

UH-sky

Startpakke skytjenester - Office 365

Design og anbefalinger

Beste praksis for innføring av Office 365 – basert på erfaringer fra flere UH-institusjoner

Dokumentversjon: 1.4
Dato: 13 desember 2016

Forfattere:

Christian A. Seneger, Christian Knarvik, Jimmy Hang og Tom-Inge Larsen (Advania Norge)
Odd A. Halseth, Rune Myrhaug, Jardar Leira (UNINETT)

Copyright © UNINETT AS

Innholdet i dette dokumentet kan bli endret uten forutgående varsel. Alle rettigheter med hensyn til kopiering og gjenbruk innehas av UNINETT etter avtale med Advania Norge, og disse rettighetene er uten vilkår delegert videre til UNINETTs medlemsinstitusjoner.

1. Innholdsfortegnelse

1. INNHOLDSFORTEGNELSE	2
2. DOKUMENTINFORMASJON	4
2.1 REFERANSER	4
3. INNLEDNING	5
3.1 FORMÅL	5
4. ROS-ANALYSE	6
4.1 EKSEMPLER PÅ TJENESTEBESKRIVELSE OG TILKNYTTET RISIKO MED BESKRIVELSE	7
4.1.1 <i>Eksempel 1</i>	7
4.1.2 <i>Eksempel 2</i>	9
5. ANBEFALTE FORBEREDELSE FOR EN VELLYKKET IMPLEMENTASJON	10
5.1 FLYTSKJEMA - IMPLEMENTERING	11
6. OVERSIKT OVER UTVALGTE GRENSEVERDIER I OFFICE 365	12
7. LISENSIERING	14
7.1 FLYTTING AV LISENSER PÅ TVERS AV OFFICE 365 TENANT-ER	14
8. HVORDAN HÅNDTERE DINE IDENTITETER	16
8.1 HYBRIDIDENTITET	17
8.1.1 <i>Microsofts tre identitetsmodeller</i>	18
8.2 FEIDE	19
8.3 EKSISTERENDE ID LØSNINGER FIM/MIM	19
8.4 AZURE AD CONNECT (AAD CONNECT)	19
8.4.1 <i>AAD Connect og forskjellige topologier</i>	20
8.4.2 <i>Immutable ID</i>	20
8.5 IDENTITETSBEHANDLING ETTER INNFØRING AV OFFICE 365	20
8.6 SSO	21
8.6.1 <i>Modern authentication</i>	22
9. FØDERERING	23
10. E-POST	25
10.1 MIGRERINGSSTRATEGIER	25
10.1.1 <i>Hybrid</i>	25
10.1.2 <i>Cutover</i>	25
10.1.3 <i>Office 365 til Office 365</i>	25
10.2 AVVIKLING AV LOKAL EXCHANGE	25
10.3 BACKUP	26
10.4 FAST TRACK	26
11. SKYPE FOR BUSINESS	27
11.1 HENSYN	27
11.1.1 <i>Telefoni</i>	27
11.1.2 <i>Innringte konferanser</i>	28
11.1.3 <i>3. parts integrasjoner</i>	28
11.2 UH SKYPE	28
11.2.1 <i>AD</i>	28

11.2.2	Telefoni.....	28
11.2.3	Innringte konferanser.....	28
11.2.4	Støttesystem	29
12.	SHAREPOINT	30
12.1	BACKUP	31
13.	ONEDRIVE	32
13.1	BRUKSOMRÅDER	32
13.2	BACKUP	32
13.3	MIGRERING	32
14.	AVVIKLINGSMULIGHETER FOR OFFICE 365	33
14.1	E-POST	33
14.2	SKYPE	33
14.3	ONEDRIVE/SHAREPOINT.....	33
15.	HVORDAN LYKKES MED DITT PROSJEKT	34

2. Dokumentinformasjon

2.1 Referanser

Referanser det henvises til i dokumentet. (Med forbehold om

Referanse Nr.	Tittel	Kort beskrivelse	Versjon	Dato
1	https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-ports/	Portoversikt AAD Connect		
2	https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-topologies/	AAD Connect og topologistøtte		
3	https://support.office.com/en-us/article/Enable-Modern-Authentication-for-Office-2013-on-Windows-devices-7dc1c01a-090f-4971-9677-f1b192d6c910	Aktivere Modern Authentication for Office 2013		
4	https://support.office.com/en-us/article/Enable-Exchange-Online-for-modern-authentication-58018196-f918-49cd-8238-56f57f38d662	Aktivere Modern Autentication for Exchange Online		
5	http://aka.ms/PublicPreview	Aktivere Modern Autentication for Skype for Business		
6	https://support.office.com/en-us/article/Ways-to-migrate-multiple-email-accounts-to-Office-365-0a4913fe-60fb-498f-9155-a86516418842	Migrering av e-post til Office 365		
7	https://technet.microsoft.com/en-us/library/hh534377(v=exc hg.150).aspx	Forutsetninger for hybridoppsett for Exchange		

3. Innledning

3.1 Formål

Dette dokumentet har som hensikt å beskrive forskjellige teknikker og teknologier som kan benyttes under en Office 365 innføring. Hvilke valg man gjør avhenger av det grunnleggende designet, og de fleste teknologiene som er beskrevet i dette dokumentet kan anvendes på flere forskjellige måter. Dokumentet er ikke ment som et designdokument med absolutte anbefalinger, men snarere et «beste praksis» dokument som beskriver de mest brukte framgangsmåtene under innføring av Office 365 i en utdanningsinstitusjon.

Deler av dokumentet fordrer teknisk forståelse rundt Office 365, Exchange, Active Directory, Skype, SharePoint, identitet og omkringliggende teknologier.

Dokumentet er én av flere dokumenter under prosjektet «startpakke skytjenester», som samlet beskriver beste praksis for innføring av skybaserte samhandlings- og kontorstøttetjenester i UH-sektoren – basert på SaaS fra «public cloud» leverandører. Første del av prosjektet beskriver spesifikt ulike sider ved innføring av Office 365 fra Microsoft.

O365 er den klart mest utbredte tjenesten under paraplyen «samhandlings- og kontorstøttetjenester» i sektoren. Ca. 90% av institusjonene har «begynt å se på» O365, og pr. august 2016 har minst 60% av institusjonene offisielt tatt i bruk én eller flere moduler i O365-porteføljen – for studenter eller ansatte, eller for begge gruppene.

Erfaringsmessig er det kontorstøttetjenesten (Office Online) og e-posttjenesten (Exchange Online) som først tas i bruk, og da ofte for studenter først og ansatte deretter. OneDrive er også en tjeneste som tidlig tas i bruk for både ansatte og studenter for deling og samhandling. Avvikling av lokale hjemmeområder er også vanlig pådriver for OneDrive-implementering. Videre ser vi at Classroom Creator og Yammer har vært tatt i bruk i tidlige faser.

Dette dokumentet er basert på erfaringer fra konsulentbransjen, som gjentatte ganger har bistått institusjoner i sektoren med overgang til O365. Dokumentet beskriver tillært «beste praksis» gjennom disse prosjektene, og tar mål av seg til å gi råd rundt valg som må tas underveis i prosessen. Det er viktig å ha klart for seg at disse anbefalingene ikke må betraktes som «fasit» og at alle innføringsprosjekt er forskjellige; forutsetningene er ulike, og målene kan også være forskjellige. Derfor må beskrivelsene i dokumentet kun oppfattes som forslag og råd. Det er fortsatt viktig at institusjonene gjør individuelle vurderinger i de valgene som må tas underveis, og at man ser at alle slike prosjekt er unike.

Likevel håper og tror vi at anbefalingene kan være til stor nytte for alle som står på spranget til å innføre O365 i sin virksomhet.

4. ROS-analyse

Informasjonssikkerhet handler om sikring av konfidensialitet, integritet og tilgjengelighet på informasjon.

Å sikre konfidensialitet innebærer å hindre uautorisert innsyn i informasjon som ikke kan være åpent tilgjengelig for alle. Å sikre integritet innebærer å hindre uautorisert endring og sletting av informasjon. Å sikre tilgjengelighet innebærer å sikre tilgang til informasjon for alle som skal ha tilgang.

Risiko- og sårbarhetsanalyse (ROS-analyse) handler om at virksomheten selv setter seg ned og analyserer svakhetene (sårbarhetene) ved et system opp mot risikoelementene konfidensialitet, integritet og tilgjengelighet, og iverksetter tiltak på de områdene hvor svakhetene anses som kritiske.

Det er anbefalt å gjennomføre en ROS-analyse før man tar i bruk skytjenester. Dette gjøres hovedsakelig for å identifisere og klassifisere eventuelle sårbarheter og feil som kan oppstå i forbindelse med implementering og bruk av Office 365. Risikoer graderes og eventuelle tiltak for å redusere disse beskrives. Dette er en teoretisk tilnærming for å kartlegge om identifiserte risikoer er akseptable eller ikke. Dette settes ut fra forhåndsgitte kriterier og vekting av disse.

Datatilsynet anbefaler at man gjennomfører ROS-analyse før man tar i bruk tjenester fra skytilbydere som Office 365, Amazon og Google Apps.

