# Scaling zero-knowledge identity.

How Self is empowering global digital identity using Google Cloud Confidential Compute

**White paper**
January 2026

Self

# Self is redefining how individuals prove who they are online without revealing sensitive personal data.

Self enables users to verify their identities or attributes (like age, nationality, or residency) while keeping underlying information fully private.

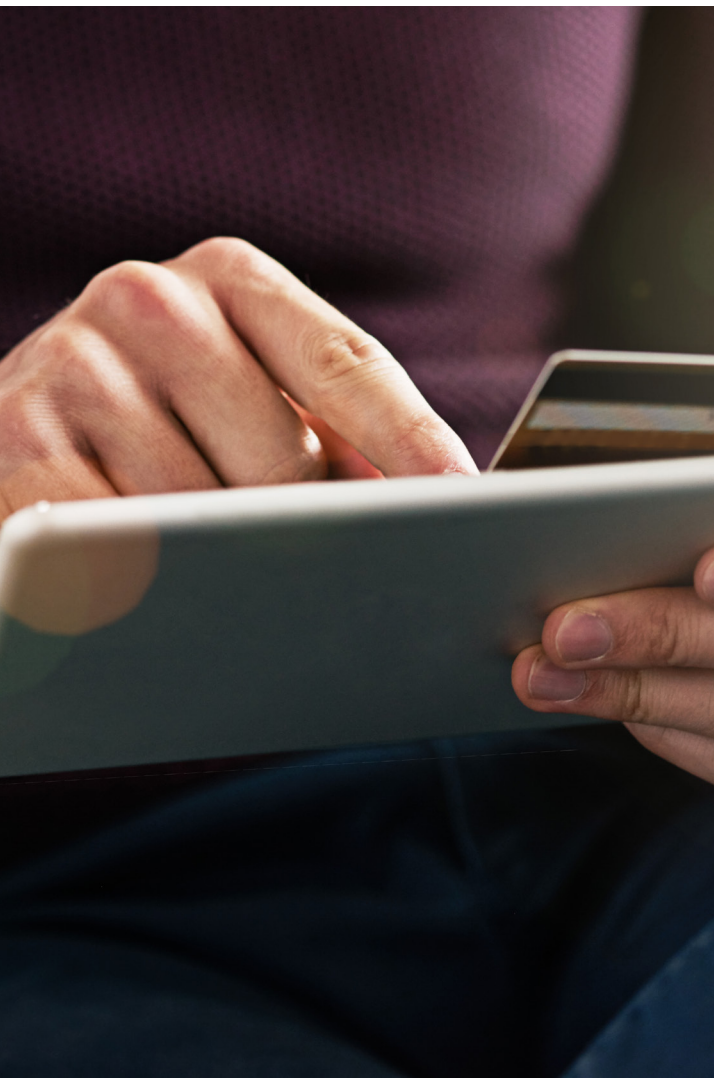
To make this possible at scale, Self built its zero-knowledge (ZK) biometric identity processing stack on Google Cloud Confidential Computing, leveraging Confidential Space to guarantee privacy, performance, and verifiability.

# The challenge.

Modern identity systems are built on trust, but traditional infrastructures expose personal information to service providers, databases, and intermediaries. Self sought to change that by making it possible to verify real-world identity credentials like biometric passports and IDs in zero-knowledge.

Biometric passports and IDs include NFC chips that store a user's biometric information, which is cryptographically signed by the user's issuing government.

**These signatures ensure that these documents cannot be forged, creating new defenses against AI-generated fake IDs.**



Leveraging biometric passports and IDs is no easy feat though, and required overcoming several major challenges:

**Signature diversity:** Different countries issue passports with different cryptographic signature schemes (RSA, ECDSA, varying hash functions). Each demands a dedicated ZK circuit.

**Massive proving keys:** The proving keys for validating national certificates can reach hundreds of gigabytes, requiring enormous RAM and compute capacity.

**User experience constraints:** Proof generation must happen fast enough to preserve a seamless user experience.

**Unlinkability:** Every identity proof must remain independent and non-correlatable to previous verifications.

**Trust boundaries:** Sensitive passport data must never leave the user's device or be visible to cloud operators.

Traditional infrastructure was not designed for this combination of cryptographic complexity and privacy requirements. Self needed a **confidential, elastic computing environment** that could handle heavy proving workloads globally without compromising verifiability or privacy.

# The solution.

## Self × Google Cloud Confidential Compute

To meet these demands, Self turned to **Google Cloud Confidential Computing**, deploying its ZK proving architecture inside **Confidential Space**, a trusted execution environment (TEE) powered by AMD Secure Encrypted Virtualization (SEV).

