

# Säker video och chatt – Tjänstebeskrivning



## Innehåll

Huvudfunktioner och egenskaper.....	2
Chattfunktion före, under och efter möten.....	2
Grupp- och enskilda videosamtal.....	3
Möten med eller utan e-legitimation (BankID, Freja eID, SITHS).....	4
Federering av chatsamtal mellan olika Hubsinstanser.....	5
Delning av skärm, dokument och länkar i realtid.....	6
Interaktiva mötesverktyg (reaktioner, handuppräckning, bakgrundsfilter).....	7
Modereringsverktyg för mötesledare.....	9
Mobil- och webbläsarstöd utan installation.....	9
Externa deltagare via länk.....	10
Integrationer och användningsflöden.....	12
Säkerhet, regelefterlevnad och driftmiljö.....	13
Confidential compute.....	14

## Säker video och chatt

Säker video och chatt är en **integrerad kommunikationsplattform** för videomöten och chatt, utformad för högsta säkerhet och dataskydd. Tjänsten bygger på beprövad öppen källkodsteknologi för **videokonferens och samarbete** och har anpassats till att passa offentlig sektors krav på sekretess.

## Huvudfunktioner och egenskaper

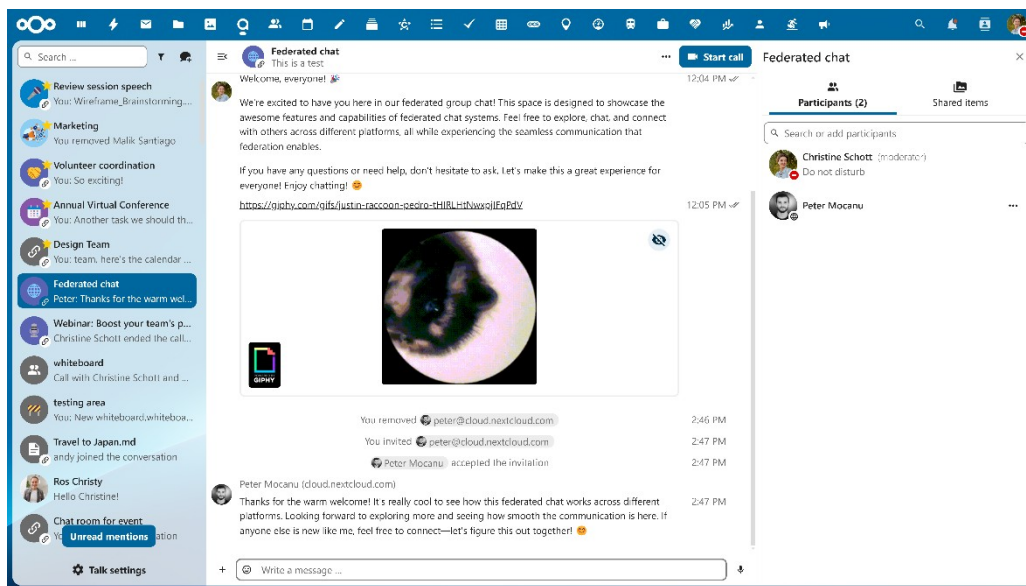
### Chattfunktion före, under och efter möten

Centralt i tjänsten är chattrum, till varje chattrum kan man koppla individer och samtala antingen via text i chattytan eller skapa upp ett videosamtal. Sättet att kommunicera har blivit vanligt i samband med Microsoft Teams som har liknande funktionalitet.

Innan mötet kan deltagare skriva förberedande meddelanden eller agendor i chatten. Under mötet fungerar chatten som ett komplement till tal och video – här kan länkar, frågor och kommentar utbytas parallellt med diskussionen. Chatten är integrerad i samma vy som videosamtalet, vilket innebär att deltagarna kan följa konversationen skriftligt utan att lämna mötesfönstret.

