PRISMPASS ECOSYSTEEM

Whitepaper v4

Een protocol voor anonieme authenticatie, selectieve identiteit en privacy-native opslag

Het licht zelf wordt nooit opgeslagen, alleen de kleur die jij kiest.

Auteur

I. Smid-Woelders

Locatie

Zwolle, Nederland

Datum

Juni 2026

Status

Vertrouwelijk concept, pre-public, voor geselecteerde reviewers

IP-bescherming

Invention Disclosure geregistreerd · Zenodo DOI: 10.5281/zenodo.20029291

Website

prismpass.globalsecurity.nu

SAMENVATTING

Wat dit document beschrijft

Elke keer dat iemand inlogt op een website, laat hij iets achter. Een naam, een e-mailadres, een wachtwoord, een sessie-ID. Servers slaan dat op. Databases groeien. Datalekken volgen.

PrismPass is een protocol dat die architectuur omkeert. In plaats van dat een server jou kent, bewijst jouw apparaat aan de server dat jij jij bent, zonder ooit iets te onthullen. De server ontvangt alleen een cryptografisch bewijs: geldig of ongeldig. Dat is alles.

Dit whitepaper beschrijft het volledige PrismPass Ecosysteem: vijf producten die samen een antwoord geven op vragen die de huidige infrastructuur nog onbeantwoord laat. Wie ben ik? Voldoe ik aan dit criterium? Wat wil ik delen? Handel ik vrij? Waar bewaar ik mijn data?

De technologie bestaat. De standaarden bestaan. Wat dit protocol toevoegt is de specifieke architecturale combinatie die privacy niet als instelling behandelt, maar als structurele onmogelijkheid om te schenden.

Product	Belofte	Status
PrismPass	Bewijst, anoniem inloggen zonder wachtwoord	PoC bewezen, 25 april 2026
PrismID	Bevestigt, selectieve identiteitsbevestiging online	Werkende demo
PrismAdd	Bekrachtigt., opt-in anoniem interesse-paspoort	Werkende demo
PrismShield	Beschermt., dwangdetectie via gedragssensoren	Hypothese + PPG-demo
PrismAir	Bewaart., identiteitsloze opslag over apparaten	PoC bewezen, 9 mei 2026

HOOFDSTUK 1

Het probleem

Wat er nog misgaat

De digitale identiteitsinfrastructuur van vandaag is gebouwd op een aanname die decennia oud is: dat een server de gebruiker moet kennen om hem te kunnen bedienen. Die aanname heeft geleid tot een wereld vol centrale databases, wachtwoordbestanden en gebruikersprofielen die wachten op het volgende datalek.

In april 2026 sloot de Nederlandse overheid een raamovereenkomst met STACKIT, een Europees cloudalternatief, mede als reactie op zorgen over de afhankelijkheid van Amerikaanse cloudproviders voor kritieke infrastructuur zoals DigiD. Dat is een begrijpelijke stap. Maar het verplaatst het probleem: de data staat nu in Europa, maar de data bestaat nog

steeds. Iemand met toegang tot die servers weet nog steeds wie er ingelogd heeft, wanneer, en met welk apparaat.[25]

De locatie van data lost het onderliggende probleem niet automatisch op: de data blijft bestaan.

Drie structurele gevolgen van de huidige data-architectuur

Wachtwoordlekken zijn het meest zichtbare gevolg. Een centrale database met wachtwoorden of wachtwoord-hashes is een aantrekkelijk doelwit. Volgens het Verizon Data Breach Investigations Report 2024 zijn gestolen inloggegevens verantwoordelijk voor 77% van de aanvallen op webapplicaties en de meest voorkomende initiële aanvalsvector bij datalekken wereldwijd. [26] Eenmaal buitgemaakt geeft zo'n database toegang tot accounts, en via wachtwoord-hergebruik ook tot accounts elders. De sector heeft hierop gereageerd met betere hashing-algoritmen[27] en

twee-factor-authenticatie, maar de centrale opslag zelf is niet ter discussie gesteld. Passkeys adresseren dit deels, maar zijn nog geen universele standaard.[14]

Sessiekoppeling is het minder zichtbare gevolg. Elke login laat een spoor achter dat servers en platforms kunnen gebruiken om gedrag over tijd te koppelen. Twee logins van dezelfde

gebruiker op hetzelfde platform kunnen door de server worden herleid tot dezelfde gebruiker, ook zonder naam of e-mailadres.[28]

Gedwongen identiteitsonthulling is het derde gevolg. Wie wil bewijzen dat hij aan een criterium voldoet, oud genoeg zijn om alcohol te kopen online, woonachtig in een bepaalde regio voor een regionale dienst, of in dienst bij een bepaald bedrijf voor een zakelijk portaal moet daarvoor doorgaans zijn volledige identiteit tonen.[29] Het gevraagde bewijs is bijna altijd

dunner dan wat er getoond wordt. Dat eIDAS 2.0 selectieve disclosure als vereiste opneemt, bevestigt impliciet dat het huidige systeem dit structureel niet biedt.[22]

Het strategische venster

Drie ontwikkelingen maken dit moment bijzonder.

De eIDAS 2.0-deadline valt in december 2026. Alle EU-lidstaten moeten dan een digitale identiteitsoplossing aanbieden. De EUDI Wallet is de Europese referentie-implementatie, maar die is nog volop in ontwikkeling en heeft moeite met de combinatie van interoperabiliteit en privacy.[30] Er is ruimte voor een aanvullend protocol dat privacy-by-design architecturaal garandeert.

Google's Privacy Sandbox en Topics API zijn in 2025 stopgezet na tegenvallende resultaten.[24] Het experiment om third-party cookies te vervangen terwijl adverteerders toch relevantie kunnen bieden, is mislukt. De zoektocht naar een alternatief model is open.

De passkey-adoptie heeft een kritische massa bereikt. Browser-ondersteuning zit op 98 procent. Apple, Google en Microsoft hebben cross-device synchronisatie geïmplementeerd.[14] De technologische basis waarop PrismPass bouwt is breed geïnstalleerd en gedragen door de grootste platforms ter wereld.

[14] FIDO Alliance, Passkey Adoption in the Wild, Industry Report 2025.

[22] eIDAS 2.0 Regulation, Europese Unie, 2024; Artikel 6a lid 4.

