



Utredning - Drift av de svenska förbindelsepunkterna (noderna) med tillhörande infrastruktur

Slutrapport

Datum: 2024-12-10

Diarienummer: 2024-7628

Sammanfattning

Utredningen har analyserat förutsättningarna för att flytta driften av eIDAS-noden och tjänsten Sweden Connect till en ny leverantör, då det befintliga avtalet löper ut 2025-12-31. Analysen har identifierat de aktiviteter och utmaningar en sådan transition (teknisk förflyttning) skulle innebära, samt de krav som ställs på Digg och en ny driftleverantör.

Verksamheten är enligt säkerhetsskyddsanalysen samhällsviktig och måste följa lagkrav, som till exempel kontinuitetshantering. Ytterligare krav från säkerhetsskyddsanalysen ska hanteras i en säkerhetsskyddsplan.

Myndighetens avsaknad av sourcingstrategi gör att det inte finns några egentliga incitament till att byta ut nuvarande lösning med Sunet.

Summering

Sunet uppfyller idag de krav Digg har på drift av eIDAS-noden och Sweden Connect-tjänsten. Att flytta tjänsten till ny leverantör är genomförbart, men förutsätter att ett transitionsprojekt (eller liknande) etableras. Utredningen har dock inte bedömt de totala kostnaderna för det. Däremot finns en uppskattning av årliga kostnader för en ny leverantör baserat på, i detta fall, Försäkringskassans egen beräkningsmodell.

Rekommendation

Utveckla och implementera en sourcingstrategi

Beslut om att byta driftleverantör och genomföra en teknisk transition bör vara en del av myndighetens sourcingstrategi. Myndigheten bör inleda en översyn av den nuvarande situationen, där olika driftleverantörer hanteras parallellt genom Avdelningen för tillit och säkerhet och Avdelningen för IT.

En övergripande sourcingstrategi bör utarbetas, med utgångspunkt i "Säker och kostnadseffektiv it-drift" (bilaga 5). Strategin bör inkludera tydliga kriterier för val av driftleverantör och ska fungera som stöd vid kommande beslut.

Beslut om leverantörsbyte rekommenderas först efter att en sådan strategi har tagits fram. Om strategin visar att ett byte är lämpligt bör en fördjupad utredning genomföras. Utredningen bör inkludera en fullständig kostnads- och riskanalys med fokus på ett transitionsprojekt.

Kortsiktig rekommendation

Behåll nuvarande leverantör

Eftersom Digg som myndighet för närvarande saknar denna övergripande sourcingstrategi för tjänster som till exempel Sweden Connect rekommenderas att den nuvarande leverantören, Sunet, behålls tills vidare. Detta säkerställer kontinuitet och minskar risken för avbrott i tjänsten.

Innehållsförteckning

Utredning - Drift av de svenska förbindelsepunkterna (noderna) med tillhörande infrastruktur	1
Sammanfattning	2
Innehållsförteckning	3
1 Bakgrund	4
1.1 Utredning: drift av de svenska förbindelsepunkterna (noderna) och tillhörande Infrastruktur	4
1.2 Metod.....	4
1.3 Avgränsningar.....	4
1.4 Förutsättningar	5
1.5 Krav på en driftsleverantör och Digg för Sweden Connect och eIDAS-noden.....	5
1.6 Drift och produktion	6
2 Beskrivning Sweden Connect.....	7
2.1 Tjänstens omfattning	8
2.2 Utveckling	8
2.3 Drift – applikation och infrastruktur	8
3 Områden att utvärdera	10
3.1 Område 1 – Infrastrukturarkitektur och tjänstens omfattning	10
3.2 Område 2 – Säkerhetsskyddsanalys och tillgänglighetskrav	14
3.3 Område 3 – Diggs sourcingstrategi.....	15
3.4 Område 4 – Kostnadsanalys (HW&SW)	16
3.4.1 Sunet.....	16
3.4.2 Försäkringskassan	16
3.5 Område 5 – Transitionsprojekt	17
3.6 Område 7 – Riskbedömning	19
3.6.1 Riskanalys – Sammanfattning och slutsatser	19
4 Sunet	20
4.1 Sunet	20
5 Bilagor.....	22

1 Bakgrund

1.1 Utredning: drift av de svenska förbindelsepunkterna (noderna) och tillhörande Infrastruktur

I regleringsbrevet 2024 fick Digg följande uppdrag:

Myndigheten ska ingå en överenskommelse med Vetenskapsrådet om it-driften av de svenska förbindelsepunkterna (noderna) för gränsöverskridande elektronisk identifiering och tillhörande infrastruktur för tiden fram t.o.m. den 31 december 2025. Överenskommelsen ska bl.a. innehålla villkoren för den ersättning som myndigheten ska betala till Vetenskapsrådet. Myndigheten ska även utreda förutsättningarna för den fortsatta it-driften för tiden efter överenskommelsens upphörande. Uppdraget ska senast den 31 mars 2025 redovisas till Regeringskansliet (Finansdepartementet).

Enligt regeringsuppdraget så framgår det att Digg är ansvariga för utredningen och Vetenskapsrådet (Sunet) ska bistå Digg i utredningen, som sedan ska redovisas senast 31 mars 2025. Det vi anser bör utredas är vilken kravställning som ska vara på drift, förvaltning och vidareutveckling på en driftsleverantör och Digg för Sweden Connect och eIDAS-noden.

1.2 Metod

För att genomföra driftutredningen och skapa ett beslutsunderlag har arbetsgruppen genomfört en nulägesanalys av den befintliga tjänsteleveransen utifrån specifika områden. Syftet med analysen är att utvärdera om den nuvarande leverantören, Sunet, uppfyller de aktuella kraven samt bedöma Sunets kapacitet att möta framtida behov.