En viktig egenskap är att chattens innehåll **finns kvar även efter att mötet avslutats**. Deltagare (både interna och externa gäster) kan återvända till samtalet i efterhand för att läsa konversationshistoriken, ladda ner delade filer eller fortsätta diskussionen asynkront. Detta gör möteschatten till ett ställe för **dokumentation och uppföljning**, där beslut och delade resurser under mötet bevaras. Chatten har stöd för formatering av text (t.ex. **fetstil**, *kursiv*, listor med mera) för att göra längre meddelanden mer läsbara. Dessutom kan meddelanden i chatten kopplas vidare in i andra delar av plattformen – exempelvis kan ett chattmeddelande omvandlas till en uppgift i uppgiftslistan eller en kalenderpost, vilket knyter samman kommunikationen med uppföljande aktiviteter.

Observera att chatten kan arkiveras eller raderas baserat på inställningar som administratören sätter.



*Chattgränssnittet när inte ett videosamtal pågår*

## Grupp- och enskilda videosamtal

Tjänsten stödjer både **gruppvideosamtal** och **enskilda videosamtal**, med end-to-end-kryptering för att skydda kommunikationens konfidentialitet. Användare kan enkelt starta **privata möten** (en-till-en) eller **offentliga/gruppmöten** med flera deltagare. Video- och ljudströmmen överförs direkt mellan deltagarna i realtid och är krypterad, utan att passera genom tredje parts servrar. Detta innebär att även metadata om samtalen hålls privat inom Hubs infrastruktur. För större möten använder plattformen en skalbar serverkomponent (High Performance Backend) som möjliggör stabila konferenser med **hundratals deltagare** utan att kompromissa säkerhet eller prestanda.

Vi kan även koppla på en SIP-brygga för att **möjliggöra inringande samtal från mobiltelefon**. Med detta tillägg är Säker Chatt och video en komplett plattform som kan användas som en ersättare till tex Skype for business

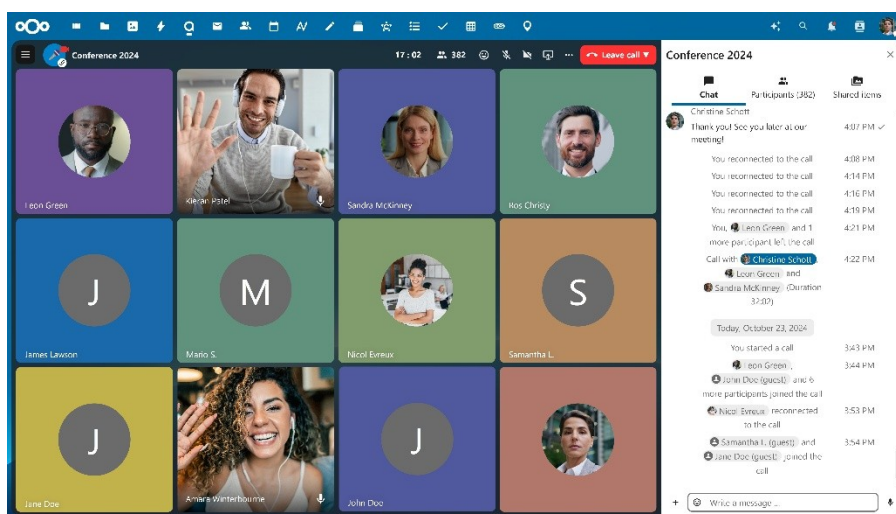
Vid start av ett möte kan värderna välja om det ska vara **publikt** (öppet via länk) eller **privat** (endast inbjudna). Deltagare har möjlighet att ansluta via valfri modern webbläsare eller mobil enhet – ingen installation eller konto krävs för gäster. Om en deltagare lämnar ett möte kan den associerade **chatrummet** fortsätta vara öppet, så att information och material finns kvar för alla

### ITSL Solutions AB

Universitetsallen 32, 852 30 Sundsvall  
+46 (0)70 – 330 11 89 • [info@itsl.se](mailto:info@itsl.se)

Organisationsnr. 559261-9265 • Innehar F-skatt

behöriga även efter att videosamtalet avslutats. Tjänsten uppfyller alla professionella krav för flexibel kommunikation, från spontana videosamtal till planerade webinarier och presentationer.