Sekretariat for informasjonssikkerhet i UNINETT (<https://www.uninett.no/infosikkerhet>) tilbyr fasilitering av ROS-analyse for UH-institusjonene. De har utviklet en egen mal for ROS-analyse av kritiske IT-systemer. Denne er benyttet ved gjennomføring ROS-analyse for innføring av O365 ved NTNU. Rapport fra denne ROS-analysen finnes her:

[ROS-analyse rapport NTNU](#)

Hvilken metode man benytter for gjennomføring av ROS-analyse er ikke det viktigste. Hovedsaken er at man i fellesskap setter seg ned å avdekker svakheter, vurderer sannsynlighet, kritikalitet og konsekvens, og iverksetter tiltak. I ytterste konsekvens kan kombinasjonen sannsynlighet/kritikalitet og konsekvens være så omfattende at det ikke er mulig å iverksette realistiske tiltak innenfor akseptable kostnadsrammer (Det handler ofte til slutt om økonomi). Da kan resultatet være at innføringen av nytt system utsettes inntil det er kommet opp andre alternativer eller grunnleggende forutsetninger er endret.

I de aller fleste tilfellene vil tiltak for å etablere tilfredsstillende informasjonssikkerhet handle om bevisstgjøring og opplæring av brukere.

Mer om ROS-analyse vil også komme på UH-sky sine nettsider.

Vedlagte eksempler er basert på mal som benyttes av konsulentselskapet Advania.

4.1 Eksempler på tjenestebeskrivelse og tilknyttet risiko med beskrivelse

4.1.1 Eksempel 1


Risk 1 – availability of ADFS

Risk ID	1
Risk Owner	
Architecture Domain	Office 365
Required Decision / Principle	High-availability.
Risk Description	ADFS unavailable or malfunctioning.
Consequence	Users cannot sign in to Office 365 services.
Probability (low/med/high)	Low
Related risks	
Current level of risk	
Mitigating actions	
Target risk level	

Risk analysis 1

Likelihood The likelihood for impact:	Rare <input type="checkbox"/> 1	Unlikely <input type="checkbox"/> 3	Possible <input checked="" type="checkbox"/> 5	Likely <input type="checkbox"/> 7	Frequent <input type="checkbox"/> 9
---	------------------------------------	--	---	--------------------------------------	--

Consequence		Incidental	Minor	Moderate	Major	Extreme	N/A
Economic (20%)		<input type="checkbox"/> 2	<input checked="" type="checkbox"/> 4	<input type="checkbox"/> 6	<input type="checkbox"/> 8	<input type="checkbox"/> 10	<input type="checkbox"/> 0
Legal (20%)		<input type="checkbox"/> 2	<input checked="" type="checkbox"/> 4	<input type="checkbox"/> 6	<input type="checkbox"/> 8	<input type="checkbox"/> 10	<input type="checkbox"/> 0
Reputational (20%)		<input type="checkbox"/> 2	<input checked="" type="checkbox"/> 4	<input type="checkbox"/> 6	<input type="checkbox"/> 8	<input type="checkbox"/> 10	<input type="checkbox"/> 0
Operational (40%)		<input type="checkbox"/> 4	<input type="checkbox"/> 8	<input checked="" type="checkbox"/> 12	<input type="checkbox"/> 16	<input type="checkbox"/> 20	<input type="checkbox"/> 0

Risk	<p>Risk score: Likelihood x (sum of consequences) = 120</p>  <p> <input type="checkbox"/> ca 0-30 <input type="checkbox"/> ca 30-100 <input checked="" type="checkbox"/> ca 100-150 <input type="checkbox"/> ca 150-300 <input type="checkbox"/> more than 300 </p> <p> No action Monitor risk Consider mitigating actions Implement mitigating actions Implement mitigating actions immediately </p>
Risk comment	
Risk mitigating suggestions already implemented	-
Risk mitigating suggestions to be considered	- Implement ADFS in HA-design

Som grunnlag for vektingen av konsekvens ligger for eksempel en matrise som sier detaljert noe om hva som ligger i de forskjellige graderingene. For eksempel kan «Economic minor» være beløp mellom 1000-10000kr eller beløp mellom 10000-100000 avhengig av hva som passer organisasjonen.

4.1.2 Eksempel 2


Risk 2 – Sensitive information and business data

Risk ID	2
Risk Owner	
Architecture Domain	Office 365
Required Decision / Principle	
Risk Description	Office 365 stores data in data centres outside of Norway, primarily in Amsterdam and Dublin, and under certain circumstances data can be stored in the US as well. Sensitive information must be treated thereafter.
Consequence	Sensitive information stored in non-compliant way can result in data loss and security not adhered to policy.
Probability (low/med/high)	Medium
Related risks	
Current level of risk	
Mitigating actions	
Target risk level	

Risk analysis 2

Likelihood The likelihood for impact:	Rare <input type="checkbox"/> 1	Unlikely <input type="checkbox"/> 3	Possible <input checked="" type="checkbox"/> 5	Likely <input type="checkbox"/> 7	Frequent <input type="checkbox"/> 9
---	------------------------------------	--	---	--------------------------------------	--

Consequence		Incidental	Minor	Moderate	Major	Extreme	N/A
	Economic (20%)	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input checked="" type="checkbox"/> 3	<input checked="" type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 0
	Legal (20%)	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input checked="" type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 0
	Reputational (20%)	<input type="checkbox"/> 3	<input type="checkbox"/> 6	<input type="checkbox"/> 9	<input checked="" type="checkbox"/> 12	<input type="checkbox"/> 15	<input type="checkbox"/> 0
	Operational (40%)	<input type="checkbox"/> 5	<input checked="" type="checkbox"/> 10	<input type="checkbox"/> 15	<input type="checkbox"/> 20	<input type="checkbox"/> 25	<input type="checkbox"/> 0

Risk	<p>Risk score: Likelihood x (sum of consequences) =</p>  <p> <input type="checkbox"/> ca 0-30 <input type="checkbox"/> ca 30-100 <input type="checkbox"/> ca 100-150 <input checked="" type="checkbox"/> ca 150-300 <input type="checkbox"/> more than 300 </p> <p> No action Monitor risk Consider mitigating actions Implement mitigating actions Implement mitigating actions immediately </p>
Risk comment	
Risk mitigating suggestions already implemented	- User training and routines
Risk mitigating suggestions to be considered	-

5. Anbefalte forberedelser for en vellykket implementasjon

Det er flere forberedelser som kan gjøres før man går i gang med selve implementeringen av Office 365.

Følgende avklaringer bør gjøres før man starter arbeidet med teknisk utførelse:

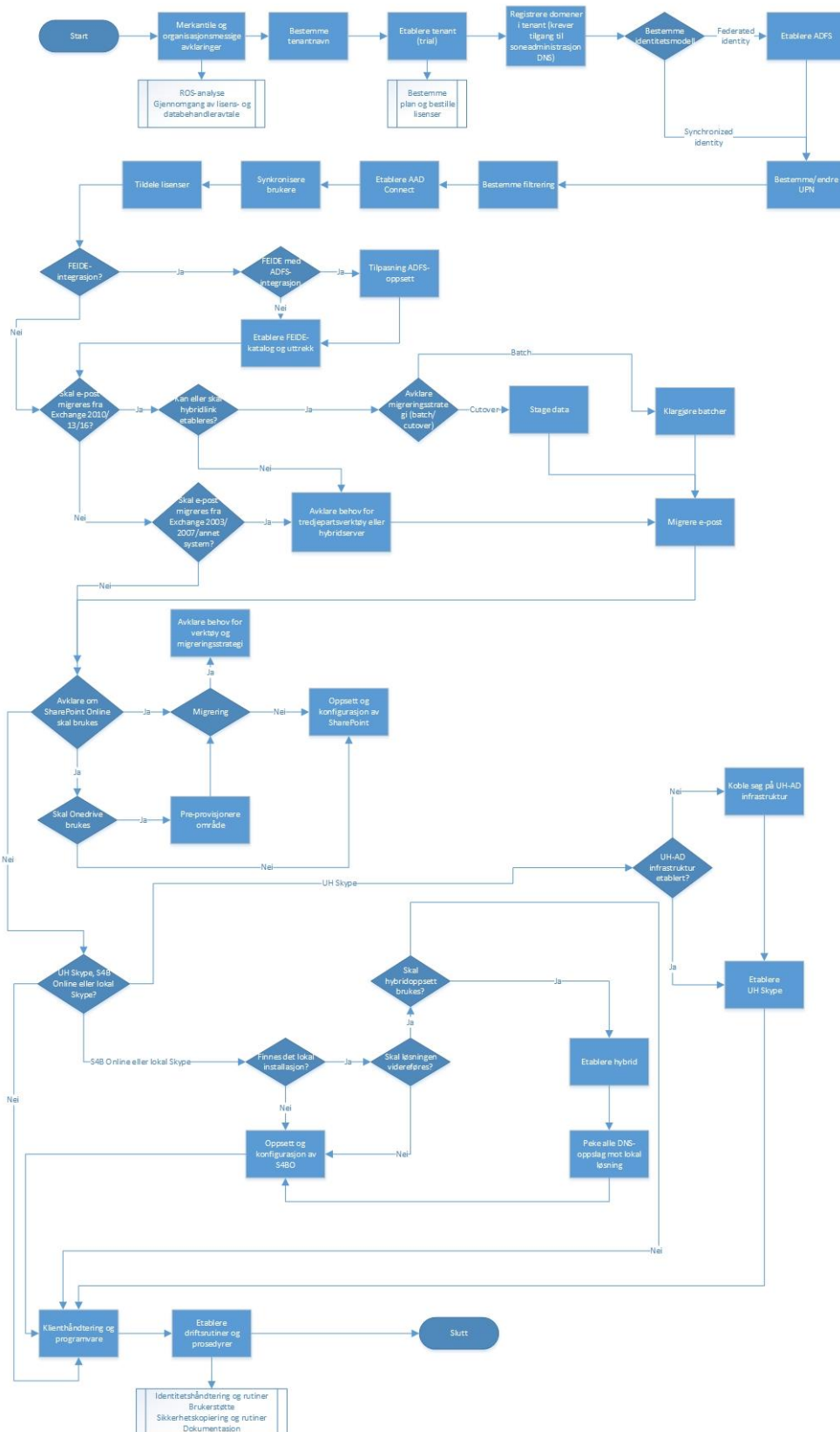
- Gjennomgang av lisens- og databehandleravtale
- ROS-analyse
- Avklare om det skal tas i bruk ny tenant eller migreres til allerede eksisterende tenant
- Få kontroll over DNS-soner for berørte domener
- Avklare behov for endring av UPN
- Avklare rekkefølge for implementering/migrering av tjenester og evt. migreringsstrategi
- Vurdere identitetsmodell
- Avklare evt. klientbehov og påkrevde versjoner for programvare