En viktig del av utredningen är att analysera den befintliga infrastrukturarkitekturen, som fungerar som en "Blueprint". Denna ritning är avgörande för att säkerställa att den nuvarande lösningen uppfyller Diggs krav samt ge en tydlig utgångspunkt vid dialog med andra leverantörer.

Resultatet från nulägesanalysen och kravspecificeringen kommer att användas för att jämföra relevanta aspekter av nuvarande och alternativa lösningar, bedöma möjligheten till en eventuell transition.

1.3 Avgränsningar

- Utredningen kommer inte att se över vilka kostnader ett transitionsprojekt skulle innebära.
- Utredningen kommer inte att utvärdera ISO 27000 relaterade delar.
- Utredningen kommer inte att utvärdera utveckling eller förvaltning som hanteras av iDsec Solutions AB, och därmed inte heller de kostnader som detta medför.

1.4 Förutsättningar

Det finns ett uttalat önskemål på Digg att minska antalet driftleverantörer samt att nya initiativ i högre grad ska drivas på Försäkringskassan IT.

I denna utvärdering jämförs nuvarande driftleverantör, Sunet, med en potentiell lösning tillsammans med Försäkringskassan IT.

Syfte och mål

Resultatet av utredningen ska klargöra vilka krav som ska ställas på eIDAS-noden och Sweden Connect och fungera som underlag för beslut om:

- En övergång till en ny leverantör.

alternativt

- Fortsatt samarbete med nuvarande leverantör.

1.5 Krav på en driftsleverantör och Digg för Sweden Connect och eIDAS-noden

eIDAS-noden eller noderna (Proxy och Connector) är en tjänst inom Digg med en egen produktägare, tjänsten tillhandahåller möjlighet att nyttja sin e-legitimation för att logga in till svenska e-tjänster eller till utländska e-tjänster inom EU.

eIDAS-förordningarna utgör den huvudsakliga drivkraften bakom merparten av arbetet på Digg. Sunet utvecklar mjukvara avseende infrastrukturen kring Sweden Connect och ansvarar för de centrala infrastrukturkomponenterna.

Hantering av tjänsten Sweden Connect och eIDAS-noden involverar tre aktörer med tydliga ansvarsområden:

1. Digg:

- Ansvarar för tjänsten och dess avtal med aktörer/användare.
- Har det övergripande ansvaret för att initiera och driva utveckling av nya funktioner och förbättringar.
- Tillhandahåller både en Produktägare för tjänsten som prioriterar backlogen och en Scrum Master, som hanterar arbetet i utvecklingsteamet.

2. iDsec Solutions AB:

- iDsec Solutions AB upphandlas som konsulter av Digg
- Leverantören som utvecklar tjänsten baserat på Diggs beställningar.
- Har expertkompetens inom IT-säkerhetsområdet och tillför teknisk specialistkunskap.

3. Sunet:

- Ansvarar för plattformen och applikationsdriften.

- Ansvarar för leveransledning och leveransstyrning samt viss utveckling kopplat till applikationens drift
- Säkerställer att systemet fungerar som förväntat genom övervakning och hantering av eventuella problem inom ramen för åtgärdsbeskrivningar och definierade processer.

1.6 Drift och produktion

Kraven på kommande driftleverantör specificeras i (bilaga 4)

Nuvarande drift: Sunet och applikationsdrift, ledning mm

I nuvarande avtal köper Digg tjänsten "applikationsdrift" från Sunet. Dagens avtal är således mer än enbart leverans av hårdvara och tillhörande tjänster. Sunet ansvarar för:

- Ledning och styrning (projekt, strategisk ledning, mm)
- Förvaltning (applikationsdrift)
- NOC (Network operation center)
- Åtgärdsplanering och hantering av metadata.
- Deployment i samtliga miljöer.

Den årliga kostnaden för denna tjänst är cirka 4,1 MSEK enligt budget.

Hårdvara och tillhörande tjänster ingår inte i det som definieras "applikationsdrift". Det är en annan budgetpost (specificeras nedan).

Utmaning vid övergång till ny leverantör

Om Försäkringskassan IT blir ny driftleverantör, åtar de sig inte ansvaret för applikationsdriften i samma omfattning som Sunet gör idag. Därför behöver denna kompetens byggas upp internt hos Digg, exempelvis genom IT-avdelningens Plattformsteam, eller genom en annan funktion.

Digg och utveckling av applikationen

För närvarande anlitar Digg iDsec Solutions AB som leverantör av utvecklingstjänster för applikationen.

- Det finns inga identifierade skäl att ändra detta upplägg i samband med att en ny driftleverantör väljs.
- Andra faktorer som skulle motivera en förändring ligger utanför ramen för denna utredning och hanteras inte här.

2 Beskrivning Sweden Connect

E-legitimationsnämnden (2011–2018) fick i uppdrag att utveckla och tillhandahålla den svenska eIDAS-noden. För att uppfylla detta tecknade myndigheten ett samarbetsavtal med Sunet (Vetenskapsrådet) för utveckling och drift. Avtalet fungerade mer som ett partnerskap för utveckling än som en traditionell beställning av driftstjänster. Även om beslutsrätt och finansiering låg hos e-legitimationsnämnden, uppmanades Sunet att föreslå förbättringar. Detta eftersom det i första hand var Sunets kunskap inom system för identitetshantering och federationer som var attraktiv för e-legitimationsnämnden.

