|  |  |
| --- | --- |
|  | Förstudie avseende anslutning till Säkerhetstjänster – AutentiseringstjänstAnslutning av <anslutande part / anslutande system> |

[blå text i mallen ska ersättas med anslutande parts uppgifter]

# Ändringshistorik mall

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Revision** | **Beskrivning** | **Författare** |
| 2020-11-19 | 0.1 | Grundläggande information och struktur | Hasanein Alyassiri, Grim Skarsgård, Niclas Hedlund, Christoffer Johansson |
| 2021-01-18 | 0.2 | Linjering med mall för IdP | Niclas Hedlund |
| 2021-05-03 | 0.3 | Tydligande krav | Niclas Hedlund |
| 2021-05-17 | 1.0 | Förtydligat kring IPadress | Niclas Hedlund |
|  |  |  |  |

**Innehållsförteckning**

Ändringshistorik mall 2

1. Inledning 4

1.1 Syfte med förstudien 4

1.2 Ändringshistorik förstudie 4

1.3 Ordlista och förkortningar 5

1.4 Referenser 5

2. Anslutning 6

2.1 Anslutande parts uppgifter 6

2.1.1 Identitet Lokal IdP 6

2.1.2 Kundkvalificering 7

2.1.3 Genomförandeplan 7

2.2 Förutsättningar 8

2.2.1 Anslutningsförutsättningar övriga komponenter/anslutningsprocess 8

2.3 Val av driftsmiljö(-er) för denna förstudie 8

3. Anslutningsarkitektur 9

3.1 Logisk anslutningsarkitektur och flöden 9

4. Kapacitet, test och kvalitetssäkring 10

4.1 Transaktionsvolymer 10

4.2 Testaktiviteter 10

4.3 Resultat 10

1. Inledning

För att kunna ansluta ett system till Säkerhetstjänster - Autentiseringstjänsten (nedan ATJ) behöver din organisation följa processen som beskrivs i

Anslutningsguide till Autentiseringstjänsten [R1] och dokumentationen [R2] är tänkt att vara stöd vid ifyllandet av denna förstudie.

* 1. Syfte med förstudien

Förstudien har följande syften:

* Säkerställande att förutsättningarna för från avsnittet ”Förutsättningar” i [R1] är på plats och följsamhet mot ”Relaying Party API” (avsnitt ”Teknisk information” i samma Guide), Ineras avtals.
* Säkerställa att system ansluts med rätt förutsättningar och förväntningar till rätt miljö
* Utgöra underlag för proaktiv resurs- och kapacitetsplanering samt möjliggöra spårbarhet för ändringar i anslutningen.

Samma förstudiemall kan med fördel återanvändas genom att endast relevanta delar uppdateras (Spara som..) men endast en miljö/system ansluts per inskickad förstudie.[[1]](#footnote-2) Undantag för multipla testmiljöer kan göras om dessa inte skiljer sig väsentligt åt och är tydligt specificerade (”vad ska anslutas till vad, med vilket metadata” etc).

* 1. Ändringshistorik förstudie

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Datum** | **Version** | **Miljö** | **Beskrivning** | **Författare** |
| [YYYY-MM-DD] | [X.Y] | [Beskrivning av ändring] | [Namn, Organisation] | [Namn, Organisation] |
|  |  |  |  |  |

* 1. Ordlista och förkortningar

|  |  |
| --- | --- |
| Begrepp | Definition |
| API | Se https://en.wikipedia.org/wiki/Application\_programming\_interface |
| Autentiseringstjänsten | Autentiseringstjänsten har syftet att facilitera autentisering med Out Of Band teknik. Det innebär att säkerhetskanalen är separerad från den primära informationskanalen. |
| Identity Provider (IdP) | Komponent i infrastrukturen som efter identifiering och godkänd autentisering av en användare, tillhandahåller elektroniska intyg (SAML biljett alternativt ”ID token” inom OIDC) med identitet och attribut tillhörande användaren och/eller hens organisation. |
| IAM | Identity and Access Management, identitets- och åtkomsthantering |
| LoA | Level of Assurance, tillitsnivå, enligt eIDAS. En kategori beskriven i [R2] som förmedlar graden av tillit (förlitande på) att den tillgångsökandes/slutanvändarens påstådda identitet är dess verkliga |
| mTLS | Mutual Transport Layer Security. “Transportlagersäkerhet”, är ett kryptografiskt kommunikationsprotokoll för säkert utbyte av krypterad information mellan datorsystem |
| PROD | Produktionsmiljö |
| QA-miljö | Quality Assurance – produktionsliknande testmiljö |
| Relying Party (RP) | Aktör eller komponent ansvarig för att begära och erhålla identitetsintyg. |

