

2010-04-08

För kännedom:
Kommundirektörer
IT-chefer/-strateger

Kommunstyrelsen

Rekommendation att anta 16 principer för samverkan inom IT-forum

Kommunerna måste för att kunna utveckla den elektroniska kommunikationen mellan **regionens kommuner, landsting, stat och privata anordnare** enas om hur säkerheten ska lösas. **Varje kommun behöver ha grundförutsättningarna klara för att bygga den struktur som krävs för att möjliggöra säker kommunikation via internet.** Grundförutsättningarna finns i de 16 principer för samverkan som tagits fram inom IT forum.

Vid arbetet har hänsyn tagits till e-delegationens arbete och de regionala förutsättningar som finns. Kommunerna i Stockholms län värnar om nätneutralitet, autentiseringsneutralitet och federationsneutralitet. Detta betyder i praktiken att vi via de 16 principerna värnar om såväl säkerhet som kostnadseffektivitet när vi skapar förutsättningar för elektroniskt informationsutbyte mellan regionens kommuner, landsting, stat och privata utförare.

Regionens samtliga kommunala IT-chefer, kommundirektörer och Stockholms läns landstings IT-ledning har ställt sig bakom förslaget. Principerna är även kommunicerade med Sveriges Kommuner och Landsting och införlivade i det nationella utvecklingsarbete som pågår.

KSLs styrelse beslutade på sitt sammanträde den 8 april 2010 att rekommendera kommunerna att anta de 16 principerna för samverkan.

Bilaga

IT-forum - 16 principer för samverkan

2010-04-08

Dnr: 2010/0016

KSL är tacksamma för att få kommunernas ställningstagande via post eller e-post till info@ksl.se före utgången av juni 2010.

Har ni frågor kontakta Karin Bengtsson, IT-forum, karin.bengtsson@ksl.se, tel 08 – 615 94 11.

Med vänlig hälsning

KOMMUNFÖRBUNDET STOCKHOLMS LÄN

Erik Langby
Ordförande

Lennart Dahlberg
Direktör

IT-FORUM STOCKHOLMS LÄN

Lennart Jonasson
Ordförande

De 16 principerna för samverkan

Syftet med de styrande principerna

Kommunerna i Stockholms län värnar om nätneutralitet, autentiseringsneutralitet och federationsneutralitet. Syftet med principerna är att underlätta gränsöverskridande samverkan utan att för den skull göra några säkerhetsmässiga avkall.

Bakgrund

En teknisk arbetsgrupp utsågs av KSL/IT-forum vars uppdrag var att ta fram ett beslutsunderlag till IT-Forums ägargrupp hur den nationella IT strategin för vård och omsorg säkerhetsmässigt bäst realiserar i Stockholmsregionen.

Inom ramen för arbetsgruppens arbete identifierades i oktober 2009 ett antal problemområden, tillika viktiga byggstenar för samverkan för kommunens samtliga verksamheter:

- Informationsklassning
- Autentisering
- Katalogsamverkan
- Identitetsfederering
- Signering
- Kryptering
- Åtkomst
- Spårbarhet
- Transport

Arbetsgruppen har inom ramen för dessa problemområden lyft fram och prioriterat ett antal viktiga vägval som flertalet berörda kommuner står inför och som rätt hanterat kan underlätta samverkan med landsting, utförare och givetvis kommuner i mellan. Vidare har arbetsgruppen identifierat ett antal vägval, grundförutsättningar, som kan anses självklara och ofta tas för givet men som inte får glömmas bort och därför här har dokumenterats.

Arbetsgruppens förslag till viktiga vägval presenterades i mitten av november 2009 för regionens kommuner i form av CIO, IT-strateg eller IT-chef där vägvalen sedermera i samstämmighet omvandlades till 16 styrande principer för samverkan.

