Tofaktorprosjektet: Ikke helt i mål, men…

Prosjektleder Frank Paul Silye
Seksjon for digitale kommunikasjonsplattformer

Tidslinje

1

MS365
Ansatte, studenter og tilknyttede

2

Feide
Sikt hadde en pågående pilotering av Feide med 2FA fra Azure AD

3

Tjenester kom underveis
2FA for RDP, VPN, Horizon og SSH

4

E-post og kalender
Exchange on-prem og dens protokoller

5

Oppsummering
Hva har vi sammen oppnådd og hva gjenstår?

MFA for MS 365

En litt rotete start!

Multi Factor Authentication

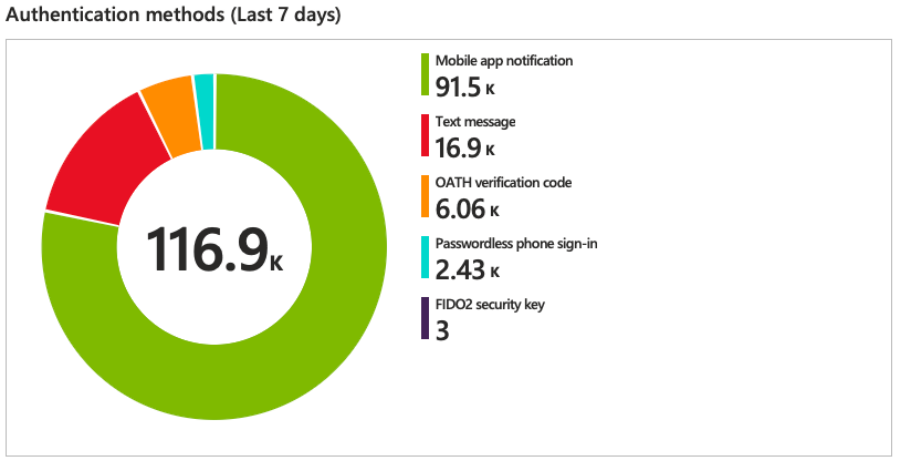
- **Azure AD** var valgt som 2FA-løsning
- Microsoft har som ellers flere løsninger, også for 2FA
  - For UiO - eneste mulige valg: 2FA med **conditional access**
- **USIT** og **IT-organisasjonen** var piloter
  - Første pilot avdekket problemer med **veiviser for MFA-oppsett**
  - Ingen leste dokumentasjonen og "alle" valgte feil oppsett: SMS
  - Vi fikk aktivert ny veiviser før Microsoft prodsatte den for vår tenant
  - En bedre utrulling ble så gjort på TF

MFA – MS 365 (Valg av 2FA-applikasjon)

- Prosjektet fikk kritikk for applikasjonene som kunne brukes
  - Kun fulgt **LSIS og dens godkjente applikasjoner**
    - Microsoft Authenticator, Google Authenticator, Enpass eller Authy
    - Regner med at flere bruker ikke-godkjente løsninger:
      - Passwords innebygget i macOS/iOS
      - Bitwarden, 1Password m. fl.
    - IT-sikkerhet kommer til å revidere listen
  - Prosjektet var klar over at ikke alle ville bruke **privat telefon** med applikasjon installert
  - 2FA fra applikasjon på egen datamaskin er problemfullt for dem som bruker flere maskiner
  - Programmerbare hardware token ble derfor bestillt opp

Litt om bruken av 2FA-applikasjoner

- Veilederen favoriserer Microsofts egen Authenticator
  - **80%** av brukermassen bruker den
    - 78% - **pushvarsel**, men informasjon om tjenesten varslet kommer fra
    - 2% av brukermassen kjører **passwordless**
  - **15%** bruker **SMS**
    - Mindre trygt
    - I 2020 begynte Microsoft å anbefale at en ikke bruker 2FA med SMS
  - **5%** bruker en **TOTP-klient**



Litt om utrullingen

- Utrullingen for MS 365 må med retrospektive øyne sies å ha gått bra
- Først fakultetsvis utrulling til **ansatte**
  - 4.574 brukerkontoer fikk 2FA aktivert
- Så **Tilknyttede**
  - Tilknyttede hadde så langt hatt en gratis A1-lisens. Problemet var at **MFA med conditional access ikke var inkludert** og tilleggslisens måtte kjøpes for 4.500 brukere
- Til slutt **studenter** - hvor vi klarte å ta hensyn til eksamensavviklingen

