Avtal om Kundens användning av Identifieringstjänst SITHS

Bilaga 1 - Specifikation av tjänsten

Mellan Inera och Kund

Innehåll

Bilaga 1 - Specifikation av Identifieringstjänst SITHS

1. INLEDNING

Detta dokument utgör Bilaga 1 - Specifikation Identifieringstjänst SITHS (nedan kallad Tjänsten), till det Avtal som upprättats mellan Inera och Kunden.

2. BAKGRUND

Inera stödjer verksamhetsutveckling i landsting, regioner och kommuner, med kvalitetssäkrade digitala tjänster, koordinering av digital utveckling samt kompetens inom interoperabilitet. Våra tjänster används av personal, invånare och beslutsfattare.

Inera tillhandahåller Tjänsten vilken består av elektronisk identifiering för personer, servrar, system och e-tjänster.

Det noteras att avtalsnamnet tidigare har varit SITHS anslutningsavtal men nu är ändrat till Avtal om kundens användning av Identifieringstjänst SITHS.

2.1 Referenser

Här listas de webbplatser, dokument och regelverk som refereras till för ytterligare information.

Referens	Beskrivning
Inera.se	Information kring tjänster och funktioner som tillhandahålls av Inera samt information kring avtal för Ineras tjänster, detaljerad arkitekturbeskrivning av Tjänsten samt tillhörande rutiner. Sådan information - vilken t.ex. kan bestå av instruktioner, stadganden och rutiner - utgör en del av detta Avtal även om den återfinnas på andra webbplatser som inera.se hänvisar och/eller länkar vidare till.

Referens	Beskrivning
Tillitsramverket för Svensk e-legitimation som återfinns på https://www.digg.se/	Tillitsramverket för Svensk e-legitimation syftar till att etablera gemensamma krav för utfärdare av Svensk e-legitimation. Kraven är fördelade på olika skyddsklasser – tillitsnivåer – som svarar mot olika grader av teknisk och operationell säkerhet hos utfärdaren och olika grader av kontroll av att en person som tilldelas en elektronisk identitet verkligen är den han eller hon utger sig för att vara. Nivåindelningen motsvarar den som används i den internationella standarden ISO/IEC 29115.
Microsoft rootcertifikatprogram	Globalt regelverk för utgivning av funktionscertifikat.
Webtrust.org	Globalt regelverk för betrodd CA.
Dnvgl.se	Särskilda bestämmelser för certifiering av ID-kort (SBC 151-U).

2.2 SITHS regelverk

Dessa dokument återfinns på Inera.se

Regelverk	Beskrivning
SITHS Certificate Policy	Certifikatpolicy som innehåller grundläggande regler för SITHS.
SITHS rutiner	Bilaga till SITHS tillitsramverk som beskriver hur de elektroniska identiteterna skapas och administreras.
SITHS tillitsramverk	Praktiskt orienterad beskrivning av regler som följer av SITHS certifikatspolicy.
SITHS tillitsdeklaration	En beskrivning av att och hur utgivningsområdet uppfyller SITHS tillitsramverk och rutiner för SITHS.

2.3 Definitioner

Term/begrepp	Definition
Ansvarig utgivare	Person som är ansvarig för all utgivning av certifikat inom sitt utgivningsområde.
Bärare	Lagringsplats för e-legitimation.
SITHS-certifikat	Elektroniskt intyg som innehåller uppgifter som möjliggör identifiering av e-legitimationens innehavare vid legitimering, underskrift eller bådadera.
SITHS PA	Den policygrupp som äger och definierar regelverket för SITHS.
SITHS Admin	Det gränssnitt som id-administratörer använder för livscykelhantering av bärare och certifikat.
SITHS utgivningsområde	En eller flera organisationer som har samma SITHSAnsvarig utgivare som lyder under SITHS tillitsdeklaration.
SITHS	En tjänst för att tillhandahålla och livscykelhantera • en elektronisk tjänstelegitimation och identitetshandling som säkert identifierar användaren och används med certifikat på ett kort eller på en mobil bärare (Mobilt SITHS) • SITHS funktionscertifikat för autentisering och kryptering av information när e-tjänster, system eller servrar kommunicerar med varandra.
e-identitetsutfärdare	Funktion hos en användarorganisation eller dess underleverantör som efter en säker identifiering utfärdar och tillhandahåller E-legitimationer till Användare.
e-legitimation	Identitetshandling i elektronisk form, som vid elektronisk kommunikation används för legitimering, underskrift eller bådadera.
Elektronisk identitet	Information som på ett tekniskt eller juridiskt tillförlitligt sätt är förbunden med en fysisk eller juridisk person och utifrån vilken personen kan identifieras i en elektronisk miljö.