2010-02-10

De 16 principerna för samverkan

#1 att utgå från SLLs & Stockholms stads metod för informationsklassning och paketera den på ett sådant sätt att den är lättillgänglig och att omvärldskraven tydligt dokumenteras

#2 att utgå från SLLs & Stockholms stads definition av faktorer och nivåer för informationsklassning och anpassa detta till att spegla en lägsta nivå för kommunen

#3 att likt Stockholms stad inkludera även spårbarhet som en faktor för informationsklassning

Syftet med princip #1, #2 och #3 är att alla inblandade parter skall ha samma syn hur information skall skyddas, i vilken grad och i förekommande fall på vilket sätt. Råder det inte samsyn kring informationsklassning försvåras ett samarbete avsevärt. Om en part identifierar berörd information som mindre skyddsvärd kan denna utgöra en stor risk för den part som gjort en annan bedömning av informationens skyddsvärde.

#4 att likställa stark autentisering med 2-faktors autentisering

Syftet med princip #4 är att säkerställa att ingen part använder otillräcklig autentisering i sammanhang där stark autentisering krävs. Syftet är också att tydliggöra att stark autentisering förutsätter två olika faktorer. Exempelvis något du vet, som ingen annan vet, och något du har, som ingen annan har.

#5 att vid samverkan acceptera följande metoder för stark autentisering; eID, PKI med lagring av nyckelpar på SmartCard eller motsvarande och metoder baserade på engångslösenord, antingen genererade i en fysisk enhet eller säkert distribuerad till fysisk enhet

Syftet med princip #5 är att inom ramen för samverkan tydliggöra vilka metoder som är accepterade för stark autentisering. Detta innebär inte att metoderna ovan likställs utan de krav som ska gälla bestäms i exempelvis policydokumentet för en identitetsfederation där förtroendenivåer baserat på metod av autentisering definieras.

#6 att tillämpa en gemensam certifikat- och utfärdarpolicy, likvärdig med SITHS, som ett minimikrav för egen eller annans PKI

Syftet med princip #6 är att inom ramen för samverkan säkerställa att samtliga berörda PKI'er inte avviker från minimikraven och därmed inte riskera att en autentisering är otillräcklig.

2010-02-10

#7 att sträva mot en autentiseringslösning, framför flera olika, för att realisera stark autentisering i den egna organisationen samt i förekommande fall samordna detta med lösningar för inpassering, lås, flex med flera

Syftet med princip #7 är att undvika att den enskilda organisationen ställs inför de problem som lösningar med flera olika likartade autentiseringslösningar kan medföra.

#8 att enbart acceptera SAMLv2, eller senare, vid identitetsfederering samt tydliggöra att det i förekommande fall är det enda sättet att logga in och säkerställa det inte finns någon bakväg in

Syftet med princip #8 är att inom ramen för samverkan tydliggöra vilka metoder för identitetsfederationer som förespråkas.

#9 att kravställa att varje ny webbaserad tillämpning som kräver autentisering bör ha stöd för SAML och där stark autentisering är nödvändig kräva stöd för SAML

#10 att utfärda SAML-biljetter och konsumera SAML-biljetter i webbaserade tillämpningar som kräver autentisering och har ett samverkansintresse

Syftet med princip #9 och #10 är att inom ramen för samverkan möjliggöra användning av den egna autentiseringslösningen förutsatt att den är tillräcklig.

#11 att tillämpa ett gemensamt regelverk för att ingå i en federation vilket även skall omfatta alternativ som exempelvis bryggade PKI'er

Syftet med princip #11 är att inom ramen för samverkan säkerställa att varje ingående IdP (identity provider) inte avviker från minimikraven och därmed inte riskera att en autentisering är otillräcklig. Syftet är också att inte låta begränsningarna i SAML verka begränsande för ett samarbete.

#12 att tillämpa en gemensam katalogpolicy, med utgångspunkt från HSA policy, som ett minimikrav för egna kataloger

Syftet med princip #12 är att förenkla katalogsamverkan och informationsutbyten

#13 att se över det egentliga behovet av faktisk PKI signering

Syftet med princip #13 är att inom ramen för samverkan hitta lösningar för signering som lever upp till verksamhetens krav och som samtidigt kan anpassas till de tekniska och juridiska begränsningar som en identitetsfederering medför.