* 1. Referenser

[R1] Anslutningsguide till Autentiseringstjänsten, [confluence.cgiostersund.se/x/-kogDQ](https://confluence.cgiostersund.se/x/-kogDQ)

[R2] Autentiseringstjänst dokumentation, [confluence.cgiostersund.se/x/aDIgDQ](https://confluence.cgiostersund.se/x/aDIgDQ)

[R3] Gemensam anslutningsinformation, [confluence.cgiostersund.se/x/dAi-DQ](https://confluence.cgiostersund.se/x/dAi-DQ)

[R4] Nätverksinställningar för IAM-tjänster, [confluence.cgiostersund.se/x/7K30Cw](https://confluence.cgiostersund.se/x/7K30Cw)

1. Anslutning

Generell information om anslutningsflöde, se avsnitt 2 i Guiden [R1].

* 1. Anslutande parts uppgifter

Fyll i lämpliga kontaktuppgifter för denna anslutning (exempel nedan)

|  |  |  |  |
| --- | --- | --- | --- |
| Namn | Roll | Organisation | Epost[[2]](#footnote-3) |
|  | <Verksamhets-/systemägare> |  |  |
|  | <Teknisk systemansvarig> |  |  |
|  | <Anslutningskoordinator / projektledare> |  |  |

|  |  |
| --- | --- |
| Översikt anslutande system | Miljö |
| Anslutande system | *[system/e-tjänst]* | *[systemmiljönamn]* |
| Identitetsutfärdare | Säkerhetstjänster - Autentiseringstjänst | *[TEST/QA/PROD]* |
| Kommunikationsnät | *[internet/sjunet]* |  |
| OrganizationDisplayName (visas vid OOB metoder i klient­-appars gränssnitt) | *[organisation/system]* |  |

* + 1. Identitet Lokal IdP

Ange er lokala IdPs HSA-id i funktionscertifikatets subjekt.

|  |  |
| --- | --- |
| **Common Namn** | **HSA-id** |
| [CN] | [HSAid] |

* + 1. Kundkvalificering

Endast kommuner, landsting, regioner, statliga eller kommunala myndigheter samt privata aktörer på uppdrag (upphandlad) av nämnda organisationer kan ansluta till Autentiseringstjänsten.

|  |
| --- |
| **Privata organisationer i egen regi eller som agent är i dagsläget ej kvalificerade** |

 ***Anslutande part (organisation):***[anslutande part med giltigt kundavtal + organisationsnummer]

***Beskrivning:*** [Beskriv kort vilket/vilka system som ansluts, vad anslutningen syftar till att uppnå.]

* + 1. Genomförandeplan

*[Beskriv översiktligt de aktiviteter och milstolpar i anslutningsprojektet som omfattar nationell infrastruktur och aktuellt system. Exempel på relevant information: Anslutning inför test, Testperiod med lasttester, Produktionssättningsdatum. Förvaltningsöverlämning.]*

|  |  |  |
| --- | --- | --- |
| Aktivitet | Period | Ytterligare upplysningar |
| *[Beskriv aktivitet]* | *[YYYY-MM – YYYY-MM]* |  |
|  |  |  |

* 1. Förutsättningar
		1. Anslutningsförutsättningar övriga komponenter/anslutningsprocess

Information om förberedelser och SKALL-krav finns i guidens avsnitt 2, [R4]. Om något saknas, förtydliga i svaret.

