Passkeys maken wachtwoorden overbodig

Bert van Dijk

**Wachtwoorden beheersen ons digitale leven.
Maar er is een slimme oplossing in aantocht: de passkey.
Maar wat is dat precies en hoe werkt het?**

Hackers vinden het fijn dat we vaak dezelfde wachtwoorden gebruiken. Wachtwoorden die ergens uitlekken of gemakkelijk te raden zijn, kunnen zij daardoor simpel misbruiken. Ook laten ze jou graag inloggen op nep-websites of loggen ze je toetsaanslagen via malware. Ook het onthouden en steeds weer invullen van die wachtwoorden is voor veel gebruikers vaak lastig. Met *passkeys* kunnen al die problemen opgelost worden. Apple gaat deze oplossing waarschijnlijk al rond oktober beschikbaar stellen in iOS 16, iPadOS 16, watchOS 9 en macOS Ventura. Hierbij vul je niet langer je gebruikersnaam en wachtwoord in maar volstaat een herkenning van je gezicht of vingerafdruk.

Passkeys van FIDO Alliance worden ondersteund door o.a. Apple, Google en Microsoft

Ondersteuning

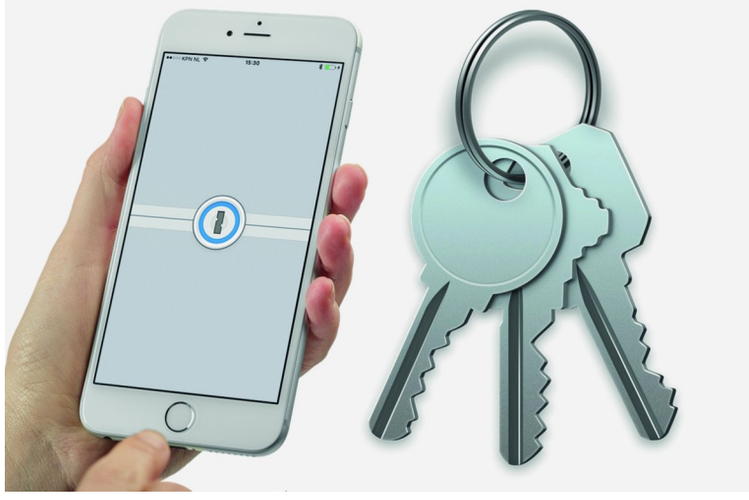
In 2021 gebruikte Apple de term *passkeys* voor het eerst op hun jaarlijkse ontwikkelaarscongres. In maart 2022 nam de FIDO Alliance (**https://fidoalliance.org**) deze nieuwe duidelijke naam over voor hun *discoverable Weauthn/Fido2*-wachtwoordvervangers die je al sinds 2018 kunt opslaan in bijvoorbeeld een YubiKey 5 usb-stick. Tegelijk maakte ze ook bekend dat je die passkeys voortaan via clouddiensten ook op meerdere apparaten kon gebruiken. In mei en juni gaven Google en Apple aan deze nieuwe techniek dit jaar al te gaan ondersteunen; Microsoft volgt waarschijnlijk iets later. Met zoveel grote spelers aan boord gaan we deze nieuwe, veilige en snelle manier van inloggen waarschijnlijk snel bij veel meer apps en websites zien dan nu bij *Inloggen met Apple* het geval is.

Voordelen passkey

Het grote voordeel van een passkey is dat je geen wachtwoorden meer hoeft te wijzigen of in te vullen. Er zijn geen wachtwoorden meer die op websites uit kunnen lekken. En omdat een passkey alleen vanaf je eigen smartphone werkt op de originele website, kunnen criminelen niet meer je inloggegevens ontfutselen met een nep-website.
Een andere leuke bijkomstigheid is dat extra controles via een code in een sms of mail niet meer nodig zijn. Ook die vervelende *captcha's* (waarbij je moeilijk leesbare letters en cijfers moet overtypen) worden helemaal overbodig. Als je inlogt via een passkey, staat immers al vast dat de juiste persoon bezig is met inloggen. Omdat alles ook heel eenvoudig werkt, is dit ook een ideale oplossing voor ouderen die moeite hebben om al die wachtwoorden te onthouden.

Omdat Apple ook watchOS 9 aanpast voor passkey, zal het mij niet verbazen als je straks ook met je Apple Watch de mogelijkheid krijgt om op al je Apple-devices nog gemakkelijker in te loggen. Als je bij het omdoen van je Apple Watch een pincode invoert, kun je nu al immers – zolang je de Apple Watch blijft dragen – zonder intoetsen van een pincode grote bedragen contactloos betalen.
Een andere toepassing is om vanuit *Instellingen* > *Wachtwoord* via Airdrop een passkey draadloos met één of meer andere gebruikers te delen. Zo kan je bijvoorbeeld gemakkelijk ook je partner laten inloggen met die passkey.

