TNO innovation for life

De Toekomst van Authenticatie: Een Analyse van de Adoptie van Passkeys en Digital Identity Wallets

TNO Publiek › TNO 2025 R10863
22 april 2025

ICT, Strategy & Policy
www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2025 – 22 april 2025

De Toekomst van Authenticatie: Een Analyse van de Adoptie van Passkeys en Digital Identity Wallets

Auteurs	Andrea Kerstens Frank Westers René Bakker Alexander van den Wall Bake
Rubricering rapport	TNO Publiek
Titel	TNO Publiek
Rapporttekst	TNO Publiek
Aantal pagina's	37 (excl. voor- en achterblad)
Aantal bijlagen	1

Inhoudsopgave

Inhoudsopgave

1 Executive Summary

1.1 Inleiding

Identity Access Management speelt een cruciale rol in de cybersecuritystrategie van organisaties. De traditionele afhankelijkheid van wachtwoorden leidt tot kwetsbaarheden, zoals phishing en brute-force aanvallen, waardoor de behoefte aan veiligere alternatieven toeneemt. Passkeys en digital identity wallets zijn twee opkomende technologieën die authenticatie zonder wachtwoord mogelijk maken en een betere beveiliging en gebruikservaring beloven. Passkeys maken gebruik van cryptografische sleutels die lokaal op een apparaat worden opgeslagen en alleen toegankelijk zijn via biometrische verificatie of een pincode, waardoor het risico op phishing en wachtwoorddiefstal aanzienlijk wordt verminderd. Digital identity wallets gaan nog een stap verder door gebruikers in staat te stellen hun digitale identiteiten, verificatiegegevens en toegangsrechten veilig op te slaan en te beheren binnen een gecentraliseerde, maar privacygerichte oplossing. Desondanks blijft de adoptie in Nederland achter. Dit rapport beschrijft de barrières en kansen die naar voren komen uit het onderzoek naar de implementatie van deze technologieën.

1.2 Onderzoeksdoel en methode

Het onderzoek richt zich op de volgende vraag: waarom is de adoptie van passkeys en digital identity wallets als authenticatiemiddel in Nederland laag? Daarbij wordt gekeken naar drie perspectieven:

- Gebruikersperspectief: acceptatie, vertrouwen en gebruiksgemak, omdat deze factoren sterk beïnvloeden of individuen bereid zijn nieuwe authenticatiemethoden te omarmen.
- Organisatieperspectief: implementatie-uitdagingen en kosten omdat organisaties bij adoptiebeslissingen vooral worden geconfronteerd met technische en financiële drempels, zoals investeringskosten en integratie met bestaande systemen.
- Technologisch: interoperabiliteit en technische randvoorwaarden, omdat de bredere inzetbaarheid van deze technologieën afhankelijk is van compatibiliteit tussen platforms en onderliggende infrastructuren.

Voor de beantwoording van deze vraag wordt zowel gebruik gemaakt van inzichten uit de literatuur als praktijkervaringen uit een expertworkshop en aanvullende interviews.

1.3 Kernbevindingen

Passkeys, gebaseerd op de FIDO2-standaard, bieden een veiliger alternatief voor wachtwoorden door middel van cryptografische sleutels. Grote technologiebedrijven zoals Apple, Google en Microsoft ondersteunen deze technologie, maar de adoptie blijft vooralsnog beperkt. Hoewel passkeys verschillende voordelen bieden, zoals verhoogde beveiliging,

phishing-resistentie en een verbeterde gebruikerservaring, zijn er nog verschillende drempels voor brede implementatie.

1. Veel gebruikers zijn onbekend met het concept en hebben vragen over de werking, specifiek met het herstelproces bij verlies van een passkey.
2. Compatibiliteitsproblemen met oudere systemen vertragen de implementatie binnen organisaties. Daarnaast vormt afhankelijkheid van IAM-leveranciers, die passkeys vaak nog niet aanbieden, een extra belemmering voor adoptie.
3. Op organisatorisch niveau zijn de kosten en capaciteitsgebrek een barrière voor het vernieuwen van een authenticatiesysteem, met name voor kleinere en middelgrote bedrijven. Het probleem wordt vaak niet als dusdanig groot gezien dat een overstap wordt gemaakt.

Digital identity wallets zijn een andere opkomende technologie die gebruikers in staat stelt om hun digitale identiteit en authenticatiegegevens op een veilige en privacyvriendelijke manier te beheren. Dit sluit aan bij bredere ontwikkelingen zoals de Europese Digital Identity Wallet (EUDI Wallet), die het gebruik van digitale identiteiten binnen de EU moet standaardiseren en vergemakkelijken. De voornaamste barrières voor de adoptie van wallets komen deels overeen met de passkeys, maar er zijn ook enkele specifiek voor wallets.

4. Wallets hebben de potentie de autonomie en privacy van gebruikers te vergroten, maar er blijft er nog veel onduidelijkheid over de precieze rolverdeling tussen gebruikers, organisaties en overheden. Daarnaast vormen het gebrek aan standaardisatie en interoperabiliteit tussen systemen belangrijke obstakels.
5. Voor veel organisaties is de adoptie van digital identity wallets primair gedreven door compliance met regelgeving, in plaats van door een strategische keuze om authenticatieprocessen te verbeteren. Op dit moment zijn er nog geen verplichtingen voor organisaties om wallets te accepteren, in de toekomst is dit voor enkele sectoren wel het geval.

Hoewel sommige van deze uitdagingen reëel zijn, hebben veel van de belemmeringen meer te maken met perceptie en communicatie rondom de oplossing dan met inherente technische of functionele problemen. Misverstanden over de werking van de technologie, zoals het herstelproces bij verlies van een passkey, of een gebrek aan duidelijke uitleg over de voordelen en werking van de technologie, dragen bij aan de terughoudendheid bij zowel gebruikers als organisaties. Dit benadrukt het belang van duidelijke communicatie en educatie om de adoptie van passkeys en digital identity wallets te versnellen.

Uit de praktijkervaringen blijkt dat er in zowel de literatuur als de interviews onvoldoende onderscheid wordt gemaakt tussen het gebruik van passkeys en digital identity wallets voor interne versus externe authenticatie. Dit onderscheid is echter essentieel, aangezien de implementatie en acceptatie van deze technologieën sterk afhangen van de context waarin ze worden toegepast. Voor intern gebruik binnen organisaties spelen vooral efficiëntie, compliance en IT-beheer een rol, terwijl voor externe klanten de gebruiksvriendelijkheid en het vertrouwen in de technologie doorslaggevend zijn. Dit vraagt om gerichte adoptiestrategieën die rekening houden met de specifieke uitdagingen en vereisten van verschillende gebruikersgroepen.

Overkoepelend: De adoptie van zowel passkeys als digital identity wallets blijft achter, ondanks hun voordelen op het gebied van beveiliging en gebruiksvriendelijkheid. Beide technologieën kampen met vergelijkbare obstakels, zoals onbekendheid bij gebruikers, technische incompatibiliteit en kosten voor organisaties.

De overstap wordt vaak pas aantrekkelijk wanneer de kosten van implementatie opwegen tegen de lange-termijnvoordelen, zoals verbeterde beveiliging en lagere operationele kosten. Voor kleinere bedrijven is de adoptie vaak minder urgent, terwijl wetgeving zoals de EUDI Wallet de adoptie voor bepaalde sectoren kan versnellen.

Hoewel passkeys en digital identity wallets verschillende toepassingen hebben, kunnen ze elkaar aanvullen. Organisaties moeten de voordelen en implementatiekosten zorgvuldig afwegen om de adoptie te versnellen, vooral wanneer strategische voordelen, zoals verhoogde beveiliging en compliance, duidelijker worden.

1.4 Aanbevelingen voor vervolgonderzoek

Om de adoptie van deze technologieën te bevorderen, wordt aanbevolen om verder onderzoek te doen naar:

1. **Het verschil tussen interne en externe adoptie** van wachtwoordloze authenticatie.
2. **De impact van digital identity wallets op de adoptie van passkeys:** stellen bedrijven de implementatie van technisch volwassen passkeys uit vanwege de ontwikkeling van digital identity wallets, die meer functionaliteiten beloven maar technisch nog minder rijp zijn (een vlucht naar voren)?
3. **Adoptiedrempels en schaalvoordelen**: hoe kan brede acceptatie worden versneld?
4. **Gebruikservaring en herstelprocessen**: hoe kunnen barrières voor gebruikers worden weggenomen?
5. **Effectieve communicatievormen richting eindgebruikers**: hoe kunnen misverstanden over de werking van passkeys en digital identity wallets worden voorkomen en gebruikers gerustgesteld worden over het herstelproces?
6. **Kosten versus baten voor organisaties en gebruikers**: wat zijn de economische voordelen en nadelen van de overstap naar passkeys en digital identity wallets en wanneer is het financieel verantwoord voor organisaties om over te stappen?

(Engelse versie)

1.1 Introduction

Identity Access Management (IAM) plays a crucial role in organizations' cybersecurity strategies. The traditional reliance on passwords leads to vulnerabilities such as phishing and brute-force attacks, increasing the need for more secure alternatives. Passkeys and digital identity wallets are two emerging technologies that enable passwordless authentication and promise improved security and user experience. Passkeys use cryptographic keys stored locally on a device, accessible only through biometric verification or a PIN, significantly reducing the risk of phishing and password theft. Digital identity wallets go a step further by allowing users to securely store and manage their digital identities, credentials, and access rights within a centralized but privacy-focused solution. Despite these advantages, adoption in the Netherlands remains limited. This report outlines the barriers and opportunities identified through research into the implementation of these technologies.

1.2 Research objective and method

The research focuses on the following question: Why is the adoption of passkeys and digital identity wallets as authentication methods in the Netherlands still low? It considers three perspectives:

- User perspective: Acceptance, trust, and ease of use, as these factors strongly influence whether individuals are willing to adopt new authentication methods.

- Organizational perspective: Implementation challenges and costs, as organizations often face technical and financial barriers—such as investment costs and integration with existing systems—when making adoption decisions.

- Technological perspective: Interoperability and technical requirements, since the broader usability of these technologies depends on compatibility between platforms and underlying infrastructures.

The research draws on insights from the literature, an expert workshop, and additional interviews.

1.3 Key findings

Passkeys, based on the FIDO2 standard, offer a more secure alternative to passwords through the use of cryptographic keys. Major tech companies like Apple, Google, and Microsoft support this technology, but adoption remains limited. While passkeys offer several advantages, such as increased security, phishing resistance, and improved user experience, there are still several barriers to widespread implementation:

1. Many users are unfamiliar with the concept and have questions about how it works, especially regarding recovery after losing a passkey.
2. Compatibility issues with legacy systems delay organizational implementation. Additionally, the dependence on IAM providers—many of whom do not yet support passkeys—poses an additional barrier to adoption.
3. At the organizational level, cost and lack of capacity are obstacles to updating authentication systems, particularly for small and medium-sized enterprises. The problem is often not perceived as urgent enough to warrant a transition.

Digital identity wallets are another emerging technology that enables users to manage their digital identity and authentication credentials in a secure and privacy-friendly way. This aligns with broader developments such as the European Digital Identity Wallet (EUDI Wallet), aimed at standardizing and facilitating digital identity use within the EU. The main barriers to wallet adoption partly overlap with those of passkeys, but there are also some wallet-specific issues:

4. Wallets have the potential to enhance user autonomy and privacy, but there is still a great deal of uncertainty regarding the precise division of roles between users, organizations, and governments. Moreover, the lack of standardization and interoperability between systems presents significant obstacles.
5. For many organizations, the adoption of digital identity wallets is primarily driven by regulatory compliance rather than a strategic decision to improve authentication processes. At present, there is no obligation for organizations to accept wallets, although this will change for certain sectors in the future.

While some of these challenges are real, many of the barriers are more related to perceptions and communication around the solution than to inherent technical or functional problems. Misunderstandings about how the technology works—such as the recovery process after losing a passkey—or a lack of clear explanations about its benefits and functioning contribute to hesitancy among both users and organizations. This highlights the

importance of clear communication and education to accelerate the adoption of passkeys and digital identity wallets.

Practice-based insights reveal that both the literature and the interviews often fail to clearly distinguish between the use of passkeys and digital identity wallets for internal versus external authentication. However, this distinction is crucial, as the implementation and acceptance of these technologies strongly depend on the context in which they are applied. For internal organizational use, factors such as efficiency, compliance, and IT management are key, while for external customers, user-friendliness and trust in the technology are decisive. This calls for targeted adoption strategies that consider the specific challenges and requirements of different user groups.

Overall:
Adoption of both passkeys and digital identity wallets remains limited, despite their benefits in terms of security and user-friendliness. Both technologies face similar obstacles, such as user unfamiliarity, technical incompatibility, and costs for organizations.

The transition often only becomes attractive when implementation costs are outweighed by long-term benefits, such as improved security and lower operational costs. For smaller companies, adoption is often less urgent, while legislation such as the EUDI Wallet may accelerate adoption in certain sectors.
Although passkeys and digital identity wallets serve different purposes, they can complement each other. Organizations should carefully weigh the benefits and implementation costs to accelerate adoption, especially when strategic advantages such as increased security and compliance become more apparent.

