Dokumenttyp: Analysrapport
Version: 0.1
Utfärdat av: John Petersson
Datum: 2019-12-31

Ev Godkänt av:
Datum:

Sammanställning analys Identitet och behörighet i federation VG

Förslag till beslut

- SITIV beslutar att godkänna uppsättning av lösning för Identitet och behörighet i federation Västra Götaland enligt analysens rekommendation.
- SITIV beslutar att godkänna uppstart av implementationsprojekt med en budget på 4 360 000 kronor med start 1 mars 2020 och omfattar implementeringsprojektets resursbehov och licenskostnaden för en IdP.

Sammanfattning

Projekt Identitet och behörighet i federation VG har hållit på sedan 1 augusti 2019, men har i praktiken varit operativ från mitten av september till 31 december 2019. Orsaken till att det dröjde med starten var resurssäkringen, som tog betydligt längre tid än förväntat. Projektet har under tiden genomfört en analys av de plattformar och ramverk som behövs för att få till en lösning för identitet och behörighet i federation för Västra Götaland.

Arbetet har genomförts genom enkäter, arbetsmöten (work shops) och genom att bygga en testlösning motsvarande en möjlig framtida skarp lösning. Sammanställningen innehåller den sammantagna bilden av analysen och projektets rekommendationer medans bilagorna innehåller det detaljerade resultatet från varje ingående aktivitet för projektet kopplat till projektplanen och dess definierade leveranser.

Arbetet har fallit ut väl och projektet har använt sig av de principer som definierats i projektplanen. Leverans sker på utsatt tid och inom tilldelad budget.

Utifrån de aktiviteter vi har gått igenom är slutsatsen den att det här inte är speciellt tekniskt svårt. Projektet har också en uppfattning om att lösningen som satts upp förefaller robust och snabb samt att det finns stora möjligheter att anpassa lösningsmönster utifrån våra krav på både funktion och hur det kommer uppfattas av slutanvändaren.

I rapporten finns det ingående beskrivet hur och vad det innebär att sätta upp den målbild projektet har haft i en skarp miljö. Kostnadsmässigt är det också attraktivt för Västra Götaland att sätta upp denna lösning i samverkan. Den stora frågan är hur detta skall förvaltas och vad som krävs för att leva upp till kraven för att kunna ingå i en federation. Dessa frågor har egna kapitel nedan som mer ingående beskriver problembilden och vad som kommer krävas av de olika parterna enligt projektets målbild. Det finns även en möjlighet att utifrån den tekniska designen implementera både diversitet och redundans, vilket ökar tillgänglighet och tillförlitlighet för lösningen.

Rekommendation

Projektets rekommendation är att gå vidare med en gemensam implementering i Västra Götaland i samverkan. Detta motiveras av;

- en attraktiv kostnadsbild
- en robust och väl fungerande teknisk lösning för identitet och behörighet utifrån redan befintliga strukturer i Västra Götaland
- en lösning som möjliggör förändringar över tid utan att det påverkar varje parts ingående system
- en säker och kontrollerad lösning som möter upp nationella- och EU-krav som finns för detta område.

Lösningen som rekommenderas omfattas av upphandling och implementering av, i Västra Götaland, gemensam IdP, med Mobilt BankID, Freja eID, SITHS och medföljande autentiseringsmetoder, kopplat till HSA och certifierad i Sambi som tillitsfederation.

Sammanställning av analysen

Nedan följer det sammanställning av analysen och testerna som genomförts i projektet och som ligger till grund för rekommendationen ovan.

Definition av Identitet och behörighet i federation

Projektet började med att det togs fram en definition av vad Identitet och behörighet i federation innebär och vad som definierar detta. Denna sammanställning blev den gemensamma godkända definitionen för projektet och projektets medlemmar och referensgrupper. Överenskommelsen inom projektet var att inte arbeta vidare med frågan innan alla var överens om att definitionerna i denna sammanställning var korrekt. Se bilaga 1.