*Exempel på gränssnitt för ett videosamtal med chattfunktion i sidopanelen.*

## Möten med eller utan e-legitimation (BankID, Freja eID, SITHS)

För extra säkerhetskrav erbjuder HubS möjligheten att kräva **elektronisk identifiering** av mötesdeltagare. Vid schemaläggning av ett möte kan organisatören välja om inloggning med e-legitimation ska krävas för att ansluta. Om detta val är aktivt behöver externa deltagare autentisera sig med **BankID, Freja eID+** eller **SITHS** (beroende på vad mötesorganisatören ställer in) innan de släpps in i mötet. Detta innebär att exempelvis medborgare eller konsulter som bjuds in till ett känsligt möte först får legitimera sig via en säker inloggningssida – samma typ av identifiering som vid e-tjänster – och först därefter får de access till videomötet.

Denna funktion är särskilt värdefull i scenario där **identitetskontroll** är viktigt, såsom vid myndighetsutövning, hälso- och sjukvårdskonsultationer eller andra konfidentiella ärenden. Genom BankID/Freja eID kan man med hög säkerhet veta **vilken person** som döljer sig bakom en anslutning, inte bara ett namn som användaren skrivit in. SITHS-stödet möjliggör dessutom säker inloggning för personal inom vård och omsorg. Alla tre metoder uppfyller högt ställda krav på tillitsnivå och är kompatibla med den svenska infrastrukturen för e-legitimation.

Rent praktiskt kan funktionen fungera så att möteslänken först leder till en **inloggningssida** där deltagaren väljer sin e-legitimation. Vid lyckad autentisering omdirigeras personen automatiskt in i mötesrummet. Om autentisering misslyckas eller inte genomförs, nekas åtkomst. Som organisatör kan man välja att aktivera detta krav per möte – t.ex. bara för de möten som behandlar sekretessbelagd information – medan andra möten kan vara öppna för gäster utan inloggning. Flexibiliteten gör att plattformen stödjer både **högt säkerhetsklassade möten** och mer informella möten, inom samma system. All hantering av e-legitimation sker via etablerade identitetsleverantörer och följer gällande standarder (OIDC/SAML2), och ingen känslig ID-information lagras på vår plattform utöver det nödvändiga för att validera sessionen.

## Federering av chatsamtal mellan olika Hubsinstanser

Den underliggande plattformen är baserad på teknologi från Opensource plattformen Nextcloud, som har inbyggt stöd för federation – en standardiserad lösning (baserad på öppna protokollet Open Cloud Mesh) som möjliggör säker kommunikation och datautbyte mellan separata serverinstanser

Varje organisation har sin egen isolerade Hubs-instans, vilket garanterar att respektive kunds data hålls åtskild och privat. Samtidigt kan dessa instanser länkas säkert: varje användare har ett Federerat Cloud-ID (likt en e-postadress) som kan delas med partnerorganisationer för att initiera en koppling.

När två organisationer har etablerat en betrodd federerad koppling kan deras användare enkelt hitta varandra och starta en gemensam chatt eller dela filer, utan att kompromissa sekretessen – all data stannar inom respektive organisations skyddade miljö.

Användaren deltar genom sitt vanliga konto och gränssnitt, och bakom kulisserna utbyter de två serverna informationen på ett kontrollerat sätt.

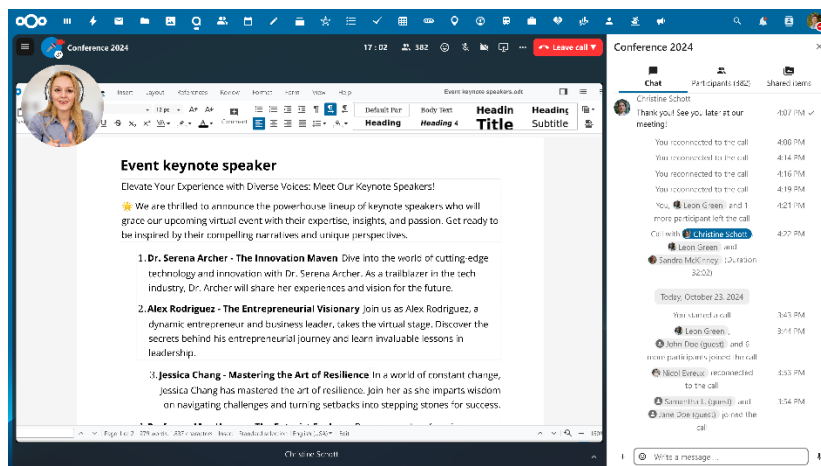
**Chatt och video över gränserna:** Hubs federationsstöd omfattar både skriftlig chatt och ljud/video-samtal. Användare kan skapa gemensamma chattrum med deltagare från andra organisationers servrar och använda alla centrala chattfunktioner (t.ex. formaterad text, omnämmanden, omröstningar m.m.)