Feide med Azure AD

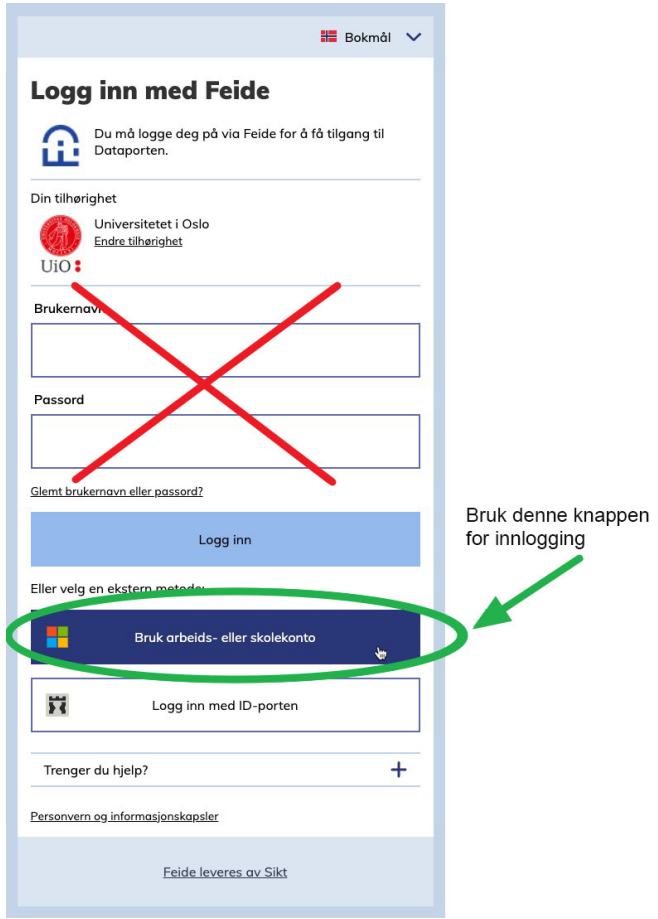
Og rotet fortsetter…

Sikt piloterte 2FA med ID-porten og Azure AD

- UiO deltok kun i pilotering av ID-porten
- Ca. 20 institusjoner var med og piloterte 2FA med Azure AD i Feide
  - UiO kom med i pilotens siste fase
- Tofaktorprosjektet trodde lenge at en kunne pilotere Feide med Azure AD på et par utvalgte tjenester
  - Realiteten var at Feide med Azure AD ville komme opp som autentiseringsløsning for alle UiOs tjenester
- Utfordringene stoppet ikke der...