#14 att ställa krav på berörda tillverkare att samverka för ett gemensamt gränssnitt mot dess signeringsfunktioner

Syftet med princip #14 är att möjliggöra en större rörlighet kring signeringsfunktioner som annars är mer eller mindre låsta till den produkt som är vald för ändamålet.

2010-02-10

#15 att sträva mot att all gränsöverskridande kommunikation skall ske över internet

#16 att möjliggöra kontroll av trafik till och från den egna infrastrukturen i en eller få kontrollpunkter

Syftet med princip #15 och #16 är att inom ramen för samverkan undvika parallell infrastruktur och istället koncentrera all samverkan till Internet och där tillse att anslutningen har erforderliga skydd.

Inleveranser från IT-forum

Flertalet principer införlivas enklast i regelverk för informationssäkerhet och där företrädesvis i dess riktlinjer. Några principer kräver nya former av policydokument som nödvändigtvis inte skall betraktas som en policy på samma nivå som exempelvis en informationssäkerhetspolicy. För att undvika missförstånd behålls därför ”defacto-namnen” på dessa dokument.

IT-forum, Kommunförbundet i Stockholms län, bidrar med följande inleveranser för att förenkla införandet av de 16 principerna för samverkan:

- Brödtext till riktlinje för informationsklassning, eller motsvarande, för att införliva princip #1, #2 och #3.
- Brödtext till riktlinje för åtkomst till information, eller motsvarande, för att införliva princip nr #3, #4, #5, #6, #7, #11.
- Certifikat policy (CP) och utfärdardeklaration (CPS), för att införliva princip nr #6.
- Anvisning/instruktion för identitetsfederering, eller motsvarande, för att införliva princip #8, #9, #10 och #11.
- Brödtext till riktlinje för systemutveckling/-anskaffning, eller motsvarande, för att införliva princip #9 och #15.
- Federationspolicy, för att införliva princip #11.
- Katalogpolicy, för att införliva princip #12
- Brödtext till riktlinje för kommunikations- och nätverksäkerhet, eller motsvarande, för att införliva princip #15 och #16.

De principer som rör signering, nr 13 och 14, innebär i nuläget inget ytterligare arbete från den enskilda organisationens sida utan här kan man vänta in KSL/IT-forums arbete och senare se vilken eventuell påverkan detta får. Mest sannolikt en anvisning/instruktion för *signering*.

2010-02-10

Egna ställningstaganden

Varje enskild organisation måste ta ställning hur stark autentisering skall realiseraras.

Princip #5 lyfter fram eID, PKI med lagring av nyckelpar på SmartCard eller motsvarande och metoder baserade på engångslösenord, antingen genererade i en fysisk enhet eller säkert distribuerad till fysisk enhet. Observera att dessa inte skall likställas, exempelvis policydokumentet för en identitetsfederation ska istället beskriva olika förtroendenivåer baserat på metod av autentisering.

Den eller de metoder som den enskilda kommunen väljer för att realisera stark autentisering kan ha påverkan på formuleringar i det egna regelverket för informationssäkerhet. Det kommer också ha påverkan på vilka övriga policydokument som är av vikt för den enskilda kommunen.

Grundförutsättningar

De 16 principerna för samverkan har arbetats fram med förutsättning:

att varje organisation har en riktlinje, instruktion eller motsvarande som beskriver hur krypteringsnycklar skall lagras, utbytas, förnyas etc

att varje organisation har en riktlinje, instruktion eller motsvarande som beskriver vilka krypteringsalgoritmer och nyckellängder som förordas

att alla datorers tid skall vara direkt spårbar till UTC(SP)* förslagsvis med en egen källa som är direktspårbar till UTC(SP)

**) UTC=Coordinated Universal Time, SP= Sveriges Tekniska Forskningsinstitut*