Det går även att initiera säkra videomöten eller röstsamtal mellan användare på olika Hubs-instanser – plattformen stödjer att organisera krypterade möten över servergränserna för exempelvis projekt med externa partners. Varje deltagare ansluter från sin egen server, men upplever det som ett gemensamt mötesrum. Detta möjliggör enkel kommunikation mellan kommuner på ett säkert sätt.

## Delning av skärm, dokument och länkar i realtid

En **skärmdelningsfunktion** är inbyggd för att underlätta presentationer och samarbeten. Under videomöten kan deltagare dela hela sin skärm eller ett specifikt programfönster med övriga, exempelvis vid genomgång av en presentation eller demonstrering av ett system. Alla andra deltagare ser den delade skärmen i realtid, och funktioner för **helskärmsläge** samt växling mellan videoflöden och skärmvy finns tillgängliga för en optimal mötesupplevelse.

Parallellt med skärmdelning stöds **direkt delning av dokument och länkar** i möteschatten. Deltagarna kan enkelt skicka filer från den integrerade filplattformen eller klistra in webblänkar i chatten under samtalets gång. Eftersom filhanteringen är tätt integrerad dupliceras inte filer i onödan – en fil som redan finns uppladdad på plattformen kan refereras direkt i mötet utan ny uppladdning. Alla delade dokument, bilder eller länkar sammanställs i en översikt, så att deltagare i efterhand kan hitta tillbaka till mötets material. Funktionen möjliggör smidigt samarbete där exempelvis **mötesanteckningar, agendor eller kalkylblad** kan öppnas och redigeras gemensamt under mötet, tack vare integrationen med kontorsprogram online (tillval).



## Interaktiva mötesverktyg (reaktioner, handuppräckning, bakgrundsfilter)

För att öka interaktiviteten och engagemanget i möten innehåller plattformen flera användbara mötesverktyg. Deltagarna kan använda **reaktionsknappar** (t.ex. tumme upp, applåd-emoji med mera) för att snabbt ge feedback utan att avbryta talaren. Reaktionen på meddelanden och inlägg visas direkt i chatten, vilket skapar en mer dynamisk kommunikation. Under pågående videomöten kan så kallade **”flytande reaktioner”** (animationer som hjärtan, konfetti etc.) aktiveras, vilka visas över videoströmmen som en lättsam feedback från publiken.

Funktionen **”räck upp handen”** är tillgänglig för mötesdeltagare som vill indikera att de önskar ordet. När en deltagare räcker upp handen markeras det tydligt i gränssnittet för moderator och övriga, så att mötesledaren kan ge ordet i turordning. Detta är särskilt värdefullt i större möten eller webbseminarier där många är närvarande. Tjänsten erbjuder även **virtuella bakgrunder och bakgrundsfilter** – användare kan välja att suddas ut sin bakgrund eller ersätta den med en bild, vilket skyddar privatlivet och ger ett professionellt intryck. Bakgrundsblur fungerar direkt i webbläsaren utan behov av extern programvara, tack vare inbyggt WebRTC-stöd för denna funktion. Sammantaget främjar dessa interaktiva verktyg en **mer engagerande och kontrollerad mötesupplevelse**, där alla kan göra sin röst hörd på ett ordnat sätt.



