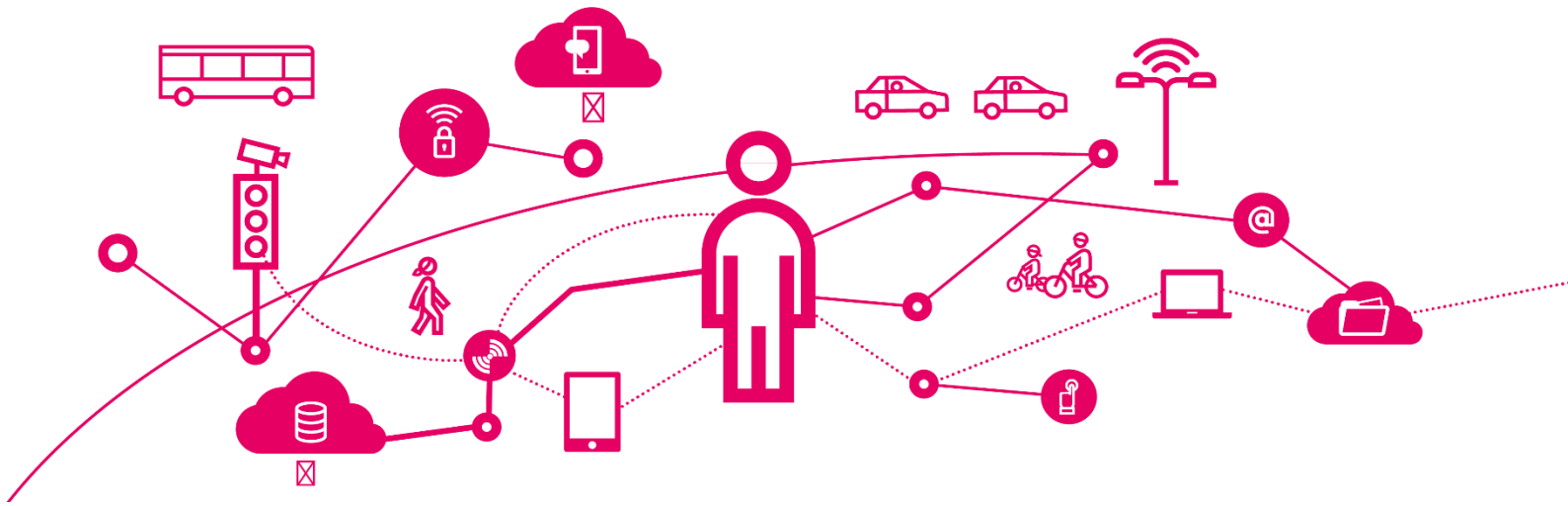
Stockholms stad

Projekt IoT Stockholm

Vägledande dokument:
Anvisning datakommunikation IoT för Stockholms stad



Projekt: IoT Stockholm
Kontaktperson: Maria Holm
Version: 1.0

Innehåll

Revisionshistorik

Version	Datum	Författare	Kommentar
1.0	2020-12-09	Carl Wahlin, Tomas Wiiand, Tommy Lundblad, Stefan Melander	Slutversion från projektet Tekniska förutsättningar inom programmet Stockholm som Smart och uppkopplad stad

1 Läsinstruktion (introduktion)

Detta dokument är en anvisning som Stockholms stads verksamheter ska använda vid:

- Införandet av nya IoT-lösningar
- Uppdatering och/eller förändringar av befintliga IoT-lösningar

Dokument kan med fördel också användas i tidigt skede inför eventuella kommande införanden (skiss- och planering), inför upphandling av IoT-utrustning, samt vid genomlysning av befintliga IoT-lösningar.

Anvisningen ägs av Stadsledningskontorets avdelning för it och digitalisering och ingår som en del i förvaltningsobjektet Gemensam Infrastruktur (GI).

Dokumentet förvaltas löpande av St: Erik kommunikation på uppdrag av GI (SLK).

