KSL Kommunförbundet Stockholms Län

2010-05-27

IT-forum Stockholms län

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 säkerhetsmässigt bäst realiseras 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.

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.

#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 indentitetsfederationer 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 begräsningarna 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.

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

#16 att möjliggöra kontroll av trafik till och från den egna infrastukturen 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.

Nyttan

De 16 principerna för samverkan förväntas till gemensamma säkerhetslösningar som kan användas i så väl den egna organisationen som över huvudmannagränser.

- Bättre harmonisering med gällande lagar och förordningar där inte minst skyddet av den personliga integriteten idag är eftersatt
- Förenklad samverkan där ständiga krav på effektivisering förutsätter samverkan i en mängd olika former
- Hög interopatibilitet där gemensamma miniminivåer och standards förordas framför specifika tillverkare och produkter vilket leder till ökad konkurrens och det i sin tur kostnadsminskningar
- Kostnadseffektivitet i form av färre tekniska lösningar som löser samma uppgift på likartat sätt
- Förenklat införande av ny tjänster, oavsett om de är i egen eller annans regi, där höga krav på säkerhet kan kombineras med användarvänlighet

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

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:

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

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*.

Nedan mappas varje princip till en inleveranser från IT-forum

Princip	**Inleverans från IT-forum**
#1, #2, #3	Riktlinje för informationsklassning
#4, #5, #6, #7, #8, #9, #10, #11	Federationspolicy
#6	Certeifikat- och utfärdarpolicy
#9, #15	Tillägg till riktlinje för systemutveckling/-anskaffning
#12	Katalogpolicy
#15, #16	Tillägg till riktlinje för kommunikations- och nätverksäkerhet (brödtext)

Egna ställningstaganden

Varje enskild organisation måste ta ställning hur stark autentisering skall realiseras. Det bör poängteras att det är inte *De 16 principerna för samverkan* som kravställer stark autentisering utan det är lagkrav, förordningar etc som kravställer stark autentisering vid hantering av information som har ett högt skyddsvärde.

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.

Nuläget vad gäller möjlighet till stark autentisering varierar stort i länets kommuner, från fullt utbyggda lösningar till totalt avsaknad. De kommuner som är längst från målet kan räkna med kostnader för hårdvara/mjukvara på upp till ~1.000 SEK/användare. Arbetskostnader av engångskaraktär och rutinkaraktär tillkommer. Den senare är för de allra flesta en redan existerande kostnad som inryms inom identitetshantering.

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.

Checklista

Följande aktiviteter bör vidtas för att införliva *De 16 principerna för samverkan*:

- Ersätt eller komplettera redan existerande riktlinje för informationsklassning med den av IT-forum inlevererade riktlinjen. Om informationssäkerhetspolicyn innehåller detaljer om informationsklassning skall spårbarhet adderas till denna. Se riktlinje för informationsklassning för detaljer.

- Komplettera redan existerande riktlinje för systemutveckling/-anskaffning med den av IT-forum inlevererade riktlinjen.

- Komplettera redan existerande riktlinje för kommunikations- och nätverksäkerhet med den av IT-forum inlevererade riktlinjen.

- Anta de av IT-foum inlevererade federationspolicy, certifikat- och utfärdarpolicy, samt katalogpolicy.

- Realisera en lösning för stark autentisering i enlighet med *De 16 principerna för samverkan* för de sammanhang där krav ställs på den samma.

Revisionshistorik

Rev 1 - Första utkast till arkitekruledningsgruppen inom KSL
Rev 2 - Arbetsmaterial för arkitekruledningsgruppen inom KSL
Rev 3 - Slutreviderat och publicerat material
Rev 4 - Arbetsmaterial för arkitekruledningsgruppen inom KSL med tillägg rörande effekter, kostnader samt checklista.