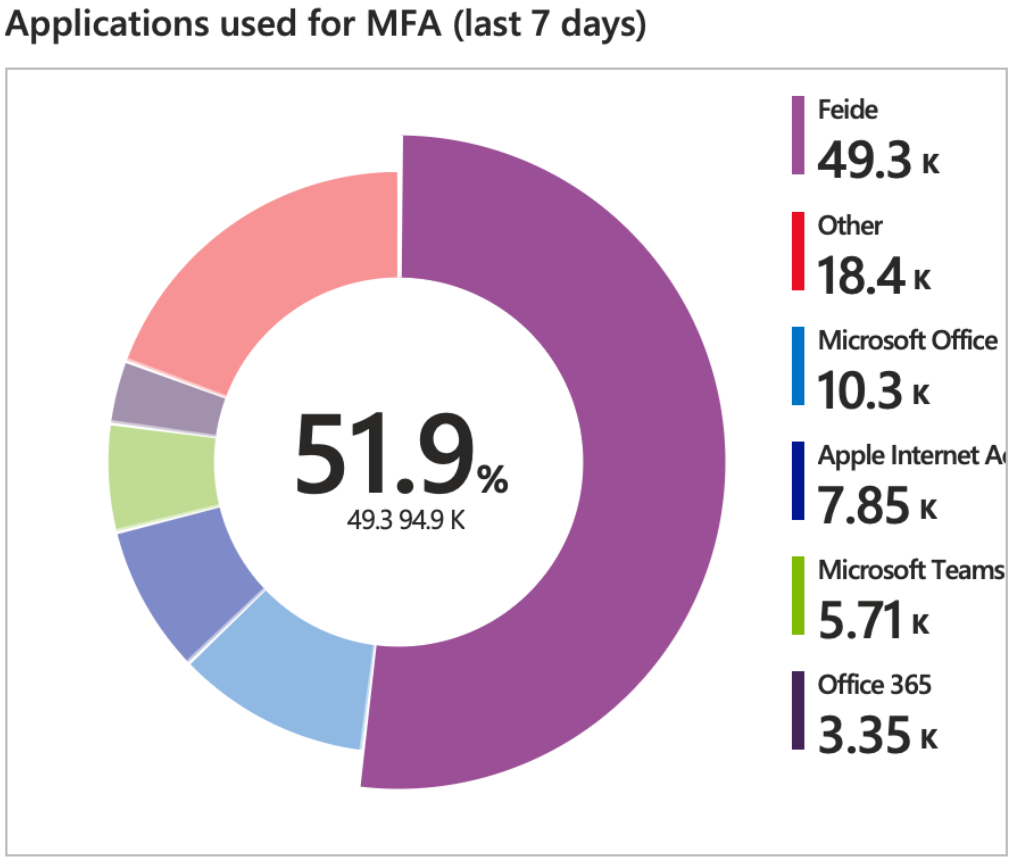
Feide med 2FA fra Azure AD

- Implementasjonen ga en **virkelig dårlig brukerreise** om en ikke samtidig som en lanserte Feide med Azure AD, deaktiverte den gamle og godt innarbeide måten å logge seg på
- Ved aktivering av Feide med Azure AD ville den gamle påloggingsløsningen tilby en annen 2FA-løsning
- Gammel påloggingsløsning ble deaktivert søndag kveld 19. juni
- Mandag morgen møtte alle brukere:
  - **«Bruk arbeids- eller skolekonto»**, og
  - UiO hadde 2FA på alle tjenester med Feide-pålogging



Feide med 2FA fra Azure AD

- 1. juli 2022: **17.500** brukerkontoer aktivert 2FA
- 11. august 2022: **23.500** brukerkontoer
- I dag utgjør **Feide 52%** av det totale antallet autentiseringer mot Azure AD



Feide med 2FA fra Azure AD

- Med **Conditional Access** som 2FA-løsning kunne vi styre hvor det skulle avkreves 2FA, og dermed **frita 2FA-kravet i Silurveien**
  - Under eksamen skal kandidatene ikke ha tilgang til mobiltelefoner eller smarteklokker
- For Silurveien jobbet prosjektet sammen med OSLOMET, som også gjennomfører eksamener der
  - OSLOMET kunne etter dette også skru av gammel pålogging i Feide

Andre tjenester underveis

Remote Desktop Connection, Horizon og SSH

Prosjektet var i gang, og mye vil ha mer

- Prosjekteier fikk etter hvert **blod på tann** og ville ha **tofaktor på mer...**
- Fjernpålogging til ens klientmaskiner og servere er utsatte angrepsflater
- Aktiviteter gjennomført som del av sikker oktober 2022:
  - **Remote Desktop Connection** – gammel teknologi hvor en bruker radius server til å avkreve 2FA
    - Virker **kun med Microsoft Authenticator**
    - Får ikke info om at du må gjøre 2FA på din telefon
    - Telefonen får ikke samme gode push varslet som andre tjenester
  - **view.uio.no** – var under stadig angrep og vi fikk satt tjenesten bak 2FA
  - **Microsoft Enterprise SSO plug-in for macOS** for Office 365 apps og Safari
  - Innføring av **Number Matching for Microsoft Authenticator**
  - **32.000** brukerkontoer hadde nå tatt i bruk 2FA
- **vpn.uio.no** – AnyConnect fikk 2FA
- **SSH** med login og rlogin, senere andre ssh-servere (utenfor prosjektet)

E-post og kalender

UiO er ikke i skyen… , så mer rot!

2FA på e-post og kalender

- Jeg er ærlig og sier sikkert litt for mye, og kommer kanskje til å bli sitert på det
- Prosjektet var fra dette punktet ikke lenger et prosjekt, prosjektdeltakerne som hadde vært med fram til da, kunne ikke lenger hjelpe i samme grad
- Har blitt et løp som i stor grad er gjort og gjøres i Seksjon for digitale kommunikasjonsplattformer (DKP), men hvor IT-hjelpen har blitt ytt av dere