Implementeringsprosessen kan illustreres med flytskjema som vist på neste side.

Merk at prosessen ikke nødvendigvis er begrenset til det som er vist i flytskjemaet.

Noen av prosessene/tiltakene i flytskjemaet er mer utfyllende beskrevet senere i dokumentet.

5.1 Flytskjema - implementering



Dokumenttittel:

Startpakke skytjenester - Office 365
Design og anbefalinger
Dokumentklassifisering: Åpen

6. Oversikt over utvalgte grenseverdier i Office 365

De ulike modulene i Office 365 er satt opp med noen standard grenseverdier som kan være viktig å kjenne til før man tar beslutninger og går videre i prosessen. Noen av disse er absolutte, mens andre er mulig å utvide etter avtale med leverandør. (Kan medføre ekstra kostnad).

Tjeneste	Beskrivelse	Grense	Kommentar
Exchange Online	Maks antall adresselister	1000	
	Maks antall OAB	250	OAB = Offline Address Book
	Maks antall ABP	250	ABP = Address Book Policy
	Maks antall GAL	250	GAL = Global Address List
	Maks størrelse postboks	50GB	E1-E5 og EDU lisenser. Avhengig av lisensstype kan det være begrensning rundt arkiveringsmuligheter og størrelse
	Maks antall Public Folders	100000	
	Maks antall elementer i postboks	1000000	
	Maks størrelse e-post	150MB	Maks størrelse settes per tenant. På e-post som sendes ut av Office 365 (eksternt) kan maks størrelse reduseres med inntil 33% pga encoding.
	Slettede elementer retention	Ingen grense	
	Elementer slettet fra slettede elementer	30 dager	Standard er 14 dager.
OneDrive	Maks filstørrelse	10GB	
	Maks lengde på filnavn/sti	256 tegn	
	Størrelse på individuell OneDrive-lagring	1TB	
	Maks opplasting	10GB for drag&drop. Andre måter: 2GB	
SharePoint Online	Maks størrelse på vedlegg	250MB	
	Maks antall brukere per gruppe	5000	
	Maks antall grupper	10000	Anbefalt maks.
	Maks antall dager backup	14 dager	Backup tas hver 12. time, bare site collections eller sub sites kan restores.
	Maks størrelse på site collection	25TB	

Skype for Business Online	Maks conversation tabs	50	
	Maks størrelse på filoverføring (p2p)	Ingen grense	Grense i møte er 500MB.
	Maks antall deltakere i møte	250	
	Levetid delt innhold i møte	15 dager	

Disse verdiene er oppdaterte per 14.11.2016, og kan uten forvarsel bli endret av Microsoft.

7. Lisensiering

Kvalifiserte utdanningsinstitusjoner kan få Office 365 Education kostnadsfritt eller oppgradere til avanserte funksjoner med betydelig rabatt. Det må bekreftes at man er en godkjent utdanningsinstitusjon for å kunne bruke disse tilbudene.

Dersom man allerede er tilsluttet en rammeavtale for Microsoft-lisenser gjennom UNINETTs innkjøpssamarbeid er det, etter UNINETT sin vurdering, ikke nødvendig å konkurranseutsette (les: anbud) tjenesten før man evt. velger å ta i bruk Office 365. Dette pga. at lisensene allerede er inkludert i eksisterende rammeavtale og ikke medfører tilleggskostnad for institusjonen.

Se følgende link for informasjon om EDU-lisenser:

<https://products.office.com/nb-no/academic/compare-office-365-education-plans>

For å få en tenant godkjent med EDU-tag gjøres det via partner eller Microsoft-kontaktperson. Microsoft forbeholder seg retten til når som helst å kontrollere at kunder er kvalifisert, og avslutte tjenesten for kunder som ikke er det.

Det er også ønskelig å knytte opp Microsoft lisensavtaler mot Office 365 tenant. På denne måten kan man få tilgjengeliggjort lisenser i O365. For eksempel om man har en lisensavtale som kvalifiserer studenter og lærere til tilgang på Office pakken, vil man få lisensen som i skrivende stund heter: «Office 365 for Students Plus» og «Office 365 for Faculty plus». Denne gir standard Office 365 Education funksjonalitet, men også tilgang til Office 365 ProPlus (C2R).

Tidligere har det vært flere «konflikter» med produkter på tvers av EDU SKU og Enterprise SKU. Dette blir det kontinuerlig jobbet med, og i skrivende stund er det ingen kjente lisenskonflikter.

For å knytte EA eller andre lisensavtaler mot Office 365 gjøres dette via Office 365 portal i tenant man ønsker å knytte mot ved å opprette supportsak direkte i tenant.

- Man trenger avtalenummer på lisensavtale som ønskes knyttet mot tenant
- Man må vite kontaktperson på lisensavtale, og sende mail fra e-postadresse som er registrert
- Man må ha informasjon om bedriftsnavn og kontaktperson til tenant
- Følge opp support tett på epost og telefon
- Få bistand av lisensrådgiver hvis nødvendig

Pr. november 2016 er Microsoft-partner for UH-sektoren Crayon AS, regulert gjennom Uninett rammeavtale. Utløpsdato for avtalen er 25. mars 2017, men denne kan forlenges med 1 + 1 år, maksimalt til 25. mars 2019.

Man trenger ikke Azure-lisenser for å ta i bruk Office 365-tjenester.

7.1 Flytting av lisenser på tvers av Office 365 tenant-er

For å flytte lisenser på tvers av tenant-er oppretter man en supportcase mot Microsoft. Dette gjøres i tenant man ønsker å flytte fra.

Eksempel på supportsak:

We want to remap our licenses from oldtenant.onmicrosoft.com to newtenant.onmicrosoft.com

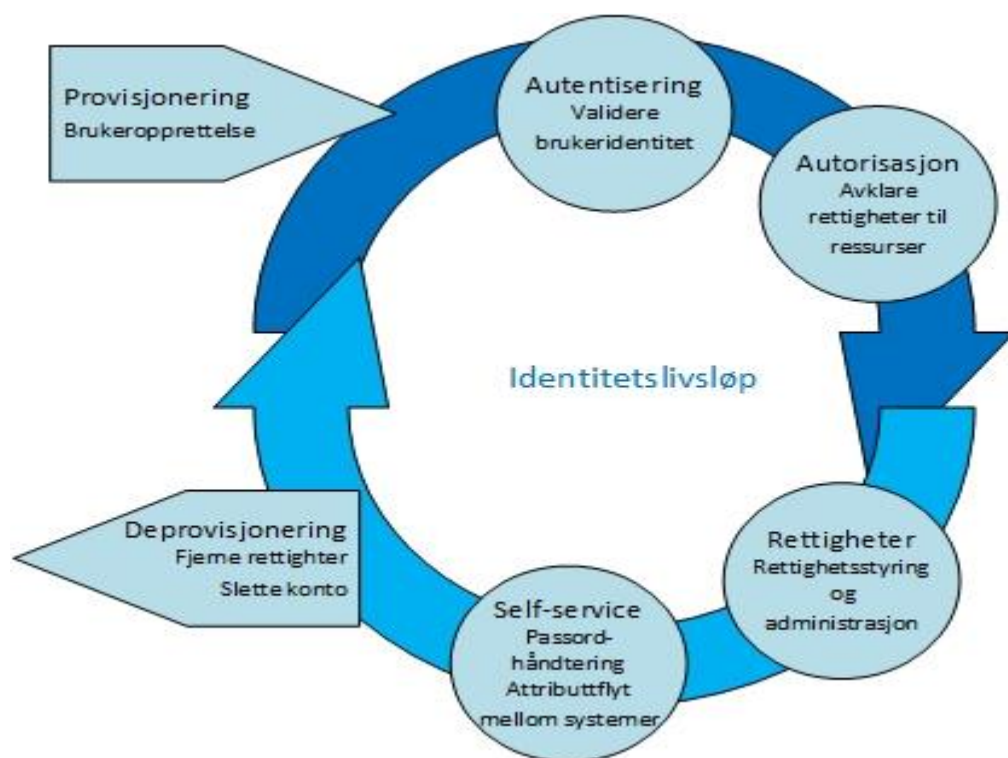
1. Enrollment Number: XXXXXXXXX

2. All subscriptions moving to the new tenant: All subscriptions

3. Are there any subscriptions on the existing tenant that you do not intend to move to the new tenant?
No
4. Incorrect/Current tenant Domain: oldtenant.onmicrosoft.com
5. Correct/Destination tenant Domain: newtenant.onmicrosoft.com
6. Reason the move is being requested: moving to new tenant

