Hälso- och sjukvårdsförvaltningen

TJÄNSTEUTLÅTANDE
2013-05-08

HSN 1305-0520

Handläggare:
Carina Landberg

Hälso- och sjukvårdsnämnden
2013-06-18, p 6

De 16 principerna för elektronisk samverkan mellan organisationer

Ärendebeskrivning

De 16 principerna för samverkan utgör en säker grund för samverkan mellan kommuner, landsting, stat och privata utförare för att bygga den tillit som behövs för att möjliggöra säkert informationsutbyte via internet.

IT-forum inom Kommunförbundet Stockholms län (KSL) har under hösten 2012 förnyat och moderniserat de 16 principerna för samverkan från år 2009 för parter inom hälso-, sjukvårds- och omsorgsområdena för beslut i respektive medlemsorganisation.

Beslutsunderlag

Förvaltningens tjänsteutlåtande, 2013-05-08
IT forum, Kommunförbundet Stockholms län, De 16 principerna för samverkan II, 2012-11-30

Ärendets beredning

Ärendet har beretts i Programberedningen för eHälsa och öppna jämförelser.

Förslag till beslut

Hälso- och sjukvårdsnämnden beslutar

att för Stockholms läns landsting anta och arbeta efter de 16 principerna för samverkan II

att i samband med upphandling, utveckling och förvaltning av system och tjänster som ska nyttjas av flera organisatoriska parter ställa krav grundade på de 16 principerna för samverkan II

att årligen redovisa läget inom Stockholms läns landsting till IT-Forum Kommunförbundet Stockholms län enligt bilaga 2 Mål i dokumentet De 16 principerna för samverkan II.

Förvaltningens motivering till förslaget

Bakgrund
Samverkan i form av elektroniskt informationsutbyte mellan myndigheter är en företeelse som i snabb takt ökat i betydelse och kommer att fortsätta öka ytterligare framöver. Under 2009 fick en arbetsgrupp inom IT-forum KSL, bemannad med regionala IT-ledare från Stockholms stad, Lidingö stad, Norrtälje och Österåkers kommuner samt Stockholms läns landsting, uppdraget att utreda hur den nationella IT-strategin för vård och omsorg säkerhetsmässigt bäst kunde realiseras i regionen.

Gruppens arbete resulterade i 16 verksamhetsoberoende principer för elektronisk samverkan, vilka sammantaget utgör grunden för ett säkert och kostnadseffektivt elektroniskt informationsutbyte mellan regionens kommuner, landstinget, staten och privata utförare.

De 16 principerna för elektronisk samverkan presenterades för regionens samtliga kommunala IT chefer/strateger, Stockholms läns landstings IT-ledning samt regionens kommundirektörer som alla ställde sig bakom förslaget. Principerna blev även kommunicerade med Sveriges kommuner och landsting (SKL) och införlivade i det nationella utvecklingsarbete som pågår.

Nuläget
IT-Forum, KSL har under hösten 2012 moderniserat och harmoniserat de 16 principerna med övrigt arbete som pågår i syfte att skapa och behålla allmänhetens förtroende för berörda parters informationshantering. Principerna har förtydligats så att det framgår att de omfattar all informationshantering, oavsett om det är i egen eller annan regi, oavsett om informationen används i stationära eller mobila enheter och oavsett om informationen utbyts mellan användare och tjänst, eller mellan tjänster.

De 16 principerna för elektronisk samverkan tar fasta på informationens rörlighet och har som yttersta mål att i varje tillfälle värna om den personliga integriteten.

Principerna följer SLL informationssäkerhetspolicy som beslutades av landstingsfullmäktige 2013-03-19.

Ekonomiska konsekvenser
Genom att långsiktigt skapa en bättre samordning runt principer mellan kommunerna och landstinget skapas bättre möjligheter att dela

information i befintliga system och landstinget slipper extra kostnader för nyutveckling.

Konsekvenser för patientsäkerhet
Då syftet med principerna är att säkra informationsöverföringen mellan olika huvudmän skapas en bättre möjlighet att dela patientinformation som leder till ett bättre patientomhändertagande.

Konsekvenser för jämställd och jämlik vård
Beslutet medför oförändrade konsekvenser för jämställd och jämlik vård.

Miljökonsekvenser
Beslutet medför oförändrade konsekvenser för miljön.

