Passkeys

Kins 2024

PASSKEYS

Hi there, hello!

```
Navn        : Per-Torben Sørensen
Alder       : 45
Bor         : Kristiansand
Titler      : MCT, MCSE M365
Bakgrunn    : Forsvaret, Ventelo, EVRY, Advania, rewired
Jobber som  : Teknisk arkitekt @ Crayon
XP          : 25 års erfaring med Micosoft
👍          : Microsoft 365, sikkerhet, PowerShell og 🌞
👎          : Usikre og gamle IT løsninger og ❄️
Blogg       : agderinthe.cloud
LinkedIn    : https://www.linkedin.com/in/pertorbensorensen
```

Crayon

15.Oktober 2024 - aka.ms/mfaforazure & AgderInThe.cloud

- MFA blir OBLIGATORISK
  - Azure admin portal
  - Entra ID (Tidl Azure AD) admin portal
  - Intune admin portal
- Husk «Break-glass» (nødtilgang) konto!
  - Sett opp FIDO2 på denne!
- «Tidlig 2025»:
  - Azure CLI
  - Azure PowerShell
  - Azure mobile app
  - Infrastructure as code (IaC) verktøy

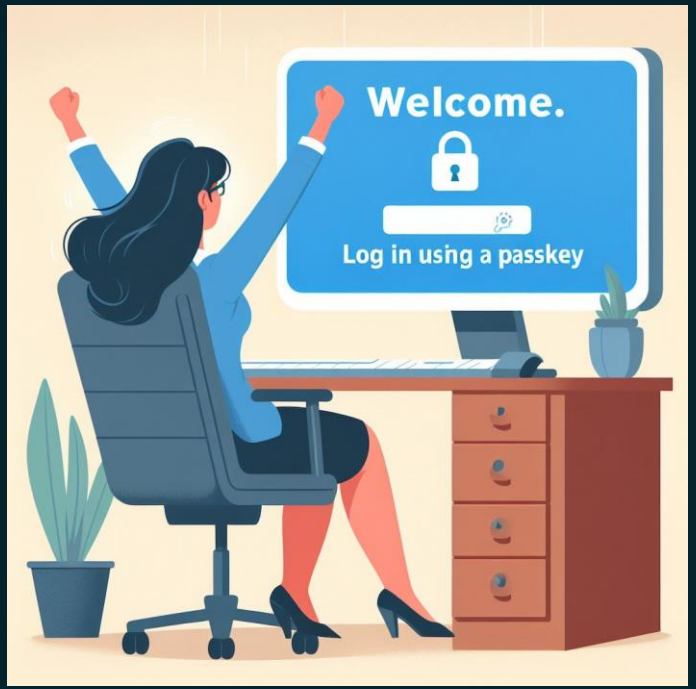
Crayon

Agenda

- ❑ Hva er passkeys?
- ❑ Hvorfor trenger vi passkeys?
- ❑ DEMO

PASSKEYS

Hva er passkeys?



- Fra FIDO alliansen
  - Allianse for alternativer til eller erstatte passord
  - Metoder som er sikrere og enklere enn passord
- Passkeys basert på asymmetriske nøkler
- I stor vekst, tilgjengelig hos mange leverandører
- Kan sees på som software-versjon av FIDO2 nøkler

Crayon

PASSKEYS

Asymmetriske nøkkelpar

- Asymmetrisk kryptering bruker nøkkelpar:
  - En offentlig nøkkel og en privat nøkkel
  - Globalt unike
- Offentlig nøkkel deles fritt

- Privat nøkkel blir hos eieren og eksponeres ALDRI

- Hvis data er kryptert/signert med offentlig nøkkel:
  - ❌ Den samme offentlige nøkkelen kan IKKE dekryptere/verifisere
  - ✅ Bare den tilhørende private nøkkel kan dekryptere/verifisere
- Hvis data er kryptert/signert med privat nøkkel:
  - ❌ Den samme private nøkkelen kan IKKE dekryptere/verifisere
  - ✅ Bare den tilhørende offentlige nøkkelen kan dekryptere/verifisere

Crayon

PASSKEYS

Passkeys opprettelse

- Logger inn med MFA for å opprette en passkey
  - Genereres lokalt på klienten
- Public key kopieres til skytjenesten
  - Domain-bound – fungerer bare på et domene
  - Opprettes lokalt og sendes over
- Private key lagres på egen enhet
  - PC / mobil / osv
  - Eksponeres **ALDRI**
- HUSK: Private og Public key er unike men hører sammen

Crayon

PASSKEYS

Passkeys generelt - pålogging

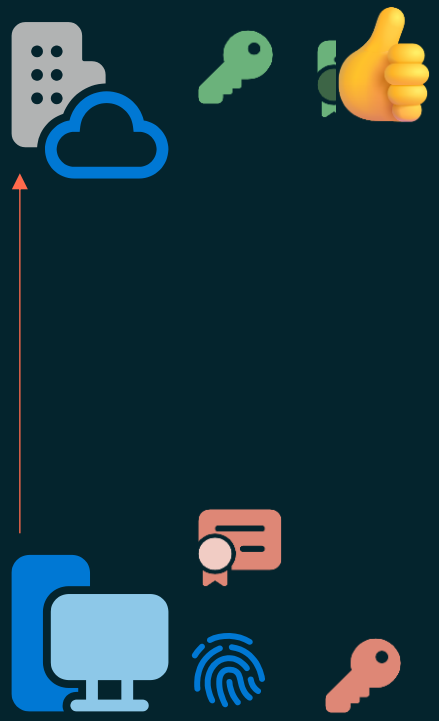
1. Bruker ønsker å logge inn på en skytjeneste med en passkey.