2FA på e-post, Exchange on-prem

- Nå var det bare å aktivere 2FA på Exchange...
- Innkommende e-post håndteres over flere protokoller:
  - **MAPI** – Outlook for Windows-maskiner
  - **EWS** (Exchange Web Services) – E-postklienter på **datamaskiner** (Apple Mail, Outlook for macOS, Evolution m. fl.)
  - **EAS** (Exchange Active Sync) – E-postklienter for **mobile enheter** (Apple Mail og Gmail)
  - **IMAP** (Thunderbird med venner)

2FA på e-post, Exchange on-prem

- **MAPI** – vi har flere tusen maskiner med modern auth aktivert for Outlook og 2FA avkreves
  - Funnet 550 maskiner med autologon (går ikke fra **nego** til **bearer**)
  - **autologon** virker ikke å være dokumentert fra Microsoft
- Noen Outlook-brukere fikk EWS-problemer (plugin-problematikk?)

Authn

The method of authentication used. Meaning how Outlook passes your credentials to the mailbox.

- CLEAR or Clear*- (meaning Basic Authentication which is being turned OFF for Microsoft hosted mailboxes and needs updating)
- NTLM
  - For older Exchange Server connections we've seen CLEAR (NTLM)
- NEGO
- KERBEROS
- ANONYMOUS
- AUTOLOGON

Not documented by Microsoft properly but used with Microsoft hosted mailboxes are:

- MSA* meaning MicroSoft Account login
