Web Authentication – Lösenordslös autentisering på webben

Joel Långnabba

Examensarbete

Informationsteknik

2023

Joel Långnabba

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informationsteknik
Identifikationsnummer:	8626
Författare:	Joel Långnabba
Arbetets namn:	Web Authentication – Lösenordslös autentisering på webben
Handledare (Arcada):	Dennis Biström
Uppdragsgivare:	

Sammandrag:

Det råder konsensus att lösenord är föråldrade och osäkra och 81% av hackningsrelaterade dataintrång utnyttjar svaga eller stulna lösenord, trots detta är lösenord den vanligaste autentiseringsmetoden på webben (Guirat & Halpin, 2018; Bonneau, et al., 2015; FIDO Alliance & W3C, 2019). Lösenord är svåra att minnas och är utsatta för ett antal attacker som avslöjar användares lösenord till en obehörig. FIDO Alliance har i samarbete med W3C skapat en standardiserad metod för säker autentisering på webben med målet att eliminera användningen av lösenord. Den nya metoden heter Web Authentication och utnyttjar asymmetrisk kryptering för att säkra användares konton. Detta examensarbete undersöker Web Authentication i syfte att sammanställa en introduktion till metoden som beskriver vad Web Authentication är, hur det fungerar och hur det används. En undersökning av lösenord utförs för att klarlägga brister med lösenord och för att belysa förbättringar som gör lösenord säkrare. Undersökningarna utförs genom systematiska litteraturöversikter. Web Authentication innebär att inga autentiseringsuppgifter lagras på en server och eliminerar därmed dataintrång vars mål är att stjäla lösenord. Web Authentication har även konstaterats vara resistent mot nätfiskeattacker. Bonneau et al. tog 2012 fram ett ramverk för jämförelse av olika autentiseringsmetoder (Bonneau, et al., 2012). Inga tidigare autentiseringsmetoder erbjuder enligt Bonneau et al. ramverk lika många fördelar som den nya metoden (Lyastani, et al., 2020). En nackdel med den nya metoden är dock svårigheten att återställa autentiseringsuppgiften vid förlust. Vid förlust av en autentiseringsuppgift behöver användaren ha en reservmetod för autentisering, detta kan till exempel vid användning av fysiska säkerhetsnycklar vara en reservnyckel. Efter åtkomst med en reservmetod måste användaren ta bort den förlorade autentiseringsuppgiften från kontot för att sedan registrera en ny autentiseringsuppgift. Detta behöver göras på alla konton där autentiseringsuppgiften är registrerad.

Nyckelord:	informationssäkerhet, asymmetrisk kryptering, webben, Web Authentication, säkerhetsnyckel
Sidantal:	50
Språk:	Svenska
Datum för godkännande:	

DEGREE THESIS	
Arcada	
Degree Programme:	Information Technology
Identification number:	8626
Author:	Joel Långnabba
Title:	Web Authentication – Passwordless authentication on the web
Supervisor (Arcada):	Dennis Biström
Commissioned by:	

Abstract:
There is consensus that passwords are outdated and insecure and 81% of hacking related data breaches leverage weak or stolen password, despite this are passwords still the most common authentication method on the web (Guirat & Halpin, 2018; Bonneau, et al., 2015; FIDO Alliance & W3C, 2019). Passwords are difficult to remember and are victim to several attacks that expose users' passwords to an unauthorized party. FIDO Alliance has in cooperation with W3C created a standardized method of secure authentication on the web with the goal of eliminating passwords. The new method is called Web Authentication and utilize asymmetric encryption for securing users' accounts. This thesis studies Web Authentication for the purpose of compiling an introduction to the method that describes what Web Authentication is, how it works and how to use it. A study of passwords is conducted with the aim of shedding light on limitations of passwords and display improvements to passwords which make them more secure. The studies are conducted through systematic literature reviews. Web Authentication implies that no credentials are stored on a server and therefore eliminates data breaches with the aim of obtaining credentials. Web Authentication has also been found to be resistant to phishing attacks. Bonneau et al. developed a framework for comparing different authentication methods in 2012 (Bonneau, et al., 2012). No previous authentication method provides in reference to Bonneau et al. framework as many advantages as the new method (Lyastani, et al., 2020). One disadvantage of the new method is however the difficulty of restoring credentials in case of loss. The user must have a backup method of authentication in place in case of loss, this can for example be a spare key when using physical security keys. After access is granted through use of a backup method the user has to remove the lost credential from the account to then register a new credential. This has to be done for all accounts where the credential is registered.

Keywords:	information security, asymmetric encryption, the web, Web Authentication, security key
Number of pages:	50
Language:	Swedish
Date of acceptance:	

INNEHÅLL

Figurer

1 INTRODUKTION

Det råder konsensus att lösenord är föråldrade och osäkra för användning på webben (Guirat & Halpin, 2018; Bonneau, et al., 2015; FIDO Alliance & W3C, 2019). Lösenord har dominerat autentisering i 50 år trots enighet bland forskare att det behövs något säkrare och mer användarvänligt. Lösenord skapades under 1960-talet vid utvecklingen av de första time-sharing operativsystemen, operativsystem som tillåter att flera användare delar samma dator samtidigt, som skydd mot att forskare använde mer resurser än beviljat, något helt annat än vad de används för på webben idag. (Bonneau, et al., 2015). Lösenord är svåra att minnas vilket leder till att användare skapar svaga lösenord och använder samma lösenord på flera webbplatser (Florêncio & Herley, 2007). Detta gör konton sårbara eftersom ett stulet lösenord på en webbplats tillåter inkräktare att attackera användares konton på andra webbplatser med samma lösenord (Das, et al., 2014). Inkräktare får tag på lösenord genom nätfiske och dataintrång (Larson, 2017; Qiunn, 2012; Weatherbed, 2022). Två-faktorautentisering i form av engångslösenord kan användas för ett till lager av säkerhet (Crum & Forster, 2018), men engångslösenord är fortfarande utsatta för nätfiskeattacker (Engedy, 2018).

W3C och FIDO Alliance introducerar en ny metod kallad Web Authentication för autentisering på webben. Web Authentication påstås vara resistent mot nätfiskeattacker och stora aktörer inom informationsteknik understöder lösenordslös autentisering med Web Authentication (FIDO Alliance & W3C, 2019). Web Authentication kallas även WebAuthn.

1.1 Syfte och forskningsfrågor

Syftet med detta examensarbete är att sammanställa en introduktion till den nya autentiseringsmetoden Web Authentication genom analys av tillgänglig information om metoden. Introduktionen ger svar på vad den nya metoden är, hur den nya metoden fungerar samt hur den används. Utöver detta presenteras tidigare forskning gällande

säkerhet och användbarhet av lösenord som autentiseringsmetod på webben för att kartlägga autentiseringsmetodens brister och förbättringsmöjligheter.

Frågeställningen som examensarbetet ska besvara blir således: *Vad är Web Authentication och hur fungerar det?* Undersökningen av lösenord som autentiseringsmetod görs för att besvara frågeställningen: *Vilka brister har lösenordsautentisering?* och *Hur kan dessa brister förebyggas?*

1.2 Avgränsning

Orsakerna till att Web Authentication har valts är att det är en W3C standard och rekommenderas av IT organisationer som är bland de största i världen. Web Authentication har även bred support över alla populära operativsystem och webbläsare (Melo, 2022). Jag kommer inte att behandla ifall Web Authentication bevarar användarens integritet eller verifikation av attestering, eftersom attestering inte krävs i majoriteten av användningsområden och är en väldigt komplex process (Ackermann, 2021). Mer information om attestering finns i Web Authentication API specifikationen sektion 6.5 eller artiklarna *WebAuthn/FIDO2: Verifying TPM Attestation* och *WebAuthn/FIDO2: Demystifying attestation and MDS* av Ackermann. ”Token binding” kommer heller inte att behandlas fastän det nämns i specifikationen eftersom ”Token Binding” går utöver omfattningen av arbetet.

2 METOD

Syftet är att presentera den nya autentiseringsmetoden Web Authentication. Detta görs genom att utföra en systematisk litteraturöversikt av tillgängligt material kring Web Authentication. Systematisk litteraturöversikt används även för undersökningen av lösenord. En systematisk litteraturöversikt är en metod där man söker fram existerande studier, väljer och utvärderar materialet, analyserar och skapar relationer mellan data och rapporterar resultatet på ett sätt som tillåter att slutsatser kan dras om vad som är känt och okänt. En systematisk litteraturöversikt utforskar en klart specificerad fråga som besvaras med redan existerande studier (Denyer & Tranfield, 2009). Informationssökning har utförts på Arcada Finna, Google Scholar och Google. Informationssökningen har även involverat sökning i källförteckningen av relevanta källor.

3 TEORI

Följande kapitel inleds av en förklaring över de tre autentiseringsfaktorerna som utgör multi-faktorautentisering, de är något man vet, något man har och något man är. Därefter ges en förklaring över asymmetrisk kryptering, den teknik som Web Authentication baseras på och till sist en lista över termer som underlättar förståelsen av examensarbetet.

3.1 Autentiseringsfaktorer

En autentiseringsfaktor är information som används för autentisering av en persons identitet. Två-faktorautentisering är en autentiseringsmekanism baserad på två typer av information, något du har och något du vet. Användaren måste ange båda typerna av information för att få tillgång till systemet. Det finns ytterligare en till faktor som baseras på något en person gör eller är (Azad, 2008). En kombination av flera autentiseringsfaktorer erbjuder bättre säkerhet än om de används enskilt.

Knowledge

Enfaktor-autentisering eller knowledge-faktor är något som användaren vet, detta kan till exempel vara ett lösenord eller en PIN-kod, hit hör även säkerhetsfrågor. Detta anses vara den svagaste nivån av autentisering eftersom ett delat lösenord ger direkt åtkomst till kontot. En obehörig person kan även utföra en mängd olika attacker för att knäcka lösenordet (Ometov, et al., 2017).

Possession

Enfaktor-autentisering erbjuder inte tillräcklig säkerhet. Därför introducerades två-faktorautentisering eller possession-based autentisering, vilket förutom en knowledge-faktor kräver något användaren har, till exempel ett smartkort, en mobiltelefon eller en säkerhetsnyckel (Ometov, et al., 2017).

Biometrisk

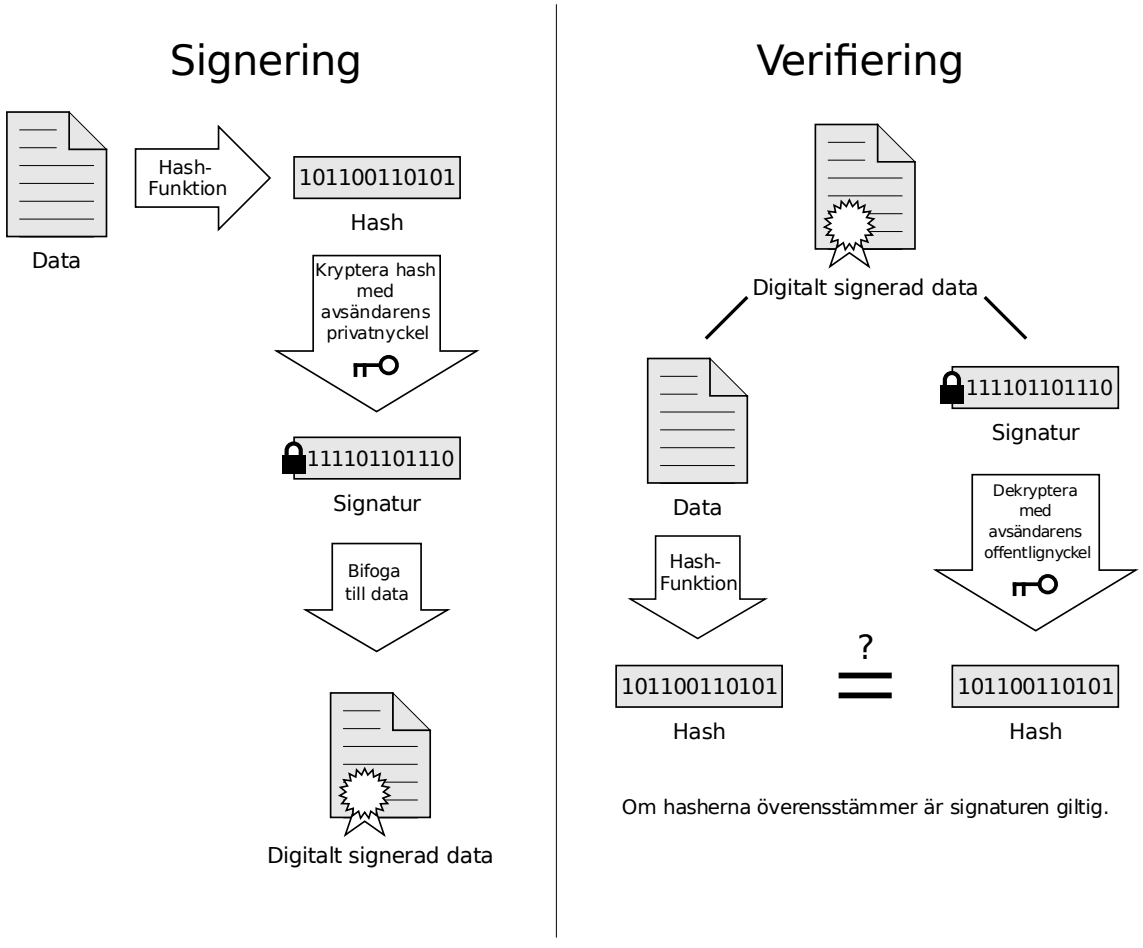
Biometrisk-autentisering är tredje faktorn som kan användas för att autentisera användaren. Biometrisk-autentisering använder användarens beteendemönster och biologiska egenskaper för att bevisa deras identitet, till exempel fingeravtryck eller ansiktsigenkänning (Ometov, et al., 2017).