1.4 Recommendations for future research

To encourage adoption of these technologies, further research is recommended on the following topics:

1. **The difference between internal and external adoption** of passwordless authentication.
2. **The impact of digital identity wallets on the adoption of passkeys:** are companies postponing the implementation of technically mature passkeys because of the development of digital identity wallets, which promise more functionality but are still less mature (a leap forward)?
3. **Adoption barriers and economies of scale:** how can widespread acceptance be accelerated?
4. **User experience and recovery processes:** how can barriers for users be removed?
5. **Effective communication methods for end users:** how can misunderstandings about how passkeys and digital identity wallets work be prevented, and how can users be reassured about the recovery process?
6. **Cost-benefit analysis for organizations and users:** what are the economic pros and cons of switching to passkeys and digital identity wallets, and when is it financially justifiable for organizations to make the transition?

2 Introductie

Identity Access Management (IAM), oftewel identiteits- en toegangsbeheer, zorgt ervoor dat gebruikers worden geverifieerd en dat hun toegang tot gevoelige gegevens wordt geautoriseerd [1]. Dit omvat een breed scala aan processen waar diverse technologieën en protocollen bij worden gebruikt, van eenvoudige wachtwoorden tot meer geavanceerde multi-factor verificatiemethoden. Het is de eerste verdedigingslinie tegen cyberdreigingen.

Echter, het beheren van IAM-systemen kan tot uitdagingen leiden bij organisaties. Naarmate organisaties groter worden en meer complexe digitale infrastructuur ontwikkelen, nemen de risico's exponentieel toe, omdat er meer gebruikersaccounts, systemen, applicaties en toegangsrechten moeten worden beheerd. Dit leidt tot kritieke kwetsbaarheden zoals ongecontroleerde toegangsrechten, inefficiënte processen, complexiteit in beheer en nalevingsproblemen. Cyberaanvallers maken hier actief misbruik van, wat kan leiden tot datalekken, identiteitsfraude en miljoenenverliezen door financiële en reputatieschade [2].

Hierdoor is IAM niet langer slechts een IT-kwestie, maar een fundamentele pijler van elke cybersecuritystrategie. Het juiste beheer ervan is essentieel om compliance te waarborgen en organisaties te beschermen in een steeds dreigender cyberlandschap [3].

De zwakste schakel? Authenticatie. Een belangrijk onderwerp binnen IAM is identity management, dat zich bezighoudt met het beheren van digitale identiteiten gedurende hun levencyclus, en de rol van authenticatie, die ervoor zorgt dat deze identiteiten op een veilige manier worden geverifieerd voordat toegang wordt verleend. Zo zijn phishing-aanvallen een veelvoorkomend probleem; ze zijn ontworpen om gebruikers te misleiden en hen ertoe aan te zetten hun inloggegevens te delen via vervalste websites of e-mails [4]. In de financiële sector leidt tot aanzienlijke verliezen voor zowel consumenten als instellingen [5]. Ook bijvoorbeeld de zorg en overheidsinstellingen zijn kwetsbaar gebleken hiervoor, deze organisaties worden geconfronteerd met meer dan 1000 aanvallen per week [3]. Daarom is onderzoek naar het verbeteren van bestaande of het invoeren van nieuwe authenticatiemiddelen nog altijd belangrijk.

Wachtwoorden zijn een fundamenteel beveiligingsrisico. Authenticatiemiddelen kunnen worden onderverdeeld in drie categorieën: "wat je weet" (bijvoorbeeld een wachtwoord), "wat je hebt" (bijvoorbeeld een fysieke sleutel) en "wie je bent" (bijvoorbeeld via een vingerafdruk) [6]. Al sinds de jaren '70 is bekend dat wachtwoorden problematisch zijn [7]. Naast phishing zijn wachtwoorden kwetsbaar voor brute force-aanvallen, waarbij cybercriminelen geautomatiseerde systemen gebruiken om wachtwoorden te raden [8].

Bovendien kiezen gebruikers vaak voor zwakke of voorspelbare wachtwoorden, hergebruiken ze wachtwoorden voor meerdere accounts, of slaan ze wachtwoorden op onveilige locaties op. Dit maakt wachtwoorden niet alleen onveilig, maar ook onhandig voor gebruikers, die vaak worstelen met het onthouden van meerdere complexe wachtwoorden [9].

Toch blijven wachtwoorden de standaard. Dit komt deels door hun eenvoud, maar ook door het gebrek aan effectieve druk vanuit de industrie om over te stappen op veiligere

alternatieven [10]. Dit roept de cruciale vraag op: waarom worden veiligere methoden niet sneller geadopteerd?

2.1 Alternatieven voor authenticatie: Passkeys en Digital Identity Wallets

De zoektocht naar veiligere alternatieven is niet nieuw [10] en heeft geleid tot de ontwikkeling van twee vooraanstaande inlogmiddelen passkeys en digital identity wallets. Beide oplossingen beloven significant verbeterde beveiliging en gebruiksvriendelijkheid [11, 12]. Passkeys gebruiken cryptografische sleutels voor wachtwoordloze authenticatie, wat het risico op phishing en brute-force aanvallen aanzienlijk vermindert. Digital identity wallets zorgen voor veilige opslag en toegang tot digitale identiteiten, waardoor gebruikers snel en zonder herhaalde inlogpogingen toegang krijgen tot meerdere diensten, wat het gebruiksgemak verhoogt. Deze technologieën zijn essentieel voor het overwinnen van de tekortkomingen van traditionele wachtwoordsystemen, die nog steeds bijdragen aan groeiende beveiligingsrisico's.

Hoewel passkeys en digitale wallets verschillende functies en toepassingsgebieden hebben, vullen ze elkaar aan binnen het bredere domein van IAM. Passkeys richten zich specifiek op veilige en wachtwoordloze authenticatie [13, 14] wat de dreiging van phishing en brute-force aanvallen aanzienlijk vermindert. Digitale wallets zijn breder en bieden gebruikers de mogelijkheid om hun digitale identiteiten, betaalmethoden en andere belangrijke informatie veilig op te slaan en te gebruiken voor authenticatie bij verschillende diensten [15]. Door hun verschillende sterke punten bieden ze samen oplossingen voor zowel gerichte authenticatiebehoeften als bredere digitale interacties.

Passkeys, geïntroduceerd als onderdeel van de FIDO2-standaard in 2018, worden steeds vaker ondersteund door grote techbedrijven zoals Google, Apple en Microsoft [16, 17]. Digital identity wallets breiden de mogelijkheden uit door niet alleen wachtwoordloze authenticatie mogelijk te maken, maar ook door meerdere digitale identiteiten en betaalmethoden veilig op te slaan, wat de bredere toepasbaarheid vergroot. Het gebruik van digital identity wallets voor authenticatie is nog een relatief nieuwe ontwikkeling, met adoptie in kinderschoenen. Dit omdat er nog veel vragen beantwoord moeten worden voordat er een productrijpe 'plug-and-play' oplossing beschikbaar is. Het wordt wel ondersteund door de recente Europese EUDI wetgeving [33], die een juridisch kader biedt voor de interoperabiliteit, veiligheid en betrouwbaarheid van dergelijke digitale identiteiten binnen de EU.

2.2 Onderzoeksdoel

Dit onderzoek richt zich op het identificeren van de belangrijkste barrières voor de adoptie van passkeys en digital identity wallets als authenticatiemiddel in Nederland. Het centrale doel is om te begrijpen waarom de adoptie van deze technologieën achterblijft, ondanks de voordelen die ze bieden op het gebied van beveiliging en gebruiksvriendelijkheid.

De centrale onderzoeksvraag luidt: Waarom is de adoptie van passkeys en digital identity wallets als authenticatiemiddel in Nederland laag? Daarnaast wordt onderzocht welke belangrijke technische, organisatorische en gebruikers-gerelateerde factoren de adoptie van passkeys en digital identity wallets belemmeren.

2.3 Methodologie

Om deze vragen te beantwoorden worden zowel de belemmeringen die bekend zijn vanuit de literatuur als de belemmeringen die in de praktijk ervaren worden, geanalyseerd. Er wordt aandacht besteed aan technische, organisatorische en gebruikersgerelateerde factoren, omdat deze vaak als cruciale dimensies worden geïdentificeerd in de adoptie van nieuwe technologieën [18]. Technische factoren bepalen de technische haalbaarheid en compatibiliteit van innovaties, organisatorische factoren beïnvloeden de bereidheid en capaciteit van organisaties om technologieën te implementeren, en gebruikersgerelateerde factoren spelen een sleutelrol in de acceptatie door eindgebruikers. Deze drie dimensies bieden een geïntegreerd kader om de complexe interacties te analyseren die de adoptie beïnvloeden.

De belemmeringen uit de praktijk worden verder onderzocht via consultaties met deskundigen tijdens een workshop en enkele aanvullende interviews. De workshop richtte zich op het externe gebruik door klanten, terwijl de interviews specifiek ook vroegen naar interne adoptie binnen organisaties. Hiermee wilden we inzicht krijgen in de specifieke uitdagingen en overwegingen rondom het gebruik van passkeys en digital identity wallets door medewerkers. Literatuurstudies bieden vaak theoretische inzichten en zijn niet specifiek gericht op Nederland. Workshops met deskundigen bieden de mogelijkheid om concrete praktijkervaringen en context specifieke uitdagingen te identificeren. Workshops zijn gekozen als methodologie, omdat ze een interactieve omgeving bieden waarin deskundigen gezamenlijk complexe adoptieproblemen kunnen bespreken, verduidelijken en prioriteren. Deze vorm bevordert de uitwisseling van verschillende perspectieven en het identificeren van onderbelichte barrières, wat waardevolle aanvulling biedt op de theoretische analyse.

De resultaten van dit onderzoek kunnen bijdragen aan een beter begrip van de oorzaken achter de lage adoptie van passkeys en digital identity wallets in Nederland. Dit inzicht kan helpen om te bepalen hoe dergelijke technologieën kunnen bijdragen aan veiligere en gebruiksvriendelijkere authenticatieprocessen. Door de barrières in kaart te brengen, biedt dit onderzoek concrete handvatten voor het ontwikkelen van strategieën die organisaties en gebruikers in staat stellen nieuwe authenticatiemethoden effectief te omarmen en implementeren. Ook wordt bekeken hoe de adoptie voor intern (medewerkers) en extern (klanten) verschillen. Daarnaast kunnen de lessen uit de adoptie van passkeys en digital identity wallets breder worden toegepast om flexibeler in te spelen op de voortdurend veranderende dreigingen in het digitale landschap.

2.4 Structuur van het rapport

De volgende hoofdstukken bieden een gestructureerd overzicht van het onderzoek:

- Hoofdstuk 3: Werking Passkeys en digital identity wallets, met de verschillen en overeenkomsten.
- Hoofdstuk 4: Een bespreking van de adoptie van deze technologieën, met inzichten uit de literatuur.
- Hoofdstuk 5: Praktijkgerichte inzichten op basis van consultaties met deskundigen.
- Hoofdstuk 6: Conclusies en aanbevelingen vervolgonderzoek.

3 Passkeys en digital identity wallets

Zoals in de introductie aangegeven zijn zowel passkeys als wallets oplossingen voor een veiliger en vaak ook functionelere manier van inloggen. De techniek waarop passkeys en wallets zijn gebaseerd verschilt echter van elkaar. In dit hoofdstuk wordt de werking van zowel passkeys als wallets beschreven. In de laatste paragraaf worden de overeenkomsten en verschillen op een rijtje gezet.

3.1 Passkeys

Passkeys zijn een veilige en gebruiksvriendelijke manier van authenticatie die de traditionele wachtwoordbeveiliging kunnen vervangen. FIDO2 is een geavanceerde open beveiligingsstandaard voor passkeys die is ontwikkeld door de FIDO (Fast IDentity Online) Alliance en de World Wide Web Consortium (W3C). Het doel van FIDO2 is om via passkeys een sterke, veilige en gebruiksvriendelijke manier van authenticatie te bieden [19].

Passkeys zijn feitelijk een cryptografisch sleutelpaar, bestaande uit een publieke sleutel en een privésleutel. De beheerder van de privésleutel kan acties hiermee digitaal ondertekenen. Vervolgens kan iedereen met de publieke sleutel controleren of deze handtekening geldig is. Tijdens het aanmaken van een account wordt een dergelijk sleutelpaar gegeneerd door de gebruiker. De publieke sleutel wordt doorgestuurd naar de website; de privésleutel wordt opgeslagen bij de gebruiker op bijvoorbeeld een YubiKey of een online password manager en kan alleen gebruikt worden na het invoeren van een PIN of met biometrische gegevens. Elk sleutelpaar is dus uniek voor een specifieke website. Bij inloggen verstuurt de website een code naar de gebruiker die deze code cryptografisch ondertekent met de privésleutel. Deze ondertekende code stuurt de gebruiker naar de website, die de handtekening controleert met behulp van de publieke sleutel. Als deze klopt, kan de gebruiker worden ingelogd. Zie de appendix voor meer technische details.