Styrkor, svagheter, möjligheter och hot (SWOT)

Projektet har under projektets gång genomfört ett antal arbetsmöten där projektet tittat på varje ingående komponent och utifrån erfarenheter och kunskap bedömt dessa komponenter i en SWOT. Detta material har sammanställts och ligger till grund för analysen, det fortsatta arbetet och projektets rekommendation, se bilaga 2.

Enkät kommuner

Projektet skickade ut en enkät till kommunerna för att undersöka hur det ser ut i varje enskild kommun och hur de arbetar med frågan identitet och behörighet i federation idag. Övervägande del av kommunerna svarade på enkäten och projektet sammanställde resultatet, se bilaga 7. Detta förfarande behövdes inte göras för VGR, då arbetet inom detta område redan var känt av projektet.

Kommunernas svar på enkätfrågorna har varit vägledande i arbetet i projektet och har även använts för att säkerställa att projektets rekommendation inte är kontraproduktiv mot kommunerna och deras nuvarande arbete och strategiska inriktning.

Avtal, avrop och upphandling

I samråd med koncerninköp VGR, Göran Hallsten, har projektet kommit fram till följande slutsatser.

IdP

När det gäller upphandling av IdP finns det flera alternativ, men rekommendationen från koncerninköp är att göra ett licensavrop via en licenspartner eller en upphandling via Kammarkollegiet. Projektet förordar att en upphandling vid Kammarkollegiet genomförs eftersom det då går att ställa krav på stöd, utbildning, förvaltning och support på ett tydligare sätt och gynnar även en samverkanslösning i större utsträckning eftersom det ger en friare möjlighet till mer komplett lösning.

Federation Sambi

Rekommendationen från koncerninköp är att en anmodan för upphandling skickas till Koncerninköp för Sambi. Beroende på belopp finns det då möjlighet att genomföra en direktupphandling. Detta behöver utredas mer beroende på hur lösningen och överenskommelsen med IIS kommer se ut.

Autentiseringstjänster

Mobilt BankID

Denna tjänst finns det redan avtal på inom VGR och flera kommuner. Dessa avtal har projektet inte undersökt, men lämnar det som en rekommendation till implementeringsprojektet att genomföra. Utifrån detta får sedan beslut tas om hur detta skall upphandlas som tjänst. Mobilt BankID innebär en tickkostnad för varje inloggning som genomförs och därför kan det vara svårt att uppskatta beloppsgränser. Se kapitel om kostnader nedan.

Freja eID

Denna tjänst får upphandlas med en traditionell upphandling. Problemet är dock att det endast finns en leverantör av denna tjänst, vilket inte möjliggör någon konkurrensutsättning.

SITHS

Eftersom SITHS redan har en befintlig infrastruktur och organisation i Västra Götaland innebär denna autentiseringsmetod inga nya kostnader eller förändringar på befintlig lösning och avtal.

EIDAS

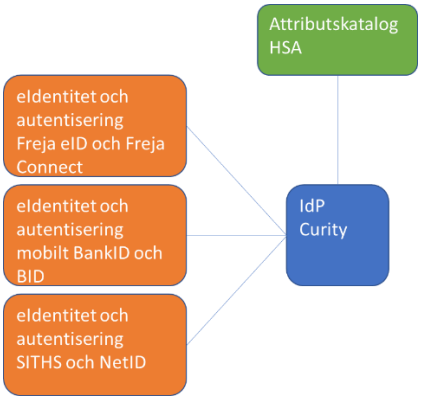
eIDAS och Sweden Connect är en tjänst som möjliggör hantering av elektronisk identifikation mellan anslutna länder. Genom att ansluta sig till den svenska noden finns det sedan möjlighet för medborgare med andra nationaliteter att använda sina egna godkända e-identiteter enligt eIDAS och att det finns en tillit kring olika länders e-identiteter.