[24] Google Privacy Sandbox Blog, Topics API Deprecation, 2025.

[25] DPIA STACKIT, Ministerie van BZK/Logius, april 2026.

[26] Verizon, Data Breach Investigations Report 2024, gestolen inloggegevens verantwoordelijk voor 77% van de aanvallen op webapplicaties; meest voorkomende initiële aanvalsvector bij datalekken wereldwijd. [27] NIST SP 800-63B, Digital Identity Guidelines, sectie 5.1.1, wachtwoordhashing vermindert risico maar heft centrale opslag niet op.

[28] Narayanan & Shmatikov (2008), 'Robust De-anonymization of Large Sparse Datasets', gedragspatronen zijn identificeerbaar zonder naam of e-mailadres.

[29] Kim Cameron, 'The Laws of Identity' (2005, Microsoft), Wet 2: Minimal Disclosure for a Constrained Use. [30] EUDI Wallet Architecture Reference Framework (ARF) v1.4, Europese Commissie, 2024, beschrijft implementatievrijheid per lidstaat en lopende ontwikkeling.

HOOFDSTUK 2

Het principe

Het licht zelf wordt nooit opgeslagen, alleen de kleur die jij kiest.

Een prisma breekt wit licht in afzonderlijke kleuren. Het licht zelf verandert niet. Wat verandert is welke kleur zichtbaar wordt, afhankelijk van de hoek. PrismPass werkt volgens hetzelfde principe: één identiteit die per context een andere kleur toont, zonder dat die identiteit zelf ooit ergens wordt opgeslagen.

De kernvraag die het protocol beantwoordt is niet 'wie ben jij?' maar 'ben jij degene die je zegt te zijn?' Dat klinkt subtiel, maar het verschil is fundamenteel. De eerste vraag vereist een naam, een profiel, een account. De tweede vraag vereist alleen een cryptografisch bewijs dat de sleutel geldig was.

Wat de server ziet

Bij elke login via PrismPass ontvangt de server precies één ding: een cryptografisch bewijs dat

de sleutel geldig was. Niet de sleutel zelf. Niet de naam van de gebruiker. Niet het apparaat. Niet de locatie. Niet een koppeling met een vorige sessie.[12]

De server kan bevestigen dat iemand is ingelogd, zonder direct te weten wie de gebruiker is. Dat is geen beperking van de implementatie. Dat volgt uit de architectuurkeuze.

Wat de gebruiker ervaart

Voor de gebruiker is de ervaring eenvoudiger dan met een wachtwoord. Vinger op het scherm, of gezicht in de camera en de login is compleet. Geen wachtwoord om te onthouden. Daardoor vervallen ook veel bekende fricties van klassieke loginflows, zoals wachtwoordresets of SMS-codes die vertraagd aankomen.

De fysieke factor bevestigt stilzwijgend de aanwezigheid. In de PoC is dit een passieve NFC-tag: een goedkoop object van enkele euro’s dat de gebruiker bij zich draagt, bijvoorbeeld als tag, kaart of ring. De tag heeft geen app en geen scherm en communiceert passief. Integratie met bestaande consumentenwearables zoals smartwatches is een architectureel pad waarvan de haalbaarheid per platform verschilt; niet elk apparaat kan een passieve NFC-tag uitlezen voor toepassingen van derden.

[12] W3C, Web Authentication: An API for accessing Public Key Credentials Level 3, 2023, sectie 6.1 beschrijft expliciet dat de server een public key en credential ID ontvangt, geen gebruikersidentiteit.

HOOFDSTUK 3

De Vijf B's, het ecosysteem

Het PrismPass Ecosysteem bestaat uit vijf producten die elk een specifieke laag van de identiteitsvraag beantwoorden. Samen vormen ze een trust stack: een gestapelde architectuur die van authenticatie via identiteit en intentie naar integriteit en opslag loopt.

Product	Tagline	Protocolvraag	Status
PrismPass	Bewijst, jij bent het	Is deze entiteit authentiek?	PoC bewezen
PrismID	Bevestigt, jij bestaat	Voldoet deze entiteit aan criterium X?	Werkende demo
PrismAdd	Bekrachtigt., jij kiest het	Wat heeft deze entiteit vrijwillig gedeeld?	Werkende demo
PrismShield	Beschermt., jij meent het	Handelt deze entiteit vrijwillig?	Hypothese + PPG-demo
PrismAir	Bewaart., zonder te weten van wie	Waar verblijft de blob als de eigenaar slaapt?	PoC bewezen

PrismPass, Bewijst.

PrismPass is het fundament van het ecosysteem. Het vervangt het traditionele login-model door een architectuur waarbij de server de gebruiker nooit hoeft te kennen.[12][13]

De driehoek bestaat uit drie factoren die elk volledig in eigendom van de gebruiker zijn: biometrie (vingerafdruk of gezichtsherkenning, verwerkt lokaal in de Secure Enclave), het apparaat (een device-seed die het apparaat nooit verlaat), en een fysieke factor (een passieve NFC-tag die een tijdgebonden nonce levert). Samen genereren ze een ephemeral key, een wegwerpsleutel die na gebruik verdwijnt.

De server verifieert alleen het cryptografische bewijs dat de sleutel geldig was. Meer niet.

Binnen de beschreven architectuur zijn twee sessies niet aan elkaar te koppelen, tenzij de gebruiker dat expliciet toestaat via een Zero-Knowledge Proof voor een specifiek attribuut.[9][10]

PrismID, Bevestigt.

PrismID is de identiteitslaag. Wie wil bewijzen dat hij aan een criterium voldoet, hoeft daarvoor niet zijn volledige identiteit te onthullen. PrismID genereert via Zero-Knowledge Proof een

bewijs dat aan een criterium is voldaan, zonder de onderliggende attribuutwaarde te onthullen.[9][11]

Belangrijk voorbehoud: PrismID werkt uitsluitend online en bij prepaid contexten. Het vervangt geen fysiek paspoort bij een politiecontrole, grensovergang of post-payment situatie. Die eerlijkheid is onderdeel van het ontwerp, geen beperking om te verbergen.

PrismAdd, Bekrachtigt.