- Bearer* denotes Modern Authentication

Som **Office-Watch** skriver det...

Incomplete documentation

Microsoft's documentation for Connection Status is **woefully incomplete and out-of-date**.

"**Description of the Connection Status dialog in Outlook**" was supposedly updated in July 2022 but doesn't look it. There are vital but missing details about modern connections to Microsoft's own hosted systems. We're talking about details that have been in place for some years yet still not made it to the documentation.

https://office-watch.com/2022/discover-mailbox-connection-details-outlook/

E-postklienter på datamaskiner

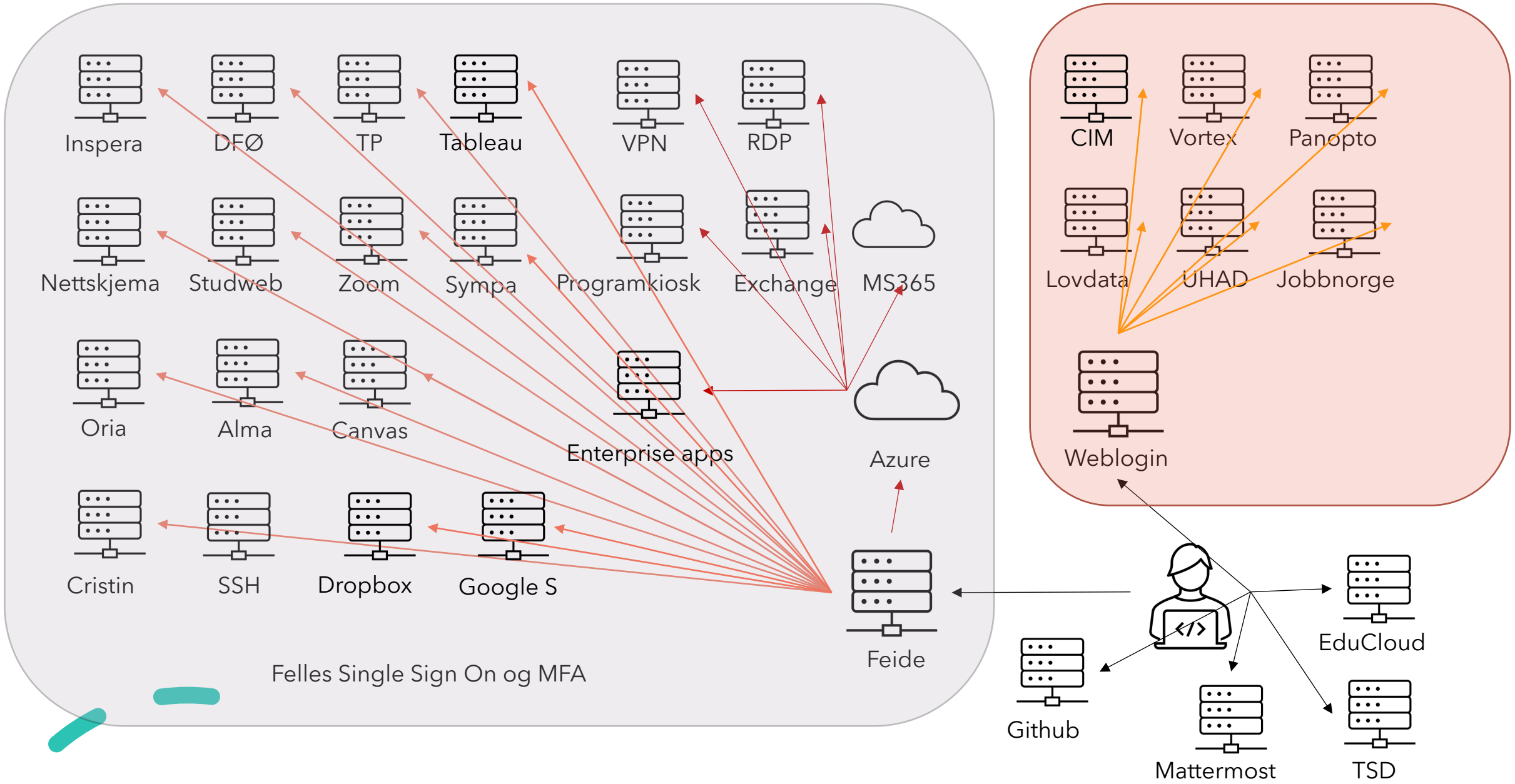
- **EWS**
  - **Mac i AD**
    - Nettverkskontoer får ikke modern auth på Apple Mail og 2FA!
    - **Flerbruksmaskiner** bundet til AD må ha **mobile accounts**
    - På stasjonær enbrukermaskin i AD må IT-ansatte aldri være den første som logger seg på
  - **Gnome Evolution**
    - Eneste støttede fullverdige e-post og kalenderklienten for Linux
    - Fungerer bra for noen – andre må reautentisere hele tiden
    - Når vi gjorde modern auth obligatorisk, fikk vi autodiscover-problem når en setter opp klienten - får ikke nødvendig token