Att ansluta sig till den svenska noden Sweden Connect innebär inga kostnader, men det krävs att det tecknas ett avtal med DIGG, Myndigheten för digital förvaltning. Det finns möjlighet för en samverkansorganisation att teckna ett sådant avtal och det behöver endast konfigureras i den gemensamma lösningen. Se bilaga 3.

Teknisk lösning

Beskrivning PoC

Den miljö projektet har satt upp för att testa de olika föreslagna teknikerna ser ut som följer.



IdPn är uppsatt i Göteborgs Stad och kopplingarna till autentiseringstjänsterna har gjorts mot befintliga testmiljöer som leverantörerna av varje tjänst tillhandahåller. Kopplingen till HSA har gjorts mot Göteborgs Stads testmiljö för HSA.

Installation och konfigurering av miljön har varit oerhört enkel och har gått förvånansvärt fort. Deltagarna i uppsättningen av lösningen anser att det har varit enkelt, smidigt och intuitivt att arbeta med miljön och resultatet har blivit rätt från början i nästan alla fall. Slutsatsen från byggandet av testmiljön är; att med adekvat utbildning av förvaltande parter kommer detta inte innebära några problem och det finns stora möjligheter att förvalta och konfigurera lösningen i egen regi. Projektet har också en uppfattning om att lösningen vi satt upp förefaller robust och snabb samt att det finns stora möjligheter att anpassa lösningsmönster utifrån våra krav på både funktion och hur det kommer uppfattas av slutanvändaren.

Katastrofhantering

En stor fråga i analysen är hur miljön skall sättas upp ur ett katastrofperspektiv. Den IdP-leverantör projektet har använt i PoC:en har erfarenhet av detta och har lämnat följande beskrivning för hur detta skall kunna sättas upp utan att licensomfattningen påverkas.

En instans av IdP sätts upp i t.ex. VGR och en instans sätts upp i t.ex. Göteborgs Stad. Den ena är s.k. kall och den andra är s.k varm. Via en lastbalanserare, t.ex. F5, går det sedan sätta upp logik som växlar mellan dessa instanser om någon av instanserna blir otillgängliga av någon orsak. De två instanserna sätts upp i befintliga datacenter, oavsett om de är geografiskt spridda, med redundans. Genom denna konfiguration implementeras både diversitet och redundans, vilket ökar tillgänglighet och tillförlitlighet för lösningen. Kommunikationen mellan dem kan gå över Sjunet/Kommunikationstorget med garanterad och övervakad tillgänglighet.

Kostnader

Total kostnad

Kostnaderna för alla de komponenter, beskrivna nedan, som behövs för att sätta upp en miljö för Identitet och behörighet i federation VG har en sammanställning enligt följande. Sammanräkningen utgår ifrån de komponenter som använts i PoC och kan komma att påverkas i de upphandlingar som kommer att krävas om miljön sätts upp för produktion. Kostnaden per part är fördelat jämnt på alla parter och det kommer behöva tas fram en fördelningsnyckel på kostnaden utifrån storleksförhållanden för varje enskild part. Denna fördelning är inte framtagen i analysen och lämnas till implementeringsprojektet. Värt att notera är att det idag redan finns överenskomna fördelningsmetoder för kostnader som skulle kunna återanvändas.

Komponent	Total kostnad (kr)	Kostnad per part (kr)
IdP Curity	1 000 000	20 000
Federation Sambi	3 150 000	63 000
Autentiseringstjänst		
Mobilt BankID	6 500 000	130 000
Freja eID	720 000	14 400
SITHS	0	0
Katalogtjänst		
HSA	0	0
EIDAS	0	0
Förvaltning	3 300 000	66 000
	14 670 000 kr/år	**293 400 kr/år**

IdP Curity

Den IdP projektet har satt upp i PoC kommer från företaget Curity. Kostnaden för denna produkt är på 1 miljon kronor per år för en licens. I detta pris ligger vidareutveckling och support inkluderat. Produkten kan då användas av hela VG och möjliggör även redundans och diversitet. Det är även möjligt att särskilja respektive organisation (multitennant) och ligger i linje med de frågor som drivs mellan Inera, Sambi/eHM och som Inerafederationen inte riktigt tar hänsyn till.