För frågor om dokumentets innehåll kontakta St: Erik kommunikation eller förvaltningsledaren för GI (SLK)

Anvisningen beskriver följande:

- Övergripande ~~vilka~~ kommunikationsteknologier som kan beställas för IoT-lösningar
- Vilka faktorer som spelar roll när du ska välja kommunikationsteknologi (olika teknologier passar bra vid olika tillfällen)
- Att du alltid bör rådfråga St: Erik kommunikation innan upphandling av IoT-utrustning (utrustning och kommunikationssätt hänger tätt ihop)
- Vägledning till hur du beställer datakommunikation för din IoT-lösning
- Dokumentets relation till andra styrande dokument i Staden

Anvisningen har tagits fram av Projektet Tekniska förutsättningar inom ramen för Programmet Stockholm som Smart och uppkopplad stad. Dokumentets huvudförfattare är Carl Wahlin (St: Erik kommunikation), Tommy Lundblad (Stadsledningskontoret avdelningen för It och digitalisering) och Tomas Wiiand, Programarkitekt Smart och uppkopplad stad
Övriga projektmedlemmar har granskat och bidragit med input.

Dokumentet har vidare granskats av programkontoret och därefter överlämnats till Stadsledningskontorets avdelning för it och digitalisering.

2 Bakgrund

Datakommunikation är en grundförutsättning för att IoT-enheter ska kunna kommunicera med sin omvärld. Stockholms stad har via AB Stokab ett väl utbyggt fibernät och via S:t Erik Kommunikation AB ett eget datakommunikationsnätverk. Genom dessa fasta förbindelser, samt via mobilbaserade datakommunikation, ansluter stadens verksamheter sina it och IoT-lösningar på ett säkert sätt till varandra, till gemensamma resurser och till internet.

IoT är viktigt för staden i utveckling mot målet om att Stockholm ska bli världens smartaste stad år 2040. Under våren 2017 beslutade Kommunfullmäktige att realisera strategin för Stockholm som smart och uppkopplad stad (Dnr 171-908/2016). Strategin fastslår ett antal principer för genomförande, däribland att öppna standarder ska användas. Dessa principer är vägledande för hur datakommunikation och IoT-lösningar tas fram, implementeras och används.
Denna anvisning ska därför ses i ljuset av dessa principer, vilka bland annat syftar till att säkerställa hög säkerhet underlätta vidareutveckling, möjliggöra byte av leverantör, samt bidra till stadsövergripande kostnadseffektivitet.

Övriga styrande dokument, samt dokument som kan vara användbara:

- *Målarkitektur IoT v.1.0*
- *Anvisningar för nätverksansluten utrustning v.0.711*
- *Hur fungerar stadens nätverk*
- *Riktlinje Informationssäkerhet* DNR 307-1396/2014, (se särskilt avsnitt 7.2)

3 Förutsättningar

Den infrastruktur för datakommunikation som finns via stadens egna nät och ansvaras av S:t Erik Kommunikation AB, ska fortsätta att användas som bas för en vidare utbyggnad till att skapa en fullt uppkopplad stad[1]. Denna befintliga infrastruktur kommer att behöva byggas ut och eventuellt kompletteras för att en full utbyggnad av uppkopplade ting ska kunna genomföras effektivt. Detta sker genom att tillföra fler anslutningsplatser till stadens egna nät i stadsmiljön samt tillföra flera möjligheter för trådlös uppkoppling.

3.1 Omfattning

Anvisningarna i detta dokument gäller i första hand hur platser i stadsmiljön som inte är uppkopplade ska kunna få en etablerad infrastruktur för datakommunikation.

Riktlinjerna gäller de ting som stadens förvaltningar och bolag vill koppla upp och nyttja, dvs ting som Stockholms stad på något sätt kontrollerar eller äger. För att nyttja data från andra organisationers eller individers uppkopplade ting, kan eventuellt alternativa sätt användas än de beskrivna i detta dokument.