Catarina Andersson Forsman
Hälso- och sjukvårdsdirektör

Patrik Hansson
Avdelningschef

KSL Kommunförbundet Stockholms Län

IT-forum Stockholms län

De 16 principerna för samverkan II

Karin Bengtsson

2012-11-30

V1.0

Förord

Mot bakgrund av att vi är en starkt digitaliserad nation där information tenderar till att flyta runt i en globaliserad tillvaro, har behovet av att värna om den personliga integriteten aldrig varit större. Oavsett hur informationen lagras, transporteras eller används ska den enskilde aldrig någonsin känna oro för hur informationen hanteras. De 16 principerna för samverkan tar fasta på informationens rörlighet och har som yttersta mål att i varje tillfälle värna om den personliga integriteten.

De 16 principerna för samverkan har sina rötter i ett arbete som gjordes 2009 för att bygga en bas för informationssäkerhet som då behövdes för att möjliggöra säker kommunikation via internet. I arbetet med att ta fram den första generationen av principerna deltog representanter från Stockholms läns landsting, Stockholms stad, Lidingö stad, Norrtälje kommun och Österåkers kommun under ledning av Karin Bengtsson, chef IT-forum, Kommunförbundet Stockholms län.

Under hösten 2012 har principerna moderniserats och harmoniserats med övrigt arbete som pågår i syfte att skapa och behålla allmänhetens förtroende för berörda parters informationshantering. Principerna har förtydligats så att det framgår att de omfattar all informationshantering, oavsett om det är i egen eller annan regi, oavsett om informationen används i stationära eller mobila enheter och oavsett om informationen utbyts mellan användare och tjänst, eller tjänster i mellan.

I arbetet med att modernisera principerna har representanter för Stockholms läns landsting, Praktikertjänst, Stockholms stad, Sollentuna kommun, Sundbybergs stad, Danderyds kommun och Kommunförbundet Stockholms län deltagit. Arbetet har letts av Carina Landberg, programchef Avdelningen E-hälsa och Strategisk IT, Stockholms läns landsting och Karin Bengtsson, chef IT-forum, Kommunförbundet Stockholms län.

De 16 principerna för samverkan ägs och förvaltas av IT-forum, Kommunförbundet Stockholms län, KSL.

Innehållsförteckning

Innehåll

Sammanfattning

De 16 principerna för samverkan utgör en säker grund för samverkan mellan kommuner, landsting, stat och privata utförare för att bygga den tillit som behövs för att möjliggöra säkert informationsutbyte via internet. Principerna inryms i följande fem block.

Informationssäkerhet:

1. *att* ha en antagen informationssäkerhetspolicy, eller motsvarande, med tillhörande styrande dokument
2. *att* ha minst en utsedd person som leder och samordnar informationssäkerhetsarbetet
3. *att* tillämpa en likvärdig metod och jämförbara nivåer för informationsklassning
4. *att* utifrån återkommande riskanalyser och inträffade incidenter vidta nödvändiga åtgärder för att upprätthålla rätt skyddsnivåer

Tillit:

5. *att* tillämpa gemensamma tillitsramverk för att skapa tillit över huvudmannagränser
6. *att* koppla informationstillgångar till relevanta tillitsnivåer

Federering:

7. *att* ha förmågan att utfärda och/eller konsumera elektroniska identitets- och behörighetsintyg
8. *att* säkerställa att alla delar i det elektroniska identitets- och behörighetsintyget följer aktuella tillitsramverk
9. *att* kravställa federativ förmåga i varje tjänst
10. *att* tillämpa gemensamma respektive sektorsrelaterade attribut som används i samverkan

Signering:

11. *att* medverka till teknik- och leverantörsneutrala lösningar för elektroniska underskrifter

Grundläggande infrastruktur:

12. *att* tillse att all gränsöverskridande kommunikation kan ske över internet
13. *att* verka för att kommunikation över öppen infrastruktur signeras och krypteras
14. *att* säkerställa robusthet i för samverkan vitala infrastrukturkomponenter
15. *att* den egna källan för tid är spårbar till den svenska nationella tidsskalan
16. *att* kravställning bör bygga på nationellt framtagna informationsstrukturer

Principerna har sin grund för att möta de högt ställda säkerhetskraven inom vård och omsorg, men det har samtidigt varit av högsta vikt att hitta en bred lösning för att täcka en huvudmans hela behov av lösningar anpassade till informationens skyddsvärde.

Det finns behov av ständiga säkerhetsförbättringar oavsett principerna, men dessa 16 principer säkerställer att alla aktörer agerar på ett likartat, jämförbart och kostnadseffektivt sätt. Principerna leder också till en bredare och smartare användning av redan gjorda investeringar och principerna minskar risken för felinvesteringar och särlösningar.