Federation Sambi

Samtliga kommuner och VGR kommer behöva hanteras som enskilda användarorganisationer och enligt prislistan kostar medlemsavgiften för en användarorganisation 50 000 kronor per år, men eftersom denna lösning innebär en organisation i samverkan är det inte troligt att den kostnaden kommer hamna på varje användarorganisation eftersom det finns samordningsvinster med detta upplägg. Till detta har vi kostnaden för tillitsgranskningen som ligger på 40 000 kronor per användarorganisation och den gäller då i tre år.

I samråd med Internetstiftelsen har projektet kommit fram till att vi, som användarorganisation, tillsammans behöver titta på en ersättningsmodell som är mer attraktiv för alla parter och där samverkan inom Västra Götaland kommer förenkla arbetet med tillit, tillitsgranskning och medlemsadministration vilket kommer bidraga till en mer attraktiv ersättningsmodell.

Autentiseringstjänster

Mobilt BankID

Ponera att en person i snitt loggar in 2 gånger per dag. Vi har totalt i lösningen för Millennium, som ett exempel, beräknat någonstans 60 000 användare. Detta ger 3 600 000 inloggningar per månad.

Svensk e-Identitet är en av leverantörerna på marknaden som levererar denna tjänst, men Nordea är den leverantör som har de bästa priserna. Kostnaden för mobilt BankID från Svensk e-Identitet och Nordea är enligt nedan. Det finns ytterligare alternativ, men projektet har utgått ifrån den mest sannolika parten, Svensk eIdentitet, samt den billigaste, Nordea. Kostnaderna som redovisas är inte på något sätt förhandlade, utan kommer utifrån organisationernas standardprislistor.

	Svensk e-Identitet	Nordea
Inloggning	0,21 kr/st	0,15 kr/st
Signering	Inte aktuellt i detta fall	Inte aktuellt i detta fall
Fast månadsavgift	1 500 kr	500 kr
Uppstartskostnad	15 000 kr	1 000 kr

Omräknat med ovanstående beräkning för antal inloggningar innebär detta en kostnad fördelat jämnt på 50 parter (VGR och 49 kommuner) enligt nedan:

Svensk e-Identitet: ungefär 190 000 kronor per år och part

Nordea: ungefär 130 000 kronor per år och part

Freja eID

Freja eID har en kostnadsmodell där man betalar 0,15 kr per transaktion, fast med ett tak på 1 kr/användare och månad. Därefter är det obegränsad användning som gäller. Organisationen som använder sig av Freja eID betalar endast för aktiva användare. Följer vi samma antaganden som för mobilt BankID blir det följande kostnader för Freja eID. Alla priser nedan utgår ifrån Freja eIDs standarprislista och är inte förhandlade priser.

Ponera att en person i snitt loggar in 2 gånger per dag. Vi har totalt i lösningen för Millennium, som ett exempel, beräknat någonstans 60 000 användare. Detta ger 3 600 000 inloggningar per månad.

	Freja eID löpande	Freja eID fast
Inloggning	0,15 kr/transaktion	1 kr/användare och månad
Signering	Inte aktuellt i detta fall	Inte aktuellt i detta fall
Fast månadsavgift	0 kr	0
Uppstartskostnad	0 kr	0

Eftersom 2 inloggningar per dag blir 60 inloggningar per månad multiplicerat med transaktionskostnaden är 9 kr, som är större än 1 kr per användare och månad, utgår vi från att användandet av Freja eID kommer följa det fasta mönstret för Freja eID.

Omräknat med ovanstående beräkning för antal inloggningar innebär detta en kostnad fördelat jämnt på 50 parter (VGR och 49 kommuner) enligt nedan:

Ungefär 14 400 kronor per år och part.

SITHS

Eftersom SITHS redan har en befintlig infrastruktur och organisation i Västra Götaland innebär denna autentiseringsmetod inga nya kostnader eller förändringar på befintlig lösning.

