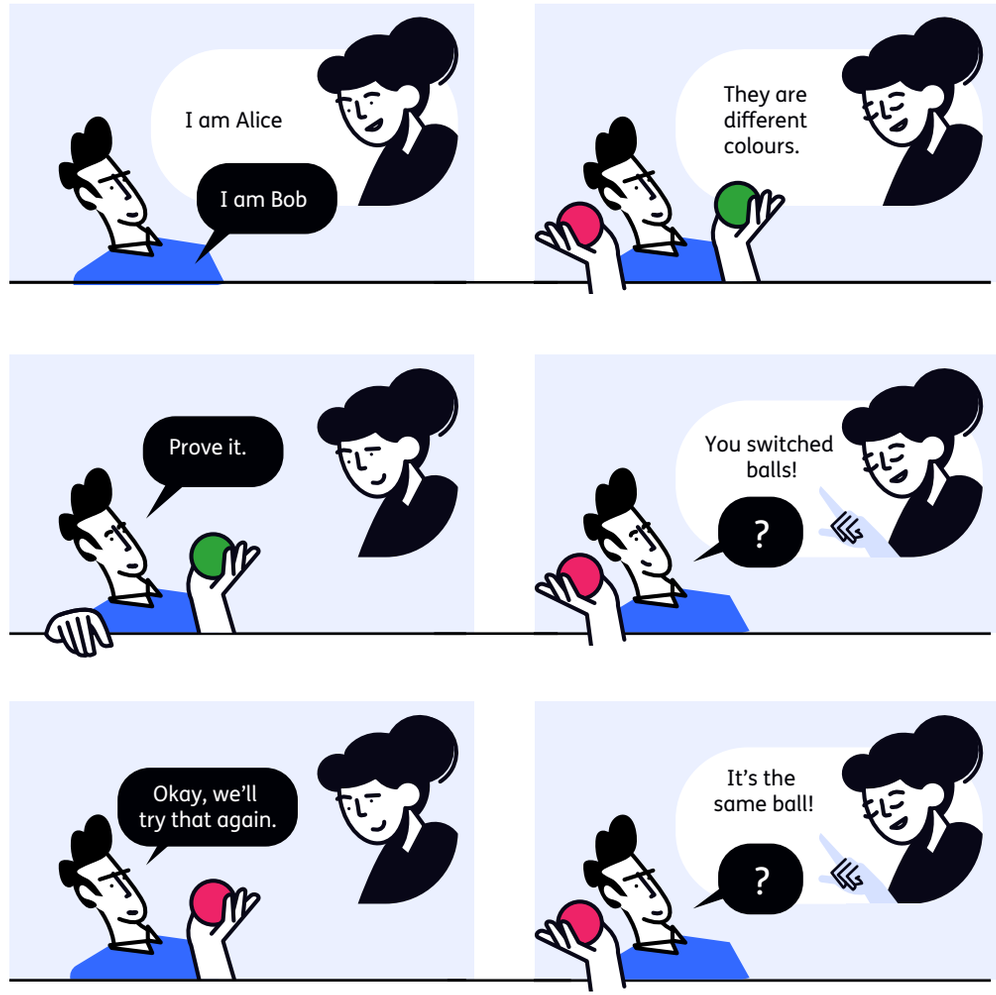
Making ZKPs Practical: Non-Interactivity
The description above is a general sketch of a ZKP in the context of age verification, where a prover and a verifier interact in several rounds. In practice, it is useful if the prover can complete the process without going back and forth with the verifier. Indeed, there are techniques to make ZKPs *non-interactive,* meaning that there is no need for back and forth communication. In this case, the prover prepares everything in advance, and the verifier only needs to check the result at the end. Non-interactivity greatly simplifies how zero-knowledge proofs can be used in real-world systems.

An intuitive example: the colour blind friend

Imagine Alice has two balls. These balls are the same size and weight — the only difference is their colour. One ball is red, the other green. Alice's friend Bob is colour blind and cannot tell the difference between the two. Alice wants to prove to Bob that she can tell the difference between them.