Apple biedt in de iCloud ruimte voor eindeloos veel passkeys. Daarnaast is een herstelprocedure met een 6-cijferige iCloud-beveiligingscode voor als je je iPhone kwijt raakt en je geen andere Apple-apparaten meer in gebruik hebt. Met de YubiKey usb-stick kun je op dit moment maar 25 passkeys bewaren en heb je wél een probleem als je de stick kwijtraakt. Wel ondersteunt de YubiKey usb-stick veel meer protocollen, maar is het door het complexere gebruik eigenlijk meer geschikt voor de wat meer technische gebruikers en gevoelige zakelijke toepassingen waarbij het belangrijk is dat je de passkeys niet kunt kopiëren.
Door de *end-to-end-encryptie* kunnen Apple en Google je passkeys niet zien of wijzigen. Apple en Google hebben beide ook aangegeven dat ze al werken aan een manier om passkeys over te zetten voor gebruikers die willen overstappen tussen een IPhone en Android-toestel. Ook Agilebits, de maker van de veel gebruikte 1Password-app, is van plan om passkeys te gaan ondersteunen.



In plaats van een wachtwoord bewaar je een passkey in je iCloud sleutelhanger en de website krijgt alleen een openbare sleutel

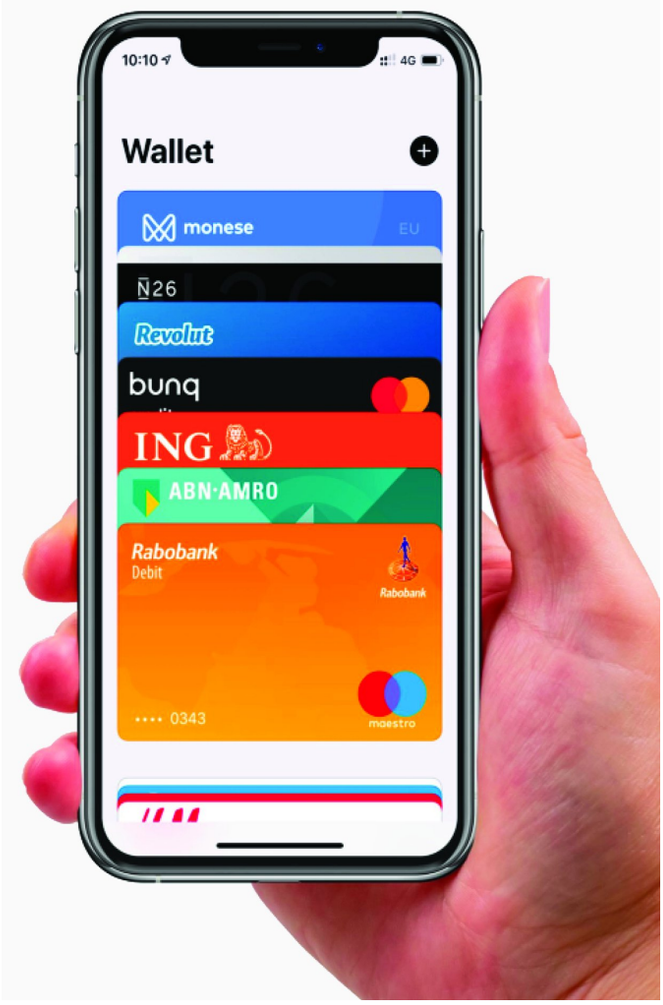
Makkelijk in gebruik

Zodra een dienst passkeys ondersteunt, kunnen ze na je inlog voorstellen om een passkey voor je aan te maken. Je hoeft

alleen te kiezen voor *Doorgaan met TouchID* (*of FaceID*) en na een herkenning van je vingerafdruk of je gezicht wordt de passkey in iCloud opgeslagen. Alleen de bijbehorende openbare sleutel wordt verzonden naar de website. Er is dus geen wachtwoord meer die kan uitlekken.
Bij een nieuwe website of app hoef je alleen een gebruikersnaam in te vullen en in een bevestigingsscherm akkoord te gaan met het opslaan van de passkey, zoals je hierboven ziet.

Als je in het vervolg kiest voor *Inloggen met passkey,* herkent je smartphone dat er voor die website al een passkey is. Zodra je die aantikt, log je direct in na een geslaagde herkenning van je vingerafdruk of gezicht.

