Legitimeringstjänst IdP för medarbetare

- Beskrivning och tjänstespecifika villkor

inera
Ett företag inom SKR

Innehållsförteckning

Legitimeringstjänst IdP för medarbetare - Beskrivning och tjänstespecifika villkor

1 Inledning

Kundens beställning av Tjänsten, regleras av det Avtal om Kundens användning av Ineras Tjänster (”Avtalet”) som Kunden tecknat med Inera. Legitimeringstjänst IdP för medarbetare - Beskrivning och tjänstespecifika villkor utgör en unik del av Avtalet. För Avtalets övriga dokument se www.inera.se.

2 Bakgrund

Inera tillhandahåller Tjänsten, vilken är en infrastrukturtjänst inom området Identitet och åtkomst, som bidrar till att säkerställa Kundens e-tjänsters säkerhet, integritet och sekretess. Tjänsten bidrar till ett effektivt och säkert informationsutbyte. De är utformade för att bidra till att uppfylla kraven på säkerhet i EU:s dataskyddsförordning, patientdatalagen (2008:355) och Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården.

Kunden önskar ansluta till och nyttja Tjänsten i enlighet med vad som framgår av detta Avtal.

3 Referenser

Källa	Beskrivning
openid.net/developers/specs/ https://oauth.net/2/	Information om för Tjänsten relevant öppen standard (OpenId Connect).
www.inera.se	Information om tjänster och funktioner som tillhandahålls av Inera.
www.oasis-open.org/standards#samlv2.0	Information om för Tjänsten relevant öppen standard (Security Assertion Markup Language).
www.riksdagen.se	Information om för Tjänsten relevanta lagrum.
www.rivta.se/documents/ARK_0031/	Information om för Tjänsten relevant dokument (Patientdatalagen i praktiken (PDLiP)).
www.rivta.se/documents/ARK_0046/	Information om för Tjänsten relevant dokument (Referensarkitektur för Identitet och Åtkomst).

www.socialstyrelsen.se	Information om för Tjänsten relevanta föreskrifter.

4 Termer och begrepp

På www.inera.se förklaras termer och begrepp gemensamma för hela Inera. De kompletteras i Avtalet av avtalsdokumentet Definitioner. Termer och begrepp vilka är unika för Tjänsten beskrivs i detta kapitel.

Term	Definition	Förklaring
Identity Provider (”IdP”)		En tjänst som på begäran utför autentisering av en användare och utfärdar identitetsintyg med uppgifter om en identifierad användare
OpenID Connect (”OIDC”)		Enligt OAuth en öppen standard för att utbyta autentisering och behörigheter.
Security Assertion Markup Language (”SAML”)		Enligt OASIS en XML-baserad öppen standard för att utbyta autentisering och behörigheter.

5 Beskrivning av Tjänsten

5.1 Övergripande beskrivning av Tjänsten

Tjänsten gör det möjligt att kontrollera och fastställa en slutanvändares identitet vid inloggning i en ansluten e-tjänst.

Tjänsten möjliggör att kontroll av slutanvändarens identitet endast behöver göras en gång, oavsett hur många e-tjänster slutanvändaren loggar in i. Denna funktion kallas för Single Sign-On (”SSO”).

När en slutanvändare loggar in i en ansluten e-tjänst ska slutanvändarens identitet kontrolleras och fastställas. Detta möjliggörs av Tjänsten genom att Tjänsten sammanställer slutanvändarens uppgifter. Denna information lagras sedan i en så kallad biljett, som används som underlag för styrning av rättigheter i de e-tjänster som biljetten används av. Biljetten kan vara av typen SAML eller OIDC.

Tjänsten stödjer Ineras Tjänst Identifieringstjänst SITHS som autentiseringsmetod.

Tjänsten har följsamhet mot Referensarkitektur för Identitet och Åtkomst och använder sig av Ineras Tjänst Katalogtjänst HSA som attributkälla.

5.2 Syfte

Tjänsten kontrollerar och fastställer en slutanvändares identitet samt behörighetsstyrande egenskaper vid inloggning.

5.3 Regelverk

Tjänsten följer:

- Villkor för anslutning till Ineras tekniska infrastruktur, se www.inera.se.

5.4 Beroenden

Tjänsten är beroende av följande av Ineras Tjänster:

- Identifieringstjänst SITHS
- Katalogtjänst HSA.

6 Behandling av personuppgifter

Tjänsten behandlar personuppgifter. Behandlingen regleras av SKR-koncernens personuppgiftsbiträdesavtal, Allmänna instruktioner och detta avtalsdokuments tjänstespecifika instruktioner, vilka är en del av Avtalet.

Kunden ska om den indirekt ansluter andra Vårdgivare följa anvisningarna i Allmänna villkor.

6.1 Personuppgiftsbehandlingens förhållanden

6.1.1 Föremålet för behandlingen

Tjänsten.

6.1.2 Behandlingens varaktighet

Tills vidare.

6.1.3 Behandlingens art

Identitetskontroll vid inloggning till en e-tjänst.