8. Hvordan håndtere dine identiteter

Det bør finnes rutiner for eller et system som håndterer identiteter og det som kan kalles et identitetslivsløp. Dette kan illustreres på følgende måte:



Fra tidligere har ikke UPN (User Principal Name) blitt brukt i stor grad, og den ble derfor ofte satt til å være lik samaccountname. UPN-suffiks stod som oftest standard til det samme som AD-domenenavnet. I en skyverden benyttes UPN som pålogging. Denne er bygd opp på samme måte som en e-postadresse, for eksempel fornavn.etternavn@domene.no. Sluttbrukere har som oftest ikke noe forhold til noe annet enn samaccountname og e-postadresse. Mange skytjenester ber bruker om å logge på med e-postadresse. I Office 365-verden tilsvarer dette UPN.

Ved bruk av Skype anbefales det å sette SIP-adressen lik UPN og e-postadresse.

Kort oppsummert: e-postadresse=SIP=UPN.

Merk også at Office-programmer som oftest spør etter e-postadresse i stedet for brukernavn ved pålogging, noe som også taler for å gjøre endringen som beskrevet over.

Dette fører videre til at de fleste har behov for å endre UPN til å være lik e-postadressen. Samaccountname forblir uendret. I et Active Directory-miljø kan brukerne da logge på klient med enten samaccountname eller UPN.

UPN blir brukerens pålogging til Office365. For en bedre brukeropplevelse, er anbefalt løsning for Office 365 og andre skytjenester at UPN blir satt til samme verdi som primær e-postadresse samt Skype adresse (fornavn.etternavn@domene.no).

Hvis primær SMTP er forskjellig fra UPN vil dette forvirre brukeren under bruk.

For eksempel:

Ola Normann har ansattnr. 12345, mens e-postadresse er ola.normann@domene.no. Hvis UPN er 12345@domene.no, mens e-postadresse og Skypeadresse er ola.normann@domene.no, vil følgende situasjon oppstå:

- Bruker setter opp Outlook, mobilsynk (iPad, smarttelefon etc) eller lignende med ola.normann@domene.no og passord.
 - o Dette fungerer ikke fordi ola.normann@domene.no ikke er gyldig pålogging i O365. Derfor får bruker spørsmål om brukernavn og passord. Da må Ola Normann skrive 12345@domene.no
- Samme vil skje i Skypeklient; bruker skriver inn ola.normann@domene.no og passord.
 - o Dette fungerer ikke og bruker må skrive 12345@domene.no i UserName i Skypeklienten.

Dersom UPN, e-postadresse og Skype-adresse er det samme vil begge klientene finne innstillinger automatisk og logge automatisk på dersom bruker skriver inn ola.normann@domene.no.

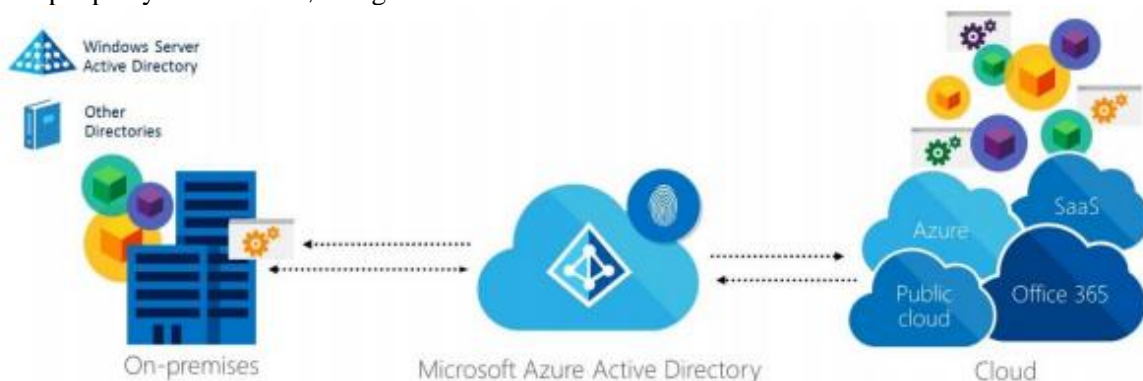
I UH-sektoren kan det være gode argumenter for å avvike fra standarden med at e-postadresse=SIP=UPN. Det er utbredt bruk av FEIDE-ID (eduPersonPrincipalName) i UH-sektoren for å logge seg på forskjellige web-tjenester. En kan derfor argumentere for at en bør benytte FEIDE attributten eduPersonPrincipalName = UPN i Office365. Dette vil lette arbeidet med å konfigurere føderert pålogging med FEIDE.

8.1 Hybrididentitet

Brukere forholder seg i dag som oftest til flere identiteter, både på jobb og privat. Skillet mellom enheter som brukes kun på jobb eller privat er i ferd med å viskes ut, og dette stiller høyere krav til identitetshåndtering.

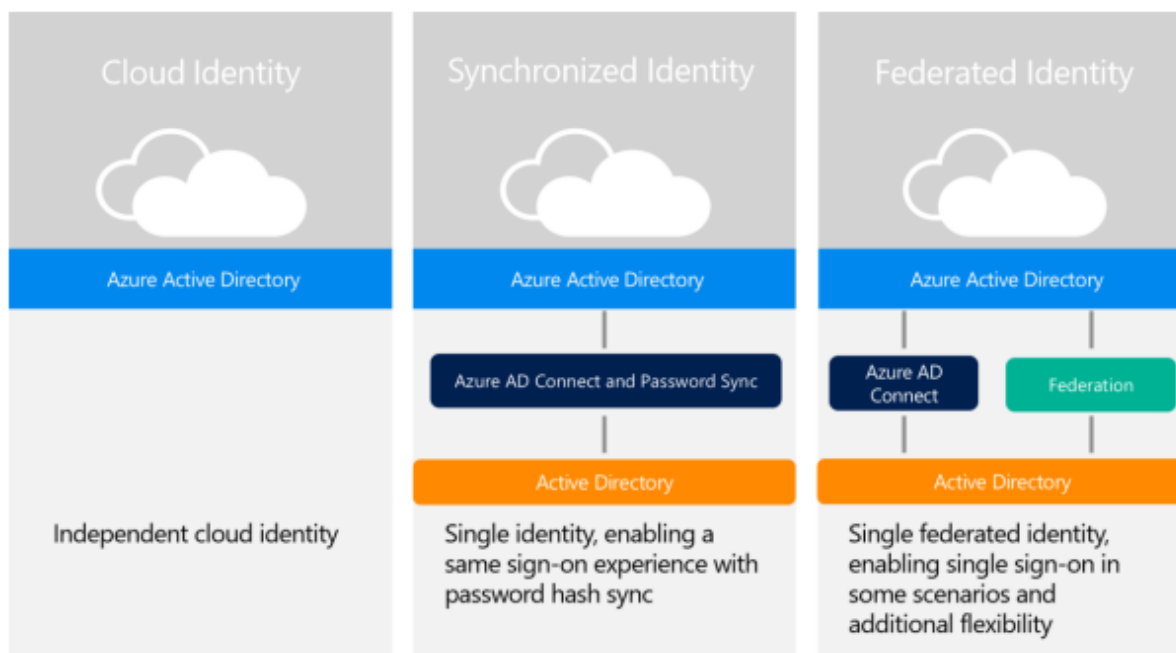
En unik identitet som brukes for autentisering og autorisasjon mot tjenester og ressurser som finnes både on-premises og i skyen kan kalles en hybrididentitet.

Eksempel på hybrididentitetløsning som bruker Azure AD som identitetskilde.



8.1.1 Microsofts tre identitetsmodeller

Microsoft gjør en inndeling av identitet i tre identitetsmodeller:



Cloud identity:

Kontoer som kun eksisterer i skyen, dvs. i Azure AD.

Synchronized identity:

Kontoer som eksisterer både on-premises og i skyen. Kontoer og passordhash synkroniseres typisk opp til skyen ved bruk av AAD Connect. Brukere gis en «same sign-on» opplevelse da brukernavn og passord er likt begge plasser.

Federated identity:

Kontoer som eksisterer både on-premises og i skyen der det i tillegg brukes en fødereringsløsning (for eksempel ADFS) i tillegg til AAD Connect.