Det är viktigt att de som berörs av principerna utvecklar sina lösningar på likartat sätt för att elektroniskt informationsutbyte ska kunna ske på så sätt att den personliga integriteten alltid skyddas. Detta oavsett hur information utbyts, hur den lagras eller hur den används.

Den första versionen av de 16 principerna för samverkan är antagna av Stockholmsregionens samtliga kommuner, antingen på politisk nivå eller på tjänstemannanivå. Stockolms läns landsting är i färd att anta principerna.

IT forum kommer årligen att följa upp användningen av principerna.

(#1) *att* ha en antagen informationssäkerhetspolicy, eller motsvarande, med tillhörande styrande dokument

Syfte & nytta

En informationssäkerhetspolicy, eller motsvarande, är ett övergripande dokument som anger mål och inriktning samt ger styrning och uppföljning av informationssäkerhetsarbetet.

Grundelementet i arbetet med informationssäkerhet är ledning och styrning. För att en organisations ledning ska kunna styra informationssäkerhetsarbetet så att det motsvarar de behov som organisationen har, krävs ett ledningssystem för informationssäkerhet (LIS). Ledningssystemet omfattar bland annat policy, styrdokument, olika modeller för exempelvis riskanalys och uppföljning. Syftet med LIS är också att skapa den säkerhetskultur som gör alla medarbetare aktiva i säkerhetsarbetet.

Utmaning

Etablering av ett ledningssystem för informationssäkerhet (LIS) är resurskrävande och det kräver ledningens engagemang.

(#2) *att* ha minst en utsedd person som leder och samordnar informationssäkerhetsarbetet

Syfte & nytta

Informationssäkerhet handlar många gånger mer om samordning än ledning. En eller flera utsedda personer som kan ge kvalificerad strategisk- och operativ rådgivning till ledning och verksamhet ur ett brett informationssäkerhetsperspektiv är en tillgång för organisationen. Det är naturligt att den eller de som är utsedda också utvecklar och upprätthåller regelverk, policys och riktlinjer samt initierar, utför och följer upp revisioner och kontroller.

Utmaning

Små och medelstora organisationer har sällan möjlighet att ha tilldelade resurser som leder och samordnar informationssäkerhetsarbetet utan arbetsuppgiften delas sannolikt med andra arbetsuppgifter. Organisationer som inte har något konkurrensförhållande, exempelvis kommuner, har visat prov på att denna typ av funktion kan delas organisationer i mellan.

(#3) *att* tillämpa en likvärdig metod och jämförbara nivåer för informationsklassning

Syfte & nytta

Syftet med informationsklassning är att ge en informationstillgång en lämplig skyddsnivå i förhållande till omfattning och detaljeringsgrad samt till informationstillgångens värde och de hot som omger den.

En informationsklassad informationstillgång ger bästa tänkbara grund för att bestämma lämpliga skyddsåtgärder för informationstillgången.

Utmaning

Informationsklassning är i ett inledande skede resurskrävande. Resultatet av en informationsklassning kräver att den som har i uppgift att skydda informationen, exempelvis en IT-avdelning eller en driftpartern, har förmågan att anpassa sig till resultatet och att organisationen tydligt uttalat konsekvenserna av en klassning.

(#4) *att* utifrån återkommande riskanalyser och inträffade incidenter vidta nödvändiga åtgärder för att upprätthålla rätt skyddsnivåer

Syfte & nytta

Återkommande riskanalyser ger en bra grund för att säkerställa rätt nivå av skydd. Riskanalyser bör med fördel utföras med stöd av information från omvärldsbevakning, resultat av tidigare riskanalyser, incidentrapportering samt affärsmässiga- och juridiska krav. Alla identifierade hot och sårbarheter bör klassificeras och riskbestämmas. Risker som bedöms som oacceptabla lindras med fördel genom införandet av säkerhetsåtgärder.

Utmaning

Ett införande av rutin för riskanalys och incidenthantering är i ett inledande skede resurskrävande. Det är också av vikt att resultatet från riskanalyserna leder till förbättring. Samma utmaningar omgärdar ett införande av incidenthanteringen.

(#5) *att* tillämpa gemensamma tillitsramverk för att skapa tillit över huvudmannagränser

Syfte & nytta

Ett tillitsramverk kravställer ett antal förmågor, så väl organisatoriska och personella som tekniska och fysiska, i syfte att skapa tillit organisationer i mellan. Ett vanligt scenario är där en part ansvarar för identifiering och behörighetstilldelning, och en annan part tillhandahåller tjänst.

