

Når Passkeys ikke er et alternativ

Nedlåst etter beste evne

Sindre Olsen – Horten Kommune



HORTEN
KOMMUNE

\$whoami

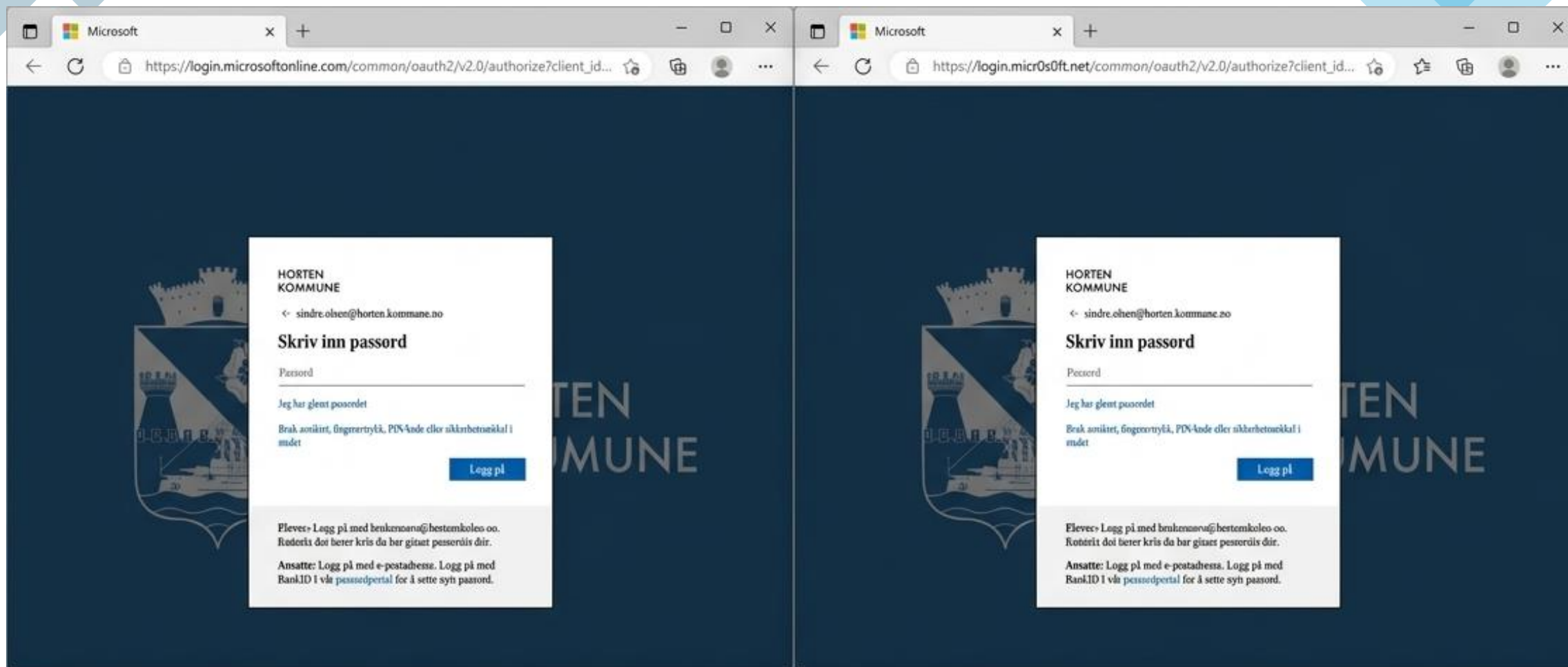
- IT sikkerhetsrådgiver (Horten Kommune)
- Master I CyberSecurity USN (Universitetet i Sørøst-Norge)
- Herding (AD, Entra, Klient, Server, Brannmur....)
- ROS
- Anskaffelser
- Oppfølging SIEM/SOC
- IoT
- ...