2. Skytjenesten generer en random challenge og signerer med sin Public key og sender til klienten med en credential ID

3. Bruker verifiserer seg **lokalt** med PIN eller biometri for å aktivere Private key

4. Private key verifiserer signatur, signerer challenge og sender den i retur med brukernavn og credential ID (bare gyldig 1 gang)

5. Skytjenesten verifiserer signaturen, sjekker credential ID og gir session token



Crayon

Agenda

- ✓ Hva er passkeys?
- ❑ Hvorfor trenger vi passkeys?
- ❑ DEMO

Lange passord hjelper ikke

2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years

2023

99,978%

2023 (ChatGPT hardware)

9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months

Crayon

PASSKEYS

Hva med passord + MFA?

- Passord kan gjettes/stjeles og brukes overalt
- Enhver MFA er bedre enn ingen MFA!
- MEN!
- Store forskjeller i sikkerhet på MFA metodene.
- «Tradisjonell» MFA sårbar for phishing angrep og SIM-swapping

Crayon

PASSKEYS

Hvorfor er passkeys bedre??

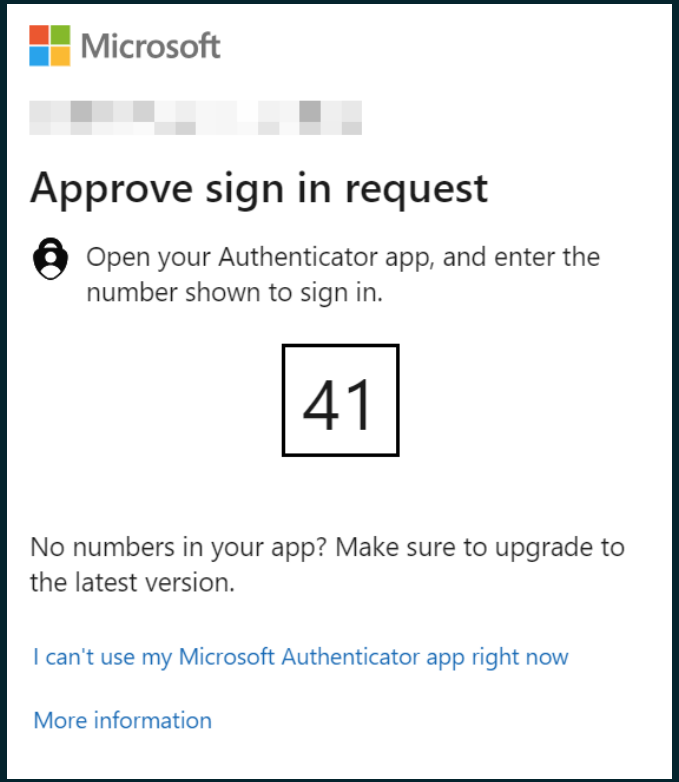
- Passord-fri autentisering
  - Phishing-resistant
  - Replay-resistant
  - Man-in-the-middle-resistant
  - Kan ikke gjettes
  - Kan ikke stjeles
- Krever normalt ikke innkjøp av hardware eller lisenser
- Autentiseringen skjer automatisk, sluttbruker bruker kun PIN/biometri
- Ingen data over nettverket som kan avlyttes og så gjenbrukes
- PIN/biometri er knyttet til enheten
- Passkey er låst til et bestemt domene (f.eks. login.microsoft.com)
- Cross-platform

Crayon

PASSKEYS

Passkeys i Entra ID er litt spesiell 🥲

- Public preview siden midten av April
  - Virker stort sett bra, noe ustabilitet
  - Ikke så brukervennlig som det burde være (demo straks)
- Kan ikke bruke passkeys for selve innloggingen på klienten
- Støtter BARE passkeys lagret i Microsoft Autheticator mobil app 😲
  - Android 14
  - iOS 17
- Brukere uten mobil kan ikke bruke passkeys (skoleelever) 😳



Crayon

Agenda

- ✓ Hva er passkeys?
- ✓ Hvorfor trenger vi passkeys?
- ❑ DEMO

DEMO – Passkeys – 2 tilnærminger

Generisk webside

Visma

Github

o.l.

Entra ID

Entra ID admin portal

Crayon

PASSKEYS

Fremtiden for passkeys i Entra ID

- Passkeys er et VELDIG bra tiltak som øker identitetsikkerheten betraktelig!
  - Begynn i dag!
- Synkronisere passkeys i Authenticator app
- Logge inn på PC med passkey? – «Vi ser på dette»
- Lagre passkey direkte på klienten?

Microsoft Entra: Expanded support for device-bound passkeys in Microsoft Entra ID

Microsoft Entra ID will add support for device-bound passkeys stored on computers and mobile devices as an authentication method in preview, in addition to the existing support for FIDO2 security keys. This enables users to perform phishing-resistant authentication using the devices that

Crayon

Til slutt

«If you want to go fast,

go alone.

If you want to go far,

go together!»

Crayon

- Link til DEMO:

- https://youtu.be/N73RUXqovqk?si=MrtZL26wl5Nl5x23

Crayon

TAKK FOR MEG!

PER-TORBEN SØRENSEN

Crayon