Tillitsramverket förenklar kravställningen i och med att den förlitande parten inte behöver specificera en unik kravbild för varje tjänst utan kan välja en nivå av tillit som står i relation till informationstillgångens skyddsvärde och krav.

Utmaning

Höga krav på tillit ställer direkt höga krav på exempelvis rutiner och efterlevnad vilket kan uppfattas besvärande, inte minst för den som har ett eftersatt informationssäkerhetsarbete.

Oavsett tillämpning av tillitsramverk eller ej kvarstår kravbilden. Till exempel gör Datainspektionen tolkningen av 31 § i personuppgiftslagen (PUL) att åtkomst till en tjänst över öppna nät, såsom Sjunet och internet, som innehåller känsliga personuppgifter, ska föregås av stark autentisering. Vidare följer av 2 kap. 5 § Socialstyrelsens författningssamling (SOSFS 2008:14) bland annat att en vårdgivare som använder öppna nät för att hantera patientuppgifter har ansvar för att det finns rutiner som säkerställer att åtkomst till patientuppgifter föregås av stark autentisering.

(#6) *att* koppla informationstillgångar till relevanta tillitsnivåer

Syfte & nytta

Informationstillgångar som är klassad i enlighet med princip #3 kan under relativt enkla former, kombinerade med invägd risk och med hänsyn till berörd författningsreglering, kopplas till ett krav på lämplig tillitsnivå. En sådan koppling gör varje val av tillitsnivå enkel och konsekvent.

Kopplingen av informationstillången, med invägd risk och med hänsyn till berörd författningsreglering, gör att varje informationstillgång får rätt nivå av skydd. Här är det rimligt att dels se tvingande kontroller på informationen, dels tillämpningskontroller vid användning av informationen.

Utmaning

Denna princip kräver att både princip #3 och princip #4 är införlivade. Det är ett relativt omfattande arbete att införliva , inte minst ur perspektivet att det är inte bara en engångsföreteelse. Det kräver en fungerande och iterativ process för att nå målet.

(#7) *att* ha förmågan att utfärda och/eller konsumera elektroniska identitets- och behörighetsintyg

Syfte & nytta

Inom ett antal branscher och sektorer ses en federativ samverkan som en form av samverkan över huvudmannagränser. För att ingå i en federation krävs att federationens aktuella tillitsramverk följs. I praktiken en översyn av rutiner och processer i identitets- och behörighetshantering. För att ingå i en federation krävs också den tekniska förmågan att utfärda och/eller konsumera elektroniska identitetsintyg. När den federativa förmågan finns är det tämligen enkelt att samverka över huvudmannagränser.

Utmaning

Samverkan över huvudmannagränser innebär så väl organisatoriska och personella som tekniska och fysiska krav vilket kan utgöra ett hinder för samverkan. Detta gäller inte minst för en organisation som har ett eftersatt informationssäkerhetsarbete.

(#8) *att* säkerställa att alla delar i det elektroniska identitets- och behörighetsintyget följer aktuella tillitsramverk

Syfte & nytta

Ett elektroniskt identitets- och behörighetsintyg innehåller ett antal delar som har till uppgift att ge förlitande part ett underlag att ge någon form av tillträde till en informationstillgång. Det elektroniska intyget har stora krav på riktighet och utfärdaren har att se till att identitetsbegrepp, tidsstämpling, signatur och tillitsnivå samt behörighetsstyrande attribut och andra former av attribut är korrekta. Utfärdandet av intyget ska ske i enlighet med det för ändamålet överenskomna tillitsramverket.

Ett enhetligt intyg, utfärdat utifrån överenskommet tillitsramverket, gör det tämligen enkelt att samverka över huvudmannagränser.

Utmaning

Samverkan över huvudmannagränser innebär så väl organisatoriska och personella som tekniska och fysiska krav vilket kan utgöra ett hinder för samverkan. Detta gäller inte minst för en organisation som har ett eftersatt informationssäkerhetsarbete.

(#9) *att* kravställa federativ förmåga i varje tjänst

Syfte & nytta

Med en federativ förmåga i tjänsten blir det tämligen enkelt att samverka över huvudmannagränser utan säkerhetsmässiga avkall.