Alice says: *"They are different colours."*
Bob is sceptical: *"Prove it."*

There is one catch: Alice does not want to tell Bob which ball is red and which one is green. In this situation, the secret data is which ball is red and which one is green, and the statement about the secret data is *<the balls are different colours>*.



To solve this, Alice suggests playing a game:

1. Bob holds up one ball.
2. Bob then hides both balls behind his back and randomly decides either to show Alice the same ball as before, or to switch the balls behind his back and show the other one.
3. Bob shows the chosen ball.
4. Alice then says either *"You switched balls"* or *"It's the same ball."*

Because Alice can see the colour difference, she will know whether Bob switched the balls or not.

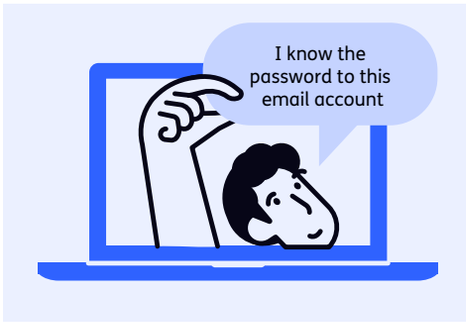
From Bob's point of view in step 4, it looks like Alice is **guessing** whether the balls were switched or not. Indeed, after playing this game once, there is a 50% chance that Alice just guessed and got lucky. That is why the above game is repeated as many times as Bob wants. For instance, when playing two rounds of the game, Alice only has a 25% chance of guessing correctly by luck. After playing ten rounds, Alice's chances of guessing correctly have already dropped to less than one in a thousand. After even more rounds, the probability of guessing correctly every time becomes vanishingly small -- so small, that Bob is convinced Alice is not just guessing and the balls truly are different colours. And, as desired, she will have demonstrated this **without ever revealing** which ball is red and which is green.

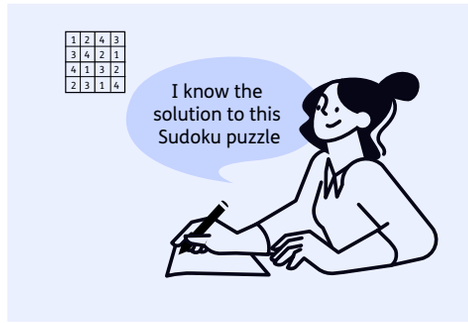
What kinds of knowledge can be proven?

We have seen that zero-knowledge proofs allow the prover to convince the verifier that some statement, like *<the balls are different colours>,* is true without revealing any extra information about the secret data. But what would qualify as a statement or as secret data for the purposes of a zero-knowledge proof? As we have seen, a zero-knowledge proof requires the secret data and the statement to be expressed mathematically. Theoretically, any kind of information—whether a number, the execution of a computer program or even something as complex as biometric data—can be expressed in mathematical form. Here are some examples of statements that can be proven with zero-knowledge proofs.

Knowledge of a secret

The prover possesses some kind of information and wants to prove to the verifier that they possess this secret information. This secret information could be many different things, such as a password, a private key, or even the solution to a sudoku puzzle. The prover does not reveal anything about the secret information except the fact that they know it; for example, they prove they have the password to an email account, without ever sharing what that password is.





Knowledge/ownership of a certain property

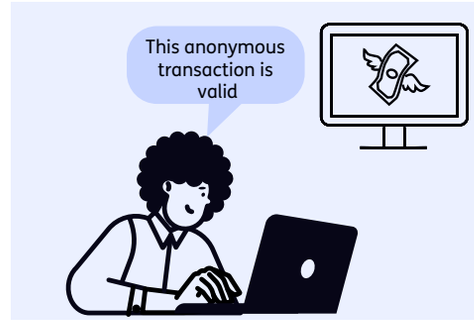
The prover has a particular property and wants to prove that this is the case without revealing extra information. This could be something like having a driver's license, specific age or income. It could even be a statement about supply chains, such as "this chip was produced in a trusted factory".