Binnen het FIDO2-protocol zijn er enkele centrale rollen (Tabel 3.1), deze zijn essentieel om te begrijpen hoe het systeem functioneert [20, 21]:

Tabel 3.1: Verschillende rollen en hun eigenschappen in het FIDO2-protocol

Rol	Beschrijving	Voorbeeld
Authenticator	De plek waar sleutelparen worden opgeslagen, zoals een hardware-token of een beveiligde module op een apparaat	YubiKey, Apple Keychain, Android Password Manager
Gebruiker	De fysieke persoon die probeert in te loggen of een account aan te maken	Een individu die inlogt op een website
Client/Host	Het apparaat waarmee de gebruiker toegang probeert te krijgen tot een dienst via het internet	Computer, smartphone
Relying Party / Server	De partij waarbij de gebruiker probeert in te loggen, bijvoorbeeld een dienstverlener of platform	E-mailprovider, bankapp

Het FIDO2-protocol bestaat uit twee belangrijke componenten: het WebAuthn-protocol van de W3C, dat verantwoordelijk is voor de communicatie tussen server, client en authenticator, en het Client To Authenticator Protocol (CTAP), dat zorgt voor veilige communicatie tussen de client en de authenticator [22]. Er zijn twee versies van het CTAP protocol. De eerste (CTAP1, tegenwoordig FIDO U2F) kan alleen gebruikt worden voor twee-factor authenticatie. De opvolger CTAP2 is flexibeler en ondersteunt gebruikersverificatie, waardoor het ook als volwaardig authenticatiemiddel gebruikt kan worden. In dit onderzoek focussen wij ons op de combinatie van WebAuthn en CTAP2, als vervanger van wachtwoorden [17].

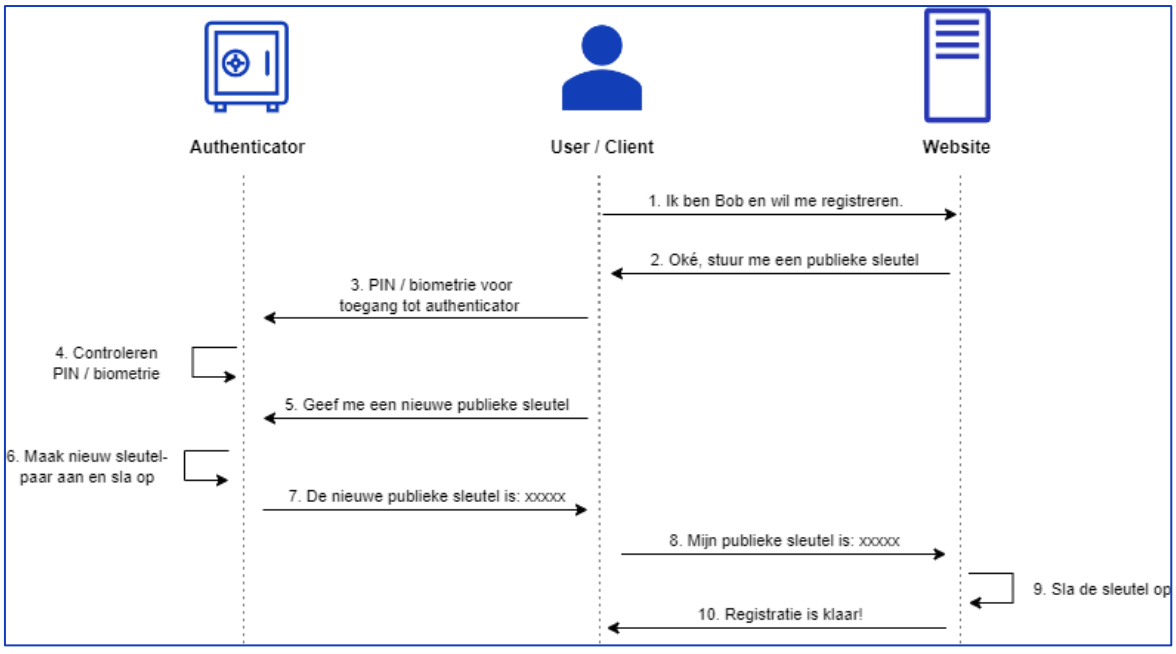
3.1.1 Registratie van een nieuwe passkey

Het registreren van een nieuwe passkey gebeurt bijvoorbeeld bij het aanmaken van een account of het omzetten van een wachtwoord naar een passkey. Vanuit gebruikersperspectief bestaat dit proces uit 2 stappen:

1. De gebruiker geeft bij de website aan dat hij zich wil registreren.
2. De authenticator vraagt de gebruiker om de toegangscode of biometrie en de gebruiker voert deze in. Hiermee is de gebruiker geregistreerd bij de website.

Op de achtergrond vinden er meer technische stappen plaats. Dit proces kan worden samengevat in zes stappen (Figuur 3.1):

1. De server stuurt informatie over diens identiteit naar de client.
2. De client controleert de identiteit van de server en stuurt het verzoek door naar de authenticator.
3. De authenticator vraagt de gebruiker om toestemming voor toegang tot de geheime sleutels.



Figuur 3.1: Hoogover overzicht van registratieproces

4. De authenticator genereert een sleutelpaar (privé- en publieke sleutel) en stuurt de publieke sleutel naar de server. De privésleutel wordt beveiligd opgeslagen op de authenticator.
5. De server slaat de publieke sleutel en een identifier op in een database.
6. Na registratie kan de gebruiker inloggen met deze passkey.

Een optionele uitbreiding op het registratieproces is het gebruik van attestaties, waarbij de server garanties kan krijgen over het type authenticator dat de gebruiker gebruikt, bijvoorbeeld voor hoogbeveiligde toepassingen. Hiermee kan de server het gebruik van bepaalde types authenticators afdwingen. Zie voor meer informatie hierover de technische appendix.

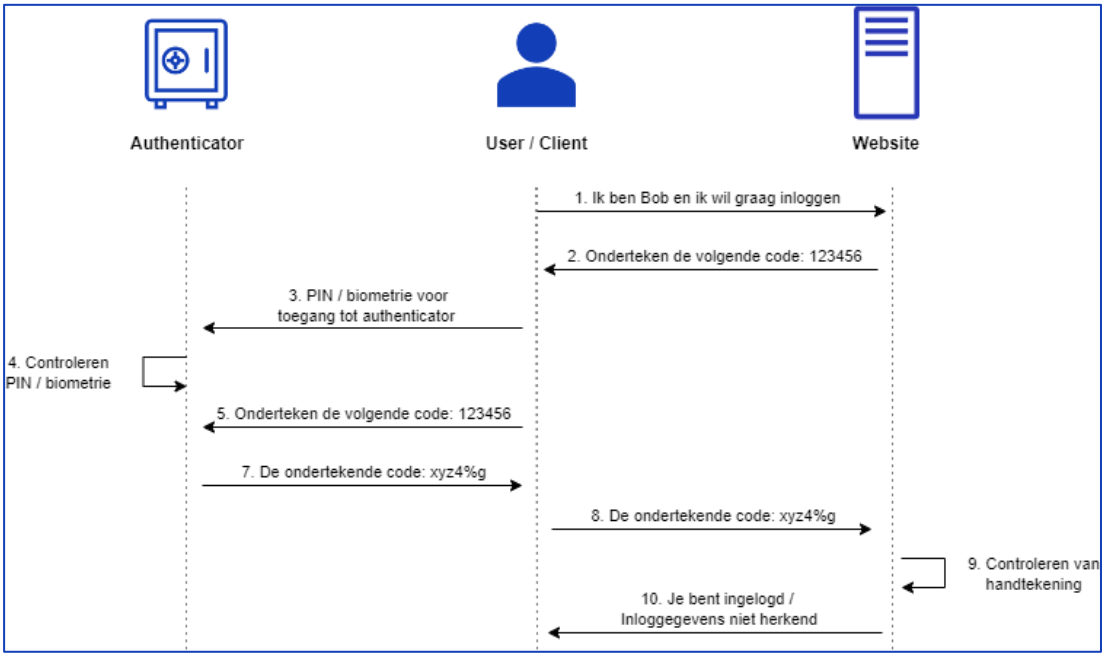
3.1.2 Inloggen met een passkey

Voor de gebruiker is het inlogproces erg vergelijkbaar met het registratieproces:

1. De gebruiker geeft bij de website aan dat hij wil inloggen.
3. De authenticator vraagt de gebruiker om de toegangscode of biometrie en de gebruiker voert deze in.
4. De gebruiker is ingelogd bij de website.

Op de achtergrond werkt het inloggen met behulp van een zogeheten ‘challenge’. Deze ‘challenge’ is een cijferreeks die de server naar de client stuurt. De server daagt de client in zekere zin uit om deze cijferreeks te ondertekenen. Als de client aan deze challenge kan voldoen, is de gebruiker dus in bezit van de privésleutel en wordt daarmee ingelogd. Het proces verloopt als volgt (Figuur 3.):

1. De server genereert een challenge en stuurt deze samen met zijn identiteit naar de client.



Figuur 3.2 Hoogover overzicht van authenticatieproces

2. De client controleert de identiteit van de server en stuurt de challenge naar de authenticator.
3. De authenticator vraagt de gebruiker om toegang tot de geheime sleutels.
4. De authenticator ondertekent de challenge met de privésleutel die is aangemaakt bij de registratie en stuurt dit terug naar de server.
5. De server verifieert de handtekening, de challenge en de counter. Indien alles klopt, is de gebruiker geauthenticeerd.

Dit zorgt voor veilige inlogprocessen zonder wachtwoorden, waarbij de gebruiker slechts biometrie of een PIN hoeft te gebruiken om toegang te krijgen tot de authenticator.

Voor organisaties betekent dit een aanzienlijke vermindering van phishing-aanvallen en datalekken, aangezien gebruikers geen wachtwoorden meer invoeren die kunnen worden onderschept. Dit past goed binnen zero-trust architecturen, waarbij elke interactie als onveilig wordt beschouwd tot bewezen veilig [23].

3.1.3 Herstel van kwijtgeraakte passkeys

Het kwijtraken van een passkey, bijvoorbeeld door het verlies van een telefoon, kan problematisch zijn. Voor de adoptie van passkeys is het daarom belangrijk om goede herstelmethoden te hebben. Er zijn verschillende strategieën die variëren in gebruiksgemak, inzetbaarheid en veiligheid. Enkele voorbeelden zijn: [24]:

- Wachtwoorden/One-time password

Een back-up wachtwoord of een eenmalige code via SMS kan worden gebruikt, maar deze methoden ondermijnen het doel van passkeys, omdat ze alsnog vatbaar zijn voor phishing.

- FIDO2-back-up token

Gebruikers kunnen een tweede back-up passkey registreren op een ander apparaat. Als de primaire passkey verloren gaat, kan de gebruiker inloggen met de back-up en een nieuwe passkey aanmaken.

- Identiteitskaart

Een digitale of fysieke ID-kaart kan gebruikt worden om toegang te herstellen, maar dit kan de privacy verminderen omdat de webservice moet weten welke ID-kaart aan welke passkey gekoppeld is.

De herstelmethoden verschillen in hun beveiligingsniveau. Het gebruik van back-up tokens wordt vaak gezien als een veiliger alternatief dan traditionele wachtwoorden of eenmalige codes. Voor sectoren met hogere beveiligingseisen, kunnen hardware tokens zoals YubiKeys worden vereist. Met deze methoden bieden passkeys een robuust kader voor wachtwoordloze authenticatie, terwijl het rekening houdt met zowel beveiliging als gebruiksgemak [25, 26].

3.1.4 Implementaties

Verschillende online password managers maken het tegenwoordig ook mogelijk om passkeys in de cloud op te slaan in plaats van op een eigen apparaat. Bekende voorbeelden zijn de Google Password Manager [27], Apple KeyChain [28], 1Password [29]. De kans op verlies is dan kleiner, omdat de passkey niet meer aan een specifiek wachtwoord verbonden is. Ook wordt het mogelijk om passkeys te synchroniseren tussen verschillende apparaten of deze zelfs te delen met anderen (Apple KeyChain) Dit vergroot het gebruiksgemak, maar aan de

andere kant wordt (afhankelijk van de specifieke implementatie) een belangrijk principe rondom passkeys gebroken: de privésleutel staat niet op de specifieke hardware van de gebruiker [24]. Hiermee vergroot het de mogelijkheden voor aanvallers om mensen passkeys te laten delen met een aanvaller, waardoor phishingaanvallen weer mogelijk worden.

