

Identifieringstjänst SITHS

- Beskrivning och tjänstespecifika villkor

Innehållsförteckning

Identifieringstjänst SITHS - Beskrivning och tjänstespecifika villkor	2
1 Inledning.....	2
2 Bakgrund	2
3 Referenser	2
4 Termer och begrepp	2
5 Beskrivning av Tjänsten.....	3
5.1 Övergripande beskrivning av Tjänsten	3
5.1.1 SITHS Ombud	3
5.1.2 Tredjepartsansluten organisation	3
5.2 Syfte	3
Tjänsten har följande tre huvudsyften	3
5.3 Regelverk.....	4
5.4 Beroenden	4
6 Behandling av personuppgifter	4
6.1 Personuppgiftsbehandlingens 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	5
6.1.5 Typ av personuppgifter	5
6.1.6 Kategorier av registrerade personer	5
6.2 Tjänstespecifika instruktioner	5
7 Anslutning till Ineras tekniska infrastruktur	6
7.1 Anslutning till nationella tjänsteplattformen	6
8 Åtaganden	6
8.1 Kundens åtaganden	6
8.2 Ineras åtaganden	7
9 Servicenivåer för tjänsten	7
9.1 Definitioner.....	7
9.2 Tillgänglighet Tjänsten	8
10 Support	8
11 Särskilda villkor avseende indirekt anslutna vårdgivare	8

Identifieringstjänst SITHS - 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. Identifieringstjänst SITHS - Beskrivning och tjänstespecifika villkor utgör en unik del av Avtalet. För Avtalets övriga dokument se www.inera.se.

Tjänsten har särskilda villkor avseende Kundens möjlighet att i enlighet med avsnitt 5 Ineras allmänna villkor indirekt ansluta andra vårdgivare, se avsnitt 11.

2 Bakgrund

Inera tillhandahåller Tjänsten för att möjliggöra elektronisk identifiering av Kundens medarbetare och uppdragstagare, servrar, system och e-tjänster inom eller för vård och omsorg.

Tjänsten tillhandahåller och möjliggör kontroll av identiteten på Kundens medarbetare och uppdragstagare samt ger spårbarhet vid åtkomst till känsliga uppgifter.

3 Referenser

Källa	Beskrivning
www.digg.se	Information om tillitsramverket för Svensk e-legitimation.
www.dnvgl.se	Information om bestämmelser för certifiering av ID-kort (SBC 151-U).
www.inera.se	Information om tjänster och funktioner som tillhandahålls av Inera.

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
SITHS -ombud	Kund som tillhandahåller Tjänsten till Tredjepartsanslutna organisationer.	
Tredjepartsansluten organisation	Organisation som via ett SITHS-ombud ansluter till Tjänsten.	
Utgivningsområde	En eller flera organisationer som har samma ansvarig utgivare vilken lyder under Tjänstens tillitsdeklaration.	

5 Beskrivning av Tjänsten

5.1 Övergripande beskrivning av Tjänsten

Tjänsten består av att enligt SITHS tillitsramverk utfärda och administrera elektroniska identiteter för personer, servrar, system och e-tjänster. De elektroniska identiteterna möjliggör stark autentisering vid inloggning till e-tjänster.

Tjänsten gör det möjligt för Kunden att utfärda elektroniska identiteter inom Kundens Utgivningsområde. Tjänsten säkerställer att tillit upprätthålls genom att elektroniska identiteter utfärdas och administreras enligt SITHS tillitsramverk och gemensamma rutiner. Kunden kan med Tjänsten utfärda e-legitimationer med tillitsnivåerna 2 och 3. Tillitsnivåerna definieras i SITHS tillitsramverk och följer tillitsramverket för Svensk e-legitimation.

5.1.1 SITHS Ombud

För att agera SITHS ombud ska kunden

- teckna Avtal med Inera
- teckna samarbetsavtal med Tredjepartsansluten organisation

5.1.2 Tredjepartsansluten organisation

En Tredjepartsansluten organisation ska teckna samarbetsavtal med SITHS-ombudet. En Tredjepartsansluten organisation får inte agera SITHS-ombud.

5.2 Syfte

Tjänsten har följande tre huvudsyften:

- Stark autentisering av Kundens medarbetare och uppdragstagare vid inloggning till e-tjänster.
- Identifiering av servrar och kryptering av information vid överföring mellan olika system. Certifikatet som används innehåller information om vilken Kund eller organisation som funktionen ingår i. Med funktion avses servrar, system och e-tjänster.
- Identifiering av servrar och kryptering av information när den överförs från en e-tjänst till en person som loggar in på en webbsida.