Varje ny tjänst som har federativ förmåga kan med mindre insatser, i jämförelse med en tjänst som har egna lösningar för identifiering, behörighet etc, införlivas i befintlig arkitektur och infrastruktur. Sett över en livscykel väntas också administrationen av tjänster med federativ förmåga minska. Exempelvis vid administration av behörigheter.

Användarupplevelsen i en federativ lösning gör ingen skillnad på om en tjänst finns i den egna organisationen eller om den återfinns i en annan organisation. Dessutom erhålls single-signon (SSO) till alla tjänster ”på köpet”.

Utmaning

För en leverantör som ännu inte implementerat en federativ förmåga för identifiering, och i förkommande fall behörighet, kan anpassningsarbetet vara betydande. Vid nyutveckling av en tjänst är det omvänt en besparing att inte behöva bygga in funktioner för olika former av identifiering, behörighetshantering etc.

(#10) *att* tillämpa gemensamma respektive sektorsrelaterade attribut som används i samverkan

Syfte & nytta

Tjänster med federativ förmåga där attribut används för behörighetstyrning etc. kan medföra omfattande flora av attribut i den egna organisationens källa för attribut (exempelvis en katalog likt AD, eDirectory, HSA eller OpenLDAP). Varje insats att ensa i attributsfloran ger betydande vinster i form av administration och säkerhet.

Utmaning

Det kan vara ett omfattande arbete att i dialog med varje leverantör av tjänst tillhandahålla de attribut som efterfrågas. Inte minst attribut som inte kan anses vara gängse för den aktuella tjänsten.

(#11) *att* medverka till teknik- och leverantörsneutrala lösningar för elektroniska underskrifter

Syfte & nytta

Det är mer regel än undantag att varje lösning för elektroniska underskrifter är hårt knutna till inlåsta/ägda lösningar, ofta levererade av ett fåtal dominerande företag. I princip är det omöjligt att ersätta en konkurrerande lösning mot en annan då varje tjänst är tajt utvecklad mot en särlösning.

En valfrihet med avseende på lösningar för elektroniska underskrifter som innebär konkurrensneutralitet är eftersträvansvärd för att minska beroende till en enskild leverantör.

Utmaning

Det är svårt att som enskild organisation påverka förändringar i redan etablerade lösningar, varför det är att anse som en långsiktig strävan att medverka till konkurrensneutrala lösningar.

(#12) *att* tillse att all gränsöverskridande kommunikation kan ske över internet

Syfte & nytta

Syftet är att inom ramen för samverkan undvika parallell infrastruktur och istället koncentrera all samverkan till internet. Koncentrationen innebär minskad exponeringen och därigenom tydliggörs riskerna vilket leder till ett förenklat säkerhetsarbete.

Internet har historiskt inte ansetts tillräckligt tillförlitlig för att ligga till grund för samverkan över huvudmannagränser varför parallella infrastrukturer etablerats. I dag är internet i de allra flesta fallen minst lika tillförlitligt som all annan infrastruktur. Oavsett form av samverkan är internet därför det självklara valet för gränsöverskridande kommunikation.

Utmaning

Det är svårt att som enskild organisation påverka förändringar i redan etablerade lösningar varför det är att anse som en långsiktig strävan att avveckla parallell infrastruktur som inte tillför någon egentlig nytta. Det är också en utmaning att tillföra tillräckligt med kontroller för de exponeringar som görs för att garantera tillit till den egna infrastrukturen.

(#13) *att* verka för att kommunikation över öppen infrastruktur signeras och krypteras

Syfte & nytta

Syftet är att en användare av en tjänst ska få en bekräftelse på användaren faktiskt kommunicerar med rätt sajt. Syftet är också att värna om användarens integritet och i förekommande fall andras integritet när de förekommer i kommunikationsutbytet.

Utmaning

Den enda egentliga utmaningen är att se till att varje tjänst (läs applikation, tillämpning eller system) signerar och krypterar sin kommunikation. Vanligtvis sker detta med redan inbyggda funktioner för exempelvis SSL/TLS.

(#14) *att* säkerställa robusthet i för samverkan vitala infrastrukturkomponenter

Syfte & nytta

I takt med att verksamheterna blir alltmer beroende av internet minskar toleransen för avbrott och andra störningar. Kraven på internetinfrastrukturen ökar ständigt och därmed behovet av robusta infrastrukturkomponenter såsom internetredundans, internetprotokoll (IPv4/IPv6), routing, brandväggar, intrångsdetektering (IDS/IPS), trafikfiltrering, viruskontroller, spamfiltrering, loggfunktioner, redundans, tunnlingsteknik, överbelastningsskydd och domännamnsservrar (DNS/DNSSEC).