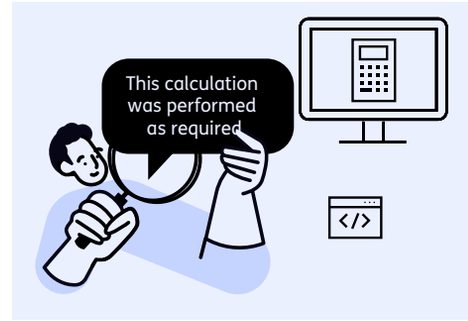
Membership of a set

The prover belongs to a certain predetermined group and wants to prove that this is the case. For example, the prover might belong to the group "citizens of the Netherlands who are eligible to vote" or "people possessing a ticket for this flight". The prover wants to prove their membership to the verifier without having to share which member of the group they are.

Correctness of computation

The prover has been entrusted to perform some kind of computation, such as a cryptocurrency transaction or running a computer script written by someone else. They wish to prove to the verifier that they did this according to the instructions they were given.





The broader context of zero-knowledge proofs

Zero-knowledge proofs have been around for decades, with the first academic paper on the topic being published by Goldwasser, Micali and Rackoff in 1985 [1]. Research continued throughout the 80s, 90s and 2000s with numerous improvements and new ideas. Since the 2010s, cryptocurrencies have spurred increased interest in ZKPs and stimulated further (academic) developments and adoption. ZKPs have several applications in the blockchain space, geared toward both privacy as well as efficiency. Outside of cryptocurrency, ZKPs adoption is still less mature, but some experts expect wide adoption of the technology in the next decades [2]. ZKPs are usually considered under the broader umbrella term of privacy-enhancing technologies (PETs)[1].

The market for ZKPs is pushed by a dynamic field of technology companies, cryptocurrency applications and research institutions, and is expected to grow significantly in the future [3] [4]. Within cryptocurrency, the biggest players using ZKPs are Worldcoin, Immutable and ZCash, each with a market cap of above around 500 million USD at the time of writing [5]. Outside of cryptocurrency, large international companies are also turning towards ZKPs. Between 2021 and 2023, Alibaba was the largest patent filer for ZKPs, and others such as Intel and Microsoft are working on the technology [6]. There are also many startups in the field, including NEXUS, RISC0, Aleph0 and StarkWare.. Notably, the potential of ZKPs is not limited to the commercial domain. Indeed, zero-knowledge proofs are clear candidates to facilitate innovative IT infrastructure concepts like Zero-Trust Security and Data-Centric Approaches. These set as explicit goals by e.g. NATO [7] [8], which may also foster adoption by other governmental or international organisations. At the same time, a lot of developments are still in the research phase, with many universities and research institutions actively working on the topic. As the technology matures, efforts into standardisation will have to be expanded to ensure consistency, security and usability of ZKP schemes across different applications. Both the International Standards Organization (ISO) and the National Institute of Standards and Technology in the USA are working on developing standards for zero-knowledge proofs [9] [10]. A community-driven effort to develop standards called ZKProof is also underway [11].

1 Privacy-enhancing technologies (PETs) | ICO

Proofs beyond privacy: ZKPs for efficiency
So far, we have focused on the privacy-preserving aspect of zero-knowledge proofs: ensuring that secret data remains hidden, even when making provable claims about it. However, some proof systems offer an additional advantage: they allow a verifier to check a statement without having to carry out the underlying computations.

This isn't particularly useful for simple statements such as <*Peggy is at least 16 years old*>, but it becomes valuable for claims like <the outcome of this very expensive calculation is 15.619>. Naively, checking whether a calculation was performed correctly would require re-doing the calculation, which may be very costly. In contrast, using zero-knowledge proofs, the correctness of somebody else's calculation can be checked by just verifying a proof. For certain proof systems, this verification procedure is much less involved than the computation underlying the statement. Using ZKPs can therefore yield significant gains in terms of efficiency and scaling for the verification of a computation.

In some cases, efficiency gains have surpassed privacy as the primary driver for using cryptographic proof systems. Some applications even use proofs which don't have zero-knowledge properties at all. These techniques are often (informally) still referred to with the abbreviation 'ZK', which can be somewhat confusing.