Identitetsmodell	Fordeler	Ulemper
Cloud identity	<ul style="list-style-type: none"> - Passer for små organisasjoner - Krever ingenting on-premises 	<ul style="list-style-type: none"> - Brukere må logge på for å nå ressurser i skyen - Passord vil antakelig ikke være like on-premises og i skyen
Synchronized identity	<ul style="list-style-type: none"> - Samme passord brukes for å autentisere mot on-premises og skytjenester - Enkelt å administrere for små og mellomstore bedrifter - SSO (Same Sign-On) til en del sky-ressurser 	<ul style="list-style-type: none"> - Passordhash synkroniseres ut i skyen
Federated identity	<ul style="list-style-type: none"> - SSO (Single Sign-On) til en del ressurser 	<ul style="list-style-type: none"> - Krever oppsett av ADFS og drift av tjenesten

	<ul style="list-style-type: none"> - Supporterer en del avanserte scenarioer - ADFS brukes av flere tjenesteleverandører, kan være hensiktsmessig å implementere uavhengig av Office 365 	<ul style="list-style-type: none"> - Bør designes som en HA-tjeneste - Hvis tjenesten er nede får ikke brukere autentisert
--	--	--

8.2 FEIDE

FEIDE brukes av de fleste utdanningsinstitusjoner for autentisering mot flere nettbaserte tjenester. Dersom det eksisterer en FEIDE-integrasjon er det anbefalt å la brukerne autentisere seg mot FEIDE. Ved bruk av ADFS og tilpasninger i «claim rule» eller tredjepartsintegrasjoner kan man også autentisere seg mot Office 365 gjennom FEIDE-pålogging. Siden føderering styres av UPN-suffiks for hvert domene ved bruk av Office 365 kan det oppstå utfordringer dersom administrasjon og studenter bruker samme UPN-suffiks. Dette kan løses ved tredjepartsverktøy i forkant (internt i organisasjonen) som kan skille på om objekter skal bruke FEIDE eller ikke.

Det er også vanlig å distribuere «smart links» til brukere for å styre de direkte mot ønsket tjeneste for autentisering – som i dette tilfellet vil være FEIDE.

8.3 Eksisterende ID løsninger FIM/MIM

Det er viktig med oversikt over identitetsløsninger om man skal gå til Office 365. Man må avgjøre om eksisterende ID løsning skal håndtere identiteter i Azure AD, eller om man skal bruke Azure AD Connect til dette (hvor ID løsning har full kontroll på AD).

Eksempel:

1. ID løsning henter sine data fra HR system eller annet system/database
2. ID løsning oppretter brukere / grupper etc i AD
3. Azure AD Connect synkroniserer dette til Azure AD

8.4 Azure AD Connect (AAD Connect)

Azure Active Directory Connect (AAD Connect) er Microsofts foretrukne verktøy for synkronisering av objekter fra Active Directory (AD) til Azure Active Directory (Azure AD). Merk at det som kalles tenant i Office 365 er det samme som en instans av Azure AD.

Applikasjonen installeres på en server som enten er innmeldt i domenet eller er standalone, og kan synkronisere opp fra domener i samme forest eller andre tilgjengelige forest-er.

Under installasjonen opprettes det konto for synkronisering mot tenant i Azure AD og en lokal servicekonto på server som AAD Connect installeres på.

AAD Connect trenger også tilgang til AD og tjenestene DNS, Kerberos, MS-RPC, LDAP/LDAPS og RPC. Selve synkroniseringen av data foregår over HTTPS-protokollen (443). For komplett portliste, se referanse 1.

Det anbefales oppsett av filtrering på OU-nivå for å ha kontroll på objekter som synkroniseres.

AAD Connect kan installeres på en domenekontroller, men det anbefales ikke.

AAD Connect kan kun synkronisere objekter mot en tenant.

AAD Connect synkroniserer tilbake enkelte attributter fra Azure AD til lokalt AD.

8.4.1 AAD Connect og forskjellige topologier

AAD Connect støtter flere forskjellige topologier.

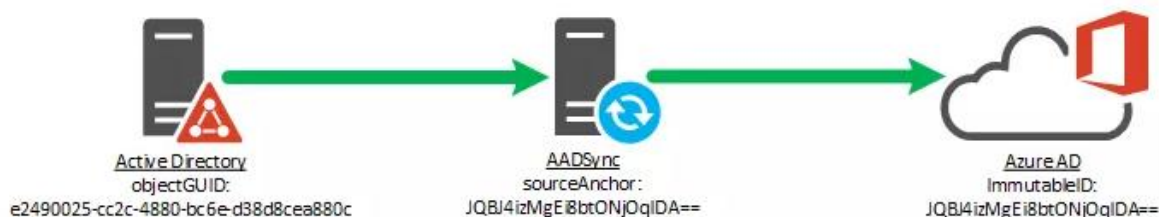
Oversikt over topologier og støtte i skrivende stund:

Topologi	Supportert	Kommentar
en forest → en AAD Connect → et Azure AD	Ja	Standardoppsett
en forest → flere AAD Connect → et Azure AD	Nei	Usupportert å ha flere AAD Connect servere mot et Azure AD
flere forest-er → en AAD Connect → et Azure AD	Ja	AAD Connect server må nå alle forest-er. Se avsnitt om immutable ID.
Flere forest-er → flere AAD Connect → et Azure AD	Nei	Usupportert å ha flere AAD Connect servere mot et Azure AD

Det finnes også andre scenarioer, som for eksempel «account-resource forest» og flere forest-er der brukerobjekter finnes i begge forest-er. Se referanser for utfyllende informasjon om dette.

8.4.2 Immutable ID

Når man setter opp synkronisering av objekter til Office 365 dannes det en base-64 verdi av attributtet objectGUID for hvert objekt – immutable ID. Dette brukes som en unik identifikator, og verdien kalles i AAD Connect databasen (metaverse) for sourceAnchor.



Så lenge et objekt flyttes mellom domener i samme forest forblir denne verdien uendret, men dersom man migrerer til en annen forest (for eksempel ved konsolidering, fusjon eller andre organisatoriske endringer) vil denne verdien bli endret. Det finnes ingen «SID history» for objectGUID. Man bør derfor planlegge hvilket attributt man velger som grunnlag for sourceAnchor.

Et alternativ er å bruke en av Exchange custom attributes, for eksempel extensionAttribute1 og lagre base-64 verdien av objectGUID der.

Merk at dette vil påvirke ADFS, da oppsettet av «relaying party trust» for Office 365 lager «claim rule» som peker på objectGUID. Dette kan redigeres i «claim rule» i ADFS management.

8.5 Identitetsbehandling etter innføring av Office 365

Så lenge identiteter synkroniseres fra et lokalt AD til Azure AD er det viktig å forstå at lokalt AD er «source of authority». Det betyr at man ikke kan endre attributter på objektene direkte i Azure AD, men endringer må gjøres i lokalt AD og synkroniseres opp.

Dette gjør seg spesielt gjeldende i forbindelse med Exchange. Mange organisasjoner ønsker å avvikle lokal Exchange etter postbokser er flyttet til Office 365, men opplever at man i praksis må beholde en Exchangeserver i «hybrid mode» og ha en hybridlink stående oppe mot Office 365. Dette er det supporterte alternativet fra Microsoft. Det støttes per nå ikke manuell redigering av attributter på

objekter. Microsoft har kommet med en gratis lisens til Exchange 2010/2013/2016 der server opererer i «hybrid mode» og man har tilgang til Exchange management.

Alternativt kan dette håndteres av en identitetsløsning som håndterer redigering/provisjonering av attributter (FIM/MIM, LCS, el).

8.6 SSO

Single Sign-On er en autentisering/autorisasjonsflyt som gjør at brukere kan bruke samme brukernavn og passord for å logge seg på flere tjenester.

Følgende tabell viser hvordan brukere autentiseres og autoriseres mot forskjellige tjenester ut fra hvilken identitetsmodell som er valgt.

		Synchronized identity	Federated identity	Synchronized med FEIDE	Federated identity med FEIDE
Domenemedlemmer og på internt nett	Nettlesere	Forms-based authentication	SSO. UPN må i noen tilfeller oppgis for redirect til ADFS.	Krever FEIDE-pålogging	Krever FEIDE-pålogging
	Outlook	Brukernavn og passord må oppgis	Brukernavn og passord må oppgis (se avsnitt om Modern authentication)	Brukernavn og passord må oppgis	Brukernavn og passord må oppgis (se avsnitt om Modern authentication)
	Skype for Business	Brukernavn og passord må oppgis	SSO. Må være autentisert mot Exchange for oppdatert kalenderinfo.	Brukernavn og passord må oppgis	SSO. Må være autentisert mot Exchange for oppdatert kalenderinfo.
	OneDrive	Brukernavn og passord må oppgis	SSO. UPN må i noen tilfeller oppgis for redirect til ADFS.	Brukernavn og passord må oppgis	SSO. UPN må i noen tilfeller oppgis for redirect til ADFS.
	Office ProPlus	Brukernavn og passord må oppgis	SSO	Brukernavn og passord må oppgis	SSO
BYOD eller på	Nettlesere	Forms-based authentication	Forms-based authentication	Krever FEIDE-pålogging	Krever FEIDE-pålogging
	Outlook, Skype, Onedrive, Office	Brukernavn og passord må oppgis	Brukernavn og passord må oppgis eller ADFS må være	Brukernavn og passord må oppgis	Brukernavn og passord må oppgis eller ADFS må være

			tilgjengelig eksternt		tilgjengelig eksternt
	Exchange ActiveSync	Brukernavn og passord må oppgis	Brukernavn og passord må oppgis	Brukernavn og passord må oppgis	Brukernavn og passord må oppgis
	Mobilapplikasjone r	Brukernavn og passord må oppgis	Brukernavn og passord må oppgis	Brukernavn og passord må oppgis	Brukernavn og passord må oppgis

Tabellen er gjeldende per dato: 10.11.2016

8.6.1 Modern authentication

«Modern authentication» tar i bruk ADAL-basert (Active Directory Authentication Library) sign-on til Office-applikasjoner. Dette muliggjør MFA, SAML-baserte tredjeparts IdP, smartkort og sertifikatbasert autentisering. Dette gjør også at Outlook ikke bruker «basic authentication» (brukernavn og passord) og gir SSO for applikasjonen. «Modern authentication» krever ADFS 3.0 eller nyere for å fungere.