3.2 Asymmetrisk kryptering

Asymmetrisk kryptering är en process som involverar ett nyckelpar, en offentlignyckel och en privatnyckel som är bundna till en person eller entitet. Nyckelparet fungerar tillsammans genom att de båda kan dekryptera data som har krypterats av den andra nyckeln. Den offentliga nyckeln ges ut och den privata ska hållas hemlig. Asymmetrisk kryptering möjliggör kryptering, dekryptering samt skapande av och verifiering av digitala signaturer. Kryptering tillåter två kommunicerande parter att gömma data de sänder sinsemellan, så att en utomstående inte ser vad data innehåller. Detta görs genom att avsändaren krypterar data med mottagarens offentliga nyckel så att mottagaren, som är den enda som besitter privat nyckeln, kan dekryptera meddelandet (IBM, 2021). Vid digital signering krypteras data med undertecknarens privata nyckel så att alla med undertecknarens offentliga nyckel kan verifiera att det är avsändaren som skapat meddelandet. Mer om digitala signaturer behandlas i nästa stycke.

En digital signatur har samma funktion som en vanlig underskrift på papper, det vill säga att kunna identifiera undertecknaren. Digitala signaturer baseras på asymmetrisk kryptering. Avsändaren skapar en signatur med hjälp av kryptering och mottagaren verifierar signaturen med hjälp av dekryptering. Detta fungerar genom att en envägs-hash skapas över data (eller meddelandet) som ska sändas och krypteras med avsändarens privata nyckel. En envägs-hash betyder att utifrån ett meddelande fås alltid samma hash, men från hashen kan meddelandet inte härledas. Den krypterade hashen tillsammans med hashningsalgoritmen som användes för att skapa hashen är en digital signatur. Den digitala signaturen kan verifieras genom att mottagaren beräknar sin egen hash över data, med hashningsalgoritmen i digitala signaturen. Mottagaren dekrypterar hashen i digitala signaturen med avsändarens offentliga nyckel och jämför den dekrypterade hashen med den hash som mottagaren själv beräknat (IBM, 2021).

För att förtydliga säkerställer en digital signatur två saker, avsändarens identitet åt mottagaren och att data hålls oförändrad. Vid verifiering av en digital signatur har mottagaren fått data, en signatur samt avsändarens offentliga nyckel. Från data beräknar mottagaren sin egen hash med algoritmen som specificeras i signaturen. Signaturen innehåller även den krypterade hashen som avsändaren beräknade före sändning. Med den offentliga nyckeln kan mottagaren dekryptera hashen, vilket bekräftar avsändarens identitet och uppenbarar hashen. Nu kan mottagaren jämföra den egna hashen med den från signaturen och säkerställa att data är oförändrat, det vill säga att data som mottagaren fått och data som avsändaren skickat är samma.



Figur 1, Digital Signature diagram (Källa: Acdx)

3.3 Termer

Autentiseringsuppgift är data som en entitet presenterar åt en annan för att bestyrka sin identitet.

Publiknyckel-autentiseringsuppgift är en autentiseringsuppgift som anger information om ett asymmetriskt nyckelpar.

Lokal autentisering betyder att en applikation autentiserar användaren mot inloggningsuppgifter lagrade lokalt på enheten (OWASP, u.d.).

Förlitande part är webbplatsen eller webbservern som hanterar autentisering av en autentiseringsuppgift som skapats av en autentiserare.

4 UNDERSÖKNING AV LÖSENORD

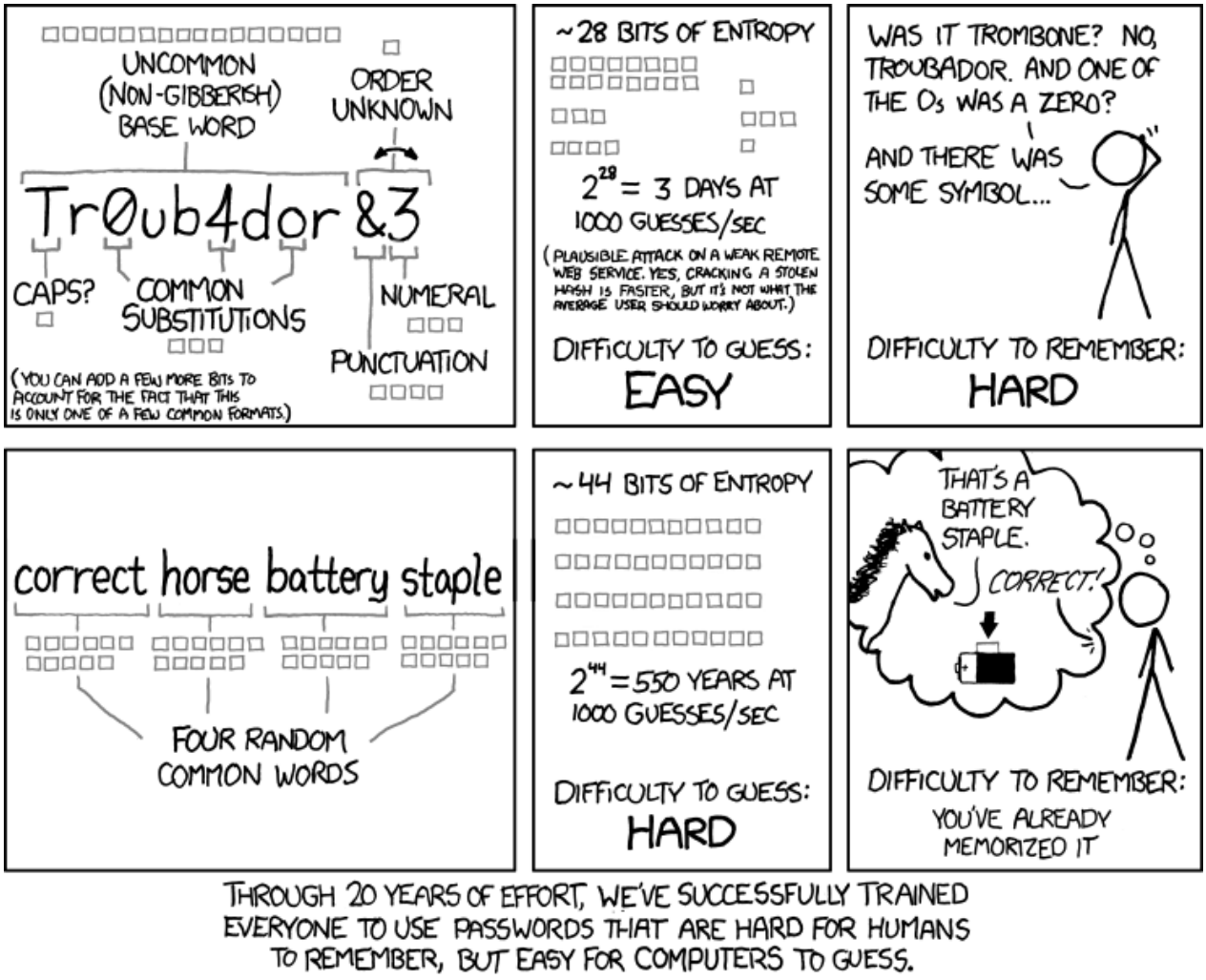
I följande kapitel behandlas brister med lösenord och hur dessa brister kan förebyggas.

4.1 Lösenordsvanor

Det är uppenbart att användare har svårt att minnas flera lösenord och för majoriteten av användare skyddas deras ökande mängd konton av ett fåtal lösenord. Användare väljer svaga lösenord, återanvänder samma lösenord på flera webbplatser och glömmer ofta sina lösenord (Florêncio & Herley, 2007). Återanvändning av lösenord utsätter säkerheten för risk eftersom en angripare som lyckas komma åt användarens konto på en tjänst även kan komma åt andra tjänster som skyddas av samma lösenord (Das, et al., 2014). Lösenord kan även vara lätta att gissa, speciellt om de är simpla eller vanliga. Enligt en artikel på Cybernews är de vanligaste lösenorden år 2023 ”123456”, ”123456789”, ”qwerty” och ”password” (Masiliauskas, 2023). I en annan studie framkommer det att 64% av användare anser att det viktigaste är att lösenord är lätta att minnas. I samma studie lyfts det fram att för 59% av användarna är rädslan att glömma lösenord den främsta, vilket får dem att använda samma eller liknande lösenord för flera konton (Petrillo, 2018). Vidare framkommer i en annan studie att 77% av deltagarna endera återanvänder eller ändrar ett existerande lösenord (Das, et al., 2014).

I en undersökning av HYPR framkommer att 78% av deltagarna har varit tvungna att återställa ett lösenord i sitt personliga liv under de senaste 90 dagarna och 57% i sitt arbetsliv (Leuthvilay, 2019). I en studie av ExpressVPN som undersökte lösenordsvanor i USA, Storbritannien, Frankrike och Tyskland nämns det att ungefär 50% av deltagarna i USA, Storbritannien och Frankrike och 35% av deltagarna i Tyskland återställer ett lösenord minst en gång i månaden. Vidare medger 21% av deltagarna i USA att de återställer ett lösenord en gång i veckan och 14% medger att de återställer ett lösenord om dagen. Återställning av ett lösenord om dagen betyder att 26 timmar i året spenderas på att återställa lösenord (ExpressVPN, 2022). En undersökning av Nordpass visar att

mer än 30% av nordamerikanska och brittiska användare anser att återställande av lösenord är psykiskt påfrestande (Rawlings, 2020).



Figur 2, "Password Strength" serie (Källa: xkcd.com)

4.2 Lösenord kan stjälas

Eftersom lösenord skyddar viktiga konton har de blivit offer för nätfiskeattacker. En nätfiskeattack innebär att en användare skickar sitt lösenord till en skadlig webbplats som liknar den riktiga webbplatsen i syfte att stjäla användarens lösenord. En nätfiskeattack är lika farlig oavsett lösenordets styrka (Florêncio & Herley, 2007).

Lösenord har varit en provisorisk lösning från första början med problem som uppstod direkt, det rapporterades många fall av att användare hade gissat varandras lösenord och ett fall där master-lösenordfilen hade läckts, som lagrades okrypterad. Dessa problem kunde enkelt lösas administrativt tack vare att alla användare var medlemmar i samma akademiska organisation. Då webbtjänster blev vanligare uppstod ett nytt problem, att återställa glömda lösenord. Detta hade tidigare gjorts manuellt av IT support men blev nu automatiserat med e-postmeddelanden. Detta gjorde e-postkonton till en svag länk och nätfiske blev ett stort problem (Bonneau, et al., 2015). Internetanvändares digitala fotavtryck leder ofta tillbaka till deras e-postadress och ett stulet lösenord tillåter en förbrytare att få åtkomst till användarens e-postkonto och därifrån återställa lösenord på andra tjänster, ladda ner personliga data, radera data och säkerhetskopior eller utnyttja användarens identitet för att skicka ut spam (Thomas, et al., 2017).

Verizons 2017 Data Breach Investigations Report är en rapport om i huvudsak bekräftade dataintrång och innehåller fall av riktiga dataintrång. I rapporten framgår att 62% av alla dataintrång använde någon form av hackning och 81% av dessa använder stulna eller svaga lösenord. Nätfiske var närvarande i över 90% av alla incidenter och dataintrång och 7,3% av användare föll offer för nätfiske, via en länk eller en öppnad bilaga. 15% av de som tidigare fallit offer för nätfiske blev även lurade en andra gång (Verizon, 2017).