### This environment guarantees that data remains encrypted in memory and at rest, and that even Google or Self cannot access sensitive user information.

Each proving instance generates an **attestation report**, cryptographically proving to the Self app that it is communicating with a verified, secure environment.

# How it works.

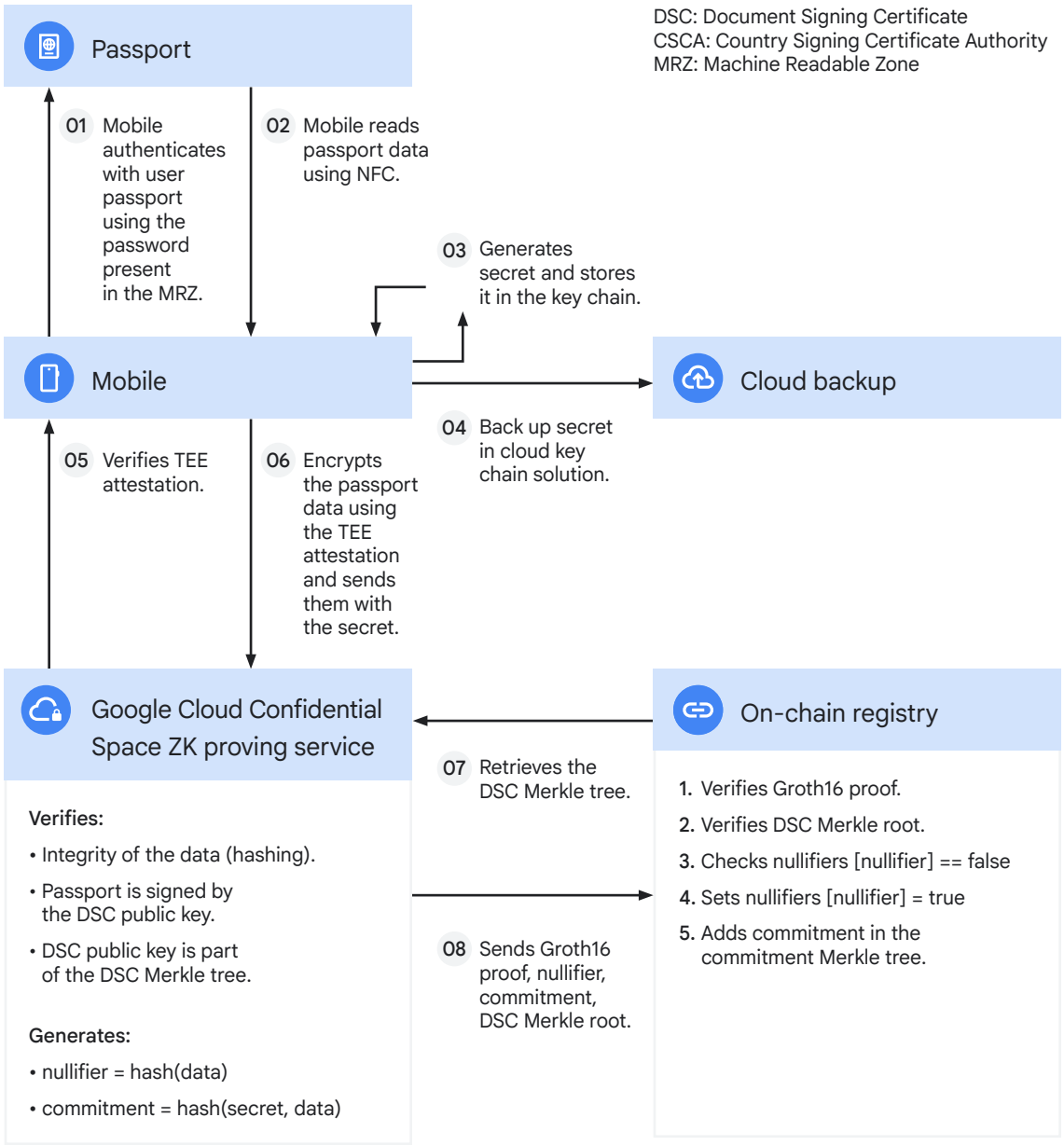
## 01 Registration

The user scans their biometric passport via NFC in the Self app.

The app verifies the chip's signature using country-specific certificates and establishes an encrypted session with a Google Cloud Confidential Space instance.

The instance verifies the document's authenticity, generates a ZK proof, and derives an **identity commitment** stored on-chain in a Merkle tree.