6.1.4 Behandlingens ändamål

Att kontrollera och fastställa en slutanvändares identitet och behörighet vid inloggning till en e-tjänst.

6.1.5 Typ av personuppgifter

För samtliga kategorier av registrerade personer behandlas följande typer av personuppgifter:

- Identifikationsnummer (personnummer)
- Identifikationsuppgifter (förnamn, efternamn och HSA-id)
- Kontaktuppgifter (e-postadress och telefonnummer).

6.1.6 Kategorier av registrerade personer

- Medarbetare hos Kunden
- Medarbetare hos Inera och Ineras underleverantörer.

6.2 Tjänstespecifika instruktioner

Inera ska vid behandling av Kundens personuppgifter vidta följande tjänstespecifika instruktioner:

1. Tillhandahålla Kunden funktionalitet för att fastställa slutanvändarens identitet med hjälp av autentiseringsmetoder baserat på Ineras Tjänst Identifieringstjänst SITHS.
2. Tillhandahålla Kunden funktionalitet för att, baserat på slutanvändarens identitet, fastställa slutanvändarens behörighet genom slagningar i attributkällan i Ineras Tjänst Katalogtjänst HSA.
3. Tillhandahålla Kunden funktionalitet för att läsa identitet och behörighet för slutanvändaren i en så kallad biljett av typen SAML eller OIDC som Kundens e-tjänst kan använda i syfte att avgöra slutanvändarens åtkomst.
4. Tillhandahålla Kunden SSO-funktionalitet så att flera av Kundens e-tjänster kan avgöra slutanvändarens åtkomst genom endast en interaktion med autentiseringsmetoden.

7 Anslutning till Ineras tekniska infrastruktur

7.1 Anslutning till nationella tjänsteplattformen

Inte tillämpligt

Denna Tjänst tillhandahålls via Ineras tekniska infrastruktur. Kunden har som en del av Avtalet förbundit sig att följa Villkor för anslutning till Ineras tekniska infrastruktur när den ansluter till, och använder, Tjänsten.

8 Åtaganden

8.1 Kundens åtaganden

Kunden åtar sig

att följa de vid var tid gällande regelverk som framgår av punkten 5.3.

att beställa och ansluta till Ineras Tjänster som framgår av punkten 5.4.

att vid incidenter och problem

a) följa Ineras processer för felsökning och avhjälpande av fel
b) samverka med Inera och de övriga aktörer som är involverade i incidenten eller incidenterna och/eller problemet eller problemen, samt deras eventuella underleverantörer, intill dess att incident och problem är slutligt hanterade.

att förse Inera med förstudie vilket utvisar Kundens avsedda anslutning till Tjänsten.

att i enlighet med av Inera godkänd förstudie, utföra kvalitetssäkring av sin anslutning till Tjänsten mot de test- och produktionsmiljöer som Inera anvisar.

att följa de anvisningar för SSO som finns publicerade på www.inera.se.

att vid var tidpunkt ha en utsedd kontaktperson som är ansvarig för kommunikation med Inera avseende Tjänsten.

8.2 Ineras åtaganden

Inera åtar sig

att tillhandahålla Tjänsten.

att så snart det är möjligt underrätta Kunden om ändringar i förhållanden som kan anses vara av betydelse för Kundens anslutning.

att vid var tidpunkt ha en utsedd kontaktperson, vilken är ansvarig för kommunikation med Kunden avseende Tjänsten.

9 Servicenivåer för tjänsten

9.1 Definitioner

Tillgänglighet ska mätas med hjälp av följande mätvärden och definitioner.

Begrepp	Definition
Avbrottstid	Avbrottstid är den tid då det föreligger ett fel eller avbrott, vilket tillhör felklass Kritisk eller Hög i enlighet med vad stadgas på www.inera.se. Beräkningen av Avbrottstiden inkluderar inte följande: • Avbrott till följd av force majeure. • Planerade avbrott.

	• Annat avbrott, vilket beror på omständigheter, vilka Inera inte svarar för.
Total tid	Den aktuella mätperioden som utgörs av kalendermånad.
Tillgänglighet	Tillgängligheten beräknas enligt följande formel: *Tillgänglighet (i procent) = 100 – (Avbrottstid/Total tid) * 100*

9.2 Tillgänglighet Tjänsten

Inera har som mål att upprätthålla en tillgänglighet på 99,95 procent (%) dygnet runt alla dagar i veckan för Tjänsten. Kunden äger dock inte rätt att göra gällande några påföljder gentemot Inera om inte nämnda tillgänglighet nås.

Inera ska vid utförande av service och underhåll av Tjänsten i möjligaste mån undvika störningar eller avbrott i IT-driften och i synnerhet undvika störningar eller avbrott under kontorstid. Inera ska på sätt Inera finner lämpligt meddela Kunden inom skälig tid före planerat driftstopp i Tjänsten.

10 Support

Inera ska tillhandahålla support gentemot Kunden i enlighet med vid var tid gällande rutiner vilka återfinns på www.inera.se.