5.3 Regelverk

Tjänsten följer:

- SITHS tillitsramverk (regler som följer av SITHS Certificate Policy)
- Tillitsramverk för kvalitetsmärket Svensk e-legitimation.

5.4 Beroenden

Tjänsten är beroende av följande av Ineras Tjänster:

- 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

Utfärdande och administration av elektroniska identiteter.

6.1.4 Behandlingens ändamål

Administration av elektroniska identiteter.

6.1.5 Typ av personuppgifter

- För samtliga kategorier av registrerade personer behandlas följande typer av personuppgifter:
 - Identifikationsnummer (personnummer, samordningsnummer)
 - Identifikationsuppgifter (förnamn, efternamn, HSA-id)
 - Kontaktuppgifter (e-postadress).
 - id-handlingens nummer
 - Biometri (foto)

6.1.6 Kategorier av registrerade personer

- Personal hos Inera
- Studenter
- Tandvårdspersonal
- Vård- och omsorgspersonal
- Övrig personal hos Kunden som har ett anställnings- eller uppdragsförhållande till Kunden.

6.2 Tjänstespecifika instruktioner

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

- 1) I enlighet med SITHS tillitsramverk
 - a) tillhandahålla funktionalitet för att Kunden ska kunna skapa elektroniska identiteter.
 - b) bevara elektroniska identiteter för medarbetare som registrerats av Kunden.
 - c) gallra bevarade elektroniska identiteter som registrerats av Kunden 10 år efter skapandedatum.
 - d) säkerställa funktionalitet för Kunden att revokera (spärra) elektroniska identiteter.
 - e) tillhandahålla funktionalitet för att säkerställa spårbarhet i Tjänsten.
- 2) Tillhandahålla funktionalitet för att Kunden ska kunna begränsa åtkomst till uppgifter om medarbetare med skyddade personuppgifter.

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 utföra autentisering och kontroll av giltighet för elektroniska identiteter där Tjänsten används i lokala system.
- att vid avbrott i Tjänstens tillhandahållande på egen bekostnad disponera och använda ett manuellt backup-system. Detta åtagande består bland annat i att säkerställa att de elektroniska identiteterna är giltiga genom att använda Tjänstens gemensamma spärrlista lokalt samt att ha en kontinuitetsplan för att säkerställa fortsatt verksamhet om det inte går att utfärda SITHS-kort och certifikat.
- att lämna in sin tillitsdeklaration enligt SITHS tillitsramverk när SITHS Policy Authority, den policygrupp som äger och definierar regelverket för Tjänsten, begär det.
- att uppfylla de krav och efterleva de regler och rutiner som framgår av SITHS tillitsramverk.
- att tillse att intern revision och uppföljning inom Kundens egen organisation utförs enligt SITHS tillitsramverk.
- att medverka i Ineras revisioner enligt SITHS tillitsramverk.
- att omgående meddela Inera om säkerhetsincident uppstår. Säkerhetsincident är en händelse som lett till bekräftad eller befarad risk som rör konfidentialitet eller riktighet.
- att omgående meddela Inera vid organisations- och funktionsförändringar som påverkar Utgivningsområdet enligt SITHS tillitsramverk.

att omgående meddela Inera om Kundens organisation upphör, samt säkerställa att samtliga certifikat som finns utfärdade för Kunden spärras enligt SITHS tillitsramverk.

Om Kunden som SITHS-ombud tillhandahåller Tjänsten till Tredjepartsansluten organisation åtar sig Kunden

att innan anslutning sker, teckna samarbetsavtal med den Tredjepartsanslutna organisationen avseende villkoren för anslutningen.

att ansvara för att den Tredjepartsanslutna organisationen uppfyller och efterlever de regler och rutiner som framgår av SITHS tillitsramverk.

att ansvara för att under en treårsperiod revidera samtliga Tredjepartsanslutna organisationer enligt SITHS tillitsramverk.

8.2 Ineras åtaganden

Inera åtar sig

att tillhandahålla Tjänsten.

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

att genomföra revisioner enligt Ineras process för risk, revision och förbättring som återfinns på www.inera.se.

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.

11 Särskilda villkor avseende indirekt anslutna vårdgivare

Vad som sägs i avsnitt 5 Ineras allmänna villkor, avseende indirekt anslutna vårdgivare, gäller inte för Tjänsten. Kunden äger inte rätt att indirekt anslutna andra vårdgivare, eller någon annan typ av aktör, till Tjänsten. Kundens enda möjlighet att tillhandahålla Tjänsten till andra aktörer är att enligt punkten 5.1.1 agera SITHS-ombud.