HSA

Kostnaden för anslutning till HSA ligger inte med i omfånget för detta projekt utan är en förutsättning som ställts från FVM. Vi tar därför inte med eventuella kostnader för part inom detta omfång.

EIDAS

Att ansluta sig till EIDAS kostar i dagsläget ingenting. Se bilaga 3.

Förvaltning

Om denna lösning sätt upp för produktion kommer det även behövas en förvaltning av denna lösning. Förvaltningen omfattar följande, men inte uteslutande, områden:

- Avtalsvård
- Leverans- och tjänsteansvar
- Utbildning och stöd
- Konfiguration
- Livscykelhantering
- Teknisk förvaltning

Utifrån lösningens karaktär har projektet uppskattat följande utifrån omfattning och komplexitet;

Förvaltningen antas, utifrån erfarenhet och omfattning, omfatta 2 fulltidsekvivalenter, vilket, beräknat på 1940 timmar per år och en snittkostnad på 850 kr/timme, skulle bli ungefär 3 300 000 kronor per år.

Implementering

Projektet har gjort en uppskattning på omfattning av resursbehov för implementeringsprojektet utifrån erfarenheter i uppsättning PoC i projektet.

Projektet anser att implementeringsprojektet skulle klara av att sätta upp den föreslagna lösningen på 7 månader och att projektgruppen i snitt skulle omfatta 3 personer över tid. Projektet har beräknat bemanningen med en timkostnad på 1000 kronor per timme, för ingående resurser, för att täcka för eventuella konsultinköp. Detta skulle med ovanstående antaganden innebära en budget för implementeringen på 3 360 000 kronor. Exkluderat från denna kostnad är de licens- och avtalskostnader som finns beskrivna ovan för lösningens ingående komponenter. Projektet har under analysen identifierat att det finns stor kompetens hos VGR och kommunerna som skulle kunna användas i en implementering och som genom utnyttjande skulle öka samverkan och delaktighet.

Tester

Uppsättningen av PoC möjliggjorde testning av lösningen på en praktisk nivå och testerna har fallit ut väl. Samtliga anslutna autentiseringsmetoder har kunnat testas och det har varit möjligt att generera SAML-biljetter för samtliga fall där biljetten har kompletterats med användarattribut från HSA. Projektet har dock inte kunnat testa inloggning till SAMSA med hjälp av SAML, eftersom VGR's miljö inte är konfigurerad för inloggning med SAML och den miljö som Cerner har tillgång till inte blivit tillgänglig för projektet. Nedan beskrivs de tester som genomförts på en övergripande nivå. Det har inte heller skett några tester på BankID på kort, då projektet kommit fram till att denna teknik inte skall sättas upp, då den inte är en önskvärd lösning för de ingående organisationerna och den är på väg bort från marknaden.

Test	Testfall	Utfall
Autentisering SITHS	Autentisering med SITHS-kort på dator.	Godkänt
Autentisering Freja	Autentisering med Freja eID på iPad	Godkänt
Autentisering mobilt BankID	Autentisering med mobilt BankID på iPhone	Godkänt