An example of using (ZK)Ps for efficiency occurs in blockchain systems. Here, cryptographic proofs allow users to verify the integrity of a blockchain without downloading and validating every block. Instead, they check a short proof generated by someone else — someone with more computational resources — who already validated the chain. As we'll explore later, similar efficiency benefits can apply to AI use cases as well.

What is currently possible?

Quite a lot is already possible with zero-knowledge proofs. Here, we outline three examples of mature applications of the technology.

Cryptocurrency users can prove the validity of transactions without revealing personal details. Zcash employs zero-knowledge proofs to enable private peer-to-peer payments. This is unlike other cryptocurrencies like Bitcoin, where transaction details (sender, recipient, and amount) are publicly visible.

Secure Remote Password Protocol (SRP) allows logins without sending passwords to the server by using ZKPs. This is already used by Apple iCloud, ProtonMail and 1Password, as it is extremely resistant to password-cracking attacks. With traditional password-authentication methods a client typically sends their password or a hashed version of it to the server, which creates risk if the server is compromised. With SRP the client proves to the server that it knows the password without revealing it or any other information that could be used to derive it. Intercepted data cannot be used by attackers to gain system access. This guarantees no information is disclosed during authentication.

Digital wallets (incl. age verification) empower users to manage their personal data securely and share it selectively. Digital wallets like Yivi (NL) are identity wallet apps that allow individuals to store personal information such as age, contact details, financial records and educational credentials directly on their smartphones, protected by a PIN. These apps use zero-knowledge proofs to enable users to authenticate themselves and share specific data attributes without disclosing unnecessary information. While generic digital wallets using ZKPs already exist and offer age verification, dedicated apps for age verification to protect minors are also in demand [15].

What will be possible in the future?

Applying for a Mortgage

By leveraging ZKPs, mortgage approvals can become faster, safer, and more privacy-friendly for both applicants and financial institutions. Applying for a mortgage usually involves sharing a significant amount of sensitive personal information with a bank or mortgage advisor. Applicants must provide documents such as their passport, pay slips, an employer's statement, details of their savings, outstanding loans, and sometimes even a health declaration. The bank or advisor then assesses the financial risk and determines whether the applicant qualifies for a loan and under what conditions.

The current mortgage application process has **several key issues**:

1. **Privacy:** Applicants must disclose more personal and financial information than necessary.
2. **Inefficiency:** Verification processes, sometimes manual, cause delays and increase costs.
3. **Liability:** Data breaches can result in severe fines for the bank.

Zero-knowledge proofs offer a way to address all these problems. At its core, the bank only needs to answer a simple question:
"Is applicant A at risk of not being able to repay a €400,000 mortgage over 30 years?"

By using a zero-knowledge proof, the customer proves the claim that they are able to repay a mortgage, without revealing any underlying data like passport, pay slips, employer's statement, savings, outstanding loans, and health declaration.

This approach resolves all the issues:

1. **Privacy is preserved, as the applicant maintains full control over their data.**
2. **Inefficiency is eliminated, since no verification of individual documents is needed.**
3. **Liability is reduced, as the bank never stores the applicant's sensitive data, removing the risk of regulatory fines in case of a data breach.**

It would require cooperation between several different entities to the use of ZKPs possible for mortgage applications. The infrastructure and incentives to make this happen will need to be developed collaboratively by financial institutions, technology providers and regulatory bodies.

Making AI verifiable

ZKPs can be used to improve the trustworthiness of AI models for consumers. Consumers typically interact with AI in the following manner: a user device sends input to an AI service, which will run the appropriate model in the cloud and send back the result to the user device. For example, for many commercial Large Language Models (LLMs) like ChatGPT, users submit questions via an app or website and receive answers calculated in the cloud.
Using the cloud for computations has some advantages, such as enabling expensive computations to be performed on dedicated hardware and allowing AI vendors to keep their parameters and model secret. However, cloud use for computations also has *several key issues*:

1. **Data:** The consumer has no way to check on which data the AI model was trained.
2. **Training:** Even if appropriate data was used for training, the consumer must trust that the vendor followed the right training procedure and that the model was not modified post-training.
3. **Inference:** Consumers simply have to believe that the right AI model was run on their input.