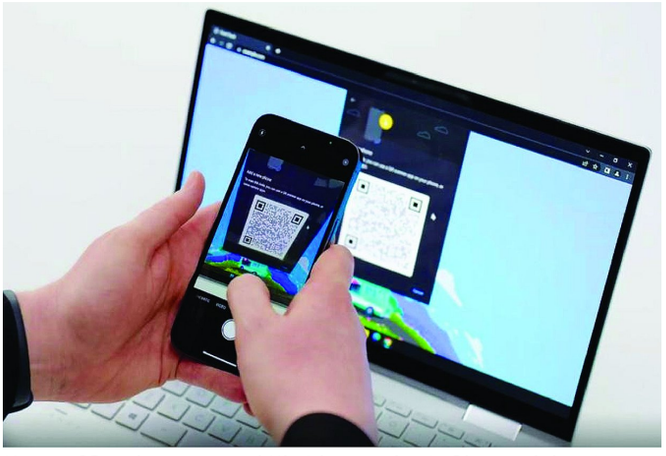
Als je niet op je eigen computer inlogt, is er geen passkey op je computer aanwezig en krijg je een keuzescherm om in te loggen met een usb-beveiligingssleutel of een passkey op je iPhone, iPad of Android-apparaat. Bij die laatste keuze verschijnt een QR-code die je kunt scannen.



Op https://apple-passkey.demo.hanko.io/ *kun je testen om via een QR-code met een passkey op een mobiel device met camera in te loggen*

Als je niet op je eigen computer inlogt, is er geen passkey op je computer aanwezig en krijg je een keuzescherm om in te loggen met een usb-beveiligingssleutel of een passkey op je iPhone, iPad of Android-apparaat. Bij die laatste keuze verschijnt een QR-code die je kunt scannen.

Heel handig is dat je zo straks via iCloud op elke computer gemakkelijk en veilig kunt inloggen bij elke app en website die passkeys ondersteunt. Ook via de wachtwoordmanager van Google's browser Chrome kun je straks passkeys gebruiken op verschillende computers.



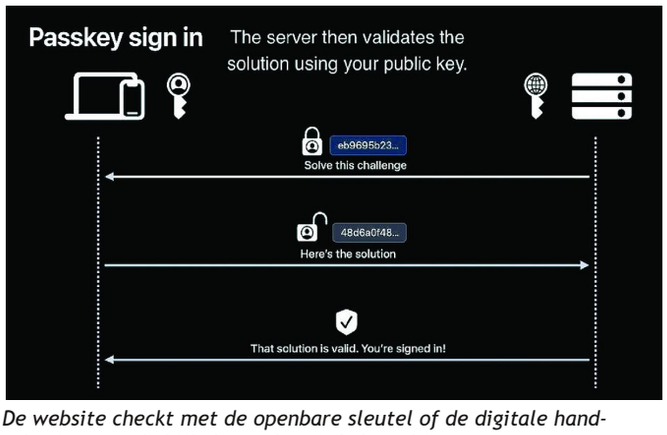
Na een QR code scan en nabijheidscontrole via Bluetooth kun je met passkeys op je iPhone ook gemakkelijk en veilig gebruik maken van websites op je computer

Dankzij het *Client To Authenticator Protocol* (CTAP) kun je je iPhone ook als *authenticator* gebruiken om veilig op je computer in te loggen in een app of website. Je scant hiervoor met je iPhone de QR-inlogcode op je computer. Deze inlog is daarna veilig via een beveiligde communicatie tussen twee *devices* die elkaar vertrouwen. Je loopt daarbij geen risico op *phishing* via een QR-code uit een e-mail of nep-website, omdat het inloggen altijd mislukt als de QR-code niet heel dichtbij je iPhone is aangemaakt. Via bluetooth wordt bij het gebruikte CTAP-protocol namelijk gecontroleerd of beide apparaten werkelijk dichtbij elkaar zijn.

De techniek

Bij een nieuwe website of app geef je eerst een gebruikersnaam door, waarna je toestel een bericht ontvangt. Met *FaceID* of *TouchID* bewijs je dat je de eigenaar bent van het toestel en worden er voor elke inlog twee sleutels aangemaakt. De geheime privésleutel wordt opgeslagen in je iCloud sleutelhanger. Hierdoor is die onleesbare passkey ook beschikbaar op je andere Apple-apparaten die gebruik maken van dezelfde Apple ID.

Als je vervolgens kiest voor inloggen met passkey, stuurt een website of app een bericht waarin het vraagt om de gebruiker van de app te verifiëren met de standaard op het apparaat aanwezige authenticatie. Als er een passkey voor die website aanwezig is in iCloud, kun je die bevestigen en met een geslaagde verificatie van je vingerafdruk of gezicht bewijs je dat je de eigenaar bent van het toestel en berekent het met de privésleutel van je passkey een digitale handtekening. Die handtekening kan de server controleren met je openbare sleutel die daar tijdens je registratie is opgeslagen. Bij een positieve uitkomst weet de service honderd procent zeker dat jij het bent en krijg je toegang tot de afgeschermde backend.



De website checkt met de openbare sleutel of de digitale handtekening met de bijbehorende privé sleutel is gezet