PrismAdd is de commerciële laag van het ecosysteem. Gebruikers beheren een lokale interesse-wallet: categorieën die zij zelf kiezen, op een moment dat zij dat kiezen, intrekbaar wanneer zij dat willen. Adverteerders ontvangen via Privacy Pass RFC 9576/9578 unlinkable

tokens die aantonen dat iemand in een bepaalde categorie geïnteresseerd is, zonder dat die iemand herleidbaar is.[15][16]

Het verschil met de stopgezette Google Topics API: daar leidde de browser interesses af zonder expliciete toestemming van de gebruiker.[24] Bij PrismAdd is de gebruiker de eigenaar van zijn eigen interesse-paspoort. Niets wordt gedeeld tenzij de gebruiker dat actief inschakelt.

PrismShield, Beschermt.

PrismShield is het meest experimentele product van het ecosysteem. Het doel: detecteren of een login vrijwillig plaatsvindt, of onder dwang. De Centroid-architectuur combineert

bewegingspatronen, hartslagvariabiliteit en contextvensters tot een gedragsbiometrisch profiel dat lokaal op het apparaat wordt verwerkt.[17][18]

Voor afzonderlijke onderdelen bestaat wetenschappelijke onderbouwing: gedragsbiometrie voor coerciedetectie is een actief onderzoeksveld met peer-reviewed publicaties.[17] Maar de

implementatievraag is nog open. Een lokaal model mist de trainingsdata die cloudgebaseerde concurrenten zoals BioCatch hebben opgebouwd over miljarden sessies.[19]

PrismShield is op dit moment een hypothese met een werkende PPG-demo, geen productierijp systeem. PrismShield hoeft niet als consumentenproduct te starten. Een wetenschappelijk onderzoeksprotocol met een universiteit of veiligheidsinstelling bouwt de trainingsdata op, valideert de nauwkeurigheid, en legt de basis voor een later product.

PrismAir, Bewaart.

PrismAir sluit het ecosysteem als vijfde product. Het lost een probleem op dat elke gebruiker herkent maar dat niemand nog heeft opgelost: data veilig bewaren op meerdere apparaten, zonder dat de opslagserver weet van wie de data is.

De architectuur: twee apparaten koppelen eenmalig via Bluetooth. Op beide apparaten bevestigt de gebruiker de koppeling met biometrie. Daarna berekenen beide apparaten zelfstandig dezelfde blob-sleutel via HKDF op basis van een gedeeld anker.[hkdf] Er reist nooit een sleutel tussen apparaten. De server ziet uitsluitend versleutelde blobs en twee cryptografische bewijzen voor dezelfde commitment. De server ziet daarbij geen directe identiteitskoppeling tussen apparaten.

De PoC is bewezen op 9 mei 2026: een versleutelde notitie aangemaakt op een laptop was leesbaar op een iPhone, zonder dat de server wist dat beide apparaten van dezelfde persoon waren.

[9] Groth, 'On the Size of Pairing-Based Non-Interactive Arguments', EUROCRYPT 2016 (Groth16-schema).

[10] Bellare et al., 'Circom: A Robust and Scalable Language for Building Complex Zero-Knowledge Circuits', 2023. [11] ZKProof Community Reference Document, zkproof.org, doorlopend.

[15] RFC 9576, The Privacy Pass Architecture, IETF, 2024.

[16] RFC 9578, Privacy Pass Issuance Protocol, IETF, 2024.

[17] ACM Computing Surveys, 'Behavioral Biometrics for Continuous Authentication', 2022. [18] IEEE TPAMI, 'Remote Cardiac Pulse Estimation', 2023 (rPPG via camera).

[19] BioCatch, Series E Financing and Healthcare/Government Expansion, 2025, miljarden sessies geanalyseerd. [hkdf] RFC 5869, HMAC-based Key Derivation Function (HKDF), IETF.

HOOFDSTUK 4

Architectuur

De driehoek

Een driehoek is het minimale gesloten systeem. Verwijder één punt en de constructie valt. PrismPass gebruikt hetzelfde principe voor de private key: drie elementen die elk op zichzelf waardeloos zijn, maar samen een geldige handtekening genereren.

Factor	Wat het is	Waarde zonder de andere factoren	Waarom alleen onbruikbaar
Biometrie	Vingerafdruk of gezicht, verwerkt in Secure Enclave / TEE	Nihil	Niet reproduceerbaar zonder levend lichaam en apparaat
Apparaat	Device-seed in hardware-beveilig de opslag	Nihil	Vereist factor 1 én factor 3 om te activeren
Wearable	Tijdgebonden NFC-nonce via passieve tag (pasje, ring, sticker), maximaal 500 ms geldig *	Nihil	Een verlopen nonce verliest praktisch zijn waarde binnen de sessie

US Patent 12389227 beschrijft tijdslimiet-gebaseerde relay-detectie op kanaalniveau. De 500 ms in deze tabel is een zelfstandige ontwerpkeuze gebaseerd op NFC-nabijheidsgedrag en staat los van die geoctrooieerde methode.[7]

De wearable heeft geen app en geen scherm. Hij communiceert passief. Op het moment van login stuurt hij één signaal: aanwezig, gekoppeld aan een levend

lichaam. De tijdgebondenheid maakt relay-aanvallen aanzienlijk moeilijker: een aanvaller die het NFC-signaal onderschept en doorstuurt, krijgt een verlopen nonce.

Wat er technisch gebeurt bij een login

Stap	Wat er gebeurt	Waar	Wat de server ziet
1	Biometrie wordt gelezen	Lokaal op apparaat	Niets
2	Wearable bevestigt aanwezigheid via NFC-nonce (passieve tag)	Tussen apparaat en wearable	Niets
3	Device-seed + biometrie + nonce combineren tot ephemeral key	Lokaal op apparaat	Niets
4	ZKP-bewijs wordt gegenereerd dat de sleutel geldig was, zonder de sleutel te onthullen[9]	Lokaal op apparaat	Niets
5	Handtekening + ZKP-bewijs worden verzonden	Netwerk	Handtekening + bewijs
6	Server verifieert: geldig of ongeldig	Op de server	Geldig of ongeldig

Stap	Wat er gebeurt	Waar	Wat de server ziet
7	Sessie gestart. Ephemeral key vernietigd.	Apparaat + server	Sessietoken (tijdelijk)

Bestaande technologie, nieuwe combinatie

PrismPass heruitvindt geen cryptografie. Het combineert bestaande, gestandaardiseerde bouwstenen op een nieuwe manier. Elk afzonderlijk component heeft prior art; de nadruk ligt hier op de combinatie en toepassing van bestaande standaarden.