Term/begrepp	Definition
Funktionscertifikat	Certifikat som identifierar ett system eller en tjänst.
HSA-id	Unik identifierare för personer, enheter, funktioner, uppdrag och organisationer i Katalogtjänst HSA.
Id-administratör	Samlingsnamn för alla administratörer som har en behörighet/roll att livscykelhantera bärare och certifikat inom tjänsten SITHS.
Katalogtjänst HSA	En elektronisk katalog som innehåller kvalitetsgranskade uppgifter om personer och verksamheter inom svensk vård och omsorg.
Lokala system	System som används av Kunden där Kunden har eget avtal med leverantören.
Mobilt SITHS	En e-legitimation som lagras i en kvalificerad applikation (motsvarar chippet på ett smart kort) på en bärare exempelvis en mobiltelefon eller en platta.
Nationella tjänsteplattformen	Nationella tjänsteplattformen är ett tekniskt integrationsnav via vilket s.k. tjänsteproducenter och tjänstekonsumenter inom den nationella infrastrukturen för vård och omsorg utbyter information. Kunden kan, genom att integrera ett eller flera av sina IT-system med Nationella tjänsteplattformen skapa förutsättningar för att delta i informationsbytet.
Ombud	De som efter SITHS PAs godkännande ansluter Tredje part till SITHS.
Referensarkitekturen	Referensarkitektur för identitet och åtkomst som beskriver hur e-tjänster och infrastrukturtjänster ska anpassas till en modern IT-arkitektur för att möta vårdens krav.
Regler för interoperabilitet inom vård och omsorg (RIV)	Ett nationellt regelverk som styr integration inom vård och omsorg. RIV täcker såväl semantisk som teknisk interoperabilitet.

Term/begrepp	Definition
Regler för interoperabilitet inom vård och omsorg - tekniska anvisningar (RIV TA)	En samling regler och anvisningar som reglerar det interoperabla informationsutbytet mellan tjänstekomponenter.
Rotcertifikatprogram	Hanterar krav på granskningsprocess för att kunna vara med på en lista över tillförlitliga rotcertifikat.
Navet	Skatteverkets elektroniska aviseringssystem för att hämta folkbokföringsuppgifter
Säkerhetstjänster	Säkerhetstjänster består av ett antal tjänster som sammantaget gör det möjligt för en organisation att reglera och följa upp åtkomsten till patientinformation.
Tredje part	Den part som ansluts till SITHS via Ombud.

3. TJÄNSTEBESKRIVNING

3.1 Beskrivning av Tjänsten

Tjänsten består i att tillhandahålla en elektronisk identitet för personer, servrar, system och e-tjänster inom offentlig sektor. Denna elektroniska identitet möjliggör stark autentisering vid inloggning till e-tjänster.

SITHS utfärdar e-legitimationer till de organisationer som är anslutna till tjänsten. SITHS säkerställer att tillit mellan organisationerna upprätthålls genom att e-legitimationerna utfärdas enligt SITHS tillitsramverk med gemensamma rutiner. Tjänsten kan utfärda e-legitimationer med tillitsnivå 2 och 3. E-legitimation med tillitsnivå 4 kan uppnås för definierade utgivningsprocesser. Tillitsnivåer 2, 3 och 4 definieras i E-legitimationsnämndens tillitsramverk.

Tjänsten tillhandahåller de programvaror som behövs för använda administrationsverktyget, SITHS Admin samt för att användare ska kunna nyttja sina e-legitimationer.

3.2 Tjänstens syften

Tjänsten har följande tre (3) huvudsyften.

a) Stark autentisering av användare vid inloggning till tjänster. SITHS-certifikatet innehåller information om vem en person är och var den arbetar.

b) Identifiering av system och kryptering av information vid överföring mellan olika system. Innehåller information om vilken organisation funktionen tillhör. För dessa certifikat finns kopplingar till HSA-katalogen för adressering av system inom vård- och omsorgsdelen av offentlig sektor.

c) Identifiering av tjänster och kryptering av information när den överförs från en tjänst till en användare. För dessa certifikat är SITHS medlem i ett antal rotcertifikatprogram för att underlätta att operativsystem (även på mobiltelefoner), webbläsare och applikationer installerar tillit till SITHS automatisk.