3.2 Digital identity wallets

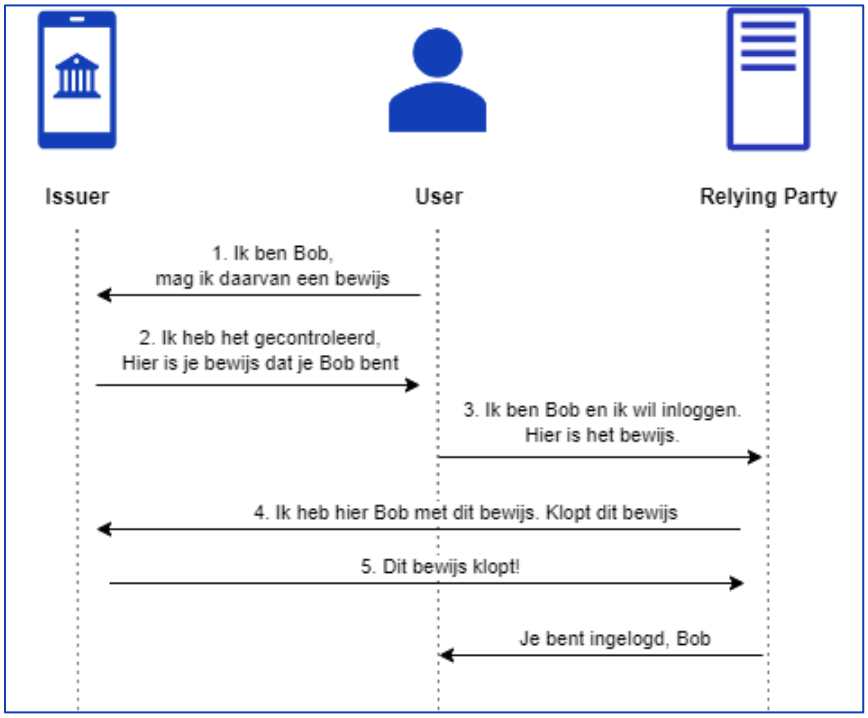
Een ander alternatief voor inloggen met wachtwoorden maakt gebruik van digital identity wallets. Binnen de context van de Europese Unie wordt gewerkt aan de European Digital Identity (EUDI) Wallet. De EUDI Wallet heeft als doel om EU-burgers, inwoners en bedrijven een digitale portefeuille te bieden waarmee zij hun persoonlijke gegevens, zoals rijbewijzen en diploma's, veilig kunnen opslaan en delen binnen de lidstaten [30]. De gegevens die worden opgeslagen in de wallet worden attestaties genoemd [12]. De EUDI Wallet sluit aan bij de bredere beweging naar self-sovereign identity (SSI), waarbij individuen meer controle hebben over hun digitale identiteiten en de informatie die zij delen. Ook kunnen de ontvangers die informatie digitaal verifiëren zonder dat de uitgever of een derde partij weet heeft van deze uitwisseling. Gebruikers hebben controle over hun gegevens en kunnen beslissen met wie ze informatie delen en voor hoelang, wat de privacy en veiligheid versterkt [31].

Digitale wallets kunnen op verschillende manieren worden geïmplementeerd, maar in vrijwel alle implementaties worden er vier rollen onderscheiden (Tabel 3.2) [15, 32]. In dit rapport gebruiken we de terminologie die gebruikt wordt in de EUDI Architecture and Reference Framework [27].

Tabel 3.2: Verschillende rollen en hun eigenschappen bij digital identity wallets

Rol	Beschrijving	Voorbeeld	Andere namen
Issuer	Een instantie die digitale attestaties verstrekt aan de gebruiker, zoals een digitale ID-kaart of een diploma.	Overheid, onderwijsinstelling	Identity Providers, Uitgevende partij
Gebruiker	De persoon die de digitale wallet beheert en bij een issuer attestaties kan opvragen om zich te identificeren bij verschillende relying parties .	Persoon met een digitale wallet	
Relying party (RP)	De partij waar de gebruiker zich identificeert door middel van een attestatie uit de wallet, zoals een bank of werkgever.	Bank, werkgever	Dienstverlener (SP), Controlerende instantie
Toezichthouder	Een instantie die toeziet op de naleving van regels en voorwaarden met betrekking tot het gebruik van digitale attestaties en wallets.	Overheid, toezichthouder	Controlling Party

In tegenstelling tot passkeys, waarbij de issuer en de relying party dezelfde partij zijn, kan een gebruiker bij een wallet-model inloggen bij een andere partij d5Aq*23an de issuer. Dit is bijvoorbeeld het geval bij het eIDAS1-model, waar een burger gebruik kan maken van een overheidsdienst in een ander land door in te loggen via het portaal van het thuisland. De relying party moet dan vertrouwen op de inloggegevens van de issuer.



Figuur 3.3 Authenticatie met wallets

3.2.1 Authenticatie met wallets

Binnen het eIDAS2-model kan een gebruiker inloggen met behulp van een wallet in de volgende stappen (Figuur 3.):

1. De gebruiker vraagt eenmalig een attestatie aan bij een issuer, bijvoorbeeld de overheid. Wanneer een gebruiker deze attestatie kwijt raakt, moet deze ook opnieuw worden aangevraagd.
2. Wanneer de gebruiker wil inloggen bij een relying party, presenteert deze de ontvangen attestatie naar die partij. Dezelfde attestatie kan meerdere keren gebruikt worden om in te loggen.
3. De relying party controleert de status de attestatie bij de issuer of een versleuteld register. Als de attestatie geldig is, wordt de gebruiker ingelogd. Zo niet, dan ontvangt de gebruiker een foutmelding.

3.3 Passkeys versus digital identity wallets: verschillen en overeenkomsten

Zowel passkeys als digital wallets bieden een manier om gebruikers te authenticeren zonder wachtwoorden, maar er zijn enkele belangrijke verschillen.

- Toepassing
  Passkeys zijn specifiek ontworpen om wachtwoorden te vervangen bij het inloggen, terwijl digital wallets breder inzetbaar zijn voor het opslaan en beheren van identiteiten, betaalbewijzen en documenten [22].
- Identiteit
  Bij digital wallets wordt de identiteit van de gebruiker bevestigd door een attestatie die is uitgegeven door een derde partij (de issuer). Bij passkeys is er geen tussenkomst van een derde partij. Dit betekent dat digital wallets, door hun afhankelijkheid van externe providers, kwetsbaar kunnen zijn voor aanvallen of fouten bij de issuer. Binnen EUDIW worden daarom ook strenge veiligheidseisen gesteld aan de issuer (LoA High) [29].
- Volwassenheid
  Passkeys zijn inmiddels ver genoeg ontwikkeld om praktisch te worden toegepast en worden ondersteund door grote technologiebedrijven. Digital wallets zijn technisch nog meer in ontwikkeling. Wel moeten eind 2026 overheidsinstanties voor strong user authentication EUDI Wallet accepteren. Vanaf eind 2027 moet EUDI Wallet ook in andere sectoren (o.a. zorg, onderwijs) worden geaccepteerd voor strong user authentication [29].

Om de effectiviteit en bruikbaarheid van zowel passkeys als digital wallets volledig te begrijpen, is het belangrijk om niet alleen naar de technologie zelf te kijken, maar ook naar de factoren die hun adoptie in de praktijk beïnvloeden. Hoewel implementatie van digitale wallets in Europa is ontworpen om de waarden van privacy en autonomie in een digitale wereld te waarborgen, is hun adoptie nog in een vroeg stadium. Passkeys daarentegen worden al ondersteund door grote technologiebedrijven en zijn technisch verder ontwikkeld.

In het volgende hoofdstuk wordt de adoptie van passkeys en wallets onderzocht vanuit gebruikers-, organisatorische en technische perspectieven. De uitdagingen die nog overwonnen moeten worden voor de brede acceptatie van deze technieken als vervanger van traditionele wachtwoorden worden geanalyseerd.

4 Adoptie: inzichten uit de literatuur

In dit hoofdstuk wordt, op basis van eerder empirisch onderzoek, de adoptie van passkeys en digital wallets besproken vanuit drie perspectieven: gebruikers, organisaties en technische implementatie. Elk perspectief biedt unieke uitdagingen en inzichten die essentieel zijn voor het begrijpen van de implementatiebarrières en -kansen van passkeys en digital wallets in verschillende contexten. Deze drie perspectieven zijn gekozen omdat ze gezamenlijk een breed en geïntegreerd inzicht bieden in de complexe factoren die de adoptie beïnvloeden, van de ervaringen en acceptatie door gebruikers tot de organisatorische bereidheid en technische haalbaarheid van de implementatie.

Hoewel er al relatief veel onderzoek is naar de adoptie van passkeys, is er minder beschikbaar over digital wallets. Dit komt doordat digital wallets een relatief nieuw concept zijn en de implementatie ervan nog in de beginfase verkeert.

4.1 Adoptie vanuit gebruikersperspectief

Eerder onderzoek rondom adoptie van passkeys bij gebruikers toonde aan dat deelnemers de FIDO2-authenticatie zonder wachtwoord verkozen boven het gebruik van een wachtwoord [33]. In dit onderzoek werd gebruik gemaakt van een between-group onderzoeksdesign, waarbij de deelnemers in een gecontroleerde omgeving interacteerden met het registratie- en authenticatieproces van webapplicaties. Deelnemers werden willekeurig toegewezen aan twee groepen: de ene groep gebruikte passkeys, terwijl de controlegroep wachtwoorden gebruikte. Elk van de groepen kreeg slechts één van de authenticatiemethoden te zien, zodat er geen vergelijkingen tussen de methoden konden worden gemaakt, wat potentieel vooringenomenheid in de resultaten zou hebben veroorzaakt. De proefpersonen kregen instructievideo's over hun specifieke authenticatiemethode, waarna zij hands-on ervaring opdeden met het registreren en inloggen op gesimuleerde websites. Dit hielp de onderzoekers inzicht te krijgen in hun gedachten en zorgen omtrent de adoptie van de technologie.

Er werden enkele bezorgdheden geuit: gebruikers gaven aan onzeker te zijn over hoe zij hun accounts zouden kunnen herstellen als de beveiligingssleutel verloren zou gaan, wat een belangrijke barrière kan zijn voor verdere adoptie. Daarnaast werden er zorgen geuit over de compatibiliteit van de hardware; sommige deelnemers hadden problemen met het correct aansluiten van de sleutel op hun apparaat of merkten dat hun hardware verouderd was. Verder bleek uit het onderzoek dat gebruikers onvoldoende duidelijke uitleg kregen over de werking van wachtwoordloze authenticatie, wat leidde tot verwarring over de beveiligingsvoordelen die passkeys [33]. Een andere studie laat zien dat gebruikers vaak een verkeerd beeld hebben van de werking van passkeys. Twee derde van de deelnemers dacht dat in het protocol hun biometrische gegevens naar de website gestuurd werden, iets wat niet het geval is. Door middel van duidelijkere notificaties kon dit aantal naar beneden worden gebracht. Ondanks deze zorgen over het versturen van biometrische gegevens, waren deelnemers in deze studie wel bereid om in te loggen met hun biometrische gegevens in plaats van met wachtwoorden [34].

In vergelijkbaar onderzoek gebruikten deelnemers een YubiKey tijdens hun dagelijkse werkzaamheden en hielden bij wanneer ze authenticeerden [35]. Deze studie werd uitgevoerd bij een klein softwarebedrijf in Duitsland. De onderzoekers pasten het bestaande inlogsysteem van de webapplicatie aan door de optie toe te voegen om in te loggen met WebAuthn en een YubiKey. Alle deelnemers kregen training in het gebruik van de beveiligingssleutel en hun dagelijkse inlogpogingen werden gemonitord. De studie duurde drie weken, waarbij de FIDO2-authenticatie op zowel een testserver als een productieserver werd ingezet. Gebruikers konden kiezen tussen inloggen met een wachtwoord of de beveiligingssleutel. Er werd gebruikgemaakt van FIDO2-compliant hardwaretokens van Yubico, en de loggegevens van inlogpogingen werden geanalyseerd, inclusief inlogtijden en foutmeldingen veroorzaakt door incompatibiliteit met bepaalde browsers.

De deelnemers reageerden positief op de beveiligingssleutels, en noemden gebruiksgemak, intuïtiviteit en gemak als voordelen. Sommige deelnemers stopten echter met het gebruik van de sleutel omdat ze ten onrechte dachten dat deze geen beveiligingsvoordelen bood of omdat ze het langzamer vonden dan hun browser's wachtwoordmanager [35]. Dit was vooral een kwestie van perceptie: de FIDO2-technologie biedt wel degelijk een hogere mate van beveiliging, maar het gebrek aan duidelijke communicatie over deze voordelen kan leiden tot misverstanden en zelfs terughoudendheid bij gebruikers. Dit benadrukt het belang van duidelijke communicatie over de daadwerkelijke voordelen van FIDO2-technologie om misvattingen te voorkomen.

Ander recent onderzoek uit 2024 geeft aan dat Chief Information Security Officers (CISOs) denken dat veel gebruikers, vooral niet-technische, overweldigd kunnen raken door de veranderingen die passkeys met zich meebrengen [17]. Deze bevindingen zijn gebaseerd op 28 semi-gestructureerde interviews met drie typen belanghebbenden: (1) bedrijven en organisaties met webplatforms voor eindgebruikers, zowel organisaties die al wachtwoordloze authenticatie hebben geïmplementeerd als die dat nog niet hebben gedaan; (2) leveranciers van wachtwoordloze oplossingen voor bedrijven; en (3) experts die bijdragen aan de FIDO2-standaard. De interviews waren gericht op het begrijpen van de ervaringen van de deelnemers met wachtwoordloze authenticatie in hun eigen organisaties, het identificeren van obstakels bij de implementatie, en het achterhalen van persoonlijke meningen over de FIDO2-standaard. Als onderdeel van de methode werd ook een card-sorting taak uitgevoerd om potentiële implementatie-uitdagingen te rangschikken en te bespreken.
Er is een aanzienlijke leercurve, en het gebrek aan bekendheid met de technologie kan leiden tot weerstand tegen adoptie. Bovendien kunnen passkeys bepaalde gebruikersgroepen uitsluiten die geen toegang hebben tot de vereiste hardware of die moeite hebben met technologie. Dit is problematisch voor essentiële diensten zoals bankdiensten, waar uitsluiting ernstige gevolgen kan hebben [17].