Technologie	Standaard / Specificatie	Rol in het protocol
WebAuthn	W3C Level 3[12]	Authenticatielaag, biometrie + apparaat
FIDO2 / Passkeys	FIDO Alliance[13]	Basis voor wachtwoordloze login
Zero-Knowledge Proofs	Groth16 via circom/snarkjs[9][10]	Identiteitsbewijzen zonder onthulling
Privacy Pass	RFC 9576/9578 (IETF)[15][16]	Unlinkable tokens voor PrismAdd
NFC / BLE	ISO 14443 / Bluetooth SIG[36]	Wearable-nonce, tijdgebonden aanwezigheid
AES-256-GCM	NIST FIPS 197 / SP 800-38D	Versleuteling PrismChat en PrismAir
HKDF / SHA-3	RFC 5869 / NIST FIPS 202	Sleutelafleiding PrismAir

Post-quantum voorbereiding

De ephemeral key-architectuur biedt mogelijk voordelen bij de overgang naar post-quantum cryptografie. Omdat elke sessie een nieuwe sleutel genereert en er geen centrale opslag is van

identiteitsdata, is er geen historische dataset die bij een toekomstige kwantumcomputer retroactief te ontsleutelen valt.[21]

Migratie naar NIST post-quantum standaarden zoals ML-KEM (FIPS 203) en ML-DSA (FIPS 204) zou grotendeels als implementatie-update kunnen plaatsvinden zonder het model fundamenteel te wijzigen.[20] De standaarden zijn gepubliceerd in 2024; de integratie is een geplande uitbreiding van het protocol.

[7] USPTO — *NFC Anti-Relay Protection* — US Patent 12389227, verleend 2025. PrismPass verwijst naar dit patent als referentie voor tijdslimiet-gebaseerde relay-detectie op kanaalniveau. De implementatiekeuzes in PrismPass zijn zelfstandige ontwerpbeslissingen gebaseerd op fysieke NFC-nabijheid (4-10 cm) en staan los van de geoctrooieerde methode. [12] W3C, Web Authentication Level 3, 2023.

[13] FIDO Alliance, FIDO2: Web Authentication, 2022.

[20] NIST, Post-Quantum Cryptography Standards, FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), 2024.
[21] IEEE Security & Privacy, 'Harvest Now, Decrypt Later: A Survey', 2023.

HOOFDSTUK 5

Bewijs

Dit hoofdstuk maakt een expliciet onderscheid tussen wat bewezen is in een werkende proof-of-concept, wat volgt uit open standaarden en academische literatuur, en wat nog hypothese is. Die afbakening is belangrijk voor een realistische technische beoordeling.

Bewezen in de PoC

Op 25 april 2026 is de kernarchitectuur van PrismPass voor het eerst werkend gedemonstreerd op gewone consumentenhardware:

- WebAuthn-authenticatie via biometrie en apparaatbinding, geïmplementeerd met SimpleWebAuthn v13.[12]
- Zero-Knowledge Proof identiteitsbewijs: bewezen dat een attribuut geldig is zonder de

onderliggende identiteit te onthullen, geïmplementeerd met circom/snarkjs en het Groth16-schema.[9][10]

- Wearable aanwezigheidsbewijs via NFC-nonce met tijdsgebonden geldigheid. [7] Bewezen in PoC 25 april 2026; fysieke nabijheid (4-10 cm, ISO/IEC 14443) als primaire relay-verdediging, nonce-venster als usability-drempel. [36] [PoC-documentatie]
- Privacy Pass-tokenarchitectuur voor unlinkable communicatie, geïmplementeerd op RFC 9576/9578 via @cloudflare/privacypass-ts v0.8.1.[15][16]
- PrismChat: versleutelde berichten tussen twee gebruikers via PBKDF2-sleutelafleiding, waarbij de server alleen ciphertext ziet.
- PrismAir: versleutelde blob gedeeld tussen laptop en iPhone via HKDF-sleutelafleiding en QR-koppelstap, bewezen op 9 mei 2026.
- Dienst-blob niveau 2: registratie van een dienst via een ECDSA P-256-sleutelpaar, waarbij de dienst zich aanmeldt met een ondertekende sleutel zonder dat centrale persoonsdata nodig is, bewezen op 7 juni 2026 via PrismGate.

Volgt uit open standaarden

Een aantal architectuurclaims volgt niet uit de PoC zelf, maar uit de eigenschappen van de gebruikte standaarden:

- Unlinkability van Privacy Pass-tokens: cryptografisch geborgd door de VOPRF P-384-constructie in RFC 9578; twee tokens zijn wiskundig niet te koppelen.[16]
- Biometrie verlaat het apparaat nooit: eigenschap van WebAuthn Level 3, de Secure Enclave op Apple-apparaten, en de Trusted Execution Environment op Android.[12]
- NFC relay-aanvalresistentie via tijdgebonden nonce: volgt uit de fysieke eigenschappen van ISO/IEC 14443. US Patent 12389227 bevestigt dat tijdslimiet-gebaseerde relay-detectie als serieus verdedigingsmechanisme wordt erkend; PrismPass hanteert fysieke nabijheid als primaire verdediging.[7]

Hypothese, nog te valideren

- PrismShield Centroid-nauwkeurigheid: de afzonderlijke sensormethoden zijn wetenschappelijk onderbouwd,[17][18] maar de gecombineerde nauwkeurigheid van het

lokale model voor dwangdetectie vereist empirisch onderzoek.

- ZKP-bibliotheekaudit: voor productie-inzet is een onafhankelijke audit van de circom/snarkjs-implementatie vereist; in de PoC is deze audit nog niet uitgevoerd.

- Productiepad PrismAir Secure Enclave: de PoC gebruikt localStorage; het productiepad via WebAuthn PRF is architectureel beschreven maar nog niet geïmplementeerd.
- Integratie met consumentenwearables: de PoC is bewezen met een passieve NFC-tag, die de fysieke factor betrouwbaar levert. Integratie met bestaande smartwatches als drager van die factor is architectureel beschreven maar nog niet bewezen, en de haalbaarheid verschilt per platform. Niet elk apparaat kan een passieve NFC-tag uitlezen voor toepassingen van derden; de passieve tag blijft daarom de aangetoonde basis.