*Hubs har stöd för reaktions-emoji och handuppräkning i mötesgränssnittet*

## Samtalsinspelning (valbar funktion)

Vid behov av dokumentation eller spridning av mötesinnehåll finns stöd för **inspelning av samtal**. Mötesorganisatören (moderatoren) kan aktivera inspelning under ett videomöte, varpå alla deltagare tydligt meddelas att **”inspelning pågår”**. En indikator i gränssnittet visar att mötet spelas in, och deltagare som ansluter sent får också denna information [rcasys.com](https://rcasys.com). Inspelningsfunktionen är som standard avstängd och kan aktiveras av administratören för de möten där det är påkallat – detta för att följa lagar och policies kring samtycke.

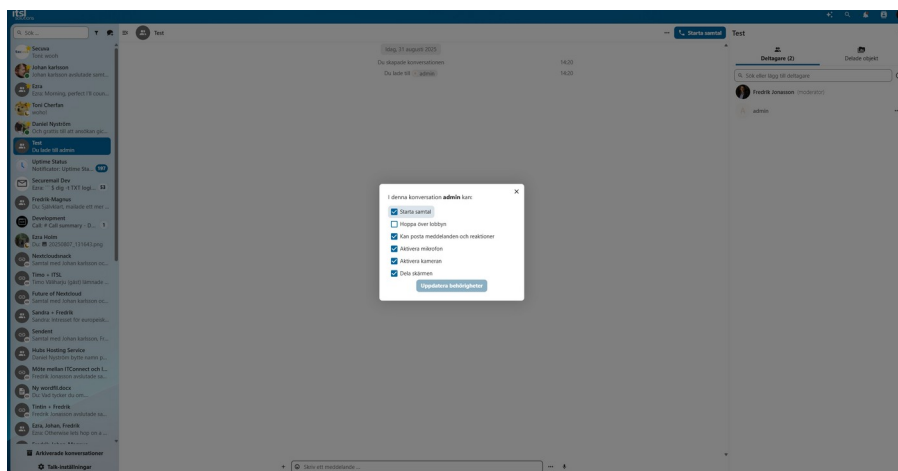
När ett inspelat möte avslutas sparas videofil (**webm-format**) säkert på servern eller en dedikerad lagringsplats. Endast mötesägaren (eller definierade behöriga) har initial åtkomst till inspelningen. Denne kan välja att dela inspelningsfilen direkt i mötets chattrum – då blir den synlig för alla deltagare att spela upp – eller behålla filen privat för intern arkivering. Inspelningsfunktionen är användbar för t.ex. kommunal verksamhet som behöver dokumentera viktiga avstämningar, eller för utbildningsändamål där inspelade lektioner ska kunna återspelas av studenter. Tjänsten tillhandahåller även **tidsangivelser** (tidsstämplar) under pågående inspelning, så att moderator lätt kan hålla reda på mötets längd. All lagring av inspelat material sker i den säkra, Sverige-baserade molninfrastruktur som tjänsten driftas på – inget skickas till extern part.

## Modereringsverktyg för mötesledare

För möten med många deltagare eller formella webinarier finns kraftfulla **modereringsverktyg** som hjälper mötesledaren att hålla ordning.

Mötesledaren (den som skapat mötet eller utsedd moderator) kan **bjuda in eller ta bort deltagare**, samt **stänga av deltagares mikrofon** vid behov. Det är också möjligt att tysta (mute) alla deltagare utom talaren för att undvika bakgrundsljud, och sedan ge ordet genom att upphäva tystnaden för en viss person. Moderatoren kan även dela ut **presentatörsbehörighet** till utvalda deltagare, vilket låter dem dela sin skärm eller ta över presentationen.

Vid öppna möten som delas via länk kan man aktivera en **väntrumfunktion** (lobby) för gäster. Externa deltagare hamnar då först i ett väntrum och kan släppas in av mötesledaren en och en eller alla på en gång. Detta förhindrar oönskade gäster från att hoppa in utan kontroll. Moderatoren kan dessutom utnyttja **hanteringen av uppsträckta händer** (se föregående avsnitt) för att ge ordet i tur och ordning, vilket är praktiskt i exempelvis kommunfullmäktigemöten eller stora presentationer. Alla moderatorverktyg är åtkomliga via ett tydligt gränssnitt: mötesledaren har en **kontrollpanel** där deltagarlista syns och åtgärder (t.ex. ”ta bort användare”, ”tysta alla”) finns med ett klick.