Åtgärder kan vara allt från fysiskt redundanta förbindelser och reserv-elverk till informationssystem för driftstörningar och informationssystem för att reducera antalet avgrävningar.

Utmaning

Robusta lösningar är tyvärr ofta också komplexa lösningar. Komplexiteten leder till ökad risk för att något blir fel och därmed bidrar till försämrad tillgänglighet. Detta måste nogsamt vägas in, på samma sätt som de ekonomiska aspekterna, när förbättringsåtgärder vidtas. Alla förbättringsåtgärder är inte förbättringsåtgärder.

(#15) *att* den egna källan för tid är spårbar till den svenska nationella tidsskalan

Syfte & nytta

Tid är den enskilt viktigaste källan för att skapa spårbarhet. Trots detta är just spårbar tid ett eftersatt område i flera organisationen. I allt fler lösningar är tid avgörande för att upprätthålla de säkerhetsmässiga kraven. I en federativ samverkan över huvudmannagränser är det ett absolut krav.

Utmaning

Den enda egentliga utmaningen för att skapa en spårbar tidskälla är just tid för införande.

(#16) *att* kravställning bör bygga på nationellt framtagna informationsstrukturer

Syfte & nytta

Syftet med att strukturera och standardisera information är att stödja en effektiv informationsförsörjning och underlätta informationsöverföring mellan olika aktörer. Detta behöver göras utifrån:

- Verksamhetsprocesser.
- Vad olika intressenter behöver kommunicera.
- Vilken typ av information de behöver i kommunikationen.

Information som är ändamålsenlig, enhetligt beskriven, strukturerad och med bibehållen mening blir återsökbar. Informationen kan då användas för att skapa sammanhållen information, förenkla informationssäkerhetsarbete, möjliggöra kunskapsstyrning och utveckling av beslutstöd, för uppföljning, jämförelse och som underlag för kvalitet och verksamhetsstyrning

Utmaning

För ett enskilt projekt kan arbetet med kravställning utifrån generella modeller och standardiserade informationsstrukturer vara resurskrävande. Det gäller att beställare/kravställare och utförare/utvecklare har en gemensam bild av verksamhetsområdet och möjligheterna att samverka mellan olika aktörer.

Ordlista

Biljett: Se Intyg

Intyg: Uppgifter om en användares identitet och/eller attribut i elektronisk form.
Engelska: Assertion

Tillitsnivå: Grad av tillit till en identitet som kan tillmätas enligt ett givet tillitsramverk.
Engelska: Levels of assurance, LoA

Tillitsramverk: Ett ramverk som behandlar tillit till utfärdade intyg
Engelska: Trust Framework

Tjänst: I detta dokument synonymt med applikation, e-tjänst, tillämpning och system.

Bilaga 1 – Måluppfyllnad

IT-forum, KSL, har i uppgift att följa upp hur principerna införlivas och tillämpas. Det görs genom en enklare enkätundersökning i september varje år där alla organisationer som antagit principerna gör en självskattning per princip. Självskattningen görs enligt följande:

- Principen tillämpas helt
    - Det innebär att principen är en införlivad del i organisationens ramverk, processer eller motsvarande.
- Principen tillämpas delvis
    - Det innebär att principen används från fall till annat där organisationen finner lämpligt, men principen är inte en införlivad del i organisationens ramverk, processer eller motsvarande. Fortsatt arbete krävs för att principen skall införlivas helt.
- Arbete påbörjat för att tillämpa principen
    - Det innebär att organisationen ännu inte tillämpar den, men har för avsikt att tillämpa den och införliva den i organisationens ramverk, processer eller motsvarande.
- Ej tillämpningsbar princip
    - Det innebär att organisationen inte kan tillämpa principen.
- Vet ej

Självskattning är till stort värde vid förvaltningen av principerna och IT-forum, KSL, får därigenom en uppfattning vilka principer som tillämpas helt eller delvis och vilka principer som inte tillämpas. Vidare ger självskattningen en indikation inom vilka eventuella områden där IT-forum, KSL, kan göra punktinsatser, exempelvis i form av workshops.

I det längre perspektivet ger självskattningen också en indikation på vilka principer som behöver omarbetas, vilka principer som medger att positionera flyttas fram etc.