I en studie utförd av Yubico framkommer att mer än hälften av deltagarna har varit med om en nätfiskeattack i deras personliga liv och att 44% av deltagarna har upplevt en nätfiskeattack i arbetslivet. 57% av deltagarna har inte ändrat sina lösenordsvanor trots att de varit med om en nätfiskeattack (Yubico, 2019). Mellan mars 2016 och mars 2017 identifierade Thomas et al. 12,4 miljoner potentiella offer för nätfiske och 1,9 miljarder stulna användarnamn och lösenord via dataintrång. Utav 750 miljoner läckta Google konton hade 51 miljoner av dem matchande lösenord. Detta betyder att stulna inloggningsuppgifter innebär en stor risk för autentiseringssystem som enbart förlitar sig på användarnamn och lösenord (Thomas, et al., 2017).

Stora dataintrång händer hela tiden, år 2013 utsattes Yahoo för ett dataintrång som påverkade tre miljarder konton, vilket var precis varje konto registrerat vid tillfället av händelsen (Larson, 2017; Selyukh, 2017). 2012 läcktes 55 000 lösenord hos Twitter

(Qiunn, 2012; Fenech, 2012) och 2022 blev inloggningsuppgifter till ungefär 10 000 personer stulna i en nätfiskekampanj som riktades mot över 130 organisationer (Weatherbed, 2022).

4.3 Möjliga förbättringar för lösenord

Här näst presenteras resultatet av undersökning av tre sätt som påstås göra lösenordsautentisering säkrare.

4.3.1 Lösenordsregler

Das, et al. (2014) påstår att avancerade lösenordsregler kan användas för att öka styrkan av lösenord. Lösenordsregler innebär att webbplatsen ställer krav på det lösenord användaren skapar, till exempel att lösenordet måste innehålla små och stora bokstäver samt siffror. Vidare menar dock Das et al. att lösenordsregler innebär en kompromiss mellan användbarhet och säkerhet, mer komplicerade lösenord leder till större svårighet att minnas lösenordet och försämrad användbarhet av tjänsten. Komplicerade lösenordsregler kan också potentiellt försämra säkerheten genom att uppmuntra användarna att skriva ner eller lagra lösenord elektroniskt som hjälp för att minnas dem (Das, et al., 2014). En Microsoft lösenordguide från 2016 berättar däremot att nästan alla lösenordsregler som påtvingas användare resulterar i sämre lösenord. Dessa kan exempelvis vara längdkrav, krav på specialtecken och regelbundna lösenordsändringar som alla skapar förutsägbar normalisering av lösenord, vilket gör det lättare för inkräktare att gissa eller knäcka lösenord (Hicock, 2016). Alex Weinert (2019) direktör för Identity Security vid Microsoft skriver i blogginlägget ”Your Pa$$word doesn't matter” att fokus på lösenordsregler är endast en distraktion från saker som verkligen hjälper så som multi-faktorautentisering. Vidare menar Weinert att lösenordssammansättning och lösenordslängd för det mesta inte spelar någon roll. Orsaken till detta är att de flesta lösenordsattacker fokuserar på att stjäla lösenord och inte knäcka dem, om ett lösenord blir stulet spelar styrkan ingen roll (Weinert, 2019).

4.3.2 Lösenordshanterare

Lösenordshanterare är applikationer som är till för att lagra och hantera inloggningsuppgifter. Fördelar med användning av en lösenordshanterare är att användaren inte längre behöver minnas alla lösenord. Användaren måste enbart minnas master-lösenordet, ett lösenord som används för att låsa upp lösenordsvalvet. Detta bidrar till att användaren kan skapa unika och starka lösenord. Lösenordshanterare kan också auto-generera starka lösenord för användaren. Lösenordshanterare som är inbyggda i webbläsaren kan även potentiellt förhindra nätfiskeattacker. Orsaken till att de kan förhindra nätfiskeattacker är för att lösenordshanteraren sparar lösenordet i kombination med webbplatsen och kan automatiskt fylla i användarnamn och lösenord då användaren besöker webbplatsen. Om användaren besöker en falsk webbplats så matar inte lösenordshanteraren in användarnamn och lösenord automatiskt eftersom den inte har några inloggningsuppgifter associerade med den falska webbplatsen och användaren kan märka att hen inte är på den riktiga webbplatsen (Malwarebytes, u.d.).

Trots fördelar med lösenordshanterare var det år 2022 endast 21% av användare som använde sig av en lösenordshanterare (Vigderman, 2023). I en studie som undersöker användares motiv för att använda eller inte använda en lösenordshanterare framkommer det att den främsta orsaken till att folk inte använder en lösenordshanterare är på grund av säkerhetsproblem, vilket visar att icke-användare är misstänksamma på grund av okunskap om teknologin (Fagan, et al., 2017).

4.3.3 Engångslösenord (OTP)

Engångslösenord erbjuder ett till lager av säkerhet utöver lösenord. Utöver användarnamn och lösenord måste användaren ange en kod, som är giltig för endast en inloggning, för att få åtkomst till kontot. Användaren kan få koden till sitt telefonnummer via SMS, eller hittar den i en applikation på mobilen eller i en säkerhetstoken. Lösenord kombinerat med engångslösenord erbjuder två-faktorautentisering genom att kräva en knowledge-faktor (lösenordet) och en possession-faktor (engångslösenordet). Fastän engångslösenordet är ett lösenord eller en kod, så är koden ett bevis på att användaren besitter den registrerade

enheten (Crum & Forster, 2018). Fördelen med OTP i mobilen är att de flesta användare redan äger en mobiltelefon.

Weinert (2020) skriver i ett annat blogginlägg att man borde byta ut användningen av två-faktorautentisering via SMS mot säkrare metoder, detta på grund av att SMS använder publika telefonnätet och Weinert menar att det är den minst säkra två-faktormetoden som är tillgänglig idag. Han menar även att innovation för säkerhet och användbarhet är begränsad (Weinert, 2020). Weinert skriver dock i ett annat blogginlägg att multi-faktorautentisering är det minsta man kan göra om man tycker att det är viktigt att skydda sina konton, oavsett metod. Att använda något utöver lösenord ökar signifikant ansträngningen för inkräktare, vilket är anledningen till att mindre än ett konto på tusen som använder två-faktorautentisering blir kapat (Weinert, 2019).

Engångslösenord är dock fortfarande utsatta för nätfiskeattacker. En nätfiskeattack mot användaren kan ske enligt följande, användaren matar in sitt lösenord på den falska webbplatsen och inkräktaren ansluter sig till den riktiga webbplatsen, då frågar webbplatsen efter ett OTP av inkräktaren som i sin tur frågar av användaren. På samma gång sänder den riktiga webbplatsen en OTP till användarens mobiltelefon och eftersom användaren tror sig logga in till den riktiga webbplatsen och förväntar sig därför att bli tillfrågad, anger OTP till den falska webbplatsen. Inkräktaren kan då ange OTP som användaren har angett till den riktiga webbplatsen och har då åtkomst till deras konto. Orsaken till problemet är att säkerheten beror på användarens förmåga att identifiera att webbplatsen är falsk (Engedy, 2018).

Enligt en artikel på The Verge använde endast 10% av Gmail konton två-faktorautentisering år 2018 (Ong, 2018). År 2021 planerade dock Google att automatiskt registrera två-faktorautentisering för 150 miljoner konton (Mardini & Kim, 2021). Enligt en studie gjord av Rublon (2022) använde just över hälften av företagen någon typ av MFA år 2022 men nästan en tredje del hade planer för att införskaffa en MFA lösning inom ett år.

5 WEB AUTHENTICATION HISTORIA

Detta kapitel behandlar uppkomsten av Web Authentication och organisationerna som gav upphov till dess utveckling.

5.1 FIDO Alliansen

FIDO Alliance grundades år 2012 av PayPal, Lenovo, Nok Nok Labs, Validity Sensors, Infineon och Agnitio och då började de arbeta på ett lösenordslöst autentiseringsprotokoll (FIDO Alliance, u.d.). Efter att FIDO Alliansen släppt FIDO UAF och FIDO U2F specifikationerna i december 2014, påbörjade FIDO Alliansen ett nytt uppdrag att göra FIDO Autentisering mer tillgänglig för användare över hela världen. FIDO Alliansen utvecklade tre tekniska specifikationer (FIDO UAF, FIDO U2F och CTAP) som definierar en webbaserad API, som gör det möjligt för FIDO Autentisering att användas rakt i webbläsare. FIDO Alliansen tog beslutet att samarbeta med World Wide Web Consortium (W3C) för att standardisera FIDO Autentisering för hela webbplattformen (FIDO Alliance, u.d.). W3C är den världsledande organisationen för webbstandarder som ansvarar för till exempel HTML (Guirat & Halpin, 2018). FIDO Alliansen lämnade år 2015 in FIDO specifikationerna för standardisering och API:t blev då Web Authentication eller WebAuthn (FIDO Alliance, u.d.).

Idag består FIDO Alliance av över 250 medlemmar som representerar globala ledare inom internettjänster, säkerhet, finans, kommunikation och regering (FIDO Alliance, 2020). Deras mission är att skapa autentiseringsstandarder som hjälper till att minska på världens beroende av lösenord. FIDO Alliance arbetar för att ändra hur autentisering funkar genom öppna standarder som är säkrare än lösenord och SMS OTP, lättare för konsumenter att använda och lättare för tjänsteleverantörer att distribuera och hantera (FIDO Alliance, u.d.).

5.2 Web Authentication Working Group

Den 8 februari 2016 blev *Web Authentication Working Group Charter* godkänd av W3C (Halpin, 2016) och konsortiet meddelade att första mötet skulle hållas den 4 mars 2016 i San Francisco (Bird, 2016). I stadgan definieras målet med Web Authentication Working Group vilket är att skapa ett standardiserat API samt standardiserade signatur- och attesteringsformat. Dessa skapar en grund som baseras på asymmetrisk kryptografi för autentisering av användare mot webbapplikationer. Gruppens allmänna mål är bland annat att eliminera användningen av lösenord som autentiseringsuppgifter och främja stöd för multi-faktorautentisering (Halpin, 2016). *FIDO 2.0 Platform Specifications 1.0* som består av tre specifikationer, *FIDO 2.0: Web API for accessing FIDO 2.0 credentials*, *FIDO2.0: Key Attestation Format* och *FIDO2.0: Signature format*, inlämnat 12 november 2015 till W3C, blev första bidraget till *Web Authentication Working Group* (Halpin, 2016; Champion, et al., 2015).

5.3 Web Authentication blir en W3C Rekommendation

Web Authentication Group publicerade *Web Authentication: An API for accessing Public Key Credentials Level 1*, som en W3C Rekommendation 4 mars 2019. Web Authentication är en kärnkomponent i FIDO Alliansens FIDO2 och är en standard för simplare och starkare autentisering. Web Authentication har stöd i Windows 10, Android och Chrome, Firefox, Edge och Safari webbläsare (Seltzer, 2019). Web Authentication Level 2 blev en W3C Rekommendation 8 april 2021 (Seltzer, 2021). Level 2 innehåller en rad korrigeringar och förbättringar till den första specifikationen (Yubico, u.d.).

Vad är en W3C Rekommendation?

En W3C Rekommendation är betraktat som en webbstandard, detta görs efter en process som är utformad för främjandet av konsensus, rättvisa, offentligt ansvar och kvalitet. Syftet med Rekommendationer är att dra uppmärksamhet till specifikationen och att uppmuntra dess spridning. Rekommendationer ökar funktionaliteten och interoperabilitet

på webben (W3C, u.d.; W3C, 2021). Interoperabilitet betyder att ”två eller flera systems förmåga att utbyta information och använda informationen som de får från varandra” eller enklare deras förmåga att fungera ihop (IDG, 2016).