Sunet hade också ett eget intresse av att gränsöverskridande e-legitimering fungerade väl, eftersom utländska studenter, lärare och forskare är en av de viktigaste målgrupperna för gränsöverskridande e-legitimering. Som en del av uppdraget utvecklades federationen Sweden Connect för att underlätta anslutningen av svenska aktörer. Sweden Connect, tillsammans med eIDAS-noderna (två separata noder som hanteras inom samma uppdrag), togs i drift strax innan Digg bildades och e-legitimationsnämnden avvecklades (2018). Vid detta skede övertog Digg hela uppdraget, inklusive samarbetet med Sunet.

Sunets roll och kompetens inom federationer

Sunet har erfarenhet att som driftleverantör driva federationer. De hanterar redan andra federationer, såsom Swamid, vilket innebär att de besitter teknisk kompetens inom drift och metadatahantering vilket är en viktig faktor för framgångsrik hantering av federationer.

Erfarenhet från Swamid och koppling till Sweden Connect

Sunet ansvarar för driften av Swamid-federationen, som på många sätt liknar Sweden Connect-tjänsten. Även om det finns vissa skillnader, exempelvis i hur registreringen av förlitande parter sker, är den tekniska hanteringen av metadata i stort sett densamma. Detta arbete kräver en erfaren och tekniskt kunnig driftspartner, och idag bär Sunet ett stort ansvar för tjänstens förvaltning och drift.

Utveckling av Sweden Connect: OpenID Federation och framtida behov

Sweden Connect står inför nästa steg i utvecklingen med införandet av ny teknik som är baserad på OpenID Federation, vilket ger stöd för avancerad hantering av behörighetstjänster.

Sunet har erfarenhet av att driva liknande initiativ inom utbildningssektorn och samarbetar med Digg i utvecklingen av prototyper och drift av dessa tjänster.

Idag saknar Digg den interna kompetensen för att hantera detta på egen hand och är därför beroende av en leverantör med djup teknisk insikt och erfarenhet.

Samarbete mellan Digg och Sunet

Digg och Sunet har ett välfungerande samarbete som präglas av flexibilitet och delat ansvar. Sunet tar fullt ansvar för att Sweden Connect-tjänsten fungerar som förväntat, inklusive aktiv

felsökning, uppdateringar och andra förvaltningsinsatser. Denna samarbetsmodell har varit bra för att säkerställa tjänstens stabilitet och kontinuerliga utveckling.

2.1 Tjänstens omfattning

Sweden Connect är ett samlingsnamn för olika komponenter. De huvudsakliga delarna av Sweden Connect hanterar såväl nationell e-legitimering som e-legitimering mellan EU:s medlemsstater. Den del som ansvarar för samarbetet inom EU kallas för eIDAS-noden eller eIDAS-noderna.

2.2 Utveckling

Utvecklingsteamet på Digg arbetar enligt SCRUM, och alla ändringar spåras och hanteras i verktyget JIRA hos Digg. Samma utvecklingsteam ansvarar för eIDAS-noderna, vilket skapar en enhetlig arbetsprocess och effektiv resursanvändning. eIDAS-förordningarna är den huvudsakliga drivkraften bakom merparten av utvecklingen som sker inom eIDAS-noderna.

Sunet utvecklar mjukvara för Sweden Connect och ansvarar för dom komponenterna. Kommunikation mellan teamen sker kontinuerligt och beställningar till Sunet kan göras via Sunets Jira.

2.3 Drift – applikation och infrastruktur

Sweden Connect består av följande komponenter:

Sweden Connect Metadata

- Ett metadataregister som hanterar information om förlitande parter och e-legitimationsutfärdare.

eIDAS Connector

- Förbinder Sverige med utländska e-legitimationer, vilket möjliggör användning av dessa inom svenska system.

eIDAS Proxy

- Kopplar utländska e-legitimationer till svenska e-tjänster.

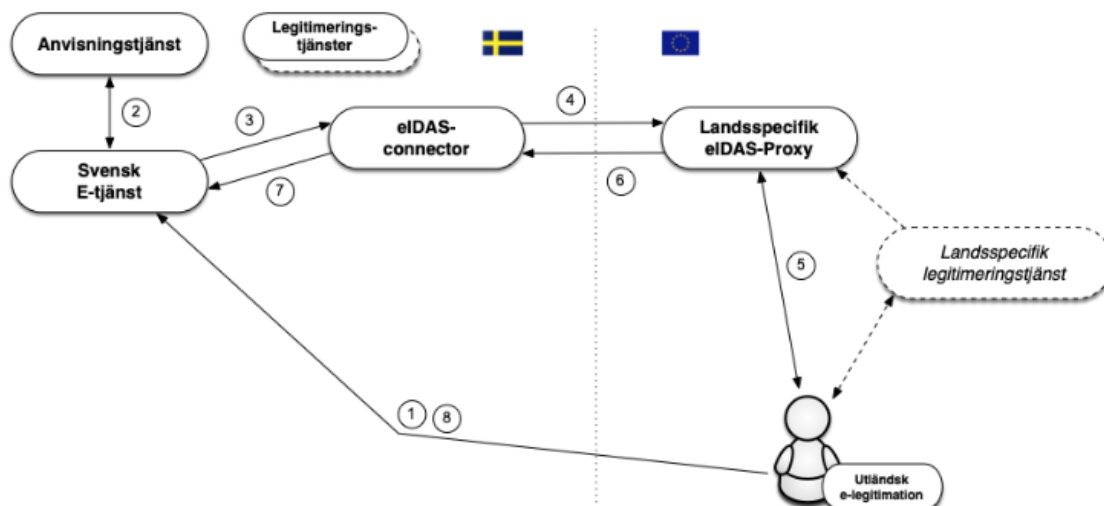
eIDAS PRID

- Stödjer eIDAS Connector genom att skapa och hantera identifieringsprocesser för alla länder som Sverige är anslutet till via eIDAS.

eIDAS DE Middleware

- Alla eIDAS-noder som kommunicerar med Tyskland måste ha denna komponent. Den är byggd av Tyskland för att kommunicera specifikt med Tyskland då deras nod inte är centraliserad.