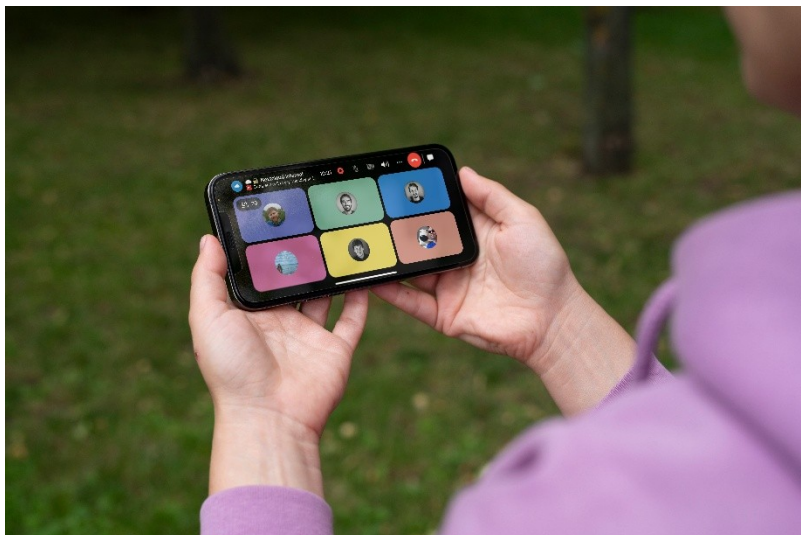
## Mobil- och webbläsarstöd utan installation

*Säker video och chatt* är **plattform- och klientoberoende**. Deltagare kan ansluta till möten direkt via en vanlig webbläsare (Chrome, Firefox, Edge, Safari m.fl.) utan att behöva installera något program eller plugin – tack vare

att tjänsten baseras på standarden WebRTC för realtidskommunikation. Gränssnittet i webbläsaren är responsivt och fungerar lika bra på en stationär dator som på en mobil enhet eller surfplatta. För användare som föredrar mobilappar finns även dedikerade appar för Android och iOS att tillgå, men dessa är inte ett krav – **all funktionalitet är åtkomlig via webben.**

För intern personal kan single sign-on användas för inloggning i tjänstens webbgränssnitt. En extern deltagare klickar bara på möteslänken och kommer direkt in i mötet via sin webbläsare, där hen anger sitt namn. Det innebär att även om mötesorganisatören använder tjänsten internt, kan t.ex. medborgare, leverantörer eller partners medverka **utan tekniska hinder**. Lösningen är utformad för att eliminera barriärer som annars uppstår med vissa proprietära system som kräver installation av klient. Dessutom finns stöd för alla vanliga operativsystem (Windows, macOS, Linux) via antingen webbläsare eller den valfria skrivbordsklient som erbjuds. Sammantaget garanterar detta **maximal tillgänglighet** – användarna kan ansluta var de än befinner sig, på valfri enhet, så länge de har internetuppkoppling.

Om administratören bestämt att inloggning ska ske med bankid eller liknande kommer den externa användaren att lotsas via vald inloggning innan hen ansluts till mötet.



## Externa deltagare via länk

Det är enkelt att involvera **externa deltagare** i säkra videomöten. Varje mötesrum kan generera en **unik inbjudningslänk** som kan skickas till

### ITSL Solutions AB

Universitetsallen 32, 852 30 Sundsvall  
+46 (0)70 – 330 11 89 • [info@itsl.se](mailto:info@itsl.se)

Organisationsnr. 559261-9265 • Innehar F-skatt

personer utanför organisationen. Genom att klicka på länken kan en gäst ansluta direkt till mötet via webbläsaren och får då tillgång till både video, ljud och chat (med de begränsningar som mötesledaren eventuellt ställt in). Gäster behöver varken konto hos er eller någon särskild programvara, vilket gör tröskeln låg för exempelvis invånare eller externa konsulter att delta i digitala möten.