Agenda

- Hvorfor phishingresistent autentisering?
- Hva er passkeys (FIDO2)?
- MFA Metoder
- Når FIDO2 ikke lar seg innføre for alle
- Løsning: Enhetskrav og IP-filtrering
- Sikker sone: Ekstra sikkerhet for sensitive applikasjoner
- Implementering og utfordringer
- Oppsummering





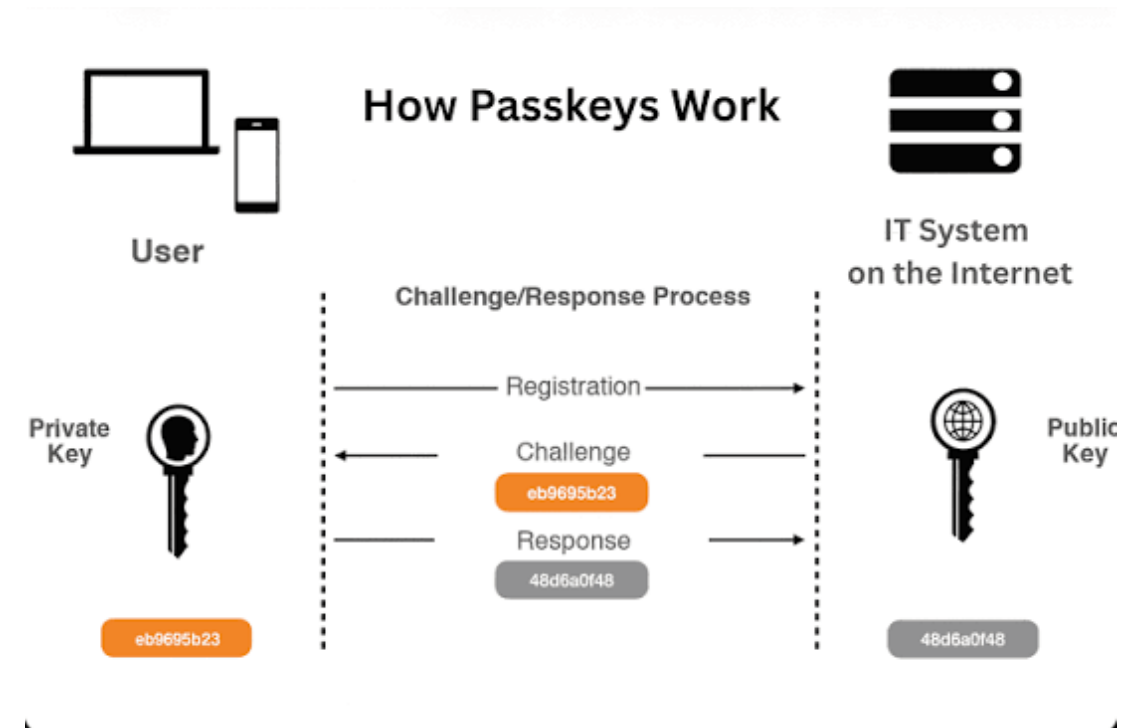
Hvorfor phishingresistent autentisering?

- Tradisjonell beskyttelse ikke godt nok -> MFA (Passord + Kode)
- Adversary-in-the-Middle (AITM) -> Omgår tradisjonell MFA
 - Angriperen plasserer seg usynlig mellom brukeren og påloggingssiden
 - Troverdige "Logg inn med Microsoft", company branding
 - Bare url er annerledes
 - Kan med dette:
 - Stjele brukerens passord
 - Fange opp og gjenbruke aktive påloggingssesjoner (sesjonstokens)
 - Omgå MFA-beskyttelse – selv med autentiseringsapp eller SMS
 - Gjennomføre angrepet uten at brukeren merker noe



Hva er Passkeys (FIDO2)

- Passkeys autentisering løser ATM-problemet
- Innloggingen er kryptografisk låst til den legitime tjenesten
 - Origin binding
- Fanget trafikk gir ingenting brukbart for angriper
- Virkemåte
 - Asymetrisk kryptografi og challenge/response
 - Privat nøkkel låses opp med pin/biometri
 - Signerer challenge fra server
 - Server verifiserer med offentlig nøkkel
- **Ingen secrets forlater enheten**
- **Funker kun for registrert origin**



Tilgjengelige løsninger - Passkeys (FIDO2)

Metode	Beskrivelse	Krav
Fysisk FIDO2-nøkkel (f.eks. YubiKey)	• Liten USB/NFC-brikke brukeren kobler til enheten ved innlogging • Høy sikkerhet • Fungerer på alle plattformer	• Anskaffes per bruker. Kost: 400–1 200 kr.
Microsoft Authenticator (passkey på mobil)	• Passkey lagret i Authenticator-appen • Samme sikkerhetsnivå som fysisk nøkkel • Krever mobil	• Smarttelefon (iOS/Android). • Gratis app.
Windows Hello for Business	• Innebygd løsning i Windows • Ansatte logger på med PIN-kode eller biometri i stedet for passord	• Krever at brukeren har en egen kommunal Windows-maskin
Synced Passkeys	• Ikke låst til enhet, synces på tvers • Mindre sikkert • Krever ikke Authenticator app	• IOS/Android enhet eller 3. parts passordwallet (Eks Bitwarden)