3.3 Kundens användning

Tjänsten har följande tre (3) användningsområden.

a) Id-administration
Anslutna organisationer får genom inloggning åtkomst och tillgång till det behörighetsstyrda administrationsverktyget som används vid utfärdande av elektroniska identiteter samt livscykelhantering av e-legitimationer och bärare.

b) Elektronisk identitet för användare
Användare identifierar sig vid inloggning i e-tjänster med ett SITHS-certifikat som ligger på ett kort eller med ett certifikat som kan användas på en mobil bärare. Även andra bärare kan bli aktuella i framtiden.

c) Elektronisk identitet för system/e-tjänst
Beställare/Mottagaren av ett SITHS funktionscertifikat för dialog med administratören om val av typ av funktionscertifikat. Kunden installerar sedan i rätt system.

3.4 Regelverk och policys

SITHS och anslutna organisationer ska följa de regelverk och policys som anges i punkt 2.1 och 2.2 för att uppnå och upprätthålla tillit och säkerhet.

Beslut om anslutning av ny organisation samt godkännande av SITHS tillitsdeklaration fattas av SITHS PA.

4. ARKITEKTURBESKRIVNING

4.1 Informationsflöden via Nationella Tjänsteplattformen

Kommunikationen med Ineras personuppgiftstjänst går via Nationella tjänsteplattformen och följer RIV och RIV TA.

4.2 SITHS relation till Säkerhetstjänster

Säkerhetstjänster använder E-legitimationer för att autentisera användare vid inloggning till en e-tjänst. SITHS används i referensarkitekturen som e-identitetsutfärdare. SITHS har som mål att använda Säkerhetstjänster för autentisering även vid inloggning till SITHS Admin.

4.3 Katalogtjänst HSA

SITHS använder Katalogtjänst HSA som informationskälla för funktionscertifikat och de e-legitimationer som utfärdas för medarbetare i vård och omsorg. HSA-id och organisationsuppgifter hämtas från Katalogtjänst HSA. HSA hämtar namn och personnummer från Skatteverkets Navet och Personuppgiftstjänsten.

5. ÅTAGANDEN

5.1 Kundens åtaganden

Kunden åtar sig i enlighet med detta Avtal.

att när SITHS PA begär lämna in SITHS tillitsdeklaration.

att uppfylla de krav och efterleva de regler och rutiner som framgår av SITHS tillitsramverk.

att snarast meddela Inera vid organisations- och funktionsförändringar som påverkar inlämnad SITHS tillitsdeklaration.

att meddela Inera uppgifter om kontaktpersoner och fortlöpande hålla dessa kontaktuppgifter uppdaterade.

att tillse så intern revision och uppföljning inom den egna organisationen utförs enligt punkt 5.3 nedan, SITHS tillitsramverk och SITHS tillitsdeklaration.

att medverka i Ineras revisioner i enlighet med detta Avtal, punkt 5.3.

att snarast meddela Inera om säkerhetsincident uppstår.

att snarast meddela Inera om Kundens organisation upphör att existera i den form den hade vid tecknandet av detta Avtal samt säkerställa att samtliga certifikat som finns utfärdade för Kunden spärras.

att lokala system utför autentisering och kontroll av giltighet för elektroniska identiteter.

att SITHS funktionscertifikat installeras och förnyas.

att vid incidenter och problem

a) följa Ineras processer för felsökning, avhjälpande av fel, systemändring, driftsättning och test.

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.

c) följa Ineras anvisningar för övervakning och Ineras tekniska SLA för Tjänsten.

att utföra kvalitetssäkring av sin anslutning till Nationella tjänsteplattformen mot de testmiljöer som Inera anvisar.

att använda sin anslutning till Nationella tjänsteplattformen mot den produktionsmiljö som Inera anvisar.

5.2 Ineras åtaganden

Inera åtar sig i enlighet med detta avtal.

att i enlighet med vad som anges i detta Avtal tillhandahålla tjänsten.

att ansvara för Tjänstens anslutning till Nationella tjänsteplattformen.

att följa vid var tid gällande tjänstekontrakt som Tjänsten använder sig av.

att granska Kundens SITHS tillitsdeklaration och återkoppla till Kunden inom skälig tid med godkännande från SITHS Policy Authority eller begäran om kompletteringar.

att etablera och vidmakthålla en förvaltningsorganisation för SITHS samt att bemanna förvaltningsorganisationen med målet att samarbete, aktuella regelverk, servicenivåer och avtal följs och utvecklas.

att följa upp Kundens följsamhet till SITHS tillitsramverk.