Tabellen i forrige avsnitt tar ikke hensyn til ADAL, noe som betyr at dersom alle krav er oppfylt på klientsiden og man aktiverer ADAL vil dette overstyre verdiene i tabellen og gi SSO mot klientapplikasjonen. Se referanse 3-5 for oppdatert informasjon om hvilke produkter og scenarioer som er støttet.

For Office 2016 er dette automatisk aktivert på klientsiden.

For Office 2013 må dette aktiveres på klientsiden. Se link i referanser.

For tjenestene i Office 365 er standardinnstillinger som følger:

Exchange Online: av (se referanse 4 for endring av dette)

Sharepoint Online: på

Skype for Business: av

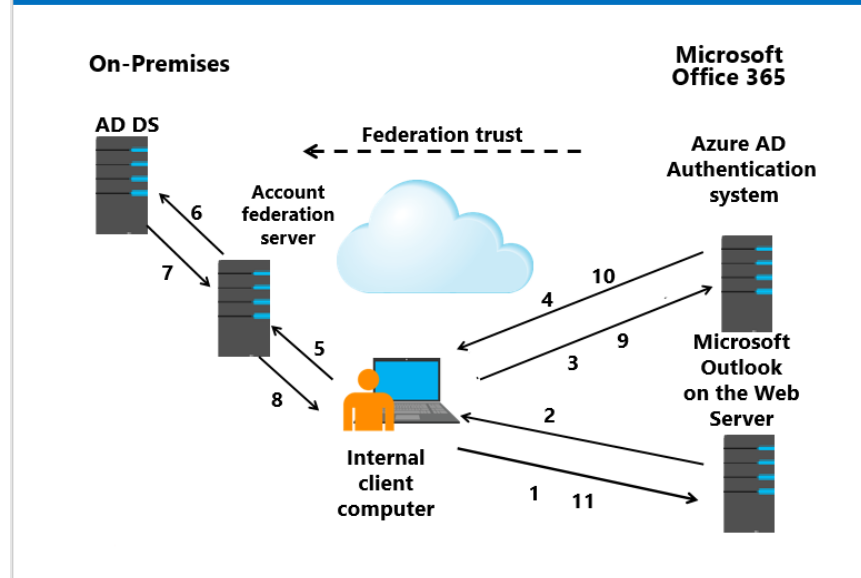
ADAL anbefales aktivert dersom klientapplikasjoner er på påkrevd versjonsnivå og ADFS er implementert.

9. Føderering

Mange organisasjoner har allerede implementert en føderingsløsning basert på STS, som ADFS. Dette brukes for å gi brukere SSO mot systemer/applikasjoner som finnes eksternt (og evt. internt). Som en del av fødereringen defineres hvilke ressurser som er tilgjengelige og hvordan tilgang til disse administreres.

Autorisasjonsflyten ved bruk av ADFS kan fremstilles på følgende måte ved bruk av Exchange Online i nettleser:

AD FS and SSO with online services



1. Bruker åpner nettleser og sender HTTPS-request mot Exchange Online.
2. Exchange Online mottar forespørsel og dersom klient er del av en Exchange hybridløsning sendes den videre til Azure AD.
3. Klient sender HTTPS-request mot Azure AD.
4. Klient blir sendt til lokal ADFS-server basert på UPN-suffiks.
5. Klient sender en HTTPS-request til ADFS-server.
6. Hvis brukeren er logget på domenet bruker ADFS-serveren Kerberos-ticket og ber AD om autentisering. Hvis brukeren logger på fra utsiden (internett) eller på en klient som ikke er med i domenet får bruker spørsmål om brukernavn og passord.
7. AD autentiserer brukeren og sender tilbake nødvendig informasjon til ADFS så den kan generere brukerens claims.
8. ADFS genererer claim for brukeren, signerer dette og sender til klienten i form av et token. Klienten sender dette til Azure AD.
9. Azure AD verifiserer at token kommer fra en part der federation trust er etablert.
10. Azure AD lager og signerer et nytt token og sender til klient som igjen videresender token til Exchange Online.
11. Exchange Online mottar token og validerer det. Det utstedes en session cookie som sier at klient er autentisert og gis tilgang til postboks.

Alt dette skjer transparent for brukeren.

ADFS bør vurderes under design av Office 365-løsninger og sees i sammenheng med andre eksterne tjenestetilbydere.

I UH-sektoren er det vanlig at det allerede finnes en fødereringsløsning, dersom det ikke gjør det er det anbefalt at dette tas med i Office 365-design. Ofte benytter man muligheten til å oppgradere eller parallell-etablere en ny ADFS-løsning basert på minimum ADFS 3.0 (Windows Server 2012R2) for å kunne ta i bruk ny funksjonalitet.

De aller fleste institusjonene i UH-sektoren, som har tatt i bruk Office365, har satt opp en lokal ADFS løsning for å håndtere føderert pålogging. Som beskrevet i kapittel **Feil! Fant ikke referanseskilden.** (FEIDE) kan en her sette opp en link mellom ADFS og FEIDE for å få pålogging i Office365 ved bruk av FEIDE.

I UH-sektoren er det to alternativer til å sette opp en lokal ADFS løsning for å få føderert pålogging:

- 1) UHAD ADFS – Kontakt USIT/UNINETT for mer informasjon.
- 2) Direkte AzureAD-FEIDE – Pilot-tjeneste. Kontakt UNINETT for mer informasjon.

10. E-post

10.1 Migreringsstrategier

Det finnes følgende migreringsstrategier å ta utgangspunkt i:

Hybrid (forutsetter Exchange 2010 med patcher eller nyere)

Cutover (fra eldre Exchange eller annet e-postsystem)

Office 365 til Office 365

Det er viktig at klientprogramvare er oppdatert til siste versjon, dette gjelder også i terminalservermiljøer. Office 365 ProPlus anbefales på klienter. Det anbefales ekstra testing i terminalservermiljøer med hensyn til caching/OST-filer og ytelse. Tjenesten bør også testes på flere lokasjoner/samband for å sikre at ytelsen er tilfredsstillende.

10.1.1 Hybrid

Oppsett av hybridlink mellom lokal Exchange og Office 365 brukes i scenarioer der man ønsker å gradvis flytte postbokser til O365. Alle e-postadresser fra lokal Exchange må være synkronisert ut til O365 før migrering starter for å sikre at e-postflyt fungerer. Dette innebærer brukere, møterom, delte postbokser, grupper, kontakter og andre ressurser.

Ved bruk av hybridlink migreres rettigheter, men det kan oppstå situasjoner der enkelte rettigheter ikke fungerer på tvers av lokal Exchange og O365. Det er anbefalt å flytte over et sett postbokser for å verifisere funksjonalitet. Det vil i denne sammenheng være gunstig at personer som samhandler migreres på samme tidspunkt.

Mobile enheter og Outlook rekonfigureres automatisk ved bruk av hybridlink.

Når det gjelder tidspunkt for endring av MX-pekere vurderes dette fra sak til sak.

10.1.2 Cutover

Ved cutover-migrering gjøres jobben som en standard e-postmigrering. Det betyr fullstendig klargjøring av nytt miljø, og brukere gis tilgang til nytt system samtidig. Man kan benytte tredjepartsverktøy eller standardverktøy.

Et annet alternativ er å ta i bruk O365 og gi brukerne tilgang på gamle data i form av PST-filer og selv la de importere dette etter behov.

10.1.3 Office 365 til Office 365

Oppsett av ny tenant gjøres på normal måte som beskrevet under Hybrid-avsnittet over.

Datamigrering gjøres ved å benytte tredjepartsverktøy eller la brukerne håndtere import selv. Spesielle hensyn må tas når det gjelder flytting av domener fra opprinnelig tenant til nyetablert tenant. Et domene kan kun være registrert i en tenant, som betyr at pålogging kan kun være aktiv mot en tenant samtidig. Migrering må derfor gjøres mot <domene>.onmicrosoft.com-adressen.

Før domenet fjernes fra opprinnelig tenant må alle oppføringer knyttet til dette domener på alle objekter være fjernet. I det man fjerner domenet fra opprinnelig tenant vil det være nedetid på tjenesten.