MFA-metoder

- Passkey (FIDO2)
- Windows Hello
- Microsoft Authenticator
- Temporary Access Pass
- SMS
- Software OATH tokens
- Voice call
- Email OTP
- QR code

MFA-metoder

- **Passkey (FIDO2)**
- **Windows Hello**
- ~~Microsoft Authenticator~~
- ~~Temporary Access Pass~~
- ~~SMS~~
- ~~Software OATH tokens~~
- ~~Voice call~~
- ~~Email OTP~~
- ~~QR code~~

Anbefalt

- Overgang til sikrere phishingresistent autentisering anbefales
 - Nasjonal sikkerhetsmyndighet (NSM)
 - [Anbefaler overgang til phishingresistent autentisering for alle virksomheter.](#)
 - Helse- og kommuneCERT
 - [Listet som anbefalt sikkerhetstiltak i Nasjonalt beskyttelsesprogram \(NBP\).](#)
 - [NHN - Solid innlogging](#)
 - Microsoft gjør Passkeys til standard, avvikler gratis SMS og Tale autentisering
 - [Passkeys by default and retirement of Microsoft-provided SMS and voice authentication](#)



Solid innlogging

- Krev FIDO2
- Kombiner passord med godkjent enhet
- Kombiner passord med godkjent IP

Solid innlogging

For å sikre innlogging mot AitM-phishing må alle brukere sikres på en av tre måter.

Solid innlogging er viktig generelt, men er spesielt relevant for Conditional Access i Entra ID.

1. Krev FIDO2-autentisering

FIDO2 (Fast Identity Online 2) er en standard for autentisering som, gjennom design, sikrer mot phishing. I FIDO2 bruker man passnøkler for å holde påloggingsnøkler, her opprettes en ny nøkkel for hver side. Disse passnøklerne kan være fysiske, for eksempel USB-nøkler, TPM-chip på maskiner, eller bygd inn i mobiltelefoner. De kan også være heldigitale. For eksempel tilbyr mange passordmanagere nå også å opprette og håndtere passnøkler. Rent generelt er fysiske sikrere enn digitale, mens digitale er mer brukervennlige. Fysiske har også en høyere kostnad. Begge typene gir god beskyttelse mot phishing.

2. Kombiner passord med godkjent enhet

Bruk tradisjonell innlogging (brukernavn og passord), men krev at innloggingen kommer fra en godkjent enhet. Typisk vil man kjenne igjen godkjente enheter med bruk av sertifikater på enheten. Dette kan være en løsning man ordner selv, eller for eksempel innrullert eller registrert som i Microsofts løsning. Denne metode sikrer mot at angriper kommer seg inn i systemene dine, men har ulemper i form at behov for å vedlikeholde hvilke enheter som er godkjente. Metoden hindrer heller ikke at passord kommer på avveie.

3. Kombiner passord med godkjent IP

Bruk tradisjonell innlogging (brukernavn og passord), men krev at innloggingen kommer fra en godkjent lokasjon (IP). Typiske godkjente IP-er vil da være kontornettverket ditt eller IP-adresser brukt om man kobler seg til via virksomhetens VPN. Åpning for alle norske IP-er er ikke tilstrekkelig. NB! Vi har tidligere oppgitt at godkjente IP-er også kan være ansattes hjemmelPer, det er nå tatt ut av anbefalingen på grunn av risikoen for at det kjører residential proxy-software på utstyr i hjemmet til den enkelte ansatte, samt bruk av CGNAT som gjør at mange husstander benytter samme IP-adresse. Metoden sikrer mot at angriper kommer seg inn i systemene dine, men har ulemper i form av vedlikeholdskostnad med IP-lister og at passord fortsatt kommer på avveie ved phishing.

Metodene kan også kombineres hvor man gir tilgang om innlogging kommer fra en godkjent IP, eller godkjent enhet eller med FIDO2-nøkkel.