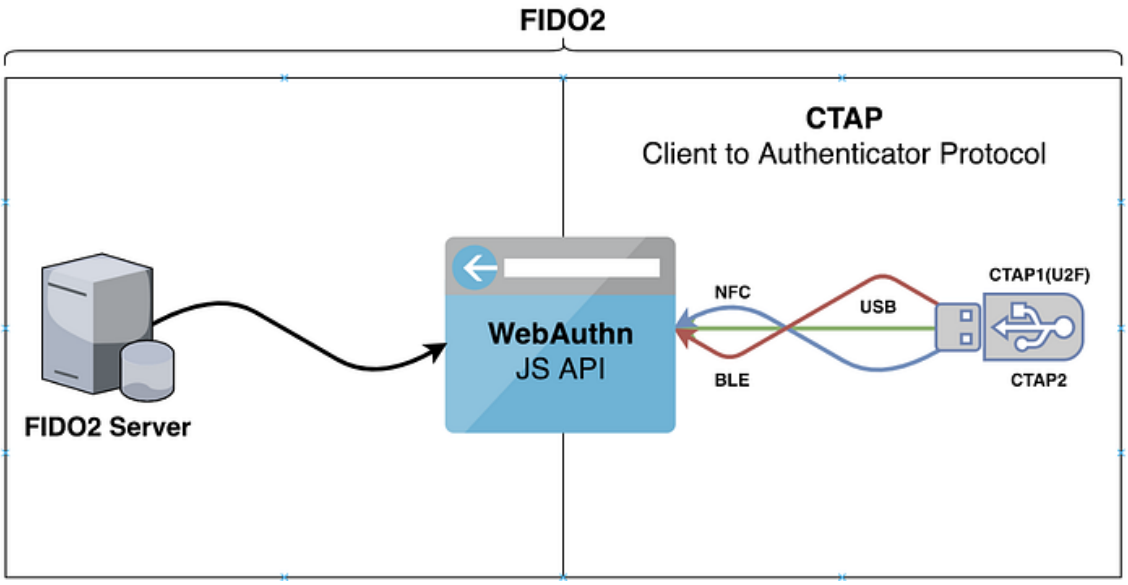
6 RESULTAT

Nedan presenteras resultat från informationssökning om Web Authentication.

Det är allmän kunskap att lösenord inte längre är effektiva. Stulna eller svaga lösenord är orsaken till 81% av dataintrång, lösenord är slöseri med tid och resurser (FIDO Alliance & W3C, 2019). Enligt en studie gjord av Yubico (2019) spenderar användare 10.9 timmar per år på att slå in och nollställa lösenord, detta kostar företag i genomsnitt 5.2 miljoner dollar årligen. Traditionell multi-faktorautentisering som till exempel SMS engångskoder ger bättre säkerhet men de är fortfarande utsatta för nätfiskeattacker, de är även svåranvända och har ett lågt användarantal. IT-branschen har samarbetat för att erbjuda en gemensam lösning till lösenordsproblemet genom FIDO2 och Web Authentication (FIDO Alliance & W3C, 2019).

6.1 Vad är FIDO2

FIDO2 består av två standardiserade komponenter, Web Authentication och CTAP2 protokollet. Web Authentication beskriver hur klienten och webbservern kommunicerar med varandra och CTAP2 beskriver hur klienten kommunicerar med autentiseraren. FIDO2 stöder lösenordslös, tvåfaktor och multifaktor autentisering med inbyggda autentiserare som skyddas med till exempel biometri eller PIN-koder, eller externa autentiserare, såsom FIDO2 säkerhetsnycklar, mobiltelefoner eller smartklockor.



Figur 3, Visualisering av FIDO2 (Källa: Y. Ackermann)

6.2 Vad är Web Authentication

Web Authentication är en specifikation och ett JavaScript API i webbläsaren vars syfte är stark autentisering av användare. Web Authentication använder inloggningsuppgifter baserade på asymmetrisk kryptering. Web Authentication består av tre komponenter som gör det hela möjligt, autentiseraren, webbläsaren och webbservern. Tjänster kan använda Web Authentication under två olika men relaterade "ceremonier", vilka är registrering och autentisering. (Hodges, et al., 2021)

Autentiseringsuppgifterna skapas och lagras i en enhet som kallas autentiserare. Då man autentiseras med lösenord lagras lösenordet i användarens hjärna och ingen enhet behövs, men vid autentisering med Web Authentication byts lösenordet ut mot ett nyckelpar som lagras i en autentiserare. Autentiseraren kan vara inbyggd i en applikation, operativsystem eller så kan den vara en fysisk säkerhetsnyckel (MDN Web Docs, u.d.).

Varje autentiseringsuppgift är bunden till en viss webbplats och lagras säkert på autentiseraren. Web Authentication tillåter lösenordslös multi-faktorautentisering med autentiserare som stöder användarverifiering, det vill säga att utöver bevis av en possession-faktor kräver dessa autentiserare till exempel en PIN-kod eller biometriska

data. Denna användarverifiering sker lokalt på enheten och används endast för upplåsning av autentiseraren vilket eliminerar behovet av att användaren delar sitt lösenord med webbplatsen (Hodges, et al., 2021). Eftersom privatnyckeln lagras säkert på autentiseraren är den även okänd för användaren och kan inte bli stulen genom nätfiske (Guirat & Halpin, 2018).

Enligt en studie utförd av Guirat och Halpin (2018) konstateras Web Authentication vara resistent mot nätfiskeattacker och man-in-the-middle-attacker. Ett system som använder Web Authentication är heller inte beroende av kunskapsbaserad autentisering så som användarnamn och lösenord utan förlitar sig på registrerade enheter som ägs av användaren. Web Authentication sänker risken för identitetskapning eftersom fysiska enheter är svårare att stjäla än lösenord (Jung & Shepherd, 2019). FIDO autentiseringsuppgifter lagras aldrig på en server och faller på så sätt inte offer för dataläckor i och med dataintrång (Lyastani, et al., 2020).

6.3 Lösenord kontra PIN-kod

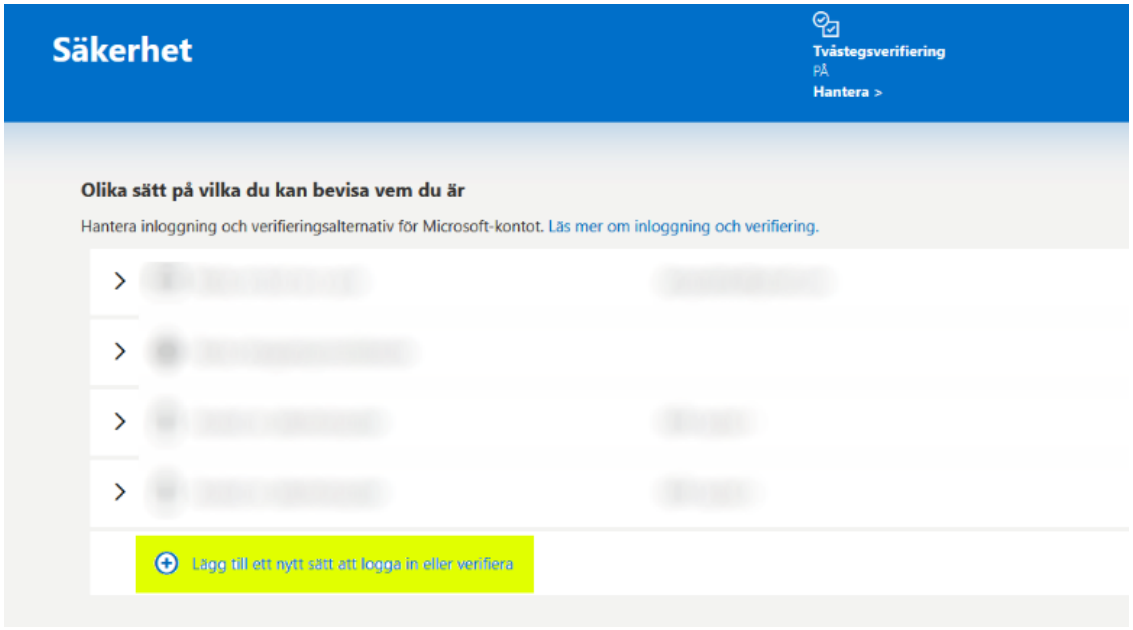
Lösenordslös autentisering kan fortfarande kräva att användaren matar in en PIN-kod i stället för ett lösenord. Fastän båda är principiella lösenord som användaren måste mata in är skillnaden att ett lösenord är en gemensam hemlighet som måste sändas till webb-platsen för verifiering och en PIN-kod existerar endast lokalt på enheten och sänds aldrig någonstans. PIN-koden används endast för att låsa upp enheten som sedan används för att skapa en digital signatur. Detta innebär att PIN-koden inte fungerar på en annan enhet och en inkräktare behöver därför både PIN-koden och enheten, en mycket svårare uppgift. Användaren behöver då också bara minnas en PIN-kod för alla webbplatser i stället för ett lösenord för varje webbplats, vilket underlättar memorering (Yubico, u.d.).

6.4 Hur används Web Authentication

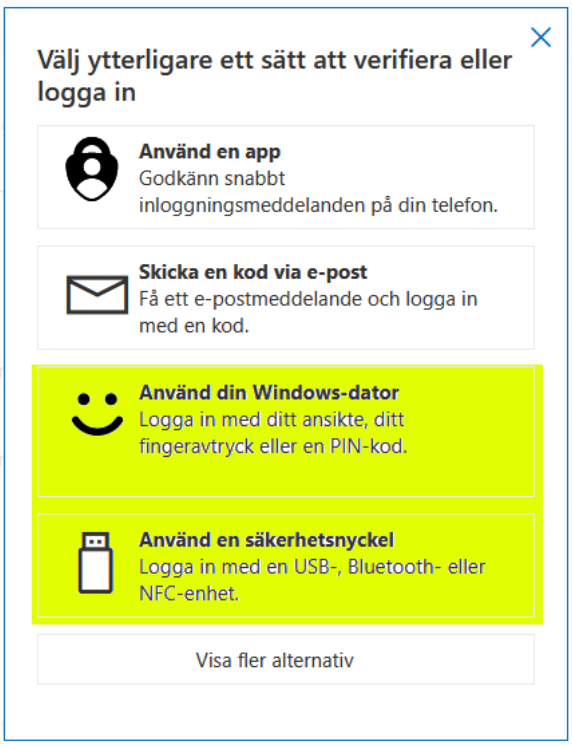
Till följande görs en demonstrering av Web Authentications användningsområden för att läsaren ska förstå vad Web Authentication handlar om i praktiken och för att ge kontext

för sektion 6.5 *”Hur fungerar Web Authentication”*. Denna sektion behandlar Web Authentications två ceremonier registrering och autentisering. Microsoft Outlook har valts för demonstreringen och orsaken till detta är att jag anser att de har bäst stöd för lösenordslös autentisering med Web Authentication.

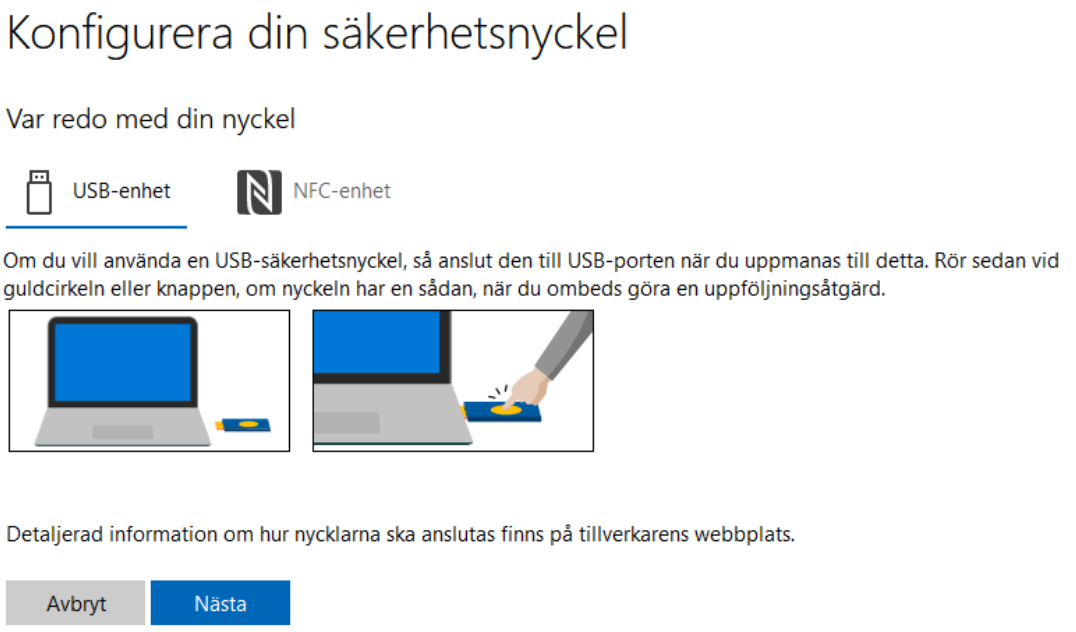
6.4.1 Demonstrering av registrering



För att sätta till en ny säkerhetsnyckel till ett Microsoft konto besöker jag säkerhetsinställningarna för kontot och väljer ”Lägg till ett nytt sätt att logga in eller verifiera”.