Hetzelfde onderzoek toont ook aan dat, hoewel niet universeel, er zorgen zijn over de opslag van biometrische gegevens, vooral in Europa. Werknemersraden in landen zoals Frankrijk en Duitsland hebben bezorgdheid geuit over waar en hoe deze gegevens worden beheerd. Daarnaast hebben sommige gebruikers negatieve ervaringen gehad met eerdere biometrische oplossingen, wat hun vertrouwen in passkeys vermindert. Er zijn ook twijfels over de toegevoegde waarde van passkeys voor mobiele apps die al lokale biometrische authenticatie aanbieden, zoals gezichtsherkenning of vingerafdrukscanners [17].

Tot slot benadrukt het onderzoek dat CISOs aangeven dat de voordelen van traditionele wachtwoorden vanwege hun universele toepasbaarheid, ongeacht het apparaat of de omgeving niet kunnen geëvenaard worden door passkeys, vooral niet in

productieomgevingen waar biometrische authenticatie onbetrouwbaar kan zijn door het gebruik van handschoenen, maskers of vuile handen. Hoewel dit geen tekortkoming van de technologie zelf is, wordt het in de praktijk wel zo ervaren door gebruikers. Voor kleinere bedrijven en individuen met beperkte middelen kunnen de kosten en complexiteit van passkey-implementatie een barrière vormen [17]. Het is daarom belangrijk om te erkennen dat sommige van deze uitdagingen meer te maken hebben met percepties en specifieke use-cases dan met de technische beperkingen van passkeys.

Het gebruikersperspectief is lastiger te onderzoeken voor digital wallets, aangezien er nog maar weinig implementatie is van de technologie. In één studie hebben onderzoekers deelnemers laten werken met een prototype wallet app vanuit een extern klantenperspectief. Hieruit blijkt dat voor gebruikers niet altijd duidelijk is wie de controle heeft over welke data. Ongeveer de helft van de deelnemers geeft aan vertrouwen te hebben een versie van de wallet app die het meest vergelijkbaar zijn met passkeys. Wanneer een derde partij de identificatie doet, heeft een meerderheid van de deelnemers vertrouwen in de veiligheid van hun gegevens. De onderzoekers concluderen dat voor adoptie van wallets door gebruikers niet gefocust moet worden op een technisch verhaal, maar de positie van de gebruiker meer centraal moet komen te staan [36].

4.2 Adoptie vanuit organisatorisch perspectief

Vanuit organisatorisch perspectief hebben bedrijven en instellingen uiteenlopende ervaringen met passkeys. In een recente studie uit 2024 werd via semi-gestructureerde interviews onder CISOs inzicht verkregen in de belangrijkste obstakels voor de adoptie van passkeys voor zowel intern gebruik bij werknemers als extern gebruik voor klanten [17]. De respondenten uitten zorgen over de kosten van hardware en de complexiteit van infrastructuur aanpassingen. Vooral voor middelgrote en kleinere organisaties blijken de investeringen in passkeys en de nodige IT-upgrades soms moeilijk te rechtvaardigen. Bovendien bemoeilijken verschillende regelgevingseisen in diverse landen de wereldwijde invoering van passkeys, wat een specifieke uitdaging is voor internationale bedrijven. Organisaties hebben vaak te maken met verschillende juridische kaders, waardoor uniforme invoering van passkeys op wereldwijde schaal lastig is. Bijvoorbeeld, de Algemene Verordening Gegevensbescherming in de EU stelt strikte eisen aan de verwerking van persoonlijke gegevens, terwijl in de VS verschillende wetgevingen zoals de California Consumer Privacy Act van toepassing zijn. Deze variaties in regelgeving maken het voor internationale organisaties lastig om passkeys wereldwijd uniform en conform in te voeren.

Daarnaast zijn de huidige mogelijkheden voor het centraal beheren van passkey-credentials beperkt. Dit maakt het voor IT-afdelingen lastig om niet-technische werknemers te ondersteunen bij het registreren van credentials. Het fysiek terughalen van beveiligingssleutels bij beëindiging van een account of dienstverband kan extra complicaties opleveren, zoals het beheren en beveiligen van hardware [17].

Tot slot zijn veel bedrijven onzeker over de noodzaak van passkeys. Sommige organisaties voelen zich al voldoende beveiligd met hun huidige oplossingen zoals multi-factor authenticatie of merken geen vraag van klanten naar passkeys. Negatieve ervaringen met andere biometrische oplossingen kunnen het enthousiasme voor passkeys verder temperen. Daarnaast bestaat er bezorgdheid over het beheer van passkeys, vooral als gebruikers een groot aantal accounts moeten beheren, wat uitdagingen kan opleveren op het gebied van gebruiksvriendelijkheid en beveiliging [17].

Bij digital wallets blijken de organisatorische barrières voor implementatie divers. Hierbij speelt de context (publiek/privaat) waarin een wallet wordt gebruikt een grote rol. In een publiek-privaat ecosysteem lijken interactiebarrières en innovatiebarrières de grootste pijnpunten bij de introductie van digitale wallets. Dit blijkt uit een Nederlands onderzoek waarin aan de hand van twee workshops barrières voor het uitrollen van digital wallets voor gebruik bij burgers in kaart zijn gebracht [37]. Interactiebarrières zijn bijvoorbeeld een gebrek aan standaardisatie, gebrek aan vertrouwen tussen partijen of angst voor monopolievorming. Voorbeelden van innovatiebarrières zijn backwards compatibility en dat het voordeel van de innovatie niet altijd ligt bij de partij die de lasten draagt. Wel was er veel discussie tussen de deelnemers van de workshop over de relevantie van elkaars barrières.

4.3 Adoptie vanuit technisch perspectief

Op technisch vlak zijn er diverse uitdagingen geïdentificeerd die de adoptie van passkeys vertragen. Onderzoek uit 2019 benoemde kort enkele conceptuele beperkingen bij het implementeren van WebAuthn door de discussies binnen de WebAuthn-ontwikkelaarsgemeenschap te analyseren. Deze beperkingen omvatten een gebrek aan kant-en-klare oplossingen, verkeerde mentale modellen over WebAuthn, en verwarrende technische details in de FIDO2-specificatie [38]. Ander onderzoek wees op mogelijke uitdagingen van het gebruik van passkeys voor wachtwoordloze authenticatie, zoals het ontbreken van een handige herstelmethode en ondersteuning voor het delen van inloggegevens [39]. Ook blijkt dat bedrijven mogelijk niet in staat zijn om de huidige FIDO2-oplossingen te implementeren die voldoen aan hun beleidsregels, de specifieke beleidsregels worden niet benoemd [40].

Daarnaast werd er geïdentificeerd dat niet alle browsers, vooral mobiele browsers, passkeys volledig ondersteunen. Zo biedt Mozilla Firefox slechts gedeeltelijke ondersteuning voor FIDO2 op bepaalde besturingssystemen. Daarnaast is legacy software, die vaak essentieel is in industriële omgevingen, meestal niet compatibel met moderne cloud-gebaseerde FIDO2-oplossingen. Dit kan resulteren in een heterogene en moeilijk te beheren authenticatie-infrastructuur voor intern gebruik bij werknemers als extern gebruik bij klanten [17].

Ten slotte, is een ander belangrijk knelpunt de complexiteit van de FIDO2-protocollen zelf. Deze zijn niet ontworpen voor implementatie door ontwikkelaars zonder specialistische kennis. Het gebrek aan uitgebreide documentatie maakt dit probleem nog groter, waardoor het voor bedrijven moeilijk is om passkeys effectief te implementeren [17]. Bedrijven die willen overstappen naar passkeys, hebben vaak te maken met een steile leercurve, en zonder de juiste ondersteuning kan dit leiden tot fouten in de uitrol en terughoudendheid om verder te gaan met de technologie.

Uit [37] blijkt dat de meningen gemixt zijn over de complexiteit van de ingebruikname van digital wallets voor burgerauthenticatie.

4.4 Takeaway

De adoptie van passkeys en digitale wallets biedt zowel voordelen als uitdagingen, die sterk afhankelijk zijn van het perspectief dat wordt ingenomen. Belangrijke nuance is dat de literatuur verder is in het onderzoek naar passkeys dan naar wallets.

Hoewel sommige van deze uitdagingen reëel zijn, hebben veel van de belemmeringen meer te maken met perceptie en communicatie rondom de oplossing dan met inherente technische of functionele problemen. Misverstanden over de werking van de technologie of een gebrek aan duidelijke uitleg dragen bij aan de terughoudendheid bij zowel gebruikers als organisaties.

In Tabel 4.1 en Tabel 4.2 worden de ervaren belemmeringen uit de literatuur omtrent passkeys en digital wallets samengevat.

Tabel 4.1: Ervaren belemmeringen passkeys uit de literatuur

Perspectief	Passkeys belemmeringen
Gebruikers	- Onzekerheid over accountherstel bij verlies van de beveiligingssleutel. - Compatibiliteitsproblemen met hardware. - Gebrek aan duidelijke uitleg over wachtwoordloze authenticatie, wat leidt tot verwarring. - Misverstanden over de werking van passkeys en biometrische gegevens.
Organisatorisch	- Hoge kosten voor hardware en infrastructuuraanpassingen, vooral voor kleine en middelgrote bedrijven. - Onzekerheid over de noodzaak van passkeys, omdat bestaande oplossingen als voldoende worden beschouwd. - Regelgevingseisen die wereldwijde invoering bemoeilijken.
Technisch	- Beperkte ondersteuning door browsers, vooral mobiele browsers. - Compatibiliteitsproblemen met legacy systemen. - Complexiteit van passkeys-implementaties, wat specialistische kennis vereist.

Tabel 4.2: Ervaren belemmeringen digital wallets uit de literatuur

Perspectief	Digital Wallets Belemmeringen
Gebruikers	- Onzekerheid over wie de controle heeft over hun gegevens. - Gebrek aan vertrouwen in de technologie bij een derde partij. - Onduidelijkheid over wat een wallet precies inhoudt, wat leidt tot verwarring.
Organisatorisch	- Financiële en operationele uitdagingen bij implementatie, afhankelijk van de context (publiek/privaat). - Interactiebarrières, zoals gebrek aan standaardisatie en vertrouwen tussen partijen. - Angst voor monopolievorming en gebrek aan voordelen voor partijen die de lasten dragen.
Technisch	- Onduidelijkheid over de technische implementatie van wallets. - Weinig ervaring met implementatie leidt tot onzekerheid en terughoudendheid bij organisaties.

5 Inzichten uit de praktijk

Theoretische inzichten en technische evaluaties bieden waardevolle informatie over de mogelijkheden en beperkingen van deze technologieën. Toch is het ook belangrijk om praktijkervaringen en expertperspectieven in te brengen. Daarom hebben we een workshop en enkele interviews georganiseerd met een diverse groep van in totaal 10 experts. We hebben specifiek gekozen voor deze experts vanwege hun directe betrokkenheid bij de implementatie en het beheer van identiteits- en toegangsbeheeroplossingen binnen organisaties. Zo kunnen IAM-managers inzicht geven in de organisatorische en gebruikersgerichte uitdagingen rondom adoptie, terwijl solution architects technische haalbaarheid en integratievraagstukken belichten. IT&C-strategiemanagers brengen een breder perspectief op strategische implementatie en beleidsvorming, en enterprise architects bewaken de compatibiliteit en samenhang met bestaande IT-systemen. Door deze verschillende perspectieven te combineren, konden we een gebalanceerd beeld vormen van allerlei type uitdagingen en kansen rondom de adoptie van passkeys en digitale wallets.

Tijdens de workshop hebben we de uitdagingen en kansen rond de implementatie van passkeys en digitale wallets binnen organisaties verkend. Hierbij werd ook aangegeven dat het verschil in toepassingen voor intern gebruik (voor medewerkers binnen de organisatie) en extern gebruik (voor klanten) verder moet worden onderzocht. Na de workshop hebben we 3 interviews gehouden met een Fraud & CIAM-expert (gespecialiseerd in het voorkomen van fraude en het beheren van klantidentiteiten en toegangsrechten), een IAM-projectmanager (verantwoordelijk voor de uitvoering van IAM-implementaties) en een productmanager IAM (die zorgt voor de ontwikkeling en levering van IAM-oplossingen) om verdere diepgang en praktijkinzichten te verkrijgen.

In dit hoofdstuk worden de opzet van de workshop, de belangrijkste inzichten uit de discussies, de inzichten uit de interviews, en de aanbevelingen voor adoptie en implementatie van deze technologieën besproken.

5.1 Methode workshop

De workshop was gericht op het verzamelen van concrete aanbevelingen om de adoptie van passkeys en digitale wallets in verschillende sectoren te bevorderen. Hierbij werd specifiek ingegaan op de praktische uitdagingen die organisaties ervaren bij de implementatie van deze technologieën. De deelnemers kwamen uit sectoren zoals de overheid, financiële instellingen, verzekeraars en pensioenfondsen, zo werd een breed en veelzijdig perspectief gewaarborgd.