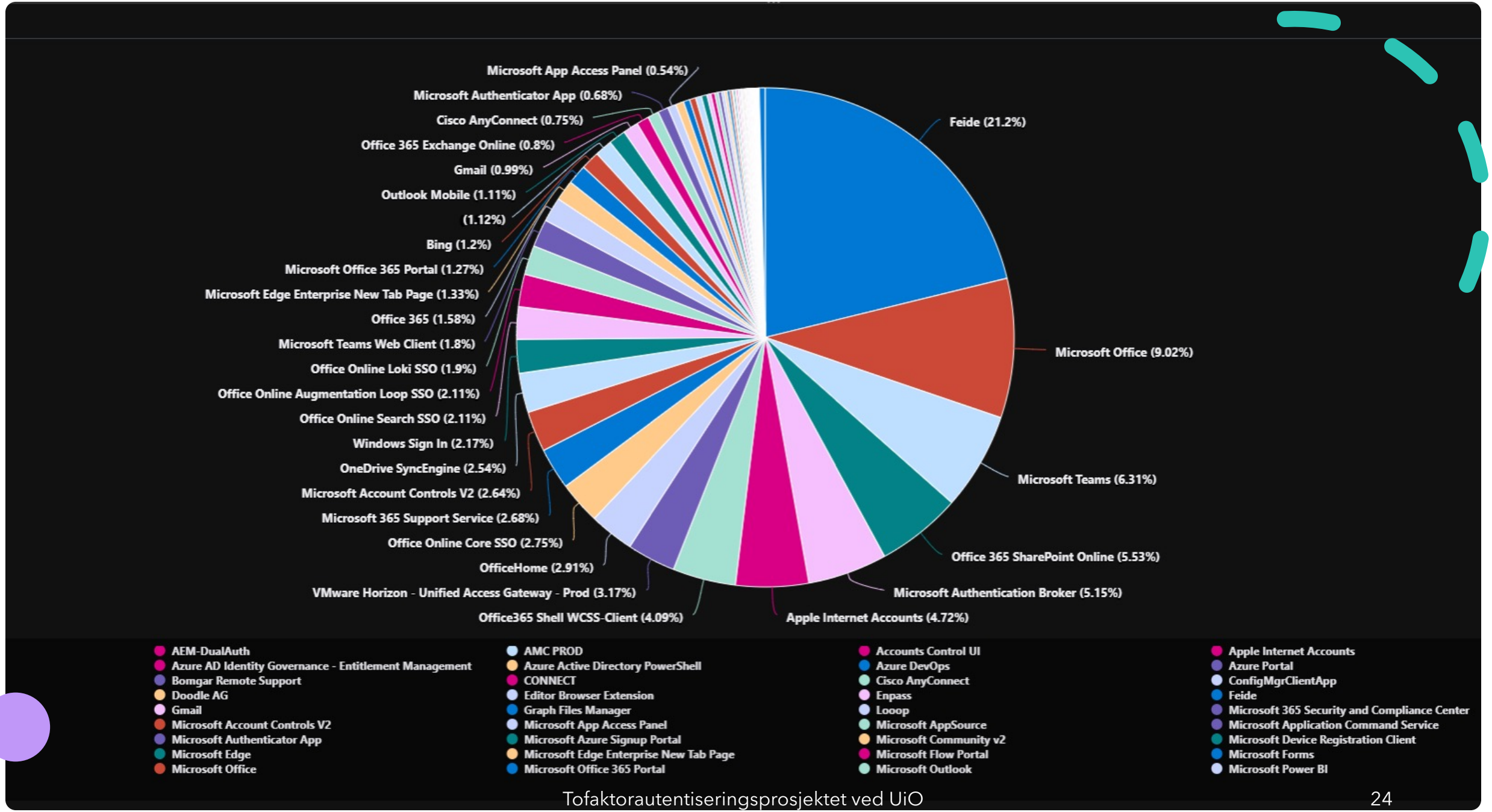
2FA på e-post, Exchange on-prem

- Og videre,
  - Ingen konsulenthjelp - Vi kan bare sky!
  - Microsoft «pusher» oss mot skyen...
    - Utviklet løsning for silent aktivering av modern auth for Apple Mail (macOS og iOS) sammen med Apple – virker bare for Exchange Online
    - Thunderbird har OAUTH2-støtte (for 2FA), det er ikke OAUTH2-støtte for Exchange on-prem. Kun i sky!
    - Thunderbird med SSH – ingen god brukeropplevelse
    - Mange bruker IMAP med annen e-postklient – på både datamaskin og mobile enheter

Oversikt - Status

Hva har vi oppnådd og hva gjenstår?


Inspera
DFØ
TP
Tableau
VPN
RDP
Nettskjema
Studweb
Zoom
Sympa
Programkiosk
Exchange
MS365
Oria
Alma
Canvas
Enterprise apps
Azure
Cristin
SSH
Dropbox
Google S
Feide
Felles Single Sign On og MFA
CIM
Vortex
Panopto
Lovdata
UHAD
Jobbnorge
Weblogin
Github
EduCloud
Mattermost
TSD