Övriga frågeställningar

Att använda sig av privata e-Identiteter

Frågan kring om Västra Götaland kan använda sig av privata eIdentiteter är utredd med inte på något sätt beslutad. Beslutet måste ske av varje enskild organisation, men projektet har ställt frågan till samtliga kommuner i enkäten som skickades ut och har kommit fram till att merparten av kommunerna anser att den kan användas eller att den implicit kommer användas om tjänsten erbjuds, eftersom det förenklar för användaren. SKL har också tagit fram en sammanställning ”Några frågor om användning Bank-ID på jobbet”, bilaga 4, där SKL kommer fram till att arbetsgivares möjligheter att finna reella alternativ till privat e-legitimation är i vissa fall begränsade, och arbetsgivaren behöver då göra riskbedömningar och överväga olika åtgärder för riskreducering. Utifrån detta kan en bedömning göras för varje verksamhet om det är motiverat att ställa krav på arbetstagaren att använda sitt privata Bank-ID för att lösa de arbetsuppgifter där det krävs säker inloggning. SKLs bedömning är att i verksamheter där inloggning med hög tillitsnivå krävs, ska arbetsgivaren göra en analys utifrån arbetsrättsliga och säkerhetsmässiga aspekter och om identifierade risker inte anses vara för stora och det inte finns något annat alternativ att tillgå är SKLs bedömning att det utifrån ett arbetsrättsligt perspektiv finns möjlighet för arbetsgivare att begära användning av privata digital identitetshandling (e-legitimation). Detta öppnar även upp för en förenkling och ett eget avgörande hos privata vårdgivare som då själva har möjlighet att välja metod.

Certifiering in i en federation

När det gäller certifiering av en användarorganisation i Sambi har vi i samråd med Internetstiftelsen gjort följande antaganden gällande tillitsramverket. De krav tillitsramverket ställer kan fördelas enligt nedanstående tabell, där organisationen för samverkan tar merparten av de krav som ställs. Det är endast de generella kraven och säkerställandet av tillitskedjan som faller på varje inblandad användarorganisation. De övriga kraven som ställs genom tillitsramverket återfinns i bilaga 5.

Krav	Användar-organisation	Samverkans-organisation	Förslag till lösning
A. Generella krav			
Övergripande krav på verksamheten			
A1. Betrodd Part som inte är ett offentligt organ ska drivas som registrerad juridisk person samt teckna och vidmakthålla för verksamheten erforderliga försäkringar.	N/A	N/A	Alla parter i detta samarbete är offentliga organ
A.2 Betrodd Part ska ha en etablerad verksamhet och vara fullt operationell i alla delar som berörs i detta dokument.	Ja	Ja	Uppfylls implicit

Säkerhetsarbete			
A.3 Betrodd Part ska för den Funktion Tillitsdeklarationen avser ha infört ett strukturerat säkerhetsarbete anpassat efter risker och säkerhetsbehov, bestående av: (a) Riskanalys avseende den Funktion som Tillitsdeklarationen avser. Denna ska ta hänsyn till skyddsvärde, befintliga skyddsåtgärder och legala krav. Riskanalysen ska omfatta analys av hot och sårbarheter, samt sannolikhet och konsekvens (skada) på Användare, den egna organisationen, andra Medlemmar och Federationsoperatören. Riskanalysen ska genomföras årligen och leda till en förbättringsplan innehållande rekommenderade säkerhetsåtgärder. (b) Ett ledningssystem för informationssäkerhet (LIS) för Funktionen baserat på ISO/IEC 27001. Säkerhetsåtgärderna ska hantera riskerna enligt riskanalysen för Funktionen. (c) Genomförd internrevision av införandet och efterlevnaden av ledningssystemet för informationssäkerhet (b). Ledningssystemet för informationssäkerhet och efterlevnaden av de krav som ställs i detta Tillitsramverk ska minst en gång per treårsperiod vara föremål för internrevision, utförd av en till Funktionen oberoende kontrollfunktion.	Ja	Ja	Samverkansorganisationen kommer ta fram en modell och en generisk process som kan implementeras i varje användarorganisation. Det pågår redan ett sådant arbete med SITHS i VG som eventuellt skulle kunna gå att återanvända i valda delar.