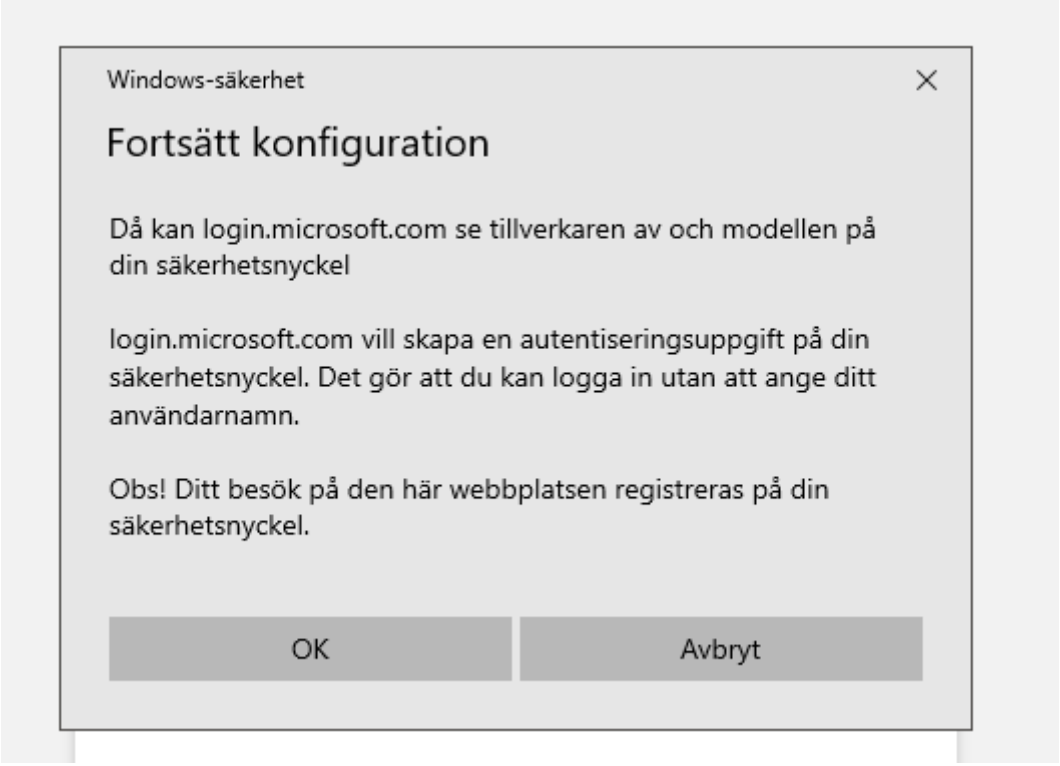


Sedan kan man välja ”Använd din Windows-dator” för att använda datorns inbyggda TPM-modul eller ”Använd en säkerhetsnyckel” för att använda en fysisk nyckel. I denna demonstration väljer jag ”Använd en säkerhetsnyckel”.

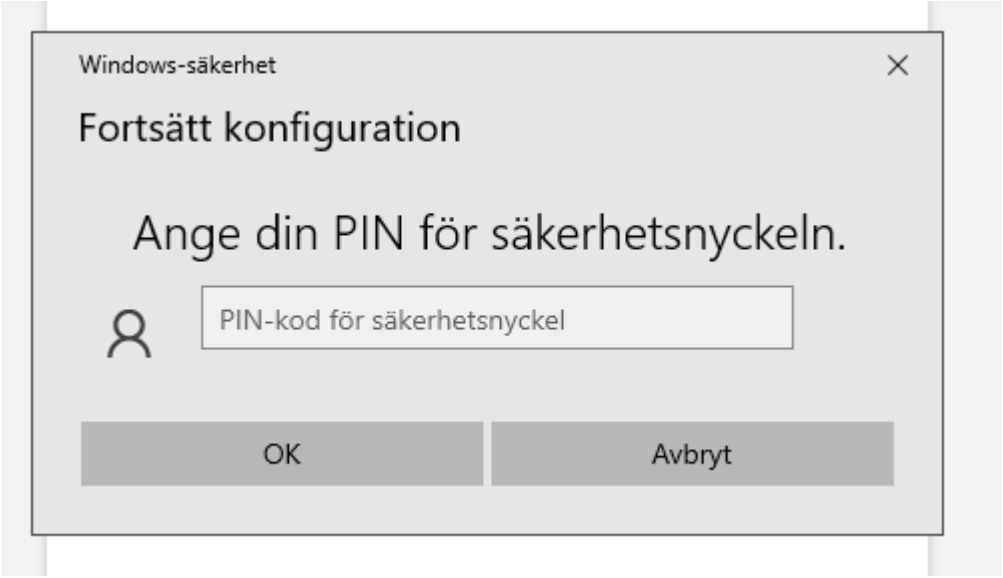


I nästa ruta väljs det gränssnitt som man önskar använda för säkerhetsnyckeln, i denna demonstration väljer jag USB och trycker ”Nästa”.

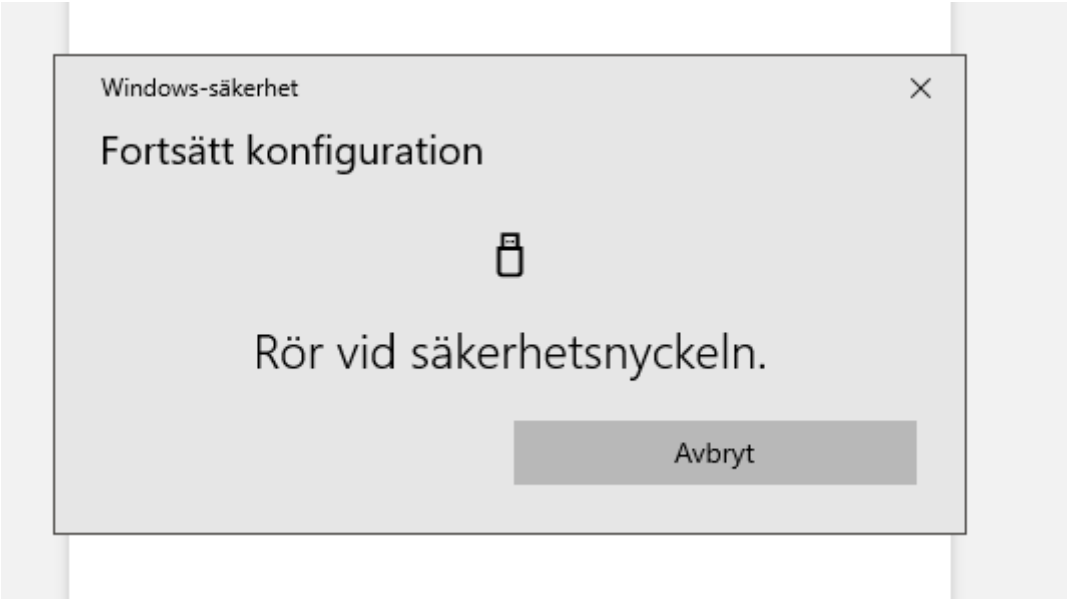
Då visas en dialog som ber användaren om tillåtelse för skapande av en säkerhetsnyckel och jag trycker OK för att ge godkännande.



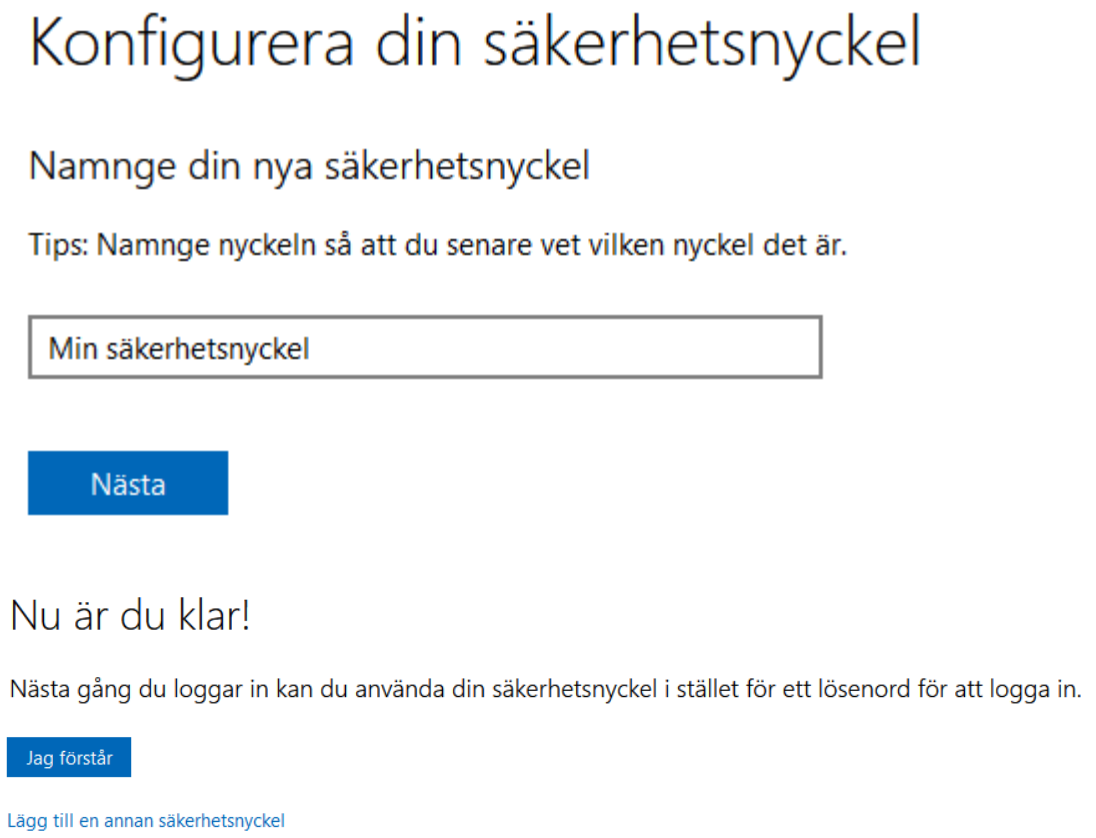
Följande ruta visas om tjänsteleverantören stöder attestering och jag trycker OK för att godkänna att webbplatsen får se information om nyckeln.



Nästa dialog frågar användaren om koden som säkerhetsnyckeln blivit konfigurerad med, detta har i demonstrationen gjorts i förväg och beskrivs inte i detta arbete. Alternativt om säkerhetsnyckeln stöder biometri kan dialogen till exempel fråga efter ett fingeravtryck. Jag matar in rätt PIN-kod och trycker på OK.



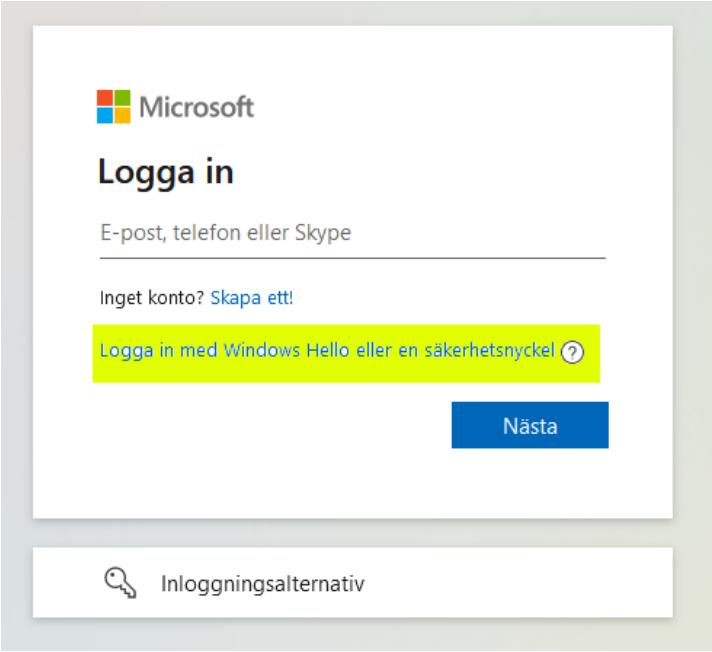
I nästa steg bör användaren röra vid säkerhetsnyckeln, detta är ingen fingeravtrycksläsare utan kontrollerar enbart användarens närvaro.