Bilaga 2 – Mål

(#1) *att* ha en antagen informationssäkerhetspolicy, eller motsvarande, med tillhörande styrande dokument

- För att uppnå målet med denna princip **ska** den egna organisationen implementerat en informationssäkerhetspolicy, eller motsvarande.

(#2) *att* ha minst en utsedd person som leder och samordnar informationssäkerhetsarbetet

- För att uppnå målet med denna princip **ska** organisationen ha minst en utsedd person som leder och samordnar informationssäkerhetsarbetet

(#3) *att* tillämpa en likvärdig metod och jämförbara nivåer för informationsklassning

- För att uppnå målet med denna princip **ska** den egna organisationen klassificera sina informationstillgångar med utgångspunkt i säkerhetsaspekterna konfidentialitet, riktighet, tillgänglighet och spårbarhet.
- Klassificeringen **bör** genomföras likvärdigt eller jämförbart med Myndigheten för samhällsskydd och beredskaps (MSB) och Swedish Standards Institute (SIS) metod för informationsklassning.

(#4) *att* utifrån återkommande riskanalyser och inträffade incidenter vidta nödvändiga åtgärder för att upprätthålla rätt skyddsnivåer

- För att uppnå målet med denna princip **ska** den egna organisationen återkommande genomföra riskanalyser och med utgångspunkt från detta också vidta säkerhetsåtgärder.

(#5) *att* tillämpa gemensamma tillitsramverk för att skapa tillit över huvudmannagränser

- För att uppnå målet med denna princip **ska** den egna organisationen leva upp till de aktuella kraven för en viss tillitsnivå i ett för ändamålet utpekat tillitsramverk.

(#6) *att* koppla informationstillgångar till relevanta tillitsnivåer

- För att uppnå målet med denna princip **ska** den egna organisationen ange relevanta tillitsnivåer för de informationstillgångar som ska tillgängliggöras.

(#7) *att* ha förmågan att utfärda och/eller konsumera elektroniska identitets- och behörighetsintyg

- För att uppnå målet med denna princip **ska** den egna organisationen uppfylla de normativa kraven för att ingå i en federation, i förekommande fall genom kravställning vid upphandling.

(#8) *att* säkerställa att alla delar i det elektroniska identitets- och behörighetsintyget följer aktuella tillitsramverk

- För att uppnå målet med denna princip **ska** den egna organisationen följa det för ändamålet överenskomna tillitsramverket vid samverkan över huvudmannagränser.

(#9) *att* kravställa federativ förmåga i varje tjänst

- För att uppnå målet med denna princip **ska** den egna organisationen kravställa federativ förmåga enligt de normativa kraven för varje ny tjänst som upphandlas.

(#10) *att* tillämpa gemensamma respektive sektorsrelaterade attribut som används i samverkan

- För att uppnå målet med denna princip **bör** enbart attribut som finns med i de normativa förteckningarna användas, exempelvis genom kravställning vid upphandling.
- I fall där attribut saknas **bör** den egna organisationen medverka till att aktuell attributsförteckning ändras för att leva upp till det identifierade behovet.

(#11) *att* medverka till teknik- och leverantörsneutrala lösningar för elektroniska underskrifter

- För att uppnå målet med denna princip **ska** den egna organisationen sträva mot att endast införa och använda öppna standards för elektroniska underskrifter, exempelvis genom kravställning vid upphandling.

(#12) *att* tillse att all gränsöverskridande kommunikation kan ske över internet

- För att uppnå målet med denna princip **ska** den egna organisationen, i varje fall den finner lämpligt, kravställa att all kommunikation kan ske över internet.
- För att uppnå målet med denna princip **ska** den egna organisationen vara mycket restriktiv till att ansluta sig till annan extern infrastruktur än internet.

(#13) *att* verka för att kommunikation över öppen infrastruktur signeras och krypteras

- För att uppnå målet med denna princip **ska** den egna organisationen, i varje fall den finner lämpligt, tillse att kommunikation över öppen infrastruktur, som internet och Sjunet, signeras och krypteras.

(#14) *att* säkerställa robusthet i för samverkan vitala infrastrukturkomponenter

- För att uppnå målet med denna princip **ska** den egna organisationen, i varje fall den finner lämpligt, upphandla robusta lösningar. Upphandlingar har i detta avseende visat sig vara ett effektivt medel för att nå förbättringsresultat i en konkurrensutsatt marknad.