Voorafgaand aan de workshop werden de deelnemers bevraagd over hun bekendheid en ervaring met passkeys en digitale wallets, om zo een goed uitgangspunt te creëren voor de discussie. Iedereen was bekend met deze inlogmiddelen in meer of mindere mate, waarvan de technische werking tijdens de workshop nog kort werd toegelicht. Deze input, samen met de bevindingen uit de literatuurstudie (hoofdstuk 4), diende als basis voor de verdere verkenning van de uitdagingen tijdens de sessie.
Tijdens de workshop gingen de deelnemers uiteen in om in groepen te brainstormen over de kansen en obstakels van passkeys/wallets aan de hand van fictieve scenario's. Dit werd gedaan aan de hand van een poster waarop al enkele stakeholders waren genoemd. De

deelnemers hadden de kans om extra stakeholders toe te voegen die relevant waren voor de casus. De kansen en obstakels werden vervolgens geplaatst bij stakeholder op wie dit een impact heeft. Daarna werd hen gevraagd om strategieën te formuleren om de gevonden obstakels te overwinnen. Alle kansen en obstakels werden gekoppeld aan de verschillende stakeholders die er binnen een organisatie aanwezig kunnen zijn.

Het doel van de interactieve workshop was dat de deelnemers niet alleen theoretische concepten bespreken, maar ook hun ervaringen uit de praktijk gebruiken over welke factoren van invloed zijn bij het adopteren van een nieuwe inlogmethode.

5.2 Inzichten uit de discussies

5.2.1 Passkeys

De deelnemers werkten met het scenario van het fictieve SunnyTrips, een toonaangevende online reisorganisatie met meer dan 2 miljoen actieve gebruikers. SunnyTrips stond voor de uitdaging om de veiligheid van hun gebruikers te verbeteren door de invoering van passkeys, een wachtwoordloze authenticatiemethode. Dit werd ingegeven door een groeiende dreiging van phishing-aanvallen, waarbij criminelen inloggegevens van klanten stalen en frauduleuze boekingen plaatsten. Ondanks het aanbieden van tweefactorauthenticatie door SunnyTrips, had slechts 40% van de gebruikers deze geactiveerd, waardoor een groot deel van de klanten kwetsbaar bleef.

Binnen de groep was er consensus dat de CISO, IAM-architect, innovatiemanager, product owner, customer service, legal officers en het IT-bestuur belangrijke stakeholders waren voor deze use case. Daarnaast werd ook de marketing- en communicatieafdeling van het bedrijf als relevante aanvulling genoemd.

Gebruikersperspectief
De deelnemers bespraken de kansen en uitdagingen van passkeys vanuit het perspectief van de gebruiker. De belangrijkste kans is dat gebruikers, zoals externe klanten, geen wachtwoorden meer hoeven te onthouden of beroep moeten doen op een wachtwoordmanager. Dit kan de de ‘seamless customer experience’ aanzienlijk verbeteren. Dit zou vooral aantrekkelijk zijn voor gebruikers die gemak en veiligheid belangrijk vinden. Daarnaast komt het veel voor dat gebruikers wachtwoorden vergeten, waardoor er voor organisaties tijd zit in het opnieuw uitreiken van de credentials. Door het gebruik van passkeys verwachtten meerdere deelnemers een kostenbesparing doordat dit minder nodig zou zijn.

Aan de andere kant waren er zorgen over hoe de implementatie aan de gebruikerskant eruit komt te zien. Hoewel gebruikers geen wachtwoorden meer hoeven te onthouden, is het een nieuwe techniek die niet iedereen zal begrijpen. Dit kan leiden tot vragen of problemen, zoals het kwijtraken van passkeys. Als concreet voorbeeld werd genoemd dat bedrijven mogelijk meer vragen zullen ontvangen van klanten die hun passkeys zijn kwijtgeraakt, wat de druk op klantenservice zou kunnen vergroten. Daarom werd benadrukt dat goede communicatie met gebruikers essentieel is, bijvoorbeeld via video's of een gebruiksvriendelijke UI, die hen stap voor stap door het proces leidt.

Uit de interviews kwam verder naar voren dat dit nog meer geldt voor leveranciers van essentiële diensten, zoals de financiële sector of overheid, waarbij het noodzakelijk is dat *alle* gebruikers met de nieuwe techniek overweg kunnen. Hierbij is ook sprake van een ‘first-mover disadvantage’, waarbij organisaties terughoudend zijn om als eerste over te stappen naar

nieuwe technologieën, uit angst voor potentiële gebruikersproblemen of het risico dat ze voorlopen op de bredere acceptatie. Een deelnemer gaf aan dat ze waarschijnlijk zullen wachten tot meer partijen passkeys hebben geadopteerd en gebruikers daardoor al bekend zijn met de nieuwe inlogmethode.

Organisatorisch perspectief

Vanuit een organisatorisch perspectief richten de obstakels zich vooral op het implementatieproces. Veel bedrijven maken gebruik van derde partijen voor het leveren van IAM-diensten. Voor de overstap naar passkeys is het belangrijk dat deze leveranciers de technologie als dienst gaan aanbieden. Totdat dat gebeurt, blijft de drempel voor adoptie hoog, omdat bedrijven afhankelijk zijn van hun leveranciers om met passkeys aan de slag te gaan. Aan de andere kant kan het ook tot bredere adoptie leiden, wanneer leveranciers actief inloggen met passkeys in hun portfolio opnemen.

Bovendien zullen de kosten in het begin waarschijnlijk hoger zijn. Er is binnen organisaties nog geen wijdverspreide kennis over passkeys, waardoor het tijd en middelen kost om medewerkers te trainen en bekend te maken met de nieuwe technologie. Dit vraagt om capaciteitsinvesteringen die pas worden vrijgemaakt wanneer het belang van de transitie duidelijk wordt erkend door de organisatie. Daarnaast werd tijdens de workshop het belang benadrukt van het intern agenderen van passkeys. Door dit onderwerp intern op de agenda te zetten, kan er binnen bedrijven meer aandacht en kennis over de technologie ontstaan.

Naast deze organisatorische uitdagingen werd tijdens de workshop ook benoemd dat de invoering van passkeys invloed kan hebben op het primaire proces. Innovaties zoals passkeys kunnen in eerste instantie extra werklast opleveren voor uitvoerend personeel, bijvoorbeeld in de klantenservice of IT-support, waar meer vragen kunnen ontstaan over het instellen en beheren van passkeys. Dit kan leiden tot weerstand, vooral als de voordelen voor interne gebruikers niet direct duidelijk zijn of als zij niet voldoende worden ondersteund bij de overgang. In sommige gevallen kan dit ertoe leiden dat bedrijven aarzelen om de technologie te implementeren, tenzij er voldoende draagvlak en interne ondersteuning is.

Tot slot gaven meerdere deelnemers in de workshop maar ook in het interview aan dat het thema binnen hun organisatie simpelweg geen prioriteit heeft. Rondom informatiebeveiliging worden andere thema's als belangrijker gezien of men ziet het inlogproces op dit moment niet als een probleem.

Technisch perspectief

Vanuit technisch oogpunt biedt de introductie van passkeys voornamelijk kansen op het gebied van veiligheid. Binnen de groep waren wel verschillende meningen over welk level of assurance wordt behaald met passkeys, wat verwijst naar het niveau van zekerheid dat een systeem biedt over de identiteit van een gebruiker bij authenticatie, variërend van lage tot hoge zekerheid. Voor sommigen zouden passkeys een vervanging zijn van wachtwoorden, anderen waren alleen bereid het te gebruiken als tweede factor. Hierbij speelt onbekendheid met de techniek ook een rol. Eén deelnemer gaf aan dat sommige implementaties van de BIO specifiek het gebruik van wachtwoorden voorschrijven, wat de overstap naar passkeys onmogelijk maakt. Om dit probleem aan te pakken, zouden standaarden en regelgeving aangepast kunnen worden om duidelijker te maken voor welke authenticatieniveaus passkeys geschikt zijn. Hierdoor zouden bedrijven meer vertrouwen kunnen krijgen in de geschiktheid van passkeys voor verschillende use cases.

Daarnaast moet er ook aan technische voorwaarden worden voldaan om de transitie soepel te laten verlopen. Zo moeten IAM-leveranciers de passkey-functionaliteit gaan ondersteunen,

anders blijven bedrijven vastzitten in hun bestaande systemen. Dit werd door de deelnemers echter wel als een oplosbaar probleem beschouwd.

5.2.2 Digital wallets

De deelnemers werkten met het scenario van de fictieve GlobalBank, een van de grootste banken in Nederland met meer dan 2 miljoen klanten. GlobalBank stond voor de uitdaging om de veiligheid van klantauthenticatie te versterken door de implementatie van een digital wallet. Dit werd ingegeven door een toenemende dreiging van frauduleuze toegang tot bankrekeningen en identiteitsfraude, vooral onder jongere klanten die het slachtoffer werden van een nieuwe phishingmethode op sociale media. Daarnaast was er de druk van Europese regelgeving die vroeg om strengere authenticatieprotocollen.

De deelnemers identificeerden verschillende belangrijke stakeholders die betrokken zouden moeten worden in het besluitvormingsproces rond de implementatie van de digital wallet. Dit omvatte onder andere de privacy officers, die verantwoordelijk zijn voor de naleving van regelgeving met betrekking tot klantgegevens. Ook de CISO speelde een cruciale rol, aangezien zij mede- verantwoordelijk zijn voor de beveiligingsaspecten van de bank en de naleving van compliance-eisen. Andere belangrijke groepen waren product owners en product managers, die de business case voor de implementatie zouden moeten ondersteunen. Juristen en risicomanagers waren eveneens belangrijke stakeholders, vooral in gevallen waar niet wordt voldaan aan de veiligheidsnormen, en uiteraard de klanten zelf, wiens acceptatie essentieel is voor het succes van de digital wallet.

Gebruikersperspectief

De digital wallet biedt kansen om de klantbeleving te verbeteren, met name door de stroomlijning van authenticatieprocessen. Dit kan resulteren in een naadloze onboarding, wat de gebruikerservaring positief beïnvloedt. Daarnaast kan de digital wallet bijdragen aan een hogere veiligheid van klantgegevens, wat niet alleen het vertrouwen van klanten versterkt, maar ook fraude helpt verminderen.

Toch werd er getwijfeld aan de mate waarin klanten, vooral met beperkte digitale vaardigheden, de digital wallet daadwerkelijk zouden omarmen. Deelnemers gaven aan dat oudere gebruikers mogelijk moeite hebben met de vereiste digitale vaardigheden om met deze technologie om te gaan, wat een belemmering kan vormen voor brede adoptie.

Organisatorisch perspectief

Vanuit organisatorisch perspectief zagen de deelnemers een belangrijke kans in het naleven van Europese regelgeving met behulp van digital wallets. Dit is voor veel organisaties een belangrijke drijfveer voor innovatie. Daarnaast kan de digital wallet organisaties helpen om hun klantprocessen te verbeteren door authenticatie te stroomlijnen en beveiliging te verhogen, wat uiteindelijk zou bijdragen aan efficiëntere processen en minder fraude. Voor interne authenticatie werd ook opgemerkt dat wallets kunnen worden gebruikt om fragmentatie tegen te gaan. Binnen de overheid hebben veel organisaties eigen HR-afdelingen die als bron van identiteiten worden gezien. Een wallet kan helpen om gemakkelijker tussen verschillende organisaties een identiteit en attributen aan te tonen, zonder dubbele informatie op te hoeven slaan. Ook biedt dit mogelijkheden om specifiekere toegangsregels in te stellen voor informatie. Dit vereist wel een onderling vertrouwen tussen de organisaties, iets wat nu nog niet altijd aanwezig is.

Echter, de adoptie van de digital wallet brengt ook uitdagingen met zich mee. Deelnemers gaven aan dat innovatie vaak wordt gedreven door compliance in plaats van security, wat een

verschil kan maken in de prioritering van digital wallet-projecten. Het overtuigen van interne stakeholders, zoals juridische teams en risicomanagementafdelingen, werd gezien als een belangrijke hindernis. Een deelnemer gaf ook aan dat dit komt omdat binnen de organisatie maar weinig mensen zich met het thema IAM bezig houden. Daarnaast is de onzekerheid over hoeveel klanten daadwerkelijk gebruik zouden maken van de digital wallet een punt van zorg voor organisaties. Hierbij werd het belangrijk gevonden dat de wallet niet ergens intern wordt ontwikkeld, maar juist in contact met de gebruikers: door veel te testen en open te staan voor input van buiten wordt de kans op een succesvolle lancering van wallets vergroot.

Technisch perspectief
Technisch gezien werd de digital wallet als een kans gezien om de authenticatieprocessen te stroomlijnen en de integratie met bestaande systemen te verbeteren. Deelnemers benadrukten dat de digital wallet makkelijker kan worden geïntegreerd wanneer deze onderdeel uitmaakt van bestaande SAAS W/CIAM-platformen, zoals OneWelcome van Thales. Deze integratie zou de overstap voor bedrijven naar digital wallets vereenvoudigen.