Länkarna kan skickas ut via e-post, SMS eller publiceras i kalenderinbjudningar. För extra säkerhet kan mötesorganisatören också koppla **lösenord** till möteslänken eller sätta en **utgångstid**, så att länken bara fungerar fram till mötets slut – detta förhindrar obehörig åtkomst om länken skulle spridas vidare av misstag. Defaultinställningen i Hubs är att samtliga externa mötesdeltagare ska identifiera sig med BankId för att säkerställa identiteten på den som ansluter till mötet.

**Inbjudan: Nytt möte i Nextcloud**

Från Anna Ignell via Hubs - ITSL Solutions på 2025-05-23 14:24

✉ Detaljerad information ⓘ Meddelandefinfo ☰ Oformatterad text

event.ics (-992 B)



Anna Ignell har bjudit in dig till "Nytt möte i Nextcloud"

► **Titel:**  
Nytt möte i Nextcloud

📅 **När**  
Om 35 minuter den fredag 23 maj 2025 mellan 15:00 - 16:00  
(Europe/Stockholm)

Acceptera

Avböj

Fler alternativ ...

*Exempel på e-postinbjudan med möteslänk samt gästvy vid anslutning.*

**ITSL Solutions AB**Universitetsallen 32, 852 30 Sundsvall  
+46 (0)70 – 330 11 89 • [info@itsl.se](mailto:info@itsl.se)

Organisationsnr. 559261-9265 • Innehar F-skatt

# Integrationer och användningsflöden

## Kalenderintegration (Hubs kalender och Outlook)

Tjänsten är **tätt integrerad med kalenderfunktioner**, både med den inbyggda kalendern i samarbetsplattformen (HUB) och med externa kalendrar som Microsoft Outlook. Internt kan användare direkt i organisationens kalender schemalägga ett videomöte genom att lägga till en **möteshändelse**. Vid skapandet av en kalenderpost finns valet ”*Skapa säkert videomöte*” – ett klick där genererar automatiskt ett mötesrum i videochatttjänsten och infogar möteslänken i kalenderinbjudan. Deltagarnas tillgänglighet kan korskontrolleras i kalendern för att hitta en tid som passar alla, och inbjudna användare får mötet inlagt i sina kalendrar tillsammans med länken för att ansluta.

## Under utveckling med leverans i början av Q1-2026

För användare som föredrar **Outlook** erbjuder vi ett plugin som ITSL utvecklar som ger liknande funktionalitet i Microsofts miljö. Direkt från Outlooks gränssnitt kan man boka ett *Säker video och chatt*-möte genom att välja alternativet att skapa ett onlinemöte. Pluginet ser till att en möteslänk genereras och bifogas i Outlook-kalenderbokningen, komplett med information för att ansluta. Detta möjliggör för t.ex. kommunanställda att fortsätta använda Outlook som vanligt, men ändå utnyttja den säkra videomötestjänsten i bakgrunden. Mötets detaljer (länk, PIN-kod om applicerbart, etc.) skickas ut till deltagarna precis som vid vanliga Teams-möten, men under huven är det den säkra, egenhostade plattformen som hanterar mötet.

Viktigt att veta är att i outlook sparas endast detaljer om personen som bokade inga detaljer om deltagare eller uppgifter om mötet sparas i bokningen i outlook. För att de den informationen måste man följa länken för att komma till chatrummet för mötet där all information finns alternativt gå till kalendern i Hubs.

Kalenderintegrationen inkluderar även **påminnelser** – inbjudna kan få e-postnotiser innan mötet börjar, och plattformen kan skicka ut notifieringar via både e-post och push (för mobilanvändare) så att ingen missar att ansluta i tid.

### ITSL Solutions AB

Universitetsallen 32, 852 30 Sundsvall  
+46 (0)70 – 330 11 89 • [info@itsl.se](mailto:info@itsl.se)

Organisationsnr. 559261-9265 • Innehar F-skatt

Det täta sambandet mellan kalender och videomöten innebär också att uppföljning underlättas. Möteschatten och inspelningar kan kopplas tillbaka till kalenderposten eller ett projekt. Om ett möte är del av ett större projekt kan man via kalendern och projekthanteringen i Hubs sammankoppla mötesrummet med tillhörande filer, uppgifter och anteckningar för helhetsöverblick.

