



## » kryptering «



### » översikt

Har Du också funderat över om informationen Du skickar via radiomodem kan avlyssnas? Allt som sänds i luften kan avlyssnas, men det finns nu en bra krypteringsenhet som gör informationen omöjlig för utomstående att tyda. Modulen kan anslutas till befintliga radiomodemsnät eller vid installation i nya nät.

Modulen, en kompakt svenskutvecklad lösning, kopplas snabbt in mellan radiomodem och utrustning och skyddar Ditt system mot avlyssning eller angrepp utifrån.

Installationstiden är minimal, kostnaden lika så. Det finns ingen anledning att vänta, kontakta oss redan idag!

Idag går utvecklingen snabbt och kraven på pålitlig och säker dataöverföring ökar. Med ett väl designat och testat radionät får Du ett system med få omsändningar och en lång problemfri drifttid, en perfekt grundsten för hög säkerhet.

Radiomodemen i Sateline-serien kommunicerar trådlöst över stora ytor och används ofta i infrastrukturella system. Därför är det extra intressant att informationen inte går att avlyssna. Därför introducerar vi nu en krypteringsmodul som går att använda i såväl gamla som nya radiomodemsnät.



### » avlyssning

I praktiken är det svårt men möjligt att avlyssna ett radiomodemssystem eftersom det inte helt går att avskärma utomstående. Om avlyssning skulle inträffa är det dock inte säkert att mottagaren kan hantera den uppfattade informationen eftersom den ofta härstammar från styr- eller övervakningssystem som få har tillgång till. Du har säkert läst artiklarna och sett nyhetsinslagen på TV om W-LAN (trådlösa nätverk) som lätt avlyssnas. Detta beror på att de flesta systems kryptering inte aktiverats, ofta eftersom installationen av krypteringsnyckeln är svår och därmed struntar många i att använda den.



### » risker

De största teoretiska riskerna är idag antingen att någon skulle avlyssna och samla in informationen, eller att systemet skulle matas med information från en "falsk" enhet vilket leder till att felaktig information erhålls hos mottagaren. För att undvika dessa situationer kan vi erbjuda en svenskutvecklad säkerhetsmodul som ansluts mellan kabel och radiomodem. Med lösningen får man både kryptering och autentisering, dvs man både skyddar informationen från avlyssning och tillåter att endast identifierade och i förväg godkända enheter kan skicka respektive ta emot informationen.



## » kryptering

Krypteringen sker med 168 bitars 3DES (Data Encryption Standard), vilket är en av världens mest beprövade krypteringsalgoritmer och specificerad av USAs standardiseringsinstitut NIST (NIST FIPS PUB 46-3). Utbyte av nycklar och automatisk identifiering för att säkerställa att rätt sändare kommunicerar med rätt mottagare sker med så kallad system SKG teknologi (Synchronous Key Generator).

Detta innebär att ingen information kan avlyssnas och inte heller kan en okänd eller falsk enhet utge sig för att vara en sändare i nätet. Således erhålls en mycket hög säkerhetsnivå och man kan därmed på ett effektivt och tryggt sätt utnyttja den trådlösa kommunikationens alla fördelar.

## » uppbyggnad

Systemet består av en adapter kallad LSM som kopplas mellan radiomodemet och utrustningen som den är ansluten till. Modulen aktiveras genom att en krypteringsnyckel laddas ned från en PC. Alla enheter i systemet konfigureras med en krypteringsnyckel. För att uppnå extra hög säkerhet kan automatiskt nyckelbyte på alla enheter genomföras utan att omkonfiguration är nödvändig. Efter en inledande synkronisering av kommunikationen sker utbytet av data transparent och med bibehållen dataöverföringshastighet.

## » undvik attacker

I höstas släppte ett forskarteam på British Columbia Institute of Technology en rapport som visar på en tiofaldig ökning av framgångsrika attacker inom process, övervakning och datainsamling. Många av de attackerade systemen hanterade kritiska samhällsfunktioner som elförsörjning, oljeraffinaderier, vattenförsörjning, transporter och kommunikation. Dessa system har historiskt sett ofta varit betraktade som immuna mot externa attacker då de varit baserade på specialanpassad teknik och isolerade från övriga IT-system. Rapporten visar dock tydligt på att en ny situation har uppstått och att man därför måste tänka om och inkludera säkerheten även i de minsta komponenterna.

## » agera redan idag

För att undvika att Ditt system avlyssnas rekommenderar vi att Du redan nu tittar igenom säkerheten och utvärderar att installera en krypteringsenhet. Kostnaden för denna är försumbar om Du jämför med nyttan den gör.