Toch blijft de integratie in bestaande systemen een belangrijke technische uitdaging. Het kost tijd en moeite om de digital wallet te implementeren en deze aan te sluiten op bestaande processen binnen de organisatie. Om deze uitdagingen te overwinnen, werd ook samenwerking met de overheid als mogelijke route genoemd. De overheid zou door middel van een breed uitrolprogramma kunnen zorgen dat burgers een digital wallet krijgen, waardoor organisaties minder moeite hebben met de invoering. Ten slotte werd gesteld dat de kosten voor de implementatie waarschijnlijk geen groot probleem zouden vormen, omdat een goede identificatie en authenticatie zichzelf terugbetaalt in betere processen en minder fraude.

5.3 Conclusies uit de praktijk

Uit de praktijkervaringen met passkeys en digital wallets blijkt dat hoewel beide technologieën aanzienlijke voordelen bieden op het gebied van beveiliging en gebruiksgemak, de daadwerkelijke implementatie wordt bemoeilijkt door verschillende factoren.

Voor passkeys geldt dat de grootste kans ligt in het verbeteren van de gebruikerservaring en het reduceren van wachtwoordgerelateerde problemen. Dit kan leiden tot kostenbesparingen en verhoogde veiligheid. Echter, obstakels zoals onbekendheid bij gebruikers, de afhankelijkheid van leveranciers en de organisatorische inspanning om de technologie te implementeren, zorgen ervoor dat bedrijven afwachtend blijven. Daarnaast speelt het ontbreken van een directe prioriteit binnen organisaties een grote rol in de langzame adoptie: het probleem wordt niet als urgent genoeg gezien.

Bij digital wallets is de kans vooral gelegen in het verhogen van de veiligheid en compliance met regelgeving, terwijl het ook mogelijkheden biedt om authenticatieprocessen te stroomlijnen. Tegelijkertijd zijn er uitdagingen op het gebied van gebruikersacceptatie, met name onder oudere gebruikers, en organisatorische prioritering. De adoptie wordt vaak gedreven door compliance in plaats van security, wat betekent dat innovatie niet altijd vanuit een strategisch perspectief wordt benaderd. Daarnaast is de onzekerheid over de daadwerkelijke gebruikersacceptatie een remmende factor.

De overeenkomsten tussen beide technologieën liggen voornamelijk in de noodzaak van bredere adoptie voordat bedrijven en gebruikers de overstap durven te maken. Organisaties willen vaak niet als eerste de sprong wagen, waardoor een ‘first-mover disadvantage’ ontstaat. Bovendien vereisen beide technologieën een nauwe samenwerking tussen

verschillende stakeholders binnen een organisatie en een duidelijke communicatie richting de eindgebruikers.

De onderstaande tabellen (Tabel 6.1 en Tabel 6.2) bieden een overzicht van de inzichten uit de literatuur over de adoptie van passkeys en digital wallets, aangevuld met praktijkervaringen uit de workshops en interviews:

Tabel 5.1: Passkeys vergelijking literatuur en praktijk

Perspectief	overeenkomsten	aanvullingen
Gebruikers	- Onzekerheid over accountherstel bij verlies van passkeys. - Verwarring over wachtwoordloze authenticatie en biometrische gegevens.	- Klantenservice krijgt meer vragen bij verlies van passkeys. - Goede communicatie (zoals video's en UI-verbeteringen) is cruciaal voor acceptatie. - Accountherstel mogelijk minder vaak nodig.
Organisatorisch	- Afhankelijkheid van leveranciers voor implementatie. - Hoge kosten voor infrastructuuraanpassingen.	- Interne agendering binnen organisaties is essentieel voor adoptie. - Gebrek aan interne kennis en urgentie vertraagt de transitie. - First mover disadvantage.
Technisch	- Compatibiliteitsproblemen met legacy-systemen. – Beperkte ondersteuning door browsers.	- Regelgeving kan adoptie bemoeilijken als authenticatiestandaarden niet worden aangepast.

Tabel 5.2: Digital identity wallets vergelijking literatuur en praktijk

Perspectief	overeenkomsten	aanvullingen
Gebruikers	- Onzekerheid over wie controle heeft over gegevens. - Gebrek aan vertrouwen in derde partijen.	- Oudere gebruikers kunnen moeite hebben met adoptie vanwege beperkte digitale vaardigheden.
Organisatorisch	- Compliance en regelgeving als drijfveren. - Angst voor monopolievorming en interactiebarrières.	- Adoptie wordt vaak gestuurd door compliance in plaats van security. - Interne weerstand bij juridische en risicomanagementteams belemmert implementatie. - Wallets kunnen fragmentatie van identiteiten tegengaan.
Technisch	- Onzekerheid over technische implementatie. - Weinig ervaring met implementatie leidt tot terughoudendheid.	- Integratie in bestaande SAAS W/CIAM-platformen zoals OneWelcome kan adoptie vergemakkelijken. - Samenwerking tussen de overheid en publieke/private sector kan adoptie stimuleren door grootschalige uitrol en goede aansluiting bij behoeften.

6 Conclusie

In dit onderzoek hebben we de adoptie van passkeys en digitale identity wallets als wachtwoordloze authenticatiemiddelen onderzocht. De adoptie van passkeys en digital identity wallets als wachtwoordloze authenticatiemiddelen biedt aanzienlijke voordelen op het gebied van beveiliging, gebruiksgemak en compliance met regelgeving. Toch blijft brede implementatie uit, door zowel technische als organisatorische barrières en uitdagingen op gebruikersniveau.

Voor passkeys ligt de grootste uitdaging bij de onbekendheid en misverstanden onder gebruikers. Hoewel passkeys phishing-resistente authenticatie mogelijk maken en de afhankelijkheid van wachtwoorden elimineren, blijft onzekerheid bestaan over accountherstel bij verlies van een passkey. Organisaties ervaren bovendien hindernissen op het gebied van infrastructuurintegratie, kosten en het ontbreken van een duidelijke urgentie om over te stappen.

Voor digital identity wallets speelt een vergelijkbaar spanningsveld. Hoewel wallets mogelijkheden bieden voor self-sovereign identity en privacy-vriendelijke authenticatie, is de adoptie en literatuur hierover nog beperkt. Technische standaardisatie en interoperabiliteit tussen systemen vormen uitdagingen, terwijl onzekerheid over de controle over persoonlijke gegevens de gebruikersacceptatie vertraagt. Organisaties implementeren wallets voornamelijk vanuit een compliance-oogpunt, maar er blijft terughoudendheid over de toegevoegde waarde en praktische uitvoerbaarheid.

Beide technologieën delen de uitdaging van een ‘first-mover disadvantage’: veel organisaties en gebruikers wachten af totdat bredere adoptie plaatsvindt, wat de overgang vertraagt. Duidelijke communicatie over de voordelen, betere ondersteuning bij implementatie en verdere standaardisatie zijn nodig om de adoptie te versnellen.

Om de overstap naar wachtwoordloze authenticatie te bevorderen, is samenwerking tussen technologieaanbieders, beleidsmakers en gebruikers essentieel. Alleen door gezamenlijke inspanningen kunnen passkeys en digital identity wallets hun potentieel volledig benutten als veilige en efficiënte alternatieven voor traditionele wachtwoorden.

6.1 Aanbevelingen voor vervolgonderzoek

Op basis van de literatuurstudie en de inzichten uit de interviews en workshops zijn er verschillende open vragen die nader onderzoek vereisen om de adoptie van passkeys en digital identity wallets beter te begrijpen en te ondersteunen.

6.1.1 Verschil tussen interne en externe adoptie

In zowel de literatuur als de praktijk blijkt dat er onvoldoende onderscheid wordt gemaakt tussen het gebruik van passkeys en digital identity wallets voor interne medewerkersauthenticatie versus externe klantauthenticatie. De eerste exploratie in de interviews laat zien dat verschillende barrières en kansen een rol spelen, afhankelijk van de

doelgroep en de context. Vervolgonderzoek kan zich richten op de vraag in hoeverre organisaties verschillende adoptiestrategieën moeten hanteren voor intern en extern gebruik, en hoe deze strategieën geoptimaliseerd kunnen worden.

6.1.2 De impact van digital identity wallets op de adoptie van passkeys

Een belangrijke vraag die in de praktijk nog niet goed beantwoord is, is in hoeverre digital identity wallets en passkeys interfererende technologieën zijn. Het kan zijn dat bedrijven wachten met de implementatie van de technisch meer volwassen passkeys vanwege de beloftevolle maar in ontwikkeling zijnde wallets (vlucht naar voren). Er is behoefte aan meer onderzoek naar hoe de invoering van wallets de implementatie en adoptie van passkeys beïnvloedt. Dit kan helpen om te bepalen of de twee technologieën verschillende markten bedienen, of dat wallets de rol van passkeys als authenticatiemiddel (gedeeltelijk) overnemen.

6.1.3 Adoptiedrempels en schaalvoordelen

Zowel passkeys als digital identity wallets kampen met een 'first-mover disadvantage', waarbij bedrijven en gebruikers aarzelen om over te stappen zolang brede adoptie uitblijft. Een beter begrip van de schaalvoordelen en kritische massa die nodig is voor versnelling in adoptie kan helpen om gerichtere implementatiestrategieën te ontwikkelen. Hierbij kan specifiek worden gekeken naar hoe early adopters en overheidsinitiatieven de markt kunnen beïnvloeden.

6.1.4 Gebruikerservaring en herstelprocessen

Voor beide technologieën speelt gebruikerservaring een cruciale rol bij adoptie. Onzekerheid over accountherstel, gebrek aan kennis en weerstand tegen verandering vormen belangrijke obstakels. Vervolgonderzoek kan zich richten op hoe gebruiksvriendelijke herstelprocessen en betere communicatie de acceptatie kunnen bevorderen.

6.1.5 Effectieve communicatievormen richting eindgebruikers

Een belangrijk aspect van adoptie is het informeren en geruststellen van eindgebruikers. Vervolgonderzoek kan zich richten op welke communicatievormen effectief zijn in het voorkomen van misverstanden over de werking van passkeys en digital identity wallets. Hoe kan bijvoorbeeld het herstelproces duidelijker worden uitgelegd, zodat gebruikers vertrouwen krijgen in het systeem? Welke kanalen en methodes zijn het meest effectief om gebruikers gerust te stellen over het gebruik en de veiligheid van deze technologieën?

6.1.6 Kosten versus baten voor organisaties en gebruikers

Een cruciale vraag voor zowel organisaties als gebruikers is of de overstap naar passkeys en digital identity wallets de kosten waard is. Vervolgonderzoek kan zich richten op het identificeren van de specifieke kosten- en batenstructuren van deze technologieën. Wat zijn de initiële kosten van implementatie versus de langetermijnvoordelen op het gebied van beveiliging, gebruiksvriendelijkheid en compliance? Hoe wegen de kosten van training, systeemintegratie en onderhoud op tegen de voordelen van verbeterde veiligheid, lagere

beheerskosten en verhoogd gebruiksgemak? Het begrijpen van deze balans kan organisaties helpen te bepalen of en wanneer het economisch verantwoord is om over te stappen op deze nieuwe technologieën.

Referenties

1. Thakur, M.A. and R. Gaikwad. *User identity and access management trends in IT infrastructure-an overview.* in *2015 International Conference on Pervasive Computing (ICPC).* 2015. IEEE.
2. Schlackl, F., N. Link, and H. Hoehle, *Antecedents and consequences of data breaches: A systematic review.* Information & Management, 2022. **59**(4): p. 103638.
3. *Rapportage Datalekken 2023.* 2024, Autoriteit Persoonsgegevens.
4. Gupta, S., A. Singhal, and A. Kapoor. *A literature survey on social engineering attacks: Phishing attack.* in *2016 international conference on computing, communication and automation (ICCCA).* 2016. IEEE.
5. Deepen Desai and R. Hegde, *Phishing Attacks Rise: ThreatLabz 2024 Phishing Report.* 2024.
6. O'Gorman, L., *Comparing passwords, tokens, and biometrics for user authentication.* Proceedings of the IEEE, 2003. **91**(12): p. 2021-2040.
7. Morris, R. and K. Thompson, *Password security: A case history.* Communications of the ACM, 1979. **22**(11): p. 594-597.
8. Bošnjak, L., J. Sreš, and B. Brumen. *Brute-force and dictionary attack on hashed real-world passwords.* in *2018 41st international convention on information and communication technology, electronics and microelectronics (mipro).* 2018. IEEE.
9. Cram, W.A., J.G. Proudfoot, and J. D'Arcy, *When enough is enough: Investigating the antecedents and consequences of information security fatigue.* Information Systems Journal, 2021. **31**(4): p. 521-549.
10. Bonneau, J., C. Herley, P.C. Van Oorschot, and F. Stajano. *The quest to replace passwords: A framework for comparative evaluation of web authentication schemes.* in *2012 IEEE symposium on security and privacy.* 2012. IEEE.
11. George, A.S., *The Dawn of Passkeys: Evaluating a Passwordless Future.* Partners Universal Innovative Research Publication, 2024. **2**(1): p. 202-220.
12. Sedlmeir, J., R. Smethurst, A. Rieger, and G. Fridgen, *Digital identities and verifiable credentials.* Business & Information Systems Engineering, 2021. **63**(5): p. 603-613.
13. Dupré, D. *Veilig inloggen zonder wachtwoord met FIDO2 security keys.* 2020; Available from: https://www.ct.nl/achtergrond/veilig-inloggen-zonder-wachtwoord-fido2/.
14. Porter, J. *The web just took a big step toward a password-free future.* 2019; Available from: https://www.theverge.com/2019/3/4/18249895/web-authentication-webauthn-world-wide-web-consortium-w3c-standard-browsers.
15. Podgorelec, B., L. Alber, and T. Zefferer. *What is a (digital) identity wallet? a systematic literature review.* in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC).* 2022. IEEE.
16. Beer, E. *FIDO2 is touted as a security panacea: Why isn't it everywhere?* 2022 [cited 2024.
17. Lassak, L., E. Pan, B. Ur, and M. Golla, *Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication.* 2024.
18. Hall, B.H. and B. Khan, *Adoption of new technology.* 2003, National bureau of economic research Cambridge, Mass., USA.
19. FIDO. *Alliance overview.* Available from: https://fidoalliance.org/overview/.
20. FIDO, *Client to Authenticator Protocol (CTAP).* 2018.
21. Guan, J., H. Li, H. Ye, and Z. Zhao. *A formal analysis of the FIDO2 protocols.* in *European Symposium on Research in Computer Security.* 2022. Springer.