Övergripande flödesbeskrivning (från Sunets wiki)



Förvaltning

Förvaltningen av eIDAS-noderna och Sweden Connect hanteras gemensamt av utvecklingsteamet och Sunet, med tydliga ansvarsområden som ibland överlappar.

Utvecklingsteamets ansvar

- Utför uppgraderingar av tekniska ramverk i eIDAS-noderna.
- Hanterar förbättringar och teknisk utveckling relaterad till plattformarnas grundfunktioner.

Sunets ansvar

Hanterar löpande förvaltning, inklusive:

- Tillägg av metadata från nya länder som ansluter sig till eIDAS.
- Administration av metadata för nya förlitande parter inom Sweden Connect.
- Uppdateringar av metadata vid behov.

Gemensamma (Digg-Sunet) underhållsåtgärder:

- Omstart av tjänster vid uppdateringar av certifikat.

- Uppdatering av operativsystem och mjukvara för att säkerställa att systemen är aktuella och säkra.

3 Områden att utvärdera

Följande områden har valts för utvärdering

- Infrastrukturarkitektur och tjänstens omfattning
- Säkerhetsskyddsanalys och tillgänglighetskrav
- Diggs sourcingstrategi
- Kostnadsanalys (HW&SW)
- Transitionsprojekt

3.1 Område 1 – Infrastrukturarkitektur och tjänstens omfattning

Enligt utredningens bedömning driftas Sweden Connect-tjänsten på en robust och säker infrastruktur. Nedan följer en översikt av den nuvarande arkitekturen och dess egenskaper:

Redundans och geografisk spridning

- Driftas på två geografiskt separerade sajter med redundans för hög tillgänglighet.

Säkerhetszoner och segmentering

- Systemet är uppdelat i säkerhetszoner (frontend, yttre säkerhetszon och separerade komponenter).
- Servrar i olika zoner är implementerade som virtuella maskiner som körs på dedikerad hårdvara.

Paketering och lastbalansering

- Alla komponenter är paketerade i Docker-containerar.
- Aktiv lastbalansering är implementerad i det publika gränssnittet för att optimera prestanda.

Säkerhet och logghantering

- Varje server är utrustad med en lokal brandvägg.
- Samtliga servrar loggar systemhändelser till en separat loggmiljö.

Övervakning

- Miljön övervakas baserat på konfigurerbara övervakningsregler.

Bedömning av den nuvarande infrastrukturen

Den nuvarande infrastrukturen bedöms väl genomtänkt och säker. Valet att använda fysisk hårdvara är ett resultat av tidigare beslut och inte kopplat till något specifikt krav (som kan identifieras i utredningen). Utredningen har inte bedömt eller utvärderat val av tekniska lösningar eller produktval för drift, leverans och deployment (installation) av applikationen.

Tjänstens omfattning och framtida behov

Utredningen har analyserat tjänstens last och prestanda under perioden 2023-10-01 till 2024-09-30 (12 månader).

Syftet med analysen är att identifiera trender och mönster i belastning och resursanvändning. Även en uppskattning har gjorts för den kommande 12-månadersperioden för att förutse framtida behov.

Tabell 1: Last på systemet

Nuvarande last	Antal anrop	Lyckade inloggningar	Del av anrop som lett till inloggning
Totalt antal anrop	1 268 562	106 692	8%
Anrop Proxy	325 490	20 585	6%
Anrop Connector	943 072	86 107	9%
Snitt per dag i perioden	3 476	292	8%

Tabell 2: Prognos kommande 12 månader är + 25%

Prognos - last	Antal anrop	Del av anrop som förväntas leda till inloggning
Totalt antal anrop	1 585 703	133 365
Anrop Proxy	406 863	25 731
Anrop Connector	1 178 840	107 634
Snitt per dag i perioden	4 344	365

Kommentar: Antal anrop och förväntad trafikökning

Informationen kommer från Sunets statistikdatabas och visar antalet anrop som mottagits av connectorn/proxytjänsten.

Exempel på anrop:

- Ett anrop genereras exempelvis när en användare besöker en sida som Skatteverket, klickar på "Logga in" och väljer "Foreign eID" som inloggningsalternativ (se nedan). Detta resulterar i ett anrop, men det behöver inte nödvändigtvis leda till en faktisk inloggning.

Skatteverkets inloggning

Logga in på Skatteverket

För att logga in behöver du identifiera dig med e-legitimation

Välj inloggning
Internationellt

FREJA
Freja
Registrerad med e-post
Välj detta om du enbart registrerat Freja med en e-postadress.

FREJA
Freja
Verifierad med ID-handling
Välj detta om du utöver e-post också verifierat Freja med en ID-handling.


Foreign eID
eID utgivet av annat land
Välj detta om du har ett eID som är utgivet i ett annat EU/EES-land än Sverige.

Förväntad trafikökning

- Den uppskattade trafiken för de kommande 12 månaderna förväntas öka med cirka 20–25 %, förutsatt att ingen ny funktionalitet tillkommer.

Matrisen beskriver en planerad ökning på 25 %, vilket motsvarar:

- Antal anrop: En årlig ökning från 1 268 562 till 1 585 703 anrop.
- Lyckade inloggningar: En ökning från 101 405 till 126 856 lyckade inloggningar per år (8% av totalt antal anrop).

Jämförelse med BankID

För kontext kan BankID nämnas i en (kanske orättvis) jämförelse, där tjänsten hanterade 7,1 miljarder användningar under 2023, vilket motsvarar över 19 miljoner anrop per dag.