(#15) *att* den egna källan för tid är spårbar till den svenska nationella tidsskalan

- För att uppnå målet med denna princip **ska** källan för tid i den egna organisationen vara spårbar till den svenska nationella tidsskalan.
- De egna systemen **bör** synkronisera mot minst tre interna tidskällor, som i sin tur synkroniserar mot direkt spårbara tidskällor. Tre källor ger möjlighet att upptäcka om någon av dem är en så kallad ”falseticker”.

(#16) *att* kravställning bör bygga på nationellt framtagna informationsstrukturer

- För att uppnå målet med denna princip **ska** den egna organisationen arbeta utifrån nationellt framtagna informationsstrukturer vid kravställning och upphandling

Bilaga 3 – Normativa specifikationer

(#1) *att* ha en antagen informationssäkerhetspolicy, eller motsvarande, med tillhörande styrande dokument

- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet MSBFS 2009:10
- Ledningssystem för informationssäkerhet SS-ISO/IEC 27001: 2006
- Riktlinjer för styrning av informationssäkerhet SS-ISO/IEC 27002:2005

(#2) *att* ha minst en utsedd person som leder och samordnar informationssäkerhetsarbetet

- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet MSBFS 2009:10
- Ledningssystem för informationssäkerhet SS-ISO/IEC 27001: 2006
- Riktlinjer för styrning av informationssäkerhet SS-ISO/IEC 27002:2005

(#3) *att* tillämpa en likvärdig metod och jämförbara nivåer för informationsklassning

- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet MSBFS 2009:10
- Ledningssystem för informationssäkerhet SS-ISO/IEC 27001: 2006
- Riktlinjer för styrning av informationssäkerhet SS-ISO/IEC 27002:2005

(#4) *att* utifrån återkommande riskanalyser och inträffade incidenter vidta nödvändiga åtgärder för att upprätthålla rätt skyddsnivåer

- Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet MSBFS 2009:10
- Ledningssystem för informationssäkerhet SS-ISO/IEC 27001: 2006
- Riktlinjer för styrning av informationssäkerhet SS-ISO/IEC 27002:2005
- Riskhantering för informationssäkerhet SS-ISO/IEC 27005:2008, IDT

(#5) *att* tillämpa gemensamma tillitsramverk för att skapa tillit över huvudmannagränser

- I första hand eLegitimationsnämndens tillitsramverk
- I andra hand Sambis (samverkan för säkrare e-hälsa) tillitsramverk, eller
- Skolfederationens tillitsramverk

(#6) *att* koppla informationstillgångar till relevanta tillitsnivåer

- Information technology – Security techniques – Entity authentication assurance framework ISO/IEC 29115
- Kantara Initiative – Identity Assurance Framework, IAF
- Office of Management and Budget, OMB – Memorandum 04-04

(#7) *att* ha förmågan att utfärda och/eller konsumera elektroniska identitets- och behörighetsintyg

- I första hand eLegitimationsnämndens tillitsramverk
- I andra hand Sambis (samverkan för säkrare e-hälsa) tillitsramverk, eller
- Skolfederationens tillitsramverk
- SAML implementationsprofilen eGov2
- SAML deploymentprofilen saml2int

(#8) *att* säkerställa att alla delar i det elektroniska identitets- och behörighetsintyget följer aktuella tillitsramverk

- I första hand eLegitimationsnämndens tillitsramverk
- I andra hand Sambis (samverkan för säkrare e-hälsa) tillitsramverk, eller
- Skolfederationens tillitsramverk

(#9) *att* kravställa federativ förmåga i varje tjänst

- SAML implementationsprofilen eGov2
- SAML deploymentprofilen saml2int

(#10) *att* tillämpa gemensamma respektive sektorsrelaterade attribut som används i samverkan

- I första hand eLegitimationsnämndens tillitsramverk
- I andra hand Sambis (samverkan för säkrare e-hälsa) tillitsramverk, eller
- Skolfederationens tillitsramverk

(#11) *att* medverka till teknik- och leverantörsneutrala lösningar för elektroniska underskrifter

- OASIS Digital Signature Services (DSS)
- PKCS #7 – Cryptographic Message Syntax Standard
- XMLdSig – W3C recommendation XML Signature Syntax and Processing

(#13) *att* verka för att kommunikation över öppen infrastruktur signeras och krypteras

- För nästintill varje standardprotokoll finns tillägg för SSL/TLS. Se resp RFC.

(#15) *att* den egna källan för tid är spårbar till den svenska nationella tidsskalan

- Tidskällan ska vara spårbar till den svenska nationella tidsskalan UTC(SP).
- Network Time Protocol RFC5905-RFC5908