A.4 Betrodd Part har inrättat en process för incidenthantering i enlighet med de av Federationsoperatören angivna instruktionerna. Se bilaga 6.	Ja	Ja	Samverkansorganisationen kommer ta fram en modell och en generisk process som kan implementeras i varje användarorganisation.
Kryptografisk säkerhet			
A.5 Betrodd Part ska skydda Funktionen mot obehörig åtkomst.	Ja	Ja	Påvisa genom styrande dokumentation att det finns ett skydd för hur vi hanterar installationen av ingående komponenter. Samverkansorganisationen kommer ta ansvar för de gemensamma delarna, men en användarorganisations egna komponenter, om de är inkopplade i tillitskedjan, behöver hanteras.
Ansvar för användning av Underleverantörer			
A.6 Betrodd Part som, i delar eller helhet, lägger ut utförande av Funktionen på Underleverantör är, oavsett avtalsform, ansvarig för Underleverantörens uppfyllande av kraven i Tillitsramverket och ska på begäran informera om vilka delar av Funktionen som är utlagda.	Ja	Ja	Om det finns delar som är utlagda på underleverantörer, skall detta redovisas.

Handlingars bevarande			
A.7 Betrodd Part ska, i tillämpliga delar, bevara: (a) avtal, (b) styrande dokument, (c) handlingar som rör förändringar av uppgifter hänförliga till Användare, Attribut och Metadata, och (d) övrig dokumentation som stöder efterlevnaden av de krav som ställs på denne, och som visar att de säkerhetskritiska processerna och kontrollerna fungerar.	Ja	Ja	Visa på att denna dokumentation lagras på ett strukturerat sätt, t.ex. på en disk med ansvarspersoner.
A.8 Tiden för bevarande ska inte understiga tre år och material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallas från integritetssynpunkt och har stöd i lag eller annan författning.	Ja	Ja	Om A.7 uppfyllt på ett strukturerat sätt, uppfylls även detta krav implicit.
Informationsplikt			
A.9 Betrodd Part ska informera Federationsoperatören vid incidenter, samt vid ändringar av kontaktpersoner och federationsgemensamma metadata.	Ja	Ja	Tas fram i den samverkande organisationen tillsammans med övriga användarorganisationen. Kommer ställa krav på användarorganisationerna att de kan utpeka kontakt- och ansvarspersoner. Det pågår redan ett sådant arbete med SITHS i VG som eventuellt skulle kunna gå att återanvända i valda delar.

I dialog med Internetstiftelsen har projektet kommit fram till att organisationen för samverkan skulle kunna sätta upp ett arbetssätt och organisation tillsammans med Internetstiftelsen som är en blandning mellan Ombud och Gruppföreträdare för att täcka in den stora massan av de krav som ställs på tillitsgranskningen. Projektet har också tillsammans med Internetstiftelsen kommit fram till att det kommer finnas ett krav att varje ingående part behöver ha ett strukturerat informationssäkerhetsarbete. GITS skulle kunna sätta upp en generell modell och struktur som möter upp de tillitskrav som finns och på så sätt tillmötesgå de krav som finns och samtidigt avlasta och

hjälpa de ingående parterna både ur ett kostnads- och arbetsbelastningsperspektiv. Det pågår redan ett sådant arbete med SITHS i VG som eventuellt skulle kunna gå att återanvända i valda delar.

I och med att Internetstiftelsen nu själva är med att förvalta Sambi, finns ett önskemål om att ingående parter i Sambi blir medlemmar i Sambis referensgrupp. På så sätt ges möjlighet att vara med och styra utvecklingen av Sambi.

Bilaga

1. Identitet och behörighet i en federerad lösning
2. SWOT Sammanställning
3. Avtal Sweden Connect sIDAS
4. Sambi Bilaga 3 Tillitsramverk v2.1
5. Några frågor om användning Bank-ID på jobbet
6. Krav på incidentrapportering Sambi
7. Identitet och behörighet i federation enkätsvar kommuner

Ärendets gång

Detta ärende har presenterats för följande grupperingar:

- Projektets interna referensgrupper enligt projektplan
- VGR IT arkitekturledning
- VGR IT ledning
- FVM
- SITIV

Bilaga 6 Krav på incidentrapportering Sambi

Syfte

Här redovisas de rutiner som ska gälla för rapportering av säkerhetsrelaterade händelser, funktionsfel och övriga störningar för medlemmar i deras tjänster relaterade till Sambi. Detta är en första version som kommer att vidareutvecklas. Det pågår redan ett sådant arbete med SITHS i VG som eventuellt skulle kunna gå att återanvända i valda delar genom samverkan.