Issues like these are addressed by the field of verifiable AI. At a high level, verifiable AI involves the AI vendor providing the results of the requested computation along with a proof that is was computed correctly. This proof allows the consumer to verify certain properties of the model and/or computation.

ZKPs can solve several key issues:

1. A **Proof of Data** shows that the data on which a model is trained satisfies certain characteristics. For example, one could show that a dataset contains no unwanted biases, without actually revealing the dataset itself.
2. A **Proof of Training** shows that the AI model was trained according to some predetermined training procedure, using exclusively a particular dataset and the appropriate parameters.
3. A **Proof of Inference** can be generated to show that the result that is sent back to the consumer was indeed arrived at by running the agreed model on the provided input. Without such a proof, the consumer has no way to check whether the AI vendor actually ran the appropriate model.

Although verifiable AI is an active area of research, these techniques are not yet used in practice much. This is likely due to a combination of two factors. Firstly, the computational cost of training and running AI models is already substantial, and incorporating ZKPs adds a significant performance overhead. Secondly, depending on the use case, there is not always a clear incentive for AI vendors to incorporate verifiability. Hopefully, verifiable AI will become more widespread as the field develops and vendors are incentivized, by vendor competition, demand from consumers or for other reasons.

Realising the potential of ZKPs

We have seen that ZKPs show promise in many different application areas. Despite their potential, however, they are not yet widely adopted. For some applications, such as the mortgage-application example sketched above, there is a lack of infrastructure and incentives that is preventing their adoption. For others, such as making AI verifiable, more research must be conducted before zero-knowledge proofs can be adopted. Both government and industry must play a key role in overcoming the barriers to the broader adoption of zero-knowledge proofs.

What governments can do

The government acts as a regulator, early adopter and funder of emerging technologies like ZKPs. The existence of zero-knowledge proofs opens the door to stricter privacy legislation, under which companies may never need to access individuals' data in the first place. However, regulatory barriers to the adoption of zero-knowledge proofs must be addressed — for example, laws that currently require banks to collect certain consumer data [12]. In addition to enabling adoption through regulation, governments can lead by example. Public services generate and manage vast quantities of sensitive data, making them ideal candidates for ZKP-based solutions. Pilots in areas like digital identity, tax filings, or eligibility verification could demonstrate both the feasibility and benefits of privacy-preserving technologies at scale.

As noted earlier, the advancement of ZKPs is being driven by a dynamic ecosystem of companies and research institutions. Continued public funding is essential to sustain academic research and to ensure that breakthroughs in this field align with societal priorities. By supporting domestic innovation and facilitating adoption of this technology, the government can help unlock new privacy-focused business models, strengthen strategic autonomy in key digital infrastructure, and capture value in the rapidly growing market.

What industry can do

Industry plays a key role in developing and delivering new technologies. Companies can invest in Research and Development on zero-knowledge proofs, creating innovative solutions to address consumer privacy issues. The large number of patents related to zero-knowledge proofs already reflects strong industry interest in the technology [6]. By offering zero-knowledge proofs to consumers, industry can help drive a technology push. This is already underway, with businesses such as JP Morgan exploring application in the finance and Walmart in supply-chain management [13].

Finally, businesses can support the zero-knowledge ecosystem by participating in and funding community-driven efforts. For example, the ZKProof initiative for standardisation includes major industry players such as Google, ING and Ethereum [11], while conferences like zkSummit receive sponsorship from a range of industry partners [14].

How TNO can help you get started with zero-knowledge proofs

TNO conducts active research into zero-knowledge proofs, ranging from fundamental mathematical research to practical, real-world applications. We aim to bridge the gap between academia, government and industry.

Curious about what zero-knowledge proofs could mean for your organisation? Don't hesitate to contact us. See the contact details on the final page of this whitepaper.

Bibliography

[1] S. Goldwasser, S. Micali and C. Rackoff, "The Knowledge Complexity of Interactive Proof-Systems," in Proceedings of the seventeenth annual ACM symposium on Theory of computing, 1985.

