

Legitimeringstjänst IdP för invånare

- Beskrivning och tjänstespecifika villkor

Innehållsförteckning

Legitimeringstjänst IdP för invånare - Beskrivning och tjänstespecifika villkor	2
1 Inledning.....	2
2 Bakgrund	2
3 Referenser	2
4 Termer och begrepp	3
5 Beskrivning av Tjänsten.....	3
5.1 Övergripande beskrivning av Tjänsten	3
5.2 Syfte	4
5.3 Regelverk.....	4
5.4 Beroenden	4
6 Behandling av personuppgifter	4
6.1 Personuppgiftsbehandlings förhållanden	4
6.1.1 Föremålet för behandlingen.....	4
6.1.2 Behandlingens varaktighet.....	4
6.1.3 Behandlingens art.....	4
6.1.4 Behandlingens ändamål	4
6.1.5 Typ av personuppgifter	4
6.1.6 Kategorier av registrerade personer	5
6.2 Tjänstespecifika instruktioner	5
7 Anslutning till Ineras tekniska infrastruktur	5
7.1 Anslutning till nationella tjänsteplattformen	5
8 Åtaganden	5
8.1 Kundens åtaganden	5
8.2 Ineras åtaganden	5
9 Servicenivåer för tjänsten	6
9.1 Definitioner	6
9.2 Tillgänglighet Tjänsten	6
10 Support	6

Legitimeringstjänst IdP för invånare - 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 invånare - 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. Den är utformad 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/	Information om för Tjänsten relevant öppen standard (OpenId Connect).
https://oauth.net/2/	Information om tjänster och funktioner som tillhandahålls av Inera.
www.inera.se	
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. 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 är av standardtypen OIDC eller SAML. 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").

Tjänsten har följsamhet mot Referensarkitektur för Identitet och Åtkomst.

5.2 Syfte

Tjänsten kontrollerar och fastställer en slutanvändares identitet vid inloggning.

5.3 Regelverk

Inte tillämpligt.

5.4 Beroenden

Inte tillämpligt.

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 vid inloggning till en e-tjänst.

6.1.5 Typ av personuppgifter

- Identifikationsnummer (personnummer eller samordningsnummer)
- Identifikationsuppgifter (förnamn och efternamn)
- Kontaktuppgifter (e-postadress och telefonnummer).

6.1.6 Kategorier av registrerade personer

- Invånare

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.
2. Tillhandahålla Kunden funktionalitet för att läsa identitet för slutanvändaren i en så kallad biljett av typen SAML eller OIDC som Kundens e-tjänst kan använda i syfte att avgöra slutanvändarens åtkomst.
3. 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.

8 Åtaganden

8.1 Kundens åtaganden

Kunden åtar sig

- att vid var tidpunkt ha en utsedd kontaktperson, vilken är ansvarig för kommunikation med Inera avseende Tjänsten.
- att vid avbrott i Tjänstens tillhandahållande på egen bekostnad disponera och använda ett manuellt backup-system. Detta åtagande består bl.a. men inte uteslutande i att Kunden manuellt ska utföra de av Tjänstens funktioner, vilka det åligger Kunden att utföra.

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: $\text{Tillgänglighet (i procent)} = 100 - (\text{Avbrottstid} / \text{Total tid}) * 100$

9.2 Tillgänglighet Tjänsten

Inera har som mål att upprätthålla en tillgänglighet på 99,80 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.