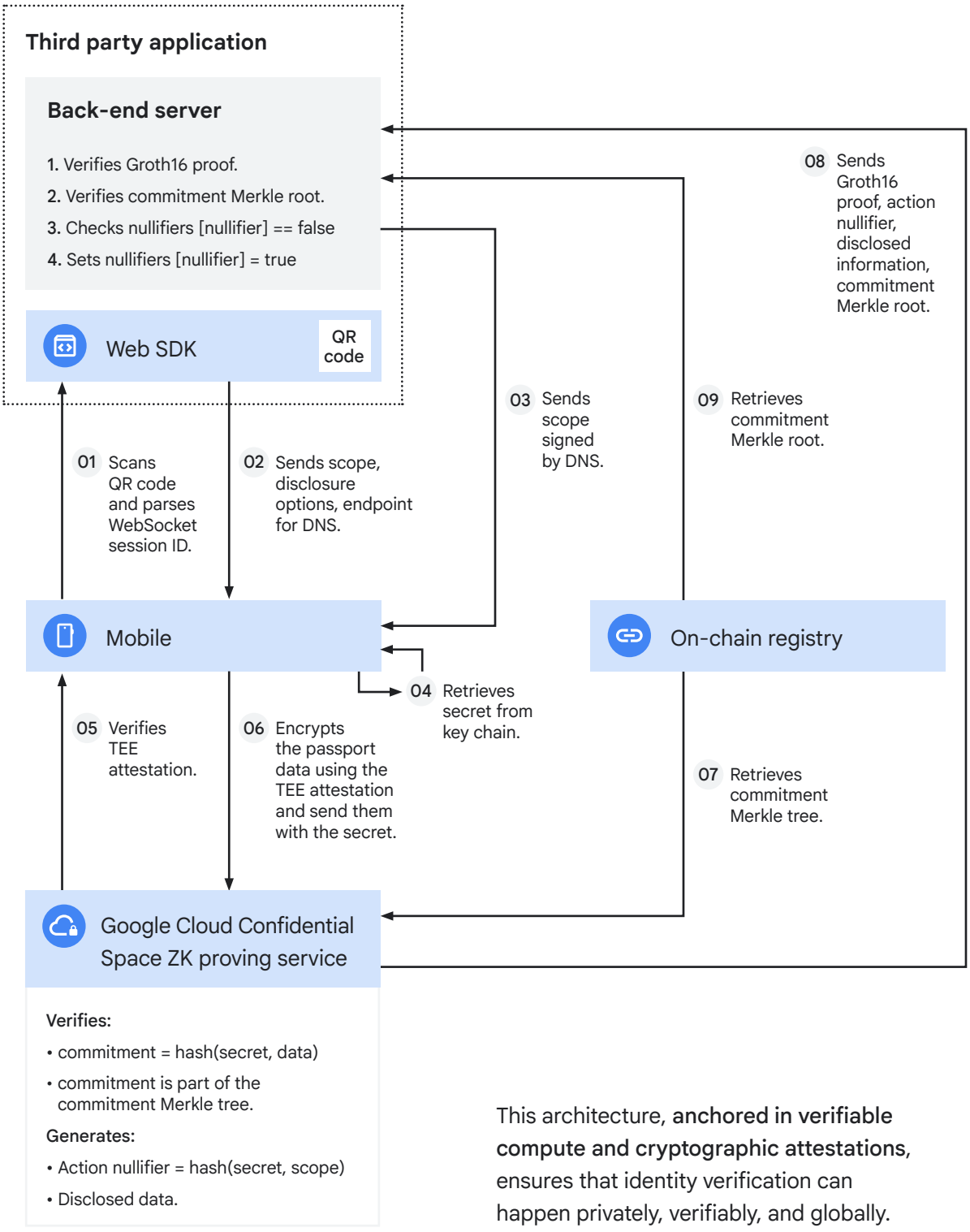
All user data is deleted immediately after proof generation; only the commitment remains, ensuring no sensitive data is retained.