10.2 Avvikling av lokal Exchange

I skrivende stund supporterer ikke Microsoft redigering av attributter som proxyaddresses, mail og mailnickname manuelt på brukerobjekter i AD. Den supporterte løsningen innebærer at man beholder

en lokal Exchange-server som ikke har noen roller, men kun brukes til administrasjon. Denne kan lisensieres kostnadsfritt med "hybrid"-lisens.

Et annet alternativ er at man har en løsning som vedlikeholder/provisjonerer attributter på brukerobjekter.

10.3 Backup

Slettede elementer ligger i papirkurven i 90 dager og blir deretter fjernet permanent hos Microsoft. Dette må sees mer på som en disaster recovery-løsning enn backup. Det finnes tredjepartsprodukter dersom man ønsker en mer fullverdig backupløsning.

Eksempler på leverandører er Veeam, Cloudfinder, Spanning (Dell EMC) og AvePoint.

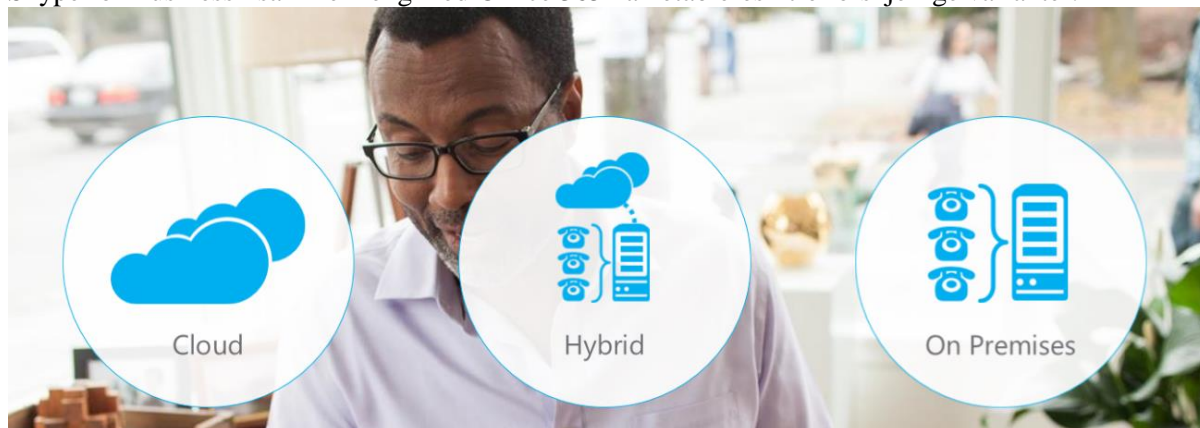
10.4 Fast Track

Fast Track er en tjeneste fra Microsoft der man kan få teknisk bistand for å ta i bruk tjenester i Office 365. Man kan også søke om tilskudd dersom man er kvalifisert for dette.

Sjekk nærmere med Microsoft-partner for å kartlegge muligheten for Fast Track-midler.

11. Skype for Business

Skype for Business i sammenheng med Office 365 kan etableres i tre forskjellige varianter.



On-Premises

Ren on-premises etablering er fullt mulig å kombinere med Office 365 generelt. Har man allerede etablert Lync 2013 eller Skype for Business 2015 kan man fortsette å benytte dette utelukkende. Man mister blant annet mulighet for «Broadcast Meetings», men kan beholde «Enterprise Voice» som før. Det er viktig å huske å ikke «enable» domenet for Skype for Business online hvis man velger ren on-premises løsning, hvis ikke kan problemer med å føderere mot andre organisasjoner på Skype for Business Online oppstå.

Hybrid

I et hybridoppsett beholder man eksisterende Lync 2013 eller Skype for Business 2015 on-premises miljø, men man kobler det sammen med Skype for Business i Office 365 tenanten slik at de kan dele på brukere i samme organisasjon. On-premises miljøet vil fremdeles kontrollere løsningen, men man har mulighet til å flytte noen brukere ut i Office 365, mens andre fremdeles vil leve på on-premises løsningen. «Enterprise voice» kan håndteres som før, og det er også mulighet å levere telefoni til brukerne som flyttes online gjennom on-premise miljøet.

Cloud

Her ligger hele Skype for Business miljøet i Office 365, og det er ingen servere on-premise. Dersom man allerede har et lokalt Lync 2013 eller Skype for Business 2015 miljø, må man gjennom hybrid for å komme til cloud uten at det skal påvirke brukerne negativt. Har man Lync 2010 må man oppgradere gjennom Skype for Business 2015.

11.1 Hensyn

11.1.1 Telefoni

Det er dessverre ikke mulig å tilby brukere norske telefonnummer i en ren cloud løsning, og det ser ikke ut til å bli mulig i nær fremtid. For å allikevel kunne levere telefoni til brukerne i en ren cloud løsning finnes det to alternativer:

- Beholde hybrid on-premises.
Det ene alternativet er å beholde eller opprette et on-premises miljø, og levere telefoni til brukere i skya igjennom denne. Summetone kan leveres gjennom en SIP trunk direkte til en leverandør, til en lokal PBX eller via en gateway til ISDN eller analoge linjer.
- Cloud Connector Edition
Cloud connector edition er et sett med virtuelle servere som blir etablert som en egen pakke

på en dedikert virtuell host og brukes som en slags «appliance» som leverer telefoni til skya. Teknisk sett er det et nedstrippet on-premises miljø som kjører inne i «appliance-n», men denne er «hands off managed». Bak denne kan man sette alle de samme typene telefonileveranser man kan bruke i en on-premises løsning, enten en SIP trunk direkte til en leverandør, til en lokal PBX eller gjennom en gateway til ISDN eller analoge linjer.

11.1.2 Innringte konferanser

Konferansenummer kan leveres gjennom Office365. Det er ikke mulig å bruke eventuelle nummer som kommer inn gjennom on-premise hybrid eller cloud connector til konferansenummer for brukere i skya.

11.1.3 3. parts integrasjoner

Direkte integrasjon med 3. parts programvare er foreløpig ikke mulig mot Office 365. Det betyr at produkter som bruker «UCMA APIet» for å integrere med Lync og Skype for Business ikke kan være med på en migrering. Eksempler på slike integrasjoner er Competella eller Trio sentralbord. Det er heller ikke mulig å lage statiske ruter av SIP trafikk i Office 365 slik man ofte har benyttet for å integrere med blant annet videokonferansesystemer. Flere av disse løsningene har mulighet til å bli rutet til med DNS SRV oppslag for «SfB federation» i stedet for direkte ruting gjennom lokal infrastruktur.

11.2 UH Skype

«UH Skype» fra UNINETT tilbyr Skype for Business som en skytjeneste og er tilgjengelig som produkt for alle UNINETT sine kunder. Tjenesten er basert på en «on-premises» versjon av Microsoft sin Skype for Business-plattform. Den redundante serverplattformen er sentralt driftet av tjenesten og den enkelte kunde forholder seg bare til egen AD og Exchange for håndtering av egne brukere. I tjenesten benyttes organisasjonens eget domene slik at man kan gjøre eventuell nødvendig federering mot andre organisasjoner. Tjenesten fungerer som hybrid-løsning i tilfeller hvor kunden samtidig ønsker å benytte tjenester fra Office 365.

11.2.1 AD

For å kunne ta i bruk tjenesten «UH Skype», kreves også bruk av tjenesten «UH AD» for synkronisering av nødvendig brukerinformasjon med organisasjonens egen AD.

11.2.2 Telefoni

«UH Skype» kan leveres både uten eller med funksjonen «Enterprise Voice» for telefoni. Dersom det ønskes telefoni, leveres det gjennom tjenestene «Sanntid» og «Sanntid tale» slik at man kan benytte de telefonnummer man allerede besitter i organisasjonen. «Sanntid tale» er knyttet opp mot den til enhver tid aktuelle avtalepartneren på telefoni. Gjennom «Sanntid» kan man også få tilpassede hybridløsninger for gradvis migrasjon fra gammel til ny telefoniplattform og tilleggsløsninger for bl.a. telefonkonferanser, faks-håndtering (fax-to-mail) og spesielle viderekoblinger av nummer.

Gjennom «Sanntid» vil alle organisasjonens telefonnummer også bli registrert i ENUM. Det tilgjengeliggjør organisasjonen for direkte oppringing fra organisasjoner som støtter dette, uten å gå veien via en telefonoperatør.

11.2.3 Innringte konferanser

Konferansenummer til bruk i «Skype for Business» vil være til et fritt valgt nummer fra organisasjonens egne nummerserier.

11.2.4 Støttesystem

«UH Skype» er teknisk fleksibel med hensyn til behovet for støttesystem og 3dje part integrasjoner. Plattformen har full tilgang til UCMA APIet og et teknisk forum tilrettelegger vurderer fortløpende behov for integrasjon etter bl.a. innmeldinger fra kundene.

Tjenesten støtter alle sentralbordsystemer som er basert på telefoniruting, samt Trio og Competella med sine API-integrasjoner.

«UH Skype» er også tett integrert med tjenesten «Nasjonal Videobro» som bl.a. gir utvidet videomøtefunksjonalitet og sømløs oversettelse mellom formatene SfB, SIP, H323 og WebRTC.