### **Teams-bridge (Under utveckling med leverans i början av Q1-26)**

För de organisationer som även använder Microsoft Teams i vissa sammanhang erbjuder vi en **integration mellan Teams och Hubs** som förenar vår säkra plattform med Teams-gränssnittet. Denna integration möjliggör att **filer och dokument som lagras i vår plattform kan nås direkt från Teams** utan att data lämnar den säkra miljön. Rent praktiskt ersätter integrationen behovet av OneDrive/SharePoint i Teams: när en användare i Teams delar en fil eller öppnar lagring, sker det mot er privata molnlagring (HUB) istället för Microsofts moln. Resultatet är en sömlös användarupplevelse – medarbetarna kan arbeta i Teams som vanligt, men all lagring och delning sker under kommunens kontroll på den svenska, GDPR-säkra plattformen.

En konkret användning av Teams-bridgen är att användare kan **se och dela filer i Teams** direkt från kommunens säkra lagring. När man klickar på ”Bifoga fil” i Teams visas filer från HUB, och alla delade dokument hålls kvar i kommunens moln istället för att laddas upp i Teams/Microsoft 365. Det ger användarna fördelen av Teams välbekanta gränssnitt kombinerat med full kontroll om vart filerna finns. Integrationerna med Outlook och Teams i sin helhet gör att plattformen kan fungera **side-by-side med befintliga verktyg**, vilket förenklar införandet – man behöver inte välja bort sina verktyg, utan kan gradvis styra känsliga möten och filer till den säkra miljön.

## Säkerhet, regelefterlevnad och driftmiljö

En **hög säkerhetsnivå** genomsyrar tjänsten "Säker video och chatt". All kommunikation (video, audio, chatt, filer) skyddas av flerskiktsskryptering. Videoströmmar och ljud överförs krypterat punkt-till-punkt mellan deltagarna, och där serverkomponenter används (för t.ex. storskaliga möten) är trafiken krypterad både i transportled (TLS) och vid behov ända ut till

klienterna (E2EE). Chatmeddelanden lagras krypterat på servern och skickas över säker anslutning.

Utöver detta finns inbyggt skydd mot intrångsförsök som brute force-attacker, AI-baserad upptäckt av misstänkt inloggningsbeteende samt stöd för moderna autentiseringsmetoder (t.ex. tvåfaktorsautentisering och SSO). Sammantaget gör dessa åtgärder att plattformen uppfyller strikta krav för **informationssäkerhet och sekretess**.

Tjänsten utmärker sig genom att erbjuda **digital suveränitet**: all data stannar på servrar som kontrolleras av kommunen (eller vald driftpartner inom nationen).

Till skillnad från kommersiella alternativ som Microsoft Teams eller Zoom, där data routas via externa moln, kan ni här lita på att **inga tredje parter har tillgång** till vare sig innehåll eller metadata. Detta underlättar regel efterlevnad enligt nationella och internationella föreskrifter (t.ex. Schrems II, Cloud Act-problematik, NIS-direktiv etc.).

## Confidential compute

Slutligen kan lösningen drifas i en **Confidential Compute-miljö** för maximal säkerhet. Detta innebär att om ni väljer att köra tjänsten i en molnplattform med stöd för konfidentiell databehandling (t.ex. virtuella servrar med hårdvarustöd för minneskryptering och isolering, som Intel SGX/TDX eller AMD SEV), så hålls data krypterad även under bearbetning. Inte ens driftleverantörens administratörer kan då läsa av klartextdata i minne eller processor. Vår plattform är kompatibel med sådan teknik och kan distribueras i container- eller VM-form på confidential cloud-infrastruktur.

För känsliga verksamheter som hanterar sekretessbelagd information innebär detta att man kan kombinera **molntjänstens skalbarhet** med **on-premise-säkerhet**, då data under hela livscykeln (at rest, in transit, in use) är skyddad.