[1] ”*IT-infrastruktur för kommunikation*” Strategin för en smart och uppkopplad stad - IT-infrastruktur för kommunikation, avsnitt 4.1.2

4 Behov

En smart stad kommer att ha olika behov av infrastruktur för datakommunikation beroende på användningsområde och vilka förutsättningar platsen har för uppkoppling/anslutning till nätet. I Staden kommer datakommunikationen för uppkopplade ting ske via en blandning av både trådad och trådlös datakommunikation.

Valet av infrastruktur, speciellt med fokus på datakommunikation, måste balansera mellan en rad krav som kan vara motstridiga. Exempelvis räckvidd, säkerhet, elförbrukning, bandbredd, tillförlitlighet, kostnad, fördröjning (latency) och avstånd mellan sändare.

Viktigt för datakommunikation i en smart stad är bland annat:

- Utvalda teknologier måste uppfylla alla verksamheters behov för att så långt som möjligt undvika de inlåsningseffekter som kan uppstå vid nyttjandet av leverantörsspecifika sensorer och datakommunikationsteknologier.
- Livslängden på vald teknologin i förhållande till övrig fysisk infrastruktur. Dvs om vald teknologi är beroende av annan fysisk infrastruktur som t.ex. en belysningsstolpe har livslängden på stolpen betydelse för valet av teknologi.
- Finansieringsmodell - hur delas och byggs infrastruktur ut så att kostnaden kan delas mellan verksamheterna som utnyttjar den?
- Flexibilitet att kunna byta ut teknologier och kunna utnyttja samma teknologi för flera ännu inte kända behov.
- Innovationsmöjligheter - då flera teknologier erbjuder eller kommer erbjuda ytterligare tjänster förutom bara datakommunikation som t.ex. positionering.
- Valet mellan licenserade och olicensierade teknologier.

Viktigt att tänka på är att övriga delar av IoT-lösningarna kan förändra behovet av infrastrukturen. Om t.ex. mera hantering av data sker i tingen, Edge, kan behovet av infrastruktur förändras.

S:t Erik Kommunikation AB tillhandahåller olika datakommunikationslösningar. I takt med att datakommunikationslösningar blir standardiserade och nya tekniker blir tillgängliga kommer S:t Erik Kommunikation ABs utbud förändras. S:t Erik Kommunikation AB ska även rådfrågas i de fall tillhandahållen datakommunikationslösning inte passar verksamhetens specifika tillämpning.

Stadens datakommunikationsnät är flexibelt och innehåller flera säkerhetsfunktioner. Det är logiskt separerat i olika säkerhetszoner beroende på stadens eller verksamhetens specifika krav. Det betyder i praktiken att verksamheten kan få en skräddarsydd nätlösning med de krav på säkerhet och separation som verksamheten behöver.

Verksamheten ska utgå från anvisningarna i detta dokument vid kravställning mot leverantörer av IoT-enheter. Kraven och rekommendationerna är framtagna för att möjliggöra säker anslutning av IoT-enheter till stadens gemensamma datakommunikationsnät och IoT-plattform.

5 Datakommunikationstekniker

Båda trafikriktningarna är viktiga för att både kunna hämta in sensordata och för att kunna styra utrustning samt ha möjlighet att uppdatera mjukvara i enheterna. IP-buren trafik är att föredra eftersom det redan idag används i hela stadens datanät.

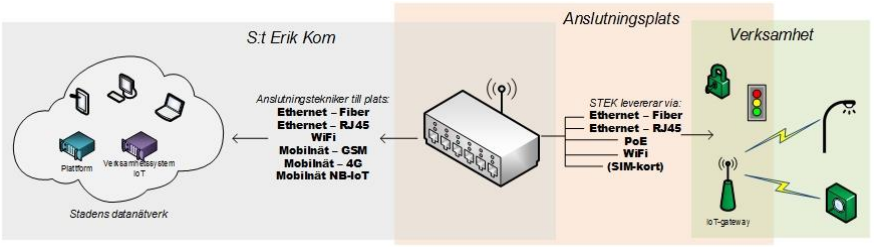
Anslutning med fasta nät bör alltid beaktas. Stadens nät finns i de flesta fastigheter där staden idag har verksamhet och även i delar av stadsmiljön. Fasta nät i form av TP-kabel eller fiber ger alltid högre kvalitet och tillgänglighet än radioburna tekniker.