22. FIDO. *Specifications Overview*. Available from: https://fidoalliance.org/specifications-overview/.
23. Stafford, V., *Zero trust architecture*. NIST special publication, 2020. **800**: p. 207.
24. Kunke, J., S. Wiefling, M. Ullmann, and L.L. Iacono, *Evaluation of account recovery strategies with FIDO2-based passwordless authentication*. arXiv preprint arXiv:2105.12477, 2021.
25. Ulqinaku, E., et al. *Is real-time phishing eliminated with {FIDO}? social engineering downgrade attacks against {FIDO} protocols*. in *30th USENIX Security Symposium (USENIX Security 21)*. 2021.
26. Apple, *Apple, Google en Microsoft gaan FIDO-standaard voor inloggen zonder wachtwoord verder doorvoeren*. 2022.
27. Google. *Passwordless login with passkeys*. 2024 27/11/2024]; Available from: https://developers.google.com/identity/passkeys.
28. Apple. *Passkeys Overview*. 2024 27/11/2024]; Available from: https://developer.apple.com/passkeys/.
29. 1Password. *Passkeys in 1Password*. 2024 27/11/2024]; Available from: https://1password.com/product/passkeys.
30. *EU Digital Identity Wallet Home*. 2024 [cited 2024 9-8]; Available from: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home.
31. TNO. *Self-sovereign identity: eenvoudig en veilig digitaal leven*. Available from: https://www.tno.nl/nl/technologie-wetenschap/technologieen/self-sovereign-identity/.
32. Connect, D., *The European Digital Identity Wallet Architecture and Reference Framework*. 2023.
33. Lyastani, S.G., et al. *Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication*. in *2020 IEEE Symposium on Security and Privacy (SP)*. 2020. IEEE.
34. Lassak, L., A. Hildebrandt, M. Golla, and B. Ur. *" It's Stored, Hopefully, on an Encrypted Server'': Mitigating Users' Misconceptions About {FIDO2} Biometric {WebAuthn}*. in *30th USENIX Security Symposium (USENIX Security 21)*. 2021.
35. Farke, F.M., et al. *{"You} still use the password after {all"}–Exploring {FIDO2} Security Keys in a Small Company*. in *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 2020.
36. Korir, M., S. Parkin, and P. Dunphy. *An empirical study of a decentralized identity wallet: Usability, security, and perspectives on user control*. in *Eighteenth symposium on usable privacy and security (SOUPS 2022)*. 2022.
37. Lukkien, B., N. Bharosa, and M. De Reuver. *Barriers for developing and launching digital identity wallets*. in *Proceedings of the 24th Annual International Conference on Digital Government Research*. 2023.
38. Alam, A., K. Krombholz, and S. Bugiel. *Poster: Let History not Repeat Itself (this Time)--Tackling WebAuthn Developer Issues Early On*. in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019.
39. Bicakci, K. and Y. Uzunay. *Is FIDO2 passwordless authentication a hype or for real?: A position paper*. in *2022 15th International Conference on Information Security and Cryptography (ISCTURKEY)*. 2022. IEEE.
40. Casey, M., et al. *An interoperable architecture for usable password-less authentication*. in *Emerging Technologies for Authorization and Authentication: Third International Workshop, ETAA 2020, Guildford, UK, September 18, 2020, Proceedings 3*. 2020. Springer.

Bijlage A: Technisch overzicht passkeys

A.1 FIDO2 Passkeys

In deze bijlage gaan we dieper in op de techniek achter passkeys. Passkeys zijn een techniek die gepubliceerd is door de FIDO Alliance. De FIDO Alliance heeft drie verschillende protocollen gepubliceerd:

- FIDO Universal Second Factor (FIDO 2UF): een protocol dat bedoeld is voor twee factor authenticatie, naast een primaire vorm van authenticatie (bijvoorbeeld een wachtwoord).
- FIDO Universal Authentication Framework (FIDO UAF): een protocol voor wachtwoordloos inloggen op apparaten met de UAF stack.
- Client To Authenticator Protocol (CTAP): een protocol voor het gebruik van externe authenticators (via USB, NFC, BLE).

Om de functionaliteiten van de FIDO 2UF en UAF samen te voegen, is een nieuw protocol ontwikkeld, dat FIDO2 wordt genoemd. Dit protocol bestaat uit twee onderdelen: het CTAP2 protocol en het Web Authentication (webAuthn) protocol. In deze bijlage focusen we op FIDO2 en gaan we dieper in op beide protocollen.

A.1.1 WebAuthn

Het W3C WebAuthn protocol is verantwoordelijk voor de communicatie tussen de client, de authenticator en de relying party (dat is, de partij bij wie een gebruiker zich wil authentiseren). Het beschrijft hoe public-key crpytography gebruikt kan worden voor het aanmaken en gebruiken van credentials en is bedoeld voor strong user authentication.
WebAuthn is te groot om hier volledig te beschrijven, dus daarom wordt hier gefocust op de belangrijkste onderdelen.

A.1.1.1 Attestation

Met behulp van attestaties is kan de server het gebruik van bepaalde type authenticators afdwingen. Dit kan bijvoorbeeld nuttig zijn in een werkomgeving, waarin de werkgever wil dat de werknemers authenticators met een bepaald veiligheidsniveau gebruiken. Ook kunnen hier public-key infrastructures worden gebruikt, zodat men weet dat de authenticator door een bepaalde organisatie is uitgegeven. Tot slot kan ook worden gevraag om attestaties op indiviueel niveau: hiermee kan een bepaalde authenticator aan een specifiek account bij de relaying party worden gekoppeld. Bijvoorbeeld kan een werkgever controleren of een medewerker inlogt met de authenticator die door het bedrijf aan die specifieke medewerker is uitgegeven. Uniek identificeerbare informatie wordt alleen uitgegeven aan partijen die de gebruiker hiervoor heeft geselecteerd.
Daarnaast kan een relying party ook eisen dat een externe authenticator (roaming authenticator of cross-plaform authenticator) wordt gebruikt, of juist een authenticator op de computer zelf (platform authenticator).
Merk dus op dat een attestatie per type authenticator uniek is. Dus bijvoorbeeld alle YubiKey4 modellen hebben dezelfde attestatiesleutel. Deze worden bij productie al op de authenticator gezet. Bij de Apple KeyChain is het bijvoorbeeld mogelijk om via attestaties af te dwingen dat alleen gemanagede telefoons als authenticator gebruikt kunnen worden.

A.1.1.2 Discoverable credentials

Voor authenticatie zijn er twee mogelijkheden. De eerste optie is dat de gebruiker zich bekend maakt zich bij de relying party, en vervolgens zoekt de relying party op welke passkey bij deze gebruiker hoort. Vervolgens vraagt de relying party specifiek deze passkey op. Dit proces werkt voor elk type passkey.
Een andere optie is dat de relying party de gebruiker vraagt de passkey op te zoeken. In dat geval gaat de gebruiker op basis van de URL op zoek naar passkeys die voor die party zijn geregistreerd. De passkeys die op basis van de URL van de relying party te vinden zijn, heten *discoverable credentials*. Per credential kan worden aangegeven of deze discoverable is of niet.

A.1.1.3 Registratie van een nieuwe passkey

Het proces van registratie staat op hoofdlijnen beschreven in de tekst. Hieronder wordt het in iets meer detail uitgewerkt. Voor een overzicht van alle mogelijk opties die de partijen aan elkaar mee kunnen geven wordt verwezen naar de W3C Recommendation.

1. De relying party genereert een random string van minstens 128 bit en een user identifier van 512 bit. Deze twee waardes worden samen met de identiteit van de server naar de client gestuurd. Merk op dat dit proces vrijwel altijd plaats vind wanneer er al een beveiligde verbinding is tussen de client en de server.
2. De gebruiker controleert de identiteit van de server . Vervolgens stuurt het een hash van random string samen met de ontvangen user id en de server id naar de authenticator.
3. Op de authenticator wordt een nieuw sleutelpaar aangemaakt (RSA of Elleptic Curve). Tevens wordt er een teller geïnitialiseerd die bij gaat houden hoe vaak deze passkey is gebruikt. Tot slot wordt er ook een credential id van minimaal 128 bits aangemaakt. De publieke sleutel, een hash van de server identiteit, de hash van de challenge en de credential id worden samengenomen in een bericht. Als er gevraagd is om een attestatie, wordt dit bericht ondertekend met de attestatiesleutel van de authenticator. Dit wordt vervolgens verzonden naar de relying party.
4. De relying party controleert allereerst of de attestatie handtekening op het bericht klopt. Vervolgens wordt gecontroleerd of alle overige waardes overeenkomen met de verwachting. Als dit het geval is, registreert de relying party de id's en de publieke sleutel in een database voor toekomstig gebruik.
5. De gebruiker registreert ook de nieuwe passkey (de id's, privésleutel en de teller) in een database voor toekomstig gebruik.

A.1.1.4 Authenticatie

Het proces van authenticatie ziet er als volgt uit:

1. De relying party genereert een random string van minsten 128 bit als *challenge*. Deze waarde wordt samen met de identiteit van de server naar de client gestuurd. Optioneel kunnen hier eisen met betrekking tot discoverable credentials worden toegevoegd.
2. De gebruiker controleert weer de identiteit van de server en stuurt deze samen met een hash van de challenge door naar de authenticator.
3. Op basis van de server of het credential id wordt in de authenticator de bijbehorende sleutel opgezocht. De teller wordt opgehoogd. Er wordt een bericht gemaakt bestaande uit de hash van de server id, de teller en de hash van de challange. Dit bericht wordt vervolgens ondertekend met de privésleutel en naar de relying party gestuurd.
4. De relying party controleert de handtekening en de inhoud van het bericht. Als alles klopt, wordt de gebruiker ingelogd. De nieuwe teller wordt opgeslagen in de database.
5. In de authenticator wordt ook de nieuwe teller opgeslagen in de database.

A.1.2 Client-To-Authenticator Protocol

Het CTAP2 protocol is een complex protocol dat zorgdraagt voor een veilige en efficiënte verbinding tussen de client, de authenticator en de gebruiker. Het zorgt er onder andere voor dat de informatie van de gebruiker (bijvoorbeeld PIN) niet onversleuteld wordt verstuurd tussen de host en de authenticator. Ook beschrijft het de functies om credentials aan te maken. Hieronder worden enkele instellingen besproken die nuttig kunnen zijn in het gebruik. Voor verdere implementatie wordt verwezen naar de documentatie van de FIDO Alliance.

A.1.2.1 Always Require User Verification

De meeste authenticators vragen de gebruikers niet altijd om een actie (PIN, vingerafdruk etc.), maar alleen wanneer deze opnieuw wordt opgestart. Met de optie ‘always_uv’ is het mogelijk om af te dwingen dat er altijd om een actie van de gebruiker wordt gevraagd bij het gebruiken van een passkey. Deze optie is overigens ook vanuit de relying party af te dwingen.

A.1.2.2 Enterprise attestation

Voor bedrijven is het mogelijk om de attestatie op de authenticator aan te passen, zodat deze binnen het bedrijf uniek te identificeren is. Dit maakt het mogelijk om werknemers met grotere zekerheid te identificeren. Hiervoor kunnen niet standaard authenticators worden gebruikt, maar deze moeten vooraf worden geprepareerd.

A.1.2.3 Authenticator Reset

Het is mogelijk een authenticator volledig te resetten. Dit leidt ertoe dat alle passkeys die erop staan worden verwijderd en alle instellingen terug worden gezet. De meeste authenticators vragen hiervoor actieve gebruikersinput, aangezien het niet mogelijk moet zijn voor een aanvaller om een dergelijke functie op afstand te activeren.

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag
www.tno.nl

TNO innovation for life