[7] USPTO — *NFC Anti-Relay Protection* — US Patent 12389227, verleend 2025. PrismPass verwijst naar dit patent als referentie voor tijdslimiet-gebaseerde relay-detectie op kanaalniveau. De implementatiekeuzes in PrismPass zijn zelfstandige ontwerpbeslissingen gebaseerd op fysieke NFC-nabijheid (4-10 cm) en staan los van de geoctrooieerde methode.

[9] Groth, EUROCRYPT 2016 (Groth16).

[10] Bellare et al., Circom, 2023.

[12] W3C WebAuthn Level 3, 2023; Apple Secure Enclave documentatie; Android Keystore System, developer.android.com.

[15] RFC 9576, IETF, 2024.

[16] RFC 9578, IETF, 2024.

[17] ACM Computing Surveys, Behavioral Biometrics, 2022.

[18] IEEE TPAMI, Remote Cardiac Pulse Estimation, 2023.

HOOFDSTUK 6

Vergelijking met bestaande oplossingen

PrismPass staat niet alleen op het veld. Er zijn concurrerende en aanvullende initiatieven. De tabel hieronder positioneert het protocol eerlijk ten opzichte van de meest relevante alternatieven.

Oplossing	Wat het doet	Wat het niet doet	Relatie tot PrismPass
Passkeys[14]	Wachtwoord elimineren; biometrie lokaal houden; phishing aanzienlijk bemoeilijken via device binding	Server weet nog steeds wie je bent; geen dwangdetectie; geen selectieve attribuutbevestiging	PrismPass bouwt op dezelfde WebAuthn-standaard maar voegt identiteitsscheiding en de wearable-factor toe
EUDI Wallet[30]	EU-brede digitale identiteitswallet; selectieve attribuutdisclosure conform eIDAS 2.0	Nog volop in ontwikkeling; privacy-garanties variëren per implementatie	Complementair: PrismPass kan als authenticatielaag onder een EUDI Wallet functioneren
Polygon ID / SpruceID	ZKP-gebaseerde verifiable credentials;	Vereist blockchain-infrastructuur;	Dichtstbijzijnde concurrent op ZKP-identiteitslaa

	self-sovereign identity	ecosysteem-adoptie beperkt; geen wearable-factor; niet gericht op gedragsbiometrie	g; PrismPass voegt de driehoeksarchitectuur en interesse-laag toe
BioCatch[19]	Gedragsbiometrie voor fraudedetectie; miljarden sessies geanalyseerd	Verwerking in centrale cloud; privacy gebaseerd op contractuele afspraken, niet op architecturele onmogelijkheid tot onthulling	Concurrent voor PrismShield-laag; BioCatch heeft massieve trainingsdata voorsprong
Privacy Pass (Cloudflare)[15][16]	Unlinkable tokens voor bot-detectie en rate limiting	Geen authenticatieprotocol; geen identiteitslaag	PrismPass gebruikt Privacy Pass RFC 9576/9578 als tokenarchitectuur voor PrismAdd

Elk afzonderlijk component heeft prior art. De toegevoegde waarde zit in de combinatie van bestaande bouwstenen. Geen van de bestaande oplossingen combineert anonieme authenticatie, selectieve attribuutbevestiging, opt-in interesse-signalering, dwangdetectie en identiteitsloze multi-device opslag in één samenhangend protocol. Dat is de architecturale ruimte die PrismPass invult.

[14] FIDO Alliance, Passkey Adoption Report 2025.
[15] RFC 9576, IETF, 2024.
[16] RFC 9578, IETF, 2024.
[19] BioCatch, Series E Financing, 2025.
[30] EUDI Wallet ARF v1.4, Europese Commissie, 2024.

HOOFDSTUK 7

Scope en grenzen

Wat PrismID niet doet

PrismID is een online identiteitslaag zonder sporen. Het vervangt geen fysiek paspoort. Bij een politiecontrole, grensovergang, bancaire KYC-procedure[31] of medische opname is een door de overheid uitgegeven identiteitsbewijs nog steeds vereist. PrismID werkt uitsluitend online en in contexten waar geen wettelijke verplichting bestaat tot verificatie door een geaccrediteerde instantie, zoals bij post-payment of fysieke levering.

Wat PrismPass niet elimineert

PrismPass scheidt de loginidentiteit van de opgeslagen persoonsdata, maar elimineert niet de noodzaak van alle persoonsdata. Een abonnement vereist een bezorgadres. Een arbeidscontract vereist een naam. Het kernpunt is architecturale

scheiding: de data die nodig is voor de dienst, bestaat uitsluitend bij de partij die hem nodig heeft, en is nooit gekoppeld aan de authenticatielaag.

Wat buiten scope valt

PrismPass specificeert het protocol. De biometrische hardware, de wearable-hardware, de Secure Enclave-implementatie en de netwerktransportlaag zijn verantwoordelijkheden van respectievelijk apparaatfabrikanten, W3C en IETF. PrismPass groeit mee met verbeteringen in die lagen zonder de eigen architectuur te hoeven wijzigen.

Endpoint-compromis, het scenario waarbij het apparaat van de gebruiker zelf volledig gecompromitteerd is, valt buiten de scope van elk authenticatieprotocol ter wereld, PrismPass incluis.[27] Dit is een algemene beperking binnen authenticatiesystemen, geen specifieke beperking van dit protocol.

Wat de dienstaanbieder ná login opslaat

Wat de dienstaanbieder ná login opslaat valt buiten de scope van PrismPass. Het protocol borgt de authenticatielaag. Wat een aanbieder daarna registreert aan gedrag, voorkeuren of transacties is een verantwoordelijkheid van die aanbieder, onderworpen aan AVG en andere toepasselijke wetgeving. PrismPass verwijdert de identiteitskoppeling bij de login; het verwijdert niet de mogelijkheid dat een dienstaanbieder zelf nieuwe data aanmaakt.