För mobila IoT-enheter, batteridrivna enheter, eller enheter som är placerade där anslutning via fasta nät inte är möjlig kan licenserade lösningar via mobiloperatörers nät vara ett alternativ. 4G, GSM, LTE-M och NB-IoT har alla olika egenskaper där behov av bandbredd, svarstider och strömförbrukning spelar in.

Stadens WiFi-nät kan också användas för sensorer samt styr- och reglerteknik. WiFi bygger på fria radiolicensband där det kan förekomma störningar. Det är därför också viktigt att staden inte bygger upp flera parallella infrastrukturer som använder samma frekvensband.

S:t Erik Kommunikation väljer en anslutningsteknik tillsammans med verksamheten baserat på verksamhetens behov av bandbredd, svarstider, SLA samt kostnad. Idag levereras datakommunikation till anslutningsplats via ethernet fiber/RJ45, WiFi eller via mobilnätet. Verksamheten kan sedan ansluta sin egen utrustning via ethernet fiber/RJ45 (med eller utan PoE), WiFi eller ett simkort som placeras i verksamhetens enhet. S:t Erik Kommunikation tar ansvar för leveransen fram till där verksamhetens IP-baserade enhet eller Edge Gateway kopplas in på anslutningsplatsen.

I de fall där verksamheten behöver ett lokalt trådlöst spridningsnät via en Edge Gateway för lokala funktioner kan verksamheten i vissa fall behöva ansvara för detta själva. S:t Erik Kommunikation bör medverka i diskussioner vilken typ av lokal datakommunikationsteknik som är lämplig för verksamhetens behov. S:t Erik Kommunikation tar även ansvar för att datakommunikationen genom stadens datanät sker på ett säkert sätt enligt de krav som ställs enligt informationsklassning av datat.



De anslutningstekniker S:t Erik Kommunikation levererar till anslutningsplatsen är vedertagna och standardiserade tekniker.

Inom IoT finns idag en mängd olika anslutningstekniker. Allt eftersom nya tekniker blir standardiserade kommer nya anslutningstekniker undersökas och eventuellt läggas till utbudet.

6 Riktlinjer

6.1 Inköp av kommunikationstjänster

S:t Erik Kommunikation tillser stadens samlade behov av datakommunikation i enlighet med kommunfullmäktiges beslut från 2008. Denna princip gäller även datakommunikation till IoT-enheter[2].

Krav

- S:t Erik Kommunikation ska alltid kontaktas när verksamheten har behov av datakommunikationslösningar.

6.2 IP-baserad datakommunikation

I stadens gemensamma nätverk används IP-baserad datakommunikation. IP-nätet gör att enheterna går att nå och övervaka på distans och går att kommunicera med direkt från centrala system.

Med IP-baserad datakommunikation kan befintliga funktioner för segmentering och säkerhet i stadens nätverk även användas för IoT-enheter. Chansen ökar också att enheter som är förberedda för att fungera på ett LAN/WAN nätverk har standardiserat stöd för bland annat autentisering och kryptering.

Att tilldela enheter IP-adress via DHCP ger många administrativa fördelar. Förutom att installatören inte behöver konfigurera enheten med en IP-adress, eller att IP-adressen måste konfigureras om vid nätförändringar, kan enheter anropas via FQDN (Fully Qualified Domain Name) i stället för en IP-adress.

Krav

- Utrustning som ansluts mot stadens datanät ska kommunicera via IP och ska använda överenskommen anslutningsteknik.

Rekommendationer

- I de fall där så är möjligt bör ingående komponenter använda IP-baserad datakommunikation.
- Om möjligt bör DHCP för tilldelning av IP-adress till enheter användas.