Sweden Connect har en daglig genomsnittlig trafik på 3 476 anrop, vilket indikerar en betydligt lägre belastning.

Slutsats

Med den förväntade trafikökningen på 25 % bedöms systemet fortsatt ha en låg belastning och ha goda förutsättningar att hantera den ökade trafiken.

Tabell 3: Prestanda och svarstider

Komponent	Min (ms.)	Max (ms.)
Proxy	500	700
Connector	500	700
Metadata	800	1100

Kommentar

De angivna svarstiderna gäller endast de delar av tjänsten som hanteras av den interna applikationen, inklusive:

- Mottagning av anrop.
- Validering av metadata.
- Leverans av svar.

Begränsning i data:

Ingen statistik finns tillgänglig för att mäta svarstider för hela flödet, vilket kan inkludera andra moment i användarens upplevelse.

Sammanhang och användarupplevelse:

Svarstiderna kan vara acceptabla i kontexten då inloggningsprocessen ofta innefattar flera steg som användaren aktivt utför, exempelvis användning av QR-läsare. Dock har ingen analys gjorts av hur märkbara dessa svarstider är för användarna.

Framtida prestandautmaningar:

Om användningen av tjänsten ökar, finns det en risk att svarstiderna blir ett prestandaproblem på sikt. Detta är dock endast ett antagande och kräver vidare analys för att bekräftas.

Tabell 4: Tillgänglighet

Miljö	Tillgänglighet (uptime)
QA	>99,99%
Prod	>99,99%

Kommentar: Tillgängligheten i systemet är hög.

Tabell 5: Driftsättningar

Miljö	Planerade driftsättningar	Akuta driftsättningar
QA	2	0
Prod	5	0

Kommentar

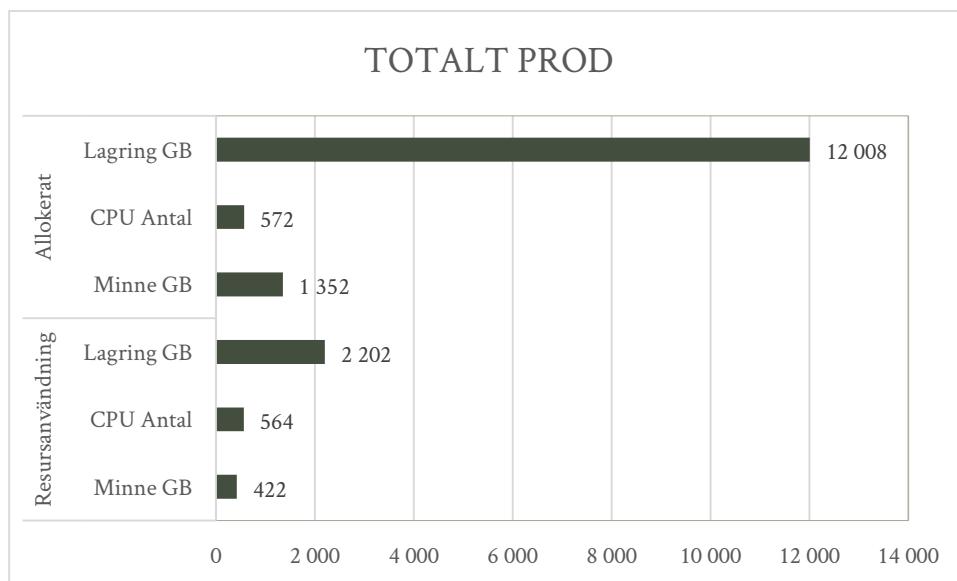
Systemet uppdateras sällan enligt statistiken. Det kan antas att vissa typer av uppdateringar, såsom ordinarie patchning och livscykelhantering, inte återspeglas i underlaget. Detta är dock inte vidare utrett.

Infrastrukturen är designad för att möjliggöra service och uppdateringar under pågående drift, vilket innebär att deploy och övrig service kan genomföras utan avbrott i tjänsten.

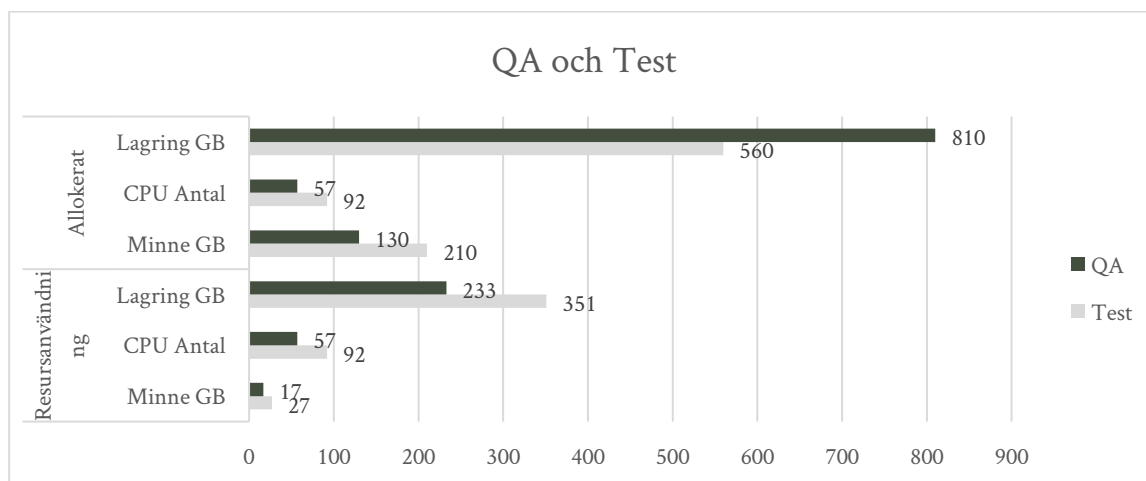
Säkerhet och kontinuitet

Inga driftsättningar kopplade till säkerhetsincidenter har rapporterats

Figur 2: Sizing av miljöer vs. Resursanvändning



Figur 3: QA och Test



Kommentar

Det finns ingen risk för resursbrist i systemet med hänsyn taget till hur systemet är konfigurerat relaterat till hur det används. Resursanvändningen ligger under allokerade resurser.