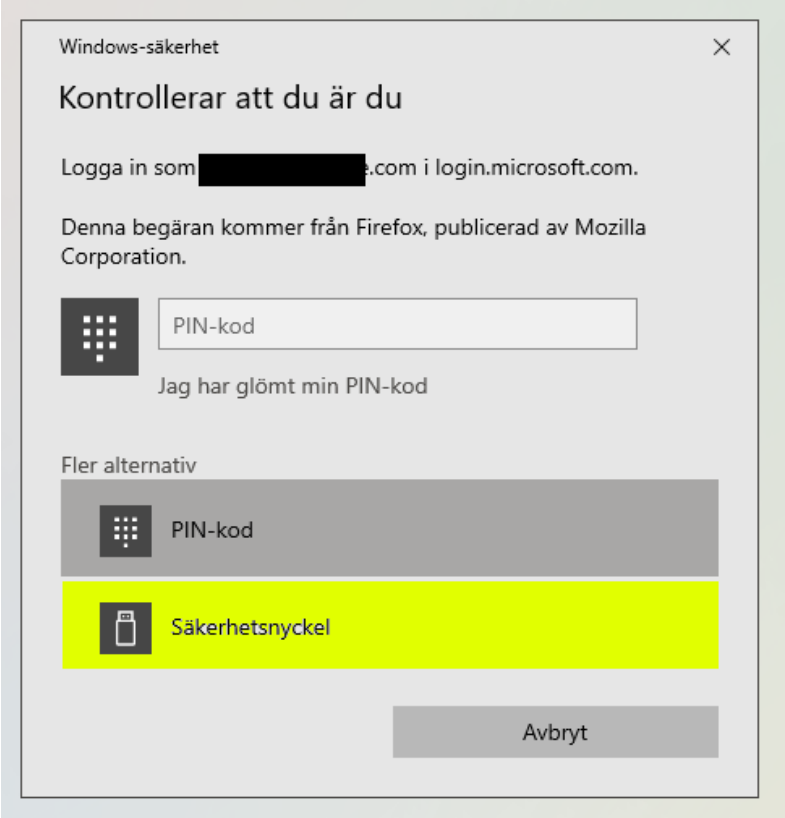
Till sist ska säkerhetsnyckeln få ett namn, detta namn är endast till för att användaren ska kunna identifiera nyckeln senare, till exempel för att ta bort den från kontot. Då är registreringen klar och nyckeln kan vid fortsättningen användas vid inloggning.

6.4.2 Demonstrering av inloggning

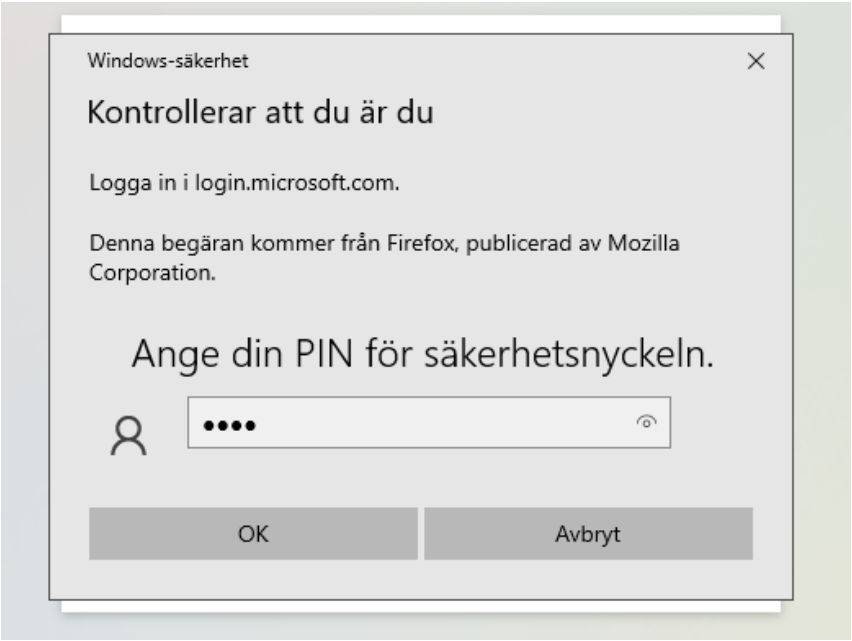
Så här går det till vid inloggning efter godkänd registrering av säkerhetsnyckeln.

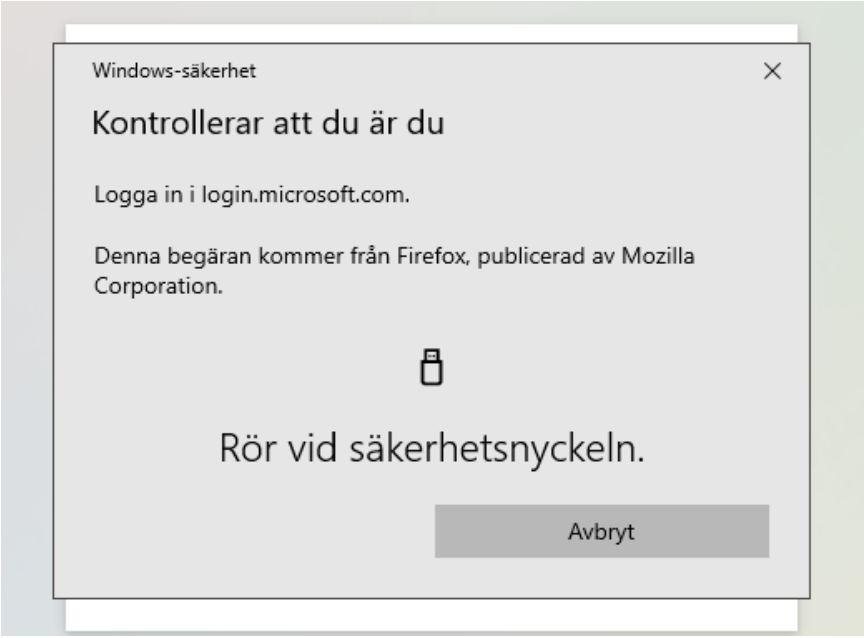


Vid inloggningssidan för Microsoft, väljs ”Logga in med Windows Hello eller en säkerhetsnyckel”.



Då visas dialog för lokal autentisering och ”Säkerhetsnyckel” väljs, då ombeds användaren att mata in PIN-koden för säkerhetsnyckeln.





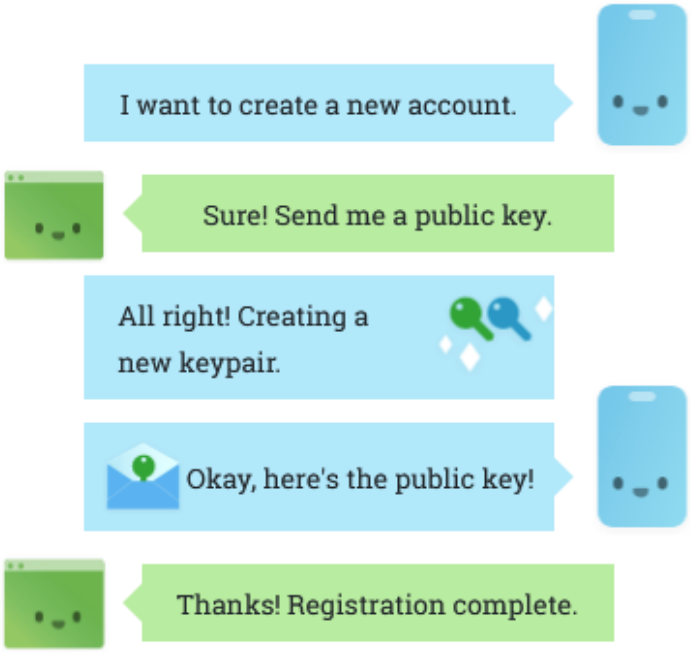
Om koden är rätt ombeds användaren att röra vid nyckeln och efter vidröring av nyckeln blir inloggningen godkänd och användaren har åtkomst till kontot.

6.5 Hur fungerar Web Authentication

Följande sektion kommer att behandla hur de två ceremonier som Web Authentication stöder fungerar. Registrering går ut på att användaren, webbservern och webbläsaren samarbetar för att skapa en ny publiknyckel-autentiseringsuppgift (eng. Public key credential), som består av en offentlig och en privat nyckel och associera den med användarens konto hos förlitande part. Detta kräver bevis för användarens närvaro eller verifikation av användaren. Efter lyckad registrering kan användaren autentiseras i den andra ceremonin, som är autentisering. Vid autentisering samarbetar användaren och webbläsaren för att bevisa åt förlitande part att användaren besitter den privata nyckeln som är associerad med den tidigare registrerade publiknyckel-autentiseringsuppgiften. Detta kräver liksom för registrering bevis för användarens närvaro eller verifikation av användaren (Hodges, et al., 2021).

6.5.1 Registrering

Till följande ges en förenklad beskrivning på hur registrering av en ny autentiseringsuppgift fungerar.

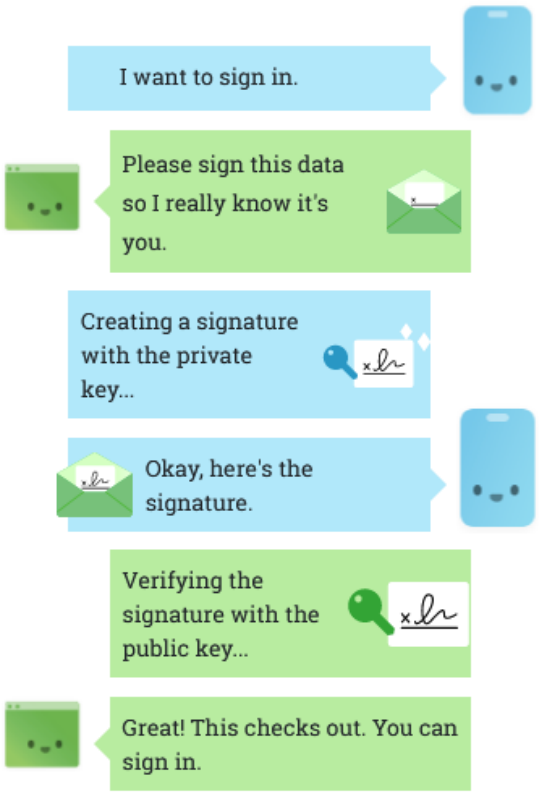


Figur 4, Simplifierad Web Authentication registreringsflöde (Källa: WebAuthn Guide)

Registrering av en ny autentiseringsuppgift börjar alltid med att webbservern genererar en utmaning, ett stort och slumpmässigt tal som endast används vid registreringsprocessen. Utmaningen skickas tillsammans med användarens kontouppgifter, som är sparade hos förlitande part, till webbapplikationen som körs i webbläsaren. Webbläsaren lägger till domännamnet till den tidigare datan och skickar den via anrop av Web Authentication API till autentiseraren som frågar efter användarens samtycke, detta görs så att skadliga webbplatser inte kan spåra användaren vilket skyddar användarens integritet. Efter användarens samtycke genererar autentiseraren ett nytt nyckelpar, en privat och en offentlig nyckel. Den privata nyckeln sparas internt i autentiseraren tillsammans med ett identifikationsnummer för det nya nyckelparet, användarens kontouppgifter och domännamnet som nyckelparet tillhör. Anropet av Web Authentication API fullgörs och identifikationsnumret och den offentliga nyckeln returneras i webbapplikationen. Webbapplikationen vidarebefordrar resultatet från Web Authentication till webbservern. På webbservern valideras utmaningen och domännamnet. Om valideringen lyckas ska webbservern lagra identifikationsnumret och den offentliga nyckeln tillsammans med användarens kontouppgifter och utmaningen ska ogiltigförklaras. Detta avslutar registreringsprocessen och användaren kan i fortsättningen autentisera sig med hjälp av autentiseraren som skapat nyckelparet (Brand, 2020; Engedy, 2018).

6.5.2 Autentisering

Till följande förklaras hur lösenordslös autentisering används efter registrering av en ny publiknyckel-autentiseringsuppgift.



Figur 5, Simplifierad Web Authentication autentiseringsflöde (Källa: WebAuthn Guide)

Ursprungsläget vid autentisering är att autentiseraren redan har en privat nyckel och webbservern har den motsvarande offentliga nyckeln som är förknippad med användarens konto. Autentiseringsflödet börjar likasom vid registrering med att webbservern genererar en utmaning. Utmaningen förhindrar vid autentisering återuppspelningsattacker, en attack som sker över nätet där en inkräktare fångar och återsänder ett meddelande som tidigare skickats mellan en legitim avsändare och mottagaren för att maskera återsändningen som giltig och på så sätt få obehörig åtkomst (Grassi, et al., 2017). Webbservern sänder utmaningen och identifikationsnumret för autentiseringsuppgiften, som sparades av webbservern under registrering, till webbapplikationen som igen lägger till webbapplikationens domännamn och skickar vidare informationen till autentiseraren via Web Authentication API. Autentiseraren söker upp den sparade informationen för den privata nyckeln med hjälp av identifikationsnumret och verifierar att domännamnet överensstämmer med det domännamn som användes vid registrering. Detta är en viktig säkerhetsåtgärd och gör autentiseraren immun mot nätfiskeattacker eftersom nätfiskeattacker vanligtvis kräver att användaren matar in sina autentiseringsuppgifter på

en falsk kopia av den riktiga webbplatsen som har ett annat domännamn. Ifall det är den rätta webbplatsen begär autentiseraren lokal autentisering av användaren, i form av till exempel en PIN-kod eller fingeravtryck. Om lokal autentisering lyckas använder autentiseraren den privata nyckeln för att skapa en kryptografisk signatur över domännamnet och utmaningen. Den privata nyckeln används endast för att signera data från webbservern och lämnar alltså inte autentiseraren. Anropet av Web Authentication API fullgörs och signaturen returneras till webbapplikationen som vidarebefordrar den till webbservern. Webbservern säkerställer att signaturen överensstämmer med den offentliga nyckeln och utmaningen i den signerade datan med den tidigare genererade utmaningen. Genom verifiering av signaturen med hjälp av den offentliga nyckeln kan webbservern kontrollera att användaren har rätt privat nyckel och verifiering av utmaningen säkerställer att signaturen kommer från rätt autentiseringstillfälle. Om verifikationen av signaturen lyckas är autentiseringen godkänd och utmaningen ska ogiltigförklaras (Brand, 2020; Engedy, 2018).