5.3 Revision

Alla anslutna organisationer ska göra en egen intern revision, för att kontrollera att de följer regelverken för SITHS. Ineras process för risk, revision och förbättring lägger

grund för att systematiskt säkerställa tillit. Processen kan användas av ombud, anslutna organisationer och Inera som stöd för intern revision.

Även externa revisioner ska göra enligt Ineras process för risk, revision och förbättring som återfinns på Inera.se.

Syftet med både den interna och externa revisionen är att följa upp hur rutiner och arbetsprocesser efterlevs i användandet av SITHS.

Krav för att säkerställa tilliten:

1. Ansluten organisation ska säkerställa sin egen tillit genom intern revision minst en (1) gång per år.
2. Ansluten organisation ska besvara en självdeklaration, som Inera tillhandahåller, minst en (1) gång per år.
3. Revision hos ansluten organisation ska göras på plats enligt Ineras revisionsprogram.
4. Utöver de fastställda revisionerna utförs ett antal revisioner varje år där urvalet av organisationer är riskbaserat. Detta bygger delvis på analysen från självdeklarationerna samt på identifierade brister från tidigare år.
5. Revision ska resultera i en revisionsrapport med identifierade avvikelser, vilken ska kommunicerad respektive reviderad organisation. I revisionsrapporten anges när åtgärdsplan ska vara inlämnad till revisorn samt tidpunkt för uppföljning av åtgärdsplanen.
6. Vid uppföljning av åtgärdsplanen ska organisationen kunna påvisa ett genomfört förbättringsarbete i enlighet med inlämnad åtgärdsplan.
7. Vid revision av ombud följer Inera upp att ombuden i sin tur säkrar tilliten hos de organisationer som är anslutna via ombudet (så kallade Tredje partsorganisationer).

5.4 Vid var tid gällande information samt ändringar i detta Avtal

Detta Avtals hänvisningar till information - t.ex. i form av instruktioner, stadganden och rutiner - på inera.se och/eller andra webbplatser som inera.se hänvisar vidare till, avser vid var tid gällande sådan information. Ineras ändringar i detta Avtal, inklusive information enligt första meningen, ska göras i enlighet med vad stadgas i Bilaga 2 - Allmänna villkor (Ineras allmänna villkor), punkt 9.1.

6. KUNDENS ÅTAGANDEN SOM OMBUD TILL TREDJE PART

Kunden kan efter SITHS PA:s skriftliga och uttryckliga godkännande ansluta en annan organisation som bedriver vård- eller omsorgsverksamhet till Tjänsten. När Kunden ansluter en sådan annan organisation till Tjänsten kallas Kunden ”Ombud” och den organisation som ansluts ”Tredje part”.

Vid Ombudets anslutning av Tredje part ansvarar Ombudet gentemot Inera för att Tredje part uppfyller de åtaganden gentemot Ombudet vilka Kunden enligt detta Avtal ska uppfylla gentemot Inera. Ombudets anslutning av Tredje part förutsätter därtill att vad som stadgas i första meningen regleras i avtal mellan Ombudet och Tredje part. Ombudets revision enligt punkt 5.3 ska även omfatta Tredje part. Tredje Part äger inte rätt att ansluta annan organisation till Tjänsten.

7. TILLÄGGSBESTÄLLNINGAR

Kunden äger rätt att beställa tilläggstjänster i enlighet med Ineras rutiner för tilläggstjänster, vilka återfinns på Inera.se.

8. SAMVERKANSFORMER

Parternas samverkan avseende Tjänsten och anslutna system, inklusive hantering av utveckling, ändring och tillägg till Tjänsten, ska hanteras i enlighet med vad som framgår av Ineras rutiner för samverkansformer, vilka återfinns på 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 Ineras rutiner för samverkansformer. Beräkningen av Avbrottstiden inkluderar inte följande: • Avbrott till följd av force majeure. • Planerade avbrott. • Annat avbrott som 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 99,98 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 meddela Kunden inom skälig tid före planerat driftstopp i Tjänsten.

9.3 Support

Inera ska tillhandahålla support gentemot Kunden i enlighet med rutiner för Kundservice och enligt prislista på Inera.se.

Meddelanden i enlighet med detta Avtal hanteras i enlighet med ovan.