Lagring och minne: Det finns överkapacitet i både lagring och minne.

CPU: Resursallokeringen för CPU är rimlig och i linje med faktisk användning.

Samma mönster finns i såväl produktionsmiljön, QA-miljön och testmiljön.

3.2 Område 2 – Säkerhetsskyddsanalys och tillgänglighetskrav

En säkerhetsskyddsanalys har genomförts. Syftet med säkerhetsskyddsanalysen är att identifiera och värdera skyddsvärda tillgångar i tjänsten/produkten/IT-systemet för att kunna analysera och

bedöma konsekvenser för verksamheten utifrån potentiella hot, sårbarheter och risker.

Analysen visar att verksamheten är av samhällsviktig karaktär. Nya uppdrag inom Sweden Connect, som kan bli aktuella framöver, skulle kunna öka den samhällsviktiga betydelsen ytterligare.

Skyddsvärda tillgångar har identifierats, deras allvarlighetsgrad har bedömts och finns beskrivna i säkerhetsskyddsanalysen (bilaga 2).

Driftutredningen ansvarar inte för att genomföra eventuella granskningar eller genomförande av aktiviteter kopplat till detta. Sammantaget ska detta påvisa om tjänsterna kan anses vara samhällsviktiga.

Resultatet av säkerhetsskyddsanalysens beskrivs i (bilaga 2).

3.3 Område 3 – Diggs sourcingstrategi

En tydlig sourcingstrategi säkerställer att IT-systemen fungerar på ett sätt som stödjer myndighetens mål, minimerar operativa och säkerhetsmässiga risker samt skapar förutsättningar för en optimal användning av resurser, både vad gäller personal och teknik. Realiteten idag är att myndigheten har dubbel leverantörsstyrning (Sunet och Försäkringskassan IT), olika tekniker för drift och underhåll samt två grupperingar som arbetar med snarlika uppgifter.

En sourcingstrategi handlar om att utveckla en långsiktig plan för hur myndigheten ska skaffa, hantera och underhålla de resurser och tjänster som behövs för att IT-miljön ska fungera effektivt, stabilt och kostnadseffektivt.

Strategin bör vara en del av hela myndighetens övergripande IT-strategi och påverkar hur IT-stödet levereras, oavsett om det sker internt eller externt.

Digg har ett uttalat önskemål om att nya initiativ i högre grad ska driftas på Försäkringskassan IT inom ramen för [Samordnad och säkert statlig it-drift](#). (Bilaga 5). Digg är sedan juni 2021 ansluten som "Liten myndighet" till Försäkringskassan IT:s samordnade statliga it-drift.

För närvarande ansvarar två avdelningar inom Digg för utveckling och drift av IT-system:

- **Avdelningen för tillit och säkerhet**, som bland annat hanterar eIDAS och Sweden Connect.
- **Avdelningen för IT**, som ansvarar för andra delar av organisationens IT-infrastruktur, samt bland annat applikationen Min Myndighetspost (MiMy).

Avsaknad av en uttalad sourcingstrategi

Digg har i dagsläget ingen formellt definierad sourcingstrategi (Bilaga 3). Detta innebär att valet av driftleverantör för eIDAS och Sweden Connect huvudsakligen har baserats på historiska beslut, där Sunet nu är den ansvarige leverantören.

I avsaknad av en övergripande sourcingstrategi finns det ingen möjlighet att i denna utredning värdera valet av driftleverantör utifrån strategiska riktlinjer eller långsiktiga mål.

3.4 Område 4 – Kostnadsanalys (HW&SW)

Syftet med analysen är att ge en tydlig bild av kostnaderna för hela miljölandskapet, inklusive alla nödvändiga resurser.

3.4.1 Sunet

Kostnadsstruktur

Enligt underlaget "Budget Digg-SUNET_2024_2025" (Bilaga 1) är kostnaderna uppdelade i tre huvudposter:

1. Personal
2. Tjänster
3. Övriga kostnader

Personal

Kostnadsposten för personal omfattar:

- Ledning och styrning: Ansvarar för strategisk och operativ styrning av tjänsten.
- Utveckling och förvaltning av applikationen: Hantering av systemutveckling och löpande underhåll.
- NOC (Network Operation Center): Ansvarar för övervakning, driftsättningar och andra operativa driftåtgärder.

Tjänster

Tjänsteposten inkluderar:

- Hårdvara: Inklusive de virtuella maskiner som är konfigurerade för tjänsten.
- Fysiska HSM (Hardware Secure Modules): Säkerhetskritiska moduler som uppfyller krav på dataintegritet och säkerhet.

Övriga kostnader

2024 och 2025 påvisar inga kostnader klassificerade som "Övriga kostnader".