[2] Stockholm stads *Strategi för en smart och uppkopplad stad* avsnitt 4, 4.2.1

6.3 Mobil datakommunikation

I de fall licenserad mobil datakommunikation, t.ex. 4G eller NB-IoT, används finns möjligheten att ansluta enheterna via APN, Access Point Name. Detta möjliggör att enheterna kan adresseras som enheter på Stadens egna när samt att dess IP-adresser inte blir publika. Detta innebär att centrala system som ska ha åtkomst till dessa enheter kan kommunicera direkt med dessa utan att passera internet förutsatt att brandväggarna tillåter detta.

Nyttjande av APN möjliggör användande av stadens övriga säkerhetsfunktioner för datakommunikation, tex brandväggar och webbfilter. Data från/till enheterna behöver inte heller passera stadens internetförbindelser utan går direkt via redundanta förbindelser till mobilnätsoperatören.

Krav

- APN kan beställas via stadens telefoniavtal och sker i samråd med S:t Erik Kommunikation.

Rekommendationer

- Nyttjande av APN bör övervägas, framför allt om enheterna av säkerhetsskäl ej bör placeras direkt på internet

6.4 Säkerhet

Stockholm stads strategi för Smart Stad fastställer att data som samlas in för ett syfte vid en tidpunkt senare kan komma att nyttjas för andra syften.[3] Data ska vara öppen och delad och ska kunna nyttjas på nya kreativa sätt i framtiden som kanske inte alltid går att förutse vid det tillfälle då data började samlas in.

Verksamheten måste redan från början blicka framåt mot en framtid där t.ex. aggregerade data från IoT-sensorer används i verksamhetssystem, oavsett vad originalsyftet med datainsamlingen var från början. Data kan komma att nyttjas antingen för beslutsunderlag eller till automatiserade system där sensordata styr system, miljöer och flöden.

Enligt stadens riktlinje för informationssäkerhet ska alla informationstillgångar klassas för att få rätt skyddsnivå[4]. Det gäller även den datainsamling som sker inom ramarna för Smart Stad och

[3] Stockholm stads *Strategi för en smart och uppkopplad stad* avsnitt 1, 4.2.1, 4.2.2, 5.1 princip 6

[4] Stockholms stads *Riktlinje Informationssäkerhet* DNR 307-1396/2014, avsnitt 7.2, samt *Handbok för informationsklassning*

IoT-lösningar. Klassning ska utföras med hjälp av verktyget KLASSA.

Klassningens resultat avgör vilka säkerhetskrav som riktas mot IoT-lösningen gällande bland annat datakommunikation.

Klassningsresultatet tillsammans med vilka verksamhetsbehov IoT-lösningen har för sin datakommunikation avgör vilka säkerhetsfunktioner som kan behöva tillämpas.

I stadens datakommunikationsnätverk finns möjligheten att logiskt separera enheter och system från varandra. I många fall kommer klassningen av informationstillgångar göra att enheter och ting hamnar i gemensamma IoT-nät. I andra fall kan säkerhetskraven från klassningen innebära att IoT-enheterna måste anslutas till helt eller delvis isolerade nät.

Säkerhetsanvisningar kan ofta uppfyllas antingen av funktioner i nätverket eller i de ting, applikationer och system som lösningen består av. Exempelvis kan kryptering hanteras antingen som en funktion i nätverket, eller som en inbyggd del i IoT-enheternas datakommunikation. Den verksamhet som implementerar en IoT-lösning ansvarar för att anvisningarna uppfylls av någon del av helhetslösningen.

Om inte IoT-enheter själva kan hantera funktioner för autentisering och kryptering kan datakommunikationsnätverket i vissa fall hantera dessa funktioner åt IoT-lösningen. Det ställer då krav på att IoT-enheterna klarar av nödvändiga funktioner såsom 802.1x autentisering.

Krav

- Data som samlas in via enheter klassas enligt stadens riktlinjer för informationsklassning
- Klassningen och IoT-lösningens funktionalitetsbehov används för att ge enheten rätt nätverksåtkomst i samråd med S:t Erik Kommunikation