6.5.3 Skydd mot kloning

En Web Authentication autentiseringsuppgift har en signaturräknare, ett tal som ökar med ett för varje lyckad autentisering. Detta värde sparas även på webbplatsen och uppdateras för varje lyckad autentisering med värdet i autentiseringsuppgiften. Vid varje ny autentisering jämförs värdet i autentiseringsuppgiften mot värdet sparat på webbplatsen. Om värdet i autentiseringsuppgiften än mindre eller lika med det värde sparat på webbservern kan det vara tecken på att autentiseraren har blivit klonad. Då kan webbplatsen använda till exempel geolokalisering eller annan data för att ta beslut om att autentisera användaren (Hodges, et al., 2021).

6.6 Användbarhet

I en studie av Lyastani et al. (2020) konstateras att användare är väldigt nöjda med att direkt byta ut text-baserade lösenord mot säkerhetsnycklar och är villiga att acceptera sådan lösenordslös autentisering framför vanliga lösenord. Lyastani et al. jämför vanliga

lösenord med en-faktor FIDO2 autentisering enligt ett ramverk utformat av Bonneau et al. (2012) som definierar 25 subjektiva faktorer för mätande av säkerhet. FIDO2 autentisering med en säkerhetsnyckel saknar endast fyra av de 25 faktorerna vilka är ”Nothing-to-Carry”, ”Easy-Recovery-from-Loss”, ”Server-Compatible” och ”Resilient-to-Theft”. ”Nothing-to-Carry” innebär att användaren inte behöver bära på ett ytterligare fysiskt objekt. ”Easy-Recovery-from-Loss” betyder att användaren kan behändigt återfå möjligheten att autentisera sig om nyckeln försvinner eller om inloggningsuppgiften glöms. ”Server-Compatible” innebär att verifiering av autentiseringsuppgiften är kompatibel med text-baserade lösenord, det vill säga att leverantörer inte behöver ändra på nuvarande autentiseringssystem för att stöda denna metod. ”Resilient-to-Theft” betyder att om autentiseringsmetoden använder ett fysiskt objekt för autentisering så kan objektet inte användas för autentisering av en annan person som får tillgång till objektet. Inga existerande alternativ till vanliga lösenord erbjuder lika många fördelar i Bonneau et al. ramverk som FIDO2 med en-faktorautentisering. I en utvärdering av användbarheten av ett annat protokoll Pico, som liknar FIDO2 uppskattade användarna att slippa lösenord men oroade sig över återställande efter förlust och att kunna blockera säkerhetsnyckeln på distans (Lyastani, et al., 2020).

6.6.1 Hur synkronisera privata nycklar?

Hur säkerhetsnycklar skapade av inbyggda autentiserare kan synkas mellan enheten är ett problem som ännu inte är löst. Hur ska användaren kunna logga in på samma konto från olika enheter? Det nuvarande sättet användaren löser detta problem på är att på varje enhet, som användaren vill kunna logga in från, registrera en ny autentiseringsuppgift. Detta kan bli besvärligt för användaren och erbjuder en dålig användarupplevelse om användaren vill kunna logga in på samma konto från flera enheter. Detta är ett svårt problem att lösa om man vill bevara säkerheten som Web Authentication tillför, bevarande av säkerheten är viktig eftersom den ökade säkerheten är den största fördelen med Web Authentication.

Samma problematik existerar om användaren byter enhet, då måste användaren först för den nya enheten registrera nya nycklar för alla konton och sedan radera alla nycklar från

alla konton som är associerade med den gamla enheten. Detta blir snabbt en besvärlig process. En alternativ lösning är att endast använda externa autentiserare, dessa är transporterbara och tillåter användning av samma nyckel på alla enheter. Externa autentiserare har dock samma problem om man tappar bort nyckeln, då måste användaren logga in med en annan metod eller med en reservnyckel som är registrerad på samma konto och radera den förra nyckeln. Yubico rekommenderar en reservnyckel för lättare återställning ifall den primära nyckeln tappas bort eller blir stulen (Yubico, u.d.).

7 KONKLUSION

I detta kapitel sammanfattar jag mina resultat och analyser i tidigare kapitel.

Lösenord är osäkra och svåra att minnas. Försök att förbättra säkerheten med lösenordregler har resulterat i sämre säkerhet och användbarhet. Lösenordshanterare och OTP kan användas för att förbättra säkerheten men de är fortfarande inte resistenta mot nätfiskeattacker.

Web Authentication är framtiden inom autentisering på webben och de största aktörerna inom IT satsar på tekniken. Web Authentication förhindrar flertal attacker som används för att få tag på inloggningsuppgifter och komma åt användares konton. Web Authentication förbättrar användarupplevelsen genom att eliminera behovet att minnas lösenord på samma gång som det förbättrar säkerheten. Med Web Authentication behöver man inte längre minnas tiotal lösenord eller använda en lösenordshanterare för hantering av lösenord. Web Authentication flyttar ansvaret från användaren att skapa säkra och unika lösenord för varje webbplats till ansvar på Web Authentication, som alltid skapar starka och unika asymmetriska nycklar, vilket eliminerar mänskliga misstag som utsätter system för risker. Web Authentication eliminerar även ansvar från tjänster att säkert förvara användarnas känsliga inloggningsuppgifter till att tjänster endast lagrar icke-känsliga offentliga nycklar.

8 DISKUSSION

Till en början hade jag tänkt utveckla ett autentiseringssystem som baserade sig på ansiktsigenkänning och förklara utvecklingsprocessen. Autentiseringssystemet skulle skapa en tredimensionell modell av användarens ansikte och spara det på en server vid registrering. Vid autentisering skulle användaren läsa av sitt ansikte igen och skicka det till servern för jämförelse. Detta system har ett antal problem, för det första går det inte att ändra personliga egenskaper som används för biometrisk autentisering (Whytock,

2022). För det andra kan biometriska data som lagras på en server stjälas (Peterson, 2015). Stulen biometriska data kan användas av en inkräktare under offrets hela livstid (Chanthadavong, 2015). Under ett möte med min handledare upptäckte vi Web Authentication och jag började då utforska den metoden.

Jag har använt en *Yubikey Security Key* några månader på ett av mina konton och det har varit enkelt. Den fyrsiffriga koden är lätt att minnas och det går snabbt att logga in. Som det framkommit i studier känner även jag stress över att glömma lösenord och det är skönt att inte behöva minnas lösenord vid användning av en FIDO säkerhetsnyckel. Största orsaken till att jag beslutade mig för att börja använda en säkerhetsnyckel var inte för säkerheten utan för att slippa lösenord. Jag har på kontot helt tagit bort lösenord som autentiseringsmetod, detta är möjligt. Som reservmetod om jag skulle tappa min primära nyckel har jag en reservnyckel som jag lagrar säkert någonstans och Microsoft Authenticator på mobilen. En stor nackdel är förstås att om jag tappar nyckeln behöver jag manuellt radera den förlorade nyckeln från alla konton och köpa en ny nyckel och även registrera den på alla konton. Jag anser dock inte att det är ett troligt scenario att tappa bort nyckeln eller att få den stulen. Inte oroar man sig för att tappa bort sin hemnyckel heller.

8.1 Begränsningar och utmaningar

Web Authentication är ännu en väldigt ny metod och det kräver tid för att förändra människors uppfattning. Lösenord har varit en del av internet ända sedan dess uppkomst och det tar tid att förändra vanor. En annan orsak som gör det svårt att byta helt från användningen av lösenord till Web Authentication är att väldigt få tjänster stöder helt eliminering av lösenord. Många tjänster använder fortfarande lösenord som den primära autentiseringsmetoden och Web Authentication om det stöds endast som en två-faktor eller multi-faktor autentisering. Jag anser att det är även viktigt att lösa problem med återställning för att folk ska se Web Authentication som ett alternativ.

Som jag nämnde i sektion 6.4 anser jag att Microsoft har bäst stöd för Web Authentication för tillfället. Detta är på grund av att varje webbplats eller tjänst ansvarar själv för att

implementera hanteringen av autentiseringsuppgifter från Web Authentication fastän det existerar fullt stöd i webbläsarna. Det finns ingen garanti för att två tjänster har implementerat hanteringen på samma sätt eller ens korrekt. Detta är en brist och enligt mig en brist som inte går att eliminera helt. Det existerar dock bra bibliotek skrivna i många programmeringsspråk där stödet finns implementerat som är fria att användas av utvecklare och organisationer som önskar implementera stödet på sina webbplatser. Varje webbplats implementation av hanteringen behöver heller inte nödvändigtvis vara öppen källkod.

Autentisering med säkerhetsnycklar eller inbyggda autentiserare är ännu inte väl känt bland folk utanför kretsen av cybersäkerhet. För att få en bred användning av ny säker autentisering med FIDO är det viktigt att på ett lätt sätt kunna kommunicera åt folk utanför kretsen av cybersäkerhet varför nuvarande autentiseringsmetoder är bristfälliga, varför FIDO autentisering är säker, hur det funkar och hur det används.

Web Authentication inloggningsuppgifter är ”trust on first use” (TOFU) vilket betyder att förlitande part litar på alla nycklar vid registrering. Detta kan tillåta en förövare att via en man-in-the-middle attack byta ut offentliga nyckeln vid registrering och på så sätt registreras förövarens nyckel hos förlitande part i stället för den legitima användarens. Efter en säker registrering är nyckeln dock svår att manipulera eftersom det då finns en gemensam tillit på säkerhetsnyckeln (Lundberg, 2022).

Dokumentation för utvecklare är bristfällig, detta tror jag gör det svårt för mindre företag att implementera Web Authentication i sina tjänster och saktar ner en bredare ibruktagning av Web Authentication. Det har under tiden jag skrivit detta arbete varit svårt att hitta bra information om Web Authentication.

8.2 Fortsatt forskning

Vidare forskning om användbarhet och integritet skulle kunna utföras. Detta arbete har ytligt behandlat användbarhet men en mer utförlig undersökning skulle kunna göras. Web

Authentication påstås bevara användarens integritet, detta blev inte undersökt i detta arbete och skulle kunna vara ett ämne för vidare forskning.

Beteendebaserad autentisering skulle även vara ett intressant ämne att utforska och jämföra med Web Authentication. Beteendebaserad autentisering är en utvecklande teknik som baseras på användarens beteendemönster. Tekniken identifierar användarens regelbundenheter i hur användaren skriver och rör sig. Till skillnad från traditionella autentiseringsmetoder som autentiserar endast då åtkomst påbörjas så utför beteendebaserad teknik en kontinuerlig autentisering som utvärderar användarens nuvarande interaktioner med systemet i realtid (Plurilock, u.d.).

KÄLLOR

Acdx, 2008. *Digital Signature diagram.* [Online] Tillgänglig: https://commons.wikimedia.org/wiki/File:Digital_Signature_diagram.svg [Använd 24 3 2023].

Ackermann, Y., 2020. *Sorting FIDO/CTAP/WebAuthn terminologies.* [Online] Tillgänglig: https://medium.com/webauthnworks/sorting-fido-ctap-webauthn-terminology-7d32067c0b01
[Använd 8 3 2023].

Ackermann, Y., 2021. *WebAuthn/FIDO2: Demystifying attestation and MDS.* [Online] Tillgänglig: https://medium.com/webauthnworks/webauthn-fido2-demystifying-attestation-and-mds-efc3b3cb3651#4e03
[Använd 8 3 2023].

akshayku, 2021. *Syncing Platform Keys, Recoverability and Security levels.* [Online] Tillgänglig: https://github.com/w3c/webauthn/issues/1640
[Använd 14 3 2023].

Azad, T., 2008. *Securing Citrix XenApp Server in the Enterprise.* u.o.:u.n.

Bird, A., 2016. *Web Authentication Working Group F2F: March 4th San Francisco.* [Online]
Tillgänglig: https://www.w3.org/blog/2016/02/web-authentication-working-group-f2f-march-4th-san-francisco/
[Använd 3 4 2023].