Budget

Post	Budget 2024	Budget 2025
Personal	4 141 040	4 141 040
Tjänster	2 604 000	2 604 000
Övriga kostnader	0	0
TOTALT	6 745 040	6 745 040

3.4.2 Försäkringskassan

Kostnadsstruktur

Försäkringskassan IT beräknar kostnader för HW genom hur mycket minne man allokerar (i Gigabyte) samt hur mycket lagring man allokerar (i Gigabyte/Terabyte). Beräkningen nedan är baserad på Försäkringskassans aktuella prislista i kombination med de uppgifter kring aktuell allokering som Sunet bidragit med. Försäkringskassan har utöver detta ett fast timpris för vissa tilläggstjänster, timpriserna är desamma oavsett vilken roll som efterfrågas (se nedan).

Uppskattade kostnader för motsvarande miljöer hos Försäkringskassan

Sizing beskrivet i minne	GB	Kostnad enl. FK	Kostnad / år
Prod 1	676	1470	993 720
Prod 2	676	1470	993 720
QA	130	1470	191 100
Test	210	1470	308 700

Sizing beskrivet i lagring (fillagring)	GB	Kostnad enl. FK	Kostnad / år
Prod 1	6004	28	168 112
Prod 1	6004	28	168 112
QA	810	28	22 680
Test	560	28	15 680

Sammanställning	Kostnad / år
Total kostnad Prod 1 och Prod 2	2 323 664
Total kostnad QA	213 780
Total kostnad Test	324 380
Total kostnad	2 861 824

Sammanfattning av infrastrukturkostnader Sunet och Försäkringskassan IT

Jämförelsetal	Kostnad / år
Infrastruktur, Sunet (tjänster i budget)	2 604 000
Infrastruktur, Försäkringskassan IT	2 861 824

3.5 Område 5 – Transitionsprojekt

Beskrivning av nuvarande miljö

Det befintliga miljölandskapet som ska flyttas omfattar:

- Miljöer: Sandbox, test-/QA-miljöer samt dubbla (redundanta) produktionssajter.

- Plattformar och resurser: Test och utveckling körs idag på Sunets IAAS (Infrastructure as a Service), där resurser delas med andra kunder.
- Gemensam infrastruktur: Hantering av certifikat (HSM), bygg, driftsättning och orkestrering (t.ex. Maven, Cosmos).
- Teknik: Test- och driftmiljöerna hanteras via Docker, där applikationer körs i containrar.

Alternativ vid transition

Försäkringskassans miljö erbjuder motsvarande funktionalitet genom OpenShift, en plattform som inkluderar Kubernetes och har inbyggda säkerhetsfunktioner samt stöd för orkestrering och skalning. Att Försäkringskassan erbjuder OpenShift innebär inte att valet behöver vara det, det bör vara ett beslut som fattas i samband med en eventuell övergång.

Aktiviteter vid transition

Ett antal aktiviteter behöver utföras för att genomföra en transition:

- Design av nytt landskap
- Beslut om plattform (OpenShift vs Docker).
- Om OpenShift inte väljs krävs utveckling av egna verktyg för orkestrering. Sunet använder egenutvecklade verktyg för orkestrering av miljön, dessa verktyg måste byggas och etableras på Digg.

Försäkringskassans kostnader vid transition

Försäkringskassan har ett timpris på 1300 SEK för alla tjänster som utförs på beställning. Transitionsprojektet skulle innefattas av detta.

Omnyckling i HSM

- Samtliga användare (länder) behöver nya certifikat, vilket kräver samordning.

Hantering av metadata

- Sunet använder egenutvecklade verktyg för metadatahantering, dessa verktyg måste byggas och etableras på Digg.

Etablering av infrastruktur

- Infrastruktur för stödsystem (exempelvis bygg och driftsättning) behöver implementeras.

Kompetensuppbyggnad

- Digg behöver skaffa teknisk kompetens inom federationer.

Anpassning av deploybeskrivningar

- Beskrivningar som idag är anpassade för Sunets miljö måste omarbetas för den nya plattformen.

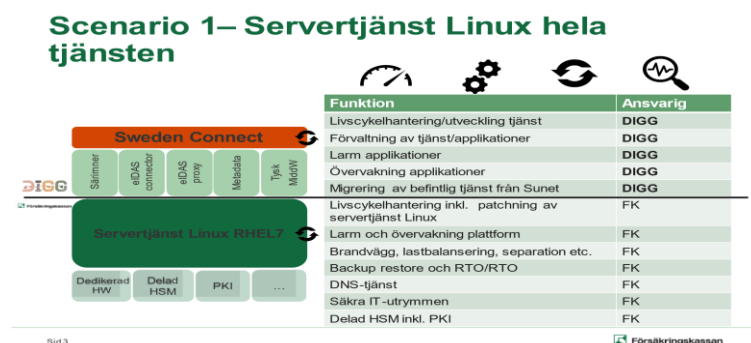
Roller och ansvar vid en transition

- Digg: Ansvarar för att etablera ett transitionsprojekt och leda arbetet.
- iDsec Solutions AB: Behöver vara djupt involverade i genomförandet.
- Sunet: Bidrar med tekniskt kunnande och kompetensöverföring.
- Försäkringskassan: Behöver initiera ett parallellt projekt för att säkerställa att den nya miljön är redo för drift (Bilaga 4).

Försäkringskassans ansvar avseende infrastrukturen och applikationen

Försäkringskassan levererar en grundinfrastruktur som Digg kan använda för att exekvera sina applikationer på. Ansvaret sträcker sig upp till applikationslagret. Det finns ingen möjlighet att köpa extra tjänster som avser något ovanför strecket i bilden nedan.

Ansvarsfördelning Försäkringskassan/Digg avseende infrastrukturen (bild från FK)



3.6 Område 7 – Riskbedömning

3.6.1 Riskanalys – Sammanfattning och slutsatser

Riskanalysen har genomförts med fokus på relevanta områden i rapporten för att adressera de aspekter som utredningen hanterat. Utgångspunkten har varit den kortsiktiga rekommendationen att behålla nuvarande leverantör.