Når Passkeys (FIDO2) ikke lar seg innføre for alle

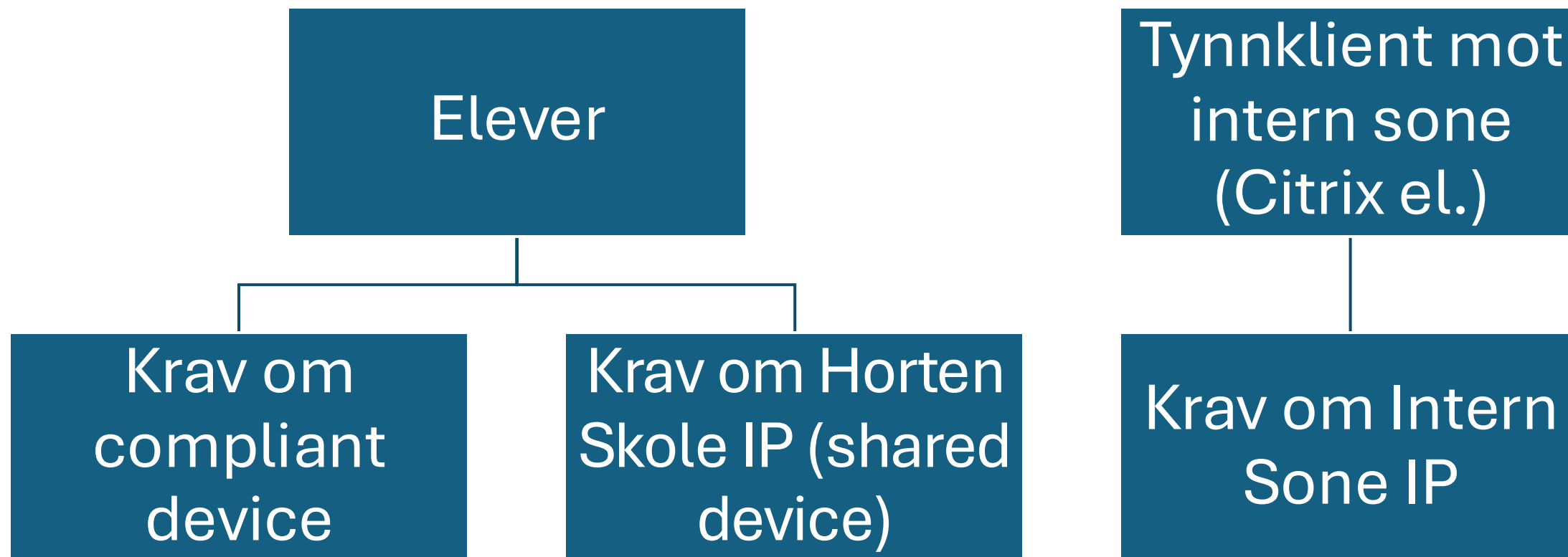


Elever -> WHFB (TUNGVINT INNRULLERING), DELTE NETTBRETT...



Brukere av tynnklient -> Fysiske FIDO nøkler (kostnad), MS Authenticator Passkey kan ikke benyttes

Løsning: Enhetskrav og IP-filtrering



Sikker sone: Ekstra sikkerhet for sensitive applikasjoner

Ekstra
sensitive
applikasjoner

Krav om egen
sikker sone
IP



CA01 Krev phishingresistent autentisering

Inkluder alle brukere, apper og nettverk

Unnta elever, andre unntaksgrupper og Intern+Sikker sone named locations

**Intern Sone
Apps/Nettverk**

CA02 Krev Intern Sone IP for Citrix Apps/Nettverk

Inkluder Citrix Apps/Nettverk

**Sikker Sone
Apps/Nettverk**

Elever

CA04 Krev Compliant Device for elever

Inkluder Citrix Apps/Nettverk

CA03 Krev Sikker Sone IP for Sikker Citrix Apps

Inkluder Citrix Sikker Apps/Nettverk



Identity

Select identity type *

Users

User *

Edit user

Target resource

Select target type *

Cloud apps

Cloud apps *

+ Select cloud app

Sign-in conditions

Device platform *

Select device platform...

Client app *

Select a client app...

Authentication flow

Select authentication flow...

Insider risk

Select Insider risk...

Sign-in risk

Select sign-in risk...

User risk

Select user risk...

IP address

Enter IP address (ex. 40.77.182.32)

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Conditional Access

Conditional Access | Policies

Microsoft Entra ID

+ New policy

+ New policy from template

Upload policy file

What if

Refresh

Preview features

Got feedback?

Overview

Policies

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. [Learn more](#)

What if

Reset

Evaluation result

Classic policies are not evaluated by this tool.