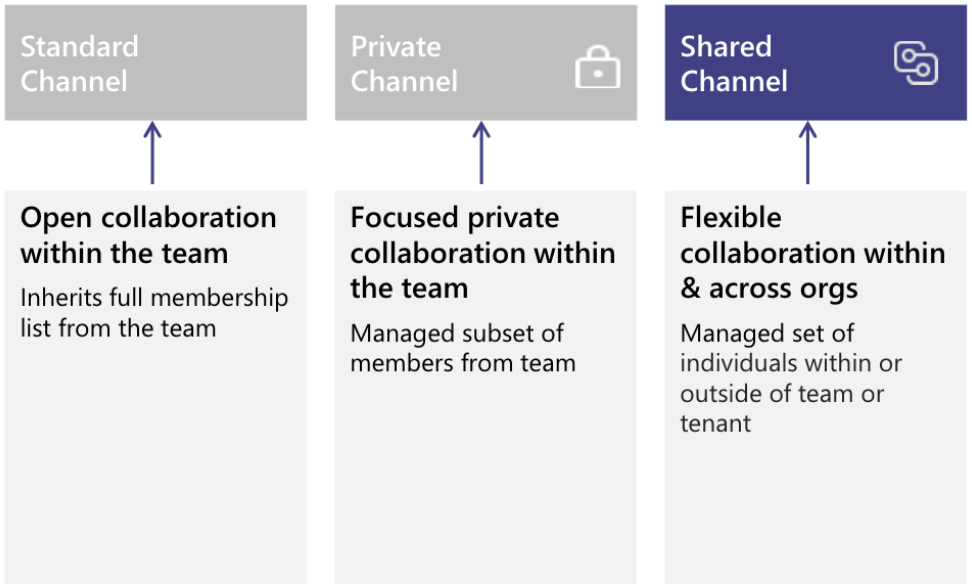

Microsoft App Access Panel (0.54%)
Microsoft Authenticator App (0.68%)
Cisco AnyConnect (0.75%)
Office 365 Exchange Online (0.8%)
Gmail (0.99%)
Outlook Mobile (1.11%)
(1.12%)
Bing (1.2%)
Microsoft Office 365 Portal (1.27%)
Microsoft Edge Enterprise New Tab Page (1.33%)
Office 365 (1.58%)
Microsoft Teams Web Client (1.8%)
Office Online Loki SSO (1.9%)
Office Online Augmentation Loop SSO (2.11%)
Office Online Search SSO (2.11%)
Windows Sign In (2.17%)
OneDrive SyncEngine (2.54%)
Microsoft Account Controls V2 (2.64%)
Microsoft 365 Support Service (2.68%)
Office Online Core SSO (2.75%)
OfficeHome (2.91%)
VMware Horizon - Unified Access Gateway - Prod (3.17%)
Office365 Shell WCSS-Client (4.09%)
Apple Internet Accounts (4.72%)
Microsoft Authentication Broker (5.15%)
Office 365 SharePoint Online (5.53%)
Microsoft Teams (6.31%)
Microsoft Office (9.02%)
Feide (21.2%)
AEM-DualAuth
Azure AD Identity Governance - Entitlement Management
Bomgar Remote Support
Doodle AG
Gmail
Microsoft Account Controls V2
Microsoft Authenticator App
Microsoft Edge
Microsoft Office
AMC PROD
Azure Active Directory PowerShell
CONNECT
Editor Browser Extension
Graph Files Manager
Microsoft App Access Panel
Microsoft Azure Signup Portal
Microsoft Edge Enterprise New Tab Page
Microsoft Office 365 Portal
Accounts Control UI
Azure DevOps
Cisco AnyConnect
Enpass
Looop
Microsoft AppSource
Microsoft Community v2
Microsoft Flow Portal
Microsoft Outlook
Apple Internet Accounts
Azure Portal
ConfigMgrClientApp
Feide
Microsoft 365 Security and Compliance Center
Microsoft Application Command Service
Microsoft Device Registration Client
Microsoft Forms
Microsoft Power BI

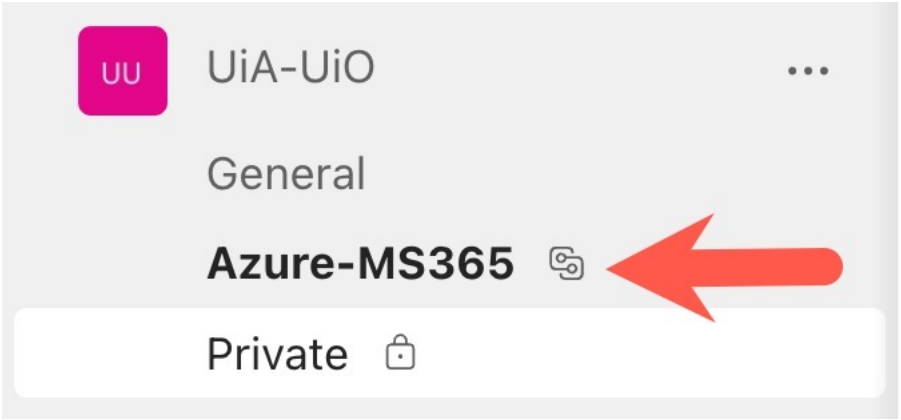
Hva har vi oppnådd...

- Over **35.000 brukerkontoer** har 2FA
- Et **stort SSO-område** med **reautentisering hver 30. dag** per program, per maskin
- Den gjengse bruker: **kun et tofaktoroppsett**
- **Autentiseringer mot Azure AD**
  - **Dager** med over **120.000 autentiseringer**
  - **Måneder** med opp til **2.7 millioner autentiseringer**
- **Redusert trusselbilde**
  - Vi så i fjor høst en **markant nedgang i kontoer på avveie** (som var prosjektets mål)
  - **Kontoer på avveie** stoppes nå av kravet om 2FA, og IT-sikkerhet får ryddet opp – kan være kontoer som har vært på avveie en stund!