Definitioner

- Rapporteringspliktig incident: en oönskad och oplanerad händelse som kan påverka användare, medlemmar eller den generella tilltron till Sambi, eller som kan innebära en störning i aktuell medlems förmåga att fullgöra åtaganden enligt regelverket,
- Allvarlig driftstörning: Rapporteringspliktig incident som har påverkan på aktuell medlems förmåga att fullgöra de driftrelaterade åtaganden som följer av regelverket för federationen och som kan innebära en betydande störning för medlem, samt
- Allvarlig säkerhetsincident: Rapporteringspliktig incident med påverkan på säkerhetsskyddet omgärdande hanteringen av tjänster, som kan komma att föranleda omedelbara åtgärder från federationsoperatörens sida.

Kontaktvägar

1. Federationsoperatören ska rapportera till medlemmar.
2. Medlemmar ska rapportera till federationsoperatören.
3. Varje medlem ska:
    a. etablera och upprätthålla kontaktvägar för rapportering till och från federationsoperatören, och
    b. hålla federationsoperatören underrättad om aktuella kontaktvägar och kontaktuppgifter för denna rapportering.
4. Rapportering och återkoppling ska ske med elektroniska medel.

Medlems incidentrapportering

1. Medlem ska utan dröjsmål rapportera allvarliga driftstörningar och allvarliga säkerhetsincidenter.
2. Så länge en rapporterad händelse är pågående ska rapporteringsskyldig medlem hålla rapportmottagare uppdaterad om händelsen.
3. Incidentrapport ska omfatta:
    a. den rapporterande medlemmens namn (rapportör),
    b. kort beskrivande benämning på händelsen (namn),
    c. unik referens för händelsen (referens),
    d. status på händelsen (status),
    e. kategorisering av händelsen (kategorisering),
    f. när händelsen inträffade eller den uppskattade tidpunkten för den (tidpunkt),
    g. när medlemmen upptäckte händelsen (upptäckt),
    h. en översiktlig beskrivning av händelsen (beskrivning), och

   i. bedömning av händelsens omfattning och konsekvenser samt annan information som kan vara av värde för övriga medlemmar (analys). Rapporten ska, såvitt avser struktur och format, utformas enligt federationsoperatörens vid var tid skäligen lämnande instruktioner. Om rapporteringsskyldig medlem inte har fullständiga uppgifter i alla delar för rapporten vid rapporteringsögonblicket kan rapporten kompletteras vid senare tillfälle. I vissa fall kan det vara lämpligt eller nödvändigt att lämna begränsat med information i incidentrapporten. Det kan till exempel gälla om händelsen polisanmäls eller för att inte känslig information ur ett informationssäkerhetsperspektiv ska avslöjas.

4. På begäran av federationsoperatören ska en rapporteringsskyldig medlem komplettera inlämnade uppgifter om en rapporteringspliktig incident med de uppgifter som behövs för att klarlägga hur händelsen kan påverka säkerhetsskyddet omgärdande hanteringen av e-legitimationer.
5. En rapporteringsskyldig medlem, som använder sig av underleverantör för att utföra del av tjänst, ska genom avtal med underleverantören säkerställa att rapporteringspliktiga incidenter kan hanteras och rapporteras på det sätt som framgår av denna bilaga.

Federationsoperatörens återkoppling

Återkoppling ska ges regelbundet och i övrigt när det behövs för säkerhetsskyddet inom federationen.

Sekretess

Incidentrapportering kan innehålla information om implementeringen av säkerhetsåtgärder, hot, risk, sårbarheter, attackvektorer eller annan information som om den blir offentlig kan öppna för säkerhetsrelaterade risker och därmed kan sannolikt orsaka skada för medlemmarna eller federationsoperatören. Därför behöver incidentrapporter sekretessprövning och få lämplig sekretessklass. Även vid utlämnade av information ska en sekretessprövning ske.