Följande områden har analyserats:

- Infrastruktur och tjänstens omfattning
- Digg sourcingstrategi
- Kostnadsanalys
- Transitionsprojekt

Sammanfattning av riskanalysen

Infrastruktur:

- **Risk:** Den nuvarande lösningen bygger på dedicerade fysiska servrar. På sikt kan infrastrukturen behöva byggas ut parallellt med befintlig lösning, vilket kräver tid och resurser.

- **Bedömning:** Låg risk på kort sikt då infrastrukturen idag är väl dimensionerad.

Svarstider:

- **Risk:** Höga svarstider på vissa komponenter kan påverka användarupplevelsen vid ökad belastning. Ingen djupare analys har gjort avseende användarnas upplevelse av dagens svarstider.

- **Bedömning:** Möjligt problem på längre sikt, men den nuvarande låga lasten minimerar risken.

Sourcingstrategi:

- **Risk:** Avsaknad av sourcingstrategi inom myndigheten kan leda till slumpmässiga beslut kring val av vilken driftleverantör man väljer för befintliga tjänster som Sweden Connect, och även kommande tjänster. Detta kan på sikt leda till flera problem, såsom suboptimering av teknikresurser och en diversifiering av tekniker och verktyg, vilket i sin tur kan resultera i oenhetliga krav på kompetens.

- **Bedömning:** Strategisk hög risk som kan påverka framtida val av driftleverantör och organisationens effektivitet. Kräver hantering för att undvika problem på sikt.

Kostnadsanalys:

- **Risk:** Kostnaderna vid en "ett-till-ett"-flytt av infrastrukturen bedöms som likvärdiga de nuvarande kostnaderna.

- **Bedömning:** Ingen omedelbar ekonomisk fördel med leverantörsbyte.

4 Sunet

Texten i kapitel 4.1 är skriven av Sunet och utgör en delbeskrivning av deras verksamheten. Den redogör för de synergier som tjänsten Sweden Connect bidrar med till deras driftverksamhet

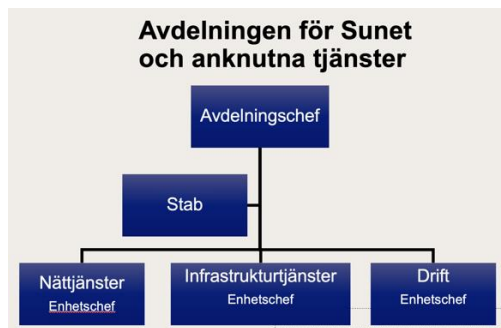
4.1 Sunet

SUNET - Swedish University NETWORK - är en gemensam resurs för digital infrastruktur för Sveriges högskolor, forskningsinfrastrukturer och kulturarvssektorn (statliga museer). SUNET bildades som ett samarbetsprojekt för att bygga gemensamma nätverk och kommunikationslösningar för landets lärosäten under 80-talet. SUNET lade grunden för Internet i Sverige under 80 och 90-talen och grundade i praktiken dagens Internet i Sverige. SUNET är idag en avdelning på Vetenskapsrådet med ca 65 anställda och heltidsengagerade konsulter.

SUNET är uppdelad på 3 enheter: Enheten för infrastruktur-tjänster, Enheten för nät och Enheten för drift. Arbetet med eIDAS-noden och Sweden Connect ligger i dagsläget i huvudsak på Enheten för drift i och med att verksamheten i huvudsak ligger i en förvaltningsfas. När det finns

utvecklingsaktiviteter så sker dessa i huvudsak inom Enheten för infrastrukturtjänster.

SUNET organisation



Enheten för Drift ansvarar för Sunets NOC (Network Operations Center), Sunet NOC opererar 24/7 365 dagar om året. All övervakning för Sweden Connect hanteras av Sunet NOC.

Enheten för Drift är uppdelad på tre delområden; Nät support, Infra Support och Media Support, varav Infra Support teamet ansvarar Sweden Connects förvaltning och drift.

SUNET har varit involverat i etableringen av Sweden Connect och eIDAS från början. Sunets roll i projektet var länge att fungera som tekniskt ledande och agerade i praktiken ledare för arbetet att ansluta eIDAS-noden till andra medlemsländer.

Högskolesektorn är en av de sektorer som har störst konkret användning av en koppling mot digital identitet utanför landets gränser. Det är jämförelsevis få tjänster som använder eIDAS-noden i praktiken men bland de största användarna är tjänster kopplade till studentmobilitet, bland annat inom Erasmus-programmet. En annan tjänst som har stor betydelse för forskningssektorn är säker inloggning till superdatorresurser inom EuroHPC-samarbetet där användningen av eIDAS-noden (via integrationer på SUNET) har bidragit till att sänka kostnaden för onboarding av forskare till känsliga resurser. Av dessa orsaker har SUNET identifierat att det är viktigt att bidra till driften och utvecklingen av eIDAS-noden och Sweden Connect.

5 Bilagor

#	Beskrivning	Placering dokument
1	Budget Digg-SUNET_2024_2025	G:\Tillit_och_säkerhet\Identitet och auktorisation\Avtal\Vetenskaps rådet\Samverkansavtal 2024-2025\Arkiv
2	Säkerhetsskyddsanalys	Säkerhetsklassat dokument. Tillgänglig via Avdelning för tillit och säkerhet (Enheten för säkerhet)
3	Mötesanteckningar sourcingstrategi	Samarbeta
4	Kravställning	Samarbeta
5	Säker och kostnadseffektiv it-drift	https://www.regeringen.se/contentassets/7dfb476c7990499f8bf194954ba460b5/sou-2021_97_webb.pdf