[2] B. Weiss, "A brief history of zero-knowledge proofs, the buzzy mathematical technique that's taken crypto by storm," Fortune Crypto, 5 June 2023. [Online]. Available: https://fortune.com/crypto/2023/06/05/zero-knowledge-proofs-history-zk-rollups-cryptography-zcash/. [Accessed 15 April 2025].

[3] DataString Consulting, "Zero Knowledge Proofs Market: Growth, Opportunities and Trends," January 2025. [Online]. Available: https://datastringconsulting.com/industry-analysis/zero-knowledge-proofs-market-research-report. [Accessed 15 April 2025].

[4] Aligned, "Aligned.co Projects $10 Billion Market for Web3 Zero-Knowledge Proof generation by the year 2030," 26 June 2024. [Online]. Available: https://www.aligned.co/blog. [Accessed 15 April 2025].

[5] CoinMarketCap, "Top Zero Knowledge Proofs Tokens by Market Capitalization," [Online]. Available: https://coinmarketcap.com/view/zero-knowledge-proofs/. [Accessed 15 April 2025].

[6] GlobalData, "Cybersecurity: who are the leaders in zero knowledge proof for the technology industry?," 11 September 2024. [Online]. Available: https://www.verdict.co.uk/innovators-cybersecurity-zero-knowledge-proof-technology/. [Accessed 15 April 2025].

[7] NATO, "NATO's Bold Digital Leap: A SECURE Cloud-Empowered Alliance," 9 12 2024. [Online]. Available: https://www.act.nato.int/article/natos-bold-digital-leap/.

[8] NATO, "NATO DIGITAL BACKBONE & NATO DIGITAL BACKBONDE REFERENCE ARCHITECTURE," [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/12/pdf/241213-DBRA.pdf.

[9] R. Viglione, "Standards for zero-knowledge proofs will matter in 2025," CryptoSlate, 15 February 2025. [Online]. Available: https://cryptoslate.com/standards-for-zero-knowledge-proofs-will-matter-in-2025/. [Accessed 15 April 2025].

[10] ISO, "ISO/IEC DIS 27565.2," [Online]. Available: https://www.iso.org/standard/80398.html. [Accessed 15 April 2025].

[11] ZKProof, "About ZKProof," [Online]. Available: https://zkproof.org/about/. [Accessed 15 April 2025].

[12] A. Ray, "Challenges of Zero-Knowledge Proof Technology for Compliance," 30 August 2023. [Online]. Available: https://www.forbes.com/councils/forbesbusinesscouncil/2023/08/30/challenges-of-zero-knowledge-proof-technology-for-compliance/.

[13] Fantastic IT, "Zero-Knowledge Proof For Businesses in 2024," 8 November 2024. [Online]. Available: https://fantasticit.com/zero-knowledge-proof-for-businesses-in-2024/. [Accessed 17 April 2025].

[14] ZKSummit, 2025. [Online]. Available: https://www.zksummit.com/. [Accessed 22 April 2025].

[15] "Development, Consultancy and Support for an Age Verification Solution," European Commission, 15 November 2024. [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/ae950883-112f-4139-989e-1c8d794bb77a-CN.

[16] eSafety Commissioner, "Tech Trends Issues Paper: Age Assurance," July 2024. [Online]. Available: https://www.esafety.gov.au/sites/default/files/2024-07/Age-Assurance-Issues-Paper-July2024_0.pdf?v=1732247092556.

[17] European Union, "Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework," 30 April 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng.

Authors
Bootsma, S.E. (Sven)
Ellen, F. (Fokel)
Otto, D.P. (David)
Sijpesteijn, T. (Thom)

Contact
Alexander van den Wall Bake

Business Consultant
Applied Cryptography & Quantum Algorithms

alexander.vandenwallbake@tno.nl
+31 6 515 813 39
www.linkedin.com/in/alexandervandenwallbake/

Context
This publication is the result of a collaboration between the Applied Cryptography and Quantum Algorithms group and TNO Vector, both of which are departments in the unit ICT, Strategy and Policy at TNO. The work was conducted as part of the ERP Next Generation Crypto project.

TNO innovation for life