Dit geldt evenzeer voor de browserkant. Trackers, fingerprinting-technieken, third-party scripts of cache-methoden die een dienst op zijn eigen pagina inzet, vallen buiten de reikwijdte van PrismPass. Het protocol borgt de anonimiteit van de toegang tot het authenticatiemoment; die garantie reikt tot de deur. Wat de pagina daaromheen laadt en wat de dienst daarachter doet, is de verantwoordelijkheid van de dienstaanbieder. Een dienst kan ervoor kiezen het inlogmoment aantoonbaar schoon te houden via een vrijwillige verificatie; dat is een optioneel keurmerk bovenop het protocol, geen eigenschap van het basisprotocol zelf.

[27] NIST SP 800-63B, Digital Identity Guidelines, sectie 8, device compromise valt buiten scope van het authenticatieprotocol.

[31] EU Anti-Money Laundering Directive (AMLD6), 2024, schrijft voor dat KYC-verificatie bij financiële instellingen door een geaccrediteerde instantie moet worden uitgevoerd.

HOOFDSTUK 8

Adoptiepad

Het kip-en-ei-probleem

Elke nieuwe authenticatiestandaard heeft hetzelfde fundamentele probleem. Gebruikers installeren het pas als er websites zijn die het ondersteunen. Websites implementeren het pas als er gebruikers zijn die het hebben. WebAuthn heeft dit probleem opgelost doordat Apple, Google en Microsoft besloten het in te bouwen voordat brede consumentenadoptie had plaatsgevonden.[14] Een vergelijkbare adoptie-dynamiek zou waarschijnlijk ook hier nodig zijn: één grote platformpartner die de standaard adopteert voor een specifieke, hoge-waarde use case.

De drie adoptielagen

Laag 1, Basis: NFC-tag of eenvoudige Bluetooth-token

Kostprijs: enkele euro's retail. Doelgroep: consumenten. Drempel: laag, een goedkoop fysiek object dat de gebruiker bij zich draagt. Dit is de instapvariant die maximale breedte bereikt maar de Centroid-dwangdetectie niet ondersteunt.

Laag 2, Werk: bedrijfswearable

Kostprijs voor de gebruiker: nihil in B2B-context waarbij de werkgever de wearable verstrekt als bedrijfsmiddel, vergelijkbaar met een toegangspas of bedrijfstelefoon. Doelgroep: B2B, met name sectoren met verhoogd risico op zakelijke dwang: financiële instellingen, zorg, overheid. Bevat HRV-sensoren en bewegingsdetectie voor de Centroid.

Laag 3, Premium: bestaande consumentenwearable

Smartwatch, luxe ring of medisch wearable. Kostprijs: al in bezit bij een substantieel deel van de doelgroep.[33] PrismPass wordt een software-integratie op bestaande hardware, geen aankoopdrempel. De haalbaarheid verschilt per platform; niet elk apparaat kan een passieve NFC-tag uitlezen voor toepassingen van derden.

Wie wint, wie moet aanpassen

Mogelijke voordelen liggen bij meerdere partijen: eindgebruikers met minder datalekken[26], kleine websites die onafhankelijk worden van Big Tech voor gebruikersbeheer[32], kleine hosters die niet langer enorme beveiligingsbudgetten nodig hebben voor centrale databases, en overheden die privacy-by-design eindelijk architecturaal geborgd zien in plaats van regulatoir afgedwongen.

De partijen die hun businessmodel moeten aanpassen zijn de grote platforms die verdienen aan gedragsprofilering.[34] De strategie is niet confrontatie maar complementariteit: PrismPass maakt het voor platforms makkelijker om te voldoen aan toenemende privacywetgeving, niet moeilijker om te verdienen.

De wearable-vereiste is het zwaarste adoptierisico

Gebruikers moeten een derde factor aanschaffen en dagelijks dragen die ze vandaag niet hebben. Laag 1 verlaagt die drempel maximaal. Laag 3 elimineert hem voor de doelgroep die toch al een smartwatch draagt.

De meest logische initiële use case is de B2B-context waarbij een werkgever de wearable verstrekt: zorg, financiële dienstverlening en overheid zijn sectoren waar zowel de dwangrisico's als de privacyvereisten het hoogst zijn.

[14] FIDO Alliance, Passkey Adoption Report 2025.

[26] Verizon DBIR 2024.

[32] w3techs.com, marktaandelen authenticatiediensten; Google en Facebook Login dekken samen meer dan 80% van social login implementaties.

[33] Statista / IDC Wearables Market Report 2024/2025, smartwatch-penetratie onder werkenden in Nederland ruim boven 30%.

[34] IAB Europe, AdEx Benchmark Report 2024; Statista, Digital Advertising Revenue by Company 2024.

HOOFDSTUK 9

Beveiliging

Het threat model van PrismPass is op één belangrijk punt anders dan klassieke systemen: er is geen centrale gebruikersdatabase met credentials om buit te maken. Daarmee wordt een veelvoorkomende aanvalsvector sterk beperkt.

Aanvalstype	Risicopositie	Toelichting
Server-datalek	Sterk verminderd	Server slaat geen persoonsdata op. Een lek levert verlopen tokens op.
Relay / man-in-the-middle	Sterk bemoeilijkt door design	Tijdgebonden nonce (500 ms) maakt relay-aanvallen aanzienlijk moeilijker; niet mathematisch onmogelijk, wel praktisch onaantrekkelijk.[7]
Kwantumcomputer (toekomst)	Voorbereid op toekomstige migratie	Ephemeral keys + modulaire cryptografielaag. Migratie naar ML-KEM is een implementatiestap.[20][21]
Biometrische spoofing	Gedelegeerd aan hardware	Verantwoordelijkheid van apparaatfabrikanten. PrismPass groeit mee met verbeteringen in liveness detection.[1][3]
ZKP-implementatie risico	PoC: acceptabel; productie: audit vereist	Bibliotheek is wisselbaar. Onafhankelijke audit is standaardvereiste voor cryptografische software in productie.[11]
Endpoint-compromis	Buiten scope	Buiten scope van elk authenticatieprotocol ter wereld. Industrie-brede grens.[27]
Supply chain wearable-hardware	Risico aanwezig; mitigatie via certificering	Goedkope NFC-hardware uit niet-gecontroleerde supply chains kan gecompromitteerd zijn bij fabricage. Mitigatie: gecertificeerde hardware voor productie-inzet;

		NFC-tags zijn vervangbaar zonder impact op de andere twee factoren.