Policies that will apply

Policies that will not apply

Search

3 policies found

Display name ↓	Grant controls	Session Controls	State	Has filter? ⓘ
CA06 - All apps: Block access from any location except Scandinavia for everyone	Block access		On	No
CA08 - All apps: Sign-in frequency		Sign-in frequency - 90 days	Report-only	No
CA09 - All apps: Global MFA Enforcement	Authentication strength - Multifactor authentication		On	No

Implementering og utfordringer

- Bygg lagvis
 - FIDO først
 - Unnta enkelte grupper, nettverk, apper -> Inkluder i andre policier
 - Bruk "**What if**"-verktøyet for å sjekke at det treffer, og at man ikke lager utilsiktede hull
 - <https://learn.microsoft.com/en-us/entra/identity/conditional-access/what-if-tool>
 - Noe er bedre enn ingenting -> ikke vent til alle kan ha passkeys
- Utfordringer
 - Applikasjoner uten federert autentisering ("Logg inn med Microsoft")
 - IP Filtreering i Brannmur for lokale applikasjoner
 - Etterspør IP filtrering hos leverandør av SaaS tjenester
 - Blokkering av applikasjon i sin helhet, ikke bare ved autentisering

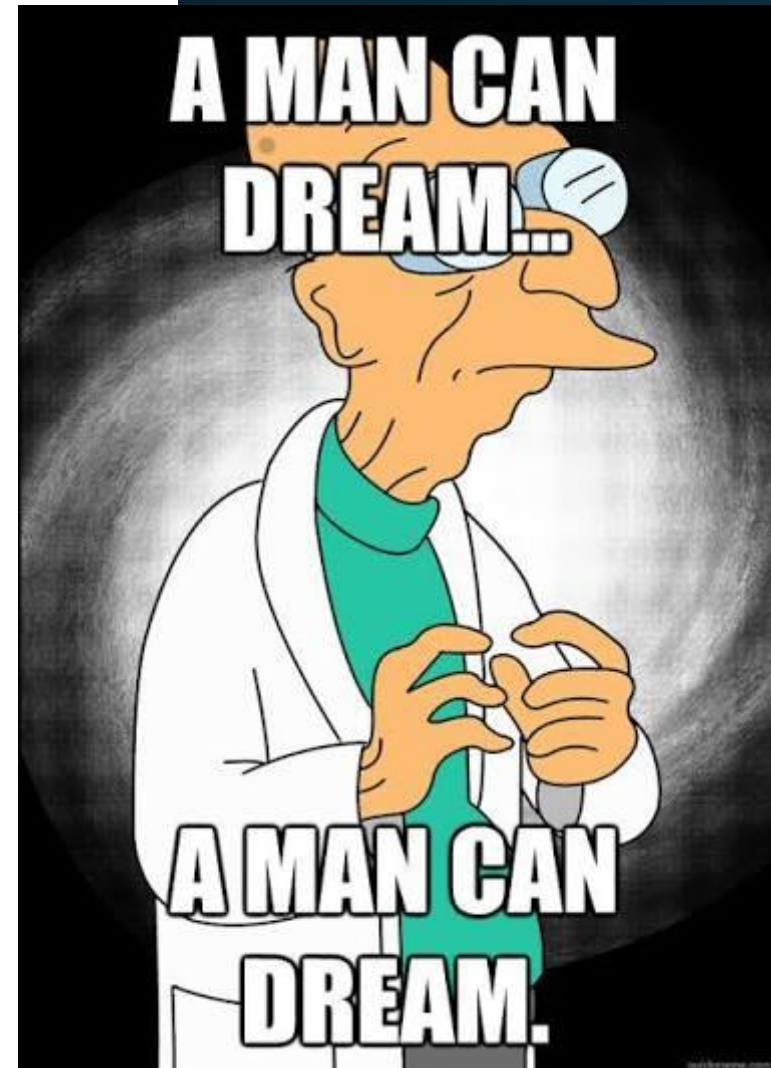


MFA metoder

- Passkey (FIDO2)
- Windows Hello
- Microsoft Authenticator <3
- Temporary Access Pass
- ~~SMS~~
- ~~Software OATH tokens~~
- ~~Voice call~~
- ~~Email OTP~~
- ~~QR code~~

Oppsummering

- Målet forblir passordløs autentisering
- Ikke alle systemer er klare for det
- Enkelte brukergrupper er kanskje ikke klare
- Anbefaling
 - Phishingresistent for alle som kan ha det
 - Benytt kombinasjon av compliant device og IP filtrering der det ikke er mulig
 - Deaktiverer gamle "svake" MFA metoder
- Sikkerhet bygges lagvis



Spørsmål?

- <https://www.nhn.no/tjenester/helsecert/nasjonalt-beskyttelsesprogram-nbp/anbefalte-sikkerhetstiltak/solid-innlogging>