2FA i Microsoft Teams

- **Azure AD B2B Direct Connect**
  Løsning hvor institusjoner som samarbeider mye kobler sammen deres Azure ADer
  - Vår Azure AD kan **settes i trust** med andre institusjoners Azure AD f. eks. BOTT-universitetene
  - Gir tilgang til **Shared Channels i MS Teams** fra annen institusjon, uten at en trenger å logge seg ut av UiOs tenant og inn på andre tenanter, og hvor en **bruker UiOs 2FA-oppsett**





Prosjekt avsluttet - Hva gjenstår for linja

- Gjøre 2FA **obligatorisk for e-postklienter** som kobler seg mot Exchange
  - Flere tusen Outlook-klienter (MAPI - Windows)
  - 8.500 klienter med modern auth på EWS og EAS
  - En del maskiner gjenstår - forsøkene på å skru på modern auth har skapt mye støy!

- **OWA (webmail)**
  - **ADFS** mister kobling mot Azure AD for MFA servere 30. sept 2024
  - Vi må finne en annen løsning for å få til MFA for OWA:
    - Pass-through
    - Password hash i sky

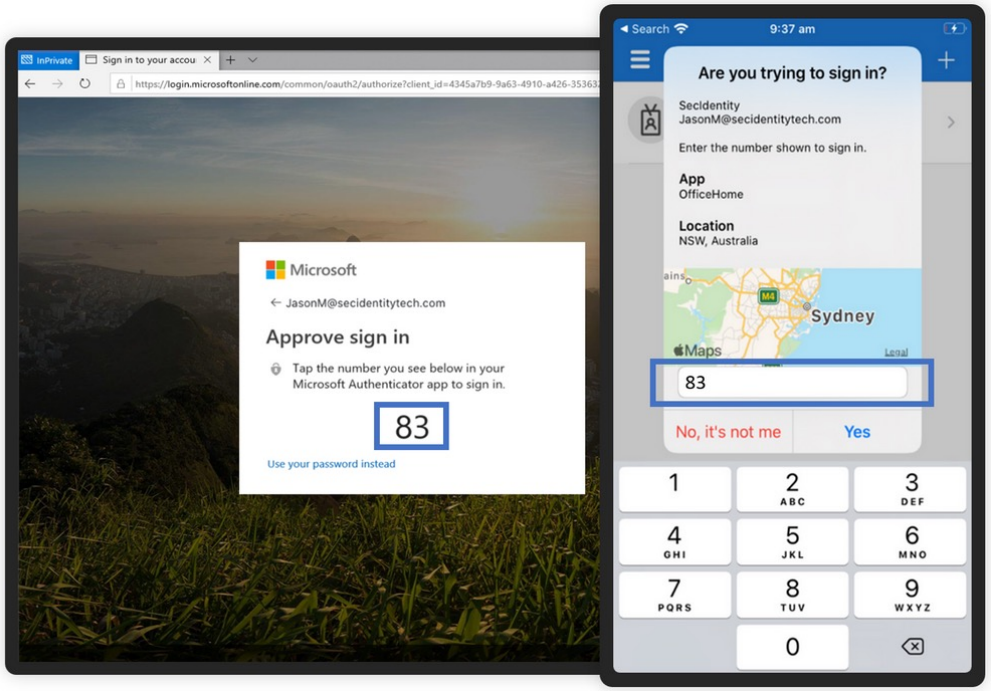
Hva gjenstår

- **Feilsøke og forbedre brukeropplevelsen** på avdekkede problemområder:
  - E-post og kalender: **IMAP** og brukere av **Evolution**
  - Linux-brukere med behov for **RDP**
  - **Få ned antallet 2FA requests**, og dermed forbedre brukeropplevelsen (Et eks. Conditional Access Policies for SSO med Firefox)

- **Weblogin** skal fases ut
  - **Sympa** er nylig flyttet til Feide
  - Tjenesteeiere må, sammen med IT-avdelingen, finne løsninger for de andre tjenestene som bruker Weblogin

2FA med Azure AD – ikke problemfritt

- **Kostnadsdrivende -** Alle på UiO trenger etter hvert en MS365-lisens
- **Lock in**
  - Autentisering flyttes til til Azure AD
  - Øker UiOs avhengighet til Microsoft 365
- **Azure AD kan gå ned -** Mange tjenester, mange brukere som da ikke får jobbet
- **MFA fatigue**
  - Vanskelig å avdekke
  - Vi tok i bruk **number matching** og **app info** i det funksjonaliteten ble lansert av Microsoft, men ikke **location** basert på IP



Stor takk til alle de som har stått på for at UiO skulle få dette til!

Frank Paul Silye

frankps@uio.no

Seksjon for digitale kommunikasjonsplattformer