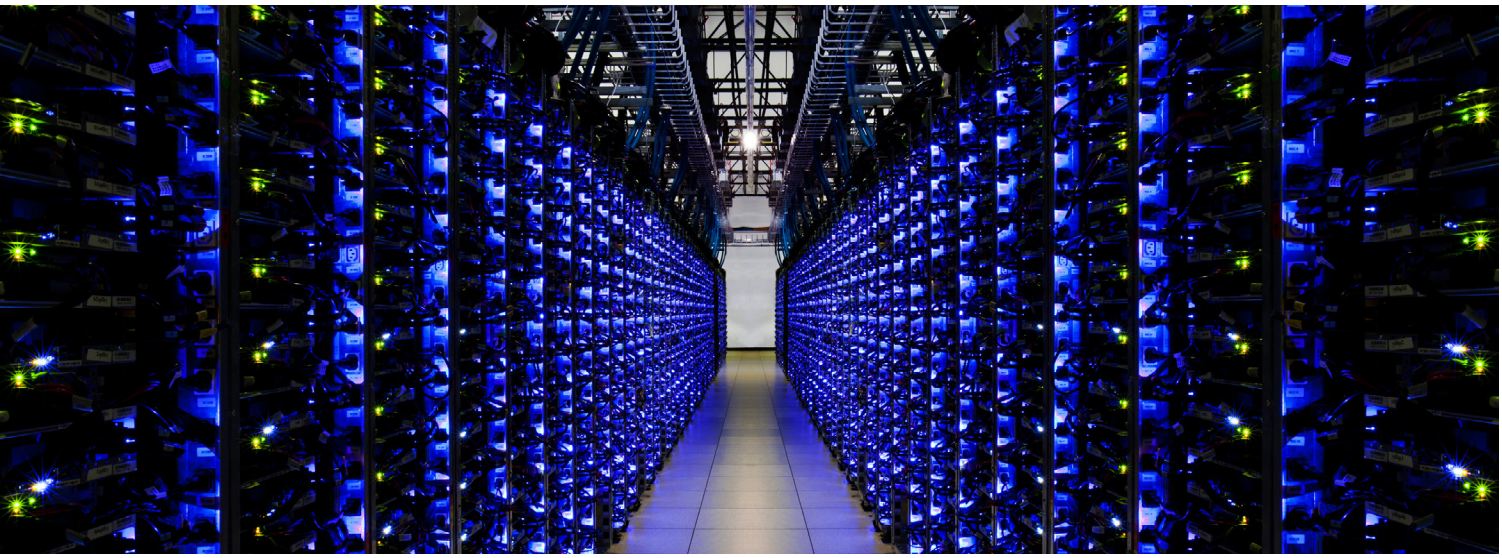

## 02 Disclosure

When another app requests verification (for example, “is this user over 18?”),
Self generates a lightweight disclosure proof referencing the on-chain commitment.

Only the requested attribute is revealed; all other data stays private and unlinkable.




This architecture, **anchored in verifiable compute and cryptographic attestations**, ensures that identity verification can happen privately, verifiably, and globally.



# Why Google Cloud.

Self selected **Google Cloud Confidential Space** for four key reasons:

## 01

### Performance and scale

Supports workloads requiring hundreds of gigabytes of RAM and parallel processing for large proving keys.

## 02

### Simplicity

Confidential Space provides native security for compute, storage, and networking without complex abstractions.

## 03

### Cryptographic attestation

Ensures the Self app can verify the integrity and origin of the proving workload before sending any passport data.

## 04

### Isolation guarantees

Hardware-based memory encryption prevents access by cloud providers, hypervisors, or internal operators.

These features make Confidential Space an ideal foundation for **privacy-preserving identity infrastructure**.

# Results.

By integrating Google Cloud's Confidential Compute platform, Self achieved:

## Global scalability

ZK identity verification now operates reliably across multiple countries and document types.

## High performance

Heavy proving circuits run efficiently and predictably, meeting real-world UX requirements.

## Privacy by design

User data is never visible outside the secure enclave, not even to Self.

## Verifiable trust

Every workload is cryptographically attested, ensuring end-to-end integrity from user to on-chain verification.

# Looking ahead.

The collaboration between Self and Google Cloud continues to expand. Future developments include:

**GPU acceleration** to further reduce proving times.

**Selfrica integration,** enabling confidential credential signing in regions with limited biometric ID penetration.

**Regional deployments** to meet data-residency requirements while minimizing latency.

**Joint research** into next-generation confidential compute primitives to push the boundaries of privacy-preserving verification.

## Together, Self and Google Cloud are laying the groundwork for a trust-minimized identity layer for the internet where users can prove who they are without ever giving up their privacy.

Self

# Self's mission is to make zero-knowledge identity practical and privacy-first.

With **Google Cloud Confidential Compute**, that vision is now reality: scalable, verifiable, and secure by design.

This partnership demonstrates how advanced cloud infrastructure and cutting-edge cryptography can come together to build a safer, more private digital future.

Google Cloud

Learn more about Self at docs.self.xyz or visit self.xyz.