12. SharePoint

Valget mellom lokal SharePoint og SharePoint Online (O365) kan være komplisert og sammensatt. De fleste bruker SharePoint til følgende:

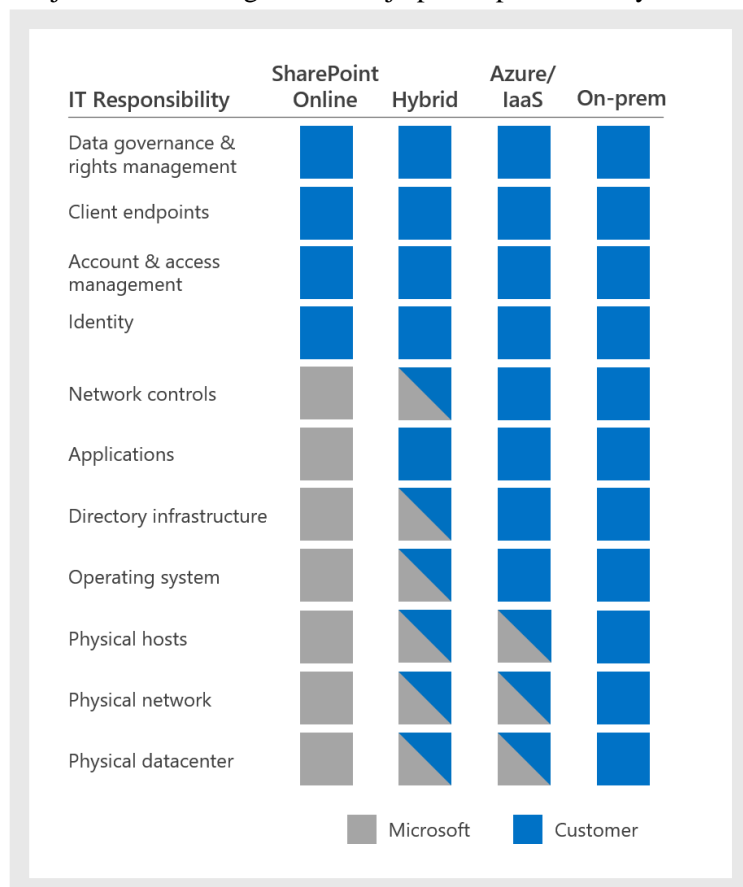
- Publisering av nyheter, bilder, HR-, HMS- og IT-informasjon samt annen relevant intern informasjon.
- Prosjektområder og avdelingsområder hvor dokumentdeling foregår mellom interne ansatte og i noen tilfeller også med eksterne.
- Publisering av portaler/sider på internett (krever lokal SharePoint)

Plassering av løsningen avhenger av flere faktorer som bør tas hensyn til, som for eksempel brukeropplevelse, samhandlingsfunksjonalitet, kostnader, etc.

Vanligvis velges et hybridoppsett som gjør at man kan velge å fase ut deler av løsningen til O365, mens man beholder andre kritiske tjenester i eget datasenter. Intranettløsninger som det er investert mye i beholdes gjerne lokalt. Løsninger som ekstranett, prosjektområder og OneDrive er som regel de første som flyttes til O365.

Hovedårsaken til dette er som regel at disse er teknisk enklest å flytte, samt mulig reduksjon av påkrevd lokal infrastruktur.

Ved en migrering til SharePoint Online, må det tas hensyn til informasjonsarkitektur, funksjonalitet rundt søk, filmetadata og versjonshistorikk. I skrivende stund kan kun filmetadata og versjonshistorikk migreres ved hjelp av 3.parts verktøy.



12.1 Backup

Det eksisterer ingen backup-tjeneste levert av Microsoft for SharePoint Online utover den innebygde papirkurv-løsningen. Når et dokument slettes vil dette ligge i "papirkurven" til SharePoint-området i 90 dager og deretter fjernes permanent. Som for Exchange Online er dette mer å betrakte som en disaster recovery-løsning. Merk også at ikke alle filtyper nødvendigvis er inkludert i det Microsoft har kopi av, det kan være begrenset til Office-dokumenter.

Dersom man ønsker backup funksjonalitet utover dette kan det implementeres ved hjelp av PowerShell eller tredjepartsløsninger.

Leverandører av slike produkter er blant annet Metalogix, CloudAlly og AvePoint.






13. OneDrive

OneDrive er en tjeneste utviklet primært som en Enterprise File Sharing (EFS) løsning, men dette er også en tjeneste som er ment å erstatte fillagring på fellesdisker.

Det er viktig å holde orden på følgende begreper når det gjelder OneDrive, siden Microsoft har flere tjenester som heter det samme.

- OneDrive – Privat: Dette er en gratis tjeneste som alle kan få ved å lage en Microsoft konto i for eksempel Outlook.com. Tjenesten kommer med en synkroniserings klient på iOS, Windows og Android.
- OneDrive for Business: Dette er hver enkelt brukers **personlige lagring** i O365 og skal brukes av brukeren for deres personlige samhandlings behov. Dette er en tjeneste som på veldig mange måter skal få bort «Shadow IT». Data i OneDrive slettes etter 30 dager som standard hvis bruker kontoen slettes fra O365. Tjenesten kommer med en synkroniseringsklient på iOS, Windows og Android.
- SharePoint dokumentbiblioteker: Dette er fellesdokument-området for samhandling, og skal brukes til lagring av felles dokumenter og informasjon. MS har lansert en preview av en ny synkroniserings klient/app for SharePoint biblioteker som også vil hete OneDrive.

I en nær fremtid vil OneDrive bruker opplevelsen se slik ut for alle brukere:

- ▼  Advania
 - >  Document Center - Forretningsforbindelse
 - >  OneDrive - Advania
 - >  OneDrive - HangConsulting
 - >  OneDrive - Personal

13.1 Bruksområder

Personlig OneDrive er tenkt brukt for lagring av personlige dokumenter og i de tilfeller man har behov for å dele et begrenset antall dokumenter med enkeltpersoner. Personlig OneDrive er ikke ment for gruppesamhandling.

SharePoint kan brukes til fellesbibliotek der man tilrettelegger for gruppesamhandling.

13.2 Backup

Det eksisterer ingen backup tjeneste levert av Microsoft for OneDrive. Avhenger av kravene for backup kan dette implementeres ved hjelp av PowerShell eller tredjepartsløsninger (se avsnitt under SharePoint og backup for mer informasjon om dette)

13.3 Migrering

Det finnes tredjepartsverktøy for migrering til OneDrive/SharePoint. Det er også mulig å utvikle egne skript for å håndtere dette.

Ved migrering av hjemmeområder blir anbefalingen ofte at brukere gjør dette selv for å få et forhold til OneDrive og bruk av tjenesten.

14. Avviklingsmuligheter for Office 365

Når det gjelder mulighet for å avslutte bruk av tjenester i Office 365 finnes det ingen standardmåte for dette. Det må planlegges for hver tjeneste som skal migreres ut.

14.1 E-post

Ved hybridoppsett kan man migrere postbokser tilbake til lokal løsning. I skrivende stund blir ikke mobile enheter automatisk rekonfigurert.

Ved migrering til andre tilbydere eller uten hybridlink anbefales bruk av tredjepartsverktøy.

14.2 Skype

I et hybridoppsett kan brukere flyttes mellom on-premises og online med administrasjonsverktøy.

Dersom brukerne er migrert ut og on-premises miljøet er avviklet, kan man etablere et on-premises miljø, sette opp en hybrid og migrere brukerne tilbake for å avvikle tjenesten i Office 365.

14.3 OneDrive/Sharepoint

Her anbefales bruk av tredjepartsverktøy og/eller PowerShell-skript for datamigrering avhengig av mengde og kompleksitet.

Identiteter kan fjernes på flere måter, men heller ikke her finnes det noen standardoppskrift. Man kan bruke AAD Connect til å fjerne alle synkroniserte brukere eller man kan endre alle brukerne i Azure AD om til rene cloud-brukere og deretter fjerne de.

15. Hvordan lykkes med ditt prosjekt

Skal du lykkes med ditt Office 365 prosjekt er det viktig å legge vekt på følgende områder tidlig i prosjektet:

- AD/Identitetsløsninger/FIM/andre
- Fødereringsløsninger mot andre systemer, for eksempel FEIDE.
- Exchange
- Skype
- SharePoint

Kompetansen på disse områdene kan bygges opp lokalt eller kjøpes hos partnere, men det er viktig at det etableres tett kontakt mellom aktørene tidlig i prosessen. Det er viktig at disse blir tidlig tatt med i dialogen i et Office 365 prosjekt for å se om det er avhengigheter eller utfordringer.

Utover dette bør en teknisk prosjektleder bestemme hvor mye og når de skal inn i prosjektløpet.

Det er viktig å ha en teknisk prosjektleder som har breddekunnskap i Office 365 og kjenner on-premises miljøet til å vite hva som skal inn når i prosjektet. En viktig oppgave er også å holde dialogen med de ulike partnere og stille riktige krav for kunden.

Det kan også være smart å ha med representanter fra ulike avdelinger/enheter i prosjektgruppa.