NFC fysieke nabijheid als veiligheidskeuze

De NFC-communicatie vereist een fysieke nabijheid van 4 tot 10 centimeter in de praktijk, met een theoretisch maximum van circa 30 centimeter.[5][8] Gecombineerd met de tijdsgebonden nonce maakt dit relay-aanvallen aanzienlijk moeilijker: een aanvaller die het signaal onderschept op grotere afstand, krijgt een verlopen nonce.

Dit is een bewuste architectuurkeuze, vergelijkbaar met de logica achter contactloze bankpassen.[emvco] Die fysieke beperking is bewust onderdeel van het beveiligingsmodel.

[1] PMC/MDPI Journal of Imaging, 'Enhancing Fingerprint Liveness Detection Accuracy Using Deep Learning', 2023. [3] LivDet, Fingerprint Liveness Detection Competition, Universiteit van Cagliari, doorlopend. [5] MDPI Electronics, 'Deep-Learning-Aided RF Fingerprinting for NFC Relay Attack Detection', 2023. [7] USPTO — *NFC Anti-Relay Protection* — US Patent 12389227, verleend 2025. PrismPass verwijst naar dit patent als referentie voor tijdslimiet-gebaseerde relay-detectie op kanaalniveau. De implementatiekeuzes in PrismPass zijn zelfstandige ontwerpbeslissingen gebaseerd op fysieke NFC-nabijheid (4-10 cm) en staan los van de geoctrooieerde methode.

[8] PMC, 'Near-Field Communication (NFC) Cyber Threats and Mitigation', 2024; NFC Forum technische specificaties, nfc-forum.org.

[11] ZKProof Community Reference Document, zkproof.org.

[20] NIST FIPS 203/204, 2024.

[21] IEEE Security & Privacy, 'Harvest Now, Decrypt Later', 2023.

[27] NIST SP 800-63B, sectie 8.

[emvco] EMVCo, contactloze betaalkaart specificaties, fysieke nabijheid als veiligheidslaag.

HOOFDSTUK 10

Governance en continuïteit

Het uitgangspunt van PrismPass is primair protocolontwikkeling en standaardisatie. Het doel is een open standaard definiëren die breed toepasbaar wordt, terwijl de uitvinder blijft verdienen aan dat gebruik.

Het referentiemodel combineert elementen van het W3C-model, waarbij een open specificatie breed geïmplementeerd kan worden, met een FRAND-licentiestructuur vergelijkbaar met die van Qualcomm voor essentiële patenten.[35] Elk van deze modellen heeft andere kenmerken; PrismPass leent specifiek het royalty-principe, niet de volledige structuur van elk model. De uitvinder behoudt IP-eigendom en ontvangt royalty's bij commerciële inzet, zonder de dagelijkse exploitatie te dragen.

De drie licentievormen

Licentievorm	Doelgroep	Model
A, Publiek / Open	Overheden, non-profits, academici, open source	Royalty-free, met verplichte naamsvermelding
B, Commercieel	Bedrijven die het protocol inbouwen in producten	FRAND-tarief (Fair, Reasonable and Non-Discriminatory), redelijk en niet-discriminerend
C, Strategisch	Grote platforms, EU-instellingen, diepgaande integratie	Onderhandelbaar, eenmalig of structureel

IP-eigendom blijft in alle gevallen bij de uitvinder. Naamsvermelding is bij alle licentievormen verplicht. De vierde hoek-vereiste, een versleuteld juridisch anker dat uitsluitend op rechterlijk bevel ontsleuteld kan worden via een geaccrediteerde instantie, zonder dat de normale werking van het protocol wordt aangetast, is niet-onderhandelbaar bij productie-inzet van PrismID of PrismChat.

Continuïteit van het protocol

Continuïteit van het protocol is geborgd via de Zenodo-registratie van de Invention Disclosure (DOI: 10.5281/zenodo.20029291) en de open standaarden waarop het bouwt. WebAuthn, Privacy Pass en de ZKP-bibliotheken zijn onafhankelijk van PrismPass en blijven functioneren. De langetermijnstrategie is overdracht van het protocolbeheer aan een onafhankelijke stichting of IETF working group, zodat continuïteit niet afhankelijk is van één persoon of organisatie.

Openstaande vragen

De governance-structuur voor de langetermijn is bewust niet vastgelegd. Relevante vragen die beantwoord moeten worden in overleg met de eerste serieuze partners:

- Welke rechtsvorm beheert het protocol als open standaard? (stichting, IETF working group, W3C community group)
- Hoe worden royalty's verdeeld als het protocol wordt uitgebreid door derden?
  • Wie heeft zitting in een eventueel technisch governance-comité?

Deze vragen zijn opengelaten omdat de antwoorden afhangen van de eerste serieuze validatie en de eerste partnergesprekken.

[35] Europese Commissie, 'Standard Essential Patents' beleidsdocument, 2023; W3C Patent Policy, 2020.

HOOFDSTUK 11

Validatie en volgende stappen

Primaire route

De primaire validatieroute loopt via onafhankelijke technische experts op het gebied van privacy-by-design en cryptografische protocollen. Een externe review is de prioritaire gate vóór publieke communicatie. Een positieve terugkoppeling geldt als waardevolle validatie van zowel de technische correctheid als de relevantie van het protocol.

Inhoudelijk perspectief uit het veld

Een terugkerend perspectief in het adoptiedebat is dat het probleem primair sociaal en politiek van aard is en dat technologie de machtsverhouding niet zelfstandig verandert. Dat is een legitiem en serieus argument dat de architectuurkeuzes van PrismPass niet weerlegt maar contextualiseert.

Alternatieve routes

Als de primaire route om welke reden dan ook niet resulteert in bruikbare validatie, zijn er alternatieve paden:

- IETF en W3C kennen community group-structuren waarbinnen een Internet-Draft ingediend kan worden voor technische peer review.
- Zenodo-publicatie van de Invention Disclosure is al een tijdgestempeld openbaar record (DOI: 10.5281/zenodo.20029291); uitbreiding naar een preprint op arXiv is een logische volgende stap.

Sequentie

De sequentiediscipline is bewust: validatie eerst, partnergesprekken tweede, publieke zichtbaarheid derde. Een te vroege publieke positionering vóór externe validatie is een mogelijk risico voor de geloofwaardigheid van het protocol.