Bonneau, J., Herley, C., Oorschot, P. C. v. & Stajano, F., 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *2012 IEEE Symposium on Security and Privacy*, pp. 553-567.

Bonneau, J., Herley, C., Oorschot, P. C. v. & Stajano, F., 2015. Passwords and the evolution of imperfect authentication. *Communications of the ACM,* Juli, 58(7), pp. 78-87.

Brand, C., 2020. *WebAuthn 101 - Demystifying WebAuthn.* [Online]
Tillgänglig: https://www.youtube.com/watch?v=RFACQvL_8S4
[Använd 7 3 2023].

Champion, M., Raman, T., Smith, B. & Lindemann, R., 2015. *Submission Request to W3C: FIDO 2.0 Platform Specifications 1.0.* [Online]
Tillgänglig: https://www.w3.org/Submission/2015/02/
[Använd 3 4 2023].

Chanthadavong, A., 2015. *Biometrics: The password you cannot change.* [Online]
Tillgänglig: https://www.zdnet.com/article/biometrics-the-password-you-cannot-change/
[Använd 8 4 2023].

Crum & Forster, 2018. *Two Factor Authentication.* [Online]
Tillgänglig: https://www.cfins.com/wp-content/uploads/2021/05/2FA-Instructions.pdf
[Använd 30 3 2023].

Das, A. o.a., 2014. The Tangled Web of Password Reuse.

Denyer, D. & Tranfield, D., 2009. Producing a Systematic Review. i: *The Sage handbook of organizational research methods.* u.o.:Sage Publications Ltd., pp. 671-689.

Docs, M. W., u.d. *Web Authentication API.* [Online]
Tillgänglig: https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API
[Använd 3 4 2023].

Engedy, B., 2018. *What's new with sign up and sign in on the web (Google I/O '18).* [Online]
Tillgänglig: https://www.youtube.com/watch?v=kGGMgEfSzMw
[Använd 7 3 2023].

ExpressVPN, 2022. *Survey: How much time do you waste resetting your passwords?.* [Online]
Tillgänglig: https://www.expressvpn.com/blog/survey-how-much-time-do-you-waste-

resetting-your-passwords/
[Använd 30 3 2023].

Fagan, M., Albayram, Y., Khan, M. M. H. & Buck, R., 2017. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences,* Issue 7.

Fenech, S., 2012. 55,000 Twitter user names and passwords leaked. *Tech Guide*, 9 Maj.

FIDO Alliance & W3C, 2019. *W3C and FIDO Alliance Finalize Web Standard for Secure, Passwordless Logins.* [Online] Tillgänglig: https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.en
[Använd 9 8 2022].

FIDO Alliance, 2020. *FIDO Alliance Debuts New Consumer Educational Site, loginwithfido.com, and New I-Mark Web Symbol.* [Online] Tillgänglig: https://fidoalliance.org/fido-alliance-debuts-new-consumer-educational-site-loginwithfido-com-and-new-i-mark-web-symbol/
[Använd 3 4 2023].

FIDO Alliance, u.d. *Alliance Overview.* [Online] Tillgänglig: https://fidoalliance.org/overview/
[Använd 3 4 2023].

FIDO Alliance, u.d. *FIDO Authentication A Passwordless Vision.* [Online] Tillgänglig: https://fidoalliance.org/fido2/
[Använd 8 3 2023].

FIDO Alliance, u.d. *FIDO2: Web Authentication (WebAuthn).* [Online] Tillgänglig: https://fidoalliance.org/fido2-2/fido2-web-authentication-webauthn/
[Använd 3 4 2023].

FIDO Alliance, u.d. *History of FIDO Alliance.* [Online] Tillgänglig: https://fidoalliance.org/overview/history/
[Använd 3 4 2023].

Florêncio, D. & Herley, C., 2007. *A Large-Scale Study of Web Password Habits*, Washington, USA: u.n.

Gong, H. L. V. o.a., 2015. *FIDO 2.0: Web API for accessing FIDO 2.0 credentials.* [Online]
Tillgänglig: https://www.w3.org/Submission/2015/SUBM-fido-web-api-20151120/
[Använd 3 4 2023].

Grassi, P., Garcia, M. & Fenton, J., 2017. NIST Special Publication 800-63-3.

Guirat, I. B. & Halpin, H., 2018. *Formal verification of the W3C Web Authentication.* Raleigh, USA, HoTSoS '18: Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security, pp. 1-10.

Halpin, H., 2016. *Web Authentication Working Group Charter.* [Online]
Tillgänglig: https://www.w3.org/2015/12/web-authentication-charter.html
[Använd 3 4 2023].

Hicock, R., 2016. *Microsoft Password Guidance.* [Online]
Tillgänglig: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf
[Använd 28 3 2023].

Hodges, J., Jones, J., Kumar, A. & Lundberg, E., 2021. *Web Authentication: An API for accessing Public Key Credentials Level 2.*. [Online]
Tillgänglig: https://www.w3.org/TR/webauthn-2/
[Använd 25 7 2022].

IBM, 2021. *Digital signatures.* [Online]
Tillgänglig: https://www.ibm.com/docs/en/ztpf/2020?topic=concepts-digital-signatures
[Använd 13 3 2023].

IBM, 2021. *Public key cryptography.* [Online]
Tillgänglig: https://www.ibm.com/docs/en/ztpf/2020?topic=concepts-public-key-cryptography
[Använd 13 3 2023].

IDG, 2016. *interoperabilitet.* [Online]
Tillgänglig: https://it-ord.idg.se/ord/interoperabilitet/
[Använd 8 5 2023].

Javatpoint, u.d. *Difference between Time-Sharing and Distributed Operating System.* [Online]
Tillgänglig: https://www.javatpoint.com/time-sharing-vs-distributed-operating-system
[Använd 8 5 2023].

Jung, J. & Shepherd, J., 2019. *What Is WebAuthn?.* [Online]
Tillgänglig: https://www.okta.com/blog/2019/03/what-is-webauthn/
[Använd 24 2 2023].

Larson, S., 2017. Every single Yahoo account was hacked - 3 billion in all. *CNN.*

Leuthvilay, L., 2019. *Study Finds 78% of People Reset a Password They Forgot in Past 90 Days.* [Online]
Tillgänglig: https://blog.hypr.com/hypr-password-study-findings
[Använd 30 3 2023].

Lundberg, E., 2022. *Yeah, the critical piece to realize is that all WebAuthn credentials are "trust on first use".* [Online]
Tillgänglig: https://github.com/w3c/webauthn/issues/1710#issuecomment-1082187565
[Använd 25 3 2023].

Lyastani, S. G. o.a., 2020. Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 268-285.

Malwarebytes, u.d. *What is a password manager?.* [Online]
Tillgänglig: https://www.malwarebytes.com/what-is-password-manager
[Använd 30 3 2023].

Mardini, A. & Kim, G., 2021. *Making sign-in safer and more convenient.* [Online]
Tillgänglig: https://blog.google/technology/safety-security/making-sign-safer-and-more-convenient/
[Använd 30 3 2023].

Masiliauskas, P., 2023. *Most common passwords: latest 2023 statistics.* [Online]
Tillgänglig: https://cybernews.com/best-password-managers/most-common-passwords/
[Använd 30 3 2023].

MDN Web Docs, u.d. *Web Authentication API.* [Online] Tillgänglig: https://developer.mozilla.org/en-US/docs/Web/API/Web_Authentication_API
[Använd 3 4 2023].

Melo, N., 2022. *WebAuthn Capabilities and Limitations.* [Online] Tillgänglig: https://www.beyondidentity.com/developers/blog/webauthn-capabilities-and-limitations
[Använd 13 3 2023].

Ometov, A. o.a., 2017. Multi-Factor Authentication: A Survey.

Ong, T., 2018. *Over 90 percent of Gmail users still don't use two-factor authentication.* [Online]
Tillgänglig: https://www.theverge.com/2018/1/23/16922500/gmail-users-two-factor-authentication-google
[Använd 30 3 2023].

OWASP, u.d. *Local Authentication on Android.* [Online] Tillgänglig: https://mobile-security.gitbook.io/mobile-security-testing-guide/android-testing-guide/0x05f-testing-local-authentication
[Använd 14 3 2023].

Parecki, A., 2018. *WebAuthn: A Developer's Guide to What's on the Horizon.* [Online] Tillgänglig: https://developer.okta.com/blog/2018/04/17/webauthn-developers-guide-to-whats-on-the-horizon
[Använd 27 3 2023].

Peterson, A., 2015. *OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought.* [Online] Tillgänglig: https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?noredirect=on
[Använd 8 4 2023].

Petrillo, K., 2018. *New Research: Psychology of Passwords, Neglect is Helping Hackers Win,* u.o.: u.n.

Plurilock, u.d. *Behavioral Biometrics.* [Online]
Tillgänglig: https://plurilock.com/what-is-behavioral-biometrics/
[Använd 7 4 2023].

Qiunn, R., 2012. 55K Twitter Passwords Leaked. *Newser*, 10 Maj.

Rawlings, R., 2020. *Password Habits in the US and the UK: This Is What We Found.* [Online]
Tillgänglig: https://nordpass.com/blog/password-habits-statistics/
[Använd 30 3 2023].

Rublon, 2022. *Almost Half of Companies Do Not Use MFA, 2022 Report Finds.* [Online]
Tillgänglig: https://rublon.com/blog/half-companies-do-not-use-mfa-2022/
[Använd 30 3 2023].

Seltzer, W., 2019. *Web Authentication Level 1 is a W3C Recommendation.* [Online]
Tillgänglig: https://www.w3.org/blog/webauthn/2019/03/10/web-authentication-level-1-is-a-w3c-recommendation/
[Använd 21 7 2022].

Seltzer, W., 2021. *Web Authentication Level 2 is a W3C Recommendation.* [Online]
Tillgänglig: https://www.w3.org/blog/webauthn/2021/04/08/webauthn-level-2-is-a-w3c-recommendation/
[Använd 21 7 2022].

Selyukh, A., 2017. Every Yahoo Account That Existed In Mid-2013 Was Likely Hacked. *NPR.*

Thomas, K. o.a., 2017. Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials.

Verizon, 2017. *2017 Data Breach Investigations Report.* [Online]
Tillgänglig: Tillgänglig:
https://www.verizon.com/business/resources/reports/2017_dbir.pdf
[Använd 2 3 2023].

Vigderman, A., 2023. *Password Manager Anuual Report 2022.* [Online] Tillgänglig: https://www.security.org/digital-safety/password-manager-annual-report/ [Använd 30 3 2023].

W3C, 2021. *W3C Process Document.* [Online] Tillgänglig: https://www.w3.org/2021/Process-20211102/ [Använd 26 7 2022].

W3C, u.d. *Standards FAQ - What does "Web standard" mean? What is a "Recommendation"?.* [Online] Tillgänglig: https://www.w3.org/standards/faq#std [Använd 26 7 2022].

Weatherbed, J., 2022. *A huge phishing campaign has targeted over 130 companies, affecting Twilio and Signal.* [Online] Tillgänglig: https://www.theverge.com/2022/8/26/23323036/phishing-scam-campaign-twilio-hack-companies [Använd 27 3 2023].

Weinert, A., 2019. *All your creds are belong to us!.* [Online] Tillgänglig: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/all-your-creds-are-belong-to-us/ba-p/855124 [Använd 30 3 2023].

Weinert, A., 2020. *It's Time to Hang Up on Phone Transports for Authentication.* [Online] Tillgänglig: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/it-s-time-to-hang-up-on-phone-transports-for-authentication/ba-p/1751752 [Använd 30 3 2023].

Whytock, P., 2022. *Think biometrics protect you from hacking…think again?.* [Online] Tillgänglig: https://www.electropages.com/blog/2022/07/think-biometrics-protect-you-hackingthink-again [Använd 8 4 2023].

Yubico, 2019. *Yubico's 2019 State of Password and Authentication Security Behaviors Report.* [Online]

Tillgänglig: https://www.yubico.com/press-releases/yubicos-2019-state-of-password-and-authentication-security-behaviors-report/
[Använd 30 3 2023].

Yubico, u.d. *Spare YubiKeys.* [Online]
Tillgänglig: https://www.yubico.com/spare/
[Använd 4 4 2023].

Yubico, u.d. *WebAuthn: Level 2 Features and Enhancements.* [Online]
Tillgänglig: https://developers.yubico.com/WebAuthn/Concepts/WebAuthn_Level_2_Features_and_Enhancements.html
[Använd 21 7 2022].

Yubico, u.d. *What is Passwordless?.* [Online]
Tillgänglig: https://www.yubico.com/resources/glossary/passwordless/
[Använd 28 3 2023].