|  |  |
| --- | --- |
| **Fråga** | **Svar** |
| Är de **generella** anslutnings­förutsättningarna [R3] på plats eller har tidsplan? | [ ]  <ev förtydligande> |
| Är de **specifika** anslutnings­förutsättningarna från på plats eller har tidsplan? Avsnitt 2 i [R2] | [ ]  *<ev förtydligande>* |
| Är förutsättningarna för **nätverk och konnektivitet** på plats? [R4]* Ange IP-adress för lokal IdP
 | [ ]  *<ev förtydligande>**<IP-adress>* |
| Görs det i anslutande IdP **avsteg från Ineras IdP autentiseringshantering**?* LoA nivå tolkas identiskt med Ineras IdP?
* Revokeringskontroll begärs utföras av Autentiseringstjänsten (checkRevocation=true)?
 | [ ]  *<ev förtydligande>*[ ]  *<ev förtydligande>* |

* 1. Val av driftsmiljö(-er) för denna förstudie

Nedan väljs vilken anslutningsmiljö som systemet för förstudien ska etablera tillit med. Observera att miljöerna har separata mobila klientapplikationer och olika godkända utfärdare av funktionscertifikat

|  |
| --- |
| **Anslutning till Produktionsmiljö kräver en separat förstudie** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Miljö** | **Val** | **Kommentar om syfte** | **Godkänd utfärdare funktionscertifikat (x.509)** | **SITHS eID App** |
| TEST | ☐ | Upplåts primärt för Inera-internt bruk och har senaste publika IdP versionen. Störningar förekommer under acceptanstester av olika IAM komponenter som sker i denna miljö | TEST SITHS e-id Function CA v1 | TEST SITHS eID |
| QA | ☐ | Produktionslik testmiljö för kunders anslutningar och system med höga krav på tillgänglighet och robusthet. Uppdateras 7-14 dagar innan produktionsmiljön. |  |
| QA SITHS eID |
| PROD | ☐ | Skarp produktionsmiljö. Endast produktions­system kan anslutas hit. | SITHS e-id Function CA v1 | SITHS eID |

1. Anslutningsarkitektur
	1. Logisk anslutningsarkitektur och flöden

[Beskriv översiktligt anslutningen med bild och text, vilka system som är inblandade och nödvändiga integrationer. Referensarkitekturens översikt nedan kan användas som utgångspunkt.

Översikten ska inkludera eventuella lokala system som t ex integrerar med ett eller flera av de nationella tjänsterna.]



Figur Exempel logisk anslutningsarkitektur

1. Kapacitet, test och kvalitetssäkring

Inför produktionssättning skall test och kvalitetssäkring genomföras för att säkerställa integrationen och den nationella infrastrukturen m a p funktion, säkerhet och trafikvolym. Finns separata dokument som beskriver dessa aktiviteter, bifoga dem i och referera till dem här.

Inera fäster ingen särskild vikt vid hur testerna genomförs men de dokumenterade resultaten ska återspegla de för anslutningen relevanta testfallen.

* 1. Transaktionsvolymer

*[Estimera hur många anrop som beräknas ske per timme samt hur de förväntas vara distribuerade över tid; en kortfattad beskrivning av systemets anropsmönster.]*

|  |  |
| --- | --- |
| Anslutande system | Uppskattat antal per timme |
| **Normalflöde**  | **Max-flöde (när inträffar det?)** |
| *[ange]* | *[antal/timme]* | *[antal/timme]* |

* 1. Testaktiviteter

*[I en förstudie för testmiljö skall detta avsnitt ha en beskrivning och gärna en tidsplan för de kvalitetssäkrande åtgärder som är planerade att utföras.]*

* 1. Resultat

*[I en förstudie för produktionsmiljö skall detta avsnitt ha resultaten från de tester som genomförts.]*

1. Exempelvis vid ändringar i metadata, kontaktuppgifter etc. [↑](#footnote-ref-2)
2. Endast funktionsbrevlådor accepteras vid anslutning till produktionsmiljö [↑](#footnote-ref-3)