Fase	Actie	Status
Nu	Technische review door onafhankelijke privacy-by-design experts	In voorbereiding
Stap 1	TNO benaderen	Email gestuurd
Stap 2	Eerste licentiegesprek met overheid of commerciële partij	Wacht op technische validatie via stap 1
Stap 3	IETF/W3C Internet-Draft indienen	Wacht op stap 2
Stap 4	Beheer overdragen aan onafhankelijke stichting	Langetermijn

HOOFDSTUK 12

Bronnen

De volgende selectie ondersteunt de architectuurclaims in dit whitepaper. Bronnen zijn in de tekst aangehaald via voetnootnummers. De volledige bronnenbijlage is beschikbaar op prismpass.globalsecurity.nu/v4/bronnen.html.

Biometrie en liveness detection

[1] PMC/MDPI Journal of Imaging, 'Enhancing Fingerprint Liveness Detection Accuracy Using Deep Learning', 2023. [2] Sumsub/Biometric Update, 'Liveness Detection: A Complete Guide for Fraud Prevention and Compliance in 2025', 2024-2025. [Commerciële bron; marktcontext]

[3] LivDet, Fingerprint Liveness Detection Competition, Universiteit van Cagliari, doorlopend. [4] IEEE Computer Society, 'Biometric Liveness Detection: Challenges and Research Opportunities', 2015.

NFC-beveiliging

[5] MDPI Electronics, 'Deep-Learning-Aided RF Fingerprinting for NFC Relay Attack Detection', 2023. [6] ESET Threat Report H1 2025, 'NFC Cyber Threats Surging'. [Commerciële bron; marktcontext] [7] USPTO — *NFC Anti-Relay Protection* — US Patent 12389227, verleend 2025. PrismPass verwijst naar dit patent als referentie voor tijdslimiet-gebaseerde relay-detectie op kanaalniveau. De implementatiekeuzes in PrismPass zijn zelfstandige ontwerpbeslissingen gebaseerd op fysieke NFC-nabijheid (4-10 cm) en staan los van de geoctrooieerde methode.

[8] PMC, 'Near-Field Communication (NFC) Cyber Threats and Mitigation', 2024; NFC Forum technische specificaties, nfc-forum.org.

Zero-Knowledge Proofs

[9] Groth, 'On the Size of Pairing-Based Non-Interactive Arguments', EUROCRYPT 2016 (Groth16-schema). [10] **IEEE:** Bellés-Muñoz et al. (2023). *Circom: A Circuit Description Language for Building Zero-Knowledge Applications*. IEEE TDSC. DOI: 10.1109/TDSC.2022.3232813. . [11] ZKProof Community Reference Document, zkproof.org, doorlopend.

WebAuthn en passkeys

[12] W3C, 'Web Authentication: An API for accessing Public Key Credentials Level 3', 2023. [13] FIDO Alliance, 'FIDO2: Web Authentication', 2022.

[14] FIDO Alliance, 'Passkey Adoption in the Wild, Industry Report', 2025.

Privacy Pass

[15] RFC 9576, The Privacy Pass Architecture, IETF, 2024.

[16] RFC 9578, Privacy Pass Issuance Protocol, IETF, 2024.

Gedragsbiometrie en dwangdetectie

[17] ACM Computing Surveys, 'Behavioral Biometrics for Continuous Authentication', 2022. [18] IEEE TPAMI, 'Remote Cardiac Pulse Estimation', 2023 (rPPG via camera).

[19] BioCatch, Series E Financing, Healthcare/Government Expansion, 2025. [Persbericht; schaal-indicatie]

Post-quantum cryptografie

[20] NIST, Post-Quantum Cryptography Standards, FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), 2024. [21] IEEE Security & Privacy, 'Harvest Now, Decrypt Later: A Survey', 2023.

Regulering en marktcontext

[22] eIDAS 2.0 Regulation, Europese Unie, 2024.

[23] CMS Law, GDPR Enforcement Tracker, doorlopend 2024-2026.

[24] Xiao, Y. et al. — Intent to Deprecate and Remove: Topics API — Chromium blink-dev mailinglist, 7 november 2025. Beschikbaar via: groups.google.com/a/chromium.org/g/blink-dev/c/_R85yctz4Rs
[25] DPIA STACKIT, Ministerie van BZK/Logius, april 2026.

Aanvullende bronnen (nieuw sinds v3)

[26] Verizon, Data Breach Investigations Report 2024, gestolen inloggegevens verantwoordelijk voor 77% van aanvallen op webapplicaties (Verizon DBIR 2024). [27] NIST SP 800-63B, Digital Identity Guidelines, sectie 5.1.1 (wachtwoordhashing) en sectie 8 (endpoint-compromis buiten scope).
[28] Narayanan & Shmatikov (2008), 'Robust De-anonymization of Large Sparse Datasets', gedragspatronen zonder naam identificeerbaar.
[29] Kim Cameron, 'The Laws of Identity', Microsoft, 2005, Wet 2: Minimal Disclosure for a Constrained Use. [30] EUDI Wallet Architecture Reference Framework (ARF) v1.4, Europese Commissie, 2024. [31] EU Anti-Money Laundering Directive (AMLD6), 2024.
[32] w3techs.com, marktaandelen authenticatiediensten.
[33] Statista / IDC Wearables Market Report 2024/2025.
[34] IAB Europe, AdEx Benchmark Report 2024; Statista, Digital Advertising Revenue by Company 2024. [35] Europese Commissie, Standard Essential Patents beleidsdocument, 2023; W3C Patent Policy, 2020. [36] ISO/IEC 14443 — Identification cards: Contactless integrated circuit cards, Proximity cards — ISO. Beschikbaar via: iso.org/standard/73596.html. [EMVCo] EMVCo, contactloze betaalkaart specificaties, fysieke nabijheid als veiligheidslaag.

Het licht zelf wordt nooit opgeslagen, alleen de kleur die jij kiest.

PrismPass Ecosysteem · I. Smid-Woelders · Zwolle, Nederland · Mei 2026
Vertrouwelijk concept · Invention Disclosure geregistreerd · Zenodo DOI: 10.5281/zenodo.20029291 prismpass.globalsecurity.nu